Хмельницький національний університет
Міністерство освіти і науки України

Хмельницький національний університет
Міністерство освіти і науки України

Кваліфікаційна наукова праця
на правах рукопису

КАШТАЛЬЯН АНТОНІНА СЕРГІЇВНА

УДК 004.7:004.75:004.49:004.62

ДИСЕРТАЦІЯ

ЕЛЕМЕНТИ ТЕОРІЇ ТА ПРАКТИКИ СТВОРЕННЯ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК В КОРПОРАТИВНИХ МЕРЕЖАХ

05.13.05 - комп'ютерні системи та компоненти

(12 Інформаційні технології)

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Подані до захисту наукові положення є власним напрацюванням. Всі використані ідеї, наукові результати, цитати супроводжуються належними посиланнями на їх авторів та джерела опублікування. Всі частини тексту дисертації, під час написання яких використовувалися технології штучного інтелекту, перевірені та відредаговані особисто.

_____ А. С. Каштальян
(підпис)

Науковий консультант: Савенко Олег Станіславович, доктор технічних наук, професор

Ідентичність примірників дисертації
засвідчую Вчений секретар СВР Андрій Мєхоров

Хмельницький – 2025

АНОТАЦІЯ

Каштальян А. С. Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 - комп'ютерні системи та компоненти (12 - Інформаційні технології). – Хмельницький національний університет, Хмельницький. 2025.

Вирішення науково-прикладної проблеми щодо неефективного функціонування та прогнозування поведінки зловмисниками мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж в частині зміни архітектури систем та їх центрів прийняття рішень з врахування попереднього досвіду із виконання таких змін для узгодження дій щодо заплутування зловмисників з архітектурою окремих засобів, які є частиною систем, для уникнення подій, при яких система готує певні відповіді, а її автономні частини при впливах на вузли в мережах, в яких вони розміщені, реагують на ці ж події по різному, тобто наявність розбалансування дій, а також забезпечення різних варіантів відповідей на повторювані зловмисні дії узгодженням дій всіх частин систем і прийняття рішень без залучення адміністратора є актуальним напрямом дослідження.

У дисертації здійснено аналіз методів синтезу обманних мультикомп'ютерних систем з приманками і пастками, класифікацію обманних систем, аналіз моделювання зловмисних загроз з використанням приманок, аналіз методів організації функціонування обманних систем та методів виявлення зловмисного програмного забезпечення і комп'ютерних атак з використанням приманок і пасток. В роботі запропонована концепція вирішення науково-прикладної проблеми, яка полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень в корпоративних мережах, розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним

атакам, розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик, запропоновано розроблені математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для вибору наступних варіантів централізації, розроблено метод визначення варіанту централізації в мультикомп'ютерних системах для вибору наступного варіанту централізації за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, розроблено метод організації функціонування контролера прийняття рішень для забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, розроблено метод організації функціонування мультикомп'ютерних систем для забезпечення спроможності систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки.

Об'єкт дослідження – процес синтезу мультикомп'ютерних систем антивірусних комбінованих приманок та пасток для виявлення зловмисного програмного забезпечення і комп'ютерних атак в корпоративних мережах.

Предмет дослідження – принципи, методи і мультикомп'ютерні системи антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж.

Метою дисертаційного дослідження є покращення функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Наукова новизна отриманих результатів полягає в наступному:

1) вперше запропонована концепція вирішення науково-прикладної проблеми, яка полягає у поєднанні та синтезі в системах таких визначальних властивостей, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних приманок і пасток в системі, що дає змогу синтезувати мультикомп'ютерні системи антивірусних комбінованих приманок і пасток в корпоративних мережах, які будуть автономними, складними в прогнозуванні їх наступних кроків та розуміння їх принципів функціонування зловмисниками, для покращення виявлення та протидії ЗПЗ і КА;

2) вперше розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, особливістю якого є вимоги щодо наявності в архітектурі систем контролера прийняття рішень та спеціалізованого функціоналу, що дає змогу впливати на рішення систем щодо їх наступних кроків та зміни архітектури і в результаті це ускладнить для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращить виявлення та протидію ЗПЗ і КА в корпоративних мережах;

3) вперше розроблено концептуальну модель мультикомп'ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також забезпечує стійкість систем при вилученні певних вузлів в корпоративних мережах та при поєднанні спеціалізованого функціоналу із

основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

4) розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах;

5) розроблено новий метод визначення варіанту централізації в мультикомп'ютерних системах, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, і який на відміну від відомих методів дає змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і обрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі;

6) вперше розроблено метод організації функціонування контролера прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

7) розроблено новий метод організації функціонування мультикомп'ютерних систем, який на відміну від відомих, дає змогу забезпечити можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а

також виокремлення контролера прийняття рішень та центру систем, що забезпечило багатоваріантність при опрацюванні відповіді на події, які викликані зовнішніми та внутрішніми впливами на системи в корпоративних мережах;

8) розроблено новий метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому на відміну відомих методів, здійснено збір даних та кластеризацію схожих зловмисників з використанням мультикомп'ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА;

9) розроблено новий метод виявлення ЗПЗ і КА, який, на відміну від відомих методів, реалізується в архітектурі мультикомп'ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи), що забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, підвищує ефективність протидії.

Практичне значення отриманих результатів. У результаті виконаного дисертаційного дослідження розроблено архітектуру і компоненти мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, здійснено їх реалізацію. Результати експериментальних досліджень підтверджують ефективність розроблених засобів, а також правильність наукових положень теорії розподілених систем, оскільки впровадження мультикомп'ютерної системи дозволяє підвищити достовірність виявлення на 3–9 % порівняно з відомими аналогами за мультиплікативним та адитивним критеріями, які враховують метрики сукупно щодо систем та хибних об'єктів атак. Встановлено, що з початку функціонування системи з контролером

прийняття рішень її інтегрований показник щодо стійкості та рівноваги становить більше 65% та зростає з часом її експлуатації, для критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи відхилення між крайніми значеннями цільової функції при штатному функціонуванні мультикомп'ютерної системи становить 3%, а при впливі на параметри одного з чотирьох критеріїв максимальне відхилення дорівнює 7% в момент впливу і в подальшому система функціонує стабільно при виконанні перебудови центру, при визначенні варіанту централізації за наявності у складі системи контролера прийняття рішень значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера, тобто за рахунок використання контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання. Крім того, розроблені правила вибору наступного варіанту виконання завдання та наступного варіанту централізації в системі забезпечують стабільність функціонування системи. При визначенні подальших кроків системи за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування було встановлено, що дисперсія відхилень між двома випадками з наявним контролером прийняття рішень і без нього становить приблизно 60% на користь системи з контролером, середнє арифметичне значення достовірності виявлення для всіх класів ЗПЗ з метаморфним функціоналом дорівнює $TPR = 75.46\%$ для тієї множини вірусів, які залишались невиявленими в досліджуваному операційному середовищі після їх проходження через системи виявлення вторгнень та антивірусні засоби, а відхилення від цього значення всіх значень розроблених дванадцяти класів не перевищує 3%, що загалом дає змогу досягти достовірності виявлення при багатоетапній перевірці до 98,8 % для всієї множини ЗПЗ з метаморфним функціоналом.

Теоретичні та практичні результати роботи впроваджено в ТОВ «ІТТ – telecommunication company» (м. Хмельницький, акт про впровадження від 10.04.2025 р.), ПП «Нолт Технолоджис» (м. Хмельницький, акт про впровадження від 15.04.2025 р.), Приватному підприємстві «Авіві» (м. Хмельницький, довідка про впровадження від 18.06.2025 р.), ТОВ «ЮКС+» (м. Хмельницький, акт про впровадження від 17.06.2025 р.), відділ протидії кіберзлочинам в Хмельницькій області Департаменту

кіберполіції Національної поліції України (м. Хмельницький, довідка про впровадження від 24.06.2025 р.), впроваджені та використовуються в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності 123 Комп'ютерна інженерія, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Теорія і технології проєктування спеціалізованих операційних систем», «Безпека та захист комп'ютерних систем» (акт про впровадження від 16.04.2025 р.), Західноукраїнському національному університеті при викладанні дисциплін на кафедрі кібербезпеки для спеціальності 125 Кібербезпека та захист інформації в курсах «Дослідження і проєктування систем захисту інформації», «Теорія і технології проєктування спеціалізованих операційних систем», «Безпека комп'ютерних та кіберфізичних систем» (акт про впровадження від 16.06.2025 р.), Національному університеті водного господарства і природокористування при викладанні дисциплін для спеціальності 125 Кібербезпека та захист інформації в курсах «Основи кібербезпеки», «Комплексні системи захисту інформації», «Виявлення вразливостей та тестування безпеки інформаційних систем» (довідка про впровадження від 14.03.2025 р.).

У вступі представлено обгрунтування актуальності науково-прикладної проблеми з покращення ефективності функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора. Також, представлено зв'язок тематики дослідження з напрямками наукових досліджень дослідників цієї проблеми в світі та подано основні наукові результати роботи, її практичне значення, перелік підприємств та установ, в яких впроваджено результати роботи.

У першому розділі здійснено аналіз предметної області дослідження, аналіз методів синтезу обманних мультикомп'ютерних систем з приманками і пастками, класифікацію обманних систем, аналіз моделювання зловмисних загроз з

використанням приманок, аналіз методів організації функціонування обманних систем та методів виявлення зловмисного програмного забезпечення і комп'ютерних атак з використанням приманок і пасток. Також, підведено підсумки проведеного аналізу та здійснено постановку науково-прикладної проблеми дослідження.

У другому розділі запропоновано концепцію вирішення науково-прикладної проблеми, яка полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для покращення ефективності виявлення зловмисного програмного забезпечення і комп'ютерних атак в корпоративних мережах, розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам, розроблено концептуальну модель мультикомп'ютерних систем, особливістю на основі визначальної характеристики, що відповідає за здійснення контролю прийнятих рішень, та решті визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі визначальних характеристик в архітектурі систем.

В третьому розділі розроблені нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які необхідні для вибору наступних варіантів централізації, та подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи, новий метод визначення варіанту централізації в системах, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану.

В четвертому розділі вперше розроблено метод організації функціонування контролера прийняття рішень для забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання

завдання, рівнів безпеки компонент системи, кількості компонент та зв’язків між ними, розроблено новий метод організації функціонування мультикомп’ютерних систем для забезпечення спроможності систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв’язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролера прийняття рішень та центру системи.

У п’ятому розділі розроблено метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснено збір даних та кластеризацію схожих зловмисників з використанням мультикомп’ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА, а також розроблено метод виявлення зловмисного програмного забезпечення та комп’ютерних атак, який реалізується в архітектурі мультикомп’ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи), що забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, підвищує ефективність протидії.

У шостому розділі здійснено постановку експериментів для реалізованого варіанту мультикомп’ютерних систем з комбінованими антивірусними приманками і пастками, проведено експериментальні дослідження щодо різних частин архітектури та щодо перевірки ефективності розроблених методів.

У висновках представлено отримані наукові та практичні результати дослідження.

У додатках представлено наукові публікації, в яких відображено наукові результати роботи, акти впровадження результатів роботи, лістинг програмного забезпечення, таблиці з результатами експериментів.

Ключові слова: мультикомп'ютерні системи, корпоративні мережі, приманки, пастки, розподілені системи, комп'ютерні мережі, прийняття рішень, зловмисне програмне забезпечення, комп'ютерні атаки, кластеризація.

ANNOTATION

Kashtalian A. S. Elements of the theory and practice of creating multicomputer systems of combined anti-virus baits and traps in corporate networks. – Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Technical Sciences in the specialty 05.13.05 - Computer Systems and Components (12 - Information Technologies). – Khmelnytskyi National University, Khmelnytskyi. 2025.

Solving the scientific and applied problem regarding the inefficient functioning and prediction of behavior by malefactors of multi-computer systems of antivirus combined baits and traps of detecting malicious software to ensure the safety and protection of corporate networks when changing the architecture of systems and their decision-making centers for the implementation. It is part of the systems to avoid events in which the system prepares certain answers, and its autonomous parts, when influenced by nodes in the networks in which they are placed, respond to the same events in different ways, that is, the presence of unbalanced actions, as well as providing different options for answers to repeated malicious actions.

The dissertation analyzes the methods of synthesis of deceptive multicomputer systems with decoys and traps, classification of deceptive systems, analysis of modeling of malicious threats using decoys, analysis of methods for organizing the functioning of deceptive systems and methods for detecting malware and computer attacks using decoys and traps. The paper proposes a concept for solving a scientific and applied problem, which consists in the development of elements of theory and practice creation of multicomputer systems from combined anti-virus decoys and traps and a decision controller in corporate networks,

the principle of synthesis of multicomputer systems with combined decoys and traps and a decision controller for detecting and countering malware and computer attacks has been developed, a conceptual model of multicomputer systems based on defining characteristics has been developed, and the development of mathematical models for the criteria of efficiency, stability, integrity and security relative to the center of the system for the selection of the following options for centralization, a method for determining the option of centralization in multicomputer systems has been developed for the selection of the next option of centralization according to complex criteria of efficiency, stability, integrity, security and taking into account the division of the type of architecture into centralized, partially centralized, partially decentralized and decentralized, the method has been developed organization of the functioning of the decision-making controller to ensure the choice of one option for performing the task from the options prepared and proposed for consideration by the system center, taking into account the previous experience of the system in the application of task execution options, security levels of system components, the number of components and connections between them, has been developed a method of organizing the functioning of multicomputer systems to ensure the ability of systems to independently change their properties, organize elements and components and establish connections between them, taking into account the state of functional and cybersecurity.

The object of research is the process of synthesis of multicomputer systems of anti-virus combined decoys and traps for detecting malware and computer attacks in corporate networks.

The subject of the study is the principles, methods and multicomputer systems of anti-virus combined decoys and traps for detecting malware and computer attacks to ensure the security and protection of corporate networks.

The purpose of the dissertation research is to improve the efficiency of the functioning of multicomputer systems of anti-virus combined decoys and traps for detecting malware and computer attacks to ensure the security and protection of corporate networks by synthesizing in their architecture the properties of hiding their presence, changing responses to repeated actions by the attacker, independent decision-making without the involvement of an administrator.

The scientific novelty of the results obtained is as follows:

1) for the first time, the concept of solving a scientific and applied problem was proposed, which consists in combining and synthesizing in systems such defining properties as variability of the type of system architecture, variability of the type and number of system centers, adaptability of the system to changes in external conditions, characteristic changes in the center of the system, self-organization of the system, flexibility of the system, independence in decision-making, permissible variability of influence on the system, variability in the presence of agents in the system for decision-making, control over the decisions made in the system, features of specialized functionality for combined anti-virus decoys and traps in the system, which makes it possible to synthesize multicomputer systems of anti-virus combined decoys and traps in corporate networks, which will be autonomous, difficult to predict their next steps and understand their principles of functioning by intruders, to improve the detection and counteraction of anti-virus decoys and CAs;

2) for the first time, the principle of synthesis of multicomputer systems with combined decoys and traps and a decision controller for detecting and counteracting runways and spacecraft has been developed, a feature of which is the requirements for the presence of a decision controller and specialized functionality in the architecture of systems, which makes it possible to influence the decisions of systems regarding their next steps and changes in architecture, and as a result, this will complicate the understanding of the functioning of such systems for attackers due to the formation of various the next steps of the system at the same initial states and will improve the detection and counteraction of runways and spacecraft in corporate networks;

3) for the first time, a conceptual model of multicomputer systems has been developed, a feature of which is the introduced defining characteristic responsible for the control of decisions made, and the rest of the defining characteristics, which in the process of functioning of systems should form the architecture of the system, independently synthesizing a set of individual defining characteristics in the architecture of systems, as well as specialized functionality has been allocated, which makes it possible to provide diversification of response options under the influence of intruders, spacecraft and the functioning of the runway, as well as ensures the stability of systems when removing certain nodes in corporate networks and when combining specialized functionality with the main

part of the system forms an integral system, which generally improves the effectiveness of counteraction to runway and spacecraft;

4) new mathematical models have been developed for the criteria of efficiency, stability, integrity and security in relation to the center of the system, which, in contrast to the well-known mathematical models for evaluating the centers of systems for the choice of the following options for centralization, are represented by analytical expressions, which take into account the features of the types of centralization in the architecture of systems, indicators of efficiency, stability, integrity and security in relation to the center of the system and make it possible to form on their basis the target function for evaluation of the following options for centralization in systems;

5) a new method for determining the option of centralization in multicomputer systems has been developed, in which the choice of the next option of centralization is carried out according to complex criteria of efficiency, stability, integrity, security and taking into account the division of the type of architecture into centralized, partially centralized, partially decentralized and decentralized, and which, in contrast to the known methods allows according to the rules for choosing a centralization option to evaluate each of the selected options depending on the number of active components of the systems at the current time and criteria, and to choose the next option from a large number of options without evaluating all options, which ensures performance and avoids full or significant partial enumeration of all options in a constantly changing environment*;*

6) for the first time, a method of organizing the functioning of the decision-making controller has been developed, the peculiarity of which is to ensure the choice of one option for performing the task from the options prepared and proposed for consideration by the system center, taking into account the previous experience of the system in the application of options for performing the task, the security levels of the system components, the number of components and the relationships between them, which made it possible to form polymorphic responses of the system to events, which are caused by external and internal influences in corporate networks;

7) a new method of organizing the functioning of multicomputer systems has been developed, which, in contrast to the known ones, makes it possible to provide the capabilities of systems to independently change their properties, organize elements and components and

establish connections between them, taking into account the state of functional and cybersecurity, as well as the separation of the decision controller and the center of systems, which provided multivariance in the processing of responses to events caused by external and internal impacts on systems in corporate networks;

8) a new method of finding similar intruders in a network of decoys by their behavioral characteristics has been developed, in which, in contrast to known methods, data collection and clustering of similar intruders has been carried out using multicomputer systems with anti-virus combined decoys and traps, themain stages of searching for such time series of intruder activity are the representation of series data, measuring the distance between the series, the clustering algorithm and providing different options for responding to recurring events, which increases the costs of intruders and the duration of the spacecraft;

9) a new method for detecting runways and spacecraft has been developed, which, in contrast to the known methods, is implemented in the architecture of multicomputer systems with combined anti-virus decoys and traps of various architecture and functional purpose, which can act as intelligent agents, perform several tasks simultaneously, interact with each other in the process of event processing with informing the center of the system, as well as implement a three-level model of event analysis (at the level of a separate decoy, groups of decoys and the entire system), which provides an adaptive, variable response, decision-making both at the level of decoys and the centers of the system, makes it difficult for attackers to understand the logic of its functioning and, accordingly, increases the effectiveness of counteraction.

Practical significance of the results obtained. As a result of the dissertation research, the architecture and components of multicomputer systems of anti-virus combined decoys and traps for detecting runways and spacecraft in corporate networks have been developed, and their implementation has been carried out. The results of experimental studies confirm the effectiveness of the developed tools, as well as the correctness of the scientific provisions of the theory of distributed systems, since the introduction of a multicomputer system allows to increase the reliability of detection by 3–9% compared to known analogues according to the multiplicative and additive criteria, which take into account metrics cumulatively for systems and false attack targets. It has been established that since the beginning of the operation of the system with a decision controller, its integrated indicator of stability and

balance is more than 65% and increases with the time of its operation, for the criteria of efficiency, stability, integrity and safety relative to the center of the system, the deviation between the extreme values of the target function during the normal operation of the multicomputer system is 3%, and when influencing the parameters of one of the four criteria, the maximum deviation is 7% at the time of impact And in the future, the system functions stably when performing the restructuring of the center, when determining the option of centralization if the decision controller system contains the value of the target function for all considered options by 50% less compared to the option without a controller, that is, due to the use of the decision controller, the selection of successful options for restructuring and the time for their implementation has been achieved by about 10%. In addition, the developed rules for choosing the next option for performing the task and the next option of centralization in the system ensure the stability of the system's functioning. When determining the further steps of the system due to the formation of polymorphic responses to events, taking into account previous experience in the use of answer options and functioning, it was found that the variance of deviations between two cases with and without an existing decision controller is approximately 60% in favor of a system with a controller, the arithmetic mean value of the detection reliability for all classes of malicious software with metamorphic functionality is equal $TPR = 75.46\%$ to for the set of viruses that remained undetected in the studied operating environment after their passage through intrusion detection systems and antivirus agents, and the deviation from this value of all values of the developed twelve classes does not exceed 3%, which in general makes it possible to achieve the reliability of detection during multi-stage verification up to 98.8 % for the entire set of malicious software with metamorphic functionality.

Theoretical and practical results of the work were implemented in ITT – telecommunication company LLC (Khmelnytskyi, implementation certificate dated 10.04.2025), Nolte Technologies PE (Khmelnytskyi, implementation certificate dated 15.04.2025), Aviva Private Enterprise (Khmelnytskyi, implementation certificate dated 18.06.2025), YUKS+ LLC (Khmelnytskyi, implementation certificate dated 17.06.2025), counteraction departmentcybercrimes in the Khmelnytskyi region of the Cyber Police Department of the National Police of Ukraine (Khmelnytskyi, certificate of implementation dated 24.06.2025), implemented and used in the educational process of Khmelnytskyi

National University when teaching disciplines at the Department of Computer Engineering and Information Systems for the specialty 123 Computer Engineering, in particular in the courses "Theory and Design of Computer and Cyber-Physical Systems and Networks", "Theory and Technologies of Design of Specialized Operating Systems", "Security and Protection of Computer Systems" (Implementation Act of 16.04.2025), Western Ukrainian National University when teaching disciplines at the Department of Cybersecurity for the specialty 125 Cybersecurity and Information Protection in the courses "Research and Design of Information Security Systems", "Theory and Technologies of Design of Specialized Operating Systems", "Security of Computer and Cyber-Physical Systems" (Implementation Act of 16.06.2025), National University of Water and Environmental Management when teaching disciplines for specialty 125 Cybersecurity and Information Protection in the courses "Fundamentals of Cybersecurity", "Integrated Information Security Systems", "Vulnerability Detection and Security Testing of Information Systems" (implementation certificate dated 14.03.2025).

The introduction presents a justification of the relevance of the scientific and applied problem of improving the efficiency of the functioning of multicomputer systems of anti-virus combined decoys and traps for detecting malware and computer attacks to ensure the security and protection of corporate networks due to the synthesis in their architecture of properties to hide their presence, changeability of responses to repeated actions by the attacker, independent adoption decisions without the involvement of an administrator. Also, the connection of the research topic with the directions of scientific research of researchers of this problem in the world is presented and the main scientific results of the work, its practical significance, the list of enterprises and institutions in which the results of the work are implemented are presented.

The first section analyzes the subject area of research, analyzes the methods of synthesis of deceptive multicomputer systems with decoys and traps, classifies deceptive systems, analyzes the modeling of malicious threats using decoys, analyzes methods for organizing the functioning of deceptive systems and methods for detecting malware and computer attacks using decoys and traps. Also, the results of the analysis are summed up and the formulation of the scientific and applied problem of the study is carried out.

In the second section, the concept of solving a scientific and applied problem is proposed, which consists in the development of elements of the theory and practice of creating multicomputer systems from combined anti-virus decoys and traps and a decision controller to improve the efficiency of detecting malware and computer attacks in corporate networks, the principle of synthesis of multicomputer systems with combined decoys and traps and a decision-making controller for detection and counteraction to malware and computer attacks, a conceptual model of multicomputer systems has been developed, a feature based on the defining characteristic responsible for controlling the decisions made, and other defining characteristics that in the process of system functioning should form the architecture of the system independently synthesizing a set of individual defining characteristics according to a closed route in the graph of defining characteristics in the architecture Systems.

In the third section, new mathematical models are developed for the criteria of efficiency, stability, integrity and security in relation to the center of the system, which are necessary for the selection of the next options for centralization, and are presented by analytical expressions, which take into account the features of the types of centralization in the architecture of systems, indicators of efficiency, stability, integrity and security in relation to the center of the system, a new method for determining the option of centralization in systems, in which the choice of the next option of centralization is carried out according to complex criteria of efficiency, stability, integrity, security and taking into account the division of the type of architecture into centralized, partially centralized, partially decentralized and decentralized.

In the fourth section, for the first time, a method of organizing the functioning of the decision-making controller was developed to ensure the choice of one option for performing the task from the options prepared and proposed for consideration by the system center, taking into account the previous experience of the system in the application of task execution options, security levels of system components, the number of components and connections between them, a new one was developed a method of organizing the functioning of multicomputer systems to ensure the ability of systems to independently change their properties, organize elements and components and establish connections between them,

taking into account the state of functional and cybersecurity, as well as the separation of the decision-making controller and the center of the system.

In the fifth section, a method for finding similar intruders in a network of decoys by their behavioral characteristics is developed, in which data collection and clustering of similar intruders is carried out using multicomputer systems with anti-virus combined decoys and traps, the main stages of searching for such time series of intruders' activity are the presentation of data in the series, measuring the distance between the rows, the clustering algorithm and providing different options for answering repetitive events, which increases the costs of intruders and the duration of the spacecraft, as well as a method for detecting malware and computer attacks, which is implemented in the architecture of multicomputer systems with combined anti-virus decoys and traps of various architecture and functional purpose, which can act as intelligent agents, perform several tasks simultaneously, interact with each other in the process of processing events with informing the system center, as well as implement a three-level model of event analysis (at the level of an individual decoy, a group of decoys and the entire system), which provides an adaptive, variable response, decision-making both at the level of decoys and centers of the system, makes it difficult for attackers to understand the logic of its functioning and, accordingly, increases the effectiveness of counteraction.

In the sixth section, experiments were set up for the implemented version of multicomputer systems with combined anti-virus lures and traps, experimental studies were carried out on various parts of the architecture and on checking the effectiveness of the developed methods.

The conclusions present the scientific and practical results of the study.

The appendices contain scientific publications that reflect scientific results of work, acts of implementation of work results, software listing, tables with the results of experiments.

Keywords: multicomputer systems, corporate networks, decoys, traps, distributed systems, computer networks, decision-making, malware, computer attacks, clustering.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України, або у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

1. Kashtalian A., Lysenko S., Kysil T., Sachenko A., Savenko O., Savenko B. Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*, 2025. *24*(1), 35-51. DOI: https://doi.org/10.47839/ijc.24.1.3875 (***Scopus***)

2. Kashtalian A., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*, 2025. № 1. Pp. 264-297. DOI: https://doi.org/10.32620/reks.2025.1.18 (категорія А, ***Scopus***)

3. Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil T. Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems*, 2023. № 4. Pp. 112-151. DOI: https://doi.org/10.32620/reks.2023.4.10 (категорія А, ***Scopus***, Q3)

4. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., & Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024. № 1. Pp. 152-175. DOI: https://doi.org/10.32620/reks.2024.1.13 (категорія А, ***Scopus***, Q2)

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

5. Денисюк Д.О., Савенко Б.О., Каштальян А.С., Іванченко О.В. Метод виявлення зловмисного програмного забезпечення на основі аналізу поведінкових патернів системи. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: технічні науки*. Том 35(74), №5. 2024. Ч.1. С.124-129. DOI: https://doi.org/10.32782/2663-5941/2024.5.1/19

6. Каштальян А. С. Методи організації функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток в корпоративних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*. 2025. № 1. С. 160–171. https://doi.org/10.31891/2219-9365-2025-81-19

7. Каштальян А. С. МЕТОД ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП’ЮТЕРНИХ АТАК МУЛЬТИКОМП’ЮТЕРНИМИ СИСТЕМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК. *Herald of Khmelnytskyi National University. Technical Sciences*, 2025, № *349*(2), С. 346-352. https://doi.org/10.31891/2307-5732-2025-349-50

8. Каштальян А. С. Мультикомп’ютерна система з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп’ютерних атак на основі мультиагентних технологій. *Вісник Хмельницького національного університету. Серія: Технічні науки* 2025, № *347* (1). С. 535-542. https://doi.org/10.31891/

9. Каштальян А. С. Концептуальна модель архітектури мультикомп’ютерних систем із приманками та пастками для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, №3, С. 22-31 https://doi.org/10.32782/IT/2023-3-3

10. Каштальян А. С. Критерій оперативності щодо варіантів централізації в архітектурі мультикомп’ютерних систем з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп’ютерних атак. *Herald of Khmelnytskyi National University. Technical sciences, [S. l.]*, v. 345, n. 6(2), p. 172–178, 2024. DOI: 10.31891/. Disponível em: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/995.

11. Каштальян А. С. Особливості правил формування варіантів централізації для мультикомп’ютерних систем в корпоративних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, [S. l.]*, n. 4, p. 386–393, 2024. DOI: 10.31891/2219-9365-2024-80-46. DOI: https://doi.org/10.31891/2219-9365-2024-80-46

12. Каштальян А. С. Принцип синтезу мультикомп’ютерних систем з комбінованих антивірусних приманок і пасток та контролеру прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*, 2023. № 4, С. 265–272. https://doi.org/10.31891/2219-9365-2023-76-35

13. Каштальян А. С. Характерні властивості централізації в архітектурі мультикомп’ютерних систем антивірусних комбінованих приманок і пасток. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2024, № 4, С. 112-124. DOI: https://doi.org/10.32782/IT/2024-4-14

14. Каштальян, А., Любінецький, Д. Розподілена самоорганізована система прогнозування зловмисної активності в комп’ютерних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*. 2022. №4. С. 49–57. https://doi.org/10.31891/2219-9365-2022-72-4-5

15. Каштальян А.С., Савенко О.С. Кластеризація зловмисників у комп'ютерних мережах за їх поведінковими характеристиками. *Вісник Хмельницького національного університету, технічні науки*, 2020, №6, С. 22-27. DOI: 10.31891/2307-5732-2020-291-6-22-27

16. Каштальян А.С., Савенко О.С. Покращення безпеки та модель антивірусних інтелектуальних приманок в корпоративних комп'ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*, 2020, №4, том 1, С. 33-38 DOI: https://www.doi.org/10.31891/2307-5732-2020-287-4-33-38

17. Каштальян А.С., Савенко О.С., Бельфер Р.Е. Моделі приманок в корпоративних комп'ютерних мережах з врахуванням типів зловмисних атак. *Вимірювальна та обчислювальна техніка в технологічних процесах*, 2020, №1, С.104-110. DOI: 10.31891/2219-9365-2020-65-1-16

18. Каштальян А.С., Савенко О.С., Грибинчук В.І. Моделі та типи приманок для зловмисних атак в корпоративних комп’ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*, 2020, №5, С. 45-50.

19. Продеус М.С., Нічепорук А. О., Каштальян А. С. Система моніторингу, виявлення, реагування та захисту інформації на основі Honeypot-файлів. *Central*

Ukrainian Scientific Bulletin. Technical Sciences. 2025. Issue 11(42), Part I. Pp. 56-67. URL: https://mapiea.kntu.kr.ua/pdf/11(42)_I/8.pdf

20. Регіда П.Г., Бармак О.В., Каштальян А.С., Манзюк Е.А. Концепція застосування розподілених систем для аналізу поліморфних вірусів. *Herald of Khmelnytskyi National University. Technical Sciences. 2024. № 331*(1). С. 38-43. https://doi.org/10.31891/2307-5732-2024-331-4

21. Семенюк, Б., Каштальян, А. Виявлення комп'ютерних атак із використанням 2D-CNN та соніфікації мережевого трафіку. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2025. № 1. С. 193–201, doi: https://doi.org/10.32782/IT/2025-1-26

Праці, які засвідчують апробацію матеріалів дисертації

22. Belfer R., Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes. *CEUR-WS*. – 2020. Vol. 2623. – Pp. 239-251. URL: https://ceur-ws.org/Vol-2623/paper21.pdf (Scopus)

23. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece. 2023. Pp. 1-6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416453 (Scopus)

24. Denysiuk D., Sochor T., Kapustian M., Kashtalian A., Drozd A. A method for detecting botnets in IT infrastructure using a neural network. CEUR Workshop Proceedings. 2024, 3736. Pp. 282–292. URL: https://ceur-ws.org/Vol-3736/paper21.pdf (Scopus)

25. Denysiuk D., Sochor T., Kapustian M., Kashtalian A., Savenko O. Methods for detecting software implants in corporate networks. CEUR Workshop Proceedings. 2024. 3675. Pp. 270–284. URL: https://ceur-ws.org/Vol-3675/paper20.pdf (Scopus)

26. Liubinetskyi D., Kashtalian A., Sochor T., Selskyi A., Klein O. Distributed System for Predicting Malicious Activity in Computer Networks. *CEUR Workshop Proceedings.* 2023. Vol. 3373. Pp. 401–410. URL: https://ceur-ws.org/Vol-3373/paper26.pdf (Scopus)

27. Kashtalian A. Honeypots Models in Computer Networks According to Mailcious Attacs Types. *Proceedings of VII International conference "Information Technology and*

Interactions" (IT&I-2020), 02-04 December 2020. – Taras Shevchenko National University, Kyiv. Pp. 71-73. URL: http://iti.fit.univ.kiev.ua/wp-content/uploads/ITI_Satellite_2020_Conference-Proceedings.pdf

28. Kashtalian A., Savenko O., Sachenko A. Agglomerative Clustering of Data Collected by Honeypots. *2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Cracow, Poland, 2021. Pp. 504-509. DOI: https://doi.org/10.1109/IDAACS53288.2021.9661027 (Scopus)

29. Kashtalian A., Sochor T. K-Means Clustering of Honeynet Data with Unsupervised Representation Learning. *International Workshop on Intelligent Information Technologies & Systems of Information Security. CEUR Workshop Proceedings*. 2021. Vol. 2853. Pp. 439–449. URL: https://www.semanticscholar.org/paper/K-means-Clustering-of-Honeynet-Data-with-Learning-Kashtalian-Sochor/ca7f4a13249eb5624f7df585f840a1e24f2e6ef4#citing-papers (Scopus)

30. Prodeus M., Nicheporuk A., Kashtalian A., Kapustian M., Sochor T. Honeypot-based monitoring, detection, response, and information protection framework. *Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 329-339. URL: https://ceur-ws.org/Vol-3963/paper26.pdf (Scopus)

31. Rehida, P., Savenko, O., Kashtalian, A., Sachenko, A. Malware Detection Tool Based on Emulator State Analysis. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023. Pp. 135-140. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348678 (Scopus)

32. Kozelskiy O., Kashtalian A., Stetsyuk V., Martiniuk D., Sachenko A. A model of an intelligent clustering system with an external module for the architecture of RTOS with intensive changes of states regarding their flexibility and balancing. *CEUR Workshop Proceedings*. 2025. 3899. Pp. 234–243. URL: https://ceur-ws.org/Vol-3899/paper21.pdf (Scopus)

33. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference*

on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023. Pp. 265-270. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348773 (Scopus)

34. Savenko B., Kashtalian A., Sochor T., Nicheporuk A. Self-Organized Distributed Anomaly Detection System in Computer Systems Based on The Principal Components Method. *CEUR Workshop Proceedings*. 2022. Vol. 3156. Pp. 329–351. URL: https://ceur-ws.org/Vol-3156/paper25.pdf (Scopus)

35. Semeniuk B., Kashtalian A., Martiniuk D., Drozd A., Abdel-Badeeh M. Salem. Detection of computer attacks based on sonification of network traffic *Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 252-263. URL: https://ceur-ws.org/Vol-3963/paper21.pdf (Scopus)

36. Савенко Б.О., Каштальян А.С. Модель антивірусних інтелектуальних приманок в комп'ютерній мережі. *Актуальні проблеми комп'ютерних наук. Збірник наукових праць за матеріалами XII всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2020»*. Хмельницький: ХНУ, 2020. С. 257-260. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/3-7-35.pdf

37. Савенко Б., Каштальян А., Петляк Н. Розподілені системи виявлення worm-вірусів. *2023 ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф.*, м. Ужгород, 2-4 трав. 2023 р. / НАУ, м. Київ, 2023. С. 37-39. http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

Публікації, які додатково відображають наукові результати дисертації

38. Каштальян А.С., Авсієвич В.Р., Нічепорук А.О., Савенко О.С. А. с. 124518, Україна. Комп'ютерна програма «Проміжне програмне забезпечення мультикомп'ютерних систем спеціалізованого призначення». Дата реєстрації 11.03.2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ…….. 30

ВСТУП…… 31

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ СТВОРЕННЯ мультикомп’ютерних СИСТЕМ АНТИВІРУСНИХ ПРИМАНОК ТА ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗПЗ ТА КА В КОРПОРАТИВНИХ МЕРЕЖАХ…..... 45

1.1. Поняття та особливості систем з приманками та пастками……... 45

1.2. Методи синтезу антивірусних приманок, пасток та їх мереж…… 57

1.3. Моделювання антивірусних приманок, пасток та їх мереж…… 73

1.4. Методи створення систем антивірусних приманок та пасток для виявлення ЗПЗ і КА……..…. 81

1.5. Визначення напрямів досліджень……. 101

1.6. Висновки до першого розділу…..……..……. 103

РОЗДІЛ 2. МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ МУЛЬТИКОМП’ЮТЕРНИХ СИСТЕМ КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗПЗ ТА КА У КОРПОРАТИВНИХ МЕРЕЖАХ……..…… 105

2.1. Концепція та принцип синтезу мультикомп’ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах…… 106

2.2. Елементи концептуальної моделі мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА…….. 117

2.2.1. Базове подання концептуальної моделі мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень…….. 118

2.2.2. Формальне подання елементів та компонентів в концептуальній моделі мультикомп’ютерних систем…… 128

2.3. Концептуальна модель мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА…… 164

2.4. Висновки до другого розділу…… 170

РОЗДІЛ 3. МАТЕМАТИЧНІ МОДЕЛІ КРИТЕРІЇВ ОЦІНЮВАННЯ ТА МЕТОД ВИЗНАЧЕННЯ НАСТУПНОГО ВАРІАНТУ ЦЕНТРАЛІЗАЦІЇ В МУЛЬТИКОМП’ЮТЕРНИХ СИСТЕМАХ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК І ПАСТОК…….. 173

3.1. Характерні властивості централізації в архітектурі мультикомп’ютерних систем антивірусних комбінованих приманок і пасток 173

3.2. Особливості правил формування варіантів централізації для мультикомп’ютерних систем…… 182

3.3. Типи централізації в архітектурі мультикомп’ютерних систем…….. 189

3.4. Математичні моделі та критерії оцінювання варіантів централізації в архітектурі мультикомп’ютерних систем……. 200

3.5. Метод та правила визначення наступного варіанту централізації в архітектурі мультикомп’ютерних систем……. 224

3.6. Висновки до третього розділу……. 235

РОЗДІЛ 4. МЕТОДИ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ КОНТРОЛЕРА ПРИЙНЯТТЯ РІШЕНЬ ТА МУЛЬТИКОМП’ЮТЕРНИХ СИСТЕМ…….. 237

4.1. Метод організації функціонування контролера прийняття рішень…. 238

4.2. Метод організації функціонування мультикомп’ютерних систем…. 257

4.3. Висновки до четвертого розділу…… 264

РОЗДІЛ 5. ВИЯВЛЕННЯ ЗПЗ ТА КА В КОРПОРАТИВНИХ МЕРЕЖАХ МУЛЬТИКОМП’ЮТЕРНИМИ СИСТЕМАМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК……... 266

5.1. Моделі зловмисних дій та приманок…….. 267

5.2. Моделі приманок в корпоративних мережах з врахуванням типів зловмисних атак…….. 277

5.3. Метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками…… 282
5.4. Метод виявлення ЗПЗ та КА мультикомп'ютерними системи антивірусних комбінованих приманок та пасток…… 305
5.5. Висновки до п'ятого розділу……... 312
РОЗДІЛ 6. МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК І РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТІВ…… 313
6.1. Методика оцінювання ефективності мультикомп'ютерних систем антивірусних комбінованих приманок та пасток…… 313
6.2. Експериментальні дослідження запропонованих рішень…… 315
6.2.1 Перший експеримент та результати…… 316
6.2.2 Другий експеримент та результати…….. 320
6.2.3 Третій експеримент та результати…… 324
6.2.4 Четвертий експеримент та результати…… 332
6.2.5 П'ятий експеримент та результати…… 339
6.2.6 Шостий експеримент та результати…… 341
6.3 Етичні аспекти та методичні рекомендації для застосування мультикомп'ютерних систем антивірусних комбінованих приманок і пасток 344
6.4 Висновки до шостого розділу……... 348
ВИСНОВКИ…… 351
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 356
ДОДАТКИ…… 393
ДОДАТОК А. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА……... 393
ДОДАТОК Б. АКТИ ВПРОВАДЖЕННЯ…… 399
ДОДАТОК В. ДЕТАЛІЗАЦІЯ ПЕРШОГО ЕКСПЕРИМЕНТУ…… 411
ДОДАТОК Г. ДЕТАЛІЗАЦІЯ ДРУГОГО ЕКСПЕРИМЕНТУ…… 418
ДОДАТОК Д. ДЕТАЛІЗАЦІЯ ТРЕТЬОГО ЕКСПЕРИМЕНТУ…… 423
ДОДАТОК Е. ДЕТАЛІЗАЦІЯ ЧЕТВЕРТОГО ЕКСПЕРИМЕНТУ…… 429

ДОДАТОК Є. РЕЗУЛЬТАТИ ПЕРШОГО ЕКСПЕРИМЕНТУ…….. 437
ДОДАТОК Ж. РЕЗУЛЬТАТИ ДРУГОГО ЕКСПЕРИМЕНТУ…….. 442
ДОДАТОК З. РЕЗУЛЬТАТИ ТРЕТЬОГО ЕКСПЕРИМЕНТУ…….. 478
ДОДАТОК И. РЕЗУЛЬТАТИ ЧЕТВЕРТОГО ЕКСПЕРИМЕНТУ…… 484

.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CSMS (Cyber Security Management System) - система управління кібербезпекою;

IDS (Intrusion Detection System) - система виявлення вторгнень;

IP (Internet Protocol) - міжмережевий протокол;

SDN (Software-Defined Network) - програмно-конфігурована мережа;

SIEM (Security Information and Event Management) - система управління інформацією та подіями безпеки;

TCP/IP (Transmission Control Protocol / Internet Protocol) - протокол керування передаванням / міжмережевий протокол;

VPN (Virtual Private Network) - віртуальна приватна мережа.

ЗПЗ – зловмисне програмне забезпечення;

ІС - інформаційна (автоматизована) система;

КА – комп’ютерні атаки;

КС - комп'ютерна система;

ОС - операційна система;

ПЗ - програмне забезпечення;

ПЛК - програмований логічний контролер;

СУІБ - система управління інформаційною безпекою;

ШІ – штучний інтелект.

ВСТУП

Актуальність роботи. Корпоративні мережі продовжують залишатись об’єктами атак зловмисників. Для забезпечення їх безпеки від комп’ютерних атак (КА) та зловмисного програмного забезпечення (ЗПЗ) розроблено та застосовується багато різноспрямованих методів, засобів та систем. Але проблема залишається, оскільки до здійснення атак на корпоративні мережі та їх ресурси зловмисників спонукає отримання певного типу вигоди, а також недосконаліть засобів та систем попередження, виявлення та протидії таким атакам, яка розглядається зловмисниками як потенційно нескладне завдання для досягнення мети. Загальні відомості про системи та засоби забезпечення безпеки корпоративних мереж зловмисник встановлює з відомостей, які надають розробники у відкритих джерелах, а також в процесі розвідки при проведенні атак. Напротязі певного часу проведення розвідки зловмисник вивчає особливості забезпечення безпеки та захисту корпоративних мереж. Як правило засоби та системи захисту реагують на зловмисні впливи повторюваними відповідями з використанням невеликого набору команд, що дає змогу зловмисникам встановити типи, особливості та недоліки в організації захисту із застосуванням відповідних засобів та систем. Тому, потребують розроблення системи попередження, виявлення та протидії ЗПЗ та КА в корпоративних мережах, які б забезпечували різні варіанти відповідей на однакові впливи від зловмисників або однакові відповіді, але сформовані різними діями. В результаті, це б ускладнило для зловмисників розуміння функціонування систем безпеки та захисту корпоративних мереж. Крім того, такі системи забезпечення безпеки та захисту могли б містити додатково приманки та пастки для заплутування зловмисників та дослідження його поведінки.

Ученими, які проводять наукові дослідження в сфері розроблення нових методів і систем виявлення ЗПЗ та КА, систем з приманками та пастками, систем забезпечення безпеки та захисту інформації, систем стійких до зловмисних впливів, розподілених систем, є Анвар А. [39, 40, 121, 124], Бісвас Д. [52], Ванг К. [238], Віола В. [257], Гнатюк С. [243], Дудикевич В. [285], Занг Ю. [33], Золфахарі Ш. [188], Ефенді М. [44], Карпінський М. [144], Кларк А. [83], Кемпвел Р. [57], Коваленко А. [316, 317],

Корченко А. [266, 301], Корченко О. [161], Летичевський О. [158, 302], Мілов О. [266], Мухін В. [167, 183], Парк К. [220], Ров Н. [212], Сардана А. [141], Саченко А. [146, 155], Сохор Т. [147, 234], Харченко В. [148, 149, 179, 210, 221], Хофер В. [175], Хохлачова Ю. [151, 152], Фенг М. [13], Фергюсен-Вальтер К. [110], Франко Д. [18], Євсєєв С. [266] та ін.

Незважаючи на значний внесок цих досліджень у вирішення проблем забезпечення кібербезпеки та захисту інформації від зловмисних програмних впливів та КА в корпоративних мережах і значний розвиток відповідних методів, систем та засобів, проблеми в контексті різноспрямованого та різнотипового зловмисного проникнення в корпоративні мережі та їх ресурси залишаються. Зокрема, розробники комерційних систем і засобів забезпечення кібербезпеки та захисту інформації в корпоративних мережах, а також незалежні дослідницькі лабораторії з тестування цих комерційних систем, не гарантують повного захисту та безпеки, що підтверджується власниками корпоративних мереж в процесі їх експлуатації. Тому, професіонали в сфері кібербезпеки та захисту інформації рекомендують будувати системи безпеки та захисту на основі комплексних рішень. Складність забезпечення кібербезпеки та захисту інформації від зловмисних програмних впливів та КА в корпоративних мережах полягає в тому, що зловмисники постійно удосконалюють моделі здійснення загроз, вдосконалюють інструментарій та засоби досягнення мети, а також використовують відомості про засоби і системи протидії їм, оскільки адміністратори корпоративних систем забезпечують їх захист і безпеку, використовуючи переважно відомі рішення та виконуючи стандартні протоколи та алгоритми дій. Тому, типова поведінка зі сторони адміністраторів відкриває зловмисникам додаткові можливості для досягнення їх мети. Щоб урізноманітнити захист корпоративних мереж можуть бути застосовані обманні системи, включно з приманками та пастками. Зловмисникам теж відомо про наявність таких засобів і можливість їх застосування. Застосування обманних систем та засобів в корпоративних мережах може ефективно заплутувати зловмисників, чим спонукає їх до суттєвих додаткових витрат часу і ресурсів. Але такі обманні системи і засоби повинні швидко реагувати на зловмисні дії та забезпечувати повноцінну імітацію відповідей, інакше зловмисники можуть встановити їх наявність та використати їх з

високою ефективністю в своїх цілях. В зв’язку з такими особливостями та специфікою застосування обманних систем та засобів вони повинні бути непомітними для зловмисників, зокрема і тих, що перебувають в периметрі захисту корпоративних мереж, виконувати завдання самостійно без залучення адміністраторів, тобто бути адаптивними, самоорганізованими, а також реагувати на події нестандартно. Такі особливості обманних систем та засобів можуть бути реалізовані безпосередньо в їх архітектурі. Таким чином, виникає протиріччя щодо синтезу обманних систем, які для приховування свого функціонування в корпоративних мережах повинні здійснювати перебудову власної архітектури та архітектури центру прийняття рішень з врахуванням різних властивостей та типів архітектури, використання методів виявлення ЗПЗ та КА, які повинні бути імплементовані в архітектурі систем, та застосуванні приманок і пасток зі своєю різною архітектурою та методами виявлення, які повинні також мати змогу підтримувати зв’язок між собою і містити інтелектуальні компоненти, тобто мати змогу формувати мережі інтелектуальних приманок та пасток. Суть протиріччя полягає в тому, що через розподілення компонент систем та наявність окремих автономних засобів, що повинні підтримуватись системами як їх частин, зміна архітектури систем та їх центрів прийняття рішень не завжди узгоджується з архітектурою окремих засобів, які є частиною систем, що призводить до подій, при яких система готує певні відповіді, а її автономні частини при впливах на вузли в мережах, в яких вони розміщені, реагують на ці ж події по іншому, тобто наявні елементи розбалансування дій, а також забезпечення різних варіантів відповідей на зловмисні дії стикається з потребою узгодження дій всіх частин систем. Протиріччя виникає через особливості внутрішньої будови обманних мультикомп’ютерних систем, що впливає на ефективність методів виявлення, відповіді зловмиснику при атаках, реагуванні на поширення ЗПЗ.

Для розв’язання зазначених протиріч сформульовано актуальну науково–прикладну проблему щодо неефективного функціонування та прогнозування поведінки зловмисниками мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж в частині зміни архітектури систем та їх центрів прийняття

рішень з врахування попереднього досвіду із виконання таких змін для узгодження дій щодо заплутування зловмисників з архітектурою окремих засобів, які є частиною систем, для уникнення подій, при яких система готує певні відповіді, а її автономні частини при впливах на вузли в мережах, в яких вони розміщені, реагують на ці ж події по різному, тобто наявність розбалансування дій, а також забезпечення різних варіантів відповідей на повторювані зловмисні дії узгодженням дій всіх частин систем і прийняття рішень без залучення адміністратора.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, представлені у дисертації, виконувались в рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми № 1Б-2019 «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» (номер державної реєстрації: 0119U100662); держбюджетної науково-дослідної теми № 1Б-2021 «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (номер державної реєстрації: 0121U109936); держбюджетної науково-дослідної теми № 2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер державної реєстрації: 0124U000980), в яких авторка дисертації була виконавцем.

Мета і завдання дослідження.

Об'єкт дослідження – процес синтезу мультикомп'ютерних систем антивірусних комбінованих приманок та пасток для виявлення ЗПЗ і КА в корпоративних мережах.

Предмет дослідження – принципи, методи і мультикомп'ютерні системи антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж.

Метою дисертаційного дослідження є покращення функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Задачі дослідження формулюються в роботі наступним чином:

1) дослідити особливості функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж та проаналізувати ефективність роботи сучасних обманних систем з приманками та пастками, а також їх архітектуру і компоненти;

2) запропонувати концепцію вирішення науково-прикладної проблеми для покращення виявлення та протидії ЗПЗ і КА в корпоративних мережах на основі особливостей архітектури систем, організації функціонування та керування множиною приманок і пасток;

3) розробити принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА із забезпеченням ускладнення зловмисникам розуміння функціонування систем за рахунок формування різних наступних кроків систем при однакових початкових станах;

4) розробити концептуальну модель мультикомп’ютерних систем для забезпечення функціонування за їх підтримки антивірусних комбінованих приманок і пасток для виявлення ЗПЗ і КА в корпоративних мережах, попередження та протидії їх проникненню та формування архітектури систем самостійно, без залучення адміністратора, урізноманітнення варіантів відповідей від них при зловмисних впливах і забезпечення їх стійкості;

5) розробити математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, та подати їх аналітичними виразами, в яких врахувати особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи та сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах;

6) розробити метод визначення варіанту централізації в мультикомп’ютерних системах, в якому забезпечити вибір наступного варіанту централізації з великої кількості варіантів без здійснення оцінювання всіх варіантів, щоб досягти швидкодії

та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі;

7) розробити метод організації функціонування контролера прийняття рішень для забезпечення вибору одного варіанту виконання завдання із пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи для забезпечення формування поліморфних відповідей системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

8) розробити метод організації функціонування мультикомп'ютерних систем для забезпечення можливості до самостійної зміни своїх властивостей в архітектурі, організації елементів та компонентів і встановленні зв'язків між ними з урахуванням стану функційної та кібер- безпеки, а також виокремлення контролера прийняття рішень та центру системи для забезпечення багатоваріантності при опрацюванні відповіді на події, які викликані зовнішніми та внутрішніми впливами на систему в корпоративних мережах;

9) розробити метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснити збір даних та кластеризацію схожих зловмисників з використанням мультикомп'ютерних систем з антивірусними комбінованими приманками і пастками та забезпечити в ньому різні варіантів відповідей на повторювані події;

10) розробити метод виявлення ЗПЗ і КА, який реалізується в архітектурі мультикомп'ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, а також в ньому реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи) для забезпечення адаптивного, варіативного реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнення зловмисникам розуміння логіки її функціонування;

11) розробити мультикомп'ютерну систему антивірусних комбінованих приманок та пасток для підтвердження спроможності реалізації запропонованих принципу та методів синтезу таких систем, підтвердження їх практичного створення та використання в експериментальних дослідженнях для порівняння з відомими системами виявлення і впровадити розроблену систему в корпоративних мережах.

Методи дослідження. Для розв’язання поставлених задач використано основні положення:

1) теорії абстрактної алгебри для представлення концептуальної моделі мультикомп’ютерних систем антивірусних комбінованих приманок і пасток для виявлення ЗПЗ і КА в корпоративних мережах на основі визначальних характеристик систем;

2) теорії розподілених систем для побудови моделей мультикомп’ютерних систем та їх компонентів, на основі яких можуть бути розроблені програмні та апаратно-програмні засоби;

3) теорії множин і теорії графів для деталізованого подання мультикомп’ютерних систем та їх компонентів, як об’єктів дослідження;

4) методи класифікації для здійснення віднесення програмних об’єктів до класів ЗПЗ і КА;

5) теорії комп’ютерних мереж для представлення і організації функціонування мультикомп’ютерних систем та їх компонентів, зокрема її програмних та апаратно-програмних компонентів.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, успішною програмною реалізацією розробленої мультикомп’ютерної системи антивірусних комбінованих приманок і пасток для виявлення ЗПЗ і КА в корпоративних мережах, ефективним практичним впровадженням результатів дисертаційного дослідження на підприємствах, що експлуатують корпоративні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

Наукова новизна отриманих результатів полягає в наступному:

1) вперше запропонована концепція вирішення науково-прикладної проблеми, яка полягає у поєднанні та синтезі в системах таких визначальних властивостей, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності

агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних приманок і пасток в системі, що дає змогу синтезувати мультикомп'ютерні системи антивірусних комбінованих приманок і пасток в корпоративних мережах, які будуть автономними, складними в прогнозуванні їх наступних кроків та розуміння їх принципів функціонування зловмисниками, для покращення виявлення та протидії ЗПЗ і КА;

2) вперше розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, особливістю якого є вимоги щодо наявності в архітектурі систем контролера прийняття рішень та спеціалізованого функціоналу, що дає змогу впливати на рішення систем щодо їх наступних кроків та зміни архітектури і в результаті це ускладнить для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращить виявлення та протидію ЗПЗ і КА в корпоративних мережах;

3) вперше розроблено концептуальну модель мультикомп'ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також забезпечує стійкість систем при вилученні певних вузлів в корпоративних мережах та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

4) розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в

архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах;

5) розроблено новий метод визначення варіанту централізації в мультикомп'ютерних системах, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, і який на відміну від відомих методів дає змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і обрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі;

6) вперше розроблено метод організації функціонування контролера прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

7) розроблено новий метод організації функціонування мультикомп'ютерних систем, який на відміну від відомих, дає змогу забезпечити можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролера прийняття рішень та центру систем, що забезпечило багатоваріантність при опрацюванні відповіді на події, які викликані зовнішніми та внутрішніми впливами на системи в корпоративних мережах;

8) розроблено новий метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому на відміну відомих методів, здійснено збір даних та кластеризацію схожих зловмисників з використанням

мультикомп’ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА;

9) розроблено новий метод виявлення ЗПЗ і КА, який, на відміну від відомих методів, реалізується в архітектурі мультикомп’ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи), що забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, підвищує ефективність протидії.

Практичне значення одержаних результатів. У результаті виконаного дисертаційного дослідження розроблено архітектуру і компоненти мультикомп’ютерних систем антивірусних комбінованих приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, здійснено їх реалізацію. Результати експериментальних досліджень підтверджують ефективність розроблених засобів, а також правильність наукових положень теорії розподілених систем, оскільки впровадження мультикомп’ютерної системи дозволяє підвищити достовірність виявлення на 3–9 % порівняно з відомими аналогами за мультиплікативним та адитивним критеріями, які враховують метрики сукупно щодо систем та хибних об’єктів атак. Встановлено, що з початку функціонування системи з контролером прийняття рішень її інтегрований показник щодо стійкості та рівноваги становить більше 65% та зростає з часом її експлуатації, для критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи відхилення між крайніми значеннями цільової функції при штатному функціонуванні мультикомп’ютерної системи становить 3%, а при впливі на параметри одного з чотирьох критеріїв максимальне відхилення дорівнює 7% в момент впливу і в подальшому система

функціонує стабільно при виконанні перебудови центру, при визначенні варіанту централізації за наявності у складі системи контролера прийняття рішень значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера, тобто за рахунок використання контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання. Крім того, розроблені правила вибору наступного варіанту виконання завдання та наступного варіанту централізації в системі забезпечують стабільність функціонування системи. При визначенні подальших кроків системи за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування було встановлено, що дисперсія відхилень між двома випадками з наявним контролером прийняття рішень і без нього становить приблизно 60% на користь системи з контролером, середнє арифметичне значення достовірності виявлення для всіх класів ЗПЗ з метаморфним функціоналом дорівнює $TPR = 75.46\%$ для тієї множини вірусів, які залишались невиявленими в досліджуваному операційному середовищі після їх проходження через системи виявлення вторгнень та антивірусні засоби, а відхилення від цього значення всіх значень розроблених дванадцяти класів не перевищує 3%, що загалом дає змогу досягти достовірності виявлення при багатоетапній перевірці до 98,8 % для всієї множини ЗПЗ з метаморфним функціоналом.

Теоретичні та практичні результати роботи впроваджено в ТОВ «ІТТ – telecommunication company» (м. Хмельницький, акт про впровадження від 10.04.2025 р.), ПП «Нолт Технолоджис» (м. Хмельницький, акт про впровадження від 15.04.2025 р.), Приватному підприємстві «Авіві» (м. Хмельницький, довідка про впровадження від 18.06.2025 р.), ТОВ «ЮКС+» (м. Хмельницький, акт про впровадження від 17.06.2025 р.), відділ протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції Національної поліції України (м. Хмельницький, довідка про впровадження від 24.06.2025 р.), впроваджені та використовуються в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп’ютерної інженерії та інформаційних систем для спеціальності 123 Комп’ютерна інженерія, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Теорія і технології проєктування спеціалізованих

операційних систем», «Безпека та захист комп'ютерних систем» (акт про впровадження від 16.04.2025 р.), Західноукраїнському національному університеті при викладанні дисциплін на кафедрі кібербезпеки для спеціальності 125 Кібербезпека та захист інформації в курсах «Дослідження і проєктування систем захисту інформації», «Теорія і технології проєктування спеціалізованих операційних систем», «Безпека комп'ютерних та кіберфізичних систем» (акт про впровадження від 16.06.2025 р.), Національному університеті водного господарства і природокористування при викладанні дисциплін для спеціальності 125 Кібербезпека та захист інформації в курсах «Основи кібербезпеки», «Комплексні системи захисту інформації», «Виявлення вразливостей та тестування безпеки інформаційних систем» (довідка про впровадження від 14.03.2025 р.).

Особистий внесок здобувача. Всі основні результати дисертаційного дослідження, які представлені до захисту, отримані автором особисто. В роботах, опублікованих одноосібно автором, отримано наступні результати: [292] - розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень; [288, 289] - розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик; [290, 291, 293] - розроблені математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для вибору наступних варіантів централізації; [287] - розроблено метод організації функціонування контролера прийняття рішень; [145] - метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками; [287] - розроблено метод організації функціонування мультикомп'ютерних систем; [286, 288] - розроблено метод виявлення ЗПЗ та КА.

У роботах, опублікованих у співавторстві, автору належать основні ідеї, теоретична та практична розробка положень, відображених у характеристиці наукової новизни отриманих результатів, а саме: [164, 165, 201, 203, 228, 300, 308] – запропонована концепція вирішення науково-прикладної проблеми; [201] - розроблено принцип і метод синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень; [11, 186, 295, 313] - розроблено концептуальну модель мультикомп'ютерних систем на основі

визначальних характеристик; [107] - розроблені математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для вибору наступних варіантів централізації; [170] - розроблено метод визначення варіанту централізації в мультикомп'ютерних системах для вибору наступного варіанту централізації; [186, 201] - розроблено метод організації функціонування контролера прийняття рішень; [186, 201] - розроблено метод організації функціонування мультикомп'ютерних систем; [146, 147, 171, 296, 297, 298, 299] - метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками; [10, 92, 96, 172, 204, 303, 312, 314] - розроблено метод виявлення ЗПЗ і КА; [294] – розроблено програмне забезпечення мультикомп'ютерних систем.

Апробація результатів дисертації. Основні положення та результати проведених у дисертаційній роботі досліджень доповідалися та обговорювалися на 15 міжнародних та всеукраїнських конференціях, а саме: 1-th, 2-th, 3-th, 4-th, 5-th, 6-th International Workshop on Intelligent Information Technologies & Systems of Information Security IntelITSIS'2020 (Khmelnytskyi, Ukraine, June 10-12, 2020), IntelITSIS'2021 (Khmelnytskyi, Ukraine, March 24–26, 2021), IntelITSIS'2022 (Khmelnytskyi, Ukraine, March 23–25, 2022), IntelITSIS'2023 (Khmelnytskyi, Ukraine, March 22–24, 2023), IntelITSIS'2024 (Khmelnytskyi, Ukraine, March 28, 2024), IntelITSIS'2025 (Khmelnytskyi, Ukraine, April 4, 2025); 11-th, 12-th IEEE Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS'2021 (Cracow, Poland, 2021), IDAACS'2023 (Dortmund, Germany, 2023); 13th, 14th International Conference on Dependable Systems, Services and Technologies DESSERT'2023 (Athens, Greece, 2023) DESSERT'2024 (Athens, Greece, 2024); 1st International Workshop on Advanced Applied Information Technologies AdvAIT'2024 (Khmelnytskyi, Ukraine - Zilina, Slovakia, December 5, 2024); 1st International Workshop on Intelligent and CyberPhysical Systems ICyberPhyS'2024 (Khmelnytskyi, Ukraine, 28 June, 2024); VII International conference of Information Technology and Interactions IT&I'2020 (Taras Shevchenko National University, Kyiv, Ukraine, 02-04 December 2020); XII Міжнар. наук.-техн. конф. «Безпека інформаційних технологій» ITSec'2023 (НАУ, м. Київ - м. Ужгород, 2-4 трав. 2023 р.); XII всеукраїнська науково-практична

конференція «Актуальні проблеми комп'ютерних наук АПКН-2020» (ХНУ, Хмельницький, 2020 р.).

Публікації. За результатами проведених досліджень основні наукові результати опубліковано у 21 науковій праці [107, 170, 186, 201, 286, 287, 288, 289, 290, 291, 292, 293, 295, 296, 297, 298, 299, 300, 303, 308, 314], з яких 4 статті опубліковані в двох наукових журналах та індексовані у наукометричній базі Scopus [107, 170, 186, 201], 17 статей у фахових наукових виданнях України категорії Б [286, 287, 288, 289, 290, 291, 292, 293, 295, 296, 297, 298, 299, 300, 303, 308, 314]. Апробація засвідчена публікаціями 16 праць в матеріалах зарубіжних та українських конференцій [10, 11, 92, 96, 145, 146, 147, 164, 165, 171, 172, 203, 204, 228, 312, 313], з яких 13 публікацій індексовано у наукометричній базі Scopus. Опубліковано одне свідоцтво про реєстрацію авторського права на твір (програму) [294].

Структура дисертації. Дисертаційна робота складається з анотації, переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел та десяти додатків. Повний обсяг роботи містить 488 сторінок друкованого тексту, з них анотація та список публікацій здобувача – на 24 стор., зміст – на 4 стор., перелік умовних скорочень – на 1 стор., основний текст – на 325 стор., список із 317 використаних джерел – на 37 стор., додатки – на 95 стор. Дисертація містить 27 рисунків та 24 таблиці в основному тексті.

РОЗДІЛ 1.
АНАЛІЗ ПРОБЛЕМ СТВОРЕННЯ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ АНТИВІРУСНИХ ПРИМАНОК ТА ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗПЗ ТА КА В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1. Поняття та особливості систем з приманками та пастками

Ресурси корпоративних мереж та компоненти їх інфраструктури залишаються найбільш цікавими для зловмисників порівняно з рештою об'єктів комп'ютеризації [273]. Вони є найбільш поширеними та типовими [67], що спрощує їх розуміння зловмисниками і, відповідно, спонукає до зловмисних дій в них. Крім того, в контексті їх конфігурування для протидії зловмисникам вони мають власні обчислювальні ресурси, які можуть бути застосовані для забезпечення кібербезпеки та захисту інформації [266, 304]. Або вони можуть доповнені певними незначними засобами чи системами [173], які в поєднанні з наявними, можуть забезпечити належний рівень кібербезпеки в них.

До розроблюваних систем забезпечення безпеки та захисту інформації [163, 275] висуваються вимоги аналогічні типовим системам щодо якості систем [148, 149] і програмних засобів [274], керування життєвим циклом [276], гарантування в життєвому циклі [179, 277, 280], цілісності систем [278], процесів життєвого циклу систем і керування ризиками [279, 281], оцінювання процесів [284], а також спеціальні вимоги в контексті специфіки виконуваних ними завдань. Такими вимогами є вимоги щодо методів захисту і безпеки прикладних програм [282], процесів оброблення вразливостей [283], керування інформаційною безпекою [275] тощо. Проте, незважаючи на такі вимоги до систем та організації процесів в них, які визначені, зокрема в [304], систематизовані та повинні бути виконанні в процесі синтезу систем, на практиці такі системи мають недоліки в частині виконання своїх функцій із забезпечення безпеки та захисту інформації, а також власної стійкості [305, 306] щодо зловмисних впливів [298].

Для певних типів зловмисних загроз розроблені окремі засоби та системи. В корпоративних мережах засоби і системи, які розроблені для виявлення ЗПЗ та

запобігання КА тощо, комбінують для покращення кібербезпеки та захисту інформації. Зокрема, застосовують системи моніторингу загроз, брандмауери, системи виявлення вторгнень тощо, але проблема протидії зловмисним впливам залишається невирішеною, тобто вони недостатньо ефективні [286, 311] не тільки при самостійному застосуванні, а також і при поєднанні на різних етапах виявлення та протидії. Найбільшою проблемою засобів і систем виявлення [295, 302] є їх неспроможність належним чином здійснювати виявлення атак нульового дня та нових зловмисних впливів, а також здійснювати детальний аналіз поведінки зловмисника.

Перспективним напрямом для подолання проблем щодо протидії та виявлення зловмисних впливів в корпоративних мережах [296, 297] є застосування технологій та засобів обману зловмисників, які можуть здійснювати впливи ззовні та зсередини корпоративних мереж. Використання таких засобів регламентовано [307] методичними рекомендаціями в [304]. Вони здатні вирішувати завдання щодо виявлення атак нульового дня, нових зловмисних впливів та збирати дані про поведінку зловмисника з метою її подальшого аналізу. Крім того, такі системи та засоби уповільнюють роботу зловмисників, створюють відчуття небезпеки для них та спонукають зловмисників неефективно використовувати свої ресурси. Засоби та системи, функціонування яких передбачає використання обманних технологій, можуть бути поєднані та поєднуються з рештою засобів та систем забезпечення безпеки і захисту інформації в корпоративних мережах, що покращує ефективність протидії зловмисним впливам. Але проблема залишається і вимагає від розробників постійного удосконалення наявних та розроблення принципово нових засобів і систем. В контексті засобів і систем для обману зловмисників можна виокремити такі напрями для подальшого розроблення, які б могли покращити їх функціонування в цілому: технології обману в корпоративних мережах; архітектура систем обману; архітектура засобів обману. Засоби обману можуть бути окремими об’єктами в корпоративних мережах, а можуть також бути частинами чи компонентами [304] обманних систем.

Технології обману в корпоративних мережах повинні постійно оновлюватись. Зловмисники отримують інформацію з відкритих джерел щодо різних комерційних

засобів та систем з обманними технологіями, які пропонуються для корпоративних мереж, тому вони можуть їх досліджувати. А також, ефективність дослідження зростатиме особливо у випадку перебування зловмисників безпосередньо в периметрі захисту корпоративних мереж. Крім того, складним завданням для розробників обманних технологій є оцінювання їх ефективності та доцільності застосування при певних умовах. Тобто, безпосередньо самі варіанти обману мають бути різноманітними і такими, що дійсно можуть спрацювати при зловмисних впливах в корпоративних мережах. Ці варіанти обману можуть бути реалізовані безпосередньо окремими засобами обману або в архітектурі систем обману [201, 310].

Кіберобман є ключовим проактивним методом кіберстійкості [54], який створює значну плутанину у виявленні та націленні на кіберактиви. Однією з ключових цілей кіберобману є приховування справжньої особистості кіберактивів, щоб ефективно відвернути супротивників від критично важливих цілей і виявити їхню діяльність на ранніх етапах ланцюжків атак. Для його забезпечення реалізовано адаптивний захист, тобто стратегію кіберзахисту, в якій набір конфігурацій системи динамічно змінюється з метою підвищення невизначеності та складності для зловмисників, які намагаються виявити та використати вразливості. Щоб покращити кібергнучкість мереж здійснюють багатовимірний адаптивний захист на рівні мережі в повному масштабі за межами фізичних обмежень мереж шляхом використання програмно-конфігурованих мереж (SDN). Також, враховуючи зростання складності кібератак, яке знижує ефективність експертного втручання людини через його повільний час реагування, потрібно розробляти обманні засоби і системи на основі динамічного прийняття рішень [54]. Системи постійно піддаються атакам, що значно спрощує завдання зловмисникам, оскільки реагування на атаки полегшує збір інформації про організацію захисту корпоративних мереж. Це пов'язано з тим, що програмне забезпечення (ПЗ) та протоколи традиційно були розроблені для забезпечення інформативного зворотного зв'язку для виявлення та виправлення помилок, а не для приховування причин несправностей. Тому, багато традиційних засобів безпеки у відповідь на спроби вторгнень дозволяють зловмисникам легко картографувати мережі і діагностувати вразливості системи.

В корпоративних мережах з часом їх експлуатації застарілі апаратні та програмні засоби замінюються новими, тому для зловмисників поле діяльності постійно підтримується в актуальному стані [54]. В змінених оновлених апаратному та програмному забезпеченні завжди з’являються певні недопрацювання розробників в контексті вразливостей, що дає змогу зловмисникам використовувати це для своїх цілей.

Використання обманних об’єктів в корпоративних мережах потребує кваліфікованого персоналу [54] і може бути складним. Зловмисник може виявити такі об’єкти та використати їх в своїх атаках. Приманки як обманні об’єкти є ресурсами в корпоративних мережах. Вони призначені для залучення, виявлення та збору інформації про КА. Переважно вони класифікуються за рівнем взаємодії, що надається потенційним зловмисникам [54]. Приманки з низьким рівнем взаємодії [54] здійснюють надання емульованих сервісів без повної функціональності серверу з метою виявлення несанкціонованої активності за допомогою псевдосервісів, що легко розгортаються. Приманки з високим рівнем взаємодії забезпечують відносно повну систему, з якою зловмисники можуть взаємодіяти, і призначені для збору детальної інформації про КА. Незважаючи на свою популярність, приманки з низьким і з високим рівнями взаємодії часто виявляються поінформованими зловмисниками, бо мають обмежений набір послуг, що дозволяє ідентифікувати їх як приманки. Наприклад, приманки можуть демонструвати шаблони трафіку та дані, які суттєво відрізняються від справжніх сервісів. Тому, розроблення приманок як окремих обманних засобів для застосування в корпоративних мережах теж залишається актуальним завданням.

Зловмисники легко досліджують сучасний Інтернет у пошуках вразливого ПЗ. Це дозволяє їм зосередити свої атаки на вразливих цілях. Вони надсилають тестові дані (зонд), які створені для масового запуску певної відомої помилки в ПЗ на багато серверів у мережі. Виправлені сервери відповідають на зонд правильно сформованим виведенням, наприклад, повідомленням про помилку. Але сервери без виправлень поводяться нестабільно, наприклад, відповідають рядком сміття або аварійно завершують роботу та перезавантажуються. Спостерігаючи за останньою реакцією, зловмисник наступним кроком надсилає більш конструктивний зловмисний запит на

невиправлені сервери. Наприклад, такий, що використовує помилку для захоплення потоку керування ПЗ користувача, змушуючи його виконувати зловмисні дії від імені зловмисника, а не просто аварійно завершувати роботу [54]. В результаті багатократних звернень зловмисника до одного і того ж ресурсу в мережах та опрацювання ним відповідей за різними своїми запитами виникає модель зв’язку між зловмисником і об’єктом атаки, яка відповідає стратегіям в теорії ігор. Це може бути використано розробниками систем та засобів з приманками з практичної сторони в реальних системах, а також і для моделювання таких відношень.

При роботі з приманками на практиці потрібно вирішити проблеми з безпекою та продуктивністю. Приманка розгалужує увесь процес сервера для створення процесу-клона у відповідь на спроби вторгнення і, при цьому, може ненавмисно копіювати певні області в адресному просторі процесів користувачів. Зокрема, в таких областях можуть бути ключі шифрування паралельних сесій, покажчики на дочірні приманки тощо. Тоді, зловмисник отримав би потенційний доступ до секретів, які може містити приманка. Практичне впровадження приманок, також, вимагає, щоб вони майже не породжували додаткових витрат для законних користувачів, працювали достатньо добре для зловмисників без породження збоїв атак і не були помітні, пропонували високу сумісність із ПЗ, яке дозволяє мультиобробку, багатопоточність та активну міграцію з'єднань між IP. Також, віддалене розгалуження сеансів зловмисників на приманки має відбуватись в реальному часі і без помітних збоїв у цільовій програмі. Це означає, що встановлені з'єднання, зокрема, з'єднання зловмисника, не повинні бути розірвані. Крім того, розгортання приманки має бути швидким, щоб не пропонувати відкриті, надійні канали синхронізації. Всі конфіденційні дані повинні бути відредаговані, перш ніж приманка відновить виконання, щоб уникнути надання зловмиснику потенційного доступу до секретів користувача. Таким чином, необхідне забезпечення продуктивності часу, яке виключає клонування на системному рівні. Наприклад, клонування віртуальних машин [91, 244] для розгалуження сеансу. Також, може бути використана альтернатива, яка базується на міграції процесів через контрольну точку перезапуску [101]. Щоб масштабуватися до багатьох одночасних атак, може бути використана віртуалізація на рівні ОС для розгортання розгалужених процесів у

контейнери-приманки, які можуть створюватися, розгортатися та знищуватися на порядки швидше, ніж інші методи віртуалізації, такі як повна віртуалізація або паравіртуалізація [247]. Віртуалізація на рівні ОС дозволяє декільком гостьовим вузлам (контейнерам) спільно використовувати ядро свого керуючого хоста. Контейнери Linux [261] реалізують віртуалізацію на рівні ОС з управлінням ресурсами через групи управління процесами та повною ізоляцією ресурсів через простори імен Linux. Це гарантує, що процеси, файлова система, мережа та користувачі кожного контейнера залишаються взаємно ізольованими.

Міграція процесів через точку перезапуску [101] полягає в передачі запущеного процесу між двома вузлами шляхом скидання його стану на джерело та відновлення його виконання на місці призначення. Ця проблема особливо актуальна для високопродуктивних обчислень. Процес точка-перезапуск відіграє ключову роль у тому, щоб зробити концепцію щодо приманок життєздатною. Він забезпечує швидкий і безперебійний механізм для забезпечення прозорого розгалуження сеансів зловмисника та добре масштабується навіть у невеликих середовищах.

Розгалужені приманки містять оманливу файлову систему, яка не приховує всі секрети, і яка може бути пронизана дезінформацією для подальшого обману, затримки та введення в оману зловмисників.

В роботі [200] визначено дві властивості, які необхідні для успішного розгортання обманних систем на основі приманок: нерозрізненість; секретність. Нерозрізненість полягає в тому, щоб обманути зловмисника. Приманки повинні бути важко відрізнюваними від реальних об’єктів в мережах. Секретність полягає в тому, що у системі відомості про обманні об'єкти є таємницею. Таким чином, застосовується принцип Керкгоффза, згідно з яким стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а має залежати тільки від ключів. Тобто, при оцінюванні надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, що використовується, крім ключів. Тобто, безпека системи повинна полягати в секреті. Це означає відмінності між обманними об'єктами від реальних, а не факт використання обманних об'єктів. Нерозрізнення виникає через нездатність зловмисника визначити успішність атаки результатом використання невиправленої вразливості або обманного об’єкту, що

маскується під невиправлену вразливість. Абсолютної, універсальної нерозрізнюваності, ймовірно, неможливо досягти, але при цьому багато форм розрізнюваності можуть бути складними для розрізнення. Секретність базується на наборі вразливостей в обманних об’єктах. Однак повне знання зловмисником деталей архітектури та їх реалізації не розкриває, які вразливості розробник виявив і виправив. Таким чином, адаптуючи принцип Керкгоффза [200] для обману, можна визначити, що обманні об’єкти не можна виявити, навіть якщо все в системі, крім них є загальновідомим. Тобто, обман ґрунтується на чітко визначених секретах, а точніше, на наборі вразливостей у цільових застосунках. Збереження цієї різниці в конфіденційності між публічністю архітектури приманок, деталей їх впровадження і таємницею того, які саме вразливості вони демонструють, важливо для створення надійних, ефективних обманних об’єктів [200] в мережах.

З часом, для покращення ефективності обманних технологій їх почали реалізовувати безпосередньо в програмних системах, в які зловмисники прагнуть проникнути, а не як незалежні системи-приманки, тобто розробляти вбудовані приманки.

Важливими характеристиками систем з приманками є їх автономність і стійкість. Висока швидкість і складність сучасних кібератак вимагає від систем кіберобману автономних для самоадаптації та стійких рішень, щоб зберегти своє функціонування у випадках невдач, які можуть розкрити активи або плани обману. Тому, потрібні методи, які будуть чітко враховувати місію захисника і місію зловмисника, а також будуть враховувати теоретичні основи, цілі, рівні та ризики автоматизації обманних систем та засобів. Оманні об’єкти можуть бути реалізовані як інтелектуальні агенти [200]. Більшість активних інструментів захисту значною мірою покладаються на методи обману. Для реалізації обману в мережах можуть бути використані методи обфускації, мутація IP-адреси, міграція потоку, мутації топології, мутації зв'язування DNS/IP.

В роботі [121] пропонується двофазний метод обману, що ґрунтується на локалізації приманки. В першій фазі розробляється проактивна політика локалізації приманки, а в другій фазі пропонується реактивний обманний підхід, що динамічно визначає розташування приманок відповідно до оновлень системи виявлення

вторгнень. Таким чином, система захисту частково відслідковує активність зловмисника. Метод обману комбінує використання теорії ігор та навчання з підкріпленням.

Стратегія розташування приманок в мережі повинна враховувати не тільки аспекти мережі, яка захищається, а й вподобання зловмисників [122]. Для досягнення цієї мети запропоновано метод із використанням теорії ігор, який генерує оптимальну стратегію розташування приманки відповідно до сценарію атака-захист. Динамічне розташування приманок [160] є ефективним при використанні розподіленої схеми використання приманок.

В роботі [39] сформульовано теоретико-ігровий підхід для опису політики локалізації приманки, що захищає найбільш цінні ресурси мережі, та розроблено модель двох гравців для дослідження компромісу різноманіття. В роботі [40] пропонується масштабований алгоритм розташування приманок над графом атак. Сформульована стратегічна гра для двох осіб з нульовою сумою між захисником і зловмисником. Ця ігрова модель враховує практичну модель загрози відповідно до наявної інформації про зловмисника. В роботі [130] розроблено новий теоретико-ігровий фреймворк, в якому реалізовано подвійну гру для проектування обманних механізмів, що складаються з генератора, стимулюючого модулятора та модулятора довіри. Показано, що оптимальний модулятор довіри може спричинити бажані дії з боку зловмисників.

В роботах [43, 212] розглянуто перелік обманних тактик, завдяки яким приманки отримують переваги. Було використано ідеї теорії кіберобману та планування.

В роботі [30] наведено унікальні переваги механізмів безпеки, які ґрунтуються на обмані та запропоновано фреймворк, за допомогою якого можна інтегрувати технологію обману в захист комп’ютерної системи. В роботі [80] розглянуто проблему захисту від атак в мережах IoT з приманками з точки зору теоретико-ігрової моделі обману з участю зловмисника та захисника. В роботі [85] запропоновано захисний механізм на основі обману, який включає теорію ігор для моделювання взаємодії між засобом захисту та зловмисником. Використано сигнальну гру з ідеальною байєсівською рівновагою для дослідження стратегій та визначення важливих наслідків для цього типу динамічних ігор з неповною інформацію. В роботі

[27] проведено дослідження двостороннього обману, при якому виконується маніпуляція як приманки, так і цільової системи. Ідея полягає в покращені захисту шляхом створення приманки, схожої на цільову систему, або наданням цільовій системі схожості із приманкою.

Використання систем з приманками пропонується в роботі [131] для забезпечення рівня безпеки, який є наступним рівнем після типових рівнів. Розроблено приманку з використанням генерації функції, в яку задано алгоритми машинного навчання з метою ідентифікації та класифікації сесій атакуючого зловмисника. В роботі [52] здійснено аналіз різних типів атак на кадри клієнта та різний підхід до їх виявлення і вирішення. В роботі [184] створено підроблений сервер для відволікання зловмисників. В корпоративних мережах для забезпечення безпеки та захисту інформації від працівників можуть застосовуватись датчики зашифрованих приманок [133]. Ефективність мережевих систем виявлення вторгнень [176] низька через високий відсоток хибно позитивних спрацювань. Використання приманок дозволяє зменшити це число. Система запобігання вторгненням є методом моніторингу зловмисної активності в системі безпеки мережі. Встановлено, що використання приманок в поєднанні з системами виявлення вторгнень зменшує кількість помилкових позитивних результатів.

Методи обману відігравали помітну роль у багатьох людських конфліктах протягом усієї історії [31]. Цифрові конфлікти не відрізняються, оскільки використання обману знайшло свій шлях до обчислення. У роботі [31] представлено модель, яка може бути використана для планування та інтеграції обману в захисні сили комп'ютерної безпеки. Обман як стратегія оборони проти зловмисників має переваги [198] і може бути привабливою новою здатністю для більш великих організацій, які бажають підвищити кількість виявлених загроз. Обман, як автоматизований реагуючий механізм, представляє собою зміну в можливостях IT-безпеки. Обман [30] може відігравати значну роль в покращенні безпеки сучасних комп'ютерних систем. Розроблений фреймворк в роботі [30] дає змогу включати інтегровану обманну технологію в захист комп'ютерної системи.

В роботі [28] запропоновано обманну гру, яка використовується для оцінювання прийняття зловмисником рішення за наявності обману. В експерименті

проаналізовано вплив двох факторів на рішення зловмисника атакувати комп'ютерну мережу: обсяг використаного обману; час обману.

В роботі [197] проведено огляд 24 робіт 2008-2018 років, які використовують теорію ігор для моделювання захисного обману для кібербезпеки та приватності. Запропонована класифікація виділяє шість типів обману: збурення; захист рухомої цілі; заплутування; змішування; привабливість; залучення зловмисника. Ці типи характеризуються своїми інформаційними структурами, діями і тривалістю, та концепцією теорії ігор.

Обманні рішення [44] можуть виявляти, аналізувати та захищати веб-застосунки від вдосконалених атак, від яких не можуть захистити існуючі рішення на основі пошуку аномалій [301] та методи запобігання атакам. В роботі [237] досліджено методи на основі кіберобману та розроблено нову концептуальну модель гібридних загроз, що включає методи обману. В роботі [82] представлено нову теоретику-ігрову модель обманної взаємодії між засобом захисту та зловмисником, яку в роботі названо кіберобман. Розглянуто випадки потужного зловмисника, якому відомо про обманну стратегію засобу захисту, та наївного зловмисника, якому це невідомо.

Необхідність зв'язку та передачі даних між споживачами (інтелектуальними лічильниками) та комунальними службами робить інфораструктуру вразливою до атак. Робота [238] сфокусована на розподілених атаках відмови в обслуговуванні в мережі. В мережу вводили приманки як систему-пастку для виявлення та збору інформації про атаку.

Активні хибні об'єкти цифрових даних розміщені серед реальних об'єктів даних і використовуються для виявлення зловмисного використання даних [51]. В роботі [73, 81] визначено мережевий обман для захисної розвідки та розроблено систему розвідувального обману, яка грунтується на програмно-конфігурованій мережі, щоб досягти обману шляхом імітаці віртуальних топологій.

У роботі [233] розроблено механізми орієнтації на користувачів, які надають мінімальну втрату корисності для гарантування конфіденційності користувача. У роботі [83] проаналізовано активний механізм оборони проти заклинювання в мережах, в яких одне або кілька джерел мережі вводять оманливий потік мережі по розрізненому шляху маршрутизації. Запобігання атакам у комп'ютерній мережі є

основною проблемою безпеки мережі [194]. Розроблено в роботі [194] нову ігрову теоретичну модель взаємодії між адміністратором мережі, який використовує обмежений ресурс для захисту мережі, і зловмисником, який слідкує за багатоступеневим планом нападу на мережу. Для розробки успішної оборони, заснованої на кібер-обману, важливо [128] використовувати стратегічне мислення та чітко врахувати дії зловмисника, коли він піддається оманливими спробами. У роботі [191] проаналізовано використання оборонного кібер-обману для підвищення безпеки та надійності мережевих систем.

Центральна ідея роботи [214] полягає у відображенні існування пристроїв вводу/виводу в комп'ютерній системі. Методи обману стали загальним рішенням виявлення інсайдерської загрози [143], і запропоновано кілька методів, таких як підходи, засновані на обманних технологіях. В роботі [190] розроблено інфраструктуру, яка здатна контролювати діяльність, яку виконують користувачі на облікових записах Gmail. В роботі [20] для захисту веб-застосунків від атак представлено архітектуру системи з приманок, яка включає слабкий модуль пароля та модуль ін'єкцій SQL, що підтримує мережу IPv6 для зйомки несанкціонованої поведінки доступу. Гібридні оборонні стратегії обману та переміщення підходів до цільової оборони поєднують прогрес машинного навчання або теорії ігор, які можуть запропонувати підвищення кібербезпеки проти зловмисників [129]. В роботі [139] представлено дослідження технології обману для пом'якшення атак на віртуальну локальну мережу для повідомлень та запропоновано розгортання захисних приманок шляхом визначення спостережуваних підграфів. Засіб захисту [69] може змінювати деякі характеристики цільових або обманних об'єктів, роблячи приманки більш ефективними. В роботі [69] представлено теоретико-ігрову модель двостороннього обману. Методи кіберобману повинні охоплювати ширшу поверхню атаки [89].

Приманки використовують як концептуальні структурні пастки [32], що приначені для блокування несанкціонованого доступу до цільової системи та даних. Приманки [57] привертають увагу дослідників як цінний метод безпеки, який можна застосовувати для послаблення мережевих атак, і дають можливість дізнатися більше про природу цих атак. В роботі [242] обговорено безпеку даних в Java на основі мережевої моделі користувача та сервера. Основними ідеями імітації захисту [174] є

побудова різноманітних функціональних еквівалентних варіантів для захищеної цілі, планування деяких варіантів для динамічного запуску паралельно, прийняття арбітражного механізму на основі політики, щоб вирішити, чиї результати поточних варіантів запуску є правильними.

Зловмисники часто впроваджують свої методи атак у ЗПЗ та використовють його як засіб для викрадення цінної інформації [235]. Необхідний комплексний аналіз ЗПЗ, щоб зрозуміти поведінку ЗПЗ на технічному та тактичному рівнях для розробки обманних прийомів та забезпечення обманних ресурсів, які можуть використовувати цю поведінку та вводити в оману ЗПЗ та прикладні потоки зловмисників. В роботі [216] розроблено мережу пісочниць, яка дозволяє контролювати та аналізувати поточні атаки під карантином з мережними процесами, і зберігає зображення вразливої та відкритої мережі.

В роботі [249] представлено огляд технології кіберобману, методологію та концепції, як успішно інтегрувати стратегію обману в активне робоче середовище. В роботі [175] роглянуто атрибути кіберфізичного обману та архітектуру системи із цими атрибутами. Методи кіберобману можна поділити на дві категорії: активний кіберобман та пасивний кіберобман [255]. Інженерія обману складається з проектування та розробки механізмів, що дозволяють обчислювальній машині ухилятися від кібератак [213]. Обман для самооборони є корисною здатністю брати участь у змагальному середовищі. У роботах [16, 63] надано огляд технологій обману як активного захисту, реалізації технології обману та виклики, що виникають при розгортанні технології обману. Одним із останніх підходів для захисту комп’ютерних систем є використання методів оборонного обману [105], щоб забезпечити зловмиснику помилкове уявлення про захищену мережу і, таким чином, збільшити зусилля, необхідні для успішного вторгнення. В роботі [257] досліджено еволюції обманних технологій, прийнятих у кіберзахисті. В роботі [270] стратегії кіберобману спрямовані на ін'єкцію навмисно фальсифікованої інформації для саботажу ранньої стадії розвідки та планування нападу, щоб зробити остаточну атаку неефективною.

Таким чином, для забезпечення безпеки та захисту інформації корпоративних мереж можуть бути застосовані обманні технології для зловмисників. Обман зловмисників, які можуть діяти ззовні та зсередини периметру корпоративної мережі,

може бути базований на збуренні, захисті рухомою цілю, заплутуванні, змішуванні, привабливості, залучення зловмисника. Переважно для аналізу та побудови моделей обманних технологій використовують теорію ігор [110]. Крім того, реалізацію обманних технологій здійснюють переважно окремими засобами-приманками або системами з приманками, причому вони можуть бути спрямовані під різні типи ресурсів корпоративних мереж. В процесі реалізації обманних технологій потрібно виріщувати завдання щодо нерозрізнюваності та секретності обманних об’єктів, суть яких полягає в тому, що повинен бути забезпечений секрет щодо обману. При цьому в частині завдань обманні об’єкти повинні бути максимально подібні до реальних об’єктів в мережах і видимі для зловмисників, а в частині завдань вони мають бути приховані, тобто перебувати в тіні.

1.2. Методи синтезу антивірусних приманок, пасток та їх мереж

Розглянемо архітектуру обманних засобів. Приманки можуть бути реалізовані за технологіями рухомих цілей, одиничними об’єктами, для IoT пристроїв, з високим та низьким рівнями інтеграції і мереж. При їх аналізі та проєктуванні часто використовують моделі та задачі теорії ігор, які дають змогу будувати відносини між зловмисниками і атакованими ресурсами корпоративних мереж моделями ігрових задач. Приманка встановлюється в мережі з метою бути атакованою, і не виконує інших функцій. Передбачається, що на приманках немає жодного корисного трафіку. Тому, якщо на приманці фіксується будь-яка активність, то вона вважається зловмисною [177].

Універсальна модель приманки, яку подано в роботі [141], включає блоки, зображені на рис. 1.1. Продукційна система приманки (production system, virtual production system) це власне «приманка». Вона забезпечує honey-файли та фальшиві системні ресурси для зловмисників. Система автоматично реагує на запити зловмисників з метою імітації реальної продукційної системи. Брандмауер забезпечує файли реєстрації інформації спроб зловмисника отримати доступ до приманки. Брандмауер налаштовується на запис у файл усіх активностей щодо приманки. Вузол моніторингу відслідковує, оцінює та фіксує загрози, що виникають в мережі

внаслідок активності зловмисників. Аналіз порядку, послідовності, часових відміток та типів пакетів, що використовуються зловмисником для доступу до приманки, комбінації кнопок, системний доступ, зміни файлів тощо, дозволяє ідентифікувати інструменти та методологію, що використовує зловмисник, а також їх наміри (несанкціонований доступ до даних, спроби віддаленого керування тощо).

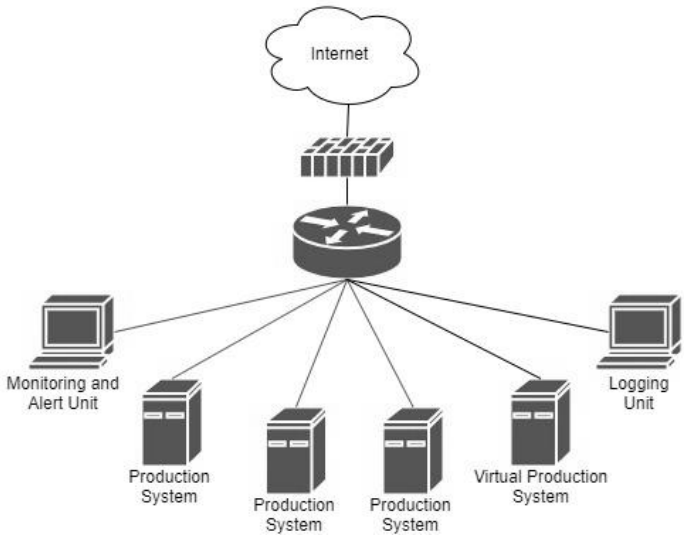


Рисунок 1.1 - Універсальна модель приманки [141]

Робота приманки в циклі виявлення та захисту від зловмисних дій розповсюджується на етапи попередження, виявлення, реагування та дослідження зловмисних дій та атак [141]. В табл. 1.1 подано рівні роботи приманки з урахуванням її функцій [141].

Таблиця 1.1

Рівні роботи приманки

Рівень	Виконувані функції
Рівень виявлення	Збір мережевого трафіку; повідомлення про виявлення приманки зловмисником
Рівень аналізу	Аналіз та оцінка дій зловмисника; аналіз виявлення приманки зловмисником
Рівень реагування	Реагування на дії зловмисника
Рівень виконання	Виявлення атак; попередження зловмисних дій

В табл. 1.2 подано основні типи приманок та їх коротку характеристику [141] за критеріями використання, рівнів взаємодії, типом розгортання обладнання та роллю.

Таблиця 1.2

Основні типи приманок

За використанням	
Виробничі (продукційні) приманки	Призначені для використання в реальних виробничих середовищах. Розташовуються всередині виробничої мережі з іншими виробничими серверами для підвищення загального рівня безпеки. Виробничі приманки є простими у використанні, потребують менше функціональності ніж дослідницькі приманки, але й надають менше інформації про атаки та зловмисників.
Дослідницькі приманки	Основною метою використання цього типу приманок є збір та дослідження інформації щодо зловмисних втручання. Такі приманки безпосередньо не підвищують рівень безпеки середовища, в якому працюють. Натомість вони досліджують загрози, з якими стикається система, для подальшого захисту від них. Дослідницькі приманки зазвичай є складними у створенні та розгортанні. Однак відслідковують більше типів атак та надають про них більше інформації.
За рівнем взаємодії	
Низького рівня взаємодії	Такий тип приманок характеризується мінімальною взаємодією з зловмисниками. Приманки не мають реальної операційної системи чи сервісів, тільки емулюють роботу певних серверів, наприклад, ftp або http. Відповідно, такі приманки є простими в розгортанні та підтримці, але відслідковують обмежену кількість дій зловмисників. Окремим підтипом є тіньові приманки, які працюють у взаємодії з системою виявлення вторгнень. Якщо система виявлення вторгнень виявляє атаку, то виявлений аномальний трафік перенаправляється на приманку замість блокування для подальшого аналізу.
Середнього рівня взаємодії	Приманки цього типу поєднують властивості приманок низького та високого рівнів взаємодії. Приманки також не мають реального середовища, але забезпечують відповіді на запити зловмисників за рахунок рівня віртуалізації. Це дозволяє отримувати більше інформації про зловмисників. Приманки є більш складними у розгортанні.

Кінець таблиці 1.2

Високого рівня взаємодії	Такі приманки мають реальну операційну систему, забезпечують високий рівень взаємодії і мають характеристики реального сервісу, що приваблює зловмисників. Тому, такі приманки дозволяють зібрати найбільше інформації про вторгнення і в більшості використовуються як дослідницькі, особливо при визначенні нових загроз. Розгортання і підтримка таких приманок є найбільш складною порівняно з іншими типами.
За типом розгортання обладнання	
Фізичні приманки	Фізична приманка є окремою машиною з запущеною операційною системою та сервісами, з якої приманка приєднана до мережі через одну IP адресу. Фізичні приманки є дорого вартісні та дещо обмежені через одну IP адресу. В більшості випадків фізичні приманки є дослідницькими.
Віртуальні приманки	Віртуальні приманки можуть розташовуватися на одній фізичній машині з іншими сервісами. Можливе розташування декількох віртуальних приманок на одній машині. Завдяки цьому віртуальні приманки відслідковують більшу кількість IP адрес та є дешевшими в розгортанні.
За роллю приманки	
Пасивні (Server Side)	Звичайні приманки є пасивними і не ініціюють обміну даними крім випадків відповідей на атаки зловмисника. Такі приманки доцільні при виявленні атак різного типу, збиранні та дослідженні інформації про вторгнень.
Активні (Client Side)	Метою активних приманок є пошук та виявлення зловмисних серверів. Попереднє виявлення зловмисних серверів дозволяє захистити вразливі застосунки клієнта.

В роботі [13] запропоновано новий тип системи приманок, що ґрунтується на обманній технології захисту. Підхід динамічного обману адаптується для збору невикористаних IP адрес у мережі із збереженням суті приманки. Невикористані IP адреси використовуються для створення динамічних віртуальних хостів, які забезпечують проактивну взаємодію із зловмисниками та перенаправляють трафік на фонові приманки, таким чином захоплюючи зловмисника в пастку. В роботі [202] представлено план розгортання контейнерної приманки, завдяки чому вона є

портативною, довговічною, простою в розгортанні та адмініструванні. Набір приманок відстежує незліченну кількість точок даних, на основі яких можна зробити висновки про дії та цілі зловмисників. В роботі [271] досліджено кібер систему приманки для вивчення використання системи приманок як обманного механізму для збору даних. Захисники можуть збирати дані про зловмисника такі як IP зловмисника, спосіб втручання в систему, використовувані типи атак, команди, які запускає зловмисник, і ЗПЗ, яке завантажується в розгорнуту систему. В роботі [166] розроблена приманка із використанням методів машинного навчання. Приманка може бути використана як пастка для підозрілих пакетів разом з методами машинного навчання, які здатні виявити ЗПЗ та класифікувати його. В якості алгоритмів класифікації використано дерева рішень та метод опорних векторів.

В роботі [262] проаналізовано сучасний стан приманок у сфері баз даних, які використовують переваги засобу захисту, а також запропоновано створення приманки бази даних із використанням відкритих технологій, таких як MySQL.

Поширення ЗПЗ за допомогою вразливостей ПЗ у веб-сторінках стало серйозною загрозою для Інтернету. В роботі [64] подано використання приманок для виявлення такого ЗПЗ. Атаки на основі вразливості базуються на застосунку на стороні клієнта, що стає головною загрозою для веб-сторінок [4]. Поширення ЗПЗ використовує вразливості ПЗ, які атакують запит на надсилання клієнта на сервер, якщо атака сталася. Це виявлення в роботі [4] базується на приманках.

В роботах [248, 272] здійснено класифікацію приманок за різними категоріями, представлено приклади приманок, які активно розробляються. В роботі [42] представлена класифікація характеристик приманки та стратегій виявлення приманок, що мінімізують частоту виявлення приманок. В роботі [246] досліджено технологічні тенденції щодо кібер-обману. В роботі [226] запропоновано нову архітектуру гібридної приманки, яка призначена для охоплення великих адресних просторів Ipv6.

У роботі [88] представлений широкий огляд середовища технологій обману, зокрема таксономії, теоретичні передумови, психологічні аспекти, а також концепції, реалізації, юридичні аспекти. В роботі [17] проведено широкий огляд приманок, ПЗ та методології аналізу даних приманок. В роботі [126] запропоновано модель на

основі приманок для системи виявлення вторгнень для отримання даних про зловмисника та було протестовано можливості та обмеження приманок. В роботі [241] розглянуто приманки з відкритим кодом, фреймворки приманок та інструменти, які допомагають розробляти та розгортати приманки, та проведено детальне обговорення системної архітектури приманок, архітектури програмного забезпечення та варіантів розгортання в хмарному середовищі. В роботі [117] пропонується нова архітектура приманки для підтримки проектування та впровадження універсальної приманки. В роботі [215] подано результат розгортання декількох приманок у віртуальному середовищі для збору слідів зловмисної активності. В роботі [41] запропоновано архітектуру приманки із використанням прослуховування портів та систему виявлення вторгнень для вивчення інформації про атаки на сервіси і визначення необхідного механізму безпеки для роботи із зловмисником.

Антивірусні програми та брандмауери захищають системи від зловмисників та різних типів вірусів. Хоча ці програми дуже ефективні проти відомих вірусів, але вони мають певні вразливості. Зловмисники можуть використовувати ці проблеми як середовище для запуску нападу на систему. Такі небезпечні ситуації вимагають механізму, який бере на себе кібератаки та вивчає їх, додатково використовуючи отримані знання для запобігання таких нападів. Одним із таких механізмів є приманка, яка створює віртуальну пастку для приманки нападників. Навмисно компрометована комп'ютерна система дозволяє зловмисникам використовувати вразливості, викриваючи свою ідентичність. В роботі [236] реалізовано такий веб-застосунок, що розкриває особу зловмисника, коли він/вона здійснює атаку.

Вразлива програма, що вимагає трафіку із зовнішнього розміщеного сервера, виконується, а користувач, який отримує доступ до трафіку, передає їх управління зловмисникам віддалено. Для виявлення такої поведінки в роботі [232] зосереджено на розгортанні приманки високої взаємодії у поєднанні з системою виявлення вторгнень на різних рівнях ОС, які працюють як клієнти.

Статична та передбачувана поведінка систем дає значні переваги зловмисникам для планування успішних атак. Розрозблено нову основу [29] для захисту рухомих цілей, що грунтується на кібер мутації та додає гнучкості кіберсистемі. Кібермутація дозволяє кіберсистемам автоматично змінювати свої параметри конфігурації в

непередбачуваний, безпечний та адаптивний спосіб, щоб проактивно досягати однієї або кількох з наступних цілей: обман зловмисників та відволікання їх від цілей; порушення планів зловмисників через зміну їх поведінки; стримування зловмисників шляхом надмірного збільшення зусиль та витрат атаки. Розглянуто кілька прикладів розроблених методів, включаючи мутацію випадкового хоста, мутацію випадкового маршрутру, мутацію відбитків дій та змінні віртуальні мережі. В роботі [102] проаналізовано витрати ресурсів на використання системи з приманками та проблеми з обмеженнями їх застосування. В роботі [94] проаналізовано витрати на розгортання приманок на прикладі Kali Linux на Raspberry PI3.

Основною метою обманних систем є формування шару захисних вузлів віртуальних мереж в хмарному середовищі, доступному через Інтернет, для відволікання та обману зловмисників. В роботі [189] представлена архітектура приманок з високою пропускною здатністю. В роботі [77] подано рішення з декількох приманок, які об'єднані в мережу приманок, і проаналізовано спроби експлуатації в частині визначення залежності, часового та просторового розподілу, прокололів, залучені автономних систем тощо. В роботі [112] представлено метод динамічного конфігурування приманки, стратегію розгортання та обслуговування, що базується на методах машинного навчання. На основі кластерів приманки автономно розгортаються в мережі. В роботі [104] розглянуто різні системи приманок та виділено два суттєвих елементи приманок. Запропоновано нову класифікацію пасток та програм безпеки з метою дослідження різних методів, включених в системи приманок.

Зловмисник, який викраде файл хешованих паролів та інвертує хеш-функцію, не зможе визначити, чи знайшов він дійсний чи хибний пароль. Спроба використання приманкового слова для входу вмикає тривогу. Допоміжний сервер відрізняє паролі користувача від приманкових паролів для процедури входу та вмикає сигнал тривоги. В роботі [142] запропоновано метод вдосконалення безпеки хешованих паролів через підтримку застосункових хибних паролів, пов'язаних з обліковим записом кожного користувача.

У роботі [268] представлено розгортання системи з приманок. Вона реалізує з високою взаємодією із безпечною оболонкою, встановленою для вивчення загальних

атак в середовищі Linux. Ця система записує імена користувачів та паролі, які намагаються ввести зловмисники з Інтернету. В роботі [59] запропоновано багатофазний механізм динамічного розгортання віртуалізованих приманок на основі прогнозування інтелектуальних атак і захисних характеристик зловмисників. У роботі [33] запропоновано адаптивний алгоритм розгортання приманок, який заснований на навчальних автоматах для покращення безпеки мережі.

В роботі [218] розроблено алгоритм тіньової (прихованої) приманки разом із сегментом препарату криптографії на основі CNN для забезпечення конфіденційності та захисту записи від зловмисників. У роботі [259] запропонована реалізація зловмисної пастки. Було створено віртуальний USB-пристрій. В роботі [50] сфокусовано на виявлення зловмисного трафіку. Було розроблено розробити приманку, яка може виявити атаки, проаналізувати зібрані дані, контролювати прогрес зловмисників та підготувати ефективний спосіб захисту від зловмисників. У роботі [115] було проведено збір та дослідження реальних комп’ютерних атак з використанням приманок. Результати роботи зосереджені на моніторингу тактики зловмисника на стандартному обладнанні. Технологія Bluetooth та притаманні ризики безпеки, які вона вводить на робоче місце, вже не можуть нехтуватись [199]. Невизнання чи відсутність адекватного захисту організації від загроз через Bluetooth збільшує ймовірність того, що несанкціонований доступ до конфіденційних даних відбудеться. Розроблено підхід до моніторингу загроз Bluetooth на основі приманок для захисту корпоративних даних. В роботі [258] розроблено приманку, яка ґрунтується на інструментах для самоаналізу та криміналістики з відкритим кодом, що забезпечують набір інформації про процеси вторгнення та інфекції, одночасно дозволяючи здійснювати автоматичне захоплення пов'язаних бінарних програм ЗПЗ.

Проблема створення приманок полягає в створенні гнучкої інфраструктури для приманок [225]. Використання контейнерів є більш ефективними для такого роду занять порівняно з іншими технологіями. Проаналізовано безпеку реалізації приманки всередині контейнерів на основі Docker.

Розподілена відмова в обслуговуванні (DDoS) є поширеним типом атаки. Існує багато типів DoS атак. Метою системи кіберзахиту є виявлення основної причини атак на корпоративну мережу. Запропоновано нову ідею в роботі [222], яка

грунтується на техніці приманки та аналізу пакетних даних, які навчені зразкам ЗПЗ. Деякі методи важко реалізувати в мережі реального підприємтсва через практичну систему навчання, яка навчається на зразках ЗПЗ або глибокому аналізі пакетів, що вимагає значної ємності для зберігання в мережі підприємства. Приманки є одним з найуспішніших методів збору зразків зловмисних програм з метою аналізу та ідентифікації атак.

В роботі [34] представлено систему приманок, яка аналізує серйозність зловмисників, які її атакують. В роботі [120] запропоновано архітектуру системи мережних приманок, яка базується на програмно-конфігурованій мережі. Система вирішує важливі проблеми існуючих приманок: цільові атаки приманок; внутрішнє розпосюдження зловмисних програм в мережах приманок; відсутність переходу на приманку. Запропоновано механізм керування підключенням, який підтримує три режими роботи: прозорий режим; режим багатоадресної передачі; режим ретрансляції. Зловмисний трафік обробляється по-різному на основі рішення контролера системи. В роботі [181] запропоновано вдосконалену систему захисту рухомих цілей на основі програмно-конфігурованих мереж. У роботі [227] для того, щоб спонукати зловмисників шпигувати та проникнути до підроблених ресурсів, система кібер-обману, що складається з різноманітних кіберпасток, використовується з приманками на основі програмно-конфігурованих мереж.

У роботі [87] запропоновано метод захисту корпоративних мереж з використанням рухомих цілей. Ідея методу в тому, щоб забезпечити в системі ймовірнісне прийняття рішень та збільшити швидкість реагування. Досягнення такого результату забезпечується шляхом повторної конфігурації мережі у прямій відповіді на виявлені загрози, пристосованої до поточної загрози та позиції безпеки, і обману зловмисників, використовуючи приманки. Рішення виконуються автоматично на основі повідомлених подій, завдань безпеки, процесів місії та станів комопнент. Використовуючи цю кодифіковану форму ситуаційної обізнаності, система може по різному реагувати на загрози щоразу, коли спостерігається активність зловмисника, що діє як бар'єр для подальшої діяльності зловмисника. В роботі [240] подано огляд різних методів захисту рухомих цілей. Методи рухомої цілі підвищують складність систем, роблять систему менш однорідною, статичною та

детермінованою. В роботі [58] запропоновано метод захисту із використанням кібер обману, що грунтується на сигнальній грі, для покращення ефективності захисту. Запропоновано використовувати захист рухомою ціллю для посилення механізму кібербезпеки. У роботі [187] запропоновано протокол ініціації сеансу специфічною приманкою, описано його розробку та впровадження для інфраструктури IP. В роботі [154] проаналізовано результати розгортання приманок низької взаємодії для моніторингу поведінки зловмисників, коли вони атакують більшість використовуваних послуг.

В роботі [7] запропоновано перехід від реактивного до проактивного використання технології з приманками. Система використовує технологію з приманками для активного захисту, заманюючи зловмисників у зазделегідь визначену "пісочницю" для спостереження за поведінкою зловмисників та методів атак. Система використовує приманку з високим рівнем взаємодії та ідею модульної архітектури, щоб відрізнити середовище приманки від центрального вузла обробки даних таким чином, щоб приманка могла отримувати більше інформації. Приманки, їх додавання, видалення, зміна та інші операції, керуються цетральним вузлом. Система, також, здійснює аналіз загроз. У роботі [195] проведено дослідження емульованих систем моніторингу зловмисних загроз, включно з приманками та “пісочницями”, та надано рекомендації для покращення виявлення вдосконалених зразків ЗПЗ та зловмисних вторгнень.

В технології приманок методи динамічного кіберобману можуть мати суттєвий вплив на ефективність. Можливості адаптації, розробка моделей кіберобману на основі поведінки зловмисників та методи штучного інтелекту дозволяють зробити приманки та їх мережі набагато ефективнішими для протидії зловмисникам [74]. В роботі [267] розроблено та впроваджено нову комплексну архітектуру мереж з приманок на основі контейнера, в якій здійснюється оцінювання стадії обману. В роботі [97] запропоновано методи автономного кіберобману, який дозволяє виконувати комплексний аналіз поведінки ЗПЗ та автоматично створює схеми обману шляхом отримання параметрів, необхідних для обману, що будуть використовуватись зловмисниками для виявлення цільових систем та досягнення своєї мети.

У роботі [76] представлено динамічну конструкцію приманки, яка автоматизує конфігурацію та розгортання хостів в мережевому середовищі. Ця система може розгорнутись без попередніх знань топології мережі. В роботі [116] запропоновано приманку, яка може характеризувати профіль зловмисника після спостереження лише за кілька взаємодій та відповідно адаптувати план кіберобману. У роботі [70] запропоновано використання штучного інтелекту з технологією приманок у хмарних середовищах для створення адаптивних, розумних приманок, здатних обманювати, виявляти та аналізувати зловмисників. В роботі [24] для більш ефективного аналізу загроз, їх виявлення та запобігання. запропоновано розробку та розгортання налаштовуваної мережі приманок на основі адаптивних методів маскування. Робота зосереджена на організації поведінкової мережі приманок. В роботі [68] представлено приманку для кіберобману на основі мутації, анонімності та різноманітності для максимізації ключових цілей обману, а саме: прихованості; виявлення та стримування; обмеження загальної вартості розгортання. В роботі [219] запропоновано приманка сумісно з NIDS для дослідження атак зловмисників на основі виконання прихованого збору інформації. У роботі [99] представлено інтелектуальну приманку, яка використовує підкріплене навчання для активного залучення та навчання з взаємодії проти зловмисника та для оптимізації обсягу зібраних даних.

Пристрої IoT є мішенню для нападів кіберзловмисників, оскільки це одна з популярних платформ [217]. У міру того, як пристрої IoT стають широко розгортаються [118], існує багато загроз системам на основі IoT через притаманні вразливості. Одним з ефективних підходів до вдосконалення безпеки IoT є розгортання систем приманок для IoT, які можуть збирати інформацію про атаку та розкривати методи та стратегії, які використовуються зловмисниками. Однак побудова приманок з високою взаємодією IoT є складним завданням через неоднорідність пристроїв IoT. Вразливості на пристроях IoT зазвичай залежать від конкретних типів пристроїв або версій ПЗ, що спонукає зловмисників виконувати попередні пробні розвідки для збору інформації про пристрої перед запуском атак. Звичайні приманки легко виявляються, оскільки їх логіка відповіді відрізняється від пристроїв IoT, які вони намагаються імітувати. В роботі [118] спочатку створено

реальну систему збору слідів атаки на основі пристроїв, щоб дізнатися, як зловмисники взаємодіють з пристроями IoT. Потім проведено моделювання поведінки атаки за допомогою процесу прийняття рішень Маркова та використано методи навчання з підкріпленням, щоб вивчити найкращі відповіді на залучення атакуючих зловмисників на основі слідів атаки. Також використано методи диференціального аналізу для мутування значень відповіді. В роботі [55] запропоновано новий метод для обману з використанням приманок. Запропоновано покращені заходи безпеки порівняно з тими, що доступні в звичайних відеокамерах з підтримкою Інтернету. В роботі [137] розглянуто впровадження приманок в IoT, які піддаються цільовому впливу зловмисників.

Через закрите програмне забезпечення та програмне забезпечення певних постачальників в промислових системах керування існують суттєві обмеження щодо вартості розробки легких у використанні приманок високого рівня взаємодії для таких систем. В роботі [127] запропоновано нову архітектуру приманки для підтримки напіввіртуальної та напівфізичної розробки та впровадження приманки. Для взаємодії з атаками архітектура розробленої приманки визначає три основних незалежних та спільних компоненти, які називаються віртуальна компонента, фізична компонента та координатор. У роботі [123] подано огляд особливостей використання рішень приманок з високим рівнем взаємодії, їх мереж та кіберобману для мереж загального призначення та промислових IoT мереж. В роботі [90] запропоновано, перевірено та критично оцінено гнучку систему приманки, яка грунтується на HTTP протоколі та імітує HTTP сервіси та застосунки. Вона покриває широкий перелік IoT пристроїв, включаючи пристрої типу "чорна скриня" без ПЗ, доступного для емуляції, хмарні сервіси та веб-сервіси. Через власні обмеження та вразливості IoT пристрої та кіберфізичні системи є популярними цілями для зловмисників. В роботі [18] запропоновано огляд досліджень приманок та мереж приманок для таких типів пристроїв та систем, класифікацію та розширений аналіз існуючих приманок та їх мереж. У роботі [15] запропоновано приманки з високим рівнем взаємодії на основі фізичних пристроїв. Ця рамка спрямована на вирішення проблем існуючих фізичних приманок, забезпечуючи переваги віртуальних приманок для ПЛК.

Поточні приманки кіберфізичної системи не здатні в достатній мірі імітувати поведінку цих систем. В роботі [211] запропонована структура системи для приманок в кіберфізичних системах, яка враховує поведінку цих систем та пристрої, які входять до складу систем. В роботі [254] пропонується модель дворівневого кібер обману для використання в кіберфізичних системах, що грунтується на сигнальних іграх для покращення захисту. Серед атак на промислові системи керування відомі зловмисні програми Stuxnet та Black Energy [65]. Анатомія цих атак вимагає застосування проактивного підходу до безпеки промислових систем керування. Приманка Conpot є приманкою з низьким рівнем взаємодії, яка емулює процеси різних кіберфізичних систем. Моделюються варіанти Conpot, зокрема модель початкового стану, модель стану тупикового блокування та модель взаємного блокування. В роботі [265] запропоновано інтерактивну приманку для системи промислового контролю. В роботі [38] розглянуто розробку та реалізацію приманок для промислових систем контролю. Приманки для промислових систем контролю повинні задовольняти як традиційним вимогам, таким як вартість і зручність обслуговування, так і більш специфічні вимоги до систем контролю. Запропоновано архітектуру віртуальної приманки промислової системи контролю з високим рівнем взаємодії на базі сервера. У роботі [23] розроблений активний підхід до безпеки для кіберфізичних систем від атак відмови в сервісі.

Атака Mirai DDoS використовує вразливі місця безпеки пристроїв IoT. Для захисту IoT пристроїв вкрай важливо розуміти стратегії відповідних зловмисників. В роботі [260] запропоновано та розгорнуто нову приманку ThingPot для пристроїв IoT. Технологія приманки імітує пристрої, які можуть бути використані зловмисниками, і реєструє їх поведінку для виявлення та аналізу використаних векторів атак. Приманка ThingPot зосереджена на протоколах застосунків IoT. В роботі [5] запропоновано новий спільний активний захист між приманкою та хмарною платформою для виявлення та захисту від майбутніх DDoS атак в контексті IoT пристроїв. В роботі [224] було розглянуто практичну масштабованість існуючих концепцій рухомих цілей та приманки з підтримкою IoT, а також проведено моделювання з використанням задач з теорії ігор. Недостатність впровадження функцій безпеки для пристроїв IoT призводить до того, що IoT пристрої чутливі до атак і є мішенями

зловмисників. Рішення в роботі [103] базується на основі приманок і передбачає отримання інформації про зловмисний трафік на етапі фільтрації для виявлення атак нульового дня та забезпечення ефективності. В роботі [36] запропоновано приманку середньої взаємодії, яка може імітувати певну серію послуг роутера для пристроїв IoT. Також, використано фактичну прошивку пристроїв IoT, яка відповідає вразливості для створення приманок, і розроблено центр управління мережею приманок, в якому розроблений механізм для розподілу команд та передачі файлів у кожен фізичний вузол. У роботі [37] представлено метод, в якому використано апаратні приманкові засоби проти апаратних вразливих місць, особливо апаратних троянських програм. Запропонована система була реалізована на Raspberry Pi та протестована на FPGA. В роботі [207] запропоновано проактивну техніку кіберобману для експертизи ЗПЗ за допомогою сканування IoT. Приманку побудовано на основі припущення, що велика мережа може позиціонуватися як велика приманка для взаємодії з ЗПЗ. У роботі [239] запропоновано інтелектуальну та високоінтерактивну приманку, яка може масштабувати вимоги дослідників, забезпечуючи дуже потрібну основу для розгортання цільових приманок для IoT.

У роботі [86] запропоновано підвищення здатності обманних засобів для виявлення атак в пов'язаній кібермережі, а також розроблено механізм виявлення аномалії на основі аналітичної послідовності шляхом маніпулювання первинними змінними та подвійними змінними, пов'язаними із запропонованим алгоритмом контролю розподіленої напруги. В роботі [220] запропоновано нову архітектуру динамічної мутації хоста, що грунтується на захисті рухомої цілі, яка здатна активно протидіяти кібератакам. Метою рухомої цілі є злам кібер ланцюга та розширення поверхні атаки таким чином, щоб збільшити вартість аналізу цілі для зловмисника та заборонити трасування сервера. Визначаються учасники, які поділяють цю політику в корпоративній мережі чи критичній інфраструктурі та визначаються функціональні модулі кожного учасника. В роботі [188] запропоновано нову архітектуру обманної маршрутизації. Нова архітектура використовує маршрутизатори-приманки лише для низхідного трафіку цензурованих користувачів.

В роботі [2] розглянуто потребу в покращених рішенням для управління безпекою хмарних обчислень. Запропоновано обманний захисний механізм на основі рухомої цілі, де ідея рухомої цілі зосереджена в частих міграціях віртуальних машин.

Розвідка IP-адреси та порту зв'язку є необхідною умовою для мережевих атак. Статичні налаштування дають велику перевагу зловмисникам у виявленні мережевих цілей та запуску атак. В роботі [150] запропоновано метод, який перетворює кінцеві хости на непередбачувані рухомі цілі шляхом прозорого інтелектуального та випадкового перетворення їх IP-адрес або портів без зменшення продуктивності мережі.

Захист рухомої цілі постійно змінює налаштування основної системи, зменшуючи рівень успішності кібератак. В роботі [19] проведено огляд останніх досліджень в розвитку захисту рухомих цілей та висвітлено як ці засоби захисту визначаються за допомогою загальної термінології, можуть бути більш ефективними за допомогою методів штучного інтелекту для прийняття рішень, як їх реалізувати та оцінити. В роботі [208] запропоновано захист рухомої цілі на основі програмно-конфігурованої мережі, яка використовує перемішування IP-адрес та номерів портів з метою заплутування (маскування) ідентифікацій мережевого та транспортного рівнів хоста та служби захисту від мережевої розвідки та атаки сканування.

В роботі [8] проаналізовано ідею обману зловмисників за допомогою фейкових сервісів та сфабикованого контенту для отримання інформації про функціонування зловмисника та перешкоджання кіберрозвідці. Вплив хибних даних дозволяє вивчати поведінку зловмисника, водночас ускладнюючи кіберрозвідку. Представлено архітектуру проксі сервера приманки, який генерує хибний контент для фейкових служб, які вводять зловмисника в оману.

Приманки, які використовуються у веб-застосунках, при взаємодії з зловмисником можуть бути ним ідентифіковані. Динамічні приманки [180] вважаються кращими завдяки свої здатності підлаштовуватися до змін середовища.

В роботі [234] проаналізовано існуючі метода та доступні вікриті рішення, які можуть бути використані для створення приманок з високим рівнем взаємодії. В роботі [62] запропоновано кластеризовану систему безпеки на основі системи приманок з високим рівнем взаємодії.

Запропонована платформа [153] з багатьма приманками як іструмент для кіберзагроз для різних класів приманок, в тому числі Windows, IoT, Embedded тощо. Приманки є досить сладними в розгортанні через наявне різноманіття IT систем та високі вимоги до приманок з високим рівнем взаємодії. В цій роботі ця складність зменшується реалізацією паравіртуалізації і дозволяє багато класів приманок різних платформ на полегшеному обладнанні. Використовується часове вікно для збору даних, які дозволяють зробити висновок про наявність кіберзагрози. Після застосування поведінкового аналізу та методів глибокого навчання для визначення патернів невідомих загроз, дані атак корелюються з різними кіберзагрозами, утворюючи "інтелект" для автономної роботи. Аналіз на основі глибокого навчання інтегрований в архітектуру для визначення невідомих загроз. В роботі [60] представлено архітектуру приманок високого рівня взаємодії, призначених для виявлення атак злому паролів та використання віртуалізації на основі контейнерів для забезпечення сеансів, необхідних для захоплення дій зловмисників.

В роботі [48] подано впровадження технологій на основі приманок у поєднанні з IDS/IPS в мережі. Дослідження підтверджують, що системи виявлення вторгнень не можуть знайти вразливості нульового дня. В роботі показано, що система з приманками в поєднанні з IDS/IPS може виявити нову спробу експлуатації вразливості. У роботі [125] подано результати двох різних дослідницьких приманок. Перша приманка розгорнута для зйомки ЗПЗ та моніторингу їх діяльності. Друга приманка була сервером для реєстрації кожної спроби зловмисного з'єднання. В результаті було встановлено, що зловмисники та ЗПЗ постійно атакують сервери, намагаючись прорватися в системи або розповсюджуватись по мережах. В роботі [251] досліджено корисність автономних обманних систем для досягнення ефективного кіберзахисту. В роботі досліджено інтеграцію автономних обчислень з ідеями теорії ігор та поведінковими властивостями для створення системи адаптивного кіберзахисту.

Таким чином, використання приманок в мережах поряд з системами виявлення вторгнень дає змогу покращити виявлення нового ЗПЗ та КА. Приманки можуть бути статичними та динамічними, а також бути інтелектуальними. Вони можуть бути адаптовані для застосування в системах з IoT, де загрози поступово з часом

зростають. Враховуючи різноманітність варіантів обману для заплутування зловмисників приманки не можуть включати всі технології обману. Потребує розроблення методів синтезу систем, які будуть здійснювати керування мережами приманок та пасток, в яких будуть реалізовані різні обманні технології.

1.3. Моделювання антивірусних приманок, пасток та їх мереж

Приманки та пастки є специфічними об’єктами в корпоративних мережах для зловмисників. Вони можуть бути видимі для зловмисника, якщо імітують певний ресурс. Або вони можуть перебувати в тіні, щоб зловмисник їх не бачив. Тоді, їх застосування має забезпечувати система. Але в обох випадках для дослідження будуть модель відносин між зловмисником та ресурсами корпоративних мереж. Як правило, переважно за основу вибирають задачу з теорії ігор для моделювання поведінки зловмисника та реакції систем з приманками або окремим приманок на дії зловмисника чи ЗПЗ. Застосовуючи моделювання при розробленні обманних об’єктів прагнуть побудувати модель, при якій приманки чи системи на їх основі отримують перевагу над зловмисником.

Для тестування захисних механізмів обманних елементів в роботі [264] було розроблено дослідницьке середовище. Для тестування в системі було реалізовано навчання з підкріпленням і зібрано активності зловмисників. Встановлено, що успішність зловмисників залежить від кількості та розташування обманних елементів. Застосовуючи розроблену модель кіберобману та її вплив на кібератаки, вбудовані в симулятор, дослідники можуть далі розробляти індивідуальні автономні агенти, що використовують обманні відповіді та проводять більш складні експерименти з обманок зловмисників за різними сценаріями та методами. Крім того, у середовище можна інтегрувати більш складні автоматизовані зловмисні агенти для перевірки їх роботи.

Для дослідників в галузі кібербезпеки залишається відкритим питання [6] щодо усунення штучних особливостей віртуальних машин для ефективної побудови обманних приманок для збору та аналізу ЗПЗ. Досліджено метод застосування Linux-контейнерів із цією метою. Теоретично Linux-контейнери мають мінімальні штучні

особливості віртуалізації та легко розгортаються на малопотужних пристроях. В роботі [6] виконані контрольовані експерименти для порівняння Linux-контейнерів та п’яти основних типів віртуальних машин. Здійснено спробу виміряти можливості обману, що можуть запропонувати Linux-контейнери, для подолання основних методів виявлення віртуального середовища. Емпірично досліджено потенційні вразливості Linux-контейнерів, що може допомогти прийняти більш обґрунтовані рішення в процесі їх розроблення.

Приманки розробляються для відволікання зловмисників від важливих ресурсів [75]. Також, вони відслідковують активність зловмисника і допомагають дослідникам вивчати патерни атак. Однак, приманки також можуть бути ідентифіковані зловмисниками за допомогою різних методів ідентифікації. В роботі [75] використовується моделювання для ідентифікації потенційних загроз, які виявляють їх існування, що робить приманку неефективною.

В роботі [9] способом отримання корисної інформації про поведінку зловмисників з низьким рівнем помилкового виявлення є використання приманок. Вони також є потужними засобами для витрачання ресурсів зловмисників та привертання їх уваги з інших критичних активів у мережі до себе. Обманна мережа з декількома приманками називається мережею з приманками. Приманки в такій мережі мають за мету співпрацю між собою для досягнення кращого результату щодо обману зловмисників. Професійні зловмисники використовують засоби виявлення, приманок у мережах. Коли зловмисник виявляє, що механізм обману розгортається, то він може змінити їх поведінку і спричинити зловмисні наслідки для мережі. Тому, мережа з приманками повинна бути досить оманливою, щоб не бути ідентифікованою. Представлені методи в роботі [9] повністю досліджені за допомогою порівняльного аналізу та моделювання. При проведенні дослідження було враховано такі параметри: толерантність зловмисника; безпечність користувачів мереж; поріг підключення до приманок; кількість тестів нападу. Також, враховано призначення кожному хосту числового значення важливості, призначення обмежених значень важливості хостам, припущення про не володіння зловмисником про типи приманок, врахування методів виявлення приманок, врахування невідомого рівня безпеки графіків атаки для захисника, дозвіл захиснику розмістити кілька приманок

на графіку атаки, припущення щодо правильності розташованих приманок, врахування нападів з зондуванням і без зондування, врахування кілька зондів для зловмисника, врахування отриманих доказів зловмисника, врахування отриманих доказів діяльності користувачів, припущення щодо автентичності користувачів, врахування різних топологічних характеристик мереж з приманками, врахування різної мережевої топології.

Однією з переваг [113] застосування обманних технологій розглядається можливість досягнення низького відсотка або навіть нуля хибно позитивних спрацювань. В роботі [113] проведено оцінювання використання обману у веб-застосунках, зокрема оцінювання кількості хибно позитивних та хибно негативних виявлень. Запропоновано фреймворк, який дозволяє додавати обман до будь-якого веб-застосунку.

В роботі [132] запропоновано декілька унікальних методів для виявлення патернів розповсюдження атаки із використанням моделей ланцюгів Маркова та аналізу складних мереж. Результати цих моделей відображають різні профілі атак та патерни взаємодії між розгорнутими сенсорами в системі приманок. Запропоновані методи оцінені на основі набору даних, що включає понад 167 мільйонів спостережених атак на глобальну розподілену систему приманок. Визначено основні приманки, які дозоляють поширення атак та показано, як профілі атак змінюються в залежності від країни походження зловмисника. Ці патерни можуть бути використані для кращого розуміння та протидії зловмисним діям. Вважається, що розташування приманок в різних георграфічних локаціях збільшує їх ефективність, однак цей факт не є достатньо дослідженим, особливо для систем раннього виявлення вторгнень. В роботі [256] досліджено патерни атак великого публічного датасету географічно розподілених приманок та створено профілі зловмисників. Розташування приманок допомагає виявити патерни атак та побудувати профілі зловмисників. Не всі дані, зібрані з георафічно розподілених приманок є однаково цінними, і можна створити систему раннього попередження вторгнень за допомогою двох розподілених приманок та робочого серверу.

Обманні методи досліджуються та вдосконалюються протягом останніх двох десятків років. Однак обман все ще включаєтсья в процес розробки ПЗ в

нестандартному порядку. Зазвичай реалізується у вигляді окремих інструментів або окремих рішень, розгорнутих на машинах-приманках. В роботі [79] запропоновано мультипарадигмовий підхід для визначення тактики обману під час розроблення ПЗ, що дозволяє виявляти конфлікти та ризики на початкових етапах розробки, зменшуючи витрати на неправильно сплановані рішення. Описано метамодель, що містить обманні концепції, яка об'єднує інші моделі, такі як цільова модель, модель функцій та поведінкові моделі для визначення статичних і динамічних аспектів операції обману. Результатом цього процесу є множина обманних тактик, що реалізується множиною обманних компонентів, які інтегровані з компонентами системи. Реалізацію цього мультипарадигмового підходу показано при розробленні стратегій захисту від обману для системи контролю.

В роботі [108] запропоновано методологію оцінювання ефективності приманок та рухомих цілей в мережі. Ця методологія дозволяє чисельно оцінити ефективність в середовищі моделювання, дозволяючи розробити рекоментадії щодо кількості приманок для розгортання та швидкості виконання мутації мережевих адрес для ефективного переривання атаки за різних конфігурацій мережі та зловмисника.

Оборонний обман [157] включає мислення, як у зловмисника, та визначення найкращої стратегії протидії загальній стратегії нападу. Тактика оборонного обману сприятлива для впровадження невизначеності для супротивників, збільшення витрат на навчання та, як наслідок, зниження ймовірності успішних нападів. У кібербезпеці, приманки, пастки, мережі приманок та переміщення цільової оборони зазвичай використовують як тактику оборонного обману. Для різних цілей були створені обманні технології. Однак існує критична потреба у застосуванні передових технологій обману. Обчислювальна розвідка забезпечує відповідний набір інструментів для створення розширених меж обману. Обчислювальний інтелект включає дві технології штучного інтелекту: глибоке навчання; машинне навчання. Ці стратегії можуть бути використані в різних ситуаціях в оборонних технологіях обману. В роботі [157] сфокусовано на тактиці обманної оборони, розгорнутої за допомогою алгоритмів глибокого та машинного навчання.

В роботі [193] досліджено ефективність розгортання приманок, зокрема в напрямі щодо змішування вузлів приманок з робочими вузлами. Це призводить до

проблеми розгортання, як засобу захисту, поєднання обманних комп'ютерів з робочими комп'ютерами, щоб примусти зловмисників виявляти свої нові атаки, мінімізуючи втрати для засобу захисту. В роботі формалізовано задачу розгортання приманок як задачу комбінаторної оптимізації та запропоновано оптимальний алгоритм (схему поліноміально-часової апроксимації). Проведено моделювання, щоб показати вплив можливостей зловмисників.

Традиційні приманки не можуть усунути увесь наявний шум та непотрібні дані, оскільки вони не мають можливості аналізувати дані. В роботі [140] запропоновано розширену приманку, яку вдосконалену методами машинного навчання, що дозволяє аналізувати дані та зменшувати вартість функціонування приманки. Для кращого очищення даних в приманці представлено алгоритм ансамблю, який можна використовувати для неоднорідного ансамблю.

Традиційні стратегії неефективні перед новими атаками в складному мережевому середовищі, такими як розширена постійна загроза [45]. В роботі [45] досліджено отримання з даних приманок тактику, прийоми та процедури суб'єкта загрози, що допомагає створювати більш ефективні стратегії захисту. Однак актуальним є питання покращення архітектури приманок, щоб їх не могли розпізнати зловмисники. Їм потрібні інтелектуальні методи для автоматичної віддаленої перевірки запуску приманок на сервері. Запропоновано [45] нову модель автоматичної ідентифікації на основі методу випадкового лісу з трьома груповими функціями: функція прикладного рівня; функція мережевого рівня; функція системного рівня. Дані для підтвердження ефективності запропонованої моделі зібрані із загольнодоступних платформ.

В роботі [49] запропоновано централізований підхід на основі приманок із програмно-визначеним перемиканням. За допомогою цього підходу забезпечується зменшення хибно позитивних спрацювань, мережевого трафіку, витрат на забезпечення кібербезпеки. Запропонована система була промодельована за допомогою програмного забезпечення GNS3.

Алгоритми виявлення спільноти призначені для групування вузлів на основі їх зв'язків та відіграє істотну роль в комплексному аналізі систем [136]. Однак з міркувань конфіденційності може бути необхідно в деяких випадках запобіги тому,

щоб спільноти або групи вузлів в складних промислових мережах були виявлені. В роботі [136] представлено та формалізовано інтелектуальні методи обману спільноти для приховування вузлів. Оцінка стійкості використовується для дестабілізації постійних спільнот у мережі, а оцінка безпеки використовується для оцінки рівня приховування вузла. Цільові функції спрямовані на мінімізацію показника стійкості та максимізацію показника безпеки вузлів у мережі. Результати моделювання показують, що запропоновані стратегії інтелектуально приховують інформацію спільноти в складній промисловій системі.

Нові мережеві атаки, такі як розширені постійні загрози, створили асиметричну динаміку між зловмисниками та захисниками [12]. Традиційні механізми захисту зазвичай зосереджуються на безпеці периметра, роблячи їх неефективними, коли зловмисники проникають у мережу. З іншої сторони, захист з кібер-обманом активно встановлює обманне середовище для маніпулювання сприйняттям та рішеннями зловмисників, тим самим затримуючи, виявляючи та потенційно перешкоджаючи атакам. У роботі [12] представлено новий підхід у захисті з кіберобманом, використовуючи технологію FPGA. Використовуючи методи переписування мережевих пакетів на FPGA, цей метод швидко генерує численні замасковані хости та порти. Реалізація такого підходу на апаратній платформі FPGA дозволяє оцінити його ефективність. У модельованих середовищах метод демонструє ефективність у побудові обманних середовищ. Перехід до реальних сценаріїв мережі, прототипна система подовжує час, який необхідний зловмисникам для виявлення справжніх ресурсів на коефіцієнт 4,5. Середній час затримки системи-прототипу в обробці 64-байтних пакетів даних становить приблизно 5,68 мс, що демонструє послідовну ефективність у різних стратегіях обману. Принципово важливо, що додаткові витрати системи залишаються мінімальними, ефективно заплутаними та стримуючими зловмисників, збільшуючи складність та витрати, пов'язані з встановленням успішних атак.

В роботі [178] запропоновано підхід для включення тактик обману на ранніх етапах розробки, що зменшує ризики конфліктів та знижує вартість рішень. Процес включає три етапи: моделювання системи (створення цільової моделі предметної галузі); моделювання безпеки (створення моделі загрози, що визначає типові

проблеми безпеки з точки зору зловмисника); моделювання кіберобману (створення моделі тактики обману, моделі зміни та моделей історії обману).

Відволікаючи увагу потенційних зловмисників і відбиваючи свої ресурси, приманки є потужним інструментом для захисту критичних активів у мережі [1]. Однак ландшафт кібербезпеки постійно розвивається, і професійні зловмисники завжди працюють над розкриттям та обходами приманок. Після того, як зловмисник успішно визначає механізм обману, вони можуть змінити свою тактику, потенційно завдаючи значної шкоди мережі. Підтримка високого рівня обману має вирішальне значення, щоб приманки залишалися невизначеними. У роботі [1] досліджуються різні методи обману, розроблені спеціально для приманок, щоб підвищити їх продуктивність, роблячи їх непроникними для виявлення. Попередні дослідження не забезпечили детального порівняння цих методик, особливо тих, які пристосовані до мереж з приманками. Тому, було класифіковано представлені методи на відповідні класи, подано їх порівняльний аналіз та оцінено їх ефективність у сценаріях моделювання. Розроблено математичну модель, яка представляє та порівнює різні дослідницькі зусилля з розроблення приманок. Запропоновано розширення методів обману для наслідування вразливості, притаманних 5G та визначені програмно-конфігурованими мережами, які вирішують проблеми, що розвиваються.

В роботі [231] представлено інтелектуальний та адаптивний агент, який використовує кіберобман для розпізнавання намірів зловмисника щодо хоста приманки. На відміну від попередніх підходів, які переважно зосереджені на затримуванні або заплутуванні зловмисників, цей метод передбачає залучення зловмисниска до взаємодії для визначення його намірів. Промодельовано обман як проблему послідовного прийняття рішень в контексті двох агентів. Представлено факторизований кінцевовкладений інтерактивний частково спостережуваний Марківський процес прийняття рішень для моделювання проблеми із декількома видами зловмисників. Метод моделює кібератаку на один хост приманки через декілька етапів від початкового входу зловмисника до досягнення ним своєї мети. Використовуючи захист, агент використовує приманки для взаємодії зі зловмисником на кількох етапах, формуючи більш точні прогнози поведінки зловмисника.

В роботі [56] встановлено, що у попередніх роботах з використанням теорії ігор для кіберобману, як правило, моделювались послідовні ігри, де маніпулюється якість та автентичність сигналу. В роботі покладаються на сигнал, який може бути обманним, при якому активно запрошуються зловмисники через виплату нагороди, щоб спонукати їх вжити неоптимальних дій. Ця модель обману має на меті вирішити взаємодію захисника з зловмисником після первинного розгортання кібер-захисних засобів. Таким чином, запропонована модель оборонного кіберобману, який включає контроль за захисним сприйняттям зловмисником кіберсередовища. Кінцева мета роботи це інформувати майбутні системи кібероборони, щоб забезпечували більш складні відповіді на поведінку зловмисників та вдосконалення оборонної позиції.

Кіберобман - це підхід, коли адміністратори мережі можуть розгорнути мережу приманкових активів з метою витрачати ресурси та час зловмисників і збирати інформацію про їх стратегії, тактику та наміри [192]. Ключова проблема в цьому кіберобмані полягає в архітектурі та розміщенні мережевих приманок для забезпечення максимальної інформації про зловмисників та його стратегій. Результат, що складається з стану безпеки та результативних дій, моделюється як частково спостережуваний процес рішення Маркова, шлях нападу зловмисника до складання фальшивих вузлів та мереж.

ЗПЗ виступає критичним компонентом в мережевих механізмах атаки та захисту [205]. Оскільки загрози ЗПЗ стають складнішими та різноманітними, необхідна автоматична класифікація зловмисних програм. При цьому потрібно враховувати узгодженість та споживання системних ресурсів, класифікацію ЗПЗ, які повинні бути сумісними з іншими пристроями безпеки для формування всебічної системи оборони. У роботі [205] запропоновано доведення попереднього тренінгу на основі поведінки ЗПЗ, захопленої за допомогою приманок всередині та поза межами захищеної системи, і оцінюється ефективність у категоризації класів зловмисних програм. Для опису ЗПЗ було розроблено моделі поведінки ЗПЗ шляхом вибору підмножини будь-якої поведінки. Потім застосовується модель попередньої підготовки, щоб вивчити внутрішній режим зловмисного коду для того, щоб керувати моделлю класифікації.

Складна топологія мереж без масштабу робить їх ідеальною мішенню для нападів [35]. Технологія на основі приманок має перспективи для вирішення проблем,

пов'язаних з worm-вірусами. У роботі [35] запропоновано нову модель розповсюдження, засновану на зворотному зв'язку приманок. Після успішного захоплення вірусу, приманка збирає поведінки, аналізує шляхи нападу, генерує інформацію про імунітет та надає імунний зворотній зв'язок сусіднім вузлам для сприяння активному захисту. В роботі введено вузол приманки на основі моделі SIR. Потім використано динамічний аналіз для обчислення порогу поширення моделі, що підтверджує глобальну стабільність рівноважного інфікування та існування рівноваги.

Таким чином, приманки, пастки та мережі приманок у корпоративних мережах слугують інструментами для виявлення та аналізу дій зловмисників. Вони можуть бути як помітними, імітуючи реальні ресурси, так і прихованими, щоб залишатися невидимими для атакуючих. У будь-якому випадку їх ефективне застосування забезпечується системою безпеки. Для дослідження взаємодії зловмисників із корпоративними ресурсами зазвичай використовують підходи з теорії ігор, що дозволяють моделювати їхню поведінку та реакцію системи на атаки. Головна мета такого моделювання – створення ефективної системи обманних об’єктів, яка надає перевагу захисним механізмам над діями зловмисників. Результати аналізу відомих рішень щодо моделювання дій зловмисників та обманних об’єктів потребують удосконалення, бо не враховують всі можливі сценарії поведінки зловмисника і можливі сценарії відповіді обманних засобів та систем. Моделювання відповідей обманних засобів та систем на відповіді зловмисників дало б змогу розробити обманні засоби та системи, поведінка яких була б важко зрозумілою зловмисникам.

1.4. Методи створення систем антивірусних приманок та пасток для виявлення ЗПЗ і КА

Одиничні обманні засоби дають змогу виявляти ЗПЗ та КА переважно за певним типом їх поведінки, тобто вони орієнтовані на виявлення певного типу ЗПЗ чи КА. Щодо їх застосування може виникнути проблема, коли зловмисник, ЗПЗ та КА не зможуть активувати такі обманні засоби. Це пов’язано, також, з певною відособленістю їх в корпоративних мережах. Одночасно в корпоративних мережах

можна розмістити декілька одиничних обманних засобів, але вони не будуть координуватись між собою. Для них можуть виділятись окремі обчислювальні ресурси в корпоративних мережах.

Для того, щоб забезпечити координацію та ефективне функціонування одиничних обманних засобів в корпоративних мережах потрібно використати обманну систему, яка б здійснювала їх координацію і взаємодію. Тоді, одиничні приманки можуть мати різні призначення, а система буде визначати їх залучення до виконання завдань. Таким чином, організовані приманки в складі системи можуть формувати цілі мережі приманок. Їх ефективність буде залежати від особливостей обманних систем, в складі яких вони функціонуватимуть, архітектури таких систем, організації центру прийняття рішень, рівня самостійності в прийнятті рішень, мінімізації залучення адміністратора системи та корпоративної мережі тощо.

Системи з приманками поділяють на дослідницькі та комерційні. Розглянемо дослідницькі обманні системи, які підтримують в своєму складі функціонування приманок різного спрямування щодо виявлення ЗПЗ та КА.

При використанні приманок мають бути досягнуті певні компроміси. З одного боку системи і сервіси приманки мають бути відповідними та привабливими для зловмисника, з іншого боку обчислювальні та супутні витрати мають відповідати функціональних та бюджетним обмеженням системи. Неможливо створити єдину незмінну конфігурацію приманок для різних типів систем та врахувати всі можливі типи зловмисників. В роботі [159] запропонований підхід, що впроваджує нові можливості до обманних систем для реалізації вибіркового встановлення приманки. Це дозволяє приманці динамічно вводити ресурси відповідно до виявлених дій зловмисника. Такі приманки складаються з простору імен ядра та віртуальних машин, які викликаються з неактивного стану. Вони, також, використовуються для динамічного перенаправлення трафіку приманок. Цей механізм перенаправлення може бути виконаний без помітної затримки.

Обман з використанням приманок може забезпечити ефективний шлях протидії кібератакам в комп’ютерних мережах [135]. В роботі [135] оцінено вплив розміру мережі на рішення зловмисника щодо кібератак, використовуючи гру в обман. Гра в обман має дві послідовні стадії: дослідження; атака. На стадії дослідження учасники

можуть перевіряти декілька веб-серверів або не перевіряти мережу. На стадії атаки учасники можуть атакувати один з досліджуваних веб-серверів або вирішити не атакувати мережу.

Для зловмисників розвідка є важливим кроком для збору даних про мережу та вибору вразливих цілей для вторгнення [124]. Захисний обман є важливою стратегією проти загроз, що дозволяє заплутувати зловмисників. Засоби захисту можуть використовувати приманки з низьким та високим рівнем взаємодії. В роботі [124] розглянуто гібридну систему приманок, що збалансовує використання двох рівнів складності приманок, приманки з високим рівнем взаємодії призначені для обману більш досвідчених зловмисників ніж приманки низького рівня взаємодії. Запропоновано модель гіпергри для двох гравців, яка описує як засіб захисту має розгортати приманки низького та високого рівня взаємодії для захисту мережі від зловмисної розвідки. Змодельовано компроміс кожного гравця для описаної стратегії для фреймворку, що враховує недосконалі знання кожного гравця про свого опонента.

Комбіновані приманки, включаючи «фронтенд» та «бекенд», широко використовуються в дослідженнях через масштабованість «фронтенду» та високий рівень взаємодії «бекенду» [263]. Але традиційні комбіновані приманки мають проблеми з контролем потоку та нереалістичним моделюванням топології. В роботі [263] запропонована нова архітектура на основі програмно-конфігурованої мережі застосованої до системи комбінованої приманки для моделювання топології мережі та перенаправлення трафіку атаки. Система використовує розширюваність та керованість контролера ПКМ для імітації великої та реалістичної мережі для залучення зловмисників та перенаправлення атак на приманку з високим рівнем взаємодії з подальшим аналізом. Це дозволяє усунути недоліки технології імітації мережі та технології керування потоком традиційної мережі приманок.

В роботі [269] розглянуто типові методи, що використовуються в приманках, токенах та засобах захисту рухомих цілей, що охоплює період з 1980-х до 2021 року. Методи з цих трьох галузей доповнюють одна одну і можуть бути використані для побудови цілісного захисту на основі обману. В роботі [269] досліджено інтегроване використання цих трьох напрямків для організованого обману. Використовуючи

адаптовану модель кіберланцюга знищення, яка може відображати поточний ландшафт загроз, і чотирирівневий стек обману, розроблено двовимірну таксономію, на основі якої класифікуються методи обману.

В роботі [72] подано розширений огляд технологічного середовища обману, а також огляд поточних тенденцій та моделей реалізації в системах виявлення вторгнень на основі обману. Останнім часом обманна технологія розглядається як рішення для виявлення з нульовим відсотком хибно позитивних спрацювань [114]. Але немає повного розуміння щодо порівняння обманних рішень з існуючими та оцінки їх ефективності. В роботі [114] проаналізовано обмеження існуючих рішень та декілька напрямків відкритих досліджень, включаючи стратегію розробки обманних рішень та інтеграції його з заданою архітектурою. В роботі [252] запропоновано обманну методологію, яку засновано на принципах військового обману, для обману зловмисного зонду на захист фізичної мережі комунікацій. Спроєктовано мережу, яка використовує схему обману, реалізовану на розумному маршрутизаторі, що може представити обманну топологію зловмиснику.

В роботі [229] запропоновано проактивну оптимізовану систему виявлення вторгнень з пасткою на основі приманки для виявлення атак нульового дня з мінімальними витратами. В роботі [47] запропоновано систему виявлення та запобігання вторгнень на основі приманок. Розроблений серверний застосунок приманки, поєднаний з СВВ для аналізу даних в реальному часі та ефективної роботи. Запропоновано систему комбінованої приманки з врахуванням переваг приманок низького та високого рівня взаємодії. Для зменшення витрат на конфігурування, підримку та керування приманками в корпоративній мережі використовуються технології віртуалізації. Система дозволяє виявляти атаки нульового дня та зменшити кількість хибно позитивних спрацювань в СВВ.

В роботі [98] представлено приманки промислових систем керування високого рівня взаємодії та продемонстровано, що мережу підключених до інтернету приманок можна використовувати для ідентифікації та профілювання цільових атак. В дослідженні використано дані мережі з 120 приманок високого рівня взаємодії в 22 країнах, які імітують ПЛК та віддалені термінали. Проведений детальний аналіз 80 тисяч взаємодій за 13 місяців, з яких лише дев'ять зловмисно використовували

промисловий протокол. Зловмисна взаємодія включала атаки на відмову в обслуговуванні, та атаки, що маніпулюють логікою і використовують недоліки в реалізації протоколу та використовують технологію переповнення буферу. Дослідження показують, що для ефективності такої мережі приманок необхідний високоякісний обман протягом тривалого часу. Надано рекомендації щодо ефективного стратегічного використання таких мереж.

Стрімкий розвиток інтернет-технологій вимагає постійного вдосконалення рішень, що забезпечують безпеку комп'ютерних систем і мереж [243], даних і критичної інфраструктури, для чого важливо отримувати інформацію про шкідливі дії [93]. Сучасні методи використовують теорію ігор і методи машинного навчання [182] для забезпечення динамічних стратегій обману, що дозволяє спостерігати, реагувати і адаптуватися до поведінки зловмисника в короткостроковій і довгостроковій перспективі. У технології на основі приманки динамічні методи обману можуть мати значний вплив на ефективність. Адаптивність, розробка моделей кіберобману, заснованих на поведінці зловмисників і методів штучного інтелекту, роблять приманки і їх мережі набагато ефективніше в протидії зловмисним атакам. Розумні приманки, які використовують методи машинного навчання, активно взаємодіють зі зловмисниками, вивчаючи їхню поведінку та адаптуючись [257].

На основі підбору, порівняння та комбінування марковських та напівмарківських моделей розробляється стратегія оцінки надійності, доступності та кібербезпеки хмарного середовища та Інтернету речей [66]. Динамічна структура системи вимагає динамічного визначення параметрів. В роботах [167, 183] запропонована модель оцінки параметрів в розподілених системах з динамічною структурою, в якій реалізовані різнорідні розподілені бази даних, така модель дозволяє розробляти нові моделі підтримки управління розподіленою системою обробки даних. Динамічні системи кіберзахисту з підтримкою методів штучного інтелекту повинні мати властивість стійкості і в роботі [210] аналізуються можливі джерела загроз для таких систем та розглядаються методи забезпечення властивості стабільності системи, які дозволяють створювати стабільні системи з використанням штучного інтелекту шляхом налаштування архітектури і сценаріїв навчання.

Одним із способів забезпечення динамічних властивостей приманок є віртуалізація. Алгебраїчні віртуальні машини дозволяють за допомогою різних методів перевіряти властивості систем і виявляти поведінку, задану у вигляді алгебраїчних шаблонів [158, 302]. У роботах [151, 152] запропоновано алгоритм вибору показників для прогнозування безпеки комп'ютерних систем, в якому використовуються багаторівневі моделі в класі лінійних і нелінійних моделей.

Нові технології та інструменти в індустрії IoT змушують зловмисників вдосконалювати існуючі атаки та розробляти нові, що може зробити деякі з цих пристроїв вразливими, тому потреба в кіберзахисті пристроїв IoT зростає [161].

У роботі [155] представлений підхід до виявлення кібератак на основі глибокого навчання шляхом стиснення параметрів мережевого трафіку. У роботі [221] розглядається трирівнева архітектура компонентів системи автоматизації будівель, а також забезпечення безпеки в них. Безпека оцінюється за допомогою моделей. Системи автоматизації будівель – це складні системи, і вони повинні мати підсистеми забезпечення кіберзахисту. Ці підсистеми повинні бути складними для розуміння зловмисниками. Квінтесенція інформаційної безпеки кіберфізичних систем подана в роботі [285]. Захист блокчейн технологій подано в роботі [144]. Частково централізовані системи виявлення ЗПЗ в комп’ютерних мережах з деталізації архітектури для уникнення виявлення подано в роботі [311]. Концепція застосування систем з приманками в розподілених ізольованих середовищах подана в роботі [309].

Системи виявлення вторгнень [245] є ключовим компонентом оборонних засобів. Оскільки звичайні IDS не масштабні для великих мереж компанії та за її межами, а також для масово паралельних атак, з'явилися спільні IDSS. Вони складаються з декількох компонентів моніторингу, які збирають та обмінюються даними. Залежно від специфічної архітектури, центральних або розподілених компонентів вони здійснюють аналіз зібраних даних для виявлення атак. Отримані сповіщення співвідносяться між декількома моніторами з метою створення цілісного виду на моніторингу мережі. В роботі [245] спочатку визначено відповідні вимоги до таких систем. Потім запропоновано вимоги і архітектуру. Системи виявлення вторгнень мають володіти здатністю масштабуватися до потреб великих корпоративних мереж та загрози масових паралельних атак. Таким вимогам

відповідають колаборативна система виявлення вторгнень, яка містить централізовані та розподілені компоненти, призначені для збору та обміну даними між вузлами для отримання цілісного уявлення про мережу.

Мережеві обманні системи [168] дозволяють модифікувати трафік практично в режимі реального часу для запобігання та зупинки кіберрозвідки та атак і критично потребують оцінювання ефективності. В роботі [168] запропоновані метрики для кількісної оцінки ефективності мережевого обману в системах на основі програмно конфігурованих мереж.

В роботі [22] представлено адаптивна система кіберобману. Вона надає унікальне представлення віртуальної мережі кожному хосту корпоративної мережі. Таким чином, представлення хоста про свою мережу, включаючи топологію підмережі та призначення IP-адрес доступних хостів і серверів, не відображає конфігурації фізичної мережі та відрізняється від представлення будь-якого іншого хоста в мережі. Запропонована система генерує мережеві представлення з необхідними властивостями та змінює вигляд мережі хостів в реальному часі, що запобігає розвідці скомпрометованих зловмисником вузлів.

Суттєвим недоліком приманок може бути те, що їх важко спроектувати таким чином, щоб зловмисник не міг відрізнити їх від реальної продуктивної системи [25]. В роботі [25] пропонується замість додавання окремих обманних систем у корпоративну мережу забезпечити самі цільові системи інструментами для активної оборони. Такий підхід до активного захисту дозволяє зменшувати витрати та складність, в той же час пропонує зловмиснику більш реалістичні цілі та дає більше часу для реагування та ідентифікації зловмисника. Запропонований прототип можна використовувати для реалізації активного захисту в будь-якій корпоративній мережі з незначним попереднім налаштуванням та обслуговуванням.

В роботі [95] запропоновано розподілену систему приманок, яка призначена для моніторингу сканування Інтернету та поведінки атак проти промислових систем управління. Система може виконувати кластеризацію та візуалізацію атак та надає інформацію про поточну ситуацію безпеки системи. Вона виконує моделювання високого рівня, глибокий аналіз даних та має роширений інтерфейс візуалізації.

В роботі [26] запропоновано обманна система виявлення вторгнень для запобігання шахрайській точці доступу за допомогою виявлення атак внутрішніх та зовнішніх зловмисників. Поєднання систем виявлення вторгнень та приманок зменшує частку хибно позитивних спрацювань. Запропонований метод складається з трьох етапів: фільтрація; система виявлення вторгнень; приманка. Трафік після проходження системи фільтрації та виявлення вторгнень перенаправляється на приманку для поглибленого дослідження.

Система з мережею приманок [134] була розроблена, щоб спростити розгортання та керування, а також зробити використання приманок більш безпечним. Використано приманки Kippo, Glasstopf, Dionaea.

Важливим завдання є не тільки наявність можливості контролювати велику кількість систем [196], а й можливість швидко реагувати на події. В роботі [196] запропоновано інструмент виявлення вторгнень на основі деяких з існуючих методів виявлення вторгнень та концепції приманок.

Існуючі приманки та їх мережі піддають різним спробам детектування та виявлення їх вразливостей. Поточна архітектура мережі приманок не повністю використовує властивості постійних приманок через їх грубий механізм контролю даних. Для подолання цієї проблеми запропоновано в роботі [119] інтелектуальну мережу приманок на основі програмно конфігурованих мереж. Вона використовує широкі можливості програмування програмно конфігурованих мереж для обходу механізмів виявлення зловмисниками та забезпечує детальний контроль даних для множини приманок. Для цього вона одночасно встановлює декілька з'єднань з набором приманок та обирає найбільш прийнятне з'єднання, щоб спонукати зловмисника залишатися на зв'язку.

Віртуальні мережі, виконані з віртуальних приманок, часто використовуються для дослідження поведінки зловмисників [109]. Традиційно використовується статична схема розгортання, в якій конфігурація мережі приманок визначається зазделегідь. Недоліком такого підходу є неможливість адаптувати конфігурацію мережі після розгортання. В роботі [109] запропоновано нову гнучку систему керування віртуальною мережею приманок, яка динамічно створюється,

конфігурується та розгортається з приманками низького та високого рівня взаємодії, які емулюють декілька ОС.

У роботі [209] використовуються методи контейнеризації для динамічного створення мереж приманок, які забезпечують обманне середовище для зловмисника, та запропоновано фреймворк для його використання в існуючій хмарній інфраструктурі. Запропонована архітектура може тимчасово захистити сервіси приманок для виявлення зловмисника та реєстрації постінцидентних або експериментальних досліджень. Використано моделювання ізоляції зловмисника в хмарних системах за допомогою докера, інтеграцію віртуальної приманки з ОС для запису логів, після чого було використано моделювання загроз на запропонованій архітектурі.

В роботі [100] використано динамічну властивість приманки з чотирьох видів сервісів запропонованої системи. Однак ця динамічна властивість відображається в розташуванні та ідентифікації, вказуючи на те, що справжні або обманні сервіси змінюються в різних хостах. Таким чином, динамічні властивості запропонованої системи відрізняються від динамічної приманки. Крім того, адаптовано блокчейн платформу для децентралізації запропонованої системи та збереження даних доступу до порту, забезпечуючи приватний ланцюг.

В роботі [106] розглянуто початкові кроки для реалізації активного захисту із використанням засобів обману для розподілених систем та побудови прототипу, який створює альтернативне середовище, що дозволяє захоплювати та маніпулювати зловмисниками без впливу на цільову систему. Цей прототип використовує програмно конфігуровані мережі та віртуалізацію для створення гнучкого середовища, в якому виконуються обманні дії. Обман залежить від цілей розподіленої системи, для якої використовується засіб захисту, зокрема від використовуваних служб, конфігурації та складності середовища. Не існує єдиної стратегії обману, яка відповідала б усім конфігураціям та цілям цільової системи. Запропонована система дозволяє конфігурувати обманну систему із блоків.

Багато систем критичної інфраструктури, під'єднаних до мережі, піддаються атакам зловмисників. Запропоновано в роботі [84] та описано фреймворк кіберобману для покращення кібербезпеки мережі за допомогою використання приманок з метою

заплутування зловмисника та відволікання його від реальних компонентів. Він містить SCADA сумісні приманки, які можуть бути згенеровані та розгорнуті в середовищах критичної інфраструктури.

Інтерес до автоматизованих агентів, які можуть приймати "розумні" рішення та планувати контрзаходи, швидко зростає. Розглянуті в роботі [250] інтелектуальні системи кіберобману. Такі системи можуть динамічно планувати стратегію обману та використовувати декілька приводів для ефективного впровадження заходів кіберобману. Також, представлено прототип фреймворку, призначеного для спрощення розробки інструментів кіберобману для інтеграції з інтелектуальними агентами.

Кіберобман забезпечує проактивний кібер захист шляхом заплутування, введення в оману або відволікання зловмисників до хибних цілей. Однак розробка адаптивних методів кіберобману в реальних мережах є складним завданням через значні зусилля, які необхідні для реалізації основних функцій конфігурування мережевої інфраструктури, необхідних для підтримки активних операцій кіберобману, включаючи спостереження, планування та розгортання ресурсів приманок в реальному часі. Тому, розробники в цій галузі часто витрачають багато часу та зусиль на створення таких інфраструктурних функцій, а не зосереджуються на розробці складних стратегій для застосування кіберобману. В роботі [138] розроблено фрейворк активного кіберобману, який забезпечує розширюваний API та механізм синтезу для розробки розширених застосувань кіберобману. API можна використовувати для спостереження за діями зловмисника, створення багатостратегічних планів обману та швидкого їз розгортання шляхом автоматичного керування конфігурацією мережі та операційними завданнями.

В роботі [230] описана методологія обманної мережі, відповідно до якої трафік перенаправляється з цільової робочої мережі на обманну мережу з ідентичної конфігурацією, зводячи до мінімуму будь-яку подальшу компрометацію даних, а також дозволяє вивчати тактики та методи зловмисників. Для приховування передачі даних з мережі до мережі використовується складна техніка перезапису пакетів за допомогою технології програмно конфігурованої мережі. Запропонована техніка

може бути застосована до різних конфігурації фізичних/віртуальних/комбінованих мереж.

В роботі [162] проведено детальний огляд основних характеристик обманних систем, розвинуто порівняльну класифікацію, в тому числі розглянуто рішення із використанням штучного інтелекту. Проводено огляд різних обманних фрейморків та запропоновано комплексний обманних фреймворк, який має декілька рівнів, призначених для впровадження та підтримки обманних механізмів кібербезпеки. Запропонований фреймворк використовує методи штучного інтелекту на всіх етапах захисту, запобігання, виявлення та реагування на зловмисні дії.

Запропоновано веб-систему кіберобману повністю високого рівня взаємодії, яка містить гібридний модуль виявлення атак, що складається з класифікатора та аналізатора [3]. Модуль виявлення направляє зловмисні HTTP запити в систему кіберобману на основі докера, яка контролюється та керується котролером докера. Ключова функція профілювання зловмисників дозволяє запропонованій системі боротися із зловмисниками, які здійснюють атаки нульового дня. Запропонована система обману може опрацьовувати всі основні атаки веб-застосунків. Запропонований фреймворк є масштабованим, гнучким, підримує модифікацію, що дозволяє застосовувати його для систем інших типів, зокрема IoT.

Критичні системи повинні володіти властивістю живучості [169, 316, 317], тобто здатністю продовжувати функціонування в умовах атак, помилок та інших інцидентів. Зазвичай це забезпечується чотирирівневим захистом, який включає запобігання, виявлення, відновлення та адаптацію. Системи захисту нової генерації повинні бути інтелектуальними, адаптивними та випереджати зловмисників. При використанні на етапах запобігання та виявлення кіберобман дозволяє відстежувати наміри, цілі та стратегії зловмисників, що сприяє у розробці процедур відновлення та адаптації. Ці процедури дозволяють системі функціонувати в середовищі, в якому діють зловмисники. Представлено в роботі [169] високорівневу архітектуру розгортання, яка використовує кіберобман для живучості системи. Також, розглянуто інші аспекти живучості на основі кіберобману, такі як додаткові витрати, продуктивність, ефективність та точність.

Гнучкість віртуалізації робить хмарну систему більш динамічною та складною, що посилює непередбачувані проблеми кібербезпеки [46]. В цьому випадку механізми захисту, які використовують статичну реалізацію, не можуть захисти поверхню атаки в динамічній хмарній системи в режимі реального часу. Для вирішення цієї проблеми представлено в роботі [46] автоматизовану систему розгортання мережі приманок для активного захисту хмарного середовища на основі контейнерів, що дозволяє оцінювати зміни структури цільової системи та автоматично оптимізувати стратегію розгортання мережі приманок. При розробці створюється граф атак для формалізації можливих подій атак в контейнерній хмарній системі, поєднується концепція ступеню централізації з графом атак для оцінки та оптимізації процесу розгортання, розробляється структура для автоматичного створення, розгортання та налаштування мережі приманок.

В роботі [14] розроблено систему, що використовується як пастка для суб'єктів загрози, щоб вважати, що це реальна система. Вразливі веб-сервери на одному сервері, а безпечний веб-сервер та сервер бази даних розгортаються на іншому. Система має на меті виявити дев'ять різних типів атак. Для аналізу рівнів трафіку та впровадження необхідних стратегій пом'якшення ситуації використовуються перевірки на маршрутах.

У роботі [315] вдосконалено принципи побудови та функціонування приманок в задачах захисту комп'ютерних систем. Було досягнуто таких результатів: розроблено метод моніторингу подій з урахуванням потреб у детальному аудиті інформації з віртуалізованих операційних систем, що виконують роль приманок; розроблено поведінкові моделі взаємодії між зловмисником та повно-інтерактивною приманкою з врахуванням особливостей їх функціонування та підходів до проведення атак, що дозволлило визначити додаткові параметри при аналізі систем та спростити виявлення атак; розроблено метод захисту приманок від атак, спрямованих на блокування та унеможливлення доступу, що ґрунтується на алгоритмах математичних методів теорії групового врахування аргументів; отримав подальший розвиток метод контролю подій в приманці, що ґрунтується на аналізі послідовностей системних викликів; отримав подальший розвиток метод організації мереж віртуальних приманок, який, на відміну від існуючих, враховує можливість аналізу

мережного потоку зловмисником та здійснює приховану передачу відомостей з віртуалізованої операційної системи приманки в базу даних для подальшого аналізу, із можливістю блокуванням спроб НСД та атак на інші системи в Інтернеті від імені приманки. На основі запропонованих методів реалізовано програмні модулі на мові програмування C++, що дало можливість отримання відомостей щодо дій користувачів у легітимних системах і приманках, які функціонують в операційній системі Linux [315].

У роботі [185] представлено гібридну систему виявлення вторгнень, що поєднує штучні нейронні мережі та інтелектуальні приманки для великої обробки даних у режимі реального часу. Система використовує обманні технології, які інтегровані в архітектуру систем. ефективності моделі та зменшення складності обчислень.

Для застосування технології обману розробляють [53] різного типу приманки та пастки, які імітують роботу реальних систем. На ринку пропонується ряд рішень, робота яких ґрунтується на застосуванні технології обману зловмисників та зловмисного програмного забезпечення. Розглянемо характерні особливості таких систем.

Основними особливостями системи Acalvio ShadowPlex [21] є запатентована архітектура обманної системи та автономний обман. Ця система автоматизує і спрощує конфігурування та розгортання приманок та пасток за допомогою попередньо визначених обманних об’єктів та об’єктів, які генерує та розміщує система на основі рекомендацій та штучного інтелекту. Вона підтримує значну кількість обманних об’єктів, в тому числі приманки, які імітують хости із запущеними операційними системами, включаючи IoT хости, приманки для кінцевих точок, фейкові записи реєстру, облікові дані, спільні диски і т. п.

Однією з перших систем з використанням технології обману, яка додала можливість реагування була Attivo ThreatDefend Deception and Response Platform [223]. Система може бути розгорнута локально, в хмарному середовищі, в центрах даних чи в гібридному середовищі. Як і в інших системах, обманні об’єкти призначені для визначення зловмисників, які намагаються отримати доступ до мережі та даних. Ця система забезпечує не тільки фіксацію спроби доступу, а забезпечує взаємодію обманного об’єкту із зловмисником, імітуючи реакцію, яку він може очікувати від

реальних об’єктів. Тобто одночасно із захистом мережі забезпечується вивчення зловмисних намірів та тактики.

Система Proofpoint Identity Threat Defense [206] створює для зловмисника обманне середовище. Безагентна архітектура запобігає виявленню обманних об’єктів зловмисниками. Система визначає будь-які зміни в середовищі та активує обманні можливості для забезпечення зупинки зловмисника до отримання ним доступу до мережевих корпоративних ресурсів. Захист від атак та раннє реагування забезпечується для поштових сервісів, мобільного зв’язку, соціальних мереж та стаціонарних робочих станцій.

Система CounterCraft Cyber Deception Platform [71] використовує для виявлення зловмисників активні приманки. Ці приманки можуть бути розгорнуті як кінцеві точки, сервери або використані в онлайн платформах, вони є гнучкими до налаштувань. Система в цілому спроектована таким чином, щоб забезпечити онлайн взаємодію із зловмисниками. Система забезпечує можливість швидкого розгортання та можливість контролю, який ґрунтується на даних, зібраних в середовищі агентами.

Система Fidelis Deception platform [111] дозволяє користувачу швидко та динамічно створити обманне середовище, яке містить приманки та пастки застосунків користувача, сервісів, мережевих з’єднань, інтегрованих облікових даних активної директорії, пам’яті, кінцевих точок, серверів. Всі дії, які відбуваються в обманному середовищі, відслідковуються і доступні адміністратору для прийняття рішення щодо вивчення дій зловмисників, знешкодження атак та захисту щодо них. Перевагами Fidelis Deception platform є: автоматичне створення реалістичного обманного середовища, яке включає приманки та пастки різного типу; побудова дійсних приманок операційної системи разом з імітованими приманками, що покривають всю корпоративну мережу; швидке розгортання та ефективність від початку роботи; висока точність з відсутністю хибно позитивних спрацювань; постійне оновлення інтелектуального обманного середовища та проактивний захист.

Системою CommVault [253] забезпечується широкий набір рішень управління даними для їх захисту, менеджменту та оптимізації. В напрямку кібербезпеки CommVault пропонується аналіз ризиків, повний захист даних включно з їх автовідновленням, сканування загроз, захист активної директорії та баз даних.

Модулі системи поєднуються можливості раннього попередження з можливостями швидкого реагування для вчасної нейтралізації атак до того, як можу бути завдана шкода. Атаки «нульового дня» також виявляються та знешкоджуються, які важко або неможливо виявити за допомогою традиційних технологій. Також система дає змогу швидко виявляти приховані атаки, які розповсюджуються в мережевому середовищі та знешкодити їх. Тобто фактично ця система пропонує ідентифікацію та запобігання атакам ще до їх початку.

Система Labyrinth Deception Platform [78, 156] створює обманне середовище, яке імітує сервіси і наповнення реальної частини мережі. Основою рішення є так звані точки (points), які представляють собою інтелектуальні хости, що імітують програмне забезпечення, контент, роутери, пристрої тощо. Ці обманні точки виявляють зловмисну активність всередині корпоративної мережі, забезпечуючи комплексний захист від можливих атак. Обманне середовище заохочує зловмисників до дій, які дозволяють виявити та відслідкувати їх активність.

Системи обману класифікують за набором ознак, серед яких такі: тип обману; мета обману; рівень системи; тип розгортання; рівень поведінки та відповідей системи; керування системою. Тип обману характеризується інформаційними структурами, діями та тривалістю. Типи обману, які використовують системи: honey-х об’єкти; захист рухомою ціллю; заплутування; збурення та залучення зловмисників. В сучасних системах обману найбільш поширеними обманними об’єктами є honey-х та об’єкти захисту рухомою ціллю. До класу honey-х входять об’єкти, які прийнято називати термінами з початком honey-, а саме: honeypots; honeynets; honeytokens; honeymails; honeyurs тощо. Статична та передбачувана поведінка цільових систем надає значні переваги зловмисникам для планування успішних атак. Захист рухомої цілі змінює налаштування основної системи, зменшуючи рівень успішності кібератак. Зміни налаштувань, або кібермутації, засновані на захисті рухомих цілей, дозволяють системам автоматично змінювати свої параметри конфігурації в непередбачуваний, безпечний та адаптивний спосіб для проактивного обману зловмисників. Кібермутації включають мутацію хостів, маршрутів та віртуальних мереж.

Головна мета обманних систем, яку вони намагаються досягти, відповідає стадії боротьби з атакою. Відповідно, до мети систем відносять покращення запобігання

атакам, вдосконалення виявлення атак, пом’якшення наслідків успішних атак. В табл. 1.3 подано класифікацію обманних систем за визначеними критеріями.

Таблиця 1.3

Класифікація обманних систем

Критерій	Типи
1	2
Тип обману	- збурення (perturbation); - захист рухомої цілі (moving target defense); - заплутування (obfuscation); - змішування (mixing); - honey-x; - залучення зловмисника (attacker engagement) honey-x об'єкти призначені для залучення
Мета обманних систем	- покращити запобігання атаці; - вдосконалити виявлення атаки; - пом’якшити наслідки успішної атаки
Одиниця обману	- рішення; - відповідь; - сервіс; - діяльність; - слабкість; - продуктивність; - конфігурація; - дані
Рівень обманних систем	- мережа; - система; - застосунок; - дані
Розгортання обманних систем	- вбудована обманна система; - обманне рішення, яке додане під час функціонування цільової системи; - обманна система, встановлена перед цільовою системою; - ізольована обманна система

Продовження таблиці 1.3

1	2
Рівень поведінки та відповідей систем	- правдива; - наївно оманлива; - інтелектуально оманлива
Організація керування системою	- централізована; - частково централізована; - частково децентралізована; - децентралізована
Топологія мережі обманних систем	- статична; - динамічна
Цільові системи	- IoT; - промислова системи та мережі; - цифрові двійники; - бази даних; - веб-застосунки; - хмарні сервіси
Типи атак	- DoS атака; - DDoS атака; - атаки, що маніпулюють логікою; - атаки, що використовують прогалини в протоколі; - атаки, що використовують переповнення буфера
Розмір обманних систем	- обсяг ресурсів
Обсяг обману можливо, застосовувати до обманних об’єктів	- низького рівня; - високого рівня
Час обману можливо, застосовувати до обманних об’єктів	- короткочасний обман; - тривалий обман

Кінець таблиці 1.3

1	2
Периметр захисту цільових систем	- зовнішній; - внутрішній; - зовнішній та внутрішній
Доступність використання	- відкриті; - комерційні

Одиниця обману стосується рівня деталізації активу об’єкта, який використовується для здійснення обману. До одиниць обману відносяться рішення/вибір (наприклад, рішення про прийняття з’єднання від IP-адреси, яка не використовується), відповідь (наприклад, імітація мережевої відповіді), сервіс (наприклад, сервіс приманки), діяльність (наприклад, обчислювальна активність приманки), слабкість (наприклад, імітована вразливість), продуктивність (наприклад, затримка відповіді), конфігурація (наприклад, імітація топології мережі) та дані (наприклад, обліковий запис). Одиниці обману можуть використовуватися як окремо, так і комбінуватися в різних поєднаннях.

Рівень обманних систем відображає рівень цільової системи, яка захищається. Відповідно до рівня цільової системи виділяють такі рівні: рівень мережі; рівень системи; рівень застосунку; рівень даних. Тип розгортання систем характеризує шлях, яким такі системи інтегруються в цільові захисні системи. Залежно від рівня інтеграції система може бути вбудована, додана під час функціонування цільової системи, встановлена перед цільовою системою та ізольована. Вбудовані системи системи мають найвищий рівень інтеграції та інтегруються в захист цільових систем на етапі планування та розробки. Системи, що додаються під час функціонування, передбачають динамічне конфігурування обманних об'єктів в процесі функціонування цільової системи. Обманні системи, які встановлені перед цільовою системою та ізольовані, мають найменший ступінь інтеграції. Рівень поведінки та відповідей обманних систем характеризує рівень обману, який може забезпечити система відповідно до відповідей на сервісні запити. Відповідно до рівня інтелектуальності відповідей поведінка обманної системи може бути правдива, наївно оманлива та інтелектуально оманлива. В системах з правдивою поведінкою

відповіді на будь-який запит завжди відображають дійсні внутрішні стани системи. В системах з наївно оманливою поведінкою процеси намагаються обманути користувача з яким взаємодіють, штучними відповідями. Однак, якщо користувачу відома ця оманлива поведінка з попередньої взаємодії, то обман може бути виявлений та попередить зловмисника про наявність обманної системи. Найвищий рівень захисту цільової системи забезпечує система з інтелектуально оманливою поведінкою, завдяки чому функціонування такої системи для користувача не відрізняється від функціонування цільової системи навіть за умови попередньої взаємодії. Така поведінка системи передбачає використання інтелектуальних методів обробки запитів користувачів, а також методів машинного навчання та штучного інтелекту. Організація керування обманними системами характеризує взаємодію між компонентами систем та взаємодію із цільовою системою. В залежності від рівня централізації система може бути централізована, частково централізована, частково децентралізована та децентралізована. Топологія обманних систем може бути статичною та динамічною.

Обсяг обманних дій, що використовуються обманними системами, може змінюватися від низького рівня до високого. Час обманних дій може змінюватися від короткотривалого то тривалого. Обманні системи містять механізми для протидії різним типам атак, включаючи DoS атаки, розподілені DDoS атаки, атаки, що маніпулюють логікою, атаки, що використовують прогалини в протоколах, атаки, що використовують переповнення буфера тощо.

Тип цільової системи, для якої захисту якої призначена обманна система, характеризує власне цільову систему. Спектр вразливостей сучасних систем постійно розширюється із розвитком сучасних технологій, відповідно додається різновидів систем, для яких розробляють обманні системи. Зростання використання пристроїв IoT, що піддаються атакам, вимагає застосування механізмів захисту на основі приманок для різних типів таких пристроїв, зокрема пристроїв відеоспостереження та відеокамер, інфраструктури вимірювальних приладів тощо.

Порівняльна характеристика існуючих систем подана в табл. 1.4.

Таблиця 1.4

Порівняння обманних систем

№ з/п	Критерій	Acalvio ShadowPlex [21]	Attivo ThreatDefend Deception and Response Platform [223]	Proofpoint Identity Threat Defense [206]	Counter Craft Cyber Deception Platform [71]	Fidelis Deception platform [111]	Comm Vault [253]	Labyrinth Deception Platform [78, 156]
1	2	3	4	5	6	7	8	9
1	Розподілена архітектура	+	+	+	+	+	+	+
2	Використання ШІ в архітектурі систем	+	+	+	+	+	+	+
3	Наявність приманок	+	+	+	+	+	+	+
4	Запатентована /унікальна архітектура системи	+	+	+	+	+	+	+
5	Наявність агентів	+	+	-	+	+	+	+

Таким чином, системи з приманками в корпоративних мережах повинні бути такими, щоб швидко приймати рішення щодо залучення приманок без залучення адміністратора, гнучко змінювати свою архітектуру в залежності від стану корпоративних мереж, мати засоби керування пастками і приманками, бути поєднаними системами виявлення вторгнень з приманками та пастками. Недоліками пропонованих систем є їх односторонність, спрямування на невелику кількість завдань, не чітка визначеність щодо низького та високого рівнів взаємодії, переважно відсутність інтелектуального аналізу даних та прийняття рішень на його основі, залучення адміністратору до опрацювання результатів роботи, використання приманок окремо від пасток, слабкий ступінь інтеграції безпосередньо системи, її центру прийняття рішень та обманних засобів з приманок і пасток.

1.5. Визначення напрямів досліджень

Для вирішення науково–прикладної проблеми та, відповідно, мети дослідження з покращення функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж необхідно здійснити розроблення теорії і практики створення розподілених систем і розв’язати такі наукові задачі:

1) дослідити особливості функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж та проаналізувати ефективність роботи сучасних обманних систем з приманками та пастками, а також їх архітектуру і компоненти;

2) запропонувати концепцію вирішення науково-прикладної проблеми для покращення виявлення та протидії ЗПЗ і КА в корпоративних мережах на основі особливостей архітектури систем, організації функціонування та керування множиною приманок і пасток;

3) розробити принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА із забезпеченням ускладнення зловмисникам розуміння функціонування систем за рахунок формування різних наступних кроків систем при однакових початкових станах;

4) розробити концептуальну модель мультикомп’ютерних систем для забезпечення функціонування за їх підтримки антивірусних комбінованих приманок і пасток для виявлення ЗПЗ і КА в корпоративних мережах, попередження та протидії їх проникненню та формування архітектури систем самостійно, без залучення адміністратора, урізноманітнення варіантів відповідей від них при зловмисних впливах і забезпечення їх стійкості;

5) розробити математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, та подати їх аналітичними виразами, в яких врахувати особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи та сформувати

на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах;

6) розробити метод визначення варіанту централізації в мультикомп'ютерних системах, в якому забезпечити вибір наступного варіанту централізації з великої кількості варіантів без здійснення оцінювання всіх варіантів, щоб досягти швидкодії та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі;

7) розробити метод організації функціонування контролера прийняття рішень для забезпечення вибору одного варіанту виконання завдання із пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи для забезпечення формування поліморфних відповідей системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

8) розробити метод організації функціонування мультикомп'ютерних систем для забезпечення можливості до самостійної зміни своїх властивостей в архітектурі, організації елементів та компонентів і встановленні зв'язків між ними з урахуванням стану функційної та кібер- безпеки, а також виокремлення контролера прийняття рішень та центру системи для забезпечення багатоваріантності при опрацюванні відповіді на події, які викликані зовнішніми та внутрішніми впливами на систему в корпоративних мережах;

9) розробити метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснити збір даних та кластеризацію схожих зловмисників з використанням мультикомп'ютерних систем з антивірусними комбінованими приманками і пастками та забезпечити в ньому різні варіантів відповідей на повторювані події;

10) розробити метод виявлення ЗПЗ і КА, який реалізується в архітектурі мультикомп'ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, а також в ньому реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи) для забезпечення адаптивного, варіативного реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнення зловмисникам розуміння логіки її функціонування;

11) розробити мультикомп’ютерну систему антивірусних комбінованих приманок та пасток для підтвердження спроможності реалізації запропонованих принципу та методів синтезу таких систем, підтвердження їх практичного створення та використання в експериментальних дослідженнях для порівняння з відомими системами виявлення і впровадити розроблену систему в корпоративних мережах.

1.6. Висновки до першого розділу

Дослідження функціонування ЗПЗ та здійснення КА зловмисниками у корпоративних мережах, показало наступні результати:

– зловмисники постійно розробляють нові моделі комп’ютерних атак;

– зловмисники для проведення атак використовують різноманітне ЗПЗ;

– зловмисники використовують засоби, які призначені для забезпечення функціонування корпоративних мереж, для виконання зловмисних дій;

– застосування сучасних ефективних методів не гарантує ефективної протидії зловмисним діям в корпоративних мережах у зв’язку з необхідністю постійного вдосконалення методів, систем та засобів протидії;

– використання систем з приманками та пастками для покращення ефективності виявлення ЗПЗ та КА є ефективним, але дорогим рішенням і потребує залучення кваліфікованого адміністратора мережі до прийняття рішення, що знижує оперативність в прийнятті рішення;

– існуючі системи з приманками та пастками побудовані переважно з використанням централізованої архітектури або з розміщенням центру у фіксованих вузлах, що активізує зловмисників до виявлення центру для атак на нього.

Відомі системи виявлення ЗПЗ та КА не забезпечують належної протидії при комбінованих атаках, особливо коли зловмисні дії здійснюються з середини та ззовні корпоративних мереж. Враховуючи актуальність виявлення ЗПЗ та КА в корпоративних мережах, необхідна розробка нових принципів та методів синтезу систем з приманками та пастками для виявлення ЗПЗ та КА в корпоративних мережах, особливо для постійно оновлюваних зловмисниками моделей КА та змінюваного ЗПЗ. З метою покращення ефективності виявлення ЗПЗ та КА у корпоративних

мережах актуальним є розроблення елементів теорії і практики створення мультикомп’ютерних систем виявлення ЗПЗ та КА з використанням антивірусних комбінованих приманок та пасток за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Основні результати розділу опубліковані у працях [286, 295, 296, 297, 298, 322].

РОЗДІЛ 2.
МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК ДЛЯ ВИЯВЛЕННЯ ЗПЗ ТА КА У КОРПОРАТИВНИХ МЕРЕЖАХ

При експлуатації корпоративних мереж використовуються різноманітні системи виявлення та протидії ЗПЗ та КА. Архітектура таких систем та їх особливості повинні бути невідомими для зловмисників. Це дасть змогу забезпечити ефективну протидію зловмисникам, які здійснюють спроби проникнення в корпоративні мережі, використовуючи різноманітні способи та засоби. Перспективним напрямом дослідження стає розробка нової архітектури систем, які б використовувались на різних етапах виявлення та протидії ЗПЗ та КА. Ці системи могли б стати основою синтезу систем з приманками та пастками для виявлення та протидії ЗПЗ і КА, що демонструють свою ефективність і, відповідно, зацікавленість в користувачів. Це підтверджується, також тим, що спостерігається стрімкий розвиток таких систем на ринку спеціалізованого антивірусного ПЗ для використання в корпоративних мережах. Розміщення таких систем в корпоративних мережах повинно залучати більшість з комп'ютерних станцій, які активно використовуються та функціонують в комп'ютерній мережі. Тому, поєднання комп'ютерних станцій з використанням проміжного ПЗ дасть змогу створити спеціалізовану мультикомп'ютерну систему. Важливою особливістю в архітектурі таких систем є реалізація спроможності, побудованої згідно неї системи, приймати рішення, відповідно до поточного стану в цілому, зокрема, для уникнення вивчення поведінки системи зловмисниками при повторенні їх дій спроможності системи при однакових початкових станах вибирати різні наступні кроки. Така вимога потребує синтезу в архітектурі системи окремого контролера за результатами прийнятих рішень відповідною підсистемою.

Для вирішення проблеми з покращення функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж здійснимо розроблення концепції, принципу синтезу та концептуальної моделі таких систем.

2.1. Концепція та принцип синтезу мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах

Користувачам комп'ютерних мереж необхідні системи для виявлення ЗПЗ та КА, які дадуть змогу, крім забезпечення безпеки на різних етапах можливого проникнення в комп'ютерні системи чи станції, що об'єднані в мережу, для етапу, коли на всіх попередніх етапах такі виявлення не були здійснені, але могли мати місце проникнення в систему. Тобто, розглядатимемо ті системи, які використовуватимуться для виявлення ЗПЗ та КА, які змогли пройти всі етапи захисту комп'ютерних станцій та мережі, і їх відсоток може бути невеликим. Крім того, такі системи повинні залучатись і до попередження та виявлення ЗПЗ та КА на всіх етапах їх спроб проникнення та інфікування об'єктів КС, як додаткові системи. Розробники різних засобів попередження, виявлення та протидії ЗПЗ та КА заявляють про великий відсоток правильного достовірного виявлення, але невеликий відсоток для невиявлених ЗПЗ та КА при стрімкому щорічному зростанні кількості таких засобів може бути великим кількісно. Це може призвести до їх проникнення в КС, що створить проблеми користувачам і, дійсно, може бути представлений певною кількістю таких засобів, для виявлення яких необхідні системи виявлення та протидії, що матимуть нестандартні конфігурування і спроможності до автоматичної зміни своєї архітектури та прийнятих рішень без втручання користувача. Потреба в таких системах зростає і через необхідність та бажання здійснення зі сторони власників комп'ютерних мереж, які, наприклад, експлуатуються на підприємствах, прихованого спостереження за процесами в мережі та виявлення тих з них, які можуть створити загрози даним, що зберігаються у відповідних ресурсах в мережі.

Серед різних за призначенням систем виявлення ЗПЗ та КА є системи, які крім виявлення загроз створюють в комп'ютерних мережах хибні об'єкти для атак, що надає змогу адміністраторам таких мереж можливість відслідковувати процеси в мережах, які є зловмисними чи аномальними і потребують зупинки. Тому, перспективними для розробки є системи, які орієнтовані на виявлення ЗПЗ та КА, що пройшли певні етапи захисту, на яких використовувались традиційні засоби і системи

попередження, виявлення та протидії, призначення яких та можливі варіанти конфігурування при використанні відомі зловмисникам. Серед таких систем особливе місце в класифікації займають системи попередження, виявлення та протидії із певною множиною приманок та пасток для ЗПЗ та КА. Їх використання створює хибні об’єкти атаки для зловмисника та дозволяє зберегти відомості про такі атаки та розповсюдження ЗПЗ в комп’ютерних станціях в мережі.

Для покращення функціонування систем виявлення та протидії ЗПЗ та КА за рахунок використання приманок та пасток, необхідним є інтегрування цих засобів в складні системи із залученням всіх комп’ютерних станцій в мережі та організації функціонування їх таким чином, щоб вони могли реагувати на зловмисні та аномальні процеси сумісно та без втручання користувача. Таким чином, необхідним є побудова не однієї приманки чи пастки в певній комп’ютерній станції, а мережі приманок та пасток для здійснення комплексного захисту комп’ютерної мережі на етапі коли КА змогли пройти через міжмережне екранування, а ЗПЗ змогло подолати перевірку антивірусними засобами і системами. Така система з приманками та пастками включатиме приманки, які здійснюють моніторинг зловмисного трафіку, тому вона може забезпечити максимально швидке його виявлення, а також виявлення патернів нових атак. Пастки при поєднанні їх в мережі можуть імітувати тіньову комп’ютерну мережу. Така система з приманок і пасток може бути комбінованою з них системою і для досягнення ефективного результату повинна включати тіньові приманки та пастки, які дозволять встановити та відслідкувати поведінку зловмисника при атаці, а також виявити ЗПЗ та КА з більшою вірогідністю. Важливим завданням, яке має бути вирішене при використанні таких систем полягає не тільки у застосуванні приманок та пасток, але й в управлінні їх використанням. Ефективність таких засобів суттєво залежить від організаційної складової частини системи. Використовуючи такі засоби в реальних системах, покращення функціонування може бути досягнуто за рахунок заміни оператора чи користувача на відповідну підсистему, яка зможе забезпечити ефективну організацію. Побудова такої системи можлива з використанням мультиагентних систем та компонентів штучного інтелекту.

Мультиагентна система приманок і пасток може містити множину приманок та пасток різного типу та призначення. Крім того, самі приманки та пастки можуть бути

побудовані з використанням компонентів штучного інтелекту. Приманки та пастки системи, які є інтелектуальними, мають ознаки інтелектуального агенту, володіють автономною та гнучкою поведінкою, що передбачає наявність в них таких характеристик:

1) реактивність – інтелектуальна приманка та пастка здатна сприймати середовище, в якому вона працює, та своєчасно реагувати на зміни, які в ньому відбуваються, відповідно до цілей функціонування;

2) проактивність – інтелектуальна приманка та пастка здатна проявляти цілеспрямовану поведінку, що передбачає прояв ініціативи, відповідно до цілей функціонування;

3) соціальні можливості – інтелектуальна приманка та пастка здатна взаємодіяти з іншими приманками (та іншими пристроями) та пастками системи відповідно до цілей функціонування.

Антивірусні приманки та пастки як окремі частини системи можуть бути окремо приманками чи пастками, але можуть бути скомбіновані разом як окремі частини системи. Взаємодія їх функціоналів між собою може бути здійснена за потреби. Також, їх інтелектуалізація може стосуватись окремо приманок і окремо пасток, коли вони поєднані, але може і бути віднесеною до обох з них одночасно.

Використання лише програмної системи одночасно в якості і приманок та системи, в якій будуть прийматись рішення щодо наступного опрацювання отриманих подій в мережі приманок та пасток і окремих приманках та пастках, є недостатнім. Це пов’язано з особливостями проведення КА та поведінкою ЗПЗ при поширенні і виконанні деструктивних дій. Тобто, вплив ЗПЗ та КА відбувається програмними засобами і, тому, забезпечення протидії винятково програмними засобами не завжди забезпечує бажаний результат, що підтверджується і розробниками систем попередження і виявлення вторгнень та антивірусних засобів. Крім того, організація ефективної взаємодії між комп’ютерними станціями в корпоративних мережах для підтримки мережних застосунків суттєво залежить від часу передачі повідомлень і їх обробки. Враховуючи такі особливості при побудові приманок, пасток та мереж приманок і пасток необхідно синтезувати систему, в якій до процесу виявлення ЗПЗ та КА були б залучені, також, комп’ютерні станції в

мережі. І така система могла б в процесі обробки отриманих даних з приманок та пасток приймати рішення про свої наступні кроки, зокрема і в частині зміни конфігурування та використання комп'ютерних станцій в мережі. Тому, синтезуємо клас мультикомп'ютерних систем комбінованих антивірусних приманок та пасток в корпоративних комп'ютерних мережах для виявлення ЗПЗ та КА поєднавши в них такі складові елементи і компоненти:

- мультикомп'ютерну систему;
- мультиагентну систему;
- приманки та пастки для виявлення ЗПЗ та КА.

А також, такі особливості і характерні властивості:

- адаптивність;
- гнучкість;
- самоорганізація;
- прийняття рішень;
- контролер прийнятих рішень;
- колективна робота агентів.

Такі вимоги до архітектури мультикомп'ютерних систем комбінованих антивірусних приманок та пасток в корпоративних мережах дадуть змогу покращити їх функціонування, бо не потребуватимуть втручання користувача при прийнятті рішень в різних поточних станах, та забезпечать спроможності користувачів корпоративних мереж до виявлення та протидії ЗПЗ та КА, покращивши ефективність виявлення та протидії.

Для синтезу систем з такими характеристиками та функційними можливостями потрібно розробити принцип їх синтезу, щоб вони містили комбіновані приманки і пастки та контролер прийняття рішень.

Такий принцип повинен визначати загальні вимоги до побудови елементів теорії створення мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. При виокремлені таких систем серед всіх систем такого призначення принцип буде відображати ті суттєві характеристики, які відповідають за правильне функціонування системи. Саме без формалізації та подання правильного функціонування системи, вона не буде

виконувати свого призначення. Крім того, принцип синтезу таких систем дасть змогу сформувати клас таких систем та буде розвивати елементи теорії мультикомп'ютерних систем в частині саме систем, в яких здійснено поєднання з контролером прийняття рішень спеціалізованого функціоналу для виявлення ЗПЗ з використанням комбінованих приманок і пасток.

Такий принцип в контексті розвитку елементів теорії мультикомп'ютерних систем є систематичним принципом, бо відноситься до задання механізмів функціонування систем. При цьому в ньому потрібно задати такі особливості і характерні властивості систем, щоб відображалась найменша кількість факторів, які визначатимуть, як функціонуватиме система.

Принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА задамо з врахуванням деталізації контролера прийняття рішень системи та спеціалізованого функціоналу для виявлення ЗПЗ з використанням комбінованих приманок і пасток.

Архітектура мультикомп'ютерних систем з врахуванням принципу синтезу таких систем може бути централізованою, децентралізованою або гібридною змішаною) з різними ступенями централізації. Відповідно, центр прийняття рішень таких мультикомп'ютерних системи може бути в одній або декількох компонентах системи і це, як і архітектура, не впливатиме на сам принцип синтезу систем та його не виконання. Центр може переміщуватись між компонентами в залежності від поточного стану системи. Також, архітектура таких систем може гнучко перебудовуватись за потреб при зміні зовнішнього середовища і впливів на систему, що характеризує специфіку виконуваних нею завдань. Але при цьому такі особливості не впливають на вимогу принципу синтезу таких систем. Особливістю пропонованого принципу синтезу систем є забезпечення контролю за прийнятими рішеннями в центрі прийняття рішень, тобто обов'язкова наявність контролера прийняття рішень. При цьому контролер прийнятих рішень повинен мати можливість впливати на їх імплементацію через затвердження до виконання або відхилення пропонованих наступних кроків системи, а також затвердження до виконання іншого близького або альтернативного рішення. Такі особливості контролера прийняття

рішень вимагаються тим, що система призначена для виконання специфічних завдань, які пов’язані з взаємодією компонентів чи елементів системи із ЗПЗ та КА. Відповідно, зловмисники можуть повторювати свої дії багатократно однаково, що буде переводити систему до одного і того ж стану та її відповідні компоненти. В результаті такого тестування системи зловмисник буде мати змогу вивчити її поведінку і за певний час зможе її обійти. Тому, контролер прийнятих рішень системи повинен здійснювати вплив на остаточне прийняття рішень через вибір наступних кроків системи, як реакцію на зміну зовнішнього середовища та стану системи і її компонент. Така зміна у виборі наступних кроків системи призведе до ускладнень для зловмисника в частині вивчення поведінки засобів виявлення протидії ЗПЗ та КА в корпоративних мережах.

Вимога поєднання в таких системах спеціалізованого функціоналу для опрацювання подій в корпоративній мережі, тобто розподілення в просторі, та наявність підсистеми прийняття рішень, в якій будуть напрацьовуватись рішення, причому їх втілення можливе тільки після затвердження контролером, встановлює фактори для розроблення принципу синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. Зокрема, формалізуємо системи, їх складові частини і їх властивості, які необхідні для виконання вимог принципу синтезу систем.

Позначимо символом $\mathfrak{P}$ принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. Тоді, ним як відображенням з усієї множини мультикомп’ютерних систем $\mathfrak{C}$ буде сформовано підмножину систем $\mathfrak{S}$, для яких буде виконуватись вимога принципу $\mathfrak{P}$. Тобто, задане відображення формулою $\mathfrak{C} \xrightarrow{\mathfrak{P}} \mathfrak{S}$ буде формувати клас систем із заданими принципом $\mathfrak{P}$ вимогами і потрібно деталізувати компоненти таких систем для подальшого їх синтезу. Задамо кожну з визначальних компонент та властивостей, що потребують імплементації в архітектурі таких систем, підмножиною $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин). Наявність можливих варіантів серед $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) є допустимим. Наприклад, такі системи можуть бути централізованими, децентралізованими або гібридними (змішаними) з певним ступенем централізації, що теж може надати

можливості для їх поділу на окремі типи, і, при цьому, вони відповідатимуть вимогам принципу $\mathfrak{P}$.

Розглянемо можливі варіанти компонентів та визначальних властивостей для класу систем $\mathfrak{S}$: $\mathfrak{V}_1$ – тип архітектури системи (централізована, децентралізована, гібридна (змішана, комбінована)); $\mathfrak{V}_2$ – типи та кількість центрів в архітектурі системи (цілісний в одній компоненті, поділений на рівнозначні частини в різних компонентах, поділений ієрархічно в різних компонентах, цілісний ієрархічний в різних компонентах); $\mathfrak{V}_3$ – адаптивність системи при зміні зовнішніх умов (зміна алгоритмів свого функціонування, зміна архітектури системи, зміна алгоритмів функціонування та зміна архітектури системи); $\mathfrak{V}_4$ – характер змін в центрі системи (зміна значень параметрів, зміна в архітектурі центру, зміна значень параметрів і зміна в архітектурі центру); $\mathfrak{V}_5$ – самоорганізація системи (створення організації функціонування складної системи, відтворення організації функціонування складної системи, вдосконалення організації функціонування складної системи), $\mathfrak{V}_6$ – гнучкість системи (швидке переналаштування системи під впливом зовнішніх подій, латентне переналаштування системи, повільне переналаштування системи); $\mathfrak{V}_7$ – самостійність у прийнятті рішень (прийняття рішень всім центром системи, прийняття рішення частиною центру системи); $\mathfrak{V}_8$ – вплив на систему (внутрішні події, зовнішні події, внутрішні і зовнішні події); $\mathfrak{V}_9$ – наявність агентів в системі для прийняття рішень (мультиагентність, один агент, відсутність агентів); $\mathfrak{V}_{10}$ – контроль прийнятих рішень в системі (наявність контролера, відсутність контролера); $\mathfrak{V}_{11}$ – наявність спеціалізованого функціоналу в системі (формування спеціалізованим функціоналом внутрішніх подій в системі за результатами виконання завдань, вплив результатів виконання завдань спеціалізованим функціоналом на зміну в архітектурі системи, формування внутрішніх подій в системі та відсутність зв’язку впливу результатів виконання завдань спеціалізованим функціоналом на зміну архітектури системи, відсутність зв’язку впливу результатів виконання завдань спеціалізованим функціоналом на зміну архітектури системи та формування внутрішніх подій в системі). Кожна з характеристик $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) є множиною, в якій наявні типові елементи, що відносяться до систем $\mathfrak{C}$. При застосуванні принципу $\mathfrak{P}$ синтезуються системи типу $\mathfrak{S}$. Для здійснення синтезу

систем згідно принципу $\mathfrak{P}$, тобто формування множини визначальних характеристик для системи типу $\mathfrak{S}$ в їх архітектурі згідно визначення прямого добутку множин $\mathfrak{V}_i$ ($i = 1,2,\dots,n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) задамо так:

$$\mathfrak{S} = \left\{\left(\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_{10,1}, \mathfrak{v}_{11}\right) \middle| \left(\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_{10,1}, \mathfrak{v}_{11}\right) \in \mathfrak{V}_1 \times \mathfrak{V}_2 \times \dots \times \mathfrak{V}_{10,1} \times \mathfrak{V}_{11}\right\}, \quad (2.1)$$

де $\mathfrak{V}_i$ ($i = 1,2,\dots,n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) – підмножини з елементами, що характеризують особливості архітектури систем; $\mathfrak{v}_{10,1}$ – елемент, що визначає наявність контролера в системі; $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$; множина $\mathfrak{V}_{10,1}$ – одноелементна множина; $\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_9, \mathfrak{v}_{11}$ – позначення елементів в множинах $\mathfrak{V}_1, \mathfrak{V}_2, \dots, \mathfrak{V}_9, \mathfrak{V}_{11}$ відповідно.

Граф відображення визначальних характеристик для систем типу $\mathfrak{S}$ в їх архітектурі у вершинах, що відповідають елементам множин $\mathfrak{V}_i$ ($i = 1,2,\dots,n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин), зображено на рис. 2.1.

Будь-який замкнений маршрут в графі відображення визначальних характеристик в архітектурі систем типу $\mathfrak{S}$ з рис. 2.1 буде завжди включати вершину $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$ з множини $\mathfrak{V}_{10,1}$. Це означає, що граф відображає архітектуру різних систем згідно принципу синтезу $\mathfrak{P}$. Вершини, які відповідають елементам певної множини $\mathfrak{V}_i$ ($i = 1,2,\dots,n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) при визначенні замкненого маршруту можуть йому належати, тобто з однієї множини до маршруту можуть включатись декілька елементів, а не тільки один. Це відображає інші варіанти в архітектурі систем типу $\mathfrak{S}$. Наприклад, система може мати не винятково централізовану, або децентралізовану, або змішану архітектури. Але вона у варіанті змішаної щодо централізації архітектури може мати централізовану і децентралізовану теж, наприклад з певними інтервалами часу тип архітектури може змінюватись на змішану, потім на централізовану і далі повертатись до змішаної або переходити до децентралізованої. Також, може бути рівень централізації і його особливість різними. Аналогічно і решта визначальних характеристик в архітектурі систем типу $\mathfrak{S}$ можуть мати такі ж особливості. Тобто, в системах типу $\mathfrak{S}$ може бути декілька елементів з певної множини $\mathfrak{V}_i$ ($i = 1,2,\dots,9,11,\dots,n_{\mathfrak{V}}$, $i \neq 10$, $n_{\mathfrak{V}}$ – кількість підмножин). Граф з рис. 2.1 поза межами наявних ребер і вершин може містити інші вершини і ребра. Але замкнений маршрут так само буде їх охоплювати і, відповідно, включати вершини і

ребра. В результаті охоплені маршрутом вершини будуть відображати визначальні характеристики синтезовані в системах типу $\mathfrak{S}$. З множини $\mathfrak{V}_{10}$ в маршрут буде включатись лише одна вершина, що належатиме цій множині. Решта вершин будуть ізольованими і в жоден маршрут не будуть включені.

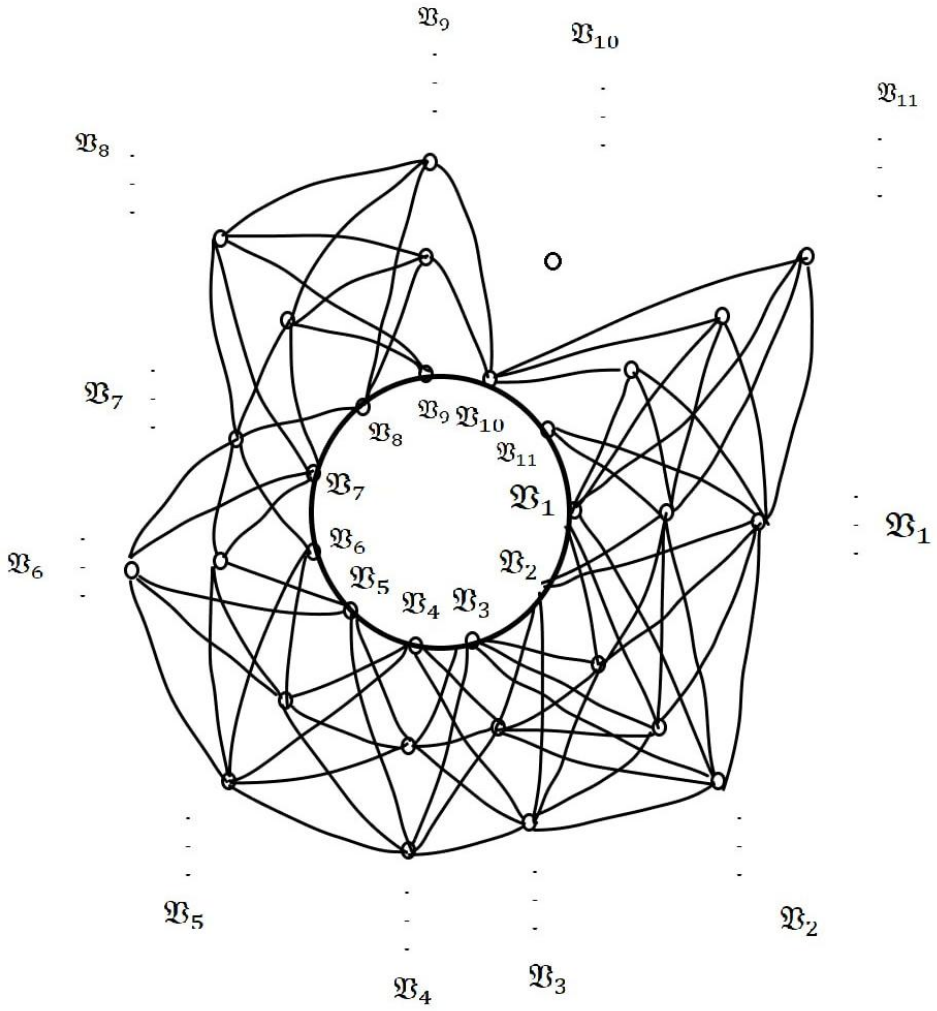


Рисунок 2.1 - Граф відображення визначальних характеристик в архітектурі систем типу $\mathfrak{S}$

Таким чином, кількість систем типу $\mathfrak{S}$ згідно принципу синтезу $\mathfrak{P}$ є різною, але згідно формули (2.1) всіх їх поєднує наявність в їх архітектурі контролера. Кількість підмножин $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) може бути різною, зокрема і менше, ніж $n_{\mathfrak{V}}$, але наявність одноелементної множини $\mathfrak{V}_{10,1}$ та множини $\mathfrak{V}_{11}$ в прямому добутку множин є обов'язковим.

Такий поділ архітектури систем за внутрішньою будовою дає змогу визначити необхідні елементи та компоненти в архітектурі системи, яка міститиме контролер та

спеціалізований функціонал, і є основою для розробки концепції та методологічних основ синтезу таких систем. На відміну від відомих принципів синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, розроблений принцип синтезу таких систем містить дві визначальні вимоги щодо архітектури систем. Контролер прийнятих рішень відокремлено від центру системи, що дає змогу формувати його архітектуру відокремлено від архітектури центру системи і, як наслідок, приймати рішення щодо напрацьованих в центрі системи рішень незалежно від нього. Це обумовлено специфікою системи та надає переваги системі безпосередньо перед зловмисниками чи їх засобами, бо формує різні остаточні відповіді системи за однакових початкових умов в різні проміжки часу, що заплутує зловмисників. Наявність спеціалізованого функціоналу, який впливатиме на внутрішні події в системі та зміну її архітектури, тобто взаємодія в системі підсистем, що забезпечують її безпосереднє функціонування та спеціалізований функціонал для виявлення та протидії ЗПЗ і КА, дає змогу покращити стійкість системи та оперативність в прийнятті рішень.

Принцип синтезу $\mathfrak{P}$, згідно якого можуть бути створені системи типу $\mathfrak{S}$, є таким, що згідно нього, також, буде здійснено перебудову архітектури в функціонуючих системах динамічно і нова архітектура теж буде відповідати системам типу $\mathfrak{S}$. Тобто, не тільки відбір систем типу $\mathfrak{S}$ з усієї кількості систем, але і формування в процесі функціонування системи, відмінної від попередньої архітектури, нової архітектури системи, яка б відповідала принципу синтезу $\mathfrak{P}$ та була віднесена до систем типу $\mathfrak{S}$.

Концепція вирішення розглядуваної проблеми полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для покращення виявлення ЗПЗ та КА в корпоративних мережах, що базується на поєднанні таких визначальних властивостей та їх синтезу в системах, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, щодо самостійності у прийнятті рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для

прийняття рішень, щодо контролю прийнятих рішень в системі, щодо особливості спеціалізованого функціоналу з комбінованих антивірусних приманок і пасток в системі.

Сформульована концепція базується на таких концептуальних положеннях:

1. Розвиток елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах згідно принципів самоорганізації, адаптивності, гнучкості, прийняття рішень, контролю прийнятих рішень, колективної роботи агентів, централізації/децентралізації, комбінування та принципу синтезу таких систем з динамічною зміною їх архітектури та обов'язковим контролем прийнятих рішень.

2. Принцип синтезу, концептуальна модель та метод організації функціонування мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах, що базується на поєднанні таких визначальних властивостей та їх синтезу в системах, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, щодо самостійності у прийнятті рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, щодо контролю прийнятих рішень в системі, щодо особливості спеціалізованого функціоналу з комбінованих антивірусних приманок і пасток в системі.

3. Модель та метод організації функціонування систем комбінованих антивірусних приманок і пасток, а також методи виявлення ЗПЗ та КА в корпоративних мережах з використанням комбінованих антивірусних приманок і пасток, імплементовані в архітектуру мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень, для покращення виявлення.

Для синтезу систем типу $\mathfrak{S}$ згідно концепції та принципу синтезу $\mathfrak{P}$ повинні бути враховані такі принципи: самоорганізації; адаптивності; гнучкості; прийняття рішень; контролю прийнятих рішень; колективної роботи агентів;

централізації/децентралізації; комбінування. Причому принцип синтезу $\mathfrak{P}$ буде використовуватись в поєднанні з принципами адаптивності і гнучкості, а також сам він буде базуватись на принципах самоорганізації; адаптивності; гнучкості; прийняття рішень; контролю прийнятих рішень; колективної роботи агентів; централізації/децентралізації; комбінування. Таке формування принципу синтезу $\mathfrak{P}$ систем типу $\mathfrak{S}$ дає змогу відділити безпосередньо саму систему від тієї частини, в якій будуть сформовані остаточні рішення щодо подальших кроків всієї системи.

Для деталізації архітектури мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, яка відповідає запропонованим концепції та принципу синтезу таких систем, потрібно розробити концептуальну модель систем з її елементами.

2.2. Елементи концептуальної моделі мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА

Для створення мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА згідно принципу $\mathfrak{P}$ синтезу таких систем потрібно розробити концептуальну модель такого класу систем $\mathfrak{S}$. Наявність такої архітектури мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА дасть змогу здійснити розроблення методологічних основ та методів створення таких систем. Розробку концептуальної моделі систем класу $\mathfrak{S}$ здійснимо з використанням математичного апарату абстрактної алгебри та теорії множин. Для розробки концептуальної моделі систем класу $\mathfrak{S}$ здійснимо аналіз можливих її складових елементів, визначимо їх та взаємодію їх між собою в контексті безпосередньо формування самої моделі. Тобто задамо всі особливості в архітектурі систем типу $\mathfrak{S}$, які визначені згідно принципу синтезу $\mathfrak{P}$, відповідними множинами та введемо відповідні принципу обмеження на елементи множин і зв'язки між ними.

2.2.1. Базове подання концептуальної моделі мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень

В концептуальній моделі мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, архітектура якої віднесена до класу систем $\mathfrak{S}$, будуть відображені елементи та компоненти, як складові частини архітектури. Тому, введемо підмножини для таких елементів та компонентів в архітектурі системи і задамо загальну множину $\mathfrak{M}_{\mathfrak{S}}$ для них так:

$$\mathfrak{M}_{\mathfrak{S}} = \bigcup_{i=1}^{n_{\mathfrak{M}_{\mathfrak{S}}}} \mathfrak{M}_i, \tag{2.2}$$

де $\mathfrak{M}_i$ - i – та підмножина для певних елементів та компонентів в архітектурі системи; $i = 1,2, \dots, n_{\mathfrak{M}_{\mathfrak{S}}}$; $n_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин.

Згідно формули (2.2) задамо кожну з введених підмножин $\mathfrak{M}_i$ ($i = 1,2, \dots, n_{\mathfrak{M}_{\mathfrak{S}}}$; $n_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин) її елементами та встановимо для кожного з них в межах заданих підмножин їх вплив на функційну та кібербезпеку системи. Визначення рівня безпеки конкретних елементів та компонентів в архітектурі системи задамо множиною функцій, кожна з функцій якої буде застосовна до елементів конкретної заданої підмножини $\mathfrak{M}_i$ ($i = 1,2, \dots, n_{\mathfrak{M}_{\mathfrak{S}}}$; $n_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин).

Задамо кожну з підмножин елементів та компонентів в архітектурі мультикомп'ютерних систем класу $\mathfrak{S}$ через їх елементи так:

$$\mathfrak{M}_j = \left\{m_{j,1}, m_{j,2}, \dots, m_{j,n_{\mathfrak{M}_j}}\right\}; \tag{2.3}$$

$$\mathfrak{M}_{10} = \left\{m_{10,1}\right\},$$

де $m_{j,I}$ – I-елемент $\mathfrak{M}_j$ підмножини; $I = 1,2, \dots, n_{\mathfrak{M}_j}$; $j = 1,2, \dots, 9,11, \dots, n_{\mathfrak{M}_{\mathfrak{S}}}$; $n_{\mathfrak{M}_j}$ – кількість елементів підмножини $\mathfrak{M}_j$; $n_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин.

Елемент підмножини $\mathfrak{M}_{10}$ є твірним і визначальним для формування архітектури систем класу $\mathfrak{S}$. Тому, підмножина $\mathfrak{M}_{10}$ в формулі (2.3) визначена одним елементом.

Множина $\mathfrak{M}_{\mathfrak{S}}$ буде містити всі елементи підмножин $\mathfrak{M}_j$ ($j = 1,2, \dots, n_{\mathfrak{M}_{\mathfrak{S}}}$; $n_{\mathfrak{M}_j}$ – кількість елементів підмножини $\mathfrak{M}_j$). В архітектурі системи класу $\mathfrak{S}$ елементи

множини $\mathfrak{M}_{\mathfrak{S}}$ можуть бути всі або може бути частина з них. Також, може бути варіант формування системи згідно входження по одному елементу з кожної із підмножин $\mathfrak{M}_{\mathfrak{j}}$ ($\mathfrak{j} = 1,2, \dots, \mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{j}}}$ – кількість елементів підмножини $\mathfrak{M}_{\mathfrak{j}}$). Тобто варіантів архітектури системи класу $\mathfrak{S}$ з комбінуванням елементів множини $\mathfrak{M}_{\mathfrak{S}}$ може бути багато, але в загальному випадку їх кількість є скінченою.

Введемо множину функцій $\mathfrak{F} = \{\mathfrak{f}_1, \mathfrak{f}_2, \dots, \mathfrak{f}_{\mathfrak{n}_{\mathfrak{F}}}\}$ ($\mathfrak{n}_{\mathfrak{F}}$ – кількість функцій в множині $\mathfrak{F}$), в якій функції будуть виконувати операції над елементами множини $\mathfrak{M}_{\mathfrak{S}}$ як окремими одноелементними множинами. Ці функції будуть діями над елементами множини $\mathfrak{M}_{\mathfrak{S}}$ і результатом цих дій буде формування різних підмножин. Такі підмножини відображатимуть архітектуру системи класу $\mathfrak{S}$. Серед цих функцій будуть такі: об'єднання елементів; вилучення елементу з підмножини; перетворення підмножини з декількох елементів на декілька одноелементних підмножин; об'єднання декількох підмножин, зміна елементів в підмножинах та інших. Таким чином, елементи множини $\mathfrak{M}_{\mathfrak{S}}$ будемо розглядати як одноелементні множини, тоді результатом виконання функцій з множини $\mathfrak{F}$ будуть підмножини з елементів множини $\mathfrak{M}_{\mathfrak{S}}$, тобто множини підмножин $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Функції будуть операторами в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Функції компонують систему класу $\mathfrak{S}$ з елементів підмножин. При цьому можуть бути одиничні елементи, а також можуть бути комбіновані варіанти з одиничних варіантів. Це досягається за рахунок розширення кількості елементів та, відповідно, їх комбінувань при переході до множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Підмножина $\mathfrak{M}_{10}$ буде визначена одним елементом і вона буде присутня в усіх варіантах поєднань підмножин, тобто елемент цієї множини буде в кожному об'єднанні підмножин. Інакше, не всі елементи множини підмножин $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ формуватимуть архітектури систем класу $\mathfrak{S}$. Таке обмеження до підмножин множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ є обов'язковим. В результати підмножини міститимуть об'єднання мінімум двох різних множин, одна з яких буде містити твірний елемент класу. Тому, одноелементних підмножин в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ не буде. Таким чином, буде справедливе функційне відображення в множині підмножин $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$:

$$\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}) \xrightarrow{\mathfrak{F}} \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}). \tag{2.4}$$

Співвідношення, яке задане формулою (2.4), означає що при виконанні функцій з множини $\mathfrak{F}$ здійснюється перехід до іншого елемента з множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Для систем класу $\mathfrak{S}$ це відображатиме зміну їх архітектури.

Введемо на множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ предикати, які будуть відображати результати входження та не входження елементів в підмножинах. І, відповідно, вони формуватимуть з елементів та компонентів відомості про певну архітектуру системи класу $\mathfrak{S}$. Задамо множину предикатів $\mathfrak{P}_{\mathfrak{M}} = \left\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_{\mathfrak{n}_{\mathfrak{P}_{\mathfrak{M}}}}\right\}$ ($\mathfrak{n}_{\mathfrak{P}_{\mathfrak{M}}}$ – кількість предикатів в множині $\mathfrak{P}_{\mathfrak{M}}$) таким чином, щоб кожен з предикатів буде задавати наявність чи відсутність елементів множини $\mathfrak{M}_{\mathfrak{S}}$ в елементах-підмножинах множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Якщо підмножини множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ будуть об'єднані і, при цьому, будуть мати різну кількість елементів, тобто буде об'єднано декілька підмножин з різними елементами і різною їх кількістю, тоді до кожної з них будуть застосовуватись різні предикати, а результат їх виконання буде сформовано множиною векторів. Підмножина буде містити елементи множини $\mathfrak{M}_{\mathfrak{S}}$ і їх кількість може бути меншою за загальну кількість елементів множини $\mathfrak{M}_{\mathfrak{S}}$, а вектор з компонентами буде мати кількість компонент, що дорівнює кількості елементів множини $\mathfrak{M}_{\mathfrak{S}}$. Якщо буде дві і більше підмножини з множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$, тоді результатом виконання предикатів на їх елементах буде множина векторів такої ж кількості. Таким чином, задамо відображення для елементів множини підмножини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$, тобто підмножини, у вектор так:

$$\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}) \xrightarrow{\mathfrak{P}_{\mathfrak{M}}} \mathfrak{W}(\mathfrak{M}_{\mathfrak{S}}), \tag{2.5}$$

де $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$ – множина векторів.

Елементи множини векторів $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$ позначимо $\mathfrak{w}_{\mathfrak{j}} = \left(\mathfrak{w}_{\mathfrak{j},1}, \mathfrak{w}_{\mathfrak{j},2}, \dots, \mathfrak{w}_{\mathfrak{j},\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}}\right)$, де $\mathfrak{w}_{\mathfrak{j}} \in \mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$, $\mathfrak{i} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$, $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$ – загальна кількість елементів і компонентів в архітектурі системи класу $\mathfrak{S}$, $\mathfrak{j} = 1,2,\dots,\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$, $\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$. Після виконання певної функції з множини функцій $\mathfrak{F}$ згідно з формулою (2.4) можливим варіантом може бути поєднання двох або більше підмножин чи зменшення кількості поєднаних підмножин. Тоді, в такому випадку кожну з підмножин множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ після виконання предикатів задамо вектором і

об’єднаємо їх в множину, яка буде множиною підмножин з елементів векторів $\mathfrak{P}\big(\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})\big)$.

Базовою множиною, в яку буде відображатись результат виконання предикату до одного елементу одноелементної підмножини, буде двохелементна множина $\{0, 1\}$. Тоді, для певної підмножини визначення значень координат векторів задамо так:

$$\mathfrak{w}_{\mathfrak{j},\mathfrak{i}} = \begin{cases} 0, \text{якщо елемент відсутній в підмножині } \mathfrak{P}_{\mathfrak{j}}(\mathfrak{M}_{\mathfrak{S}}), ; \\ 1, \text{якщо елемент наявний в підмножині } \mathfrak{P}_{\mathfrak{j}}(\mathfrak{M}_{\mathfrak{S}}); \end{cases} \tag{2.6}$$

$$\mathfrak{w}_{10,1} = 1,$$

де $\mathfrak{i} = 1,2, \dots, \mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$, $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$ – загальна кількість елементів і компонентів в архітектурі системи класу $\mathfrak{S}$, $\mathfrak{j} = 1,2, \dots, \mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$, $\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{P}_{\mathfrak{j}}(\mathfrak{M}_{\mathfrak{S}})$ – $\mathfrak{j}$ – тий елемент множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

Таким чином, архітектура мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА згідно принципу $\mathfrak{P}$ синтезу таких систем в корпоративних мережах в поточний момент часу визначатиметься елементом множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ так:

$$\mathfrak{P}_{\mathfrak{f}}(\mathfrak{M}_{\mathfrak{S}}) \in \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}), \tag{2.7}$$

де $\mathfrak{P}_{\mathfrak{f}}(\mathfrak{M}_{\mathfrak{S}})$ - $\mathfrak{f}$ – тий елемент множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{f} = 1,2, \dots, \mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$; $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

Згідно формул (2.2)-(2.7) задамо архітектуру мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень алгебраїчною системою типу $\tau = (\alpha, \beta)$ так:

$$\mathfrak{A}_{\mathfrak{S}} = \langle \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}), \mathfrak{F}, \mathfrak{P}_{\mathfrak{M}} \rangle, \tag{2.8}$$

де $\mathfrak{F}$ – множина функцій заданих на множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{P}_{\mathfrak{M}}$ – множина предикатів заданих на множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\alpha = \mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$, $\beta = 1$ – арності операцій, тому тип системи $\tau = \big(\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}, 1\big)$; $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

В системі класу $\mathfrak{S}$, яку задано формулою (2.8), виділено елементи та компоненти множиною їх властивостей і зв’язки між ними. Елементи відображають в архітектурі системи її цілісні частини, а компоненти відображають розподілені частини. Кожен з

таких елементів та компоненті при деталізації міститиме елементи, які будуть ієрархічно структурованими. Система, крім визначених функційних завдань, які формуватимуть процеси в ній, має свої внутрішні особливості сформовані елементами множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ та функціями і предикатами, які на них впливатимуть. Це формуватиме внутрішні процеси в ній і буде надавати їй власні властивості, які формуватимуться згідно поєднання властивостей, визначених для неї в поточний момент часу елементами множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

Якщо враховувати в архітектурі наявність лише елементів та компонентів з яких вона буде сформована в певні поточні моменти часу і, при цьому, не враховувати події, які призвели до зміни її архітектури, тобто які саме функції були виконані для зміни її архітектури, тоді модель такого класу систем $\mathfrak{S}$ задамо за формулою (2.9):

$$\mathfrak{A}_{\mathfrak{M},\mathfrak{S}} = \langle \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}), \mathfrak{P}_{\mathfrak{M}} \rangle; \qquad (2.9)$$
$$\forall\, \mathfrak{k}\colon \mathfrak{V}_{10,1} \subset \mathfrak{P}_{\mathfrak{k}}(\mathfrak{M}_{\mathfrak{S}}),$$

де $\mathfrak{P}_{\mathfrak{M}}$ – множина предикатів заданих на множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\alpha = \mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$, $\beta = 1$ – арності операцій, тому тип системи $\tau = \left(\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})},\ 1\right)$; $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$, $\mathfrak{P}_{\mathfrak{k}}(\mathfrak{M}_{\mathfrak{S}})$ – $\mathfrak{k}$ – тий елемент множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{k} = 1,2,\dots,\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$; $\mathfrak{V}_{10,1} = \{\mathfrak{v}_{10,1}\}$; множина $\mathfrak{V}_{10,1}$ – одноелементна множина.

Концептуальну модель архітектури системи задано не тільки виразом, в якому визначено величину $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, але й умовами та обмеженнями щодо її елементів в контексті поставленої проблеми. Подання концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ згідно формули (2.9) є базовим. Воно потребуватиме деталізації.

Модель задана формулою (2.9) є концептуальною моделлю такого класу систем $\mathfrak{S}$, оскільки в ній враховані властивості, що синтезовані в її архітектурі, та їх активізація в поточні моменти часу. Ці синтезовані властивості системи реалізовані елементами та компонентами системи. Так задана концептуальна модель є абстрактною моделлю, бо встановлює синтезовані властивості і зв'язки між ними в архітектурі мультикомп'ютерних систем класу $\mathfrak{S}$ їх формальним описом. Для повного задання всіх елементів концептуальної моделі в частині її внутрішнього наповнення потрібно розробити механізми функціонування елементів та компонентів в архітектурі системи, їх взаємодії, логіки формування та виконання процесів в них і

між ними. Також, доповненням до запропонованої концептуальної моделі мають бути результати дослідження щодо обмеження до її застосування чи її повноти поширення на розглядуваний клас систем $\mathfrak{S}$. Тобто, запропонована концептуальна модель повинна охоплювати всі архітектури систем класу $\mathfrak{S}$. Крім цього, в так синтезованій архітектурі згідно моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ не повинна формуватись нова якість системи, яка б відносила систему до іншого класу систем, відмінного від класу систем $\mathfrak{S}$. Така якість може формуватись на рівні розв'язання поставлених завдань для системи і реалізованих в ній методів, але не формування іншого класу систем.

Гіпотеза. Концептуальна модель мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$, є повною, тобто такою, що охоплює всі архітектури систем класу $\mathfrak{S}$.

Для доведення цієї гіпотези розглянемо окремо повноту з охоплення всіх таких систем та повноту в контексті неможливості появи нових типів архітектури згідно синтезу закладених в них декількох властивостей, які не відносяться до такого класу систем, а також їх поєднання. Для цього сформулюємо і доведемо окремі леми, як додаткові твердження, які використаємо при доведенні чи спростуванні висунутої гіпотези.

Лема 1. Концептуальна модель мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$ задає всі архітектури систем класу $\mathfrak{S}$ та не задає інших, відмінних від систем класу $\mathfrak{S}$.

Доведення. Для доведення задання концептуальною моделлю з формули (2.9) архітектури систем класу $\mathfrak{S}$ розглянемо формулу (2.1), якою характеризуються клас систем типу $\mathfrak{S}$ згідно принципу $\mathfrak{P}$. В формулі (2.1) клас систем типу $\mathfrak{S}$ подано через конкретні властивості. Їх імплементація в архітектурі системи буде формувати певну конкретну архітектуру. При різних комбінуваннях елементів різних підмножин $\mathfrak{V}_i$ ($i = n_{\mathfrak{V}},\ n_{\mathfrak{V}} -$ кількість характеристик) будуть отримуватись системи з різною архітектурою. Причому, це стосується як формування різних систем з різною архітектурою, так і певної системи, в якої архітектура буде змінюватись протягом певного часу її функціонування. Тоді, такі характеристики будуть окремими

елементами у відповідних підмножинах $\mathfrak{V}_i$ ($i = n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість характеристик) як початково їх задано в формулі (2.1). Також, ці елементи будуть об'єднуватись як окремі елементи окремих підмножин для формування різних систем з різною архітектурою, так і будуть поєднуватись елементи з однієї підмножини для формування одного типу систем зі змінюваною архітектурою. Ці так сформовані підмножини будуть відповідати елементам множини підмножин $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ з формули (2.1).

Припустимо, множина $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ охоплює меншу кількість елементів, ніж наявна кількість елементів в формулі (2.1). Можливі два варіанти. В першому варіанті, якщо в неї міститься елемент $\mathfrak{v}_{10,1}$, що визначає наявність контролера в системі і $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$, тоді оскільки він є твірним для класу систем типу $\mathfrak{S}$, то які б не були елементи в решті підмножин з формули (2.1), концептуальна модель системи охоплює саме такий клас систем, бо згідно розробленого принципу $\mathfrak{P}$ отримуємо систему з архітектурою, що відноситься саме до такого класу. Яка б кількість елементів підмножин не була б в підмножинах або доповнила їх в перспективі в моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.9)) такі підмножини включено разом з їх елементами та обмеженням, яке задано твірним для класу систем елементом. Тобто, в розробленій моделі передбачено доповнення нових характеристик в архітектуру систем такого класу. Якщо в другому варіанті в неї не міститься елемент $\mathfrak{v}_{10,1}$, що визначає наявність контролера в системі, тоді цей варіант не відноситься до розробленої концептуальної моделі системи згідно принципу $\mathfrak{P}$.

Припустимо, множина $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ охоплює більшу кількість елементів, ніж наявна кількість елементів в формулі (2.1). Тоді, так само як для попереднього випадку можливі два варіанти. Варіант відсутності твірного елементу класу аналогічний попередньому висновку. Для варіанту наявності твірного елементу можливе збільшення елементів підмножин, які визначають певні типові характеристики і, тоді доповнюємо відповідні підмножини новими елементами, а розроблена модель включає саме підмножини, тому вона враховує цей варіант. А у випадку, коли нові елементи не відноситимуться до жодного типу, тоді доповнюємо систему новою множиною характеристик, а модель утворена так, що може бути розширена новими підмножинами.

Таким чином, концептуальна модель мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$ задає всі архітектури систем класу $\mathfrak{S}$ та не задає інших, відмінних від систем класу $\mathfrak{S}$. Визначальною характеристикою такого класу систем є твірний елемент, можливість до масштабування, збільшення або зменшення кількості підмножин, що містять відповідні елементи та компоненти. Лему доведено.

Лема 2. Концептуальна модель мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$ не задає нових типів архітектури систем, які не відносяться до такого класу систем, через поєднання та комбінування елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

Доведення. Припустимо, що поєднання та комбінування елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$, які формуватимуть архітектуру систем класу $\mathfrak{S}$, може призвести до синтезу нової архітектури систем, які будуть відмінні від класу систем $\mathfrak{S}$. Тобто, в результаті поєднання та комбінування елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ формуються системи з архітектурою, які не відносяться до класу систем $\mathfrak{S}$. Тоді, можливі два випадки. В першому випадку концептуальна модель задає такі системи і вони не відносяться до класу систем $\mathfrak{S}$, а це неможливо, бо якщо вона задає їх, то вони містять твірний елемент і, відповідно, до них застосовується принцип $\mathfrak{P}$. В другому випадку концептуальна модель не задає такі системи і вони не відносяться до класу систем $\mathfrak{S}$ і до них, відповідно, не застосовується принцип $\mathfrak{P}$. Тобто, в результаті синтезу наявних характеристик, припустимо, що сформувались архітектури систем, які увійшли до іншого класу систем або вони синтезуються згідно іншого принципи синтезу, відмінного від принципу $\mathfrak{P}$. Тоді, результатом за припущенням будуть утворені системи з різною архітектурою, які синтезуються згідно двох різних принципів синтезу. Якщо це так, тоді згідно принципу $\mathfrak{P}$ множина всіх систем $\mathfrak{C}$ за заданою формулою $\mathfrak{C} \xrightarrow{\mathfrak{P}} \mathfrak{S}$ буде формувати клас систем із заданими принципом $\mathfrak{P}$ та другий клас систем, які не відповідають цьому принципу синтезу. А другий принцип формуватиме теж два класи систем в множині всіх систем $\mathfrak{C}$ і один з них буде згідно

припущення задаватись концептуальною моделлю $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.9)). Тоді, ці множини сформовані згідно двох принципів можуть мати і можуть не мати перетинів. Якщо вони не мають перетинів між собою, то твірний елемент $\mathfrak{V}_{10,1}$ буде належати двом різним класам в одній загальній множині, що неможливо. Якщо ж так утворені класи згідно двох принципів синтезу мають перетин, але при цьому не збіжні, то твірний елемент $\mathfrak{V}_{10,1}$ буде належати перетину, але це суперечить початковому припущенню про те, що концептуальна модель не задає такі системи, тому припущення про перетин таких класів є не правильним. Отже, лему доведено.

Згідно леми 2 отримуємо такий наслідок.

Наслідок 1. Поглинання властивості із зміною її функційного призначення, яку задає твірний елемент, в результаті синтезу систем через комбінування властивостей неможливе.

Дійсно, якщо в архітектурі систем синтезованих згідно принципу $\mathfrak{P}$ твірний елемент буде комбінуватись з рештою елементів простим або складним комбінування, то загальна властивість, яка ним визначається, буде зберігатись.

Згідно доведених лем проведемо доведення теореми для підтвердження висунутої гіпотези.

Теорема 1. Концептуальна модель мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$, є повною, тобто такою, що охоплює всі архітектури систем класу $\mathfrak{S}$.

Доведення. Розглянемо випадки з можливою архітектурою різних систем, які відповідають розробленій концептуальній моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.9)). Використаємо для доведення метод математичної індукції.

1. Нехай елемент множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ містить дві підмножини з множини $\mathfrak{M}_{\mathfrak{S}}$. Оскільки він відповідає вимогам принципу $\mathfrak{P}$ синтезу таких систем, тоді одна з цих підмножин буде $\mathfrak{V}_{10,1}$. Її можна вважати першою підмножиною, яка буде поєднана з другою підмножиною. Неважливо, яку властивість буде характеризувати друга одноелементна підмножина. Важливим є те, що в контексті першого кроку методу математичної індукції було виділено один елемент для початку застосування методу. Згідно леми 1 і леми 2 такий випадок відповідає тому, що концептуальна модель

мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$, що містять об'єднані дві підмножини, є повною. Дійсно, це підтверджується виділеним твірним елементом, який наявний в кожному поєднанні з різними одноелементними підмножинами. Якщо друга підмножина буде не одноелементною, тоді скільки б в ній не було елементів, то щодо такого випадку теж виконуються леми 1 і 2. Таким чином, для випадку з двома підмножинами, а фактично на одній підмножині з різною кількістю елементів та множиною з твірним елементом теорема виконується.

2. Припустимо, що теорема правильна для випадку, коли поєднані $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})} - 1$ ($\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$) елементів множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$. Оскільки, наявна відповідність вимогам принципу $\mathfrak{P}$ синтезу таких систем, тоді одна з цих підмножин буде $\mathfrak{V}_{10,1}$. Решта підмножин можуть бути одноелементними та багатоелементними і їх загальна кількість буде $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})} - 2$.

3. Нехай кількість об'єднаних підмножин буде складати $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ ($\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$). Тоді, виділимо підмножину з твірним елементом окремо і решту об'єднаних підмножин розподілимо на будь-які дві підмножини, одну з яких вибираємо довільним чином. Вона буде одноелементною або багатоелементною множиною. В результаті отримуємо три виділені підмножини. Для підмножини з твірним елементом класу та вибраною підмножиною застосовуємо перший крок методу математичної індукції і отримуємо синтез двох підмножин з твірним елементом. А на наступному кроці застосовуємо другий крок вже до $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})} - 1$ ($\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$) елементів множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$.

Згідно методу математичної індукції теорему доведено.

Таким чином, доведено, що концептуальна модель мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень в корпоративних мережах, яку задано формулою (2.9) для класу систем $\mathfrak{S}$, є повною і охоплює всі архітектури систем класу $\mathfrak{S}$. Згідно наслідку 1 з леми 2 поглинання

властивості, яку задає твірний елемент класу, із зміною її функційного призначення через комбінування властивостей неможливе.

Концептуальна модель мультикомп’ютерних систем, яку задано формулою (2.9) для класу систем $\mathfrak{S}$, є базовою і її елементи потребують деталізації з урахуванням середовища функціонування систем, архітектури корпоративних мережі та компонентів і елементів системи. Така деталізація дасть змогу уточнити щодо елементів множин в концептуальній моделі, доповнити її новими множинами та зв’язками між ними для досягнення належного адекватного відображення систем класу $\mathfrak{S}$.

2.2.2. Формальне подання елементів та компонентів в концептуальній моделі мультикомп’ютерних систем

Деталізуємо та доповнимо цю концептуальну модель систем класу $\mathfrak{S}$ з врахуванням середовища її функціонування, територіального розміщення мультикомп’ютерних систем, завдань внутрішнього рівня системи, завдань спеціалізованого функціоналу, особливостей внутрішньої архітектури системи, контролера прийнятих рішень.

Невід’ємною частиною проєктованих мультикомп’ютерних систем буде середовище корпоративної мережі. Врахування його наповнення буде впливати на результат виявлення та протидії ЗПЗ і КА. Те, з яких складових частин і як вони будуть взаємодіяти між собою, впливатиме на результат роботи всієї системи та формуватиме її компоненти і елементи. Тому, здійснимо формалізоване задання середовища корпоративної мережі.

Всі комп’ютерні станції знаходяться в корпоративній мережі і поєднані певним чином між собою, що дозволяє передавати повідомлення між ними. В певній частині комп’ютерних станцій або в усіх них можуть міститись компоненти системи класу $\mathfrak{S}$. Тобто, компонентів системи класу $\mathfrak{S}$ може бути менше, ніж кількість комп’ютерних станцій в корпоративній мережі. Тип зв’язку між ними та їх територіальне розміщення розглядатимемо та формалізуватимемо окремо від середовища корпоративної мережі. Таким чином, позначимо комп’ютерні станції, сервери,

мобільні комп'ютерні, пристрої під'єднані в загальну мережу, вершинами графа, а зв'язки між ними ребрами. Введемо множину вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},1}$ для позначення комп'ютерних станцій та множину ребер $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},1}$ для позначення зв'язків між ними і такі множини використаємо для задання середовища корпоративної мережі. Тоді, граф $\mathfrak{G}_1 = \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},1}\right)$ $(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},1} \subseteq \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},1} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},1})$ буде описувати стан корпоративної мережі на рівні наявності в ній вузлів та зв'язків між ними. Для розроблення доповнення концептуальної моделі системи в частині середовища її функціонування таке представлення є недостатнім, бо не відображає в корпоративній мережі сегменти та одиничні вузли. Введемо для такого випадку множину вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$. Її елемент позначатимуть комп'ютерні станції, які експлуатуються користувачами. Множину вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ введемо так, що її елементи позначатимуть сервери. Множину вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ введемо так, що її елементи позначатимуть маршрутизатори (комутаторів). Поділ множини вершин з виділенням окремої множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$ для комп'ютерних станцій та окремої множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ для серверів, хоча вони матимуть спільні зв'язки з елементами множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, є необхідним для врахування функційного призначення такого вузла в корпоративній мережі і, відповідно, відображення такої особливості в архітектурі системи класу $\mathfrak{S}$. А також введемо множину ребер $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ для позначення зв'язків між ними і такі множини використаємо для задання середовища корпоративної мережі на рівні функційного призначення її вузлів. Тоді, для такого задання визначимо граф:

$$\mathfrak{G}_2 = (\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}), \tag{2.10}$$

де $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2} \subseteq \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right)$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2} = \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2}$ – множина всіх вершин графа $\mathfrak{G}_2$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ – множина ребер графа.

На відміну від задання графом $\mathfrak{G}_1$, задання компонентів корпоративної мережі графом $\mathfrak{G}_2$ враховує функційне призначення вузлів та розподіляє сегменти мережі за рахунок введення множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ і $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Множина $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},1}$ не обов'язково містить всі елементи множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ і $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Аналогічно множини ребер $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},1}$ і $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ є різними,

оскільки, наприклад, в множині ребер $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ враховано ті з них, які є інцидентними елементам множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$.

Множина $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ може бути порожньою, тобто $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} = \emptyset$. Тоді, системи класу $\mathfrak{S}$ будуть встановлені в межах сегментів, які визначатимуться елементами множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$. В цьому випадку $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2} \subseteq \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}\right)$.

Аналогічно до попереднього випадку, множина $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$ може бути порожньою, тобто $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} = \emptyset$. Тоді, системи класу $\mathfrak{S}$ будуть встановлені в межах сегментів, які визначатимуться елементами множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$. В цьому випадку $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2} \subseteq \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}\right)$.

Множина $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ може бути одноелементною. Тоді, системи класу $\mathfrak{S}$ будуть встановлені в межах сегментів, які визначатимуться елементами підмножин множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$ та обов’язково елементом множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$.

Потужності множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$ та $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ можуть бути однаковими і, при цьому, в множині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ може бути по одному елементу, тобто по одному ребру, для кожного елементу з множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, який відповідному лише одному елементу з множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}$. Тоді, така інтерпретація відображатиме під’єднання кожної комп’ютерної станції до одного окремо виділеного для неї маршрутизатора. Тоді, системи класу $\mathfrak{S}$ будуть встановлені в окремих комп’ютерних станціях в межах одноелементних сегментів, які визначатимуться елементами підмножини множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Решта елементів, що не увійшли в розглядувану попередню підмножину, будуть належати підмножині множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, яка відображатиме зв’язок з елементами множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$.

Такі граничні випадки та не виокремлені решта граничних випадків для трьох множин показують можливість перебування систем класу $\mathfrak{S}$ в середовищі заданому графом з формули (2.10). Таким чином, середовище для функціонування систем класу $\mathfrak{S}$ задане за формулою (2.10) враховує внутрішні особливості компонентів корпоративної мережі та може масштабуватись.

Елементи множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ є точками з'єднання в графі $\mathfrak{G}_2$ і вилучення їх з графа призведе до його розпаду на частини. В контексті корпоративних мереж, одна з частин буде залишатись функціонувати. Тому, система класу $\mathfrak{S}$ теж втратить частину своїх компонентів. В зв'язку з цим, важливим в системах класу $\mathfrak{S}$ є збереження повноцінного функціонування обох частин в корпоративній мережі при наявності точок з'єднання в графі $\mathfrak{G}_2$ та їх подальшу синхронізацію при подальшому додаванні вершини з множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Тобто, продовження функціонування обох частин окремо, потім їх об'єднання і обробку такої події в центрі системи. В одній частині графа в результаті вилучення точки з'єднання вершини стануть ізольованими. Відповідно компоненти системи класу $\mathfrak{S}$ теж стануть відокремленим і вони можуть продовжити своє функціонування з врахуванням опрацювання нової конфігурації корпоративної мережі. Після поновлення точки з'єднання центр системи повинен синхронізувати події в цих компонентах та в решті компонент системи. В такому варіанті з вилученням точки з'єднання центр системи може бути або в зв'язній частині графа, або в ізольованих вершинах, або в обох частинах, якщо він розподілявся в компонентах. Найменш проблемний варіант – це коли центр системи перебував на момент вилучення точки з'єднання в зв'язній частині графа, тоді архітектура системи класу $\mathfrak{S}$ буде перебудована і система продовжить роботу з тією частиною, що залишилась. Якщо центр системи перебуватиме в ізольованих вершинах, тобто в незв'язній частині графа, тоді в зв'язній частині повинен бути сформований новий центр системи, який після повернення вилученої точки з'єднання синхронізує результати своєї роботи за час функціонування з центром в ізольованих вершинах. Третій варіант, коли центр системи на момент вилучення точки з'єднання перебуватиме в обох частинах, якщо він розподілявся в компонентах, також допускатиме виконання дій аналогічно до другого варіанту. Але ці варіанти не повністю враховують особливості моделі архітектури (формула (2.9)) систем класу $\mathfrak{S}$, в якій наявний твірний елемент $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$.

Аналіз можливих реакцій контролера в різних випадках, включаючи і випадки із вилученням точки з'єднання, будемо розглядати в цілісному контексті щодо моделі архітектури контролера та його місця в моделі архітектури всієї системи через відповідно множини подій та реакцій систем класу $\mathfrak{S}$. А в розглядуваному випадку

контролер співвідноситимемо до середовища його можливого функціонування. Контролер може бути розміщено так само, як і центр системи. Тоді, він повинен відповідно реагувати на подію із вилученням точки з'єднання. Всі три випадки для центру системи із вилученням точки з'єднання аналогічні і для контролера. Але, якщо контролер знаходиться у вузлах системи класу $\mathfrak{S}$, які відмінні від вузлів, в яких знаходиться центр системи, тоді додаються ще варіанти щодо середовища функціонування та вилучення точки з'єднання.

Якщо центр системи після вилучення точки з'єднання залишається в зв'язній частині графа, а контролер в незв'язній частині графа, тобто в ізольованих вершинах. Тоді, системи класу $\mathfrak{S}$ повинні зупинити своє функціонування в корпоративній мережі та за потреби заблокувати решту процесів. Але в такому випадку буде знижена їх стійкість, що в контексті поставлених завдань спеціалізованого функціоналу є недопустимим. Тому, компоненти системи, які будуть перебувати в ізольованих вершинах, продовжать своє функціонування з обмеженими можливостями і, при цьому, вони враховуватимуть свій поточний стан з обмеженнями. А оскільки центру системи в цих компонентах немає, тоді контролер, який може бути в одній або більше компонент, які ізольовані, буде неактивним, бо відсутній центр системи. А центр системи в такому варіанті буде в зв'язній частині графа і для того, щоб система функціонувала в зменшеній формі, потрібно щоб функціонал контролера був в цій же частині в неактивному стані, тобто повинен бути резервний функціонал контролера в одній з компонент системи поза сегменту, в якому після вилучення точки з'єднання, залишились ізольовані вершини. Дійсно, при наявності контролера в активному стані в компонентах незв'язної частини графу недоцільно в цій же частині розміщувати резервний функціонал контролера. Якщо декілька точок з'єднання буде вилучено з графа, тоді розміщення резервного функціоналу контролера в неактивному стані в одному екземплярі недостатньо. Таким чином, крім контролера в активному стані, потрібно в кожному сегменті корпоративної мережі, тобто в кожній з підмножин, що визначають сегмент корпоративної мережі, повинен міститись елемент, що відповідає функціоналу контролера. В такому випадку тільки один з таких функціоналів буде активним, а решта неактивними. Архітектура контролера може визначати варіанти його розміщення в компонентах. Зокрема, він може міститись винятково в одній

компоненті, а може бути розподілений між декількома компонентами, але ці його розподілені елементи між різними компонентами повинні бути в межах одного сегменту, який визначається точкою з'єднання.

Якщо центр системи після вилучення точки з'єднання залишається в незв'язній частині графа і контролер теж в незв'язній частині графа, тобто вони будуть в ізольованих вершинах, тоді системи класу $\mathfrak{S}$ повинні зупинити своє функціонування в корпоративній мережі та заблокувати решту процесів. Такий випадок суттєво впливає на стійкість системи в цілому. Компоненти в зв'язній частині графа могли б продовжувати виконання поставлених для них завдань, але саме така особливість в архітектурі системи унеможливлює повноцінне функціонування решти системи і збереження в ній синтезованих властивостей в частині центру системи та контролера. Тому, функціонали центру системи та контролера повинні бути в усіх сегментах, що задані точками з'єднання у графі, в неактивному стані і тільки один з кожного з них у активному стані. Центр системи та контролер згідно їх конкретних архітектурних особливостей та архітектури системи в цілому можуть бути розподілені між декількома компонентами, а не бути винятково в одній компоненті. В такому випадку всі ці їх елементи повинні бути в компонентах певного цілісного сегменту корпоративної мережі, які визначатимуться елементом множини вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Дійсно, центр системи та контролер можуть бути розміщені в декількох компонентах, а може бути випадок при якому центр системи буде в декількох компонентах, а контролер – в одній компоненті і навпаки. А, також, центр системи та контролер можуть бути в різних компонентах окремо або в частині компонент чи всіх компонентах розподіленими. Центр системи та контролер можуть розподілятись в компонентах з однаковим функціоналом кожен або розподіляти один функціонал елементами між компонентами. Які б не були варіанти розміщення центру системи та контролера, вони повинні бути в одному сегменті корпоративної мережі, причому один з них може бути в активному стані, а інший – в неактивному стані.

Якщо центр системи після вилучення точки з'єднання залишається в незв'язній частині графа, тобто в ізольованих вершинах, а контролер в зв'язній частині графа. Тоді, системи класу $\mathfrak{S}$ повинні зупинити своє функціонування в корпоративній мережі та за потреби заблокувати решту процесів. Це суттєво впливатиме на стійкість

системи та можливість продовжувати своє функціонування, враховуючи при цьому специфіку поставлених завдань для систем класу $\mathfrak{S}$. Варіанти з розподіленням центру системи та контролера між компонентами аналогічні до розглянутих випадків при розміщенні контролера в незв'язній частині графа, а центру системи в зв'язній частині графа. Таким чином, центр системи та контролер повинні бути в кожному сегменті корпоративної мережі в активному/неактивному станах для забезпечення належної стійкості та рівноваги системи.

Якщо центр системи та контролер після вилучення точки з'єднання залишаться в зв'язній частині графа, то система продовжить функціонування після відповідного масштабування в зменшеній архітектурі. Після поновлення точки з'єднання центр системи опрацює інформацію з компонент, що були в ізольованих вершинах. В зв'язку з можливим функціонуванням компонент в ізольованих вершинах при вилученні точки з'єднання необхідно в архітектуру таких компонент синтезувати функціонал, що забезпечуватиме їх функціонування в таких умовах із зниженням рівня функційності від початково заданого.

Якщо центр системи та контролер після вилучення точки з'єднання залишаться в зв'язній та незв'язній частинах графа. Такий варіант можливий, коли вони розподілені між різними компонентами і для прийняття результуючого рішення опрацьовуються дані зі всіх компонент, в яких знаходяться центр системи чи контролер в активному стані. Функціонування системи можливе в в зв'язній частині графа та в ізольованих вершинах в незв'язній частинах графа, в яких наявні компоненти з контролером та центром системи. Таким чином, для такого випадку залишиться певна менша частина ізольованих вершин, в яких функціонування систем класу $\mathfrak{S}$ буде зупинено. В подальшому при поновленні в графі точки з'єднання результати роботи в різних частинах графа будуть синхронізовані. Якщо ж елементи контролера в різних частинах графа і центра системи в одній частині та навпаки, тоді частина графа, в якій відсутній контролер або центр системи, буде співвідноситись з розглянутими випадками.

Аналогічні варіанти випадів відносяться до наявного будь-якого моста в графі.

Розглянуті варіанти із точкою чи точками з'єднання в графі, а також мостом чи мостами, доводять наслідок щодо особливостей в моделі архітектури систем класу $\mathfrak{S}$.

Наслідок 2. В моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула(2.9)) систем класу $\mathfrak{S}$ кожна з підмножин, що задають сегменти корпоративної мережі, тобто частини графа, які пов'язані з певними точками з'єднання чи мостами, як елементами з множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, повинні містити не менше одного елементу з властивістю твірного елементу та не менше одного елементу з властивістю центру системи.

В формулі (2.9) не представлено підмножин, які задають сегменти корпоративної мережі, тобто частини графа, що пов'язані з певними точками з'єднання чи мостами, як елементами з множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, Тому, потрібно ввести їх формалізоване представлення, обмеження, що задаються ними, зв'язок з елементами множин з формули (2.10) та доповнити результатом формулу (2.9), як додаткове обмеження для моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$. Для цього потрібно описати системи класу $\mathfrak{S}$ в співвіднесені її та її компонентів у вузлах корпоративної мережі.

Задамо типові компоненти систем класу $\mathfrak{S}$ множиною $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$ так:

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1} = \left\{ \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}} \right\}, \tag{2.11}$$

де $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathfrak{I}}$ – $\mathfrak{I}$-елемент множини типових компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$, тобто кількість типових компонент.

Типові компоненти визначатимуться своїми функційними можливостями через синтез в них властивостей, які визначені в множині $\mathfrak{M}_{\mathfrak{S}}$. Всі типові компоненти різнитимуться між собою набором елементів. Наприклад, якщо всі елементи частини компонент будуть однакові і контролер розподілений між частиною компонент з однаковим функціоналом, то це буде одна типова компонента. Якщо ж всі елементи частини компонент будуть однакові і контролер розподілений між частиною компонент з різними елементами його функціоналу, то це будуть різні типові компоненти. Базових типових компонент буде чотири. Зокрема, до них віднесемо такі: компоненти, які не містять функціоналів центру системи, контролера та спеціалізованих для виявлення та протидії ЗПЗ та КА, а містять елементи для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи; компоненти, в яких містяться елементи

для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами, для забезпечення комунікації з центром системи та виконання функцій контролера; компоненти, в яких містяться елементи для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами, для забезпечення комунікації з центром системи та виконання спеціалізованого функціоналу; компоненти, в яких містяться елементи для забезпечення перебування у вузлі корпоративної мережі, для доповнення новими елементами, для забезпечення виконання функцій заданих певними елементами, для забезпечення комунікації з контролером та виконання функцій центру системи. Перший тип компонент фактично буде нуль-компонентами, які необхідні для оперативного заповнення в них необхідних елементів в процесі функціонування систем класу $\mathfrak{S}$ за потреб реагування на зовнішні та внутрішні події в системі та корпоративній мережі. Також, такі компоненти потрібні для підтримки зв’язку між компонентами систем класу $\mathfrak{S}$ у вузлах корпоративної мережі. Якщо кількість потрібних компонент суттєво менше за кількість вузлів корпоративної мережі, тоді частина вузлів не міститиме компонентів систем класу $\mathfrak{S}$ і, як наслідок, не буде здійснюватись пасивний моніторинг стану вузла, навіть через активність нуль-компоненти за рахунок зв’язку з центром системи. Тому, для покриття всіх вузлів корпоративної мережі, якщо потрібна забезпеченість тільки частини з них повноцінними функціоналами решти трьох типів, потрібно використовувати нуль-компоненти. Невелика кількість елементів таких нуль-компонентів не впливатиме на завантаженість відповідних комп’ютерних станцій. Реалізація можливості доповнення таких нуль-компонент новими елементами дає змогу бути системам класу $\mathfrak{S}$ гнучкими, що при вирішенні призначеного типу завдань з їх специфікою є важливим.

Решта три базових типи компонент можуть бути окремими компонентами у вузлах корпоративної мережі, а можуть комбінуватись через елементи з визначеними функційними можливостями. Множина типових компонентів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$ систем класу $\mathfrak{S}$ буде містити всі типи компонентів з можливими варіантами поєднання різних елементів в них.

Приймемо за мінімальну одиницю в компонентах систем класу $\mathfrak{S}$ елемент компонента, який виконує певну завершену дію, тобто певну функцію. В розглянутій нуль-компоненті такі елементи призначені для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи. Також, такими елементами будуть ті, які відповідатимуть за функціонування центру системи, контролера, спеціалізованого функціоналу. Але вони можуть бути поділені і на менші елементи, тобто можуть складатись з певних елементів, які можна розміщувати в одній компоненті в одному вузлі корпоративної мережі або в декількох. Особливо це актуально для спеціалізованого функціоналу, який повинен мати можливість виконувати багато різних завдань різного спрямування. І, тому він повинен ділитись на менші завершені елементи. Взагалі, центр системи, контролер та спеціалізований функціонал повинні бути задані певними своїми множинами елементів, де елементи є завершеними і можуть бути розміщеними в різних вузлах корпоративної мережі та при цьому виконувати поставлені завданні, як ніби вони знаходяться в одному вузлі цілісно. Така вимога необхідна для синтезу компонентів систем класу $\mathfrak{S}$ через специфіку завдань для неї. Центр системи, контролер та спеціалізованого функціоналу можуть бути задані окремими цілісними елементами. Така їх організація теж є допустимою. Може бути варіант, коли з них частина задані єдиними цілісними елементами, а частина, наприклад спеціалізований функціонал, різними елементами. Взагалі доповнення спеціалізованого функціоналу в процесі тривалого функціонування системи в корпоративній мережі є необхідним. Тому, його необхідно задавати саме сукупністю елементів. Крім того, в процесі виконання завдань спеціалізованим функціоналом можуть виникати внутрішні зміни в ньому, які формуватимуть його нову якість, зокрема може бути здійснене, наприклад самонавчання. Тоді, такі оновлені зміни повинні отримати всі решта типових компонентів системи з такими ж елементами спеціалізованого функціоналу.

Таким чином, в системах класу $\mathfrak{S}$ для чотирьох базових компонент та похідних від них компонент елементи, з яких вони складаються, можна поділити на чотири підмножини. Елементи першої підмножини, в яку входять елементи, що необхідні для

забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи, сукупно можуть формувати окремі компоненти і обов'язково сукупно входитимуть до всіх решти компонент, які матимуть додатково ще елементи. Задамо елементи базових типів компонент підмножинами так:

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}\right\};$$

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}}\right\};$$

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}}\right\}; \qquad (2.12)$$

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}}\right\},$$

де $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ – підмножина елементів для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{l}_1}$ – $\mathfrak{l}_1$-елемент першої підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{l}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, тобто кількість базових типових елементів для різних компонент; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$ – підмножина елементів для забезпечення функціонування центру системи; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{l}_2}$ – $\mathfrak{l}_2$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{l}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$ – підмножина елементів для забезпечення функціонування контролера; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{l}_3}$ – $\mathfrak{l}_3$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathfrak{l}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$ – підмножина елементів для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення

комунікації з центром системи; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{l}_4}$ – $\mathfrak{l}_4$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$; $\mathfrak{l}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$.

Множину $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ всіх елементів, з яких формуватимуться компоненти системи, визначимо як об'єднання підмножин так:

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}} = \bigcup_{\mathfrak{l}=1}^{4} \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{l}}; \tag{2.13}$$

$$\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}} = \sum_{\mathfrak{l}=1}^{4} \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{l}}},$$

де $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}}$ – кількість елементів в множині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$.

Введемо множину функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \left\{\mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}\right\}$ ($\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість функцій в множині $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$), в якій функції будуть формувати компоненти елементами, тобто будуть задавати таке відображення:

$$\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}: \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}} \to \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}. \tag{2.14}$$

Деталізуємо формулу (2.14). Функції в множині $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ задамо як $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}}$ – аргументні, тобто такі, що міститимуть $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}}$ – аргументів з елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$. Кількість функцій $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ в множині $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ при такому їх задані буде дорівнювати кількості елементів в множині компонентів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$ з формули (2.11), тобто $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$. Таким чином, для кожної компоненти з множини компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$ буде однозначно визначена функція, яка при виконанні формуватиме наповнення компоненти елементами. Для двох різних за наповненням компонент буде дві різні функції з множини функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$. Це важливо при перебудові архітектури систем класу $\mathfrak{S}$ в процесі їх функціонування в корпоративних мережах. В результаті такого задання функцій множиною $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ на наборі компонент у вузлах корпоративної мережі буде однозначно визначено по кожній компоненті функцію, якою було сформовано компоненту, і підмножина цих функцій задаватиме поточний стан систем класу $\mathfrak{S}$. Центр системи буде визначати в поточний момент часу функціонування системи щодо наповнення певної компоненти елементами і запускатиме на виконання відповідну функцію. Елементи систем класу $\mathfrak{S}$, що

формують множину елементів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ можуть зберігатись в різних компонентах різних вузлів корпоративної мережі або в одному місці. Для забезпечення стійкості системи при перебудові її архітектури і враховуючи специфіку завдань для системи елементи, з яких формуватимуться компоненти систем класу $\mathfrak{S}$ можуть бути розміщені в тих же компонентах, в яких вони вже є в активному стані і в одній з компонент системи, яку сформовано з усіх можливих елементів. Такі елементи можуть доповнювати компоненти, а можуть і вилучатись з компонент. Рішення щодо вилучення та доповнення елементів приймає центр системи і погоджує контролер. Забезпечення стійкості системи та оперативності при формуванні чи зміні наповнення елементами в компонентах потребуватиме використання резервування елементів у визначених компонентах системи. Функцію з множини функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ задамо згідно формули (2.14) для її деталізації так:

$$(\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}},$$
$$\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}})$$
$$\xrightarrow{\mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathrm{I}}} \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathrm{I}}, \tag{2.15}$$

де $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathrm{I}}$ – I-елемент множини типових компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$; $\mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$, тобто кількість типових компонент, а також і кількість функцій в множині функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість функцій в множині $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathrm{I}}$ – I-елемент множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathrm{I}_1}$ – I_1-елемент першої множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathrm{I}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathrm{I}_2}$ – I_2-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathrm{I}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathrm{I}_3}$ – I_3-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathrm{I}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathrm{I}_4}$ – I_4-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$; $\mathrm{I}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$.

Таким чином, так задані функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ за формулами (2.14) та (2.15) будуть використовуватись при перебудові архітектури системи або при її формуванні. Якщо певна компонента систем класу $\mathfrak{S}$ буде містити в активному стані певну кількість елементів і центр системи прийме рішення про доповнення функціоналу компоненти елементами, які в поточний момент часу наявні або не наявні в компоненті, то відповідна функція перевірить наявність частини елементів і доповнить її новими, відсутніми в ній елементами. Функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ є багатоаргументними і їх аргументи поділяються в загальному випадку на чотири групи: аргументи, що задають наявні в компоненті елементи; аргументи, що задають відсутні в компоненті елементи, але ці елементи повинні доповнити компоненту; аргументи, що задають наявні в компоненті елементи, але після виконання функції вони мають бути вилучені з компоненти або переведені до пасивного стану; аргументи, що задають відсутні в компоненті елементи і вони після виконання функції не будуть додані в компоненту. Така організація формування компонентів систем класу $\mathfrak{S}$ через виконання відповідних функцій з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ дає змогу організувати формування та перебудову системи за функційним принципом. Перелік функцій з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ задається таким чином, щоб він враховував, також, можливість поєднання елементів між собою в компоненті для виконання завдань. Тому, функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ не охоплюють всеможливі комбінації зі всієї множини елементів, з яких можуть формуватись компоненти систем класу $\mathfrak{S}$. Таке формування функцій зменшує їх кількість в множині $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ порівняно зі всеможливими комбінаціями з варіантів поєднання елементів. Доповнення нових елементів під час експлуатації системи може бути здійснено за рахунок доповнення їх функціоналу в наявні елементи або через резервування нуль-елементів для подальшого їх наповнення певним функціоналом при початковому формуванні системи. В такому випадку з використанням нуль-елементів в множині функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ будуть задаватись функції для цих універсальних нуль-елементів, а для решти функцій ці універсальні нуль-елементи будуть враховуватись у всеможливих поєднаннях з наявними елементами, тобто нуль-елементи розглядатимуться такими,

що можуть поєднуватись з будь-якими наявними з визначеним функціоналом елементами та між собою.

До кожної з компонент системи можуть бути застосовні будь-які з функцій множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$. Після їх виконання буде сформована компонента з елементами і ця компонента буде одним з елементів множини компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$.

Для кожної функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ задамо обернені функції і, відповідно, множину для обернених функцій $\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ так:

$$\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}: \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1} \to \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}. \tag{2.16}$$

Тоді, множина $\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \left\{\mathfrak{f}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{f}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{f}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}\right\}$, кожна функція цієї множини є оберненою до відповідної функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, кількість таких функцій дорівнює кількості функцій з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, тобто $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} = \mathfrak{n}_{\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$. Використовувати ці функцій буде безпосередньо кожна компонента. Вони необхідні для здійснення самоконтролю щодо цілісності компоненти і її відповідності заданому центром системи формуванню з елементів. В процесі функціонування компоненти деякі її елементи, враховуючи специфіку поставлених завдань, можуть втрачати функційність або деградувати. Компонента не володіє інформацією про те, якою функцією вона сформована. Тому, вона запускає почергово функції з множини $\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, тобто обернені функції і звіряє результат їх виконання з наявним переліком елементів. При визначенні відповідної функції, результат надсилається в центр системи для підтвердження цілісності компоненти.

Функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ будуть використовуватись для формування та перебудови системи через наповнення її компонент елементами. А функції з множини $\mathfrak{F}^{\mathfrak{S},-1}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ будуть надавати центру системи інформацію щодо наповнення компонент елементами з метою проведення самоконтролю.

В процесі функціонування систем класу $\mathfrak{S}$ потрібно забезпечити активний та неактивний стани певних елементів функціоналу, тобто забезпечити активність чи пасивність певних елементів компонент. Для систем, які вирішують складні спеціалізовані завдання, враховуючи їх специфіку і принцип синтезу, може бути

потрібним здійснити, наприклад, переміщення центру системи чи контролера. Тоді, фізично елементи, які відповідають за такі функції, можуть залишатись в тих же компонентах, але центром системи можуть бути переведені в пасивний стан. І, навпаки, для появи центру системи, чи контролера, чи іншого функційного елементу компоненти центру системи достатньо перевести елемент в компоненті з пасивного стану в активний, якщо такий елемент є наявним в компоненті. Якщо ж його немає в компоненті, тоді для його доповнення в компоненту потрібно виконати одну з функцій з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$. Переміщення, наприклад, центру системи чи контролера через переведення елементів, що їх забезпечують в одних компонентах до пасивного стану, а в інших до активного стану буде тільки частиною кроку. Також, потрібно буде доповнювати компоненту, в якій буде елемент переведений до активного стану, актуальною інформацією про події в системі. Для решти елементів одного переведення до активного стану може бути достатнім.

Для виконання переведення елемента компоненти до активного чи пасивного станів введемо множину функцій $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2} = \{\mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \mathfrak{f}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,2}\}$ на множині елементів $\bigcup_{\mathfrak{l}=2}^{4} \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{l}}$ з формул (2.12) та (2.13). До елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ ці функції не застосовуються, бо ці елементи відповідають за безпосереднє функціонування компоненти у вузлі корпоративної мережі. Функції з множини $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$ виконують зворотні дії і вони не є оберненими. Рішення про їх виконання приймає центр системи. Функції є двох аргументними. Результатом виконання функції є блокування елементу або переведення його до активного стану. Аргументами функцій є номер компоненти за списком в системі та номер елементу за загальним списком функційних елементів для наповнення компонент. Таким чином, завдяки використанню цих функцій центр системи може формувати компоненти з однаковими елементами, але ці компоненти можуть відрізнятись набором своїх функцій через переведення частини їх елементів до пасивного стану. Така потреба є в зв’язку з специфікою завдань для системи і компонент зокрема. В процесі дослідження системою складних процесів, які пов’язані з виявленням ЗПЗ та КА, потрібно їй формувати, наприклад, декілька хибних об’єктів атак різних за наповненням. Тому, виділення окремих функцій для виконання таких завдань є доцільним.

Введемо множину векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}} = \left\{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},2}, \dots, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}}\right\}$ ($\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$), в елементах якої буде фіксуватись формування систем класу $\mathfrak{S}$ у співвіднесені до середовища їх функціонування та відображення кожної компоненти в ньому окремим вектор $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I}}$, де $\mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$. Такий вектор міститиме в своїх координатах інформацію про компоненту такого змісту: номер компоненти за списком системи; тип компоненти з переліку компонент множини компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ визначеній за формулою (2.13); номер вузла в корпоративній мережі; тип вузла в корпоративній мережі. Таким чином, вектори будуть містити чотири координати і їх задамо так:

$$\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I}} = \left(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},2}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},3}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},4}\right), \tag{2.17}$$

де $\mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},1}$ – значення номеру компоненти за списком системи; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},2}$ - тип компоненти з переліку компонент множини компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ визначеній за формулою (2.13), тобто компонента визнається винятково одним з елементів множини компонент; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},3}$ - номер вузла в корпоративній мережі, який задано стандартною системою найменувань вузлів; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathrm{I},4}$ - тип вузла в корпоративній мережі, який визначається співвіднесенням до однієї з трьох підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$.

Сукупність всіх векторів з множини векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ з визначеними в них конкретизованими значеннями координат формують відомості про систему в частині середовища її функціонування та наповнюваності компонент у вузлах корпоративної мережі.

Кількість елементів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ може змінюватись. Доповнення чи вилучення компонентів системи не впиватиме на кількість елементів. При задані множини векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ будуть враховані потенційні вузли, в які можуть бути розміщені компоненти системи. Таким чином, елементами множини векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ будуть ті, які відображатимуть наявне розміщення компонентів у вузлах корпоративної мережі та потенційно можливе розміщення. Тому, вилучення або

доповнення компонент з системи через їх вилучення або доповнення в конкретних вузлах не впливатиме на кількість елементів множини векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$. Враховуючи специфіку завдань для систем класу $\mathfrak{S}$, центр таких систем повинен володіти інформацією про вузли корпоративної мережі, в яких відсутні компоненти системи. Такі вузли можуть бути, згідно покладених на них функцій, без компонент системи в корпоративній мережі. Але в подальшому вони можуть отримати такі компоненти. Задамо їх у відповідних координатах вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1} = 0$, $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},2} = 0$, $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},4} = 0$ і номер вузла в корпоративній мережі, який задано стандартною системою найменувань вузлів, $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},3}$. Тоді, система буде володіти відомостями про своє оточення в цій же корпоративній мережі.

Для оперативного встановлення та отримання відомостей в системі про стан наявних активних і пасивних та відсутніх елементів в компонентах введемо множину предикатів $\mathfrak{P}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}\}$ таким чином, щоб для кожної компоненти формувались за потреби два вектори, які задамо такою множиною векторів $\mathfrak{V}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}\}$.

Кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$ дорівнює кількості елементів множини елементів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ з якої формуються компоненти системи збільшеній на одиницю, тобто $\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}} + 1$. Координати вектору, починаючи з другої координати і до останньої координати, прийматимуть значення з множини $\{0, 1\}$, де значення «0» вказуватиме на відсутність елементу в компоненті, а значення «1» - наявність елементу в компоненті. Першою координатою вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$ буде номер компоненти з системи, який задано першою координатою вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I}}$, який визначено за формулою (2.17). Ця перша координата $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}$ ($\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$) відображає значення номеру компоненти за списком системи. Тоді, відображення задамо так:

$$(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}) \xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}; \quad (2.18)$$
$$\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}},$$

де $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$.

Деталізуємо в формулі (2.18) множину і вектор так:

$$(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}},$$

$$\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}})$$

$$\xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} (\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,2}, \dots, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}}}); \mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}};$$

$$\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,0} = \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1};$$

$$\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} + \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}} + \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}} + \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}, \tag{2.19}$$

де $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ згідно формули (2.17); $\mathrm{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{r}_1}$ – координата вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$; $\mathfrak{r}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}}$; $(\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} + 1)$ – кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathrm{I}_1}$ – I_1-елемент першої множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathrm{I}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathrm{I}_2}$ – I_2-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathrm{I}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathrm{I}_3}$ – I_3-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathrm{I}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathrm{I}_4}$ – I_4-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$; $\mathrm{I}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,0}$ – перший елемент вектору.

Вектор, який визначено за формулами (2.18) і (2.19), потрібен для встановлення наявних елементів в компонентах системи в поточний момент часу. Оскільки компоненти системи будуть ставати активними переважно тільки після увімкнення комп’ютерних станцій, то центр системи повинен володіти інформацією про те, з яких елементів сформовані компоненти системи. А також, така інформація потрібна для поточного виконання завдань, їх перерозподілу між компонентами. В зв’язку з потребою мати відомості про активний та пасивний стани елементів в компонентах, наявність яких визначена у векторі $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$, введемо другий вектор $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$. Його

координатами будуть результати виконання предикату $\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ застосовні до кожного наявного елементу в компоненті.

Аналогічно до першого вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$ з множини векторів $\mathfrak{V}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ визначимо другий вектор $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$. Кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ дорівнює кількості елементів множини елементів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ з якої формуються компоненти системи збільшеній на одиницю, тобто $\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}} + 1$. Приймемо, що координати вектору, починаючи з другої координати і до останньої координати, прийматимуть значення з множини $\{0, 1, 2\}$, де значення «0» вказуватиме на відсутність елементу в компоненті, значення «1» - наявність елементу в компоненті та його перебування в ньому в пасивному стані і значення «2» - наявність елементу в компоненті та його перебування в ньому в активному стані. Першою координатою вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ буде номер компоненти з системи, який задано першою координатою вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I}}$, який визначено за формулою (2.17). Ця перша координата $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}$ ($\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$) відображає значення номеру компоненти за списком системи. Тоді, відображення задамо з врахуванням предикату, який буде застосовний до наявних елементів в компонентах, а відомості про відсутні елементи будуть відображені відповідними значенням як у векторі $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$, так :

$$(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}) \xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}; \quad (2.20)$$
$$\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}},$$

$\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$,

Деталізуємо множину $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ та вектор $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ в формулі (2.20) так:

$$(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,1}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}},$$
$$\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}})$$
$$\xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} (\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I},1}, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,1}, 1, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,2}, \dots, \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}}});$$
$$\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}; \mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}};$$

$$\text{якщо } \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{k}} = 0 \; \forall \; \mathfrak{k} = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}}, \text{ то } \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{k}} = 0, \qquad (2.20.1)$$

де $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$ згідно формули (2.17); $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{r}_2}$ – координата вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$; $\mathfrak{r}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}}$; $(\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} + 1)$ – кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{l}_1}$ – $\mathfrak{l}_1$-елемент першої множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{l}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2,\mathfrak{l}_2}$ – $\mathfrak{l}_2$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{l}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3,\mathfrak{l}_3}$ – $\mathfrak{l}_3$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathfrak{l}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4,\mathfrak{l}_4}$ – $\mathfrak{l}_4$-елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$; $\mathfrak{l}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$.

Особливістю в формулах (2.19) та (2.20.1) є те, що елементи $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}}$ повинні бути обов'язково в усіх компонентах, бо вони забезпечують підтримку функціонування всієї системи і компоненти зокрема. При цьому вони можуть бути переведені до пасивного стану, але на певний час, бо інакше тоді компонента перестане бути частиною системи і через певний час центр системи її вилучить та повідомить адміністратору системи про необхідність аналізу відповідної комп'ютерної станції. Таку особливість щодо наявності цих елементів в усіх компонентах задамо так:

$$\forall \; \mathfrak{k} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} : \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{k}} = 1, \qquad (2.21)$$

де $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{k}}$ – координати вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$.

Таким чином, обмеження щодо координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$ в формулі (2.19), яке задане формулою (2.21) буде доповнювати концептуальну модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, яку задано формулою (2.9). Аналогічно, таке ж обмеження введемо щодо координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ в формулі (2.20) так:

$$\forall\, \mathfrak{k} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}} : \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{k}} = \begin{cases} 1, \text{якщо } \mathfrak{k} - \text{елемент } \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{k}} \text{ в пасивному стані} \\ 2, \text{якщо } \mathfrak{k} - \text{елемент } \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{k}} \text{ в активному стані} \end{cases}, \quad (2.22)$$

де $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{k}}$ – координати вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів в підмножині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,\mathfrak{k}}$ - $\mathfrak{k}$ – елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$.

Розглянемо наповнення вузлів корпоративної мережі апаратним і програмним забезпеченням та їх вплив на архітектуру систем класу $\mathfrak{S}$. Вузли корпоративної мережі будуть відрізнятись між собою. Частина з них може бути однаковою і бути в кінцевих вершинах графу $\mathfrak{G}_2$ (формула (2.10)), тобто може і позиціонуватись однаково, А частина з них може бути однаковою і при цьому бути в різних сегментах або однакових. Все це впливатиме на їх безпеку та захист інформації в них. Крім того, в контексті виконання спеціалізованих завдань визначених для систем класу $\mathfrak{S}$ важливим є оцінювання на початковому етапі встановлення компонентів системи такого показника апаратного забезпечення вузла як функційна безпека. Апаратні ресурси вузла та функційна безпека в ньому впливатимуть на архітектуру систем класу $\mathfrak{S}$ і, тому, повинні бути враховані в концептуальній моделі архітектури. Аналогічно, це ж стосується і програмного забезпечення кожної конкретної комп'ютерної станції. Причому в програмному забезпеченні можна виділити такі основні його типи за призначенням: операційні системи; програмне забезпечення спрямоване на захист інформації від ЗПЗ та КА; прикладне програмне забезпечення користувачів корпоративних мереж.

Введемо для кожного вузла корпоративної мережі інтегрований показник апаратно-програмного забезпечення комп'ютерної станції в контексті її апаратного та програмного забезпечення для співвіднесення його значень в різних вузлах. Це дасть змогу оцінювати вузли за їх функційною безпекою, можливістю навантаження, оперативністю виконання завдань, що безпосередньо впливає на можливості та ефективне виконання завдань системами класу $\mathfrak{S}$. Значення таких інтегрованих показників з різних вузлів корпоративної мережі будуть використані центром системи для розподілення на виконання спеціалізованих завдань, також, для прийняття рішень про подальші кроки системи тощо.

Нехай інтегрований показник апаратно-програмного забезпечення комп'ютерної станції позначимо $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}$. Для кожної комп'ютерної станції його значення можуть бути різними, але й можуть бути однаковими. Також, вузлами, в яких визначатиметься його значення, можуть бути елементи різних підмножин вершин графа, зокрема підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, які задані за формулою (2.10). Ваги вершин з трьох різних підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ визначатимуться по-різному, а ваги елементів однієї підмножини однаково.

Інтегрований показник апаратно-програмного забезпечення комп'ютерної станції позначимо $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}$ та визначимо з врахуванням таких показників: показник апаратного забезпечення $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}$; показник програмного забезпечення $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}$; показник типу вузла $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}$. Визначимо кожен з показників таким чином, щоб його значення належало проміжку $[0,1]$. А, також, визначення значення показника задамо так, що показник певної характеристики для двох різних комп'ютерних станцій з відповідно різними значеннями буде кращим у випадку, коли його значення більше, і гіршим, коли його значення менше. Менше значення одного з двох показників не означає в цьому контексті, що воно гірше і, тому, недопустиме. Воно може бути більше певного порогового значення і, тому, вважатись прийнятним, а може бути нижче і, тому, вважатись неприйнятним. Для визначення значення показників потрібно враховувати характерні особливості апаратного чи програмного забезпечення, а також їх взаємодію між собою та розміщення. Тому, будемо використовувати для визначення значення кожного з розглядуваних показників структурні і параметричні характеристики. Кожна з характеристик повинна бути визначена числовим значенням і всі ці числові значення для їх використання як аргументів функції при визначенні певного з трьох показників можуть попередньо унормовуватись між собою, а можуть не унормовуватись, але при цьому тоді при конструюванні функції повинні враховуватись межі діапазонів їх значень. Ці особливості потрібно враховувати вже безпосередньо при визначенні функцій.

Задамо показник апаратного забезпечення $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}$ комп'ютерної станції так:

$$\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}} = \mathfrak{F}^{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}}\left(\mathfrak{i}^{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},1}}, \mathfrak{i}^{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},2}}, \dots, \mathfrak{i}^{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},n_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}}}}\right), \tag{2.23}$$

де $\mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ – функція, що визначає значення показника апаратного забезпечення $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}$ комп'ютерної станції згідно значень його структурних і параметричних характеристик $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},1}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},2}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \dots, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$; $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a},\mathfrak{I}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ - значення структурної чи параметричної характеристики; $\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}}$ – кількість значень структурних чи параметричних характеристик показника апаратного забезпечення $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}$, як аргументів функції $\mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$.

Аналогічно визначимо решту дві функції для двох показників.

Задамо показник програмного забезпечення $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}$ комп'ютерної станції так:

$$\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}} = \mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}\left(\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},1}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},2}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \dots, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}\right), \tag{2.24}$$

де $\mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ – функція, що визначає значення показника програмного забезпечення $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}$ комп'ютерної станції згідно значень його структурних і параметричних характеристик $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},1}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},2}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \dots, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$; $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p},\mathfrak{I}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ - значення структурної чи параметричної характеристики; $\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}$ – кількість значень структурних чи параметричних характеристик показника програмного забезпечення $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}$, як аргументів функції $\mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$.

Задамо показник типу вузла $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}$ комп'ютерної станції так:

$$\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}} = \mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}\left(\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},1}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},2}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \dots, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}\right), \tag{2.25}$$

де $\mathfrak{F}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ – функція, що визначає значення показника типу вузла $\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}$ комп'ютерної станції згідно значень його структурних і параметричних характеристик $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},1}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},2}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}, \dots, \mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$; $\mathfrak{i}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v},\mathfrak{I}}^{\mathfrak{S}}}^{\mathfrak{I}_{\mathfrak{p},\mathfrak{v}}^{\mathfrak{S}}}$ – значення структурної чи параметричної характеристики; $\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{I}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}^{\mathfrak{S}}}$ – кількість значень структурних чи

параметричних характеристик показника типу вузла $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}$, як аргументів функції $\mathfrak{F}^{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}}$.

Згідно формул (2.23)-(2.25) визначимо інтегрований показник апаратно-програмного забезпечення комп'ютерної станції позначимо $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}$ так:

$$\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}} = \mathfrak{F}^{\mathfrak{S}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}\left(\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}\right), \tag{2.26}$$

де $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}$ – функція, що визначає значення інтегрованого показника апаратно-програмного забезпечення комп'ютерної станції згідно значень його структурних і параметричних характеристик, які враховані при визначенні показників $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}$ як аргументи функції.

Конкретні параметри кожної з характеристик показників, що враховуватимуться в формулах (2.23) – (2.25) з кожної комп'ютерної станції в корпоративній мережі, будуть співвідноситись між собою для визначення мінімального і мінімального значень серед них.

Всі значення інтегрованого показника апаратно-програмного забезпечення комп'ютерних станцій унормуємо.

Результати з отриманих значень в кожному вузлі корпоративної мережі за формулою (2.26) будуть використовуватись центром системи для визначення варіантів подальших її кроків. Особливістю цих показників є те, що вони, також, пов'язані з множинами $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{B},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{B},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{B},2,3}$, які задані в формулі (2.10). В результаті застосування формули (2.6) до кожної з вершин графа $\mathfrak{G}_2$, який визначено за формулою (2.10), отримуємо граф зі зваженими вершинами.

Наслідок 3. Граф $\mathfrak{G}_2$ (формула 2.10), який задає середовище корпоративної мережі на рівні функційного призначення її вузлів та інтегрованого показника (формула (2.26)) апаратно-програмного забезпечення кожного вузла, є зваженим графом.

Таким чином, згідно наслідку 3 стає можливим виділення компонент у вузлах корпоративної мережі для систем класу $\mathfrak{S}$, в яких інтегрований показник апаратно-програмного забезпечення має вищий рівень порівняно з вузлами, в яких розміщено решту компонент, і це дає змогу центру системи виділити їх та розмістити в таких

компонентах елементи, які забезпечуватимуть функціонування центру системи, контролера та решту спеціалізованих завдань.

Розміщення вузлів корпоративної мережі на території підприємства, організації чи установи, зокрема наявність віддалених частин, та організація їх взаємодії впливатимуть на архітектуру систем класу $\mathfrak{S}$. Відповідно, потрібно врахувати особливості розподілення вузлів корпоративної мережі в просторі в концептуальній моделі архітектури $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.9)) систем класу $\mathfrak{S}$. Граф $\mathfrak{G}_2$ (формула(2.10)) формується з врахуванням множини вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, елементи якої позначатимуть маршрутизатори та комутатори. В результаті розглядатимемо всю корпоративну мережу як граф $\mathfrak{G}_2$ з виділенням в ньому вершин, що належать множині вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Вершини з цієї множини відображають в корпоративній мережі точки з'єднання і мости в графі та сегменти. Таке виділення цих вершин дає змогу порівнювати ці точки з'єднання між собою в контексті формування надійнішого місця розміщення комп'ютерних станцій та його визначення серед всіх наявних в поточний момент часу в корпоративній мережі. Це потрібно для центру системи, щоб правильно розподіляти елементи в компонентах системи та ставити завдання для виконання в певних компонентах. Тому, точки з'єднання в графах потребують оцінювання за певними критеріями для визначення надійнішого місця розміщення комп'ютерних станцій, тобто для порівняння різних сегментів корпоративної мережі між собою. Вибір критеріїв для проведення оцінювання здійснимо з врахуванням технічних особливостей побудови та розміщення корпоративних мереж.

Нехай множина вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ задана такими елементами $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{V},2,3,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{V},2,3,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{V},2,3,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}}}\right\}$, де $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}}$ – кількість вершин, що належать множині вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$. Для вершин з множини вершин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ визначимо функцію, яка встановлюватиме кожній з них вагу. Така вага кожної вершини буде рейтингом серед ваг решти вершин. Вона буде вказувати на рівень надійності розміщення сегменту корпоративної мережі, що визначається точкою з'єднання, в контексті доступу до нього і пов'язаних з ним кінцевих вершин, територіального розташування, доступу в приміщення, доступу до конкретних станцій користувачами, доступу безпосередньо

до серверів тощо. Більше значення ваги вершини серед ваг двох вершин вказуватиме на кращий варіант розміщення.

Задамо значення ваг вершин з множини вершин $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ множиною ваг точок з'єднань таким чином: $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}} = \left\{\mathfrak{m}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}, \mathfrak{m}_{\mathfrak{V},2,3,2}^{\mathfrak{S},\mathfrak{V}}, \dots, \mathfrak{m}_{\mathfrak{V},2,3,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}}^{\mathfrak{S},\mathfrak{V}}\right\}$, де $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}} = \mathfrak{n}_{\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}}$. Кожен елемент множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$ буде відповідним за порядковим номером елементу з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$. Тоді, задамо множину функцій $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}} = \left\{\mathfrak{f}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}, \mathfrak{f}_{\mathfrak{V},2,3,2}^{\mathfrak{S},\mathfrak{V}}, \dots, \mathfrak{f}_{\mathfrak{V},2,3,\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}}^{\mathfrak{S},\mathfrak{V}}\right\}$, в якій буде $\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}$ функцій. Кожна з цих функцій буде обчислювати значення ваги точки з'єднання винятково за однією з характеристик розміщення вузлів в корпоративній мережі. Таким чином, кількість таких характеристик визначатиме кількість функцій в множині $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$. Кожна з функцій множини $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$ буде застосовною до всіх елементів множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$. Згідно так заданих множин задамо відображення між множинами так:

$$\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}} \xrightarrow{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}} \mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}. \tag{2.27}$$

Деталізуємо в формулі (2.27) множини через їх елементи так:

$$\mathfrak{m}_{\mathfrak{V},2,3,\mathfrak{l}}^{\mathfrak{S},\mathfrak{V}} = \frac{\sum_{\mathfrak{f}=1}^{\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}} \left(\mathfrak{y}_{\mathfrak{V},2,3,\mathfrak{f}}^{\mathfrak{S},\mathfrak{V}} \cdot \mathfrak{f}_{\mathfrak{V},2,3,\mathfrak{f}}^{\mathfrak{S},\mathfrak{V}}\left(\mathfrak{m}_{\mathfrak{V},2,3,\mathfrak{l}}^{\mathfrak{S}}\right)\right)}{\sum_{\mathfrak{f}=1}^{\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}} \mathfrak{y}_{\mathfrak{V},2,3,\mathfrak{f}}^{\mathfrak{S},\mathfrak{V}}}, \tag{2.28}$$

де $\mathfrak{l} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}$ - кількість функцій в множині $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}}$ – кількість елементів множин $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ та $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$; $\mathfrak{y}_{\mathfrak{V},2,3,\mathfrak{f}}^{\mathfrak{S},\mathfrak{V}}$ – коефіцієнти для співвіднесення ваг всіх функцій з множини $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$; $\mathfrak{f} = 1,2,\dots,\mathfrak{n}_{\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}}$.

Таким чином, множина $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$ буде сформована елементами, що обчислюватимуться за формулою (2.28). Функції будуть застосовні до усіх елементів з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$. В формулі (2.28) аргументом функції є один елемент, але при обчисленні значення функції будуть враховані всі наявні елементи в множині $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$. Поєднання в формулі (2.28) всіх функцій з множини $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$ та всіх елементів з

множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ дає змогу здійснити обчислення значення ваги з врахуванням усіх можливих особливостей розміщення вузлів корпоративної мережі та врахування їх всіх співвідносно до вузла, для якого обчислюється значення ваги. Оскільки функції визначають значення з проміжку $[0,1]$, то значення ваги вершини теж буде належати проміжку $[0,1]$, оскільки коефіцієнти, які в формулі (2.8), будуть мати унормовані значення.

Значення ваг вершин з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ за критерієм розміщення комп'ютерних станцій на території підприємства і їх загального місця в структурі корпоративної мережі, які обчислені за формулою (2.28), будуть відрізнятись від ваг цих же вершин, які обчислені за критерієм їх апаратно-програмного забезпечення. Центр системи буде використовувати значення ваг вершин з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$, які обчислені за різними критеріями, для визначення подальших кроків системи.

В функціях з множини функцій $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$ будуть враховані особливості розміщення комп'ютерних станцій на території підприємства і їх загального місця в структурі корпоративної мережі в контексті надійнішого сегменту і вузла з функціональної та кібербезпеки. Функції з множини $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$, враховуючи їх призначення для визначення значень елементів з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$, повинні враховуватись в концептуальній моделі систем класу $\mathfrak{S}$. Задамо кожну з таких функцій відповідним переліком критеріїв, спрямуванням за певними особливостями архітектури корпоративної мережі та визначенням відмінностей між розглядуваними вузлами.

Корпоративна мережа може бути територіально розподілена так: 1) всі її вузли перебувають в одному приміщенні і поєднані дротовим зв'язком; 2) всі її вузли перебувають в різних приміщеннях на території підприємства і поєднані дротовим зв'язком; 3) всі її вузли перебувають в одному приміщенні і поєднані дротовим зв'язком та допускають поєднання бездротовим зв'язком; 4) всі її вузли перебувають в різних приміщеннях на території підприємства і поєднані дротовим зв'язком та допускають поєднання бездротовим зв'язком; 5) всі її вузли перебувають в різних приміщеннях на різних віддалених між собою територіях підприємства і поєднані дротовим зв'язком, що належить підприємству; 6) всі її вузли перебувають в різних приміщеннях на різних віддалених між собою територіях підприємства і поєднані

дротовим та бездротовим зв’язком, що належить підприємству; 7) всі її вузли перебувають в різних приміщеннях на різних віддалених між собою територіях підприємства і поєднані дротовим зв’язком, що не належить підприємству, а є мережами загального доступу. Можуть бути, також, і інші варіанти принципово відмінні від розглянутих, а також варіанти, що є комбінаціями розглянутих варіантів. В таких варіантах з комбінуванням розглянутих варіантів потрібно розглядати випадки, коли більшість вузлів корпоративної мережі і першочергово її основна частина перебувають у варіанта 1 чи 2, а решта суттєво менша кількість вузлів перебуває так, що відноситься до варіантів 3-7. Також, організація бездротового зв’язку теж може мати різні варіанти. Таким чином, задамо функцію $\mathfrak{f}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}$ такою, що визначає вагу вершини з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ за критерієм територіального розподілення вузлів корпоративної мережі в приміщеннях підприємства. Розглянуті варіанти 1-7 та похідні від них варіанти є дискретними величинами і можуть бути задані числами з проміжку $[0,1]$. Всі ці величини залежать від конкретного випадку з варіантів 1-7 та похідних з них варіантів, а також від кількості вузлів корпоративної мережі, і для кожного набору елементів з множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$ будуть визначатись з врахуванням функційної та кібербезпеки. Причому, кількість вузлів корпоративної мережі буде впливати на значення функції $\mathfrak{f}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}$ для решти однакових показників. Також, для тих самих елементів множини $\mathfrak{M}_{\mathfrak{V},2,3}^{\mathfrak{S}}$, які мають найвище значення функції $\mathfrak{f}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}$ у варіанті 1 значення буде вище , ніж у варіанті 7. Безпосереднє визначення функції $\mathfrak{f}_{\mathfrak{V},2,3,1}^{\mathfrak{S},\mathfrak{V}}$ та деталізації обробки її аргументів є необхідним при розробці методу внутрішньої організації функціонування систем класу $\mathfrak{S}$.

Розглянемо призначення другої функції $\mathfrak{f}_{\mathfrak{V},2,3,2}^{\mathfrak{S},\mathfrak{V}}$ з множини $\mathfrak{F}_{\mathfrak{V},2,3}^{\mathfrak{S},\mathfrak{V}}$. Корпоративна мережа може містити або переважно містить за певних правил її розроблення частини, які поділені за певним призначенням і їх як правило називають сегментами. Сегменти корпоративної мережі можуть бути такі: демілітаризована зона; серверна частина; робочі місця користувачів (приватна зона). В демілітаризованій зоні переважно містяться загальнодоступні сервіси. Вона фактично виступає додатковим рівнем безпеки. Сервери та комп’ютерні станції можуть бути в різних сегментах корпоративної мережі, а можуть бути змішано в різних сегментах або комбінуванням

окремого та змішаного варіантів. В контексті функційної та кібербезпеки точки з'єднання графа, які є визначальними для сегментів корпоративної мережі, в різних варіантах поділу її на частини будуть мати різні ваги як вершини графа. Величини, які будуть аргументами функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,2}$, теж є дискретними величинами і, тому, потребують їх співвіднесення між собою за критерієм віднесення до сегменту та з врахуванням кількості вузлів в таких сегментах і в корпоративній мережі в цілому. Значення функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,2}$, як ваги вершини, для вершини, що відповідає сегменту з демілітаризованою зоною переважно буде меншим, ніж для вершини, що відповідає сегменту з серверами. Таким чином, значення функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,2}$ може бути визначено згідно варіантів з сегментами, кількості вузлів корпоративної мережі в сегментах, загальної кількості різних елементів підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ та результатів їх порівняння за критерієм в контексті функційної та кібербезпеки.

В корпоративну мережу може бути дозволено під'єднання з-за меж територіально розміщених її компонентів. Кількість користувачів таких під'єднань може бути різною. Доступ до ресурсів корпоративної мережі для користувачів може бути різним і їх можливості для виконання певної роботи теж можуть різними. Мінімізована кількість таких під'єднань може бути прийнята при визначенні значення ваги для вершини, в сегменті якої надається такий доступ, за більше значення, ніж у випадку більшої кількості під'єднань, більшої кількості користувачів, більшої можливості з виконання роботи з-за меж підприємства тощо. Задамо функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,3}$ для визначення ваги вершини за критерієм щодо доступності і можливості роботи в корпоративній мережі з-за меж території підприємтва. В цьому випадку деталізація показників оцінювання в функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,3}$ може, також, враховувати зв'язок мережами загального доступу, зв'язок безпосередньо мережею підприємства, бездротовий зв'язок безпосередньо із мережею підприємства за умови близькості точки під'єднання тощо.

Топологія комп'ютерної мережі впливає на функційну та кібербезпеку. Тому, для врахування типу топології задамо функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,4}$. Визначимо її так, щоб значення обчислене цією функцією було більше в тому випадку, коли топологія мережі є найбільш вдалою, зокрема, наприклад, топологія «зірка». Системи класу $\mathfrak{S}$ будуть

функціонувати згідно наявної топології, але вони можуть використовувати і свою топологію, а також перебудовувати свою архітектуру включно з топологією. Але визначення функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,4}$ буде враховувати лише топологію комп'ютерної мережі підприємства та кількість комп'ютерних станцій, серверів. Таким чином, для визначення функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,4}$ будуть враховуватись, також, елементи підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ та їх кількість і тип зв'язку між ними. Результатом виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,4}$ буде значення ваги вершини, як елементу з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що відображатиме топологію для сегменту мережі порівняно з рештою вершин, як елементів з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, та кількістю вузлів в кожному сегменті.

Враховуючи розподілення вузлів корпоративної мережі, важливою характеристичною властивістю для систем класу $\mathfrak{S}$ буде час, який витрачатиметься на пересилання повідомлень між вузлами. Специфіка завдань для систем класу $\mathfrak{S}$ така, що при їх виконанні можуть виникати часові затримки при пересиланні повідомлень і центр системи повинен володіти інформацією про тривалість пересилання повідомлень. Наприклад, якщо після спроби встановити з'єднання повідомлення втрачено в мережі з певних причин, то центр системи повинен обробити таку подію з врахуванням відомостей про орієнтовний час на пересилання типового повідомлення. Для визначення типового часу пересилання повідомлення між вузлами в мережі задамо двох аргументну функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,5}$, в якій аргументами будуть елементи підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ та елементи, в яких буде центр системи. Топологія мережі зі складною архітектурою, також буде впливати на час пересилання повідомлень. Результатом виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,5}$ буде значення ваги вершини, як елементу з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що відображатиме час надсилання повідомлення до центру системи. При зміні місця центру це значення буде змінюватись після виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,5}$.

Граф $\mathfrak{G}_2$ (формула (2.10)) відображає вузли корпоративної мережі. Для оцінювання центром системи виділимо в ньому дерево та встановимо центр дерева. Це потрібно для визначення вузла в корпоративній мережі, який буде відображати центр в мережі щодо решти вузлів. Визначення такого центру задамо функцією $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,6}$

і здійснимо його за алгоритмом, згідно якого послідовно покроково вилучаються всі граничні вершини. Якщо таких вершин буде дві, то кожна з них буде центром і, тоді, для використання центром системи вибираємо за центр одну з них. Аналогічно, виконуємо таку ж функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,6}$ для вершин, в яких будуть розміщені компоненти систем класу $\mathfrak{S}$. В результаті отримуємо центр корпоративної мережі та центр системи і визначаємо відхилення в кількості ребер графа. Такий аналіз закладаємо як показних для центру системи. Він визначатиме оптимальне розміщення центру системи після прийняття рішення щодо перебудови архітектури системи та розміщення центру системи і контролера у вузлах корпоративної мережі. Таке порівняння двох центрів є необхідним у випадку, коли система класу $\mathfrak{S}$ в процесі функціонування не буд містити всіх компонент. Може бути такий випадок, що центр системи буде взагалі у вузлі, що є кінцевою вершиною графа в поточний момент часу. При переміщенні центру системи і контролера врахування такої інформації щодо фізичного центру системи є необхідним, бо впливатиме на час пересилання повідомлення та забезпечення показника їх стійкості в системи. Результатом виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,6}$ буде значення ваги вершини, як елементу з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що відображатиме найкоротший шлях до центру системи та номер вершини, в якій буде центр дерева графа.

Центр системи може бути розподілений в різних вершинах. Тоді, функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,6}$ потрібно виконати і для цих вершин. В результаті отримання таких трьох результатів центр системи буде визначати місця з вершин для наступного розміщення центру системи з врахуванням ваги вершин, як елементів з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$.

Визначення центру системи потрібно для того, щоб при перебудові системи він не розмістився повністю в одному сегменті або в декількох віддалених сегментах.

При визначенні вершини, в якій буде центр корпоративної мережі, та вершини, в якій буде центр системи, потрібно мати відомості про маршрути, якими будуть передаватись повідомлення в мережі для компонентів системи. Функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,7}$ задамо так, щоб вона визначала всі маршрути між вершинами, які задані елементами з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, з рештою вершин та видавала найдовший. При перебудові

системи такі маршрути будуть оновлюватись після виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,7}$. Крім того, отримані маршрути будуть використані для виконання спеціалізованих завдань, в яких потрібно спрямовувати КА на хибні об'єкти для атак. Результатом виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,7}$ буде значення ваги вершини, як елементу з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що відображатиме найдовший маршрут в дереві графа.

Кожна вершина дерева графа $\mathfrak{G}_2$ (формула (2.10)), які визначаються елементами з підмножин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}$ мають свої ваги згідно інтегрованого показника $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}$ (формула (2.26)) апаратно-програмного забезпечення комп'ютерної станції чи серверу, тоді задамо функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,8}$ так, що її значенням будуть ваги вершин, які задані елементами підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що визначатимуться як середньоарифметичні значення ваг кінцевих вершин, що формують кожен сегмент корпоративної мережі.

Функцію $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,9}$ задамо таким чином, що кожен елемент підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ отримувати вагу за критерієм, який враховує фізичний доступ до комп'ютерних станцій в приміщеннях, розподіл доступу за визначеними ролями для користувачів чи довільний доступ. Результатом виконання функції $\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,8}$ буде значення ваги вершини, як елементу з підмножини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$, що відображатиме фізичний доступ до комп'ютерних станцій та доступ користувачів за ролями.

Таким чином, множина функцій $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$ дає змогу отримати числові значення ваг вершин графа $\mathfrak{G}_2$ (формула (2.10)). Значення ваг будуть використані центром системи для визначення подальших кроків системи. Кількість функцій з множини функцій $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$ може бути збільшена за рахунок доповнення нових особливостей, що характеризуватимуть вершини графа. Крім того, для обчислення значень ваг вершин центр системи може за певних визначених умов використовувати не всі функції, а частину з них.

Розглянемо місце центру системи і контролера в базовому поданні концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.9)) та у взаємодії між собою. Порівняно з рештою визначальних характеристик ці компоненти в архітектурі системи пов'язані між собою та подані трьома визначальними властивостями з відображенням їх відповідно трьома множинами. Цей зв'язок між центром системи та контролером

випливає з функційного призначення контролера. Його завданням є затвердження або відхилення рішення щодо подальших кроків системи, які сформовано центром системи. Також, контролер повинен формувати базу з попередніх рішень та відповідей на них від центру системи та від нього. Таким чином, контролер безпосередньо взаємодіє саме з центром системи і не взаємодіє з рештою підсистем. Тому, контролер, який визначений елементом одноелементної множини $\mathfrak{V}_{10,1}$, при синтезі систем згідно їх визначальних властивостей, що задані множинами $\mathfrak{V}_i$ $(i = n_{\mathfrak{V}}, n_{\mathfrak{V}} - \text{кількість характеристик})$, не поєднується з усіма ними, а може бути тільки поєднаним з множинами $\mathfrak{V}_1$ та $\mathfrak{V}_2$. Решта визначальних властивостей, що задані множинами $\mathfrak{V}_i$ $(i = n_{\mathfrak{V}}, n_{\mathfrak{V}} - \text{кількість характеристик})$, крім множини $\mathfrak{V}_{10,1}$ $(i = 10)$, можуть в процесі синтезу системи поєднуватись, а не комбінуватись простим поєднанням.

Центр системи формується при синтезі в системі таких визначальних властивостей: $\mathfrak{V}_1$ – тип архітектури системи (централізована, децентралізована, гібридна); $\mathfrak{V}_2$ – типи та кількість центрів в архітектурі системи (цілісний в одній компоненті, поділений на рівнозначні частини в різних компонентах, поділений ієрархічно в різних компонентах, цілісний ієрархічний в різних компонентах). При цьому центр системи призначений для опрацювання результатів функціонування системи протягом певного часу і на поточний момент та результатів виконання завдань спеціалізованим функціоналом. Оскільки система є розподіленою з багатьма компонентами, то при виборі варіанту з централізованою архітектурою центр системи не зможе перебувати в усіх компонентах, як наприклад при варіанті з децентралізованою архітектурою. Але принцип синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$ передбачає забезпечення використання багатоваріантності в процесі функціонування таких систем, тобто зміну централізації системи при перебудові її архітектури. Тому, центр системи згідно таких вимог не може бути розподілений в усіх компонентах одночасно на увесь тривалий період експлуатації системи, бо на певному етапі система може прийняти рішення про перехід до централізованої архітектури. Не всі компоненти системи можуть бути одночасно у ввімкнених комп'ютерних станціях. Частина комп'ютерних станцій може бути не увімкнена і може бути так, що частина компонент, які саме містяться у ввімкнених комп'ютерних станціях, всі будуть

містити елементи для функціонування центру системи і саме в активному стані. В цьому випадку тоді всі компоненти в поточний момент часу будуть містити центр системи і, при цьому, архітектура може бути задана не децентралізовано, а саме централізовано. Тоді, контролер буде взаємодіяти з кожним центром системи і, відповідно, з усіма наявними в системі компонентами в поточний момент часу. Центр системи можна було б не виділяти окремою підсистемою а інтегрувати безпосередньо в спеціалізований функціонал. І, тоді архітектура системи буде децентралізованою або централізованою з розділенням центру системи між усіма компонентами системи в процесі її тривалого функціонування. Але в такому випадку зникає можливість перебудовувати систему в частині її центру до меншої кількості компонент з центром системи відносно загальної їх кількості та до частково централізованої архітектури. Для розглянутих випадків контролер міг би взаємодіяти в системі з окремими компонентами, в яких був би центр системи чи система була б без явно виокремленого центру. В цьому випадку в компоненті виконувалось би спеціалізоване завдання і в цій же компоненті повинно прийнятись рішення щодо результату такої роботи, тоді це рішення повинно аналізуватись контролером. Таким чином, окремого центру системи немає, але виконувані завдання можуть за відсутності контролера і бути як результат прийнятих рішень центром системи. Але оскільки згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$ контролер повинен бути обов'язково, то такі варіанти щодо централізації такого типу неможливі: 1) центр системи не виділено окремо, всі компоненти системи виконують завдання і видають рішення, які по суті приймаються центром, що міститься в них; 2) центр системи виділено окремо і він розподілений між усіма компонентами на увесь час функціонування системи. У варіанті 2) система не зможе перебудовувати свій центр згідно частково централізованої архітектури. При цьому вона може перебудовувати свій центр згідно децентралізованої або централізованої архітектури, де централізована архітектура вимагатиме наявності в кожній компоненті окремого або розподіленого центру системи. А розподілення центру системи лише між частиною компонент, не всіма компонентами вже є неможливим. Таким чином, доведено твердження щодо обмеження згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$ в частині вимог до елементів множин $\mathfrak{V}_1$ та $\mathfrak{V}_2$.

Теорема 2. Згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$ центр системи, який задано визначальними властивостями з елементів множин $\mathfrak{V}_1$ та $\mathfrak{V}_2$, синтезується в елементах множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$, яку визначено в формулі (2.12), і не повинен поєднуватись з елементами множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$, $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$ в єдину підсистему компоненти.

Дійсно, якщо центр системи буде поєднано з контролером, то тоді центр системи та контролер при перебудові системи повинні бути разом, як окрема підсистема, здійснювати переміщення в іншу одну й ту ж компоненту або в різні компоненти. Це суперечить принципу синтезу $\mathfrak{P}$, в якому задається вимога, що центр системи може бути в компонентах, в яких відсутній контролер. Таким чином, отримуємо наслідок з теореми 2.

Наслідок 4. Елементи множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$, $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$, $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$, $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$ не поєднуються між собою так, щоб було сформовано новий елемент, який належить двом і більше з цих множин одночасно.

Наслідок 5. Згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$ елементи множин $\mathfrak{V}_1$ та $\mathfrak{V}_2$ та одноелементної множини $\mathfrak{V}_{10,1}$ не поєднуються в єдиному елементі, що належав би множині елементів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$, з елементів якої формують компоненти системи.

Згідно теореми 2 та наслідків 4 і 5 отримуємо такі обмеження на елементи концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, яку задано базовим подання згідно формули (2.9):

$$\forall\, \mathfrak{j}, \mathfrak{i}\colon \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{i}} \cap \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{j}} = \emptyset; \qquad (2.29)$$

$$\mathfrak{i} = 1,2,3,4;\ \mathfrak{j} = 1,2,3,4;\ \mathfrak{j} \neq \mathfrak{i}.$$

Таким чином, згідно формул (2.10) – (2.29) деталізовано та доповнено концептуальну модель систем класу $\mathfrak{S}$, яку задано базовим поданням у формулі (2.9), формальним поданням її елементів та компонентів з врахуванням середовища функціонування, територіального розміщення мультикомп'ютерних систем, завдань внутрішнього рівня системи, завдань спеціалізованого функціоналу, особливостей внутрішньої архітектури систем, контролера прийнятих рішень.

Концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ мультикомп'ютерних систем, яку задано базовим поданням згідно формули (2.9), потребує розширення щодо множин, зв'язків між ним та обмежень, що встановлюються принципом синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$, згідно визначень множин та зв'язків між ними і їх елементами, які встановлені згідно формул (2.2) – (2.8) і формул (2.10) – (2.29).

2.3. Концептуальна модель мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА

Згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$, деталізації множин і їх елементів в формулі (2.9), обмежень на елементи в множинах, що випливають з вимог принципу синтезу $\mathfrak{P}$, та згідно визначень і відображень в формулах (2.2) – (2.29) концептуальну модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ архітектури мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА задамо так:

$$\mathfrak{A}_{\mathfrak{M},\mathfrak{S}} = \langle \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}), \mathfrak{P}_{\mathfrak{M}} \rangle:$$

$$1)\ \forall\, \mathfrak{k}\colon \mathfrak{V}_{10,1} \subset \mathfrak{P}_{\mathfrak{k}}(\mathfrak{M}_{\mathfrak{S}});\ \mathfrak{P}_{\mathfrak{k}}(\mathfrak{M}_{\mathfrak{S}}) \in \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}});\ \mathfrak{k} = 1,2,\dots,\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})};$$

$$2)\ \mathfrak{M}_{\mathfrak{S}} = \bigcup_{\mathfrak{i}_1=1}^{\mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}} \mathfrak{M}_{\mathfrak{i}_1};\ \mathfrak{M}_{\mathfrak{i}_1} = \left\{\mathfrak{m}_{\mathfrak{i}_1,1}, \mathfrak{m}_{\mathfrak{i}_1,2}, \dots, \mathfrak{m}_{\mathfrak{i}_1,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{i}_1}}}\right\};\ \mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{i}_1}};\ \mathfrak{M}_{10} = \{\mathfrak{m}_{10,1}\};$$

$$3)\ \mathfrak{P}(\mathfrak{M}_{\mathfrak{S}}) \xrightarrow{\mathfrak{P}_{\mathfrak{M}}} \mathfrak{W}(\mathfrak{M}_{\mathfrak{S}});\ \mathfrak{w}_{\mathfrak{j}} \in \mathfrak{W}(\mathfrak{M}_{\mathfrak{S}});\ \mathfrak{w}_{\mathfrak{j}} = \left(\mathfrak{w}_{\mathfrak{j},1}, \mathfrak{w}_{\mathfrak{j},2}, \dots, \mathfrak{w}_{\mathfrak{j},\mathfrak{i}_2}, \dots, \mathfrak{w}_{\mathfrak{j},\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}}\right);$$

$$\mathfrak{w}_{\mathfrak{j},\mathfrak{i}} = \begin{cases} 0, \text{якщо елемент відсутній в підмножині } \mathfrak{P}_{\mathfrak{j}}(\mathfrak{M}_{\mathfrak{S}}), \\ 1, \text{якщо елемент наявний в підмножині } \mathfrak{P}_{\mathfrak{j}}(\mathfrak{M}_{\mathfrak{S}}); \end{cases}$$

$$\mathfrak{w}_{10,1} = 1;\ \mathfrak{j} = 1,2,\dots,\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})};\ \mathfrak{i}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$$

$$4)\ \mathfrak{G}_2 = (\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2});$$

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2} \subseteq \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1}\right) \cup \left(\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \times \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}\right);\ \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2} = \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3};$$

$$5)\ \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1} = \left\{\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,2}, \dots, \mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}}\right\};$$

$$\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}} = \bigcup_{\mathfrak{l}_1=1}^{4} \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{l}_1};\ \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}} = \sum_{\mathfrak{l}_1=1}^{4} \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{l}_1}};$$

$$\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}: \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}} \to \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1};$$

$$6)\ \mathfrak{P}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1} = \left\{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}\right\};$$

$$\left(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{l}_3,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}\right) \xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1};\ \left(\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{l}_3,1}, \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}\right) \xrightarrow{\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2};$$

$$\mathfrak{l}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}};\ \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,0} = \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{l}_3,1};\ \mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}};\ \mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} = \mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}};$$

$$\text{якщо } \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{f}_1} = 0\ \forall\ \mathfrak{f}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}},\ \text{то } \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{f}_1} = 0;$$

$$\forall\ \mathfrak{f}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}}: \mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,\mathfrak{f}_2} = 1;$$

$$7)\ \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}} = \mathfrak{F}^{\mathfrak{S}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}\left(\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}\right);$$

$$8)\ \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3} \xrightarrow{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}} \mathfrak{M}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3};\ \mathfrak{m}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{l}_4} = \frac{\sum_{\mathfrak{f}_3=1}^{\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}} \left(\mathfrak{y}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{f}_3} \cdot \mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{f}}\left(\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{V},2,3,\mathfrak{l}_4}\right)\right)}{\sum_{\mathfrak{f}_3=1}^{\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}} \mathfrak{y}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{f}_3}};$$

$$9)\ \forall\ \mathfrak{g}_1, \mathfrak{g}_2: \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{g}_1} \cap \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{g}_2} = \emptyset;\ \mathfrak{g}_1 = 1,2,3,4;\ \mathfrak{g}_2 = 1,2,3,4;\ \mathfrak{g}_1 \neq \mathfrak{g}_2, \quad (2.30)$$

де $\mathfrak{M}_{\mathfrak{S}}$ – множина елементів та компонентів в архітектурі системи, які сформовані згідно заданих визначальних властивостей; $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$ – множина підмножин; $\mathfrak{P}_{\mathfrak{M}}$ – множина предикатів заданих на множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{P}_{\mathfrak{f}}(\mathfrak{M}_{\mathfrak{S}})$ – $\mathfrak{f}$ – тий елемент множини $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{f} = 1,2,\dots,\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$; $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_{\mathfrak{S}})$; множина $\mathfrak{V}_{10,1} = \{\mathfrak{v}_{10,1}\}$; $\mathfrak{V}_{10,1}$ – одноелементна множина; $\mathfrak{M}_{\mathfrak{i}_1}$ - $\mathfrak{i}_1$ – та підмножина для певних елементів та компонентів в архітектурі системи; $\mathfrak{i}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин; $\mathfrak{m}_{\mathfrak{i}_1,\mathfrak{I}}$ – $\mathfrak{i}_1$-елемент $\mathfrak{M}_{\mathfrak{i}_1}$ підмножини; $\mathfrak{I} = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{i}_1}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{i}_1}}$ – кількість елементів підмножини $\mathfrak{M}_{\mathfrak{i}_1}$; $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$ – множина векторів; елемент $\mathfrak{w}_{\mathfrak{j}} \in \mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$; $\mathfrak{j} = 1,2,\dots,\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$; $\mathfrak{w}_{\mathfrak{j},\mathfrak{i}_2}$ – $(\mathfrak{j},\mathfrak{i}_2)$ – координата вектору $\mathfrak{w}_{\mathfrak{j}}$; $\mathfrak{i}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$; $\mathfrak{G}_2$ – граф зв'язків компонентів середовища комп'ютерної мережі; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2} = \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,1} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,2} \cup \mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2}$ – множина всіх вершин графа $\mathfrak{G}_2$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},2}$ – множина ребер графа; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$ – множина типових компонентів систем класу $\mathfrak{S}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathfrak{l}_2}$ – $\mathfrak{l}_2$-елемент множини типових компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{l}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$ – кількість елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$ – множина елементів, з яких формуватимуться компоненти системи; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ – підмножина елементів для забезпечення перебування у вузлі корпоративної

мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},2}$ – підмножина елементів для забезпечення функціонування центру системи; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},3}$ – підмножина елементів для забезпечення функціонування контролера; $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},4}$ – підмножина елементів для забезпечення перебування у вузлі корпоративної мережі, для забезпечення виконання функцій заданих певними елементами, для доповнення новими елементами та забезпечення комунікації з центром системи; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}}$ – кількість елементів в множині $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T}}$; $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ – множина функцій; $\mathfrak{P}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$ – множина предикатів для встановлення відомостей в системі про стан наявних активних і пасивних та відсутніх елементів в компонентах; $\mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}, \mathfrak{p}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$ – предикати з множини $\mathfrak{P}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1,0}$ – перша координата вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$, яка є значенням номеру компоненти з системи; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{I}_3,1}$ - значення номеру компоненти за списком системи; $\mathfrak{I}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – кількість векторів в множині векторів $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}$; $\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} = \mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{r}_1}$ – координата вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$; $\mathfrak{r}_1 = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}}$; $(\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}} + 1)$ – кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,1}$; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2,\mathfrak{r}_2}$ – координата вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$; $\mathfrak{r}_2 = 1,2,\dots,\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}}$; $(\mathfrak{n}_{\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}} + 1)$ – кількість координат вектору $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},1,2}$; $\mathfrak{F}^{\mathfrak{S}}_{\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v}}}$ – функція, що визначає значення інтегрованого показника апаратно-програмного забезпечення комп'ютерної станції згідно значень його структурних і параметричних характеристик, які враховані при визначенні показників $\mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{a}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{p}}, \mathfrak{I}^{\mathfrak{S}}_{\mathfrak{p},\mathfrak{v},\mathfrak{v}}$ як аргументів функції; $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$ – множина функцій $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3} = \left\{\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,1}, \mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,2}, \dots, \mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}}\right\}$; $\mathfrak{I}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}}$; $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}$ - кількість функцій в множині $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}}$ – кількість елементів множин $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}$ та $\mathfrak{M}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$; $\mathfrak{y}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{f}_3}$ – коефіцієнти для співвіднесення ваг всіх функцій з множини $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}$; $\mathfrak{f}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}$.

Таке задання концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ систем класу $\mathfrak{S}$ згідно формули (2.30) враховує множинність елементів, які знаходяться у відносинах та зв'язках один з

одним і утворюють певну цілісність та єдність частин, що відповідає визначенню систем. Задані в формулі (2.30) взаємозв'язки між частинами системи та її внутрішня організованість мають конкретні властивості, які змінюються відповідно до зовнішніх і внутрішніх впливів та мети використання системи.

В концептуальній моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ систем класу $\mathfrak{S}$ виокремлено компоненти і елементи. Причому, частина компонентів містить, також, менші компоненти та елементи. Тому, синтезовані системи класу $\mathfrak{S}$ є складними. Також, в моделі виділені елементи системи мають своє призначення, між ними визначено ієрархію та вони взаємопов'язані. Відповідно, системи класу $\mathfrak{S}$ синтезовані згідно їх визначальних властивостей, які в загальному випадку не отримуються поєднанням властивостей їх компонентів, а функційні можливості системи в цілому є більшими, ніж функційні можливостей її частин. Розглянемо функційну впорядкованість систем класу $\mathfrak{S}$, тобто вираження того, як елементи, компоненти та ієрархічні рівні системи пов'язані та взаємодіють між собою, а також які властивості має цілісність, що утворена ними. Зображення місця розміщення і зв'язків елементів та компонентів концептуальної моделі в узагальненій архітектурі середовища функціонування систем класу $\mathfrak{S}$ з врахуванням задання концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ (формула (2.30)) подано на рис. 2.2.

Співвіднесення елементів та компонентів концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, мультикомп'ютерних систем класу $\mathfrak{S}$ та середовища функціонування систем на рис. 2.2 відображає вузли корпоративної мережі, в які можуть бути встановлені компоненти системи. При цьому вони відповідають елементам множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2}$ всіх вершин графа $\mathfrak{G}_2$. Допускається, що компоненти мультикомп'ютерної системи класу $\mathfrak{S}$ можуть бути не в усіх вузлах корпоративної мережі. Таким чином, компоненти мультикомп'ютерної системи класу $\mathfrak{S}$ в контексті зображеному на рис. 2.2 і в формулі (2.30) підтверджують можливість масштабування системи на довільну кількість елементів множини $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2}$. А концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ архітектури мультикомп'ютерних систем класу $\mathfrak{S}$ є повною, бо охоплює визначальні властивості таких систем, принципи згідно яких вони синтезуються та відношення визначені в 1)-9) формули (2.30). Підтвердженням синтезу саме систем згідно концептуальної

моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ є наявність загальноприйнятих ознак систем: цілісність, латентність, підсилення ефективності системи за рахунок сукупності компонентів, поділ на частини із зв'язками між ними, наявність властивостей не властивих підсистемам і блокам, саморегулювання, багатоваріантність, взаємодія із зовнішнім середовищем. Ці ознаки потребуватимуть деталізації в контексті подання організації функціонування систем класу $\mathfrak{S}$.

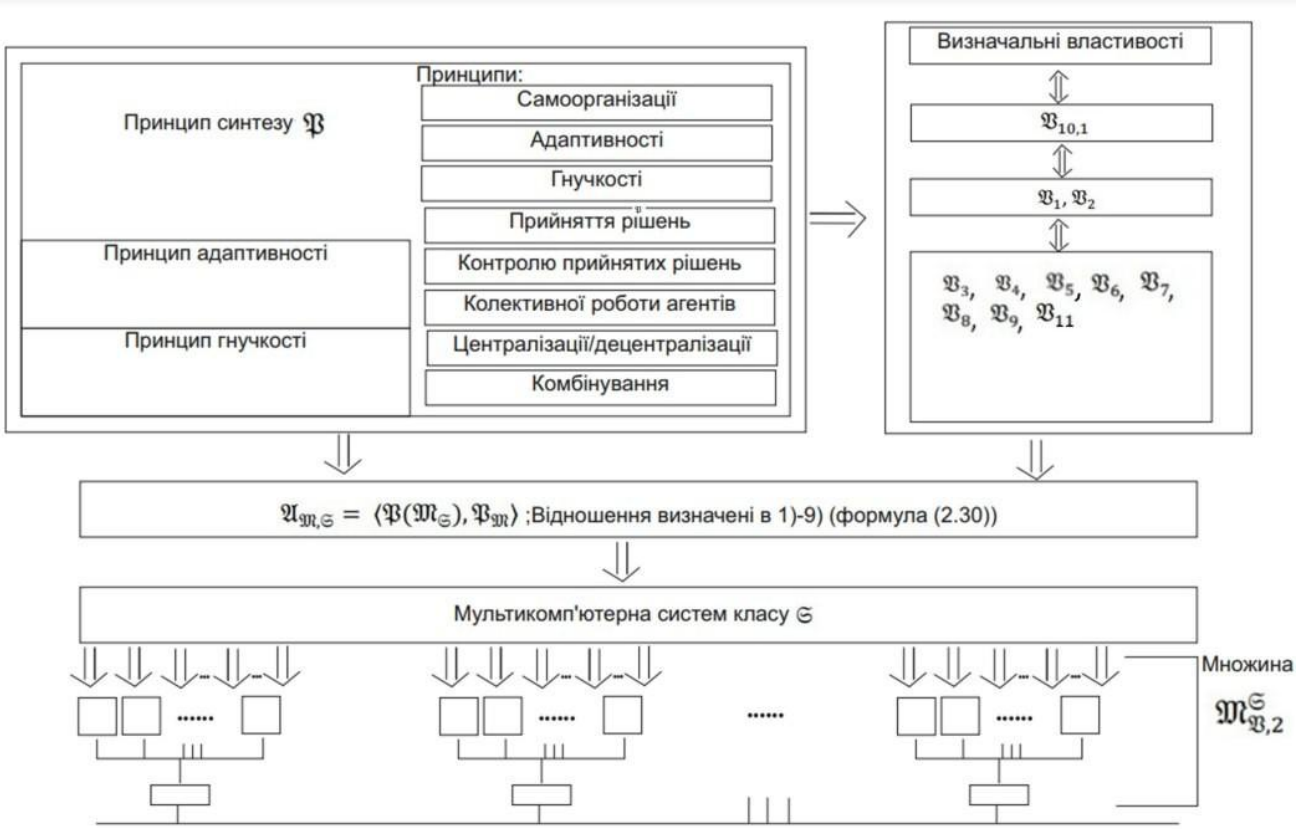


Рисунок 2.2 – Співвіднесення елементів та компонентів концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, мультикомп'ютерних систем класу $\mathfrak{S}$ та середовища функціонування систем

В концептуальній моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ мультикомп'ютерних систем класу $\mathfrak{S}$ визначено її основні елементи: умови функціонування системи, які визначені характером взаємодії між нею та її оточенням, а також між елементами системи; можливості керування системою та виділено склад керованих змінних системи. Крім того, метою дослідження систем класу $\mathfrak{S}$ для покращення їх функціонування та виконання поставлених завдань є покращення їх характеристик в частині безпосередньо архітектури та в частині спеціалізованого функціоналу, які повинні бути органічно поєднані в одне ціле.

На відміну від відомих моделей мультикомп’ютерних систем, що призначені для забезпечення функціонування за їх підтримки антивірусних приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, а також для попередження та протидії їх проникненню, в концептуальній моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ мультикомп’ютерних систем класу $\mathfrak{S}$ введено визначальну характеристику, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем класу $\mathfrak{S}$ повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі (рис. 2.1) відображення визначальних характеристик в архітектурі систем типу $\mathfrak{S}$, а також виділено спеціалізований функціонал, який сумісно з загальною частиною системи формує систему як єдиний сенсор. Визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень і виділена окремим елементом в концептуальній моделі, фактично задає властивість штучної свідомості з обмеженими можливостями, які визначені завданнями систем типу $\mathfrak{S}$. Це дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ. В результаті розуміння поведінки системи буде суттєво ускладнене. Решта визначальних характеристик дають змогу збільшити кількість варіантів архітектури та, відповідно, їх використання при перебудові систем типу $\mathfrak{S}$, що дає змогу не тільки урізноманітнити систему через її різну змінювану архітектуру, але й забезпечує її стійкість при вилученні певних вузлів в корпоративній мережі. Поєднання спеціалізованого функціоналу із загальною частиною системи формує систему як єдиний сенсор, що покращує ефективність протидії ЗПЗ та КА.

Важливою особливістю задання концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ мультикомп’ютерних систем класу $\mathfrak{S}$ згідно формули (2.30) є врахування в ній визначальних властивостей, що дають змогу формувати систему за певними принципами, тобто здійснювати фактично вертикальне її подання, та безпосередньо через подання систем у співвіднесенні до середовища їх функціонування в корпоративних мережах, тобто здійснюючи її горизонтальне подання. Такі два подання в моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ здійснено узгоджено. Таким чином, концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ адекватно відображає системи класу $\mathfrak{S}$ через визначальні властивості та середовище функціонування.

Таким чином, розроблена концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ мультикомп'ютерних систем класу $\mathfrak{S}$ містить необхідні елементи, що визначають моделі. Вона є абстрактною моделлю і відображає визначальні характеристики та особливості систем класу $\mathfrak{S}$ щодо середовища корпоративних мереж. Її особливими елементами є контролер прийнятих рішень, динамічний синтез архітектури згідно визначальних властивостей, поєднання спеціалізованого функціоналу з частиною системи в єдиний сенсор. Дана концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ є основою для розробки методу організації функціонування мультикомп'ютерних систем класу $\mathfrak{S}$ з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах, а також методу організації функціонування комбінованих антивірусних приманок і пасток та методів виявлення ЗПЗ та КА з використанням комбінованих антивірусних приманок і пасток, імплементованих в архітектуру таких систем для покращення виявлення. Відповідно ці методи та розроблена концептуальна модель будуть методологічною основою створення мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА.

2.4. Висновки до другого розділу

Запропонована концепція вирішення проблеми полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для покращення виявлення ЗПЗ та КА в корпоративних мережах, що базується на поєднанні таких виділених визначальних властивостей та їх синтезу в системах, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних приманок і пасток в системі. Визначальним елементом у цій концепції є необхідність синтезу в

мультикомп’ютерних системах зі спеціалізованим функціоналом контролера прийнятих рішень.

Розроблений принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА містить дві визначальні вимоги щодо наявності в архітектурі систем контролера та спеціалізованого функціоналу. Вони впливають на рішення системи щодо її наступних кроків та зміни архітектури. В результаті це ускладнить для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращити ефективність виявлення та протидії ЗПЗ і КА в корпоративних мережах. Цей принцип є основою розвитку елементів теорії та практики створення таких систем. Такий поділ архітектури систем за внутрішньою будовою дасть змогу визначити необхідні елементи та компоненти в архітектурі системи, яка міститиме контролер та спеціалізований функціонал, і є основою для розробки концепції та методологічних основ синтезу таких систем.

Розроблено концептуальну модель мультикомп’ютерних систем, в якій на відміну від відомих моделей мультикомп’ютерних систем, що призначені для забезпечення функціонування за їх підтримки антивірусних приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, а також для попередження та протидії їх проникненню, в концептуальній моделі мультикомп’ютерних систем введено визначальну характеристику, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, який сумісно з загальною частиною системи формує систему як єдиний сенсор, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також дає змогу не тільки урізноманітнити систему через її різну архітектуру, але й забезпечує її стійкість при вилученні певних вузлів в корпоративній мережі та при поєднанні

спеціалізованого функціоналу із загальною частиною системи формує систему як єдиний сенсор, що в цілому покращує ефективність протидії ЗПЗ та КА.

Згідно концептуальної моделі для забезпечення функціонування мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролера прийняття рішень для виявлення ЗПЗ та КА в корпоративних мережах потрібно розробити метод організації функціонування таких систем, а також метод організації функціонування комбінованих антивірусних приманок і пасток та методи виявлення ЗПЗ та КА з використанням комбінованих антивірусних приманок і пасток, імплементованих в архітектуру таких систем для покращення ефективності виявлення.

Основні результати розділу опубліковані у працях [11, 164, 165, 186, 201, 203, 228, 288, 289, 292, 295, 300, 308, 313].

РОЗДІЛ 3.
МАТЕМАТИЧНІ МОДЕЛІ КРИТЕРІЇВ ОЦІНЮВАННЯ ТА МЕТОД ВИЗНАЧЕННЯ НАСТУПНОГО ВАРІАНТУ ЦЕНТРАЛІЗАЦІЇ В МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМАХ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК І ПАСТОК

Архітектура мультикомп'ютерних систем антивірусних комбінованих приманок і пасток, яку синтезовано згідно їх визначальних характеристичних властивостей, потребує деталізації в частині організації внутрішніх складових частин таких систем та загальної організації для забезпечення ефективного функціонування таких систем. Кожна з включених визначальних характеристичних властивостей в архітектурі мультикомп'ютерних систем потребує розроблення функційного подання для забезпечення реалізації так і для поєднання з рештою визначальних властивостей. З цих визначальних властивостей особливе місце займають контролер та централізація. Вони першочергово впливають на функціонування таких систем через прийняття ними рішень. Тому, в контексті синтезу мультикомп'ютерних систем антивірусних комбінованих приманок і пасток розглянемо розроблення організації функціонування систем, роботу контролера прийняття рішень та забезпечення централізації в архітектурі систем.

3.1. Характерні властивості централізації в архітектурі мультикомп'ютерних систем антивірусних комбінованих приманок і пасток

При здійсненні синтезу мультикомп'ютерних систем антивірусних комбінованих приманок і пасток згідно різних характеристичних властивостей та принципів потрібно враховувати особливості централізації, тобто архітектуру та функційні можливості центрів таких систем. Покращення функціонування муьтикомп'ютерних систем антивірусних комбінованих приманок і пасток залежить від організації та особливостей функціонування центру в архітектурі таких систем, оскільки це впливає на комунікацію між вузлами. Вузли системи розподілені, тоді час на прийняття рішень та надсилання відповідних повідомлень є важливими

характеристиками. Крім того, приховування центру мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для уникнення його виявлення зловмисниками, які діють ззовні або з середини периметру корпоративної мережі, є важливою характеристикою та спроможністю систем класу $\mathfrak{S}$. Тому, потрібно на архітектурному рівні при синтезі систем класу $\mathfrak{S}$ забезпечити їх централізацію таким чином, щоб системи самостійно приховували свій центр, а також щоб забезпечувались ефективна взаємодія між їх вузлами і швидке прийняття рішень та підтримувалась цілісність системи в процесі експлуатації.

Серед визначальних властивостей для систем класу $\mathfrak{S}$ було виділено в формулі (2.30) таку властивість як $\mathfrak{V}_2$, яка характеризує типи та кількість центрів в архітектурі системи. В загальному випадку ця властивість щодо центру системи може буде реалізована так: цілісний центр в одній компоненті; центр поділений на рівнозначні частини в різних компонентах; центр поділений ієрархічно і міститься в різних компонентах; центр є цілісним, ієрархічним та міститься в різних компонентах. З використанням такої стратегії щодо синтезу центру в архітектурі систем класу $\mathfrak{S}$ можуть бути різні варіанти та варіації, які будуть основою при функціонуванні центру системи в поточний момент часу. Наприклад, центр систем класу $\mathfrak{S}$ в поточний момент часу може бути в одному вузлі, а далі протягом певного інтервалу часу вже бути розподілений в декількох компонентах системи у різних вузлах корпоративної мережі. Також, зловмисник з середини мережі може відімкнути обладнання і корпоративна розділиться на два або більше сегментів. Таку модель зловмисної поведінки потрібно враховувати при організації функціонування центру системи.

Для реалізації в архітектурі систем класу $\mathfrak{S}$ таких властивостей центру розподілимо на підмножини всі можливі варіанти та їх варіації, а також здійснимо дослідження центру на предмет відповідності його очікуваним результатам з ефективності його приховування, прийняття рішень, організації комунікації між компонентами системи в різних вузлах корпоративної мережі та забезпечення підтримки цілісності системи, враховуючи гнучкі переходи центру системи до різних варіантів.

Виділимо спочатку потенційні варіанти організації центру системи, а потім їх варіації. У системах з більше ніж однією компонентою, які розміщені у різних вузлах

корпоративної мережі, можна синтезувати в архітектурі системи центр чотирма різними варіантами: централізована архітектура; частково централізована архітектура; частково децентралізована архітектура; децентралізована архітектура. Позначимо ці варіанти в множині варіантів централізації так:

$$M_{\mathfrak{V}_2,centr,v_1} = \{m_{\mathfrak{V}_2,centr,v_1,1}, m_{\mathfrak{V}_2,centr,v_1.2}, m_{\mathfrak{V}_2,centr,v_1,3}, m_{\mathfrak{V}_2,centr,v_1,4}\}, \quad (3.1)$$

де елемент $m_{\mathfrak{V}_2,centr,v_1,1}$ відображає централізовану архітектуру систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_1.2}$ – частково централізовану архітектуру системи; $m_{\mathfrak{V}_2,centr,v_1,3}$ – частково децентралізовану архітектуру системи; $m_{\mathfrak{V}_2,centr,v_1,4}$ – децентралізовану архітектуру системи.

Наступним параметром, який потребує врахування, буде варіант з розподіленням центру системи між її компонентами в різних вузлах корпоративної мережі. Задамо його множиною $M_{\mathfrak{V}_2,centr,v_2}$ так:

$$M_{\mathfrak{V}_2,centr,v_2} = \{m_{\mathfrak{V}_2,centr,v_2,1}, m_{\mathfrak{V}_2,centr,v_2.2}\}, \quad (3.2)$$

де елемент $m_{\mathfrak{V}_2,centr,v_2,1}$ відображає поділ центру системи між компонентами в різних вузлах для систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_2.2}$ відображає неподільність центру системи між компонентами в різних вузлах для систем класу $\mathfrak{S}$, тобто перебування його в одній компоненті.

Для варіанту, який задано множиною за формулою (3.2), потрібно врахувати можливість тимчасового розділення системи на дві або декілька частин. Причини розділення можуть бути різними. Але їх потрібно врахувати. Бо при наявності центру в одній із частин після розділення системи, решта частин системи повинні підтримувати своє функціонування. Інакше після повернення до повноцінного функціонування системи в цілісному поданні, довіра до частин, які функціонували без центру системи буде знижена і потребуватимуть повного дослідження її компоненти та вузли корпоративної мережі. Також, можуть бути і інші причини, але всі вони за відсутності центру системи в її частинах, які відокремились, знижують довіру до результатів її роботи. Тому, параметром, який потребує врахування, буде варіант з розподіленням центру системи між її компонентами в різних вузлах корпоративної мережі при розподіленні її на незв'язні частини. Навіть для

централізованої архітектури систем класу $\mathfrak{S}$ при її розділенні на незв'язні частини вважатимемо, що центр системи буде в кожній з таких частин. Задамо такий варіант з наявністю центру системи в незв'язних частинах систем класу $\mathfrak{S}$ множиною $M_{\mathfrak{V}_2,centr,v_3}$ так:

$$M_{\mathfrak{V}_2,centr,v_3} = \{m_{\mathfrak{V}_2,centr,v_3,1}, m_{\mathfrak{V}_2,centr,v_3.2}\}, \quad (3.3)$$

де елемент $m_{\mathfrak{V}_2,centr,v_3,1}$ відображає наявність центру системи в незв'язних частинах систем класу $\mathfrak{S}$ після їх розділення; елемент $m_{\mathfrak{V}_2,centr,v_3.2}$ відображає наявність центру системи лише в одній з незв'язних частин систем класу $\mathfrak{S}$ після їх розділення, тобто в решті частин системи центр відсутній.

У варіантах з розділенням центру системи між компонентами у різних вузлах корпоративної мережі потрібно враховувати задані зв'язки між компонентами центру системи. Вони впливатимуть на швидкість прийняття рішень, бо будуть залежати від часу витраченого на обмін повідомленнями між собою. Ці зв'язки можуть бути встановлені між всіма компонентами, в яких буде міститись центр системи, а можуть бути задані лише частково, тобто не повністю і, відповідно, не формуватимуть відношення «всі до всіх». Між компонентами, в яких міститься центр системи, може бути організована ієрархічна підпорядкованість. Такі особливості в архітектурі центрів систем класу $\mathfrak{S}$ потрібно врахувати. Тому, задамо множиною $M_{\mathfrak{V}_2,centr,v_4}$ особливості зв'язків між компонентами при його розподілені між компонентами в різних вузлах корпоративної мережі так:

$$M_{\mathfrak{V}_2,centr,v_4} = \{m_{\mathfrak{V}_2,centr,v_4,1}, m_{\mathfrak{V}_2,centr,v_4.2}, \dots, m_{\mathfrak{V}_2,centr,v_4,n\ centr,v_4}\}, \quad (3.4)$$

де елемент $m_{\mathfrak{V}_2,centr,v_4,1}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно відношення «всі до всіх»; елемент $m_{\mathfrak{V}_2,centr,v_4.2}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно відношення «один до всіх» архітектуру систем класу $\mathfrak{S}$; $m_{\mathfrak{V}_2,centr,v_4,3}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно послідовної топології; $m_{\mathfrak{V}_2,centr,v_4,4}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «кільце»; $m_{\mathfrak{V}_2,centr,v_4,5}$

відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «решітка»; $m_{\mathfrak{B}_2,centr,v_4,6}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «тор»; $m_{\mathfrak{B}_2,centr,v_4,7}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «куб»; n_{centr,v_4} – кількість варіантів зв'язків між компонентами з центром системи архітектури систем класу $\mathfrak{S}$.

Введемо, також, множину $M_{\mathfrak{B}_2,centr,v_5}$, елементи якої будуть характеризувати ієрархію компонентів, що містять центр системи, або будуть вказувати на те, що всі компоненти з центром системи є рівнозначними. Рівнів ієрархії компонентів з центром системи може бути декілька і не обов'язково два, як їх мінімальна кількість. Тобто, частина елементів може бути на вищому рівні ієрархії, а частина на нижчому рівні ієрархії. Більша кількість рівнів ієрархії може передбачати встановлення певної топології для таких компонентів, а також визначення для компонентів центру системи з певних рівнів ієрархії заданої функційної спроможності в ієрархії прийняття рішення. Ієрархія для компонентів центру системи може і не стосуватись обмеженої функційної спроможності, а може бути введена лише для оптимізації зв'язків між компонентами. Задамо множину $M_{\mathfrak{B}_2,centr,v_5}$ переліком таких елементів:

$$M_{\mathfrak{B}_2,centr,v_5} = \left\{m_{\mathfrak{B}_2,centr,v_5,1}, m_{\mathfrak{B}_2,centr,v_5.2}, m_{\mathfrak{B}_2,centr,v_5.3}, \dots, m_{\mathfrak{B}_2,centr,v_5,n_{centr,v_5}}\right\}, \quad (3.5)$$

де елемент $m_{\mathfrak{B}_2,centr,v_5,1}$ відображає один рівень ієрархії, тобто фактично відображає відсутність ієрархічних рівнів; елемент $m_{\mathfrak{B}_2,centr,v_5,2}$ відображає два рівні ієрархії; елемент $m_{\mathfrak{B}_2,centr,v_5.3}$ відображає три рівні ієрархії між компонентами з центром системи архітектури систем класу $\mathfrak{S}$; $m_{\mathfrak{B}_2,centr,v_5,n_{centr,v_5}}$ відображає $n_{centr,v_5} - 1$ рівнів ієрархії між компонентами з центром системи архітектури систем класу $\mathfrak{S}$; n_{centr,v_5} – кількість елементів множини $M_{\mathfrak{B}_2,centr,v_5}$.

Напрям передачі повідомлень між компонентами систем згідно встановлених зв'язків може бути одностороннім, двостороннім або комбінованим. Тобто, передача повідомлень при організації комунікації між частинами центру системи може мати обмеження. Без обмежень буде двостороння комунікація. З обмеженнями буде односторонння комунікація, при якій повідомлення можуть переміщуватись за

встановленим маршрутом. Наприклад, якщо є перехід від однієї компоненти до другої, то зворотного переходу може не бути, а для того, щоб реалізувати передачу в зворотньому напрямі потрібно надсилати повідомлення за маршрутом, який преведе у вказану компоненту проходячи через певні компоненти. Аналогічно, для змішаної комунікації частина компонент буде забезпечена двосторонньою комунікацією, а частина односторонньою. Задамо множиною $M_{\mathfrak{V}_2,centr,v_6}$ варіанти передачі повідомлень з різними типами комунікації так:

$$M_{\mathfrak{V}_2,centr,v_6} = \{m_{\mathfrak{V}_2,centr,v_6,1}, m_{\mathfrak{V}_2,centr,v_6.2}, m_{\mathfrak{V}_2,centr,v_6,3}\}, \quad (3.6)$$

де елемент $m_{\mathfrak{V}_2,centr,v_6,1}$ відображає двосторонню комунікацію між компонентами; елемент $m_{\mathfrak{V}_2,centr,v_6.2}$ відображає односторонню комунікацію між компонентами; елемент $m_{\mathfrak{V}_2,centr,v_6.3}$ відображає змішану комунікацію між компонентами.

Дійсно, при різних варіантах в архітектурі систем з частковою централізацією переважатиме змішана комунікація між компонентами. У варіантах централізованої або децентралізованої архітектури, якщо не встановлено додаткових обмежень, переважатиме двостороння комунікація. Встановлення обмежень на здійснення комунікації між компонентами центру системи може бути необхідним, враховуючи специфіку завдань системи, потребу в заплутуванні зловмисників та приховуванні компонент центру системи.

Центр системи може бути в частині компонент, а не точно в усіх компонентах системи. Тобто, центр системи може бути розподіленим між певною частиною компонент, а в частині компонент його може не бути взагалі. Також, можливі варіанти, коли центр системи розподілено в усі компоненти. Задамо множиною $M_{\mathfrak{V}_2,centr,v_7}$ варіанти передачі повідомлень з різними типами комунікації так:

$$M_{\mathfrak{V}_2,centr,v_7} = \{m_{\mathfrak{V}_2,centr,v_7,1}, m_{\mathfrak{V}_2,centr,v_7.2}\}, \quad (3.7)$$

де елемент $m_{\mathfrak{V}_2,centr,v_7,1}$ відображає наявність розподілених частин центру системи в усіх компонентах систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_7.2}$ відображає наявність розподілених частин центру системи в певних компонентах систем класу $\mathfrak{S}$, тобто не в усіх компонентах.

Згідно множини, яку задано формулою (3.7), можуть бути варіації щодо перебування розподілених частин центру системи в компонентах в активному та неактивному станах. Введемо для визначення цих варіацій множину $M_{\mathfrak{V}_2,centr,v_8}$ так:

$$M_{\mathfrak{V}_2,centr,8} = \{m_{\mathfrak{V}_2,centr,v_8,1}, m_{\mathfrak{V}_2,centr,v_8.2}, m_{\mathfrak{V}_2,centr,v_8.3}\}, \quad (3.8)$$

де елемент $m_{\mathfrak{V}_2,centr,v_8,1}$ відображає наявність розподілених частин центру системи в компонентах, які для нього задані, винятково в активному стані; елемент $m_{\mathfrak{V}_2,centr,v_8.2}$ відображає наявність розподілених частин центру системи в компонентах, які для нього задані, в двох станах (активний стан, пасивний стан); елемент $m_{\mathfrak{V}_2,centr,v_8,3}$ відображає наявність всіх розподілених частин центру системи в компонентах, які для нього задані, винятково в пасивному стані.

Активний стан розподіленої частини центру системи в певній компоненті означає його функціонування в поточний момент часу. Пасивний стан розподіленої частини центру системи в певній компоненті означає його перебування в поточний момент часу в очікуванні вказівки про перехід до активного стану.

Центр системи може бути розподілений так, що в усіх компонентах системи, в яких передбачено його наявність, буде однаковий функціонал. Тобто, всі компоненти, в яких буде наявний функціонал центру системи, будуть мати однакові функціонали. Якщо центр системи біде характеризуватись елементом $m_{\mathfrak{V}_2,centr,v_5,1}$ з формули (3.5), то всі компоненти з центром системи будуть фактично формувати децентралізовану архітектуру центру системи. Але центр системи може не бути в контексті ієрархії згідно формули (3.5), а може мати розділення таким чином, що декілька основних функцій будуть в окремих компонентах і матимуть вищий пріоритет порівняно з рештою функцій, які будуть перебувати в решті компонент, в яких задано функціонал з центром системи. В цьому варіанті центр системи складається з функцій, які розподілено між різними компонентами, і частина з них або одна є основними чи основною. Таким чином, центр розподілений за його частинами. Також, може бути варіант розподілу центру системи таким чином, що частина компонент міститиме основні функції центру системи, а решта компонент, в яких задано центр системи, другорядні. При цьому варіанті частина компонент з основними функціями центру системи буде рівнозначною між собою. Це важливо у випадку розпаду системи на

декілька частин через розділення вузлів корпоративної мережі на певний інтервал часу. Тоді, буде збережено стійкість системи і вона зможе продовжити свою роботу. Введемо для визначення цих варіантів з розподіленням функцій центру системи множину $M_{\mathfrak{V}_2,centr,v_9}$ так:

$$M_{\mathfrak{V}_2,centr,9} = \{m_{\mathfrak{V}_2,centr,v_9,1}, m_{\mathfrak{V}_2,centr,v_9.2}, m_{\mathfrak{V}_2,centr,v_9.3}\}, \quad (3.9)$$

де елемент $m_{\mathfrak{V}_2,centr,v_9,1}$ відображає випадок, коли всі компоненти, в яких наявний функціонал центру системи, будуть мати однакові функціонали; елемент $m_{\mathfrak{V}_2,centr,v_9.2}$ відображає випадок, коли центр системи має розділення таким чином, що декілька основних функцій будуть в окремих компонентах і мають вищий пріоритет порівняно з рештою функцій, які перебувають в решті компонент, в яких задано функціонал з центром системи; елемент $m_{\mathfrak{V}_2,centr,v_9.3}$ відображає випадок, коли варіант розподілу центру системи такий, що частина компонент містить основні функції центру системи, а решта компонент, в яких задано центр системи, другорядні, і, при цьому варіанті частина компонент з основними функціями центру системи буде рівнозначною між собою.

Функціонал центру системи може бути сформовано таким чином, що він буде складатись з незалежних підсистем. Для їх запуску в різних вузлах корпоративної мережі можна використовувати процедуру віддаленого запуску. Тоді, такий функціонал розподіленої частини центру системи може міститись в різних компонентах, в який задано функціонал центру системи, і буде формуватись з різних незалежних підсистем різних компонент. Головною незалежною підсистемою буде та підсистема, яка при встановлені функціоналу центру системи визначена і закріплена за відповідною компонентою. Таку організацію функціоналу компоненти центру системи вважатимемо динамічною. Якщо ж функціонал компоненти центру системи складається з незалежних підсистем і всі вони встановлені в одну компоненту та запускаються в ній при виклику з головної підсистеми, то таку організацію функціоналу компоненти центру системи вважатимемо статичною. У випадку наявності одночасно двох варіантів з динамічною та статичною організацією функціоналу компоненти центру системи, тоді вважатимемо таку організацію змішаною. Для систем *класу* $\mathfrak{S}$ змішана організація може виникнути після повернення

системи до цілісної, якщо перед цим було розділення. Під час її розділення в одній частині могла бути задіяна модель із динамічною організацією, а в решті частин – модель з статичною організацією. Після об'єднання фактично стає змішана організація. Задамо ці випадки множиною $M_{\mathfrak{V}_2,centr,v_{10}}$ так:

$$M_{\mathfrak{V}_2,centr,10} = \{m_{\mathfrak{V}_2,centr,v_{10},1}, m_{\mathfrak{V}_2,centr,v_{10}.2}, m_{\mathfrak{V}_2,centr,v_{10}.3}\}, \quad (3.10)$$

де елемент $m_{\mathfrak{V}_2,centr,v_{10},1}$ відображає динамічну організацію *функціоналу розподіленої частини центру системи*; елемент $m_{\mathfrak{V}_2,centr,v_{10}.2}$ відображає статичну організацію *функціоналу розподіленої частини центру системи;* елемент $m_{\mathfrak{V}_2,centr,v_{10}.3}$ відображає змішану організацію функціоналу розподіленої частини центру системи.

Розглянемо введені множини та їх елементи згідно формул (3.1) - (3.10) в поєднанні для забезпечення централізації в системах класу $\mathfrak{S}$. Таке поєднання множин та їх елементів між собою забезпечить відображення особливостей центру системи за різновидами його архітектури, які необхідно використовувати при функціонуванні систем класу $\mathfrak{S}$ з метою приховування центру системи та заплутування зловмисників. Фактично, перебуваючи в одному із визначених центром системи можливих варіантів централізації, система перебуває в заданому стані, який характеризує її архітектуру в поточний момент часу. Протягом часу функціонування системи можуть самостійно змінювати варіанти централізації, переходячи при цьому до іншого стану.

Подамо в табл. 3.1 фрагмент варіантів централізації з особливостями, які відображені елементами в формулах (3.1) - (3.10).

Таблиця 3.1

Фрагмент варіантів централізації в архітектурі систем

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	$M_{\mathfrak{V}_2,centr,v_1}$				$M_{\mathfrak{V}_2,centr,v_2}$		$M_{\mathfrak{V}_2,centr,v_3}$		$M_{\mathfrak{V}_2,centr,v_4}$				$M_{\mathfrak{V}_2,centr,v_5}$					$M_{\mathfrak{V}_2,centr,v_6}$			$M_{\mathfrak{V}_2,centr,v_7}$		$M_{\mathfrak{V}_2,centr,8}$			$M_{\mathfrak{V}_2,centr,9}$			$M_{\mathfrak{V}_2,centr,10}$		
	$m_{\mathfrak{V}_2,centr,v_1,1}$	$m_{\mathfrak{V}_2,centr,v_1.2}$	$m_{\mathfrak{V}_2,centr,v_1.3}$	$m_{\mathfrak{V}_2,centr,v_1.4}$	$m_{\mathfrak{V}_2,centr,v_2,1}$	$m_{\mathfrak{V}_2,centr,v_2.2}$	$m_{\mathfrak{V}_2,centr,v_3,1}$	$m_{\mathfrak{V}_2,centr,v_3.2}$	$m_{\mathfrak{V}_2,centr,v_4,1}$	$m_{\mathfrak{V}_2,centr,v_4.2}$	...	$m_{\mathfrak{V}_2,centr,v_4,n\ centr,v_4}$	$m_{\mathfrak{V}_2,centr,v_5,1}$	$m_{\mathfrak{V}_2,centr,v_5.2}$	$m_{\mathfrak{V}_2,centr,v_5.3}$	...	$m_{\mathfrak{V}_2,centr,v_5,n\ centr,v_5}$	$m_{\mathfrak{V}_2,centr,v_6,1}$	$m_{\mathfrak{V}_2,centr,v_6.2}$	$m_{\mathfrak{V}_2,centr,v_6.3}$	$m_{\mathfrak{V}_2,centr,v_7,1}$	$m_{\mathfrak{V}_2,centr,v_7.2}$	$m_{\mathfrak{V}_2,centr,v_8,1}$	$m_{\mathfrak{V}_2,centr,v_8.2}$	$m_{\mathfrak{V}_2,centr,v_8.3}$	$m_{\mathfrak{V}_2,centr,v_9,1}$	$m_{\mathfrak{V}_2,centr,v_9.2}$	$m_{\mathfrak{V}_2,centr,v_9.3}$	$m_{\mathfrak{V}_2,centr,v_{10},1}$	$m_{\mathfrak{V}_2,centr,v_{10}.2}$	$m_{\mathfrak{V}_2,centr,v_{10}.3}$
1	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
2	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
3	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
4	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
5	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	1	0	0	1	0	0
6	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
7	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
8	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
9	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
10	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	1	0	0
11	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	1	0	0
12	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	1	1	0	1	0	0	1	0	0	1	0	0

Таким чином, здійснено подання характерних властивостей варіантів централізації в системах класу $\mathfrak{S}$ множинами, які задано за формулами (3.1) - (3.10), та встановлено кількість можливих варіантів. Отриманий результат щодо кількості варіантів відображає потенційну складність при здійсненні вибору наступного варіанту централізації. Розроблене подання через характерні властивості необхідне для формування правил визначення наступного варіанту централізації в архітектурі систем *класу* $\mathfrak{S}$, враховуючи потенційно велику кількість можливих варіантів.

3.2. Особливості правил формування варіантів централізації для мультикомп'ютерних систем

Кількість варіантів централізації в архітектурі мультикомп'ютерних систем з врахуванням особливостей, які відображені елементами в формулах (3.1) - (3.10), дорівнює 231 і більше. Кількість особливостей можна збільшити до певного числа $N_{centr,var}$, збільшивши кількість елементів за рахунок деталізації елементів з формул (3.1) - (3.10), тоді кількість варіантів централізації буде дорівнювати $2^{N_{centr,var}}$. Ця кількість варіантів є достатньо великою і не може зберігатись безпосередньо системою у вигляді таблиці з усіма значеннями. Її формування на початку встановлення та організації роботи мультикомп'ютерних систем вимагатиме певного часу. При користуванні такою готовою таблицею, незалежно від програмної реалізації, центр системи витрачатиме час на пошук варіанту. Тому, через витрати часу такий спосіб не є ефективним. Використаємо для подання варіантів централізації в архітектурі мультикомп'ютерних систем з врахуванням особливостей правила.

Перебування мультикомп'ютерних систем в одному з варіантів централізації в поточний момент часу будемо визначати їх перебуванням у визначеному відповідному стані. Таким чином, перехід від одного варіанту централізації в процесі функціонування мультикомп'ютерних систем буде означати перехід між станами. Перебування в певному стані мультикомп'ютерних систем не обов'язково дозволяє здійснити перехід до будь-якого із решти станів. Наприклад, якщо система розподілилась на дві, тоді перехід до варіанту централізації з одним центром є неможливим.

Після встановлення компонентів мультикомп’ютерних систем в корпоративних мережах виникає питання формування варіанту централізації. Такий варіант централізації міг би бути заданий адміністратором системи, який встановлював її компоненти та здійснював перший запуск. Але для уникнення можливого зловмисного впливу адміністратора на систему потрібно забезпечити самостійне визначення системою варіанту централізації. Також, початок функціонування системи, який розпочинається щоденно із увімкнення комп’ютерних станцій з компонентами системи теж потребує зміни варіанту централізації порівняно з попереднім днем функціонування. Наприклад, в попередній день функціонування система завершила роботу в одному із станів, а наступного дня продовження роботи в тому стані неможливе. Для однозначного визначення варіантів централізації потрібна гнучка організація функціонування цієї підсистеми, яку можна забезпечити, наприклад, задавши певну множину правил.

Таким чином, потрібно задати множину правил для визначення варіанту централізації систем на етапі початкового першого запуску системи, щоденного запуску системи та в процесі тривалого функціонування системи, до якого не відносяться події періодичного щоденного запуску системи.

Варіантів централізації, які підготовлені відповідною підсистемою системи, повинно бути декілька. Це пов’язано з тим, що контролер системи повинен оцінити ці варіанти в контексті фактично переходу зі стану в стан системи з врахуванням попереднього досвіду і затвердити один з таких варіантів. Тому, підготовка декількох варіантів централізації для наступного стану системи додає складності в підсистему, яка відповідає за підготовку таких варіантів.

Система може не використати певну велику кількість варіантів, але вона повинна мати можливість формувати будь-який з варіантів централізації. Частина варіантів за час її функціонування не буде не тільки обрана, але й розглянута. Варіантів централізації багато. Але ставити обмеження на певні варіанти централізації не потрібно, бо це може спростити доступ до системи для зловмисників. Тому, кількість можливих варіантів централізації має бути максимально можливою з допустимих варіантів.

Задамо правила формування варіантів централізації для мультикомп'ютерних систем множиною правил:

$$M_{Pr} = \left\{m_{Pr,1}, m_{Pr,2}, \dots, m_{Pr,N_{M_{Pr}}}\right\}, \quad (3.11)$$

де $m_{Pr,i}$ – i-те правило вибору варіанту централізації в мультикомп'ютерних системах; $i = 1,2, \dots, N_{M_{Pr}}$; $N_{M_{Pr}}$ – кількість правил в множині правил M_{Pr}.

Правила, які задані множиною M_{Pr}, будуть визначати умови, при виконанні яких перехід із стану в стан буде дозволений. За відсутності набору правил, які можуть бути виконані, перехід зі стану в стан буде заборонений. Це необхідно в контексті того, що не з усіх станів можна перейти в усі стани. Наприклад, якщо в системі був варіант централізації з єдиним центром без поділу компонентів на декілька незв'язних підмножин, тоді вона не може перейти до варіанту централізації, який може бути для двох підмножин компонентів, що були сформовані в результаті вимикання певного обладнання в комп'ютерній мережі. Цей випадок, також, може бути віднесений до аварійних і, тому, перехід до нього не може бути детермінований, а потребує окремого опрацювання. Також, варіантами централізації в системі, в які не можна перейти із наведеного прикладу з одним центром системи, можуть бути варіанти з ієрархією, якщо не всі комп'ютерні станції, в яких знаходяться компоненти системи, увімкнені. Або, якщо частково централізована архітектура системи в поточний момент часу повинна змінитись на частково децентралізовану архітектуру і при цьому тільки незначна частина компонент систем функціонує, бо решта перебуває в неувімкнених комп'ютерних станціях. І тоді, щоб перейти до частково децентралізованої архітектури в системі треба спочатку здійснити перехід до повністю децентралізованої архітектури, а потім вже з неї може бути забезпечений перехід до частково децентралізованої архітектури з врахуванням і використанням наявних в системі компонент в увімкнених комп'ютерних станціях. Тобто, такий перехід можливий лише за умови наявності проміжного перехідного стану системи, після якого можливий перехід до вказаного стану, який визначено частково децентралізованою архітектурою. Таким чином, на переходи між станами системи в контексті централізації впливатиме наявність компонент системи в увімкнених комп'ютерних станціях. Якщо всі комп'ютерні станції увімкнені, тоді спроможності

в системі для переходів зі стану до будь-якого стану збільшуються. Якщо ж не всі комп'ютерні станції увімкнені, тоді кількість можливих варіантів станів в контексті централізації зменшується. В зв'язку з цим потрібно формувати правила, також, з врахуванням повноти системи в контексті її компонентів. Такі правила, тоді, вимагатимуть динамічного формування. Важливим показником в контексті забезпечення переходу зі стану до стану в підсистемі забезпечення централізації є час. Оцінювання його для забезпечення переходів є необхідним, оскільки при виборі варіантів для переходу цей показник повинен враховуватись сукупно з показником повноти системи в контексті наявних компонент.

При переході зі стану до стану, коли контролер вже вибрав варіант централізації, може виникнути проблема, що завершити цю дію повністю вже неможливо через зміну конфігурування системи наявними компонентами. Наприклад, частина комп'ютерних станцій з компонентами вимкнена, а частина увімкнена. І, при цьому, система не може вже повернутись до попереднього стану через ці ж проблеми. Тоді, потрібні правила для встановлення варіанту централізації в системі.

Таким чином, для забезпечення переходів від одного стану централізації до іншого сформуємо правила, з яких частина правил буде динамічно формуватись на основі простіших правил. Врахуємо в процесі вибору чи формування правил показник часу на перехід від стану до стану та показник повноти системи в контексті наявних компонент в увімкнених комп'ютерних станціях. Також, сформуємо частину правил, які будуть використовуватись системою для вирішення питання централізації за умови неможливості завершити перехід до наступного стану і повернутись до переднього стану. Крім того, в результаті опрацювання всіх вхідних даних для здійснення зміни варіанту централізації система може прийняти рішення про те, щоб залишитись в поточному стані.

Стан системи в поточний момент часу задамо вектором $V_{Pr,i}$ ($i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – кількість станів системи). Згідно табл. 3.1 число $N_{V_{Pr}} \geq 2^{31}$. Значення елементів множин з формул (3.1) – (3.10) задамо елементами множини $\{0; 1\}$. Тоді, введемо булеву функцію для відображення активності/неактивності ознаки, яку задано елементом множин з формул (3.1)-(3.10), так:

$$F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,m}, i\right) = \begin{cases} 0, якщо\ елемент\ відсутній; \\ 1, якщо\ елемент\ присутній, \end{cases} \quad (3.12)$$

де l – кількість множин; $l = 1,2, \dots 10$; m – ий елемент в множині $M_{\mathfrak{B}_2,centr,l}$; i – номер стану системи.

Таким чином, вектор $V_{Pr,i}$ ($i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – кількість станів системи) визначимо його координатами так:

$$V_{Pr,i} = \left(F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, i\right), F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, i\right), \dots, F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, i\right)\right), \quad (3.13)$$

де $i = 1,2, \dots, N_{V_{Pr}}$; $N_{V_{Pr}}$ – кількість станів системи; i – номер стану системи.

Тоді, матрицю $M_{V_{Pr}}$ станів системи в частині організації централізації задамо так:

$$M_{V_{Pr}} = \begin{pmatrix} V_{Pr,1} \\ V_{Pr,2} \\ \dots \\ V_{Pr,N_{V_{Pr}}} \end{pmatrix}, \quad (3.14)$$

де $N_{V_{Pr}}$ – кількість станів системи; $V_{Pr,i}$ – вектор, який задає стан системи в поточний момент часу; $i = 1,2, \dots, N_{V_{Pr}}$.

При деталізації випадків та відповідно збільшення елементів множин кількість станів системи *в частині організації централізації, які відображено в матриці* $M_{V_{Pr}}$, може бути збільшена, або при зменшенні елементів - зменшена.

Перехід від стану до стану, який визначатиметься правилами з множини правил M_{Pr} задамо функцією $F^{M_{Pr}}$ так:

$$F^{M_{Pr}}: \left(V_{Pr,potochn}, M_{V_{Pr}}, M_{Pr}, P_{Pr}\right) \to V_{Pr,nast}, \quad (3.15)$$

де $V_{Pr,potochn}$ – вектор, який задає стан системи в поточний момент часу і наявний в матриці станів $M_{V_{Pr}}$; $M_{V_{Pr}}$ – матриця станів системи в частині організації централізації; M_{Pr} – множина правил; $V_{Pr,nast}$ – вектор, який задає наступний стан системи в поточний момент часу; P_{Pr} – множина показників, які характеризують поточний стан системи та процеси в ній.

Множину P_{Pr} задамо її елементами так:

$$P_{Pr} = \left\{p_{Pr,1}, p_{Pr,2}, \dots, p_{Pr,N_{P_{Pr}}}\right\}, \quad (3.16)$$

де $p_{Pr,i}$ – i - тий показник, *що характеризує поточний стан системи та процеси в ній;* $i = 1,2, \dots, \mathrm{N}_{P_{Pr}}$; $\mathrm{N}_{P_{Pr}}$ – кількість показників, які характеризують поточний стан системи та процеси в ній і впливають на зміну варіанту централізації в системі.

Нехай $p_{Pr,1}$ – час на вибір варіанту централізації в системі та перехід з одного стану до іншого стану при зміні централізації, $p_{Pr,2}$ – показник наявних компонент в увімкнених комп'ютерних станціях, $p_{Pr,3}$ - показник неможливості завершити перехід до наступного стану і повернутись до переднього стану; $p_{Pr,4}$ – показник перебування системи в аварійному стані тощо. Аварійним станом є стан, який виникає в системі, коли вимикається певне обладнання і компоненти системи поділяються на декілька незв'язних підмножин. Тоді, для кожної з утворених підсистем вибирається варіант централізації. При цьому в кожній з підсистем можуть бути різні варіанти централізації. При поверненні з такого стану системі потрібно враховувати, також, попередній стан, в якому вона перебувала до потрапляння в аварійний стан. Взагалі для такого класу систем обов'язково потрібне зберігання протягом всього часу їх експлуатації інформації про всі вибрані стани, показники та застосовувані правила при виборі варіантів централізації. Наприклад, з певного стану до іншого можна перейти за наявності певної кількості компонент системи в увімкнених комп'ютерних станціях, але при іншій кількості компонент перехід до цього стану може бути неможливим і буде перехід до іншого стану.

Згідно формули (3.15) перехід до наступного стану може бути в різних часових проміжках функціонування системи з використанням різних правил з множини правил M_{Pr} і при різних показниках з множини показників P_{Pr}, які характеризують поточний стан системи та процеси в ній.

Розділимо правила з *множини правил* M_{Pr} (формула (3.11)) на групи, в які будуть віднесені правила з певними спільними ознаками. Виділимо такі спільні ознаки для поділу правил на групи:

1) перехід з певного стану до наступного обраного стану;

2) перехід до певного стану в результаті аварійної ситуації та повернення до штатного режиму роботи системи;

3) формування нових правил системою з використанням наявних в множині правил та їх використання при переході системи з певного стану до наступного обраного стану.

Введемо матрицю M_{Pr}^1 для зберігання інформації про тип правила, тобто до якої групи воно відноситься, час застосування правила за умови виконання згідно нього переходу, номер правила з множини правил M_{Pr}. Задамо матрицю M_{Pr}^1 так:

$$M_{Pr}^1 = \begin{pmatrix} m_{Pr,1}^1 & m_{Pr,2}^1 & \dots & m_{Pr,N_{M_{Pr}^1}}^1 \\ t_{Pr,1}^1 & t_{Pr,2}^1 & \dots & t_{Pr,N_{M_{Pr}^1}}^1 \\ N_{M_{Pr},1} & N_{M_{Pr},2} & \dots & N_{M_{Pr},N_{M_{Pr}^1}} \end{pmatrix}, \quad (3.17)$$

де $N_{M_{Pr}^1}$ – кількість успішно завершених переходів між станами системи; $i = 1,2,\dots,N_{M_{Pr}^1}$; $m_{Pr,i}^1$ – номер групи правила для i – того переходу; $t_{Pr,i}^1$ – поточний час для завершеного i – того переходу; $N_{M_{Pr},i}$ – номер елементу з множини правил на i – тому переході.

Цією матрицею M_{Pr}^1 задано інформацію про попередні стани системи при організації переходів, а також про використовувані правила та час повного завершення переходів. Така інформація потрібна системі для прийняття рішень щодо наступного варіанту централізації та у випадку виникнення аварійних ситуацій.

Для забезпечення виходу із нестандартних або аварійних ситуацій потрібні окремі правила. Якщо виникла аварійна або нестандартна для системи ситуація, тоді незв'язні частини системи приймають рішення про варіант централізації в частинах, а при подальшому переході до штатного режиму роботи системи варіант централізації визначається теж за окремими правилами. Також, наприклад, може бути ситуація переходу до певного стану, коли система не змогла завершити відповідні дії, а повернутись до попереднього стану вже неможливо в результаті аварійної чи нестандартної ситуації, яка може бути зумовлена зміною в архітектурі системи. Тоді, повернення до штатного режиму роботи системи потребує правил, які б забезпечували встановлення варіанту централізації за наявних умов. Тому, при функціонуванні системи множина правил має бути поділена на групи правил, які можуть бути застосовані лише за визначених умов.

До третьої групи правил віднесемо правила, які формуються самою системою з використанням простіших правил, тобто конструюються нею для вибору наступного варіанту централізації. Така група правил вноситься до множини правил самою системою. Потреба у формуванні такої групи правил виникає в процесі функціонування системи, коли запропоновані з першої групи правил варіанти централізації є повторюваними або їх кількість не задовольняє вимоги контролера. Тоді, система за загальним перебором формує нові правила і, якщо їх приймає контролер, то вони включаються в множину правил до третьої групи.

Перша група правил формує не тільки правила переходу з одного стану до іншого стану в штатному режимі роботи, встановлюючи при такій дії інший варіант централізації в системі. Тобто, правила першої групи задають не тільки просту комбінацію можливих варіантів елементів множин, які задано формулами (3.1)-(3.10). Серед правил першої групи повинні бути правила, які відхиляють варіанти централізації в системі, які є неможливими. Наприклад, якщо варіант централізації в системі передбачає централізацію, тоді він не може поєднуватись з варіантом, в якому передбачено поділ на декілька незв'язних підмножин множини компонентів системи. Або, наприклад, якщо система частково децентралізована, тоді неможливим є варіант з великою кількістю рівнів ієрархії в ній. Таким чином, в штатному режимі роботи системи правила формують новий варіант централізації в системі не простим перебором всіх можливих варіантів, а з урахуванням неможливості поєднання певних властивостей, які задано елементами множин.

Поділ правил на три групи відображає особливості їх застосування в поточний момент часу функціонування системи з врахуванням подій, які відбуваються в системі при виконанні нею завдань, зокрема і зміни варіанту централізації.

3.3. Типи централізації в архітектурі мультикомп'ютерних систем

Для формування правил деталізуємо особливості чотирьох основних варіантів централізації. Здійснимо задання систем класу $\mathfrak{S}$ їх компонентами так;

$$A^{\mathfrak{S}} = \left\{A_1^{\mathfrak{S},\mathrm{k}}, A_2^{\mathfrak{S},\mathrm{k}}, \dots, A_{N_{A^{\mathfrak{S}}}}^{\mathfrak{S},\mathrm{k}}\right\}, \tag{3.18}$$

де $A^{\mathfrak{S}}$ – позначення системи класу $\mathfrak{S}$; $A_i^{\mathfrak{S},\mathrm{k}}$ - i-та компонента системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$; $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $N_{A^{\mathfrak{S}}}$ – кількість компонентів в системі $A^{\mathfrak{S}}$.

Враховуючи необхідність у поданні варіантів централізації в системі розподілимо компоненти системи $A^{\mathfrak{S}}$ на дві підмножини. До першої підмножини віднесемо компоненти, які в поточний момент часу є активними компонентами центру системи. До другої підмножини віднесемо компоненти, які в поточний момент часу не є компонентами центру системи. Вважатимемо, що будь-які компоненти системи $A^{\mathfrak{S}}$ можуть бути активними компонентами центру, якщо вони перебувають в увімкнених комп'ютерних станціях. Активними компонентами вважатимемо компоненти, які функціонують в складі системи в поточний момент часу. Допускатимемо, що компоненти системи $A^{\mathfrak{S}}$ можуть бути активними, але вони не обов'язково в поточний момент часу можуть належати центру системи. Тоді, задамо множину компонентів системи $A^{\mathfrak{S}}$ так:

$$A^{\mathfrak{S}} = A_1^{\mathfrak{S}} \cup A_2^{\mathfrak{S}}, \tag{3.19}$$

де $A_1^{\mathfrak{S}}$ – підмножина активних компонент центру системи; $A_2^{\mathfrak{S}}$ – множина компонент системи, які в поточний момент часу не є компонентами центру системи.

Задамо ці дві підмножини елементами так:

$$A_1^{\mathfrak{S}} = \left\{A_{1,1}^{\mathfrak{S},\mathrm{k}}, A_{1,2}^{\mathfrak{S},\mathrm{k}}, \dots, A_{1,N_{1,A^{\mathfrak{S}}}}^{\mathfrak{S},\mathrm{k}}\right\}; \tag{3.20}$$

$$A_2^{\mathfrak{S}} = \left\{A_{2,1}^{\mathfrak{S},\mathrm{k}}, A_{2,2}^{\mathfrak{S},\mathrm{k}}, \dots, A_{2,N_{2,A^{\mathfrak{S}}}}^{\mathfrak{S},\mathrm{k}}\right\},$$

де $A_{1,i}^{\mathfrak{S},\mathrm{k}}$ - i-та компонента підмножини $A_1^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$; $i = 1,2,\dots,N_{1,A^{\mathfrak{S}}}$; $N_{1,A^{\mathfrak{S}}}$ – кількість елементів в підмножині $A_1^{\mathfrak{S}}$; $A_{2,j}^{\mathfrak{S},\mathrm{k}}$ - j-та компонента підмножини $A_2^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$; $j = 1,2,\dots,N_{2,A^{\mathfrak{S}}}$; $N_{2,A^{\mathfrak{S}}}$ – кількість елементів в підмножині $A_2^{\mathfrak{S}}$; $N_{A^{\mathfrak{S}}} = N_{1,A^{\mathfrak{S}}} + N_{2,A^{\mathfrak{S}}}$.

З урахуванням введених множин та підмножин згідно формул (3.18) - (3.20) задамо модель $M_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$ так:

$$M_{A^{\mathfrak{S}}}^{\mathfrak{S}} = \left(A_1^{\mathfrak{S}}, A_2^{\mathfrak{S}}, \mathrm{G}_{A^{\mathfrak{S}}}^{\mathfrak{S}}\right), \tag{3.21}$$

де $G_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ – граф, в якому вершинами є компоненти системи $A^{\mathfrak{S}}$.

В моделі $M_{A^{\mathfrak{S}}}^{\mathfrak{S}}$, яку задано формулою (3.21) розділено елементи підмножин $A_1^{\mathfrak{S}}$ та $A_2^{\mathfrak{S}}$, що відповідає поділу компонент центру системи і компонент, які не відносяться до компонент з центром системи в поточний момент функціонування системи. Підмножини $A_1^{\mathfrak{S}}$ та $A_2^{\mathfrak{S}}$ в певні поточні моменти часу можуть бути порожніми обидві одночасно або одна з них. Крім того, компоненти системи $A^{\mathfrak{S}}$, які були задані для її формування і які в поточний момент часу перебувають у вимкнених комп'ютерних станціях, не приймають участі в функціонуванні системи, тому їх не розглядатимемо в контексті завдання формування варіанту централізації.

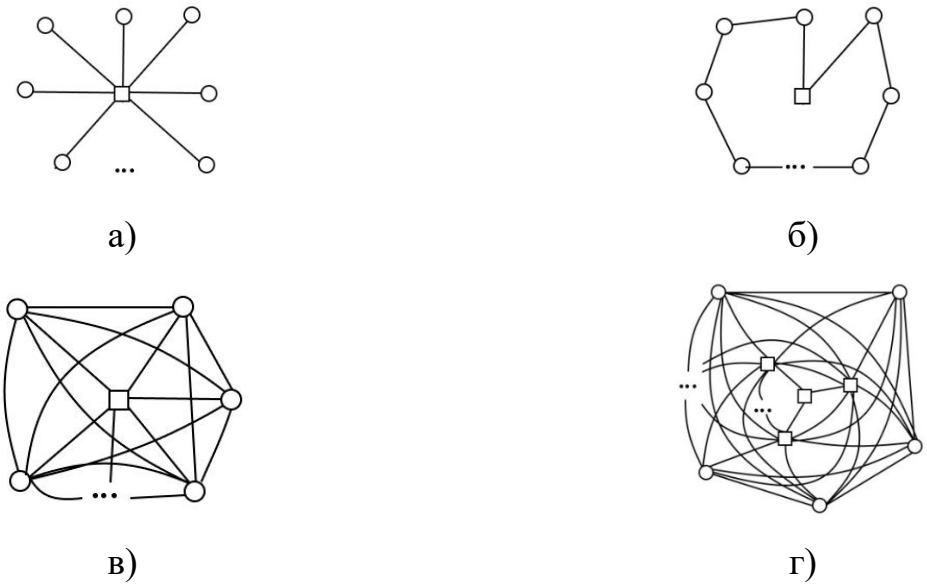
Задамо граф $G_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ так, щоб ним відображалась топологія системи та централізація в ній.

Розглянемо варіант формування централізації в системі за наявності елементу $m_{\mathfrak{V}_2,centr,v_1,1}$ (формула (3.1)), який відображає централізовану архітектуру систем класу $\mathfrak{S}$. Тоді, граф $G_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ зобразимо на рис. 3.1 з урахуванням ієрархії та без ієрархії серед компонент центру, розподілення центру між компонентами та його цілісність, компонент центру, різні відношення компонентів між собою при встановлення зв'язку між ними і центру зокрема тощо. На рисунках вершини графа для компонент з центром системи позначимо квадратами, вершини для компонент без центру системи – колами.

Зображені на рис. 3.1 а)-г) чотири варіанти саме централізованої архітектури системи не є усіма можливими варіантами, які задані формулами (3.1)-(3.10), а лише зображають частину основних з них і є необхідними для забезпечення розмежування цієї централізованої архітектури від решти варіантів централізації з можливою архітектурою в системах, які задані елементами $m_{\mathfrak{V}_2,centr,v_1.2}$, $m_{\mathfrak{V}_2,centr,v_1,3}$, $m_{\mathfrak{V}_2,centr,v_1,4}$ *з множини* $M_{\mathfrak{V}_2,centr,v_1}$.

Але такі варіанти централізації не збіжні з варіантом часткової централізації, бо при ній центр системи не тільки перебуває в декількох компонентах, але й навіть при його поділі між компонентами напрацьовує єдине рішення або певну кількість варіантів рішень. У варіанті ж часткової централізації в системі центр системи буде функціонувати в декількох компонентах і не в одній компоненті. Компоненти

системи з центром будуть напрацьовувати рішення в кожній з активних компонент центру системи, а далі сумісно визначатимуть один або більше варіантів рішень згідно принципу децентралізації. Тобто при прийнятті остаточного рішення всі компоненти з центром системи будуть функціонувати як децентралізована система. Напрацьовані рішення центром системи будуть обов'язковими для виконання призначеним компонентам. Часткова централізація в системі A^{Θ} може бути організована в ієрархічно сформованих компонентах центру системи. Це може бути при поділі функцій центру компоненти між декількома компонентами, але при цьому таких компонент центру, для яких функції поділені між декількома компонентами, є не менше двох. Таким чином, навіть при поділі функцій компоненти центру рішень, які напрацьовані в цих компонентах, буде не менше двох. На рис. 3.2 зображено варіанти частково централізованих розподілених систем.

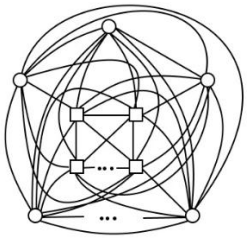


а) б)

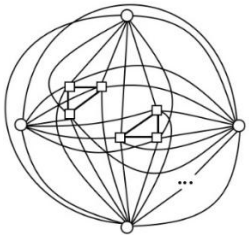
в) г)

Рисунок 3.1 - Варіанти централізованої архітектури в системі A^{Θ}:

а) центр в одній компоненті, зв'язок компонентів системи тільки винятково з одним центром, топологія «зірка»; б) центр в одній компоненті, зв'язок компонентів системи тільки винятково з сусідніми компонентами, топологія «кільце»; в) центр в одній компоненті, зв'язок компонентів системи з одним центром та між собою; г) центр розподілений в декількох компонентах, компоненти з центром містяться на двох рівнях ієрархії, зв'язок компонентів системи тільки з компонентами з центром другого рівня ієрархії



а)



б)

Рисунок 3.2 - Варіанти частково централізованих розподілених систем:
а) в кожній компоненті знаходяться і виконуються всі функції центру системи;
б) функції центру системи компоненти розподілені між декількома компонентами

Для варіанту з елементом $m_{\mathfrak{V}_2,centr,v_1,3}$ множини $M_{\mathfrak{V}_2,centr,v_1}$ (формула (3.1)) отримуємо частково децентралізовану архітектуру системи $A^{\mathfrak{S}}$. Її особливість полягає в тому, що частина компонентів системи відносяться до системи, в якій децентралізована архітектура, і рішення в них напрацьовуються за принципом децентралізації. Ці компоненти вважатимемо основними компонентами системи. Решта компонент системи, які не відносяться до основних компонент системи, пов'язані з окремими основними компонентами та для них рішення та команди надсилаються із з'єднаними з ними основних компонент. Зв'язки таких неосновних компонент з рештою компонент системи, крім однієї основної компоненти, відсутні. На рис. 3.3 зображено варіант системи з частково децентралізованою архітектурою.

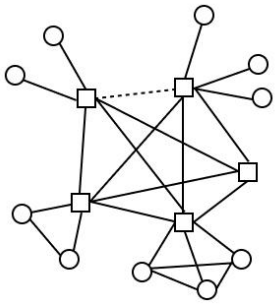
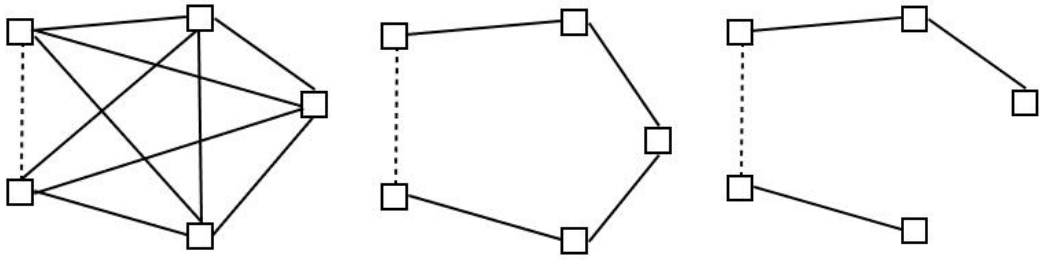


Рисунок 3.3 - Варіант частково децентралізованої розподіленої системи

Варіант системи $A^{\mathfrak{S}}$ з елементом $m_{\mathfrak{V}_2,centr,v_1,4}$ відображає децентралізовану архітектуру. Характерними особливостями систем з такою архітектурою є рівнозначність кожної компоненти як центру системи. Особливими випадками для децентралізованої архітектури зв'язки між всіма компонентами або частиною з них, встановлення ієрархії при поділі функцій центру системи між декількома

компонентами тощо. На рис. 3.4 зображено варіанти системи $A^{\mathfrak{S}}$ з децентралізованою архітектурою.

Аналогічно до рис. 3.1 граф $\mathrm{G}_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ задано на рис. 3.2 – 3.4. Тому, модель задана формулою (3.21) конкретизована на рівні множин та графа зв'язків між елементами множин, які позначено двома типами вершин. Базуючись на моделі поданій так, дослідимо ефективність системи для чотирьох випадків, які формуються елементами множини $\mathrm{M}_{\mathfrak{B}_2,\mathrm{centr},\mathrm{v}_1}$ (формула (3.1)).



а) б) с)

Рисунок 3.4 - Варіанти частково централізованих розподілених систем:
а) всі компоненти є однаковими і між ними встановлено відношення «всі до всіх»;
б) всі компоненти є однаковими і зв'язки між ними встановлені згідно топології «кільце»; с) всі компоненти є однаковими і зв'язки між ними встановлені згідно топології «дерева»

Таким чином, зображені на рис. 3.1-3.4 приклади можливих варіантів централізації в системах класу $\mathfrak{S}$ враховують особливості елементів множини $\mathrm{M}_{\mathfrak{B}_2,\mathrm{centr},\mathrm{v}_1}$ і частково особливості певних елементів множин, які задано формулами (3.2) - (3.10). Кількість можливих варіантів централізації в системах класу $\mathfrak{S}$ з їх врахуванням є суттєво більшою. Це створює проблеми зловмисникам при спробах проникнення в корпоративну мережу. Для моделі системи, яку задано за формулою (3.21), графи з рис. 3.1-3.4 належать множині графів $\mathrm{G}_{A^{\mathfrak{S}}}^{\mathfrak{S}}$. Також, різні можливі варіанти графів, які задані на підмножинах $A_1^{\mathfrak{S}}$ та $A_2^{\mathfrak{S}}$, належать множині графів $\mathrm{G}_{A^{\mathfrak{S}}}^{\mathfrak{S}}$, тому модель $M_{A^{\mathfrak{S}}}^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ однозначно визначається підмножинами $A_1^{\mathfrak{S}}$ та $A_2^{\mathfrak{S}}$ та множиною графів $\mathrm{G}_{A^{\mathfrak{S}}}^{\mathfrak{S}}$.

Не всі компоненти системи можуть мати між собою зв’язки. Така організація функціонування компонент в системі і комунікація передбачена можливими варіантами централізації. Тому, оскільки не всі варіанти системи передбачають наявність зв’язків між усіма компонентами, тоді ефективність організації системи в різних варіантах централізації буде відрізнятись між ними. Крім того, різні варіанти централізації в системі розподіляються за чотирма класами архітектури систем: централізовані; частково централізовані; частково децентралізовані; децентралізовані. Внутрішня організація централізації у відповідних компонентах впливатиме також на кількість зв’язків між компонентами, бо зв’язки будуть і між компонентами центру системи. Система може змінювати варіант централізації довільним чином, тобто може переходити від використання варіанту з одного класу до будь-якого з трьох класів або залишатись в тому ж класі, але з іншим варіантом централізації. Все це впливатиме на ефективність функціонування класу $\mathfrak{S}$. Тому, необхідно дослідити вплив кількості зв’язків між компонентами системи в залежності від варіантів централізації і враховувати отриманий результат для визначення наступного варіанту централізації в системі в процесі її функціонування.

Дослідимо систему за параметром кількості зв’язків між її компонентами з врахуванням різної архітектури центру системи та типу його розміщення в компонентах. Ефективність типу архітектури в системі будемо розглядати за критеріями кількості можливих варіантів центру системи та кількості зв’язків між компонентами. Наявність більшої кількості варіантів центру системи дає перевагу системі при спробі зловмисника виявити вузли комп’ютерної мережі з компонентами, в яких міститься центр системи. Тоді, системи з таким типом централізації будуть ефективніші за критерієм кількості варіантів центру системи порівняно з архітектурою, в якій кількість варіантів є меншою. Другим важливим критерієм є кількість зв’язків між компонентами. При цьому окремо потрібно розглядати компоненти з центром системи та компоненти без центру системи в поточний момент часу. Оскільки система є розподіленою, то кількість зв’язків буде впливати на оперативність при надсиланні повідомлень, команд тощо. А також буде впливати на зворотній зв’язкок між компонентами. Розподіл центру між частиною компонент може бути здійснено так: центр розподілений на окремі функції, які розміщено в

різних компонентах; центр розміщено в різних компонентах і всі ці компоненти організовані згідно децентралізованої архітектури та містять однаковий функціонал центру системи. У випадку розподілу центру системи на окремі функції, які розміщено в різних компонентах, підтримка стабільного зв'язку суттєво впливатиме на функціонування системи. Тому, така організація централізації порівняно з варіантом децентралізованого функціонування компонент з центром є більш залежною від стабільності з'єднань між компонентами системи.

Встановлення кращого з чотирьох основних типів централізації в архітектурі системи дасть змогу при визначенні наступного варіанту архітектури за допомогою відповідної функції оцінювання підготувати кращий варіант архітектури, середній та гірший. Далі контролер для вибору остаточного варіанту здійснить вибір в залежності від минулих рішень щодо вибору типу централізації в архітектурі системи. Таким чином, поділ варіантів централізації в архітектурі системи на чотири розглядувані класи дасть змогу здійснити їх цілісне оцінювання в контексті їх ефективності порівняно між собою.

Якщо в системі в поточний момент часу централізована архітектура, то може бути щонайменше два основних випадки: центр системи перебуває в одній компоненті; центр системи розподілений між декількома компонентами. У випадку розподілення центру системи між декількома компонентами, між якими розподіляються функції з центру системи, тобто окремі функції системи будуть в окремих компонентах, а разом вони формуватимуть центр системи, кількість варіантів центру системи буде залежати від кількості залучених компонент, в які буде розподілений центр системи.

Кількість варіантів централізації $\mathrm{N}_{\mathrm{centr},1}^{A^{\Subset}}$ в системі з централізованою архітектурою обчислюємо для випадку розміщення центру системи в одній компоненті так:

$$\mathrm{N}_{\mathrm{centr},1}^{A^{\Subset}} = \sum_{\mathrm{i}=1}^{N_{A^{\Subset}}} \mathrm{C}_{\mathrm{i}}^{1} = \frac{N_{A^{\Subset}}+1}{2} \cdot N_{A^{\Subset}}, \tag{3.22}$$

де $\mathrm{N}_{\mathrm{A}^{\Subset}}$ – загальна кількість компонент в системі $\mathrm{A}^{\Subset}$.

Кількість варіантів централізації $\mathrm{N}_{\mathrm{centr},2}^{A^{\Subset}}$ в системі з централізованою архітектурою обчислюємо для випадку розміщення центру системи в декількох компонентах так:

$$\mathrm{N}_{\mathrm{centr},2}^{A^{\Subset}} = \sum_{\mathrm{i}=2}^{N_{A^{\Subset}}} \sum_{\mathrm{j}=2}^{\mathrm{i}} \mathrm{C}_{\mathrm{i}}^{\mathrm{j}} \cdot \mathrm{C}_{\mathrm{j}}^{1}, \tag{3.23}$$

де $N_{A^{\Subset}}$ – загальна кількість компонент в системі; $N_{A^{\Subset}} > 1$; i – кількість компонент в системі в поточний момент часу; j – кількість компонент з центром системи в поточний момент часу.

В розглядуваному варіанті централізованої архітектури кількість компонент з центром є меншою на одну компоненту від кількості всіх компонент системи, які активні в поточний момент часу. Кількість варіантів централізації $\mathrm{N}_{\mathrm{centr},12}^{A^{\Subset}}$ в системі з централізованою архітектурою обчислюємо так:

$$\mathrm{N}_{\mathrm{centr},12}^{A^{\Subset}} = \sum_{\mathrm{i}=1}^{N_{A^{\Subset}}} \mathrm{C}_{\mathrm{i}}^{1} + \sum_{\mathrm{i}=2}^{N_{A^{\Subset}}} \sum_{\mathrm{j}=2}^{\mathrm{i}} \mathrm{C}_{\mathrm{i}}^{\mathrm{j}} \cdot \mathrm{C}_{\mathrm{j}}^{1}. \tag{3.24}$$

Для частково централізованої архітектури системи $A^{\Subset}$ характерним, на відміну від централізованої архітектури з поділом центру між компонентами і розподіленням між ними функцій центру, є те, що компоненти з центром системи містять однакові функціонали і прийняття рішення такими центрами здійснюється згідно принципу децентралізації за певними критеріями. Такими критеріями може буде варіант з пропонованих рішень, який отримано з більшості компонент з центром системи. Або варіант, що отримано з призначених для формування рішення компонент системи з центром. Але, незалежно від критерію формування варіанту прийнятого рішення, визначальним для такої архітектури системи є обов'язкова наявність мінімум в двох компонентах центру системи з однаковим функціоналом і їх функціонування згідно принципу децентралізації. Тоді, кількість варіантів часткової централізації в системі буде обчислюватись так:

$$\mathrm{N}_{\mathrm{centr},3}^{A^{\Subset}} = \sum_{k=2}^{N_{A^{\Subset}}-1} \sum_{i=2}^{N_{A^{\Subset}}} \sum_{j=2}^{i} C_i^j \cdot C_j^k, \tag{3.25}$$

де $N_{A^{\Subset}}$ – загальна кількість компонент в системі; i – кількість компонент в системі в поточний момент часу; j – кількість компонент з центром системи в поточний момент

часу; k – кількість компонент, в яких може бути центр системи, тобто компоненти, в які при встановлені системи встановлено функціонал центру системи.

Для наявності саме часткової централізації в архітектурі системи і, відповідно, уникнення переходу до децентралізованої архітектури кількість компонент з центром системи в поточний момент часу j $<$ $N_{A^{\Subset}}$. Аналогічно, j $>$ 1, інакше архітектура системи стане централізованою.

Частково децентралізована архітектура системи $A^{\Subset}$ визначається компонентами з центром системи, які організовані згідно принципу децентралізації, кількість яких менше загальної кількості компонент, бо решта компонент мають з'єднання з компонентами з центром системи і отримують від них команди та повідомлення. Таким чином, кількість варіантів в системах з частково децентралізованою архітектурою обчислюємо так:

$$\mathrm{N}_{\mathrm{centr},4}^{A^{\Subset}} = \sum_{j=2}^{N_{A^{\Subset}}-1} \sum_{i=2}^{N_{A^{\Subset}}} C_i^j, \tag{3.26}$$

де $N_{A^{\Subset}}$ – загальна кількість компонент в системі; і – кількість компонент в системі в поточний момент часу; j – кількість компонент з центром системи в поточний момент часу.

Для уникнення переходу до повністю децентралізованої архітектури кількість компонент з центром системи в поточний момент часу j $<$ $N_{A^{\Subset}}$.

Можуть бути інші варіанти формування рішень компонентами з центром системи, але їх кількість за наявності різних варіантів буде фактично однаковою, тому формула (3.26) дає змогу обчислити кількість варіантів.

Децентралізована архітектура в системі $A^{\Subset}$ визначається всіма компонентами з центром системи. Всі компоненти системи в такій архітектурі є однаковими і рішення приймається ними на основі певних заданих для цього критеріїв. Таким чином, кількість варіантів в системах з децентралізованою архітектурою обчислюємо так:

$$\mathrm{N}_{\mathrm{centr},5}^{A^{\Subset}} = \sum_{i=N_{A^{\Subset}}}^{N_{A^{\Subset}}} C_i^{N_{A^{\Subset}}} = 1, \tag{3.27}$$

де $N_{A^{\Subset}}$ – загальна кількість компонент в системі; і – кількість компонент з центром системи в поточний момент часу.

Розглянемо приклади з різною кількістю різних варіантів централізації в

архітектурі системи. В табл. 3.2 наведено приклади та результати щодо кількості варіантів, які обчислено за формулами (3.22), (3.23), (3.25)-(3.27), для $N_{A^{\mathfrak{S}}} = 50$. Ці приклади з табл. 3.1 не є повною кількістю варіантів, які подано в табл. 3.1.

Таблиця 3.2

Кількість варіантів централізації в архітектурі систем

Тип централізації в архітектурі систем	Наявність поділу центру між компонентами системи	Формула	Значення кількості варіантів
Централізована	ні	(3.22)	1275
Централізована	так	(3.23)	$\sum_{i=2}^{50}\sum_{j=2}^{i} C_i^j \cdot C_j^1$
Частково централізована	так	(3.25)	$\sum_{k=2}^{49}\sum_{i=2}^{50}\sum_{j=2}^{i} C_i^j \cdot C_j^k$
Частково децентралізована	так	(3.26)	$\sum_{j=2}^{49}\sum_{i=2}^{50} C_i^j$
Децентралізована	так	(3.27)	1

Таким чином, загальна кількість варіантів формування центру системи, обчислення яких задано формулами (3.24) - (3.27), є прийнятною для використання в системах класу $\mathfrak{S}$, оскільки така стратегія в контексті формування центру системи в її компонентах знімає обмеження, дозволяє центру системи підібрати наступний варіант свого розміщення та варіанту архітектури. Це дає змогу створювати проблеми зловмисникам у виявленні компонент з центром системи та встановленні типу архітектури централізації з метою розуміння ним принципів її функціонування. Загальна кількість варіантів центру системи є більшою, бо залежить від поділу центру між компонентами для частково централізованої та частково децентралізованої архітектури. Розподілення центру між компонентами системи з використанням різної топології між ними збільшить кількість варіантів централізації. Крім того, на кількість варіантів впливатиме також і кількість компонент в системі, в яких не буде центру системи, оскільки всі вони разом будуть об’єктами дослідження зловмисників. Враховуючи таку різноманітність варіантів, яка відображена кількісно формулами

(3.22), (3.23), (3.25) - (3.27), потребують розроблення правила, які задано множино M_{Pr} згідно формули (3.11), визначення наступного типу централізації архітектури в компонентах системи та визначення їх безпосереднього розміщення в конкретних компонентах.

3.4. Математичні моделі та критерії оцінювання варіантів централізації в архітектурі мультикомп'ютерних систем

Поділ на такі чотири основні типи архітектури необхідний при формуванні наступного типу архітектури, бо кожен тип архітектури буде формувати свій варіант прийняття рішень в центрі системи $A^{\Subset}$. Встановимо критерії для оцінювання розглядуваних чотирьох типів централізації в системі. Розроблення методики оцінювання варіантів централізації необхідно для її використання системою при виборі наступного варіанту централізації. Перехід системи до наступного варіанту централізації є складною дією. Варіантів, до яких може перейти система, є багато і тому важливим є визначення такого варіанту, який був би можливим для швидкого та безпечного переходу. Враховуючи дуже велику кількість можливих варіантів централізації в системі, в які можна перейти, постає проблема оптимального вибору кращого варіанту, тому необхідна цільова функція оцінювання наступних варіантів централізації, значення якої будуть базуватись на критеріях та будуть використовуватись контролером при затвердженні варіанту централізації, який буде задано в системі при переході від попереднього варіанту.

Вибір критеріїв будемо здійснювати виходячи з мети цільової функції оцінювання для вибору одного з чотирьох типів централізації, яка полягає в мінімізації свого значення. Тобто значення цільової функції будуть вказувати на те, наскільки ефективний один з чотирьох типів архітектури в залежності від кількості компонент в системі і їх активності в поточний момент часу. В даному підході до побудови цільової функції вибору враховуватимемо кількість компонент в системі, зокрема і активних в поточний момент часу. Чотири типи централізації в архітектурі системи не можуть бути оцінені тільки простим ранжуванням між собою за чотирма рівнями. Можуть бути такі випадки, коли один з типів з більшою кількістю компонент

є менш ефективним порівняно з типом архітектури, в якій при такій же кількості компонент менша ефективність, а при меншій кількості компонент є краща ефективність. Тобто для різних типів централізації при різній кількості компонент можуть бути перетини в класах їх типів за ефективністю. Для оцінювання типів централізації в архітектурі в залежності від чотирьох основних типів введемо такі критерії: оперативність; стійкість; цілісність; безпека. Для аналітичного подання критеріїв використаємо такі показники: час для виконання перебудови архітектури в частині централізації; час для підготовки рішень щодо наступного варіанту централізації в архітектурі системи; загальна кількість компонент в системі; кількість активних компонент центру в системі в поточний момент часу; кількість компонент з центром системи в поточний момент часу; кількість компонент центру системи в новому варіанті, в який планується перехід на наступному кроці; кількість сегментів в корпоративній мережі; наявність компонент системи в демілітаризованій зоні корпоративної мережі; наявність компонент системи у серверних вузлах; наявність функціоналу центру системи у вузлах в демілітаризованій зоні; наявність функціоналу центру системи у серверних вузлах.

Задамо цільову функцію оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації так:

$$\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{f}_{1,\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}}\right),\mathrm{f}_{2,\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{p}_{2,\mathrm{kr}}^{\mathrm{centr}}\right),\ldots,\mathrm{f}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}},\mathrm{kr}}}^{\mathrm{centr}}\left(\mathrm{p}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}},\mathrm{kr}}}^{\mathrm{centr}}\right),\mathrm{F}_{\mathrm{var}}^{\mathrm{centr}}(\mathrm{u}),\mathrm{F}_{\mathrm{var}}^{\mathrm{centr}}(\mathrm{v})\right)\rightarrow \min, \quad (3.28)$$

де $\mathrm{f}_{\mathrm{i,kr}}^{\mathrm{centr}}\left(\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}\right)$ – i - та функція, що задає обчислення значення i – того критерію; $\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}$ – вектор, координатами якого є параметри i – того критерію та варіант централізації; $\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}}$ – кількість аргументів функції $\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}$ та кількість векторів $\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}$; вектор $\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}=\left(\mathrm{p}_{1,\mathrm{i,kr}}^{\mathrm{centr}},\mathrm{p}_{2,\mathrm{i,kr}}^{\mathrm{centr}},\ldots,\mathrm{p}_{\mathrm{N}_{\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}},\mathrm{i,kr}}}^{\mathrm{centr}},\mathrm{V}_{\mathrm{Pr,u}},\mathrm{V}_{\mathrm{Pr,v}},A_{1,u}^{\circledS},A_{1,v}^{\circledS},A_{2,u}^{\circledS},A_{2,v}^{\circledS}\right)$, де $\mathrm{p}_{\mathrm{m,i,kr}}^{\mathrm{centr}}$ – значення m-того параметру для i – того критерію щодо v – того варіанту централізації в системі; $\mathrm{N}_{\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}}$ – кількість параметрів i – того критерію; u та v – номери варіантів централізації; u – номер поточного варіанту централізації в системі; v – номер досліджуваного варіанту централізації в системі після u – того номеру

варіанту централізації; $V_{Pr,u}, V_{Pr,v}$ – вектори, які задаються координатами за формулою (3.13); $F_{var}^{centr}(v)$ – функція, значенням якої є номер одного з типів централізації в системі в поточний момент часу або номер досліджуваного типу; $A_{1,u}^{\mathfrak{S}}$ – підмножина активних компонент центру системи при u – тому поточному номеру варіанту централізації; $A_{2,u}^{\mathfrak{S}}$ – множина компонент системи, які в поточний момент часу не є компонентами центру системи при u – тому поточному номеру варіанту централізації; $A_{1,v}^{\mathfrak{S}}$ – підмножина активних компонент центру системи для v – номеру досліджуваного варіанту централізації в системі, який може бути після u – того номеру варіанту централізації; $A_{2,v}^{\mathfrak{S}}$ – множина компонент системи, які в поточний момент часу не є компонентами центру системи для v – номеру досліджуваного варіанту централізації в системі, який може бути після u – того номеру варіанту централізації.

Множини компонент системи $A_{1,u}^{\mathfrak{S}}, A_{1,v}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}}$ будуть відображати тип компонент в контексті централізації і відомості про них необхідні, щоб застосувати критерії щодо оперативності, стійкості, цілісності та безпеки. Цими множинами будуть означені компоненти в поточний момент часу при певному варіанті централізації і для досліджуваного варіанту централізації, щоб оцінити його допустимість в наступному варіанті централізації.

Для досліджуваного значення функції F_{kr}^{centr}, яку задано за формулою (3.28) значення $N_{F_{kr}^{centr}} = 4$, оскільки визначено чотири критерії. Кількість критеріїв може бути збільшена, але їх доповнення повинно враховувати вимоги щодо їх незалежності та вимоги щодо уникнення компенсації результуючих значень.

Задамо функцію $F_{var}^{centr}(v)$ так:

$$F_{var}^{centr}(v) \to \{1,2,3,4\}, \tag{3.29}$$

де значення $\{1\}$ відповідає централізованій архітектурі, тобто $F_{var}^{centr}(v) = 1$; значення $\{2\}$ – частково централізованій архітектурі, тобто $F_{var}^{centr}(v) = 2$; значення $\{3\}$ – частково децентралізованій архітектурі $F_{var}^{centr}(v) = 3$; значення $\{4\}$ – децентралізованій архітектурі $F_{var}^{centr}(v) = 4$.

З врахуванням формули (3.13) вектор $p_{i,kr}^{centr}$ задамо в розширеній формі так:

$$\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}} = \begin{pmatrix} \mathrm{p}_{1,\mathrm{i,kr}}^{\mathrm{centr}}, \mathrm{p}_{2,\mathrm{i,kr}}^{\mathrm{centr}}, \dots, \mathrm{p}_{\mathrm{N}_{\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}},\mathrm{i,kr}}^{\mathrm{centr}}, \\ \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_1,1}, \mathrm{u}), \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_\mathrm{l},2}, \mathrm{u}), \dots, \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_{10},3}, \mathrm{u}), \\ \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_1,1}, \mathrm{v}), \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_\mathrm{l},2}, \mathrm{v}), \dots, \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_{10},3}, \mathrm{v}), \\ A_{1,u}^{\mathfrak{S}}, A_{1,v}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}} \end{pmatrix}. \quad (3.30)$$

Розглянемо визначення кожного із чотирьох обраних критеріїв. Визначимо критерії спочатку в загальному випадку так:

$$\mathrm{f}_{\mathrm{i,kr}}^{\mathrm{centr}} \begin{pmatrix} \mathrm{p}_{1,\mathrm{i,kr}}^{\mathrm{centr}}, \mathrm{p}_{2,\mathrm{i,kr}}^{\mathrm{centr}}, \dots, \mathrm{p}_{\mathrm{N}_{\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}},\mathrm{i,kr}}^{\mathrm{centr}}, \\ \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_1,1}, \mathrm{u}), \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_\mathrm{l},2}, \mathrm{u}), \dots, \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_{10},3}, \mathrm{u}), \\ \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_1,1}, \mathrm{v}), \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_\mathrm{l},2}, \mathrm{v}), \dots, \mathrm{F_{Pr}}(\mathrm{m}_{\mathfrak{V}_2,\mathrm{centr},\mathrm{v}_{10},3}, \mathrm{v}), \\ A_{1,u}^{\mathfrak{S}}, A_{1,v}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}} \end{pmatrix} \to [0,1], \quad (3.31)$$

де $\mathrm{i} = 1,2,3,4$.

Числові значення обчислені для кожного з цих критеріїв будуть належати числовому відрізку $[0,1]$. Для кожного розглядуваного варіанту централізації в системі, який може бути наступним в архітектурі системи, цільова функція оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації буде мінімізуватись за рахунок наявних в критеріях параметрів.

Визначимо критерій щодо оперативності функцією $\mathrm{f}_{1,\mathrm{kr}}^{\mathrm{centr}}(\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}})$, яка задає обчислення числового значення з урахуванням параметрів вектору $\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}}$, координати якого визначаються за формулою (3.30). Оскільки оперативність характеризується швидкістю передачі інформації та своєчасністю її отримання, то для визначення відповідного їй критерію будемо враховувати час, а також з урахуванням розподілення системи будемо враховувати кількість компонент, які будуть залучені в процес передачі та отримання інформації.

Деталізуємо визначення критерію $\mathrm{f}_{1,\mathrm{kr}}^{\mathrm{centr}}(\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}})$ щодо оперативності з урахуванням співвідношень між певними параметрами, які задані у векторі $\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}$ за формулою (3.30). Нехай показник $\mathrm{p}_{1,1,\mathrm{kr}}^{\mathrm{centr}} = \mathrm{t}_1^{\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}}}$ – час для підготовки рішення центром системи щодо певного наступного типу централізації. Для різних типів

централізації цей час буде різним, оскільки різні типи централізації передбачають залучення різної кількості компонент для формування центру системи. Процес безпосередньої зміни типу централізації в системі вимагатиме певного часу для проведення різних його етапів і, при цьому, може бути так, що частина цих етапів буде виконуватись паралельно, що зменшить час реалізації всього процесу. Тому, введемо для подання показники, які відображатимуть етапи процесу зміни типу централізації:

1) $p_{2,1,kr}^{centr} = t_2^{p_{1,kr}^{centr}}$ – час для визначення нових компонент з функціоналом центру та компонент без такого функціоналу;

2) $p_{3,1,kr}^{centr} = t_3^{p_{1,kr}^{centr}}$ – час для повідомлення компонентам про наступний стан централізації і їх призначення в новій архітектурі системи;

3) $p_{4,1,kr}^{centr} = t_4^{p_{1,kr}^{centr}}$ – час на повідомлення всім компонентам системи про завершення поточного типу централізації в архітектурі системи;

4) $p_{5,1,kr}^{centr} = t_5^{p_{1,kr}^{centr}}$ – час отримання підтвердження від всіх компонент системи про опрацювання ними повідомлення про завершення поточного типу централізації та перехід до нового типу централізації в архітектурі системи;

5) $p_{6,1,kr}^{centr} = t_6^{p_{1,kr}^{centr}}$ – час надсилання команди всім компонентам системи про початок роботи з новим центром системи та отримання підтвердження від них про успішний перехід;

6) $p_{7,1,kr}^{centr} = t_7^{p_{1,kr}^{centr}}$ – час надсилання повідомлень між компонентами центру системи для узгодження роботи;

7) $p_{8,1,kr}^{centr} = k_8^{p_{1,kr}^{centr}}$ – загальна кількість компонент в системі;

8) $p_{9,1,kr}^{centr} = k_9^{p_{1,kr}^{centr}}$ – кількість активних компонент системи в поточний момент часу;

9) $p_{10,1,kr}^{centr} = k_{10}^{p_{1,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу;

10) $p_{11,1,kr}^{centr} = u_{11}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі для підмножин $A_{1,u}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}$;

11) $p_{12,1,kr}^{centr} = v_{12}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти системи в поточний момент часу у вузлах корпоративної мережі для підмножин $A_{1,v}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}}$;

12) $p_{13,1,kr}^{centr} = u_{13}^{p_{1,kr}^{centr}}$ – вектор, координатами якого є відомості про компоненти центру системи в поточний момент часу у вузлах корпоративної мережі для підмножини $A_{1,u}^{\mathfrak{S}}$, *які відображають активні компоненти центру і неактивні, але які були означені як такі, що вони є частиною центру системи*;

13) $p_{14,1,kr}^{centr} = k_{14}^{p_{1,kr}^{centr}}$ – кількість неактивних компонент з функціоналом центру системи в поточний момент часу;

14) $p_{15,1,kr}^{centr} = k_{15}^{p_{1,kr}^{centr}}$ – кількість неактивних компонент без функціоналу центру системи в поточний момент часу;

15) $p_{16,1,kr}^{centr} = k_{16}^{p_{1,kr}^{centr}}$ – кількість сегментів в корпоративній мережі, в які встановлено компоненти системи;

16) $p_{17,1,kr}^{centr} = k_{17}^{p_{1,kr}^{centr}}$ – кількість компонент системи в демілітаризованій зоні корпоративної мережі;

17) $p_{18,1,kr}^{centr} = k_{18}^{p_{1,kr}^{centr}}$ – кількість компонент системи у серверних вузлах;

18) $p_{19,1,kr}^{centr} = k_{19}^{p_{1,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні;

19) $p_{20,1,kr}^{centr} = k_{20}^{p_{1,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у серверних вузлах.

Для децентралізованої архітектури показники часу $t_7^{p_{1,kr}^{centr}}$ будуть більшими порівняно з іншими типами архітектури. Для централізованого типу архітектури без розподілення центру системи $t_7^{p_{1,kr}^{centr}} = 0$. Якщо тип централізації в архітектурі

системи відмінний від децентралізованого типу, тоді на показник часу $t_7^{p_{1,kr}^{centr}}$ буде впливати кількість компонент з центром системи. Із збільшенням їх кількості зростатиме час для узгодження роботи між ними.

Для децентралізованої архітектури показник $t_2^{p_{1,kr}^{centr}} = 0$, оскільки рішення щодо часу для визначення нових компонент з функціоналом центру та компонент без такого функціоналу приймати не потрібно, оскільки всі ці компоненти будуть компонентами центру. Але в такій архітектурі час $t_7^{p_{1,kr}^{centr}}$ надсилання повідомлень між компонентами центру системи для узгодження роботи буде найбільшим порівняно з рештою типів архітектури.

Визначимо $f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right)$ для критерію щодо оперативності так:

$$f_{1,kr}^{centr}\left(p_{1,kr}^{centr}\right) = 1 - \frac{1}{9}\cdot\left(\frac{\sum_{i=1}^{7} t_i^{p_{1,kr}^{centr}}}{\sum_{i=1}^{7} t_{i,max}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}}}{k_9^{p_{1,kr}^{centr}}} + \frac{k_{10}^{p_{1,kr}^{centr}}}{k_{10}^{p_{1,kr}^{centr}} + k_{14}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - \left(k_{15}^{p_{1,kr}^{centr}} + k_{16}^{p_{1,kr}^{centr}}\right)}{k_8^{p_{1,kr}^{centr}}} + \right.$$

$$\left. \frac{k_{16}^{p_{1,kr}^{centr}} - 1}{k_{16}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - k_{17}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}} + \frac{k_{17}^{p_{1,kr}^{centr}} - k_{19}^{p_{1,kr}^{centr}}}{k_{17}^{p_{1,kr}^{centr}}} + \frac{k_8^{p_{1,kr}^{centr}} - k_{18}^{p_{1,kr}^{centr}}}{k_8^{p_{1,kr}^{centr}}} + \frac{k_{18}^{p_{1,kr}^{centr}} - k_{20}^{p_{1,kr}^{centr}}}{k_{18}^{p_{1,kr}^{centr}}}\right), \qquad (3.32)$$

де $t_{i,max}^{p_{1,kr}^{centr}}$ – найбільше значення часу за і-тою характеристикою, яке було отримано в процесі функціонування системи, починаючи з першого самостійного рішення системою; $i = 1, \dots, 7$.

Таким чином, критерій щодо оперативності може бути визначений за формулою (3.32) і значення обчислені з його визначення можуть бути використані в цільовій функції (формула (3.28)) оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації. В формулі (3.32) враховано досвід функціонування системи в частині самостійного прийняття рішень щодо наступного варіанту централізації і збереження отриманих показників для використання в подальших кроках їх найбільших значень.

Стійкість системи при визначенні критерію $f_{2,kr}^{centr}\left(p_{2,kr}^{centr}\right)$ будемо розглядати тільки щодо її центру. Під стійкістю центру системи незалежно від типу централізації в архітектурі системи будемо вважати його здатність при зміні внутрішніх і зовнішніх

параметрів забезпечувати функціональність в операційному середовищі, зокрема і у випадку мінімальної втрати функціональності. Зовнішні впливи можуть бути в той час, коли система здійснює перебудову варіанту централізації. Або коли відбувається зловмисна атака і вона впливає на компоненти з функціоналом центру, бо проводиться на вузли комп'ютерної мережі, в яких знаходяться компоненти з центром системи. Можуть бути, також, інші зовнішні події, які впливатимуть на роботу центру. Наприклад, вихід з ладу обладнання, яке поєднує частини вузлів мережі і, відповідно, тоді система буде розпадатись на частини. Внутрішніми впливами на роботу центру системи можуть бути незавершені обміни повідомленнями. Оскільки система розподілена, то можуть виникати позаштатні ситуації з обладнанням і в такому випадку обмін повідомленнями може перериватись, а деякі з них можуть втрачатись. Також, можуть бути перервані для частини компонент системи операції з формування нового центру. Для визначення критерію щодо стійкості центру системи сформуємо дві множини можливих подій, що впливатимуть на функційність центру системи, які викликані зовнішніми та внутрішніми впливами, а також їх поєднанням. Задамо множину подій, які викликані в центрі системи зовнішніми впливами і впливають на його стійкість, так:

$$A^{z}_{2,kr} = \left\{a^{z}_{2,kr,1}, a^{z}_{2,kr,2}, \dots, a^{z}_{2,kr,N_{A^{z}_{2,kr}}}\right\}, \tag{3.33}$$

де $a^{z}_{2,kr,i}$ – i – тий елемент, що відповідає події, яка викликана зовнішніми впливами; $N_{A^{z}_{2,kr}}$ – кількість елементів в множині $A^{z}_{2,kr}$; $i = 1,2, \dots, N_{A^{z}_{2,kr}}$.

Задамо множину подій, які викликані в центрі системи внутрішніми впливами і впливають на його стійкість, так:

$$A^{v}_{2,kr} = \left\{a^{v}_{2,kr,1}, a^{v}_{2,kr,2}, \dots, a^{v}_{2,kr,N_{A^{v}_{2,kr}}}\right\}, \tag{3.34}$$

де $a^{v}_{2,kr,i}$ – i – тий елемент, що відповідає події, яка викликана внутрішніми впливами; $N_{A^{v}_{2,kr}}$ – кількість елементів в множині $A^{v}_{2,kr}$; $i = 1,2, \dots, N_{A^{v}_{2,kr}}$.

Задамо множину подій, які викликані в центрі системи поєднанням внутрішніх та зовнішніх впливів і впливають на його стійкість, так:

$$A_{2,kr}^{vz} = \left\{a_{2,kr,1}^{vz}, a_{2,kr,2}^{vz}, \dots, a_{2,kr,N_{A_{2,kr}^{vz}}}^{vz}\right\}, \quad (3.35)$$

де $a_{2,kr,i}^{vz}$ – i – тий елемент, що відповідає події, яка викликана зовнішніми впливами; $N_{A_{2,kr}^{vz}}$ – кількість елементів в множині $A_{2,kr}^{vz}$; $i = 1,2, \dots, N_{A_{2,kr}^{vz}}$.

Частина подій, яка впливатиме на роботу центру системи і його стійкість та задано множиною $A_{2,kr}^{vz}$, може бути породжена тільки поєднанням як зовнішніх так і внутрішніх впливів. Якщо ж подія породжена окремо зовнішнім або внутрішнім впливом, але при цьому відбулось їх поєднання, то такі події віднесемо до множин $A_{2,kr}^{z}$ і $A_{2,kr}^{v}$.

Кожна з подій, які впливатимуть на стійкість центру системи, буде порушувати стійкість центру системи з певною ймовірністю. Тому, визначимо стійкість центру системи величиною $P_{st}^{centr}(t)$, значення якої буде належати відрізку $[0,1]$ та буде залежати від часу. Тобто, при різних значеннях часу можливі різні значення стійкості або в процесі функціонування системи стійкість центру системи протягом певного часу може змінюватись. Центр системи буде стійкішим при більшому значенні величини $P_{st}^{centr}(t)$, тобто чим ближче значення $P_{st}^{centr}(t)$ до одиниці, то стійкість центру системи краща.

Задамо в загальному поданні критерій щодо стійкості центру системи з врахуванням формули (3.31) так:

$$P_{st}^{centr}(t) = 1 - f_{2,kr}^{centr}\left(\begin{array}{c} p_{1,2,kr}^{centr}, p_{2,2,kr}^{centr}, \dots, p_{N_{p_{i,kr}^{centr}},2,kr}^{centr}, \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, u\right), F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, u\right), \dots, F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, u\right), \\ F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_1,1}, v\right), F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_l,2}, v\right), \dots, F_{Pr}\left(m_{\mathfrak{B}_2,centr,v_{10},3}, v\right), \\ A_{1,u}^{\mathfrak{S}}, A_{1,v}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}} \end{array}\right), \quad (3.36)$$

На відміну від визначення критерію оперативності, для критерію щодо стійкості центру системи визначено величину стійкості функцією $P_{st}^{centr}(t)$ через функцію $f_{2,kr}^{centr}$, яка є кращою при значенні близькому до одиниці, а функції для критеріїв повинні бути близькими до нуля, бо цільова функція F_{kr}^{centr} (формула (3.28)) оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації повинна бути мінімізована.

Деталізуємо значення аргументів функції $f_{2,kr}^{centr}$, тобто критерій щодо стійкості центру системи, так:

1) $p_{1,2,kr}^{centr} = t$ – поточний час, в якому здійснено визначення величини $P_{st}^{centr}(t)$;

2) $p_{2,2,kr}^{centr} = k_1^{p_{2,kr}^{centr}}$ – загальна кількість компонент в системі поточний момент часу t (якщо система функціонує тривалий час, то загальну кількість компонент системи може бути змінено);

3) $p_{3,2,kr}^{centr} = k_2^{p_{2,kr}^{centr}}$ – кількість активних компонент системи в поточний момент часу;

4) $p_{4,2,kr}^{centr} = k_3^{p_{2,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу;

5) $p_{5,2,kr}^{centr} = k_4^{p_{2,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони не підтвердили свою активність як компоненти центру системи та продовжують функціонувати як частина системи;

6) $p_{6,2,kr}^{centr} = k_5^{p_{2,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені коректно разом з комп’ютерними станціями, в які встановлені;

7) $p_{7,2,kr}^{centr} = k_6^{p_{2,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені аварійно разом з комп’ютерними станціями, в які встановлені;

8) $p_{8,2,kr}^{centr} = k_7^{p_{2,kr}^{centr}}$ – кількість активних компонент центру системи в поточний момент часу;

9) $p_{9,2,kr}^{centr} = u_8^{p_{2,kr}^{centr}}$ – вектор, координатами якого є відомості про події з множини подій $A_{2,kr}^{z}$ до поточного часу визначеного показником $p_{1,2,kr}^{centr} = t$, які викликані в центрі системи зовнішніми впливами, і впливають на його стійкість;

10) $p_{10,1,kr}^{centr} = u_9^{p_{2,kr}^{centr}}$ – вектор, координатами якого є відомості про події з множини подій $A_{2,kr}^{v}$ до поточного часу визначеного показником $p_{1,2,kr}^{centr} = t$, які викликані в центрі системи внутрішніми впливами, і впливають на його стійкість;

11) $p_{11,1,kr}^{centr} = u_{10}^{p_{2,kr}^{centr}}$ – вектор, координатами якого є відомості про події з множини подій $A_{2,kr}^{vz}$ до поточного часу визначеного показником $p_{1,2,kr}^{centr} = t$, які викликані в центрі системи зовнішніми і внутрішніми впливами, які викликані в центрі системи поєднанням зовнішніх і внутрішніх впливів і впливають на його стійкість;

12) $p_{12,2,kr}^{centr} = k_{11}^{p_{2,kr}^{centr}}$ – кількість неактивних компонент з функціоналом центру системи в поточний момент часу;

13) $p_{13,2,kr}^{centr} = k_{12}^{p_{2,kr}^{centr}}$ – кількість неактивних компонент без функціоналу центру системи в поточний момент часу;

14) $p_{14,2,kr}^{centr} = k_{13}^{p_{2,kr}^{centr}}$ – кількість сегментів в корпоративній мережі, в які встановлено компоненти системи;

15) $p_{15,2,kr}^{centr} = k_{14}^{p_{2,kr}^{centr}}$ – кількість компонент системи в демілітаризованій зоні корпоративної мережі;

16) $p_{16,2,kr}^{centr} = k_{15}^{p_{2,kr}^{centr}}$ – кількість компонент системи у серверних вузлах;

17) $p_{17,2,kr}^{centr} = k_{16}^{p_{2,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні;

18) $p_{18,2,kr}^{centr} = k_{17}^{p_{2,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у серверних вузлах;

19) $p_{19,2,kr}^{centr} = k_{18}^{p_{2,kr}^{centr}}$ – кількість частин системи, в кожній з яких є компоненти з функціоналом центру системи, при тимчасовому поділу системи;

20) $p_{20,2,kr}^{centr} = k_{19}^{p_{2,kr}^{centr}}$ – кількість частин системи, в яких немає активних компонент з функціоналом центру системи, при тимчасовому поділу системи;

21) $p^{centr}_{21,2,kr} = k^{p^{centr}_{2,kr}}_{20}$ – кількість частин системи, в яких є активні компоненти з функціоналом центру системи, при тимчасовому поділу системи;

22) $p^{centr}_{22,2,kr} = t^{p^{centr}_{2,kr}}_{21}$ – час протягом якого система функціонувала без центру системи до поточного часу, який визначено показником $p^{centr}_{1,2,kr} = t$;

23) $p^{centr}_{23,2,kr} = k^{p^{centr}_{2,kr}}_{22}$ – кількість подій з множини подій $A^{z}_{2,kr}$ до поточного часу визначеного показником $p^{centr}_{1,2,kr} = t$, які викликані в центрі системи зовнішніми впливами, і впливають на його стійкість;

24) $p^{centr}_{24,1,kr} = k^{p^{centr}_{2,kr}}_{23}$ – кількість подій з множини подій $A^{v}_{2,kr}$ до поточного часу визначеного показником $p^{centr}_{1,2,kr} = t$, які викликані в центрі системи внутрішніми впливами, і впливають на його стійкість;

25) $p^{centr}_{25,1,kr} = k^{p^{centr}_{2,kr}}_{24}$ – кількість подій з множини подій $A^{vz}_{2,kr}$ до поточного часу визначеного показником $p^{centr}_{1,2,kr} = t$, які викликані в центрі системи зовнішніми і внутрішніми впливами, які викликані в центрі системи поєднанням зовнішніх і внутрішніх впливів і впливають на його стійкість;

26) $p^{centr}_{26,2,kr} = k^{p^{centr}_{2,kr}}_{25}$ – кількість $N_{A^{z}_{2,kr}}$ елементів в множині $A^{z}_{2,kr}$, тобто кількість координат у векторів $u^{p^{centr}_{2,kr}}_{8}$;

27) $p^{centr}_{27,1,kr} = k^{p^{centr}_{2,kr}}_{26}$ – кількість $N_{A^{v}_{2,kr}}$ елементів в множині $A^{v}_{2,kr}$, тобто кількість координат у векторів $u^{p^{centr}_{2,kr}}_{9}$;

28) $p^{centr}_{28,1,kr} = k^{p^{centr}_{2,kr}}_{27}$ – кількість $N_{A^{vz}_{2,kr}}$ елементів в множині $A^{vz}_{2,kr}$, тобто кількість координат у векторів $u^{p^{centr}_{2,kr}}_{10}$.

Для кожного з векторів $u^{p^{centr}_{2,kr}}_{8}$, $u^{p^{centr}_{2,kr}}_{9}$, $u^{p^{centr}_{2,kr}}_{10}$ за його координатами потрібно встановити ймовірність впливу на стійкість центру системи. Нулеві координати векторів будуть вказувати на відсутність подій. Ненульові значення координат векторів будуть вказувати на кількість подій в центрі системи. Якщо значення координати більше одиниці, тоді подія, яка відповідає певній координаті, відбулась

певну кількість разів, що спричинить більший вплив. Кожна з подій має свій вплив на центр системи. Дійсно, деякі з подій щодо центру системи можуть зупинити його роботу. Тоді, такі події, які відображені координатами у векторах будуть зі 100% ймовірністю зупиняти функціонування центру системи. А будуть події, які частково впливатимуть на його функціонування і за певних обставин він зможе продовжувати свою роботу. Тоді, такі події матимуть ймовірність менше 100%. Але може бути при поєднанні певних подій суттєве зменшення можливості функціонування центру системи, яке по суті не буде дорівнювати 100%, а буде близьким до 100%. Ймовірність події щодо впливу на стійкість функціонування центру системи, прояв якої задано координатою вектору, буде знаходить в межах відрізку [0,1]. Якщо протягом певного часу функціонування центру були прояви декількох подій, то їх ймовірності будуть додаватись, але у випадку появи події і подолання системою її наслідків, то через певний час відомості про таку подію залишаться лише в архіві про події, а не у векторі. У векторі будуть відображатись лише актуальні події. Після їх опрацювання значення координат векторів будуть оновлюватись. Задамо функції, які будуть встановлювати ймовірність події для координат векторів так:

$$F^{i}_{u^{p^{centr}_{2,kr}}_{7+i}}\left(u^{p^{centr}_{2,kr}}_{7+i,J},t\right)=$$

$$\begin{cases} 0, \text{якщо } u^{p^{centr}_{2,kr}}_{7+i,J}=0; \\ P, \text{якщо центр системи продовжує функціонувати; } 0<P<1; \\ 1, \text{якщо } u^{p^{centr}_{2,kr}}_{7+i,J}>2 \text{ або центр системи припинив функціонування,} \end{cases} \quad (3.37)$$

де $i=1,2,3$; J – номер координати вектору; $J=1,2,\dots,N_{A^{q}_{2,kr}}$; $N_{A^{q}_{2,kr}}$ - кількість елементів в множині $A^{q}_{2,kr}$; q відповідає z, якщо $i=1$; q відповідає v, якщо $i=2$; q відповідає vz, якщо $i=3$.

Значення P не залежить від кількості активних компонент центру системи, кількості всіх компонент системи, проблемних компонент системи. Це значення характеризує лише подію і її вплив на стійкість системи. Врахування кількості компонент системи та центру системи з різними варіантами в поточний момент функціонування здійснимо безпосередньо при визначенні величини $P^{centr}_{st}(t)$

безпосередньо за формулою (3.36). Для визначення значення P можна відсортувати всі можливі події, що впливають на стійкість системи в залежність від одного з чотирьох типів її можливої архітектури і від найменшого впливу до найбільшого впливу, та надати їм значення таким чином:

$$P = 1 - \frac{1}{k}, \tag{3.38}$$

де k – номер відсортованих координат вектору; $k = 1,2, \dots, N_{A_{2,kr}^{q}}$; $N_{A_{2,kr}^{q}}$ – кількість елементів в множині $A_{2,kr}^{q}$; q відповідає z, якщо $i = 1$; q відповідає v, якщо $i = 2$; q відповідає vz, якщо $i = 3$.

Значення величини P можуть бути визначені і іншими аналітичними виразами. На це впливатимуть особливості аналізованих подій в співвіднесенні між собою щодо впливу на стійкість системи. В контексті розглядуваних подій щодо центру системи, то ними можуть бути, наприклад, такі: в процесі функціонування центру системи втрачено зв'язок з однією з компонент центру системи; втрачено зв'язок з компонентою, що не належить центру системи; центр системи розподілився на дві частини через втрату з'єднання; центр системи не завершив перехід до наступної визначеної ним нової архітектури тощо. Згідно таких подій потрібно сформувати бази подій для кожної з трьох множин $A_{2,kr}^{z}$, $A_{2,kr}^{v}$, $A_{2,kr}^{vz}$ і задати параметри координат векторів $u_{8}^{p_{2,kr}^{centr}}$, $u_{9}^{p_{2,kr}^{centr}}$, $u_{10}^{p_{2,kr}^{centr}}$ із значеннями ймовірності впливу на стійкість центру системи. Кожне значення координат векторів буде залежати від чотирьох типів централізації в архітектурі системи. Наприклад, втрата компоненти з центром системи для централізованої архітектури з розміщенням центру в одній компоненті призведе до виходу з ладу всього центру системи і, тоді, значення $F^{i}_{u_{7+i}^{p_{2,kr}^{centr}}}\left(u_{7+i,J}^{p_{2,kr}^{centr}}, t\right) =$ 1 (формула (3.37)). Але для децентралізованого типу архітектури така подія вплине незначно і цей вплив буде тільки щодо витрат часу на встановлення факту зменшення системи і центру системи на одну компоненту.

Отримавши визначення значень координат векторів за формулою (3.38) здійснимо визначення величини $P_{st}^{centr}(t)$ так:

$$P_{st}^{centr}(t) = 1 - \frac{k_2^{p_{2,kr}^{centr}}}{k_1^{p_{2,kr}^{centr}}} \cdot \frac{k_7^{p_{2,kr}^{centr}}}{e+k_3^{p_{2,kr}^{centr}} - k_5^{p_{2,kr}^{centr}}} \cdot \frac{k_3^{p_{2,kr}^{centr}} - k_4^{p_{2,kr}^{centr}} - k_6^{p_{2,kr}^{centr}} + e}{e+k_3^{p_{2,kr}^{centr}}} \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}} + e}{e+k_1^{p_{2,kr}^{centr}}} \cdot$$

$$\frac{t - t_{21}^{p_{2,kr}^{centr}} + e}{e+t} \cdot \frac{1}{3} \cdot \left(\sum_{J=1}^{N_{A_{2,kr}^z}} F^1_{u_8^{p_{2,kr}^{centr}}} \left(u_{8,J}^{p_{2,kr}^{centr}}, t \right) + \sum_{J=1}^{N_{A_{2,kr}^v}} F^2_{u_9^{p_{2,kr}^{centr}}} \left(u_{9,J}^{p_{2,kr}^{centr}}, t \right) + \right.$$

$$\left. + \sum_{J=1}^{N_{A_{2,kr}^{vz}}} F^3_{u_{10}^{p_{2,kr}^{centr}}} \left(u_{10,J}^{p_{2,kr}^{centr}}, t \right) \right) \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}} + e}{e+k_1^{p_{2,kr}^{centr}}} \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}} + e}{e+k_1^{p_{2,kr}^{centr}}} \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}} + e}{e+k_1^{p_{2,kr}^{centr}}} \cdot$$

$$\frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}}}{k_1^{p_{2,kr}^{centr}}} \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}}}{k_1^{p_{2,kr}^{centr}}} \cdot \frac{k_1^{p_{2,kr}^{centr}} - k_1^{p_{2,kr}^{centr}} + e}{e+k_1^{p_{2,kr}^{centr}}} \cdot \frac{1}{k_1^{p_{2,kr}^{centr}}}, \qquad (3.39)$$

де $e = 0{,}00001$; J – номер координати вектору; $J = 1,2,\dots,N_{A_{2,kr}^v}$; $N_{A_{2,kr}^v}$ - кількість елементів в множині $A_{2,kr}^v$; $J = 1,2,\dots,N_{A_{2,kr}^z}$; $N_{A_{2,kr}^z}$ - кількість елементів в множині $A_{2,kr}^{vz}$; $J = 1,2,\dots,N_{A_{2,kr}^{vz}}$; $N_{A_{2,kr}^{vz}}$ - кількість елементів в множині $A_{2,kr}^{vz}$; $N_{A_{2,kr}^{vz}}$ – кількість елементів в множині $A_{2,kr}^{vz}$; $k_i^{p_{2,kr}^{centr}}$ – показники для критерію щодо стійкості; $i = 1,2,\dots,24$; t – поточний час.

Таким чином, критерій щодо стійкості центру системи може бути визначений за формулою (3.39) і значення обчислені з його визначення можуть бути використані в цільовій функції (формула (3.28)) оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації.

Визначимо критерій щодо цілісності центру системи функцією $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$, яка задає обчислення числового значення з урахуванням параметрів вектору $p_{3,kr}^{centr}$, координати якого визначаються за формулою (3.30). Під цілісністю центру системи будемо розглядати внутрішню єдність пов’язаних між собою компонент центру системи і частини, з яких сформовано центр системи. Для варіанту централізованої архітектури центру системи з його розміщенням в одній компоненті будемо розглядати тільки єдність частин, з яких сформовано центр системи. Цілісність центру системи буде відображати єдність його частин і зв’язків між ними порівняно з зовнішніми до нього компонентами системи та зовнішніми компонентами по відношенню до системи. Таким чином, в корпоративній мережі в контексті цілісності центру системи можна виділити чотири типи зв’язків: між компонентами центру

системи; між компонентами системи поза центром; між компонентами центру системи і компонентами поза центром; між компонентами, що не належать системі. Тоді, можна визначити пріоритетність процесів центру системи порівняно з рештою типів зв'язків в системі і поза нею. Зв'язки між компонентами центру системи повинні бути пріоритетними порівняно із зв'язками, які підтримують цілісність системи. Крім того, зв'язки між компонентами поза центром системи та мін ними і компонентами центру системи мають різні пріоритети, але в контексті цілісності саме центру системи мають однаковий пріоритет, оскільки вони відповідають за збереження та підтримку цілісності всієї системи.

Цілісність центру системи позиціонуватимемо окремо від її стійкості, оскільки цілісність розглядаємо щодо зв'язків для оцінювання єдності центру системи, а стійкість центру системи розглядали як його здатність продовжувати виконувати поставлені завдання в умовах виходу з ладу частини компонентів і елементів при внутрішніх і зовнішніх впливах. Тому, введемо показники для функції $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$ щодо єдності центру системи через особливості зв'язків між компонентами і його елементами так:

1) $p_{1,3,kr}^{centr} = t$ – поточний час, в якому здійснено визначення величини $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$;

2) $p_{2,3,kr}^{centr} = k_1^{p_{3,kr}^{centr}}$ – загальна кількість компонент в системі поточний момент часу t (якщо система функціонує тривалий час, то загальну кількість компонент системи може бути змінено);

3) $p_{3,3,kr}^{centr} = k_2^{p_{3,kr}^{centr}}$ – кількість активних компонент системи в поточний момент часу;

4) $p_{4,3,kr}^{centr} = k_3^{p_{3,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу;

5) $p_{5,3,kr}^{centr} = k_4^{p_{3,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони не підтвердили свою активність як компоненти центру системи та продовжують функціонувати як частина системи;

6) $p_{6,3,kr}^{centr} = k_5^{p_{3,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені коректно разом з комп'ютерними станціями, в які встановлені;

7) $p_{7,3,kr}^{centr} = k_6^{p_{3,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені аварійно разом з комп'ютерними станціями, в які встановлені;

8) $p_{8,3,kr}^{centr} = k_7^{p_{3,kr}^{centr}}$ – кількість активних компонент центру системи в поточний момент часу;

9) $p_{9,3,kr}^{centr} = k_8^{p_{3,kr}^{centr}}$ – повна розрахункова кількість з'єднань між всіма компонентами центру системи в поточний момент часу, тобто кількість ребер в повному графі, в якому вершинами є компоненти центру системи;

10) $p_{10,3,kr}^{centr} = k_9^{p_{3,kr}^{centr}}$ – наявна кількість з'єднань між всіма компонентами центру системи в поточний момент часу, тобто кількість ребер в графі, в якому вершинами є компоненти центру системи;

11) $p_{,11,kr}^{centr} = k_{10}^{p_{3,kr}^{centr}}$ – повна розрахункова кількість з'єднань між всіма компонентами системи в поточний момент часу, тобто кількість ребер в повному графі, в якому вершинами є компоненти системи;

12) $p_{12,3,kr}^{centr} = k_{11}^{p_{3,kr}^{centr}}$ – наявна кількість з'єднань між всіма компонентами системи в поточний момент часу, тобто кількість ребер в графі, в якому вершинами є компоненти системи;;

13) $p_{13,3,kr}^{centr} = k_{12}^{p_{3,kr}^{centr}}$ – кількість сегментів в корпоративній мережі, в які встановлено компоненти системи;

14) $p_{14,3,kr}^{centr} = k_{13}^{p_{3,kr}^{centr}}$ – кількість компонент системи в демілітаризованій зоні корпоративної мережі;

15) $p_{15,3,kr}^{centr} = k_{14}^{p_{3,kr}^{centr}}$ – кількість компонент системи у серверних вузлах;

16) $p_{16,3,kr}^{centr} = k_{15}^{p_{3,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у вузлах в демілітаризованій зоні;

17) $p_{17,3,kr}^{centr} = k_{16}^{p_{3,kr}^{centr}}$ – кількість компонент з функціоналом центру системи у серверних вузлах;

18) $p_{18,3,kr}^{centr} = k_{17}^{p_{3,kr}^{centr}}$ – кількість частин системи, в кожній з яких є компоненти з функціоналом центру системи, при тимчасовому поділу системи;

19) $p_{19,3,kr}^{centr} = k_{18}^{p_{3,kr}^{centr}}$ – кількість частин системи, в яких немає активних компонент з функціоналом центру системи, при тимчасовому поділу системи;

20) $p_{20,3,kr}^{centr} = k_{19}^{p_{3,kr}^{centr}}$ – кількість частин системи, в яких є активні компоненти з функціоналом центру системи, при тимчасовому поділу системи;

21) $p_{21,3,kr}^{centr} = t_{20}^{p_{3,kr}^{centr}}$ – час протягом якого система функціонувала без центру системи до поточного часу, який визначено показником $p_{1,3,kr}^{centr} = t$;

22) $p_{22,3,kr}^{centr} = k_{21}^{p_{3,kr}^{centr}}$ – загальна кількість елементів (частин) центру системи, які можуть бути розміщені в різних компонентах та підтримувати між собою зв’язок для виконання завдань;

23) $p_{23,3,kr}^{centr} = k_{22}^{p_{3,kr}^{centr}}$ – поточна кількість компонент, в яких розміщено елементи (частини) центру системи;

24) $p_{24,3,kr}^{centr} = k_{23}^{p_{3,kr}^{centr}}$ – загальна кількість з’єднань між компонентами системи протягом часу t;

25) $p_{25,3,kr}^{centr} = k_{24}^{p_{3,kr}^{centr}}$ – загальна кількість з’єднань між компонентами центру системи протягом часу t.

Показник $k_{24}^{p_{3,kr}^{centr}}$ буде відображати пріоритет з’єднань при деталізації критерію щодо цілісності. Аналогічно до попередніх двох критеріїв, які визначено відповідними функціями функція $f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right)$, кращим значенням з двох отриманих значень те, яке є меншим, тобто ближчим до числа нуль. Згідно введених показників деталізуємо функцію так:

$$f_{3,kr}^{centr}\left(p_{3,kr}^{centr}\right) = 1 - \frac{k_2^{p_{3,kr}^{centr}}}{k_1^{p_{3,kr}^{centr}}} \cdot \frac{k_7^{p_{3,kr}^{centr}} + k_5^{p_{3,kr}^{centr}}}{k_3^{p_{3,kr}^{centr}}} \cdot \frac{k_7^{p_{3,kr}^{centr}} - k_6^{p_{3,kr}^{centr}} + e}{k_7^{p_{3,kr}^{centr}} + e} \cdot \frac{k_7^{p_{3,kr}^{centr}} - k_4^{p_{3,kr}^{centr}} + e}{k_7^{p_{3,kr}^{centr}} + e} \cdot$$

$$\frac{k_7^{p_{3,kr}^{centr}}}{k_8^{p_{3,kr}^{centr}}} \cdot \frac{k_{11}^{p_{3,kr}^{centr}}}{k_{10}^{p_{3,kr}^{centr}}} \cdot \frac{k_{12}^{p_{3,kr}^{centr}} - k_{15}^{p_{3,kr}^{centr}} - k_{16}^{p_{3,kr}^{centr}}}{k_{12}^{p_{3,kr}^{centr}}} \cdot \frac{k_{17}^{p_{3,kr}^{centr}} - k_{18}^{p_{3,kr}^{centr}}}{k_{17}^{p_{3,kr}^{centr}}} \cdot \frac{k_{19}^{p_{3,kr}^{centr}} - k_{18}^{p_{3,kr}^{centr}}}{k_{19}^{p_{3,kr}^{centr}}} \cdot \frac{t - t_{20}^{p_{3,kr}^{centr}}}{t} \cdot$$

$$\frac{k_{21}^{p_{3,kr}^{centr}} - k_{22}^{p_{3,kr}^{centr}} + e}{k_{21}^{p_{3,kr}^{centr}} - 1 + e} \cdot \frac{k_{22}^{p_{3,kr}^{centr}} + e}{k_{23}^{p_{3,kr}^{centr}} + e}, \qquad (3.40)$$

де $e = 0{,}00001$; t – поточний час.

Таким чином, критерій щодо цілісності центру системи може бути визначений за формулою (3.40) і значення обчислені з його визначення можуть бути використані в цільовій функції (формула (3.28)) оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації. Особливістю визначення критерію цілісності є врахування пріоритету з'єднань в системі між компонентами, варіантів з'єднань в контексті компонент з центром системи, можливого розподілу центру системи на елементи з розміщенням їх в різних компонентах. Таке визначення критерію при врахуванні його в цільовій функції за умови досягнення мінімізації її значення буде основою при підготовці наступного варіанту централізації в системі, оскільки, крім оцінювання поточного варіанту централізації, буде забезпечувати даними щодо оптимальних варіантів та оптимальної кількості з'єднань між компонентами центру системи.

Визначимо критерій щодо безпеки центру системи функцією $f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right)$, яка задає обчислення числового значення з урахуванням параметрів вектору $p_{4,kr}^{centr}$. Безпеку центру системи будемо розглядати за двома основними характеристиками: виконання центром системи коректно і в повному обсязі наявних до нього вимог; стан захищеності для забезпечення конфіденційності, доступності і цілісності інформації. Для кожної з характеристик введемо показники рівнів безпеки так: $P_{bezp,1}^{centr}(t)$ – рівень функційної безпеки; $P_{bezp,2}^{centr}(t)$ – рівень кібербезпеки. Загальний рівень безпеки центру системи задамо з врахуванням значень для характеристик так:

$$P_{bezp}^{centr}(t) = \alpha_1 \cdot P_{bezp,1}^{centr}(t) + \alpha_2 \cdot P_{bezp,2}^{centr}(t), \qquad (3.41)$$

де α_1 – ваговий коефіцієнт для першого рівня $P_{bezp,1}^{centr}(t)$; α_2 – ваговий коефіцієнт для другого рівня $P_{bezp,2}^{centr}(t)$; $\alpha_1 + \alpha_2 = 1$; t – поточний час; $0 \le P_{bezp,1}^{centr}(t) \le 1$; $0 \le P_{bezp,2}^{centr}(t) \le 1$.

Тоді, критерій щодо безпеки центру системи визначимо так:

$$f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right) = 1 - (\alpha_1 \cdot P_{bezp,1}^{centr}(t) + \alpha_2 \cdot P_{bezp,2}^{centr}(t)). \quad (3.42)$$

Згідно критерію щодо безпеки, який задано за формулою (3.42), приймемо, що кращим з двох значень, які отримано за критерієм, буде менше з двох значень. Для рівня безпеки $P_{bezp}^{centr}(t)$ (формула (3.41)) кращим буде більше з двох значень.

Введемо показники для одного з варіантів детальнішого визначення критерію щодо безпеки центру системи $f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right)$ так:

1) $p_{1,4,kr}^{centr} = t$ – поточний час, в якому здійснено визначення величини $P_{bezp}^{centr}(t)$;

2) $p_{2,4,kr}^{centr} = k_1^{p_{4,kr}^{centr}}$ – загальна кількість завдань, які виконував центр системи за час функціонування системи t;

3) $p_{3,4,kr}^{centr} = k_2^{p_{4,kr}^{centr}}$ – загальна кількість завдань, які виконував центр системи за час функціонування в своєму поточному варіанті централізації;

4) $p_{4,4,kr}^{centr} = k_3^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи виконав повністю за час функціонування системи t;

5) $p_{5,4,kr}^{centr} = k_4^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи виконав повністю за час функціонування в своєму поточному варіанті централізації;

6) $p_{6,4,kr}^{centr} = k_5^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи не зміг виконати за час функціонування системи t;

7) $p_{7,4,kr}^{centr} = k_6^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи не зміг виконати за час функціонування в своєму поточному варіанті централізації;

8) $p_{8,4,kr}^{centr} = k_7^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи продовжує виконувати в поточний момент часу t, включно з початком виконання при попередніх варіантах централізації;

9) $p_{9,4,kr}^{centr} = k_8^{p_{4,kr}^{centr}}$ – кількість завдань, які центр системи продовжує виконувати в своєму поточному варіанті централізації;

10) $p_{10,4,kr}^{centr} = k_9^{p_{4,kr}^{centr}}$ – кількість переходів центру системи до нової архітектури централізації протягом часу t;

11) $p_{11,4,kr}^{centr} = k_{10}^{p_{4,kr}^{centr}}$ – кількість невдалих переходів центру системи до нової архітектури централізації протягом часу t, тобто таких які не відбулися, але розпочинались;

12) $p_{12,4,kr}^{centr} = k_{11}^{p_{4,kr}^{centr}}$ – кількість активних компонент в системі з функціоналом центру системи в поточний момент часу;

13) $p_{13,4,kr}^{centr} = k_{12}^{p_{4,kr}^{centr}}$ – загальна кількість компонент в системі з функціоналом центру системи визначена при останньому переході до нової архітектури централізації;

14) $p_{14,4,kr}^{centr} = k_{13}^{p_{4,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи, але вони не підтвердили свою активність як компоненти центру системи та продовжують функціонувати як частина системи;

15) $p_{15,4,kr}^{centr} = k_{14}^{p_{4,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи в поточний момент часу, які були визначені як активні для участі в роботі центру системи в останньому варіанті централізації, але вони були вимкнені аварійно разом з комп’ютерними станціями, в які встановлені;

16) $p_{16,4,kr}^{centr} = k_{15}^{p_{4,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи протягом всього часу її функціонування від початку роботи до часу t, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені аварійно разом з комп’ютерними станціями, в які встановлені;

17) $p_{17,4,kr}^{centr} = k_{16}^{p_{4,kr}^{centr}}$ – кількість компонент в системі з функціоналом центру системи для поточного варіанту централізації, які були визначені як активні для

участі в роботі центру системи, але вони були вимкнені коректно разом з комп’ютерними станціями, в які встановлені;

18) $p^{centr}_{18,4,kr} = k^{p^{centr}_{4,kr}}_{17}$ – кількість компонент в системі з функціоналом центру системи для всіх варіантів централізації протягом всього часу функціонування системи до часу t, які були визначені як активні для участі в роботі центру системи, але вони були вимкнені коректно разом з комп’ютерними станціями, в які встановлені;

19) $p^{centr}_{19,4,kr} = k^{p^{centr}_{4,kr}}_{18}$ – кількість сегментів в корпоративній мережі, в які встановлено компоненти центру системи;

20) $p^{centr}_{20,4,kr} = k^{p^{centr}_{4,kr}}_{19}$ – загальна кількість сегментів в корпоративній мережі;

21) $p^{centr}_{21,4,kr} = k^{p^{centr}_{4,kr}}_{20}$ – кількість демілітаризованих зон корпоративної мережі;

22) $p^{centr}_{22,4,kr} = k^{p^{centr}_{4,kr}}_{21}$ – кількість демілітаризованих зон корпоративної мережі з компонентами центру системи;

23) $p^{centr}_{23,4,kr} = k^{p^{centr}_{4,kr}}_{22}$ – кількість сегментів в корпоративній мережі з серверними вузлами;

24) $p^{centr}_{24,4,kr} = k^{p^{centr}_{4,kr}}_{23}$ – кількість сегментів в корпоративній мережі з серверними вузлами, в яких розміщені компоненти центру системи;

25) $p^{centr}_{25,4,kr} = k^{p^{centr}_{4,kr}}_{24}$ – кількість поділів центру системи на частини протягом часу функціонування системи;

26) $p^{centr}_{26,4,kr} = k^{p^{centr}_{4,kr}}_{25}$ – кількість поділів центру системи на частини протягом поточного варіанту централізації системи;

27) $p^{centr}_{27,4,kr} = k^{p^{centr}_{4,kr}}_{26}$ – кількість частин системи, в кожній з яких є компоненти з функціоналом центру системи, при тимчасовому поділу системи;

28) $p^{centr}_{28,4,kr} = k^{p^{centr}_{4,kr}}_{27}$ – кількість частин системи, в яких немає активних компонент з функціоналом центру системи, при тимчасовому поділу системи;

29) $p_{29,4,kr}^{centr} = k_{28}^{p_{4,kr}^{centr}}$ – кількість частин системи, в яких є активні компоненти з функціоналом центру системи, при тимчасовому поділу системи;

30) $p_{30,4,kr}^{centr} = t_{29}^{p_{4,kr}^{centr}}$ – час протягом якого система функціонувала без центру системи до поточного часу, який визначено показником $p_{1,4,kr}^{centr} = t$;

31) $p_{31,4,kr}^{centr} = p_{30}^{p_{4,kr}^{centr}}$ – середньоарифметичне значення рівня кібербезпеки комп'ютерної станції з компонентою з центром системи;

32) $p_{32,4,kr}^{centr} = k_{31}^{p_{4,kr}^{centr}}$ – кількість компонент центру системи, які були вилучені з системи через високий рівень інфікування ЗПЗ або в результаті проведеної комп'ютерної атаки на комп'ютерну станцію з відповідною компонентою;

33) $p_{33,4,kr}^{centr} = k_{32}^{p_{4,kr}^{centr}}$ – кількість компонент без центру системи, які були вилучені з системи через високий рівень інфікування ЗПЗ або в результаті проведеної комп'ютерної атаки на комп'ютерну станцію з відповідною компонентою.

34) $p_{34,4,kr}^{centr} = k_{33}^{p_{4,kr}^{centr}}$ – кількість компонент центру системи в поточному варіанті централізації;

35) $p_{35,4,kr}^{centr} = k_{34}^{p_{4,kr}^{centr}}$ – загальна кількість компонент системи.

Згідно введених показників $p_{1,4,kr}^{centr} - p_{35,4,kr}^{centr}$ деталізуємо функцію $f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right)$ для критерію щодо безпеки центру системи так:

$$f_{4,kr}^{centr}\left(p_{4,kr}^{centr}\right) = 1 - \left(\alpha_1 \cdot \frac{k_3^{p_{4,kr}^{centr}} + e}{k_1^{p_{4,kr}^{centr}} + e} \cdot \frac{k_4^{p_{4,kr}^{centr}} + e}{k_2^{p_{4,kr}^{centr}} + e} \cdot \frac{k_6^{p_{4,kr}^{centr}} + e}{k_5^{p_{4,kr}^{centr}} + e} \cdot \frac{k_8^{p_{4,kr}^{centr}} + e}{k_7^{p_{4,kr}^{centr}} + e} \cdot \frac{k_9^{p_{4,kr}^{centr}} - k_{10}^{p_{4,kr}^{centr}} + e}{k_9^{p_{4,kr}^{centr}} + e} \cdot \right.$$

$$\frac{k_{11}^{p_{4,kr}^{centr}} + e}{k_{12}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{11}^{p_{4,kr}^{centr}} + k_{13}^{p_{4,kr}^{centr}} + k_{14}^{p_{4,kr}^{centr}} + k_{16}^{p_{4,kr}^{centr}} + e}{k_{12}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{21}^{p_{4,kr}^{centr}}}{k_{20}^{p_{4,kr}^{centr}}} \cdot \frac{k_{18}^{p_{4,kr}^{centr}}}{k_{19}^{p_{4,kr}^{centr}}} \cdot \frac{k_{23}^{p_{4,kr}^{centr}} + e}{k_{22}^{p_{4,kr}^{centr}} + e} \cdot \frac{k_{25}^{p_{4,kr}^{centr}} + e}{k_{24}^{p_{4,kr}^{centr}} + e} \cdot$$

$$\left. \frac{k_{28}^{p_{4,kr}^{centr}} + e}{k_{26}^{p_{4,kr}^{centr}} + k_{27}^{p_{4,kr}^{centr}} + e} \cdot \frac{t - t_3^{p_{4,kr}^{centr}}}{t} + \frac{\alpha_2}{3} \cdot \left(p_{30}^{p_{4,kr}^{centr}} + \frac{k_{33}^{p_{4,kr}^{centr}} - k_{31}^{p_{4,kr}^{centr}} + e}{k_{33}^{p_{4,kr}^{centr}} + e} + \frac{k_{34}^{p_{4,kr}^{centr}} - k_{31}^{p_{4,kr}^{centr}} - k_{32}^{p_{4,kr}^{centr}} + e}{k_{34}^{p_{4,kr}^{centr}} + e} \right) \right), \quad (3.43)$$

де $e = 0{,}00001$; t – поточний час; α_1 – ваговий коефіцієнт для першого рівня $P_{bezp,1}^{centr}(t)$; α_2 – ваговий коефіцієнт для другого рівня $P_{bezp,2}^{centr}(t)$; $\alpha_1 + \alpha_2 = 1$.

Таким чином, критерій щодо безпеки центру системи може бути визначений за формулою (3.42) з варіантом деталізації згідно формули (3.43) і значення обчислені з його визначення можуть бути використані в цільовій функції (формула (3.28)) оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації. Особливістю визначення критерію щодо безпеки центру системи є врахування рівнів функційної безпеки та кібербезпеки щодо комп'ютерних станцій, в яких розміщені компоненти центру системи. Це дає змогу оцінити поточний стан централізації, врахувати оцінки з попередніх варіантів централізації та використати ці результати для визначення наступного варіанту централізації в системі. Аргументами в функції для критерію щодо безпеки центру системи, які враховані і впливають на результат оцінювання, є кількість компонент, які були вилучені системою в зв'язку з проведеними атаками на комп'ютерні станції, в яких вони знаходяться. Врахування таких показників є важливим в контексті призначення систем класу $\mathfrak{S}$.

Таким чином, в результаті розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання варіантів централізації в системах, особливістю яких є приховування компонент з центром системи від його виявлення зловмисниками.

Розроблені математичні моделі оцінювання центрів систем для вибору наступних варіантів централізації базуються на параметрах, які відображають особливості середовища корпоративних мереж, об'єктів та процесів взаємодії в мультикомп'ютерних системах. Важливим елементом цих математичних моделей є врахування розподілення варіантів централізації за її типами: централізовані; частково централізовані; частково децентралізовані; децентралізовані. Оскільки перехід від поточного варіанту централізації до наступного варіанту в архітектурі систем в межах одного типу централізації може бути здійснено простіше ніж між

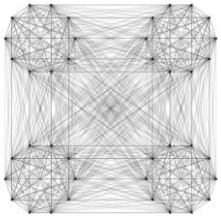
різними типами централізації, то така характеристика впливає на загальну оцінку наступного варіанту централізації. Також, крім критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, важливим елементом системи оцінювання є інформація про попередні стани системи при організації переходів, а також про використовувані правила та час повного завершення переходів. Тобто, в математичні моделі оцінювання наступних варіантів централізації закладено попередній досвід функціонування систем, який подано числовими значеннями. Тому, особливістю рішення щодо розроблених математичних моделей оцінювання наступних варіантів централізації є отримання з їх застосуванням числового значення для визначення наступного варіанту централізації з урахуванням попереднього досвіду використання варіантів централізації в системі та критеріїв, кількість яких може бути різною, включно з їх параметрами. Оцінювання згідно таких моделей можуть бути використанні при розробленні обманних систем, включно з пастками та приманками. Ці моделі, також, розроблені таким чином, що можуть бути модифіковані за потреби. Включені до них параметри можуть бути змінені, розширені або зменшені, що не впливатиме на загальну конструкцію аналітичних виразів. Можливим варіантом щодо параметрів є варіант, при якому параметри моделей можуть бути змінюватись системою в процесі свого функціонування за рахунок врахування нвутрішніх і зовнішніх впливів.

3.5. Метод та правила визначення наступного варіанту централізації в архітектурі мультикомп’ютерних систем

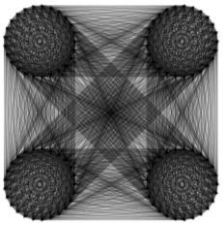
Визначення наступного варіанту централізації в архітектурі вимагає оцінювання можливих варіантів та вибір найкращого варіанту з врахуванням стану системи і середовища корпоративної мережі, зовнішніх впливів та рівня завантаження ресурсів. Але розглядуваних варіантів є дуже багато і оцінювання кожного з них потребує багато часу, що в умовах постійно змінюваного середовища може призвести до втрати актуальності результату вибору. В табл. 3.1 задано фрагмент з можливими варіантами централізації в архітектурі мультикомп’ютерних систем з врахуванням особливостей, які відображені елементами в формулах (3.1)-(3.10), а загальна кількість варіантів

становить більше 2^{31}. Тому, актуальним завданням є розроблення методу визначення наступного варіанту централізації в архітектурі систем класу 𝔖. Він повинен бути розробленим таким чином, щоб його можна було реалізувати в архітектурі систем класу 𝔖, тобто щоб згідно кроків цього методу центр системи визначав потенційні варіанти централізації, витрати ресурсів та час на їх визначення були мінімальними, ці варіанти були б ефективними для подальших кроків системи, в ньому було враховано постійну змінюваність операційного середовища, не використовувався б повний або значний частковий перебір всіх варіантів, а також щоб був врахований попередній досвід з вибору попередніх варіантів.

Якщо розподілити всі варіанти централізації в архітектурі систем класу 𝔖 за чотирма типами (централізована, частково централізована, частково децентралізована, децентралізована) в окремі класи, кожен клас подати багатокутником з кількістю вершин відповідною кількості варіантів і встановити з'єднання між усіма вершинами в багатокутниках та між ними, то отримаємо модель варіантів централізації згідно станів, які подані вершинами. Кожна вершина багатокутника буде відповідати винятково за один варіант централізації в архітектурі класу 𝔖. Встановлені зв'язки між вершинами відповідають за переходи між варіантами централізації. Оскільки між будь-якою парою вершин встановлені зв'язки, то перехід можливий з будь-якого варіанту централізації до будь-якого варіанту. Але при врахуванні особливостей поточного стану в системі не всі варіанти будуть рівноцінними для переходу в них, тому потрібні правила, згідно яких будуть визначені перспективні варіанти для переходу. На рис. 3.5 зображено чотири багатокутники і всі вершини їх між собою з'єднані. На рис.3.5 а) зображено варіант з чотирма 10-кутниками, а на рис. 3.5 б) – 25-кутник. Багатокутники можуть мати для кожного класу різну кількість вершин.



а) 10-кутники



б) 25-кутники

Рисунок 3.5 – Стани централізації в архітектурі систем класу 𝔖

Таким чином, варіантів для переходу від одного варіанту централізації до іншого багато. Центр системи міг би вибирати наступний варіант централізації за однією із стратегій. Наприклад, вибирати з того ж класу типів централізації, обов'язково з іншого класу варіантів централізації тощо. Але використання такого підходу до вибору наступного варіанту централізації в системі для розглядуваного типу систем класу $\mathfrak{S}$ не підходить, оскільки поведінка таких систем та їх реакція на впливи повинна бути непередбачуваною та такою, щоб зловмисник не зміг її вивчити. Взагалі відповідь повинна бути ефективною, тобто варіант централізації, і, при цьому, бути поліморфною. Під поліморфною відповіддю системи визначатимемо відповідь системи, яка при однакових впливах надаватиме ефективні відповіді на впливи, зокрема близькі або однакові за змістом чи суттю, але кроки з яких буде сформовано відповідь, та їх послідовність повинні бути різними. Тобто, при кожному однаковому впливі, які повторюють з певною періодичність або через певний час, система буде на однакові впливи надавати відповідь, кроки досягнення якої будуть різними.

Враховуючи необхідність врахування центром системи результативності попередніх варіантів централізації в архітектурі систем, тобто врахування попереднього періоду функціонування систем в частині використання різних варіантів централізації як сформованого досвіду, введемо функцію оцінювання попередніх варіантів централізації так:

$$\mathrm{F}_{\mathrm{OD}}^{\mathrm{centr}}\left(\mathrm{V}_{\mathrm{Pr,potochn}}, M_{\mathrm{V_{Pr}}}, P'_{Pr}\right) \to [0,1], \tag{3.44}$$

де $\mathrm{V}_{\mathrm{Pr,potochn}}$ – вектор (формула (3.13)), який задає стан системи в поточний момент часу і наявний в матриці станів $M_{\mathrm{V_{Pr}}}$; $M_{\mathrm{V_{Pr}}}$ – матриця станів (формула (3.14)) системи в частині організації централізації; P'_{Pr} – множина показників (формула (3.16)), які характеризують поточний стан системи та процеси в ній в момент перед переходом системи до іншого варіанту централізації.

Значення функції $\mathrm{F}_{\mathrm{OD}}^{\mathrm{centr}}$ буде оцінено числом з проміжку $[0,1]$. Більшому значенню функції $\mathrm{F}_{\mathrm{OD}}^{\mathrm{centr}}$ з двох значень буде відповідати краще значення. Аргументи $\mathrm{V}_{\mathrm{Pr,potochn}}, M_{\mathrm{V_{Pr}}}, P'_{Pr}$ в функції $\mathrm{F}_{\mathrm{OD}}^{\mathrm{centr}}$ будуть надавати результати функціонування системи з певним варіантом централізації і значення в них будуть містити накопичені на момент завершення поточного варіанту централізації, тобто перед початком

переходу до наступного варіанту централізації, значення, які будуть формувати досвід системи в частині централізації. Фактично функція F_{OD}^{centr} є функцією винагороди кожного варіанту централізації в архітектурі системи. Якщо варіант централізації повторився декілька разів протягом певного часу функціонування системи, то будемо використовувати для різних за часом періодів функціонування системи з одним і тим же варіантом централізації його середньоарифметичне значення за умови різниці між такими значеннями, що буде менше певного порогового значення (наприклад, 1%). Якщо ж значення будуть відрізнятись більше ніж на встановлене порогове значення, тоді вони повинні бути оцінені поточним центром системи на предмет впорядкованості за зростанням, тобто щодо покращення функціонування системи з таким центром в наступному його використанні. Якщо так, тоді ці значення фіксуються, як окремі значення. Якщо ж друге значення буде меншим за перше значення, тоді такий варіант централізації в подальшому не буде вибиратись системою, а значення фіксуються в системі. Якщо функцією F_{OD}^{centr} оцінюються варіанти централізації в системі, які ще не використовувались, то її значення для них дорівнює нулеві.

До визначення значення функції F_{OD}^{centr} для кожного варіанту централізації в системі, які були використані, додамо функцію $F_{OD,t}^{centr}$, яка відображатиме час кожного використаного варіанту централізації в системі на основі вектору стану системи в поточний момент часу (формула (3.13)). Тоді, для кожного варіанту централізації по його завершенню використання в системі буде зафіксовано два значення: оцінка результативності; час перебування системи в такому варіанті централізації.

Також, додамо до характеристики використаного варіанту централізації в системі таку числову характеристику як кількість використаних спроб певного варіанту централізації. Задамо визначення її значення функцією $F_{OD,k}^{centr}$, аргументом якої буде номер варіанту централізації в системі.

Таким чином, з використанням функції оцінювання результативності попередніх варіантів централізації в архітектурі систем, часу кожного використаного варіанту централізації та кількості використаних спроб певного варіанту централізації буде накопичуватись інформація про попередній період функціонування систем в частині

використання різних варіантів централізації. Нею буде задаватись частина досвіду системи разом з його оцінкою результативності та часу перебування.

При виборі наступного варіанту централізації в системі потрібна функція, яка визначатиме можливість переходу до наступного варіанту централізації. Наприклад, система в процесі функціонування визначилась щодо наступного варіанту централізації, після чого розподілилась на дві незв'язні частини або частина компонент, які планувались для подальшого використання з функціоналом центру вимкнули, тоді запланована перебудова центру буде неможлива. Таким чином, ця функція визначатиме стан системи щодо спроможності реалізувати перехід після всіх дій з підготовки переходу. Вона буде враховувати поточну інформацію про компоненти системи. Задамо її так:

$$\mathrm{F}_{\mathrm{P}}^{\mathrm{centr}}\left(\mathrm{V}_{\mathrm{Pr,potochn}}, \mathrm{V}_{\mathrm{Pr,nast}}, M_{\mathrm{V_{Pr}}}, P_{Pr}, A^{\mathfrak{S}}\right) = \begin{cases} 0, \text{перехід неможливий;} \\ 1, \text{перехід можливий,} \end{cases} \quad (3.45)$$

де $\mathrm{V}_{\mathrm{Pr,potochn}}$ – вектор (формула (3.13)), який задає стан системи в поточний момент часу і наявний в матриці станів $M_{\mathrm{V_{Pr}}}$; $M_{\mathrm{V_{Pr}}}$ – матриця станів (формула (3.14)) системи в частині організації централізації; $\mathrm{V}_{\mathrm{Pr,nast}}$ - вектор (формула (3.13)), який задає очікуваний наступний стан системи; P'_{Pr} – множина показників (формула (3.16)), які характеризують поточний стан системи та процеси в ній в момент перед переходом системи до іншого варіанту централізації; $A^{\mathfrak{S}}$ – *множина компонент системи*.

Для уникнення повного перебору при виборі варіантів централізації в архітектурі систем класу $\mathfrak{S}$ необхідно використати стратегії вибору елементів для формування варіанту централізації. Введемо множину стратегій $\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}} = \left\{\mathrm{m}_{\mathrm{str,nast},1}^{\mathrm{centr}}, \mathrm{m}_{\mathrm{str,nast},2}^{\mathrm{centr}}, \ldots, \mathrm{m}_{\mathrm{str,nast,N}_{\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}}}^{\mathrm{centr}}\right\}$, де $\mathrm{N}_{\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}}$ – кількість стратегій вибору наступного варіанту централізації. Наприклад, елементи множини стратегій $\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}$можуть бути такими: $\mathrm{m}_{\mathrm{str,nast},1}^{\mathrm{centr}}$ – найбільше значення *цільової функції* $\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}$ оцінювання наступних варіантів централізації зі всіх раніше розглядуваних та використаних варіантів; $\mathrm{m}_{\mathrm{str,nast},2}^{\mathrm{centr}}$ – найменше значення *цільової функції* $\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}$ оцінювання наступних варіантів централізації зі всіх раніше розглядуваних та використаних варіантів; $\mathrm{m}_{\mathrm{str,nast},3}^{\mathrm{centr}}$ – випадковим чином згенероване число, яке не

більше кількості всіх можливих варіантів; $m_{str,nast,4}^{centr}$ – значення *цільової функції* F_{kr}^{centr} дорівнює нулеві; $m_{str,nast,5}^{centr}$ – варіант централізації, який отримується з попереднього варіанту заміною одного елемента в одній з множин заданих формулами (3.1)-(3.10); $m_{str,nast,6}^{centr}$ – варіант централізації, який отримується з попереднього варіанту заміною одного елемента в двох множинах заданих формулами (3.1)-(3.10); $m_{str,nast,7}^{centr}$ – варіант централізації, який отримується з попереднього варіанту заміною одного елемента в трьох множинах заданих формулами (3.1)-(3.10); $m_{str,nast,8}^{centr}$ – варіант централізації, який отримується з поточного варіанту заміною одного елемента в чотирьох множинах заданих формулами (3.1)-(3.10) тощо. Стратегій визначення наступного варіанту централізації може бути багато, але оптимальними з них є ті, які надають один варіант без використання повного чи часткового перебору з усіх можливих варіантів та без пошуку найбільшого чи найменшого значення певних функцій, оскільки для виконання таких дій витрачаються обчислювальні ресурси та час. Але варіанти з використанням значень цільової функції можуть бути, якщо забезпечити сортування її значень для вже використаних варіантів централізації. Важливою особливістю при виборі наступного варіанту централізації, тобто фактично його побудови, є одночасне задання варіанту безпосередньо самою стратегією вибору, як наприклад в стратегіях $m_{str,nast,5}^{centr} - m_{str,nast,8}^{centr}$ та типових до них. Такі стратегії дають змогу формувати варіант централізації з дуже близькими характерними властивостями, більш близькими, менш близькими та протилежними.

Також, необхідно враховувати кількість застосувань стратегій, щоб уникнути застосування декількох або однієї стратегії постійно. Тому, введемо функцію для визначення кількості застосувань конкретної стратегії так:

$$F_{str,K}^{centr}\left(m_{str,nast,m}^{centr}\right) = k_m, \tag{3.46}$$

де $m_{str,nast,m}^{centr}$ – m-тий елемент множини стратегій $M_{str,nast}^{centr}$; $m = 1,2,\dots,N_{M_{str,nast}^{centr}}$; $N_{M_{str,nast}^{centr}}$ – кількість стратегій вибору наступного варіанту централізації; k_m – кількість застосувань певної m - стратегії вибору варіанту централізації.

Врахування вибору самих стратегій при виборі наступного варіанту в контексті їх впливу на результат функціонування системи та її центру враховано в цільовій

функції оціненим значенням функціонування системи з таким центром, тому окремо враховувати вибір стратегії як складову частину, яка впливатиме на функціонування системи і її центру, не доцільно, бо буде дублювання цього показника.

Поточний центр системи при вирішенні замінити його на інший повинен для вибору контролером системи підготувати п’ять варіантів. Такими варіантами можуть бути такі: найближчий варіант централізації до поточного, тобто варіант тієї ж архітектури, що і поточна архітектура центру системи; три варіанти з решти трьох типів централізації в архітектурі системи; варіант, в якому відсутні всі елементи множин, з яких сформовано поточний варіант централізації. Решту завдань, які може виконувати система, опрацьовує центр системи або визначені ним компоненти системи і так само для них готується 3-5 рішень щодо конкретної відповіді на відповідні впливи або періоди в функціонуванні системи.

Визначимо показники, які необхідно використати при визначенні наступного варіанту централізації згідно правил, які задано множиною правил $\mathbf{M_{Pr}}$ за формулою (3.11), в системах класу $\mathfrak{S}$, так:

1) поділ правил на групи (g_l^{centr}, $l = 1,2,3$) за результатом переходу до наступного обраного стану та формуванням нових правил з використанням матриці M_{Pr}^1 (формула (3.17), яка містить інформацію про тип правила, час застосування правила за умови виконання згідно нього переходу, номер правила з множини правил $\mathbf{M_{Pr}}$;

2) функція $F^{M_{Pr}}$ переходу з поточного стану до наступного стану, яку визначено за формулою (3.15), з фіксуванням поточного стану вектором $V_{Pr,potochn}$ та визначення наступного стану вектором $V_{Pr,nast}$;

3) множини, якими задані характерні властивості варіантів централізації і які задано за формулами (3.1)-(3.10);

4) стан системи, який визначено вектором $V_{Pr,i}$ за формулою (3.13) і матрицею $M_{V_{Pr}}$ станів системи за формулою (3.14);

5) множина P_{Pr} показників, які характеризують поточний стан системи та процеси в ній, задана формулою (3.16);

6) множина $A^{\mathfrak{S}}$ (формула (3.18)) задання систем класу $\mathfrak{S}$ переліком компонент;

7) поділ компонентів з множини $A^{\mathfrak{S}}$ на дві підмножини (формули (3.19), (3.20));

8) цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації (формула (3.28)) згідно критеріїв щодо оперативності, стійкості, цілісності, безпеки центру системи;

9) час t функціонування системи від початку її запуску;

10) час $F_{OD,t}^{centr}$ кожного використаного варіанту централізації в системі;

11) функція F_{OD}^{centr} винагороди кожного варіанту централізації в архітектурі системи;

12) функція $F_{OD,k}^{centr}$ кількості використаних спроб певного варіанту централізації та функція $F_{OD,z}^{centr}$ кількості всіх варіантів централізації, які були в системі за час t, причому однакові варіанти централізації в різний час вважатимемо різними для обчислення значення функції $F_{OD,z}^{centr}$;

13) кількість активних компонент N_A^{centr} в системі від загальної кількості компонент, в яких наявний центр в поточний момент функціонування системи та може бути центр системи за наступного варіанту централізації;

14) функція F_P^{centr}, яка відображає неможливість поєднання певних характерних властивостей, тобто яка вилучає варіанти з усіх розглядуваних варіантів;

15) номер $(n_s^{centr},\ s = 1, \dots, 4)$ типу архітектури централізації (n_1^{centr} – *централізована;* n_2^{centr} – частково централізована; n_3^{centr} – частково децентралізована; n_4^{centr} – децентралізована);

16) множина стратегій $M_{str,nast}^{centr}$ вибору елементів для формування варіанту централізації та кількість їх попередніх застосувань

Задамо правила з множини правил M_{Pr} (формула (3.11)), згідно яких буде визначатись наступний варіант централізації в системах класу $\mathfrak{S}$, з урахуванням показників, заданих в пунктах 1) - 16) так:

$$m_{Pr,s} = (s = 1, \dots, 4)$$

$$\forall A^{\mathfrak{S}}: ((g_1^{centr} = \text{true}) \text{ and } (g_2^{centr} = \text{false}) \text{ and } (g_3^{centr} = \text{false})) \text{ and}$$

$$(V_{Pr,potochn} \neq V_{Pr,nast}: \exists j\ F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,j}, potochn) \neq F_{Pr}(m_{\mathfrak{B}_2,centr,v_l,j}, nast)) \text{ and}$$

$$(\{m_{\mathfrak{B}_2,centr,v_1,j_1}\} \cup \{m_{\mathfrak{B}_2,centr,v_2,j_2}\} \cup \{m_{\mathfrak{B}_2,centr,v_3,j_3}\} \cup$$

$\{m_{\mathfrak{V}_2,centr,v_4,j_4}\} \cup \{m_{\mathfrak{V}_2,centr,v_5,j_5}\} \cup \{m_{\mathfrak{V}_2,centr,v_6,j_6}\} \cup \{m_{\mathfrak{V}_2,centr,v_7,j_7}\} \cup \{m_{\mathfrak{V}_2,centr,v_8,j_8}\} \cup \{m_{\mathfrak{V}_2,centr,v_9,j_9}\} \cup \{m_{\mathfrak{V}_2,centr,v_{10},j_{10}}\})$ and $(V_{Pr,potochn} = V_{Pr,N_{V_{Pr}}}$, тобто $\forall$ j : $F_{Pr}(m_{\mathfrak{V}_2,centr,v_l,j}, potochn) = F_{Pr}(m_{\mathfrak{V}_2,centr,v_l,j}, N_{V_{Pr}}))$ and $(\{p_{Pr,1}\} \cup \{p_{Pr,2}\} \cup \ldots \cup \{p_{Pr,N_{P_{Pr}}}\})$ and $(\{A^{\mathfrak{S}}_{1,1}, A^{\mathfrak{S}}_{1,2}, \ldots, A^{\mathfrak{S}}_{1,N_{1,A^{\mathfrak{S}}}}\} \cup \{A^{\mathfrak{S}}_{2,1}, A^{\mathfrak{S}}_{2,2}, \ldots, A^{\mathfrak{S}}_{2,N_{2,A^{\mathfrak{S}}}}\})$ and $(0 \le F^{centr}_{kr} \le 1)$ and $(F^{centr}_{OD}(V_{Pr,nast2}, M_{V_{Pr}}, P'_{Pr}) \ge F^{centr}_{OD}(V_{Pr,nast1}, M_{V_{Pr}}, P'_{Pr}))$ *and* $(0 \le F^{centr}_{OD}(V_{Pr,nast}, M_{V_{Pr}}, P'_{Pr}) \le 1)$ and $((F^{centr}_{OD,t}(V_{Pr,nast}) = 0)$ or $\frac{t-(F^{centr}_{OD,t}(V_{Pr,nast})}{t} \le e_1^{centr})$ and $((F^{centr}_{OD,k} = 0)$ or $(\frac{F^{centr}_{OD,k}}{F^{centr}_{OD,z}} \le e_1^{centr}))$ and $(N^{centr}_{A} \ge 2)$ and $(F^{centr}_{P}(V_{Pr,potochn}, V_{Pr,nast}, M_{V_{Pr}}, P_{Pr}, A^{\mathfrak{S}}) = 1)$ and $(\frac{N^{centr}_{A}}{N} \ge e_1^{centr})$ and $((n^{centr}_{s,potochn} = n^{centr}_{s,nast})$ or $((n^{centr}_{s,potochn} \ne n^{centr}_{s',nast}$ and s = 1, … ,4 and $s' = 1, \ldots, 4$ *and* $s' \ne$ s) and $n^{centr}_{s',nast}))$ *and* $(\frac{k_m}{\sum_{m=1}^{N_{M^{centr}_{str,nast}}} k_m} \le e_2^{centr}) \Rightarrow V_{Pr,nast}$;

$m_{Pr,5}$ = $\forall A^{\mathfrak{S}}$: $((g^{centr}_1 = false)$ and $(g^{centr}_2 = true)$ and $(g^{centr}_3 = false)) \Rightarrow m_{Pr,s}$ and $V_{Pr,nast'} \ne V_{Pr,nast}$: $\exists$ j $F_{Pr}(m_{\mathfrak{V}_2,centr,v_l,j}, nast') \ne F_{Pr}(m_{\mathfrak{V}_2,centr,v_l,j}, nast)) \Rightarrow V_{Pr,nast}$;

$m_{Pr,6}$ = $\forall A^{\mathfrak{S}}$: $((g^{centr}_1 = false)$ and $(g^{centr}_2 = false)$ and $(g^{centr}_3 = true))$ and $(e_3^{centr} > 2)$ and mod $(m_{Pr,1}$ *or* $m_{Pr,2}$ or $m_{Pr,3}$ *or* $m_{Pr,4}$ or $m_{Pr,5})$,

де g_l^{centr} – група правил ($l = 1,2,3$); $m_{Pr,i}$ – і-те правило вибору варіанту централізації в мультикомп'ютерних системах; $i = 1,2, \ldots, N_{M_{Pr}}$; $N_{M_{Pr}}$ – кількість правил в множині правил M_{Pr}; де l – кількість множин ($l = 1,2, \ldots 10$); j_l-тий елемент в множині $M_{\mathfrak{V}_2,centr,l}$; i – номер стану системи; $V_{Pr,potochn}$ – вектор, який задає стан системи в поточний момент часу і наявний в матриці станів $M_{V_{Pr}}$; $M_{V_{Pr}}$

– матриця станів системи в частині організації централізації; $\mathrm{M_{Pr}}$ – множина правил; $\mathrm{V_{Pr,nast}}$ – вектор, який задає наступний стан системи в поточний момент часу; P_{Pr} – множина показників, які характеризують поточний стан системи та процеси в ній; $p_{Pr,i} - i$ – тий показник ($i = 1,2, \dots, \mathrm{N}_{P_{Pr}}$), що характеризує поточний стан системи та процеси в ній; $\mathrm{N}_{P_{Pr}}$ – кількість показників, які характеризують поточний стан системи та процеси в ній і впливають на зміну варіанту централізації в системі; $A_{1,i}^{\mathfrak{S}} - i$-та компонента ($i = 1,2, \dots, N_{1,A^{\mathfrak{S}}}$) підмножини $A_1^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$; $N_{1,A^{\mathfrak{S}}}$ – кількість елементів в підмножині $A_1^{\mathfrak{S}}$; $A_{2,j}^{\mathfrak{S}}$ – j-та компонента ($j = 1,2, \dots, N_{2,A^{\mathfrak{S}}}$) підмножини $A_2^{\mathfrak{S}}$ системи $A^{\mathfrak{S}}$ класу $\mathfrak{S}$; $N_{2,A^{\mathfrak{S}}}$ – кількість елементів в підмножині $A_2^{\mathfrak{S}}$; $N_{A^{\mathfrak{S}}} = N_{1,A^{\mathfrak{S}}} + N_{2,A^{\mathfrak{S}}}$; $\mathrm{nast1}, \mathrm{nast2}$ – номери останніх однакових варіантів централізації в архітектурі системи, яка може бути знову в наступному варіанті; $s' = 1, \dots, 4$; $\mathrm{m}_{\mathrm{str,nast,m}}^{\mathrm{centr}}$ – m-тий елемент множини стратегій $\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}$; $\mathrm{m} = 1,2, \dots, \mathrm{N}_{\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}}$; $\mathrm{N}_{\mathrm{M}_{\mathrm{str,nast}}^{\mathrm{centr}}}$ – кількість стратегій вибору наступного варіанту централізації; $\mathrm{k_m}$ – кількість застосувань певної m – стратегії вибору варіанту централізації; $\mathrm{V}_{\mathrm{Pr},nast'}$ - вектор наступного варіанту централізації, до якого система не змогла перейти, тобто варіант який не відбувся; mod – функція зміни елементів в аргументі-правилі; $e_1^{centr} = 0{,}25$ – перше порогове значення; $e_2^{centr} = 0{,}1$ – друге порогове значення; $e_3^{centr} = 2$ – третє порогове значення.

Отримані правила дають змогу системам класу $\mathfrak{S}$ визначати самостійно наступний варіант централізації. При цьому, в правилах враховано не тільки успішний перехід системи до наступного варіанту централізації, але і варіант, коли система не змогла здійснити перехід до наступного варіанту централізації. Також, система може вибрати правило з третьої групи правил, коли тривалий час на неї здійснюються впливи і попередні варіанти правил не можуть забезпечити формування її центру таким чином, щоб стабілізувати її функціонування. Модифікація базових правил здійснюється за рахунок часткової або повної зміни їх параметрів. Розроблені правила враховують специфіку систем класу $\mathfrak{S}$, які є розподіленими та призначені для функціонування при зловмисних впливах самостійно без втручання адміністратору.

Згідно отриманих правил задамо основні кроки методу визначення наступного варіанту централізації в системах класу $\mathfrak{S}$ так:

1) настання подій (отримання впливів або вказівок) для початку зміни архітектури системи;

2) якщо контролером системи затверджено рішення щодо зміни варіанту централізації в системі, то перехід до кроку 3), інакше перехід до кроку 9);

3) визначення типу події та встановлення для класу правила;

4) якщо подія щодо зміни варіанту централізації в системі передбачає плановий перехід, то застосовувати правила $m_{Pr,s}$ $(s = 1, \dots, 4)$ для підготовки п’яти варіантів централізації;

5) якщо подія щодо зміни варіанту централізації в системі пов’язана з тим, що перехід до наступного варіанту централізації в системі не відбувся або не може бути завершеним, то застосовувати правило $m_{Pr,5}$ для підготовки п’яти варіантів централізації;

6) якщо подія щодо зміни варіанту централізації в системі пов’язана з тим, що перехід до наступного варіанту централізації в системі не відбувся або не може бути завершеним тривалий час і багатократне застосування (перевищення порогового значення) правила $m_{Pr,5}$ не дало результату, то застосовувати правило $m_{Pr,6}$ для підготовки п’яти варіантів централізації;

7) якщо успішно виконано один з кроків 4)-6), то перехід до кроку 8), інакше залишатись в поточному стані і розпочати виконання кроку 1);

8) передача контролера п’яти потенційних варіантів централізації в системі для затвердження наступного варіанту централізації;

9) перехід до визначення варіанту зміни решти архітектури в системі, яка не містить центру системи.

Суть методу визначення наступного варіанту централізації в системах класу $\mathfrak{S}$ полягає у використанні правил, які забезпечують уникнення часткового або повного перебору варіантів з можливих варіантів централізації, за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, що дає змогу згідно правил вибору варіанта централізації

здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і підібрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі.

Таким чином, розроблено метод визначення варіанту централізації в системах класу $\mathfrak{S}$, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, що дає змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і підібрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного перебору всіх варіантів в динамічно змінюваному середовищі.

3.6. Висновки до третього розділу

Здійснено подання характерних властивостей варіантів централізації в системах класу $\mathfrak{S}$ множинами та встановлено кількість їх можливих варіантів. Отриманий результат щодо кількості варіантів відображає потенційну складність при здійсненні вибору наступного варіанту централізації. Розроблене подання через характерні властивості необхідне для формування правил визначення наступного варіанту централізації в архітектурі систем класу $\mathfrak{S}$. Обрунтовано поділ правил на три групи, що дало змогу відобразити особливості їх застосування в поточний момент функціонування системи з врахуванням подій, які відбуваються в системі при виконанні нею завдань, зокрема і зміни варіанту централізації.

Встановлено загальну кількість різних варіантів формування центру системи, які є прийнятними для використання в системах класу $\mathfrak{S}$. Застосування такої стратегії в контексті формування центру системи в її компонентах усуває обмеження та дозволяє центру системи підібрати наступний варіант свого розміщення і варіанту архітектури.

Це дає змогу створювати проблеми зловмисникам у виявленні компонент з центром системи та встановленні типу архітектури централізації з метою розуміння ним принципів її функціонування.

Розроблено математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які подані аналітичними виразами та враховують особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах.

Розроблено метод визначення варіанту централізації в системах класу $\mathfrak{S}$, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, що дало змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і підібрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного та значного часткового перебору всіх варіантів в змінюваному середовищі корпоративних мереж.

Основні наукові результати опубліковані в працях [107, 170, 290, 291, 293].

РОЗДІЛ 4.
МЕТОДИ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ КОНТРОЛЕРА **ПРИЙНЯТТЯ РІШЕНЬ** ТА МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ

Характерні властивості мультикомп'ютерних систем, які задано в концептуальній моделі за формулою (2.30) та які відображено множинами за формулами (3.1) - (3.2), повинні бути враховані при організації функціонування таких систем. В концептуальній моделі мультикомп'ютерних систем прийняття рішень щодо подальших кроків системи, виконання завдань тощо виділено в дві окремі частини: центр системи; контролер прийняття рішень. Центр системи призначений для підготовки варіантів відповіді систем на внутрішні і зовнішні події, щодо подальших кроків систем, щодо наступного варіанту централізації в архітектурі систем тощо. Кількість цих варіантів повинна бути більше одного варіанту. Контролер прийняття рішень з врахуванням попереднього досвіду функціонування систем та вирішення завдань в системах повинен прийняти рішення щодо вибору одного варіанту із запропонованих центром системи. Причому, на одні і ті ж впливи, особливо коли вони однаково повторювані за певний проміжок часу, контролер повинен підібрати варіант відповіді системи, який не обов'язково повинен бути таким, що вже був при такому ж впливі чи події. Тобто, контролер прийняття рішень повинен реагувати не стандартно на однакові події. Це необхідно реалізувати в системах класу $\mathfrak{S}$ враховуючи їх спрямування щодо попередження, виявлення та протидії ЗПЗ та КА в корпоративних мережах. Зловмисники, які можуть діяти як з середини так і ззовні корпоративної мережі, не повинні розуміти принципів функціонування систем з метою уникнення можливості їх вивчення для проникнення в корпоративні мережі.

Складність при реалізації систем класу $\mathfrak{S}$ полягає в тому, щоб при формуванні поліморфної відповіді від них на впливи, прийняті рішення дії були найбільш коректними і ефективними, враховуючи покладену на них самостійність в прийнятті рішень. Тому, організація їх функціонування та роботи контролера прийняття рішень потребують розроблення відповідних методів, які повинні забезпечити їх коректне функціонування та уникнення вивчення принципів їх функціонування

зловмисниками. Тоді, такі системи стали б основою для втілення в них різноспрямованих спеціалізованих методів з попередження, виявлення та протидії ЗПЗ та КА, включно з використанням приманок та пасток.

4.1. Метод організації функціонування контролера прийняття рішень

Функціонування контролера прийняття рішень в архітектурі систем класу 𝔖 є визначальним саме для цього класу систем і потребує розроблення методу організації такого функціонування, яке включатиме безпосередньо внутрішні дії в ньому, взаємодію з центром системи та взаємодію із елементами та компонентами систем. Розглянемо місце контролера прийняття рішень в архітектурі систем класу 𝔖 та його завдання.

Центр системи готує для визначених завдань, які може розв’язувати в системі, від трьох до п’яти варіантів відповідей з урахуванням попереднього досвіду функціонування системи, зокрема і можливості повторення певних варіантів та їх урізноманітнення. Контролер прийняття рішень отримує від центру системи запропоновані ним варіанти відповідей для виконання завдань, які виникли під час функціонування системи. Подальші дії контролера прийняття рішень полягають у визначенні лише одного варіанту для використання в системі при виконанні завдання. При цьому вибір єдиного варіанту здійснюється з врахуванням попереднього досвіду функціонування системи з використанням цього варіанту, якщо він вже був раніше, та решти варіантів. Контролер прийняття рішень, також, незалежно від центру системи враховує кількість активних компонент систем та їх розміщення у вузлах в комп’ютерних мережах, значення критеріїв оцінювання варіантів та цільової функції. Після затвердження єдиного варіанту, тобто наступних кроків системи для виконання завдання, контролер передає результат центру системи для фіксування і використання на наступному кроці підготовки варіантів виконання такого ж завдання. Центр системи після отримання відповіді від контролера запускає процес виконання завдання. Центр системи взаємодіє з контролером прийняття рішень згідно схеми зображеної на рис. 4.1.

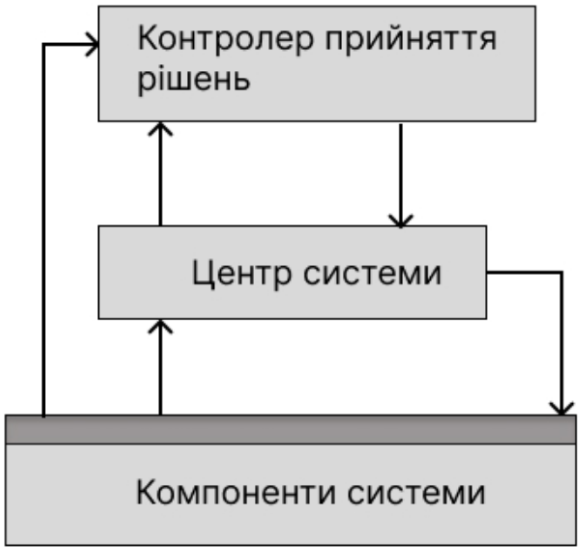


Рисунок 4.1 - Схема взаємодії контролера прийняття рішень та центру системи

Завдання, які можуть виконувати системи класу $\mathfrak{S}$, задамо множиною завдань системи $M_{pz}^{\mathfrak{S}}$ так:

$$M_{pz}^{\mathfrak{S}} = \left\{ m_{pz,1}^{\mathfrak{S}}, m_{pz,2}^{\mathfrak{S}}, \dots, m_{pz,N_{M_{pz}^{\mathfrak{S}}}}^{\mathfrak{S}} \right\}, \quad (4.1)$$

де $m_{pz,i}^{\mathfrak{S}}$ – i-те завдання; $i = 1,2, \dots, N_{M_{pz}^{\mathfrak{S}}}$; $N_{M_{pz}^{\mathfrak{S}}}$ – кількість завдань, які може виконувати система.

Кількість завдань, на виконання яких організовано системи класу $\mathfrak{S}$, може бути змінена в процесі їх функціонування. Виконання частини завдань може бути заблоковано в результатів зовнішніх і внутрішніх впливів на системи класу $\mathfrak{S}$ або в результаті контрольованого зменшення адміністратором. Також, кількість завдань може бути збільшено адміністраторами систем класу $\mathfrak{S}$. Тобто, кількість завдань для систем класу $\mathfrak{S}$ є динамічно змінюваною. Деталізуємо перелік основних завдань систем класу $\mathfrak{S}$ без завдань спрямованих на початкове формування систем так:

1) $m_{pz,1}^{\mathfrak{S}}$ – планова перебудова архітектури систем класу $\mathfrak{S}$;

2) $m_{pz,2}^{\mathfrak{S}}$ – перебудова архітектури систем класу $\mathfrak{S}$, яка викликана зовнішніми впливами;

3) $m_{pz,3}^{\mathfrak{S}}$ – перебудова архітектури систем класу $\mathfrak{S}$, яка викликана внутрішніми впливами;

4) $m_{pz,4}^{\mathfrak{S}}$ – вибір наступного варіанту централізації в архітектурі систем класу $\mathfrak{S}$;

5) $m_{pz,5}^{\mathfrak{S}}$ – опрацювання подій, які викликано зовнішніми впливами;

6) $m_{pz,6}^{\mathfrak{S}}$ – опрацювання подій, які викликано внутрішніми впливами;

7) $m_{pz,7}^{\mathfrak{S}}$ – перебудова зв'язків в компонентах систем поза їх центру;

8) $m_{pz,8}^{\mathfrak{S}}$ – активізація окремих приманок та пасток в системах класу $\mathfrak{S}$;

9) $m_{pz,9}^{\mathfrak{S}}$ – активізація комбінованих антивірусних приманок та пасток в системах класу $\mathfrak{S}$;

10) $m_{pz,10}^{\mathfrak{S}}$ – вимкнення частини компонент в системах класу $\mathfrak{S}$;

11) $m_{pz,11}^{\mathfrak{S}}$ – опрацювання результатів роботи приманок та пасток в системах класу $\mathfrak{S}$;

12) $m_{pz,12}^{\mathfrak{S}}$ – вибір наступних компонент для центру системи;

13) $m_{pz,13}^{\mathfrak{S}}$ – вибір наступних компонент для контролера прийняття рішень;

14) $m_{pz,14}^{\mathfrak{S}}$ – опрацювання подій, які пов'язані з аварійним вимкненням комп'ютерних станцій з компонентами системи;

15) $m_{pz,15}^{\mathfrak{S}}$ – долучення компонент систем класу $\mathfrak{S}$ після увімкнення комп'ютерних станцій з компонентами та призначення їм відповідного статусу для виконання завдань;

16) $m_{pz,16}^{\mathfrak{S}}$ – видалення компонент систем класу $\mathfrak{S}$ після коректного ввимкнення комп'ютерних станцій з компонентами та передача їх функцій з виконання завдань іншим компонентам;

17) $m_{pz,17}^{\mathfrak{S}}$ – формування системи разом з центром та контролером в окремій незв'язній частині всієї системи в результаті її розпаду;

18) $m_{pz,18}^{\mathfrak{S}}$ – формування системи разом з центром та контролером з окремих незв'язних частин всієї системи в результаті встановлення зв'язку між частинами і перехід її в цілісну систему;

19) $m_{pz,19}^{\mathfrak{S}}$ – встановлення аварійного стану всієї системи чи її частин;

20) $m_{pz,20}^{\mathfrak{S}}$ – встановлення штатного режиму роботи всієї системи чи її частин.

При початковому формуванні систем класу $\mathfrak{S}$ в корпоративних мережах адміністратор встановлює компоненти у визначені вузли мережі та призначає одну з компонент для центру системи. На цьому першому етапі контролер прийняття рішень буде активним в тій же компоненті, що й центр системи. В подальшому функціонуванні систем класу $\mathfrak{S}$ контролер може бути в різних компонентах, зокрема і в активних компонентах з центром системи.

Для кожного із завдань, які може виконувати система і які задано елементами множини завдань системи $M_{pz}^{\mathfrak{S}}$ в формулі (4.1), може бути сформовано центром системи декілька варіантів їх виконання. Це пов'язано з тим, що мультикомп'ютерна система має багато компонентів з однаковими функціоналами і при підготовці варіантів виконання завдання можуть залучатись для його виконання різні компоненти, а також система може містити різні методи виконання одного й того ж завдання. Враховуючи призначення систем класу $\mathfrak{S}$ для забезпечення функціонування приманок та пасток, а також для створення проблем зловмисникам в контексті дослідження принципів функціонування таких систем, для виконання одного і того ж завдання, потреба у підготовленні варіанту виконання для якого викликана періодичними повтореннями, можуть бути варіанти виконання такі, що відрізнятимуться або методами виконання і/або залученням різної кількості компонент. Тому, їх кількість буде потребувати організації вибору. Для виконання такого вибору, аналогічно до правил і методу визначення наступного варіанту централізації в архітектурі систем класу $\mathfrak{S}$, потрібно здійснювати оцінювання кожного з варіантів виконання завдання з врахуванням попереднього досвіду функціонування систем класу $\mathfrak{S}$, кількості активних компонент в поточний момент часу, результативності повторень варіантів та врахування рівнів безпеки в компонентах.

Введемо для кожного завдання з множини завдань системи $M_{pz}^{\mathfrak{S}}$ (формула (4.1)) множину потенційних варіантів виконання так:

$$M_{vvp}^{m_{pz,i}^{\mathfrak{S}}} = \left\{ m_1^{m_{pz,i}^{\mathfrak{S}}}, m_2^{m_{pz,i}^{\mathfrak{S}}}, \dots, m_{N^{\mathfrak{S}}}^{m_{pz,i}^{\mathfrak{S}}} \right\}_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}, \tag{4.2}$$

де $m_{pz,i}^{\mathfrak{S}}$ – і-те завдання; $i = 1,2,\dots,N_{M_{pz}^{\mathfrak{S}}}$; $N_{M_{pz}^{\mathfrak{S}}}$ – кількість завдань, які може виконувати система; $m_j^{m_{pz,i}^{\mathfrak{S}}}$ – j-тий варіант виконання і-того завдання $m_{pz,i}^{\mathfrak{S}}$; $j = 1,2,\dots,N_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}^{\mathfrak{S}}$; $N_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}^{\mathfrak{S}}$ – загальна кількість варіантів виконання і-того завдання $m_{pz,i}^{\mathfrak{S}}$.

Тоді, загальна кількість $K_{vvz}^{\mathfrak{S}}$ всіх варіантів виконання всіх завдань систем класу $\mathfrak{S}$ визначимо так:

$$K_{vvz}^{\mathfrak{S}} = \sum_{i=1}^{N_{M_{pz}^{\mathfrak{S}}}} N_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}^{\mathfrak{S}}, \tag{4.3}$$

де $m_{pz,i}^{\mathfrak{S}}$ – і-те завдання; $i = 1,2,\dots,N_{M_{pz}^{\mathfrak{S}}}$; $N_{M_{pz}^{\mathfrak{S}}}$ – кількість завдань, які може виконувати система; $m_j^{m_{pz,i}^{\mathfrak{S}}}$ – j-тий варіант виконання і-того завдання $m_{pz,i}^{\mathfrak{S}}$; $j = 1,2,\dots,N_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}^{\mathfrak{S}}$; $N_{M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}}^{\mathfrak{S}}$ – загальна кількість варіантів виконання і-того завдання $m_{pz,i}^{\mathfrak{S}}$ (формула (4.1)).

Загальна кількість $K_{vvz}^{\mathfrak{S}}$ всіх варіантів виконання всіх завдань систем класу $\mathfrak{S}$ буде визначати потенційну кількість станів, в які будуть переходити системи з урахуванням їх збільшення за рахунок змінюваної кількості компонент в поточний момент часу функціонування системи та можливості залучення кожного разу різних активних компонент.

При затвердженні остаточного варіанту виконання завдання із запропонованих варіантів центром системи контролер прийняття рішень повинен враховувати попередній досвід застосування варіантів виконання завдань або його відсутність у випадку не застосування розглядуваного варіанту для затвердження жодного разу. Певні варіанти виконання завдання могли бути застосовані багатократно і кожного разу їх застосування могло приносити різні результати для виконання завдання та впливу безпосередньо на саму систему. Задамо попередній досвід з використання варіанту, який задано для кожного завдання з множини завдань $M_{pz}^{\mathfrak{S}}$ (формула (4.1)) множиною $M_{vvp}^{m_{pz,i}^{\mathfrak{S}}}$ потенційних варіантів виконання завдання за формулою (4.2), виконання завдання вектором $v_{m_j^{m_{pz,i}^{\mathfrak{S}}}}^{pdvz}$ варіантів виконання завдання так:

$$v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}}} = \left(v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},1}, v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},2}, \dots, v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},N^{\Theta}_{v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}}}}} \right), \quad (4.3)$$

де $m^{\Theta}_{pz,i}$ – і-те завдання; $i = 1,2,\dots,N_{M^{\Theta}_{pz}}$; $N_{M^{\Theta}_{pz}}$ – кількість завдань, які може виконувати система; $m_j^{m^{\Theta}_{pz,i}}$ – j-тий варіант виконання і-того завдання $m^{\Theta}_{pz,i}$; $j = 1,2,\dots,N^{\Theta}_{M^{m^{\Theta}_{pz,i}}_{vvp}}$; $N^{\Theta}_{M^{m^{\Theta}_{pz,i}}_{vvp}}$ – загальна кількість варіантів виконання і-того завдання $m^{\Theta}_{pz,i}$; $v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},k}$ – k-тий показник, який характеризує попередній досвід з використання варіанту $m_j^{m^{\Theta}_{pz,i}}$ виконання завдання $m^{\Theta}_{pz,i}$; $k = 1,2,\dots,N^{\Theta}_{v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}}}}$; $N^{\Theta}_{v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}}}}$ – загальна кількість показників, які характеризують попередній досвід з використання варіанту $m_j^{m^{\Theta}_{pz,i}}$ виконання завдання $m^{\Theta}_{pz,i}$.

Всі показники, які задано координатами вектору $v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}}}$ (формула(4.3)), задамо числовими значеннями з відрізку $[0,1]$. Приймемо з будь-яких двох різних значень одного з показників більше значення кращим з двох значень в контексті показника. Тоді, значення показника, яке буде найближчим до одиниці, буде характеризувати досягнення відповідного рівня для показника. Введемо такі показники в контексті оцінювання попереднього досвіду пропонованих до затвердження варіантів для контролера прийняття рішень:

1) $v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},1}$ – надійність роботи центру системи протягом часу функціонування розглядуваного варіанту виконання завдання;

2) $v^{pdvz}_{m_j^{m^{\Theta}_{pz,i}},1}$ – надійність роботи всієї системи протягом часу функціонування розглядуваного варіанту виконання завдання;

3) $v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}},1}$ – оцінка якості виконання завдання з використанням розглядуваного варіанту для події, яка спонукала застосування цього варіанту виконання завдання;

4) $v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}},1}$ – оцінка якості виконання всіх завдань системою протягом часу використання розглядуваного варіанту для події, яка спонукала застосування цього варіанту виконання завдання.

Також, кількість показників для оцінювання попереднього досвіду використання варіанту виконання завдання може бути збільшено.

Введемо для і-того завдання з множини завдань системи $M^{\Subset}_{pz}$ (формула (4.1)) множину $M^{pdvz}_{v^{pdvz}_{M_{vvp}^{m^{\Subset}_{pz,i}}}}$ векторів варіантів виконання і-того завдання $m^{\Subset}_{pz,i}$ так:

$$M^{pdvz}_{v^{pdvz}_{M_{vvp}^{m^{\Subset}_{pz,i}}}} = \left\{ v^{pdvz}_{m_1^{m^{\Subset}_{pz,i}}}, v^{pdvz}_{m_2^{m^{\Subset}_{pz,i}}}, \dots, v^{pdvz}_{m_{N^{\Subset}_{M_{vvp}^{m^{\Subset}_{pz,i}}}}^{m^{\Subset}_{pz,i}}} \right\}, \quad (4.4)$$

де $m^{\Subset}_{pz,i}$ – і-те завдання; $i = 1,2,\dots,N_{M^{\Subset}_{pz}}$; $N_{M^{\Subset}_{pz}}$ – кількість завдань, які може виконувати система; $m_j^{m^{\Subset}_{pz,i}}$ – j-тий варіант виконання і-того завдання $m^{\Subset}_{pz,i}$; $j = 1,2,\dots,N^{\Subset}_{M_{vvp}^{m^{\Subset}_{pz,i}}}$; $N^{\Subset}_{M_{vvp}^{m^{\Subset}_{pz,i}}}$ – загальна кількість варіантів виконання і-того завдання $m^{\Subset}_{pz,i}$; $v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}},k}$ – k-тий показник, який характеризує попередній досвід з використання варіанту $m_j^{m^{\Subset}_{pz,i}}$ виконання завдання $m^{\Subset}_{pz,i}$; $k = 1,2,\dots,N^{\Subset}_{v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}}}}$; $N^{\Subset}_{v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}}}}$ – загальна кількість показників, які характеризують попередній досвід з використання варіанту $m_j^{m^{\Subset}_{pz,i}}$ виконання завдання $m^{\Subset}_{pz,i}$.

Згідно формул (4.1) та (4.4) задамо множину $M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz}}_{vvp}}}$ попереднього досвіду з використання всіх варіантів, які задано для кожного завдання з множини завдань $M^{\Subset}_{pz}$ (формула (4.1)), так:

$$M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz}}_{vvp}}} = \bigcup_{i=1}^{N_{M^{\Subset}_{pz}}} M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz,i}}_{vvp}}}, \tag{4.5}$$

де $m^{\Subset}_{pz,i}$ – і-те завдання; $i = 1,2,\dots,N_{M^{\Subset}_{pz}}$; $N_{M^{\Subset}_{pz}}$ – кількість завдань, які може виконувати система; $M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz,i}}_{vvp}}}$ – множина векторів варіантів виконання і-того завдання $m^{\Subset}_{pz,i}$.

Таким чином, отримана множина $M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz}}_{vvp}}}$ (формула (4.5)) містить відомості про попередній досвід застосування варіантів виконання завдань, які вже під час функціонування системи затверджувались контролером прийняття рішень.

Кожне із завдань, які задамо множиною завдань системи $M^{\Subset}_{pz}$ (формула(4.1)), можуть мати варіанти виконання задані множиною $M^{m^{\Subset}_{pz,i}}_{vvp}$ потенційних варіантів виконання. Крім врахування попереднього досвіду їх застосування, потрібно також оцінювати ці варіанти перед тим, як контролер прийняття рішень буде обирати один варіант із запропонованих центром системи. Частина варіантів із запропонованих або навіть усі запропоновані варіанти виконання завдання можуть бути такими, що раніше не застосовувались. Тоді, врахування попереднього досвіду неможливе. Якщо ж частина варіантів раніше вже застосовувалась, тобто в системі наявні числові дані щодо результатів функціонування при таких варіантах, то можуть бути варіанти, які раніше не застосовувались. Тоді, вони не матимуть жодних оціночних значень і їх складно оцінити контролером. Для врахування таких варіантів, а також всіх варіантів на початкових етапах функціонування систем, де відсутній попередній досвід для варіантів, введемо цільову функцію для оцінювання кожного варіанту виконання

завдань з врахуванням критеріїв, які будуть визначальними в контексті певних варіантів виконання завдань.

Задамо цільові функції для оцінювання варіантів виконання завдань так, що кращим значенням з двох значень буде менше значення та всі значення, отримуванні при обчисленні цільової функції, будуть належати відрізку $[0,1]$. Нехай визначення цільових функцій задамо так:

$$\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{f}_{1,\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\right),\mathrm{f}_{2,\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{p}_{2,\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\right),\dots,\mathrm{f}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}},\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{p}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}},\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\right)\right)\right)\rightarrow\min, \tag{4.6}$$

де $\mathrm{m}_{\mathrm{pz,i}}^{\Subset}$ – i-те завдання; $\mathrm{i}=1,2,\dots,\mathrm{N}_{\mathrm{M}_{\mathrm{pz}}^{\Subset}}$; $\mathrm{N}_{\mathrm{M}_{\mathrm{pz}}^{\Subset}}$ – кількість завдань, які може виконувати система; $\mathrm{f}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{centr}}\right)$ – j - та функція, що задає обчислення значення j – того критерію; $\mathrm{j}=1,2,\dots,\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}}$; $\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$ – вектор, координатами якого є параметри j – того критерію та варіант виконання завдання; $\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}}$ – кількість аргументів функції $\mathrm{F}_{\mathrm{kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$ та кількість векторів $\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$.

Розглянемо визначення кожного із критеріїв. Визначимо критерії в загальному випадку так:

$$\mathrm{f}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\left(\mathrm{p}_{1,\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}},\mathrm{p}_{2,\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}},\dots,\mathrm{p}_{\mathrm{N}_{\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}},\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}\right)\rightarrow[0,1], \tag{4.7}$$

де $\mathrm{p}_{\mathrm{k,j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$ – k-та координата вектору $\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$ показників для критерію $\mathrm{f}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$; $\mathrm{k}=1,2,\dots,\mathrm{N}_{\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}}$; $\mathrm{N}_{\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}}$ – кількість координат вектору $\mathrm{p}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$ показників для критерію $\mathrm{f}_{\mathrm{j,kr}}^{\mathrm{m}_{\mathrm{pz,i}}^{\Subset}}$.

Критерії будуть включати важливі показники в контексті оцінювання наступних варіантів виконання завдань системою. Такими критеріями можуть бути критерії

щодо безпеки системи, оперативності прийняття рішень в ній, цілісності системи, стійкості системи, стійкості центру системи, цілісності центру системи тощо.

Числові значення обчислені для кожного з цих критеріїв будуть належати числовому відрізку [0,1]. Для кожного розглядуваного варіанту цільова функція оцінювання наступних варіантів виконання завдання для вибору одного з варіантів буде мінімізуватись за рахунок наявних в критеріях параметрів.

Таким чином, отримані цільові функції $F_{kr}^{m_{pz,i}^{\circledcirc}}$ (формула (4.6)) для оцінювання наступних варіантів виконання завдання будуть визначати значення для варіантів, які розглядатиме контролер прийняття рішень.

Для забезпечення виконання завдань мультикомп'ютерними системами потрібно враховувати перед початком виконання завдань чи в процесі вибору варіантів виконання завдань стан окремих компонент та стан системи в цілому, а також наявність активних компонент системи в ній в поточний момент часу.

Стан окремої компоненти розглядатимемо в контексті функційної та кібербезпеки конкретної комп'ютерної станції, в яку вона встановлена. Функційну безпеку будемо розглядати частиною загальної безпеки у компонентах в комп'ютерних станціях, які формують мультикомп'ютерну систему та її визначення будемо здійснювати з урахуванням рівня правильно працюючої системи і її компонент при умовах збоїв обладнання і змін оточуючого середовища. Кібербезпеку конкретної комп'ютерної станції будемо розглядати як стан захищеності даних в електронному вигляді від їх несанкціонованого використання або зловмисних дій з цими даними. Введемо множину M_{komp}^{fbkb} показників, якими будуть характеризуватись функційна та кібербезпека комп'ютерних станцій і компоненти системи в них, так:

$$M_{komp}^{fbkb} = \left\{ m_{komp,1}^{fbkb}, m_{komp,2}^{fbkb}, \dots, m_{komp,N_{M_{komp}^{fbkb}}^{fbkb}}^{fbkb} \right\}, \tag{4.8}$$

де $m_{komp,\mathrm{k}}^{fbkb}$ – k-тий показник, який характеризує стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній; $\mathrm{k} = 1, 2, \dots, N_{M_{komp}^{fbkb}}^{fbkb}$; $N_{M_{komp}^{fbkb}}^{fbkb}$ –

загальна кількість показників, які характеризують стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній.

До показників, які характеризують стан функційної і кібербезпеки комп'ютерної станції та компоненти системи в ній, віднесемо такі: тип операційної системи; заповнення оперативної пам'яті у відсотках; загальний обсяг оперативної пам'яті; тип систем виявлення вторгнень; тип антивірусних засобів; заповнення жорсткого диску; загальний обсяг жорсткого диску; наявність під'єднаних периферійний пристроїв; завантаженість центрального процесора постійними процесами; тип центрального процесора тощо.

Введемо множину функцій M_f^{fbkb} *для визначення рівня функційної та кібербезпеки* комп'ютерної станції та компоненти системи в ній згідно показників (формула (4.8)) так:

$$M_f^{fbkb} = \left\{ f_{f,1}^{fbkb}, f_{f,2}^{fbkb}, \dots, f_{f,N_{M_f^{fbkb}}^{fbkb}}^{fbkb} \right\}, \tag{4.9}$$

де $f_{f,\mathrm{k}}^{fbkb}$– k-та функція, яка характеризує рівень функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній згідно k-того показника (формула (4.8)); $\mathrm{k} = 1, 2, \dots, N_{M_f^{fbkb}}^{fbkb}$; $N_{M_f^{fbkb}}^{fbkb}$– загальна кількість функцій, які характеризують стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній згідно показників визначених за формулою (4.8).

Кожна з функцій визначених у множині функцій M_f^{fbkb} (формула (4.9)) видає значення, що належить відрізку [0,1], з урахуванням конкретного показника у визначеній комп'ютерній станції та здійснює його унормування з рештою значень для цього ж показника з усіх комп'ютерних станцій, в яких встановлені компоненти системи. Визначимо функції так:

$$\mathrm{p}^{\mathrm{n}^{\Subset}} = f_{f,\mathrm{k}}^{fbkb}\left(m_{komp,\mathrm{k}}^{fbkb}, \mathrm{n}^{\Subset}\right), \tag{4.10}$$

де $m_{komp,\mathrm{k}}^{fbkb}$– k-тий показник, який характеризує стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній; $\mathrm{k} = 1, 2, \dots, N_{M_{komp}^{fbkb}}^{fbkb}$; $N_{M_{komp}^{fbkb}}^{fbkb}$–

загальна кількість показників, які характеризують стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній; $f_{f,\mathrm{k}}^{fbkb}$– k-та функція, яка характеризує рівень функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній згідно k-того показника (формула (4.8)); $\mathrm{k} = 1, 2, \dots, N_{M_f^{fbkb}}^{fbkb}$; $N_{M_f^{fbkb}}^{fbkb}$– загальна кількість функцій, які характеризують стан функційної та кібербезпеки комп'ютерної станції та компоненти системи в ній згідно показників визначених за формулою (4.8); $\mathrm{n}^{\mathfrak{S}}$ – номер компоненти системи; $\mathrm{p}^{\mathrm{n}^{\mathfrak{S}}}$ – рівень функційної та кібербезпеки, який характеризує компоненту з номером $\mathrm{n}^{\mathfrak{S}}$.

Тоді, системи класу $\mathfrak{S}$ з урахуванням формул (4.8) - (4.10) будуть характеризуватись вектором рівнів функційної та кібербезпеки усіх компонент. Задамо цей вектор врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи в ній так:

$$\mathrm{v}_{\mathrm{t}}^{\mathrm{p}^{\mathrm{n}^{\mathfrak{S}}}} = \left(\mathrm{t}, \mathrm{p}^{1^{\mathfrak{S}}}, \mathrm{p}^{2^{\mathfrak{S}}}, \dots, \mathrm{p}^{\mathrm{n}^{\mathfrak{S}}}\right), \tag{4.11}$$

де t – поточний час отримання всіх значень $\mathrm{p}^{\mathrm{i}^{\mathfrak{S}}}$; $\mathrm{i}^{\mathfrak{S}} = 1, 2. \dots, \mathrm{n}^{\mathfrak{S}}$; $\mathrm{n}^{\mathfrak{S}}$ – кількість компонент системі; $\mathrm{p}^{\mathrm{i}^{\mathfrak{S}}}$ – значення рівня функційної та кібербезпеки комп'ютерної станції та $\mathrm{i}^{\mathfrak{S}}$- тої компоненти системи в ній.

Визначимо стан функційної та кібербезпеки системи вектором $\mathrm{v}_{\mathrm{t}}^{\mathfrak{S}}$ так:

$$\mathrm{v}_{\mathrm{t}}^{\mathfrak{S}} = \left(\mathrm{t}, \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}^{\mathfrak{S}}} \mathrm{p}^{\mathrm{i}^{\mathfrak{S}}}}{\mathrm{n}^{\mathfrak{S}}}\right), \tag{4.12}$$

де t – поточний час отримання всіх значень $\mathrm{p}^{\mathrm{i}^{\mathfrak{S}}}$; $\mathrm{i}^{\mathfrak{S}} = 1, 2. \dots, \mathrm{n}^{\mathfrak{S}}$; $\mathrm{n}^{\mathfrak{S}}$ – кількість компонент у системі; $\mathrm{p}^{\mathrm{i}^{\mathfrak{S}}}$ – значення рівня функційної та кібербезпеки комп'ютерної станції та $\mathrm{i}^{\mathfrak{S}}$- тої компоненти системи в ній.

Таким чином, для контролера прийняття рішень щодо затвердження наступного варіанту виконання завдань визначено рівні функційної та кібербезпеки комп'ютерної станції та $\mathrm{i}^{\mathfrak{S}}$- тої компоненти системи в ній та в цілому системи за формулами (4.11) і (4.12).

Введемо додатково до величини рівня безпеки системи, який задано за формулою (4.12) рівень зв'язку між компонентами в системі, який буде характеризуватись станом зв'язку. Задамо його вектором $v_z^{\Subset}$ зв'язку компонентів в системі так:

$$v_z^{\Subset} = \left(t, \frac{\sum_{i=1}^{n^{\Subset}} z^{i^{\Subset}}}{2n^{\Subset}}\right), \tag{4.13}$$

де t – поточний час отримання всіх значень $p^{i^{\Subset}}$; $i^{\Subset} = 1, 2. \dots, n^{\Subset}$; $n^{\Subset}$ – кількість компонент системі; $z^{\Subset}$ – кількість зв'язків між компонентами у системі згідно встановленої в ній поточній топології; $z^{i^{\Subset}}$ – кількість зв'язків $i^{\Subset}$- тої компоненти системи з рештою компонент.

Зміст формули (4.13) для величини, що характеризує станом зв'язку між компонентами системи, полягає в тому, що при наявності всіх заданих зв'язків отримуємо штатний режим зв'язків при якому $v_t^{\Subset} = (t, 1)$. Якщо ж певні зв'язки втрачено між компонентами, тоді значення другої координати вектору $v_t^{\Subset}$ буде менше одиниці. Для повноти подання зв'язків для кожної компоненти задамо вектор так:

$$v_t^{z^{n^{\Subset}}} = \left(t, z^{1^{\Subset}}, z^{2^{\Subset}}, \dots, z^{n^{\Subset}}\right), \tag{4.14}$$

де t – поточний час отримання всіх значень $z^{i^{\Subset}}$; $i^{\Subset} = 1, 2. \dots, n^{\Subset}$; $n^{\Subset}$ – кількість компонент системі; $z^{i^{\Subset}}$ – кількість зв'язків $i^{\Subset}$- тої компоненти системи з рештою компонент.

Для визначення повноти зв'язків введемо вектор $v_{t,z}^{z^{n^{\Subset}}}$, в якому будуть відображені координатами величини $p^{z^{i^{\Subset}}}$, що виражатимуть співвідношення наявних зв'язків $i^{\Subset}$-ої компоненти до кількості визначених зв'язків для неї системою. Визначимо вектор $v_{t,z}^{z^{n^{\Subset}}}$ так:

$$v_{t,z}^{z^{n^{\Subset}}} = \left(t, p^{z^{1^{\Subset}}}, p^{z^{1}}, \dots, p^{z^{n^{\Subset}}}\right), \tag{4.15}$$

де t – поточний час отримання всіх значень $p^{z^{i^{\Subset}}}$; $i^{\Subset} = 1, 2. \ldots, n^{\Subset}$; $n^{\Subset}$ – кількість компонент системі; $p^{z^{i^{\Subset}}}$ – співвідношення наявних зв'язків $i^{\Subset}$-ої компоненти до кількості визначених зв'язків для неї системою.

Якщо значення $p^{z^{i^{\Subset}}} = 1$, тоді наявна кількість зв'язків для компоненти збігається з визначеною кількістю, яку встановлено системою. Якщо $p^{z^{i^{\Subset}}} < 1$, тоді наявна кількість зв'язків для компоненти менша визначеної кількості, яку встановлено системою, і така подія потребує дослідження системою. Якщо $p^{z^{i^{\Subset}}} > 1$, тоді наявна кількість зв'язків для компоненти більше визначеної кількості, яку встановлено системою, і така подія потребує особливого дослідження системою. Втрата зв'язків або їх збільшення від визначеної кількості будуть впливати на функціонування контролера прийняття рішень, оскільки така подія вимагатиме виконання окремого завдання із встановлення причин та усунення проблеми.

Для вибору одного з п'яти варіантів виконання завдання контролером прийняття рішень потрібно в ньому задати певний перелік стратегій за якими буде здійснено вибір на затвердження одного варіанту. Всі п'ять варіантів можуть мати різні числові характеристики. Також, може бути так, що частина з них вже раніше була застосована і наявні результати такого застосування в множині $M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)). Або жоден з варіантів ще не застосовувався для виконання завдань протягом всього часу функціонування системи. При функціонуванні системи в перші дні її функціонування, також, пропоновані контролера до розгляду варіанти можуть бути такими, що ще не були застосовані і, відповідно, по ним відсутній попередній досвід їх застосування. Можливі випадки багатократного застосування певних варіантів і різні результати оцінювання таких застосувань. Крім того, для заплутування ймовірного зловмисника, який здійснює повторювані впливи в корпоративній мережі, що породжують однакові події, на які реагують сенсори системи і, відповідно, система повинна виконувати завдання щодо опрацювання таких подій. При частому повторенні таких подій контролер повинен затверджувати варіант, який не повторюється на ці ж події, формуючи тим самим поліморфну відповідь від системи. Тому, для реалізації контролера в ньому повинні міститись

стратегії вибору варіанту виконання завдання з урахуванням всіх початкових умов в системі на момент вибору варіанту.

Задамо множину стратегій $S^{\Subset}_{kontr}$ вибору наступного варіанту виконання завдання контролером прийняття рішень так:

$$S^{\Subset}_{kontr} = \left\{ s^{\Subset}_{kontr,1}, s^{\Subset}_{kontr,2}, \dots, s^{\Subset}_{kontr,N^{str}_{S^{\Subset}_{kontr}}} \right\}, \quad (4.16)$$

де $N^{str}_{S^{\Subset}_{kontr}}$ – загальна кількість стратегій в множині стратегій $S^{\Subset}_{kontr}$ вибору наступного варіанту виконання завдання контролером прийняття рішень; $s^{\Subset}_{kontr,k}$ - k-та стратегія вибору наступного варіанту виконання завдання контролером прийняття рішень; $k = 1, 2, \dots, N^{str}_{S^{\Subset}_{kontr}}$.

Наприклад, стратегіями вибору наступного варіанту виконання завдання контролером прийняття рішень можуть бути такі:

1) $s^{\Subset}_{kontr,1}$ – вибір варіанту з найбільшим значенням цільової функції $F^{m^{\Subset}_{pz,i}}_{kr}$ (формула (4.6));

2) $s^{\Subset}_{kontr,2}$ – вибір варіанту з найменшим значенням цільової функції $F^{m^{\Subset}_{pz,i}}_{kr}$ (формула (4.6));

3) $s^{\Subset}_{kontr,3}$ – вибір варіанту з другим значенням після мінімального значення цільової функції $F^{m^{\Subset}_{pz,i}}_{kr}$ (формула (4.6));

4) $s^{\Subset}_{kontr,4}$ – вибір варіанту з третім значенням після мінімального значення цільової функції $F^{m^{\Subset}_{pz,i}}_{kr}$ (формула (4.6));

5) $s^{\Subset}_{kontr,5}$ – вибір варіанту виконання завдання, який вже повторювався більшу кількість разів порівняно з рештою розглядуваних варіантів згідно даних з множини $M^{pdvz}_{v^{pdvz}_{м^{m^{\Subset}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)) з використання всіх варіантів;

6) $s^{\text{Ю}}_{\text{kontr},6}$ – вибір варіанту виконання завдання, який вже повторювався найменшу кількість разів порівняно з рештою розглядуваних варіантів згідно даних з множини $M^{pdvz}_{v^{pdvz}_{M^{m^{\text{Ю}}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)) з використання всіх варіантів;

7) $s^{\text{Ю}}_{\text{kontr},7}$ – вибір варіанту виконання завдання, який вже повторювався другу за кількістю від варіанту з найбільшою кількістю разів порівняно з рештою розглядуваних варіантів згідно даних з множини $M^{pdvz}_{v^{pdvz}_{M^{m^{\text{Ю}}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)) з використання всіх варіантів;

8) $s^{\text{Ю}}_{\text{kontr},8}$ – вибір випадковим чином варіанту виконання завдання з двох варіантів, які вже повторювався однакову найменшу кількість разів порівняно з рештою розглядуваних варіантів згідно даних з множини $M^{pdvz}_{v^{pdvz}_{M^{m^{\text{Ю}}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)) з використання всіх варіантів;

9) $s^{\text{Ю}}_{\text{kontr},9}$ – вибір випадковим чином варіанту виконання завдання з двох варіантів, які вже повторювався однакову найбільшу кількість разів порівняно з рештою розглядуваних варіантів згідно даних з множини $M^{pdvz}_{v^{pdvz}_{M^{m^{\text{Ю}}_{pz}}_{vvp}}}$ попереднього досвіду (формула (4.5)) з використання всіх варіантів;

10) $s^{\text{Ю}}_{\text{kontr},10}$ – вибір варіанту виконання завдання, в якому заплановано залучення компонент з рівнем безпеки, який вище рівня безпеки системи (формули (4.11), (4.12));

11) $s^{\text{Ю}}_{\text{kontr},11}$ – вибір варіанту виконання завдання, в якому заплановано залучення компонент з рівнем безпеки, який вище рівня безпеки системи (формули (4.11), (4.12)) та який менше рівня безпеки системи не більше ніж на 10%;

12) $s^{\text{Ю}}_{\text{kontr},12}$ – вибір варіанту виконання завдання, в якому заплановано залучення компонент із станами зв’язку, для яких відповідні значення визначені координатами вектору $v^{z^{n^{\text{Ю}}}}_{t,z}$ за формулою (4.15) повністю відповідають визначеним системою;

13) $s^{\mathfrak{S}}_{\text{kontr},13}$ – вибір варіанту виконання завдання, в якому заплановано залучення компонент із станами зв'язку, для яких відповідні значення визначені координатами вектору $v^{z^{n^{\mathfrak{S}}}}_{t,z}$ за формулою (4.15) менше значень визначених системою, але містять не менше двох зв'язків визначених у відповідних координатах вектору;

14) $s^{\mathfrak{S}}_{\text{kontr},13}$ – вибір варіанту виконання завдання, в якому заплановано залучення компонент із станами зв'язку, для яких відповідні значення визначені координатами вектору $v^{z^{n^{\mathfrak{S}}}}_{t,z}$ за формулою (4.15) менше значень визначених системою, але містять не менше половини зв'язків визначених у відповідних координатах вектору.

Перелік стратегій не є вичерпним. Також, ці стратегії можуть бути базовими і використовуватись окремо кожна або комбінуванням декількох з них. Згідно базових стратегій контролер може застосувати правило формування складних стратегій з базових стратегій. Задамо правила формування стратегії вибору наступного варіанту виконання завдання контролером прийняття рішень так:

$$P^{1}_{\text{str}}: s^{\mathfrak{S}}_{\text{kontr,i}} \wedge s^{\mathfrak{S}}_{\text{kontr,j}} \wedge s^{\mathfrak{S}}_{\text{kontr,k}}, \forall\, i = 1,2,3,4, j = 5,6,7,8,9,10, k = 11,12,13,14;$$

$$P^{21}_{\text{str}}: s^{\mathfrak{S}}_{\text{kontr,i}} \wedge s^{\mathfrak{S}}_{\text{kontr,j}}, \forall\, i = 1,2,3,4, j = 5,6,7,8,9,10;$$

$$P^{22}_{\text{str}}: s^{\mathfrak{S}}_{\text{kontr,i}} \wedge s^{\mathfrak{S}}_{\text{kontr,k}}, \forall\, i = 1,2,3,4, k = 11,12,13,14;$$

$$P^{23}_{\text{str}}: s^{\mathfrak{S}}_{\text{kontr,k}} \wedge s^{\mathfrak{S}}_{\text{kontr,j}}, \forall\, j = 5,6,7,8,9,10, k = 11,12,13,14;$$

$$P^{3}_{\text{str}}: s^{\mathfrak{S}}_{\text{kontr,i}}, \forall\, i = 1,2, \dots, 14. \qquad (4.17)$$

Контролер прийняття рішень згідно переліку стратегій вибору наступного варіанту виконання завдання контролером прийняття рішень випадковим чином вибирає правило задане формулою (4.17) та застосовує його до п'яти варіантів, які підготував центр системи. Схему з даними для контролера прийняття рішень та співвідношення між основними компонентами систем класу $\mathfrak{S}$ зображено на рис. 4.2.

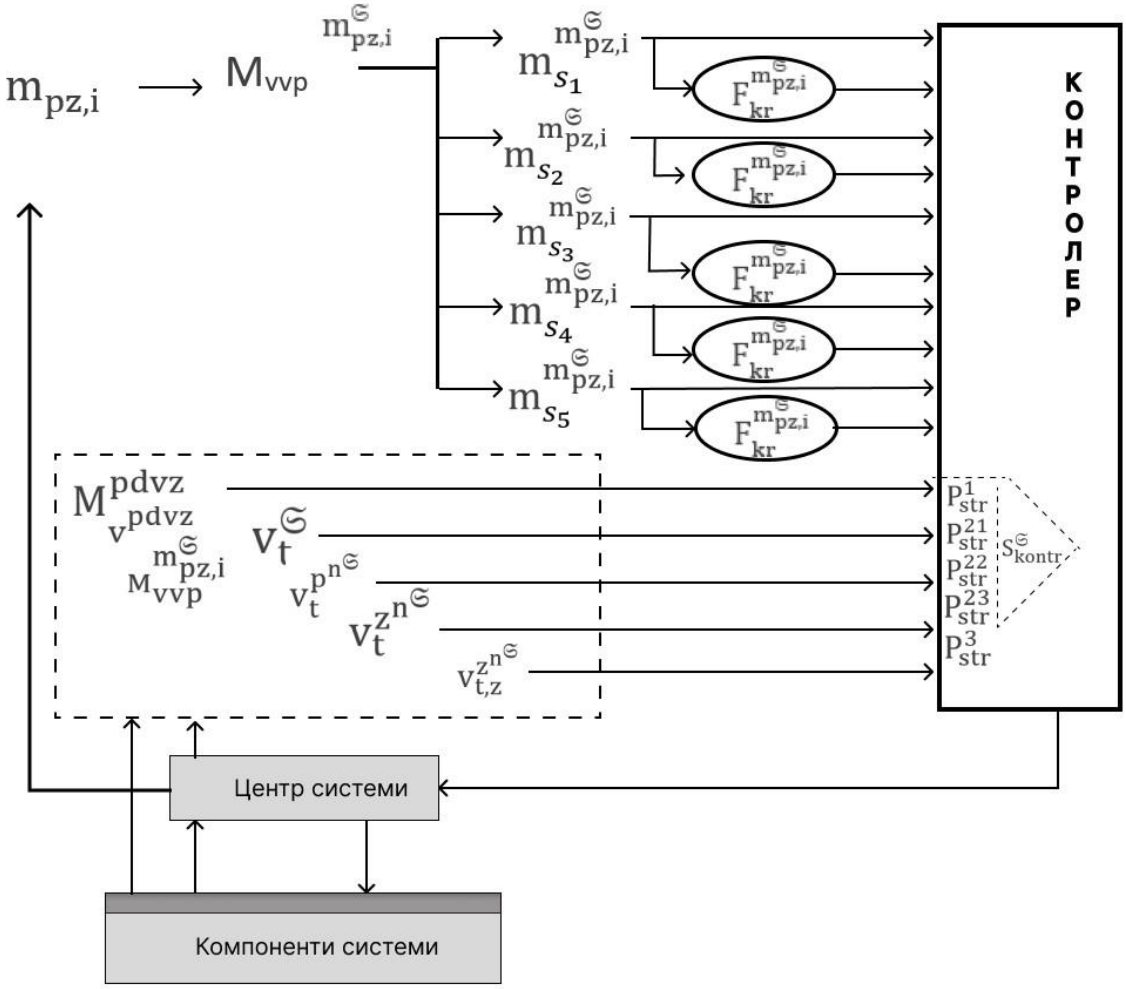


Рисунок 4.2 - Схема подачі вхідних даних на контролер прийняття рішень

Таким чином, в результаті опрацювання вхідних даних контролером прийняття рішень отримуємо варіант виконання завдання, яким сформовано поліморфну відповідь системи на подію, що викликана внутрішніми і зовнішніми впливами в корпоративній мережі. Для організації функціонування необхідно розробити метод згідно якого б функціонував контролер прийняття рішень в мультикомп'ютерних системах.

Задамо метод організації функціонування контролера прийняття рішень основними кроками з урахуванням вхідних даних для опрацювання та правил так:

1) формування контролера прийняття рішень у визначених компонентах системи;

2) перебудова архітектури контролера прийняття рішень;

3) переміщення контролера прийняття рішень до визначених компонент системи;

4) встановлення зв'язку між компонентами, що містять поточний контролер прийняття рішень та рештою компонент системи;

5) отримання вхідних даних від центру системи та решти компонент системи у форматі i-те завдання $m^{\Subset}_{pz,i}$ $(i = 1,2, \dots, N_{M^{\Subset}_{pz}}$; $N_{M^{\Subset}_{pz}}$ – кількість завдань, які може виконувати система) (формула (4.1)), j-тий варіант $m_j^{m^{\Subset}_{pz,i}}$ виконання i-того завдання $m^{\Subset}_{pz,i}$ $(j = 1,2, \dots, N^{\Subset}_{M_{vvp}^{m^{\Subset}_{pz,i}}}$; $N^{\Subset}_{M_{vvp}^{m^{\Subset}_{pz,i}}}$ – загальна кількість варіантів виконання i-того завдання $m^{\Subset}_{pz,i}$) (формула (4.2)), k-тий показник $v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}},k}$ характеристики попереднього досвід з використання варіанту $m_j^{m^{\Subset}_{pz,i}}$ виконання завдання $m^{\Subset}_{pz,i}$ $(k = 1, 2, \dots, N^{\Subset}_{v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}}}}$; $N^{\Subset}_{v^{pdvz}_{m_j^{m^{\Subset}_{pz,i}}}}$ – загальна кількість показників, які характеризують попередній досвід з використання варіанту $m_j^{m^{\Subset}_{pz,i}}$ виконання завдання $m^{\Subset}_{pz,i}$) (формула (4.4)), множини $M^{pdvz}_{v^{pdvz}_{M_{vvp}^{m^{\Subset}_{pz}}}}$ попереднього досвіду (формула (4.5)), значення цільової функції $F_{kr}^{m^{\Subset}_{pz,i}}$ (формула (4.6)) для розглядуваних варіантів виконання завдання, вектор $v_t^{p^{n^{\Subset}}}$ врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи (формула (4.11)), вектор $v_t^{\Subset}$стану функційної та кібербезпеки системи (формула (4.12)), вектор $v_t^{z^{n^{\Subset}}}$ подання зв'язків для кожної компоненти (формула (4.14)), вектор $v_{t,z}^{z^{n^{\Subset}}}$ повноти зв'язків (формула (4.15)), k-та стратегія $s^{\Subset}_{kontr,k}$ вибору наступного варіанту виконання завдання контролером прийняття рішень $(k = 1, 2, \dots, N^{str}_{S^{\Subset}_{kontr}}$; $N^{str}_{S^{\Subset}_{kontr}}$ – загальна кількість стратегій в множині стратегій $S^{\Subset}_{kontr}$ вибору наступного варіанту виконання завдання контролером прийняття рішень) (формула (4.16));

6) вибір випадковим чином та застосування одного з правил формування стратегії вибору наступного варіанту виконання завдання контролером прийняття рішень (формула (4.17));

7) передавання результату з вибору наступного варіанту виконання завдання до центру системи та решти компонент системи.

Таким чином, розроблено метод організації функціонування контролера прийняття рішень, суть якого полягає у забезпеченні вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дає змогу сформувати поліморфну відповідь системи на подію, яка викликана зовнішніми та внутрішніми впливами в корпоративних мережах.

4.2. Метод організації функціонування мультикомп'ютерних систем

Концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ систем класу $\mathfrak{S}$ згідно формули (2.30) враховує множинність елементів, які знаходяться у відносинах та зв'язках один з одним і утворюють певну цілісність та єдність частин. Задані за формулою (2.30) взаємозв'язки між частинами системи та її внутрішня організованість мають конкретні властивості, які змінюються відповідно до зовнішніх і внутрішніх впливів та мети використання систем класу $\mathfrak{S}$. Для організації функціонування таких систем потрібно врахувати не тільки правила внутрішньої організації між елементами та компонентами і правила взаємодії між ними, але потрібно забезпечити зміну їх визначальних властивостей. Тобто, в процесі функціонування системи класу $\mathfrak{S}$ повинні змінювати набір визначальних характеристик. Ці набори визначальних характеристик визначені множинами за формулами (2.3) і допускають велику кількість варіантів. Таким чином, системи класу $\mathfrak{S}$ в процесі свого функціонування в корпоративних мережах багатократно змінюють свої властивості і, тому, з врахування таких особливостей потрібно розробити метод організації функціонування систем, особливістю якого були б можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення

зв’язків між ними. Організація централізації в системах класу $\mathfrak{S}$ та наявність контролера прийняття рішень деталізовані і задані відповідними методами. При цьому, вони є невід’ємними частинами систем класу $\mathfrak{S}$ і, тому, повинні бути враховані при організації взаємодії всіх частин систем. Призначення систем класу $\mathfrak{S}$ може бути задано відповідним спеціалізованим функціоналом, який буде визначальним в контексті призначення та віднесення до певного класу систем. Оскільки такі системи повинні містити множину приманок та пасток для ЗПЗ і КА, а також їх комбінацій, та враховуючи що вони є розподіленими, то організація саме таких систем повинна передбачати підбір компонент для виконання завдань і багатоваріантність в контексті виконання певного конкретного завдання.

Задамо системи класу $\mathfrak{S}$ так, щоб їх визначення включало всі компоненти, елементи та зв’язки між ними. Використаємо задання систем класу $\mathfrak{S}$ їх компонентами за формулою (3.18) множиною $A^{\mathfrak{S}}$. Розділимо компоненти систем класу $\mathfrak{S}$ на дві підмножини: активні компоненти, тобто компоненти в увімкнених комп’ютерних станціях; неактивні компоненти. До підмножини неактивних компонент систем класу $\mathfrak{S}$ віднесемо ті з них, які знаходяться у вимкнених комп’ютерних станціях або вилучені чи заблоковані системою в певний момент часу. Тоді, множину $A^{\mathfrak{S}}$ з врахуванням такого поділу задамо так:

$$A^{\mathfrak{S}} = A_1^{\mathfrak{S},\mathrm{a}} \cup A_2^{\mathfrak{S},\mathrm{p}}, \tag{4.18}$$

де $A_1^{\mathfrak{S},\mathrm{a}}$ – підмножина активних компонент системи $A^{\mathfrak{S}}$; $A_2^{\mathfrak{S},\mathrm{p}}$ – множина компонент системи, які в поточний момент часу знаходяться у вимкнених комп’ютерних станціях або вилучені чи заблоковані системою в певний момент часу.

Задання систем класу $\mathfrak{S}$ множиною $A^{\mathfrak{S}}$ за формулою (4.18) враховує всі компоненти порівняно із заданням за формулою (3.18), в якому враховано також всі компоненти системи, але в контексті активних компонент центру системи та таких, які в поточний момент часу не є такими. Тобто, обидва задання множиною $A^{\mathfrak{S}}$ систем класу $\mathfrak{S}$ охоплюють всі компоненти, але є відмінними через об’єднання різних підмножин. З формул (3.18) та (4.18) отримуємо такі наслідки:

$$A_1^{\mathfrak{S},\mathrm{a}} \supseteq A_1^{\mathfrak{S}};\ A_2^{\mathfrak{S}} \supseteq A_2^{\mathfrak{S},\mathrm{p}}. \tag{4.19}$$

З наслідку заданого формулою (4.19) випливає, що кількість компонент, які містять функціонал центру системи, охоплює всю кількість компонент системи. Це необхідно в контексті вибору варіанту централізації в архітектурі системи, наприклад з децентралізованим типом, при якому для виконання функцій центру системи залучаються всі компоненти. Або для інших типів централізації в архітектурі систем ця вимога збільшує кількість варіантів для розміщення центру системи в активних компонентах. Таким чином, системи класу $\mathfrak{S}$ будуть характеризуватись загальною кількістю компонент, кількістю активних компонент, кількістю активних компонент центру системи, кількістю компонент у вимкнених комп'ютерних станціях, кількістю компонент вилучених системою самостійно. Тоді, згідно значень щодо кількості компонент кожного типу система буде визначатись ними і перебуватиме в певному стані. Задамо вектор $v^{\mathfrak{S}}_{t,st,k}$, який буде характеризувати стан систем класу $\mathfrak{S}$ типами компонент в поточний момент часу функціонування систем так:

$$v^{\mathfrak{S}}_{t,st,k} = \left(t, k^{\mathfrak{S}}_{st,1}, k^{\mathfrak{S}}_{st,2}, k^{\mathfrak{S}}_{st,3}, k^{\mathfrak{S}}_{st,4}, k^{\mathfrak{S}}_{st,5}\right), \tag{4.20}$$

де t – поточний час функціонування системи; $k^{\mathfrak{S}}_{st,1}$ – загальна кількість компонент в системі, яка визначена при її формуванні адміністратором системи; $k^{\mathfrak{S}}_{st,2}$ – кількість активних компонент системи в поточний час t; $k^{\mathfrak{S}}_{st,3}$ – кількість активних компонент центру системи в поточний час t; $k^{\mathfrak{S}}_{st,4}$ – кількість компонент системи у вимкнених комп'ютерних станціях в поточний час t; $k^{\mathfrak{S}}_{st,5}$ – кількість компонент, які вилучені системою самостійно в поточний час t.

Якщо $k^{\mathfrak{S}}_{st,2} = k^{\mathfrak{S}}_{st,3}$, тоді система в поточний момент часу t має децентралізований тип архітектури. Також, співвідношення $k^{\mathfrak{S}}_{st,2} + k^{\mathfrak{S}}_{st,4} + k^{\mathfrak{S}}_{st,5} = k^{\mathfrak{S}}_{st,1}$ характеризує повноту системи щодо розподілу за типами компонент та може бути використано для здійснення самоконтролю в ній. Якщо $k^{\mathfrak{S}}_{st,5} > k^{\mathfrak{S}}_{st,2}$, то система перебуває в критичному стані і її рівень безпеки є таким, що вказує на необхідність дослідження спроможності виконувати завдання. Якщо $k^{\mathfrak{S}}_{st,4} > k^{\mathfrak{S}}_{st,2}$, то система не має достатньої повноти, щоб виконувати завдання. Аналіз аналогічних співвідношень щодо кількості компонент різного типу в поточний момент часу t дає змогу системі самостійно

встановити спроможність виконувати завдання та коректність її архітектури в контексті поділу компонент за формулою (4.20).

Введемо вектор $v^{\mathfrak{S}}_{T,st,k}$ характеристики системи протягом всього часу її функціонування згідно задання всіх векторів, які визначено за формулою (4.20) так:

$$v^{\mathfrak{S}}_{T,st,k} = \left(v^{\mathfrak{S}}_{t_1,st,k}, v^{\mathfrak{S}}_{t_2,st,k}, \dots, v^{\mathfrak{S}}_{t_{N_{v^{\mathfrak{S}}_{T,st,k}}},st,k} \right), \quad (4.21)$$

де t_i – поточний час функціонування системи для і-того вектору $v^{\mathfrak{S}}_{t_i,st,k}$; $i = 1,2,\dots,N_{v^{\mathfrak{S}}_{T,st,k}}$; $N_{v^{\mathfrak{S}}_{T,st,k}}$ – кількість координат вектору $v^{\mathfrak{S}}_{T,st,k}$, тобто кількість отриманих даних для векторів $v^{\mathfrak{S}}_{t_i,st,k}$.

Таким чином, вектор $v^{\mathfrak{S}}_{T,st,k}$ буде містити характеристики системи протягом всього часу її функціонування через певні часові інтервали і система при виконанні завдань буде використовувати відомості про свої попередні варіанти. Для деталізації відомостей про компоненти в архітектурі систем класу $\mathfrak{S}$ введемо для кожної компоненти вектор $v^{\mathfrak{S}}_{T,k,i}$ (i – номер компоненти) функціонування компоненти протягом всього часу функціонування системи. Така інформація надаватиме відомості центру системи для підготовки варіантів виконання завдань, зокрема для вибору компонент, в яких будуть виконуватись завдання. Задамо вектор $v^{\mathfrak{S}}_{T,k,i}$ (i – номер компоненти) функціонування компоненти так:

$$v^{\mathfrak{S}}_{T,k,i} = \left(t, t_i, s_{a,i}, t_{i,1}, t_{i,2}, t_{i,3}, t_{i,4}, t_{i,5} \right), \quad (4.22)$$

де t – поточний час функціонування системи; t_i – поточний час функціонування компоненти системи, тобто крайній час перебування компоненти в активному стані; $s_{a,i}$ – активний (значення «1»)/неактивний(значення»0» стан компоненти в поточний момент часу t функціонування системи; $t_{i,1}$ – загальний час перебування компоненти в активному стані протягом часу t функціонування системи; $t_{i,2}$ – час перебування компоненти в активному стані в складі центру системи; $t_{i,3}$ – час перебування компоненти в активному стані поза центром системи; $t_{i,4}$ – час перебування компоненти у вимкненій комп’ютерній станції; $t_{i,5}$ – час перебування компоненти

серед компонент, які вилучені системою самостійно; $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $N_{A^{\mathfrak{S}}}$ – кількість компонентів в системі $A^{\mathfrak{S}}$.

Тоді, сукупність всіх векторів, які задано за формулою (4.22) при $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$ ($N_{A^{\mathfrak{S}}}$ – кількість компонентів в системі $A^{\mathfrak{S}}$) буде містити часові характеристики всіх компонент системи і буде використана при виборі наступних компонент для виконання завдань. За формулою (4.22) можна встановити співвідношення часу для окремих компонент. Наприклад, повинні виконуватись такі співвідношення при $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$ ($N_{A^{\mathfrak{S}}}$ – кількість компонентів в системі $A^{\mathfrak{S}}$): $\mathrm{t_{i,1}} = \mathrm{t_{i,2}} + \mathrm{t_{i,3}} + \mathrm{t_{i,4}} + \mathrm{t_{i,5}}$; $\mathrm{s_{a,i}} = 1$, якщо $\mathrm{t} = \mathrm{t_i}$ тощо. Такі співвідношення дають змогу системі приймати рішення щодо подальших кроків з виконання завдань у певних компонентах.

Розглянемо, також, час для встановлення зв'язку між різними компонентами системи. Відомості про нього необхідні для систем класу $\mathfrak{S}$, оскільки вони є розподіленими і, тому, цей параметр є критичним для виконання ними завдань. Введемо матрицю $\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}$ крайнього часу витраченого на встановлення зв’язку між двома компонентами системи так:

$$\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}} = \begin{pmatrix} \mathrm{t}_{1,1}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}} & \cdots & \mathrm{t}_{1,N_{A^{\mathfrak{S}}}}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}} \\ \vdots & \ddots & \vdots \\ \mathrm{t}_{N_{A^{\mathfrak{S}}},1}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}} & \cdots & \mathrm{t}_{N_{A^{\mathfrak{S}}},N_{A^{\mathfrak{S}}}}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}} \end{pmatrix}, \tag{4.23}$$

де $\mathrm{t}_{\mathrm{i,j}}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}}$ – крайній час витрачений на встановлення зв’язку між i-тої компонентою та j-тою компонентою; $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $\mathrm{j} = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $N_{A^{\mathfrak{S}}}$ – кількість компонент в системі $A^{\mathfrak{S}}$.

Час, який витрачено на встановлення зв’язку між i-тою компонентою та j-тою компонентою може відрізнятись від часу на встановлення зв’язку між j-тою компонентою та i -тою компонентою. Тобто, матриця $\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}$ не є симетричною відносно головної діагоналі. Також, приймемо $\mathrm{t}_{\mathrm{i,j}}^{\mathrm{M}^{\mathfrak{S}}_{\mathrm{T,k}}} = -1$ у випадку відсутності встановлення зв’язку між i-тою компонентою та j-тою компонентою. Такий зв’язок може бути відсутнім завдяки виконанню завдань без потреби в такому зв’язку, через наявну топологію в системі, що не передбачає такого зв’язку, через втрату з’єднання.

Відомості щодо зв'язків між компонентами містяться у векторі $v_z^{\mathfrak{S}}$ зв'язку компонентів в системі (формула (4.13)), вектор $v_t^{z^{n^{\mathfrak{S}}}}$ повноти подання зв'язків для кожної компоненти (формула (4.14)), вектор $v_{t,z}^{z^{n^{\mathfrak{S}}}}$ співвідношення наявних зв'язків компоненти до кількості визначених зв'язків для неї системою (формула (4.15)). Таким чином, для систем класу $\mathfrak{S}$ встановлено, крім відомостей про зв'язки, час витрачений на їх встановлення. Це дає змогу системам самостійно оцінювати компоненти щодо доцільності їх залучення до виконання завдань, а також визначати проблемні компоненти.

Введемо матрицю $M_{T,k,s}^{\mathfrak{S}}$ середнього часу витраченого на встановлення зв'язку між двома компонентами системи так:

$$M_{T,k,s}^{\mathfrak{S}} = \begin{pmatrix} t_{1,1}^{M_{T,k,s}^{\mathfrak{S}}} & \cdots & t_{1,N_{A^{\mathfrak{S}}}}^{M_{T,k,s}^{\mathfrak{S}}} \\ \vdots & \ddots & \vdots \\ t_{N_{A^{\mathfrak{S}}},1}^{M_{T,k,s}^{\mathfrak{S}}} & \cdots & t_{N_{A^{\mathfrak{S}}},N_{A^{\mathfrak{S}}}}^{M_{T,k,s}^{\mathfrak{S}}} \end{pmatrix}, \quad (4.24)$$

де $t_{i,j}^{M_{T,k,s}^{\mathfrak{S}}}$ – середній час витрачений на встановлення зв'язку між i-тої компонентою та j-тою компонентою; $i = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $j = 1,2,\dots,N_{A^{\mathfrak{S}}}$; $N_{A^{\mathfrak{S}}}$ – кількість компонент в системі $A^{\mathfrak{S}}$.

Визначення наступного значення $t_{i,j}^{M_{T,k,s}^{\mathfrak{S}}}$ середнього часу на встановлення зв'язку між компонентами у випадку наявності попереднього значення обчислюємо як їх середньоарифметичне значення. Можливі варіанти визначення значення з урахуванням зважених коефіцієнтів, а також із введенням певних умов. Середній час, який витрачено на встановлення зв'язку між i-тою компонентою та j-тою компонентою може відрізнятись від середнього часу на встановлення зв'язку між j-тою компонентою та i -тою компонентою, тому матриця $M_{T,k,s}^{\mathfrak{S}}$ не є симетричною відносно головної діагоналі. У випадку відсутності встановлення зв'язку між i-тою компонентою та j-тою компонентою приймемо значення $t_{i,j}^{M_{T,k,s}^{\mathfrak{S}}} = -2$. Цей випадок характеризує зв'язок, який може бути відсутнім завдяки виконанню завдань без

потреби в такому зв'язку, через наявну топологію в системі, що не передбачає такого зв'язку або через технічну втрату з'єднання.

Для організації функціонування мультикомп'ютерних систем з урахуванням визначених в них компонентів та зв'язків між ними задамо основні кроки методу так:

1) поточне формування системи (формула ((4.18)) з активних компонент, які знаходяться в щойно увімкнених комп'ютерних станціях або знаходились в увімкнених раніше комп'ютерних станціях;

2) постійне отримання даних щодо часу функціонування системи та її компонент для формування вектору $v_t^{p^{n^{\Subset}}}$ врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи (формула (4.11)), вектору $v_{T,st,k}^{\Subset}$ буде містити характеристики системи протягом всього часу її функціонування через певні часові інтервали (формула 4.21), вектору $v_{T,k,i}^{\Subset}$ (i – номер компоненти) функціонування компоненти (формула 4.22) протягом всього часу функціонування системи ($i = 1,2, \dots, N_{A^{\Subset}}$; $N_{A^{\Subset}}$ – кількість компонентів в системі $A^{\Subset}$), матриці $M_{T,k}^{\Subset}$ крайнього часу витраченого на встановлення зв'язку між двома компонентами системи (формула 4.23), матриці $M_{T,k,s}^{\Subset}$ середнього часу витраченого на встановлення зв'язку між двома компонентами системи (формула 4.24);

3) отримання даних на виконання вказівок від центру системи та контролера прийняття рішень для формування вектору $v_t^{p^{n^{\Subset}}}$ врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи (формула (4.11)) та вектору $v_t^{\Subset}$ стану функційної та кібербезпеки системи (формула (4.12));

4) отримання даних на виконання вказівок від центру системи та контролера прийняття рішень для формування вектору $v_t^{z^{n^{\Subset}}}$ подання зв'язків для кожної компоненти (формула (4.14)), вектору $v_{t,z}^{z^{n^{\Subset}}}$ повноти зв'язків (формула (4.15));

5) виявлення події в корпоративній мережі, яка викликана зовнішніми і внутрішніми впливами, її ідентифікація та здійснення вибору завдань з множини завдань системи $M_{pz}^{\Subset}$ (формула (4.1)) для відповіді на подію;

6) запуск центру системи для підготовки варіантів відповідей для виконання завдання щодо події з п.5;

7) запуск контролера прийняття рішень для затвердження варіанту виконання завдання з п.6;

8) передача на виконання та виконання затвердженого варіанту виконання завдання з п.7;

9) вилучення системою частини компонент, в яких значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи (формула (4.11)) та стану функційної та кібербезпеки системи (формула (4.12)) перевищує допустимі значення;

10) виконання п.1-п.9 для кожної незв'язної частини системи при її поділі;

11) повторне виконання п.6-п.8 у випадку невиконання п.8;

12) виконання п.1-п.4 у випадку успішного виконання п.8.

Таким чином, розроблено метод організації функціонування мультикомп'ютерних систем, особливістю якого стало забезпечення можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролера прийняття рішень та центру системи, що дало змогу забезпечити багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі.

4.3. Висновки до четвертого розділу

Здійснено формальне подання компонентів системи та зв'язків між ними, виділено в архітектурі мультикомп'ютерних систем окремо центр системи та контролер прийняття рішень. Отримано аналітичні вирази процесів в мультикомп'ютерних системах, які забезпечують спроможності систем до самостійного прийняття рішень щодо виконуваних завдань.

Розроблено метод організації функціонування контролера прийняття рішень. Його особливістю є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів

безпеки компонент системи, кількості компонент та зв’язків між ними. Це дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах.

Розроблено метод організації функціонування мультикомп’ютерних систем, який дає змогу забезпечити можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв’язків між ними з урахуванням стану функційної та кібербезпеки. В ньому враховано виокремлення контролера прийняття рішень та центру системи. Це забезпечило багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі.

Основні наукові результати опубліковані в праці [186, 201, 287].

РОЗДІЛ 5.
ВИЯВЛЕННЯ ЗПЗ ТА КА В КОРПОРАТИВНИХ МЕРЕЖАХ МУЛЬТИКОМП'ЮТЕРНИМИ СИСТЕМАМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК

Розроблена архітектура мультикомп'ютерних систем, в яких наявний контролер прийняття рішень, може бути доповнена засобами та периферійними компонентами, що будуть частиною всієї системи. Система може забезпечувати розв'язування завдань без додаткових засобів, які розміщено окремо в інших комп'ютерних станціях. При цьому вона обирає варіанти виконання завдань для заплутування зловмисників, тобто її поведінка та реакція при здійсненні повторюваних зловмисних впливів є різною. При доповненні системи засобами чи периферійними компонентами, які можуть бути розміщені в комп'ютерних станціях, в яких вже наявні компоненти системи, або в комп'ютерних станціях чи пристроях, в яких вони відсутні, система може додатково здійснювати забезпечення безпеки та захисту корпоративних мереж, збільшуючи свою функційність та спроможності. В такому поданні системи будемо позиціонувати її частину без додаткових засобів чи периферійних компонент як центральну частину, яка може самостійно виконувати завдання. Додаткові периферійні засоби і компоненти будемо розглядати як частини систем, які можуть самостійно виконувати завдання і, при цьому, узгоджувати вибір варіантів виконання завдань з центром системи та контролером прийняття рішень. Доповнення системи такими засобами та компонентами відповідає модульному підходу до її масштабування та дасть змогу урізноманітнити відповіді системи на зловмисні прояви та дії. Зокрема, для опрацювання подій в корпоративних мережах, які відносяться до області відповідальності системи можуть бути залучені окремо центральна частина системи або додаткові периферійні засоби чи компоненти під керуванням центральної частини системи. Тому, розроблення додаткових периферійних засобів та компонентів системи є необхідним для урізноманітнення варіантів виконання однакових завдань, а також покращення ефективності виявлення ЗПЗ та КА.

5.1. Моделі зловмисних дій та приманок

Атака на інфраструктуру або ресурси корпоративних мереж зі сторони зловмисників може бути здійснена ззовні або зсередини корпоративних мереж. Також, для здійснення атаки можуть бути виконані зловмисні впливи або застосоване ЗПЗ, яке розроблено заздалегідь і наповнене необхідними функціями. Його частина може бути розміщена в корпоративних мережах для забезпечення подальшого доступу до її ресурсів та інфраструктури. Крім того, комп'ютерні віруси також будуть впливати на функціонування елементів та компонентів корпоративних мереж і стати об'єктом дослідження системи. При цьому, вони можуть бути засобами зловмисників, але можуть також поширюватись іншими зловмисниками, які не сфокусовані на певних корпоративних мережах. Враховуючи особливості зловмисних атак на інфраструктуру та ресурси корпоративних мереж, задамо узагальнену модель зловмисних дій щодо ресурсів та інфраструктури корпоративних мереж так:

$$\mathfrak{M}_{\mathfrak{h}} = \left(\mathfrak{K}_{\mathfrak{h}}, \mathfrak{R}_{\mathfrak{h}}, \mathfrak{D}_{\mathfrak{h}}, \mathfrak{P}_{\mathfrak{h}}, \mathfrak{V}_{\mathfrak{h}}, \mathfrak{G}_{\mathfrak{h}}\right), \tag{5.1}$$

де $\mathfrak{K}_{\mathfrak{h}}$ – множина компонентів інфраструктури корпоративних мереж; $\mathfrak{R}_{\mathfrak{h}}$ - множина ресурсів корпоративних мереж; $\mathfrak{D}_{\mathfrak{h}}$ – множина зловмисних дій та впливів; $\mathfrak{P}_{\mathfrak{h}}$ – здійснення зловмисних дій ззовні, зсередини та комбіновано по відношенню до конкретних корпоративних мереж; $\mathfrak{V}_{\mathfrak{h}}$ – множина відповідей від засобів та систем забезпечення безпеки та захисту корпоративних мереж; $\mathfrak{G}_{\mathfrak{h}}$ – граф зв'язків між елементами множин $\mathfrak{K}_{\mathfrak{h}}, \mathfrak{R}_{\mathfrak{h}}, \mathfrak{D}_{\mathfrak{h}}, \mathfrak{P}_{\mathfrak{h}}, \mathfrak{V}_{\mathfrak{h}}$.

В залежності від зловмисних дій та впливів засоби та системи забезпечення безпеки і захисту корпоративних мереж можуть відповідати по різному або однаково на повторювані дії. При цьому може бути так, що зловмисник не отримає жодної відповіді або система/засіб не здійснить жодної реакції на зловмисну дію чи вплив, але така її поведінка теж може бути варіантом виконання завдання щодо опрацювання такої події. Розвиток такої поведінки системи, також, може стосуватись спостереження за наступними зловмисними діями чи впливами. Якщо зловмисні дії

виконуються комп’ютерними вірусами, тоді система може бачити повторювані дії з втілення коду у виконувані програми.

Відповіді системи можуть бути різними. Якщо в її складі наявні приманки та пастки, тоді зловмисні дії можуть залишитись, також, без відповіді, якщо система спрямує зловмисника на такі хибні об’єкти атак в корпоративних мережах чи зловмисник/зловмисні об’єкти самі потраплять в них.

Відповіді на події надає система, хоча вони можуть бути сформовані з урахуванням роботи додаткових периферійних компонентів чи засобів. Для розширення обманної спроможності мультикомп’ютерних систем доповнимо їх хибними об’єктами для атак різного призначення. Ці об’єкти, також, можуть бути різними за архітектурою, призначенням і, відповідно, розміщенням в корпоративних мережах.

Додатковими периферійними компонентами чи засобами можуть бути приманки та пастки, які додатково будуть розширювати функційні спроможності систем. Вони можуть бути спрямованими на конкретні зловмисні дії, ЗПЗ, КА чи комп’ютерні віруси та бути видимими в корпоративних мережах, а можуть бути невидимими для зловмисників і система буде їх використовувати приховано. Взагалі приманки встановлюються в мережі з метою бути атакованими, і не передбачено виконання ними інших функцій. На приманках не повинно бути корисного трафіку, а якщо він наявний, тоді вважатимемо таку активність зловмисною. Роботу приманки в циклі виявлення та захисту від зловмисних дій поділимо на етапи: попередження; виявлення; реагування; дослідження зловмисних дій та атак. Приманку реалізують як вразливий сервіс для притягування зловмисників. Таким чином, часто зловмисні сервіси розпочинають атакувати першочергово приманку. Захопивши активність зловмисника сервіс-приманка використовує засоби для утримання зловмисника, сповільнюючи його доступ до робочих сервісів, або в найкращому випадку запобігаючи йому. В цьому випадку використання приманок дозволяє попередити атаки щодо діючих сервісів та систем. Функція виявлення модифікованих атак та нових типів атак приманками є критично важливою функцією для швидкого реагування та попередження втручання в мережу. На цьому етапі приманки формують невеликий та змістовний обсяг інформації про несанкціоновані дії.

Функція реагування на дії зловмисників вимагає попередньої інформації як щодо самого зловмисника, так і щодо його попередніх дій та завданої шкоди. Приманки збирають всю інформацію про атаку з самого її початку, на відміну від робочих сервісів з системами виявлення вторгнень. Крім того, взаємодія приманки із зловмисником може надати додаткову інформацію, яка необхідна для ефективного реагування на атаку. Приманки є засобами для дослідження нових типів зловмисних дій та їх модифікацій. Вся інформація, зібрана приманками, стосується тільки несанкціонованих дій, тому це є найбільш ефективний спосіб отримання такої інформації порівняно з іншими, наприклад з аналізом усього трафіку робочих сервісів.

Для захисту комп'ютерних мереж системою приманок комп'ютерної мережі система приманок передбачає їх розташовують у місцях можливого зловмисного втручання. Відносно комп'ютерної мережі можна виділити зовнішнє розташування приманок, внутрішнє та в демілітаризованій зоні (ДМЗ).

Розглядатимемо мультикомп'ютерну систему включно з множиною інтелектуальних приманок, які виконують постійний моніторинг мережі. Зовнішні приманки приєднані безпосередньо до мережі інтернет перед брандмауером. Цей тип приманок має найвищий рівень взаємодії та представляє собою фізичний сервіс з операційною системою, який емулює роботу реальних сервісів та відповідає на запити зловмисників. За рахунок цього, а також за рахунок розташування приманки у місці без будь-якого захисту від втручань, приманка дає змогу зібрати максимально можливий обсяг інформації про дії зловмисників. Приманки, які розташовані в зоні ДМЗ, є фізичними і віртуальними, в залежності від їх кількості. Фізичні приманки працюють постійно під час роботи мережі. Віртуальні приманки можуть бути статичними і динамічними. Статичні приманки, так само як фізичні, працюють постійно. Динамічні приманки працюють підключаються за необхідності, якщо є потреба виявляти додаткові загрози або отримати більше інформації про дії зловмисників.

Основна множина приманок розташована всередині мережі і призначена для моніторингу безпеки сервісів та пристроїв підключених до мережі, в тому числі до внутрішньої локальної мережі. Так само як і в зоні ДМЗ всередині мережі

використовуватиметься множина статичних та динамічних приманок, серед яких є фізичні та віртуальні. Кількість статичних приманок та їх розташування в мережі фіксована. Система приманок є мережею із своєю архітектурою та власною системою сервісів та фактично вбудована в мережу робочих сервісів, що значно підвищує контрольованість та захищеність системи в цілому. Елементами роботи мережі приманок є контроль даних, захоплення даних та збір даних.

Контроль даних системою приманок призначений зменшувати ризики здійснення атак щодо робочих сервісів, розміщених в мережі. Основною метою контролю дій зловмисника є швидке та ефективне реагування на них. Крім того, зловмиснику не повинно бути відомо, що його дії контролюються. Для зменшення ризиків система приманок повинна відповідати таким вимогам. Контроль мережі має поєднувати ручний та автоматичний. Для захисту від втручань необхідно щонайменше два рівні контролю даних. Також, приманки повинні мати можливість підтримувати всі вхідні та вихідні з'єднання і контролювати будь-яку несанкціоновану активність. Здійснення контролю даних повинно конфігуруватися центром системи в будь-який час. Контроль зв'язку з центром системи та адміністратором повинен бути організований таким чином, щоб він складно відслідковувався зловмисником. В системах з приманками має бути забезпечена наявність щонайменше двох методів для попередження про зловмисну активність і можливість віддаленого адміністрування контролю даних.

Захоплення даних є наступною вимогою до мережі приманок. Критично важливим є те, що захоплення активності приманкою має бути невідоме зловмиснику. До захоплення даних мережею приманок висуваються такі вимоги: дані, які захоплені приманкою, не зберігаються нею локально для того, щоб зловмисник не мав до них доступу; будь-який вплив інший даних не повинен впливати на процес захоплення даних приманкою; до активностей, які повинні відслідковуватися та фіксуватися, відносяться активності мережі, системи, застосунків та користувачів; адміністратор та центр системи повинні мати змогу віддалено відслідковувати роботу мережі приманок у реальному часі; захоплені дані повинні автоматично зберігатися для подальшого аналізу; інформація про захоплені дані повинна підтримуватися для кожної приманки мережі; адміністратор або центр системи повинні виконувати

оновлення приманок, які виявлені зловмисником; потрібно забезпечувати цілісність даних, які захоплені мережею приманок.

Збір даних мережею приманок призначений для подальшого їх аналізу та інтеграції з даними про зловмисні дії, отримані з інших джерел. Ця інформація використовується для поточного та подальшого запобігання атакам. Для збору даних до мережі приманок висуваються вимоги: кожна приманка має унікальний ідентифікатор для взаємодії з мережею; можливість анонімізації даних, що стосуються приманок в мережі; обмін даними виконується із забезпеченням конфіденційності та цілісності даних; стандартизація та синхронізація обміну захопленими даними всередині мережі приманок.

Мережа приманок виконує функцію поточного та перспективного захисту мережі від певної множини зловмисних втручань, в тому числі від автоматизованих (автоматичних) атак та персоналізованих втручань.

Таким чином, вимоги до мереж приманок можуть бути реалізовані з підтримкою мультикомп’ютерних систем антивірусних комбінованих приманок та пасток. Приманки виступають в такій системі периферійними засобами, завданням яких є спрямування зловмисників на себе. Центр системи дає змогу проімітувати активність таких периферійних засобів, щоб вони стали помітними для зловмисників. Поєднання їх в єдину інтелектуальну мережу дає змогу покращити застосування обманних технологій щодо зловмисників в корпоративних мережах.

До складу мультикомп’ютерних систем необхідно включати тіньові приманки. Вони можуть функціонувати як інтелектуальні агенти в корпоративних мережах. Така приманка аналізує трафік комп’ютерної мережі на основі власної множини моделей детекторів аномалій , які формуються на основі власного досвіду приманки, а також досвіду інших агентів системи. Робота приманки оптимізується таким чином, щоб забезпечити оптимальну стратегію поведінки та зростання інтегральної функції винагороди при тривалій роботі, внаслідок чого підвищується точність виявлення зловмисних вторгнень та забезпечується автономне функціонування приманки. Мультикомп’ютерна система є основою для наповнення її такими приманками в комп’ютерних мережах. Тобто, крім прийняття рішень в центрі системи, такі приманки можуть приймати певні визначені дії самостійно. Наявність таких

приманок зумовлена, наприклад, направленням зловмисного трафіку або дій зловмисника для їх захоплення та подальшого аналізу. При цьому, зловмисник не бачить такі приховані засоби.

Для захисту комп'ютерних мереж системою приманок їх розташовують у місцях можливого зловмисного втручання. Відносно комп'ютерної мережі можна виділити зовнішнє розташування приманок, внутрішнє та в зоні ДМЗ. Прикладом архітектури мультикомп'ютерної системи, що підтримує функціонування множини інтелектуальних приманок, які виконують постійний моніторинг мережі зображено на рис. 5.1.

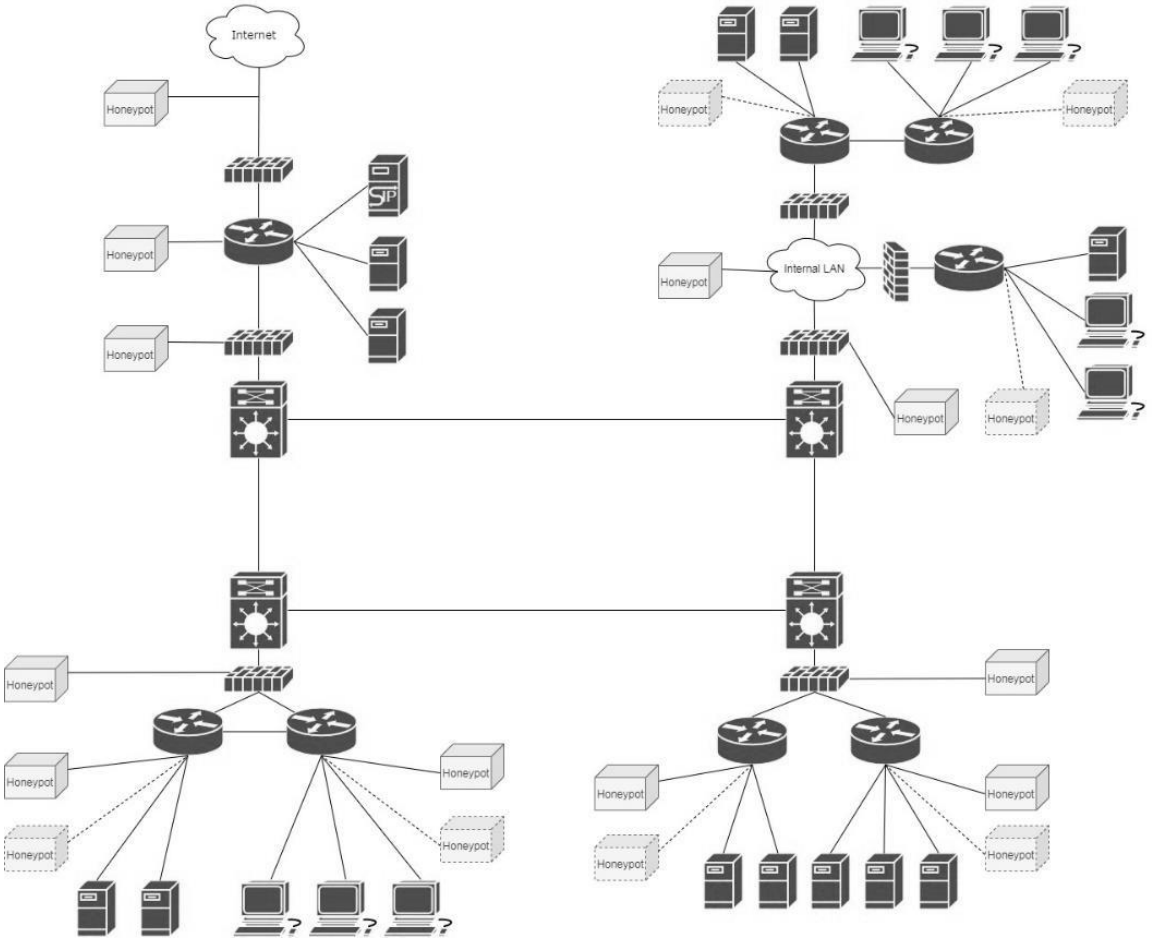


Рисунок 5.1 - Система з приманками

Розглянемо приманки, які наявні в системі на рис. 5.1. Зовнішні приманки приєднані безпосередньо до мережі інтернет перед брандмауером. Приманки, які розташовані в зоні ДМЗ є фізичними і віртуальними, в залежності від їх кількості. Фізичні приманки працюють постійно під час роботи мережі. Віртуальні приманки можуть бути статичними і динамічними. Статичні приманки, так само як фізичні,

працюють постійно. Динамічні приманки працюють підключаються за необхідності, якщо є потреба виявляти додаткові загрози або отримати більше інформації про дії зловмисників. Основна множина приманок розташована всередині мережі і призначена для моніторингу безпеки сервісів та пристроїв підключених до мережі, в тому числі до внутрішньої локальної мережі. Так само як і в зоні ДМЗ всередині мережі використовується множина статичних та динамічних приманок, серед яких є фізичні та віртуальні.

Приманку можна створити так, що вона буде позиціонуватись як інтелектуальний агент. Приманка як агент працює в швидко змінюваному та непередбачуваному середовищі. Тіньова приманка працює паралельно з основним сервісом. Робота може бути організована в двох варіантах: на приманку надходить той же трафік, який надходить на робочий сервіс; на приманку надходить тільки той трафік, який визначений СВВ як підозрілий (зловмисний).

На приманці проводиться аналіз трафіку для виявлення аномалій в онлайн режимі. Приманка містить множину моделей, призначених для виявлення аномалій (детекторів аномалій). Задамо їх множиною $M_a = \{m_{a1}, m_{a2}, \dots, m_{an}\}$. Моделі можуть працювати одночасно або вибірково. В результаті роботи набору детекторів аномалій отримують множину виявлених аномалій $O = \{o_1, o_2, \dots, o_n\}$. Приманка може працювати в таких режимах: автономний; режим керування адміністратором; змішаний режим.

На приманці зберігається попередня інформація про множину патернів атак $P = \{p_1, p_2, \dots, p_n\}$. Патерни атак отримують з різних джерел: автоматичної системи виявлення патернів (різного типу моделі кластеризації даних, отриманих приманками, які працюють тільки із зловмисним трафіком); інструкції адміністратора.

Середовище, в якому функціонує приманка, характеризується мережним трафіком, і представляє собою множину послідовностей станів $S^* = \{S_1^*, S_2^*, \dots, S_n^*\}$. Передбачається, що в будь-який момент часу середовище знаходиться в одному з цих станів. Приманка приймає рішення з множини рішень $D = \{d_1, d_2, \dots, d_n\}$. Приклади таких рішень: d_1 – нормальний трафік; d_2 – аномальний трафік, є збіги з екземплярами множини патернів; d_3 – аномальний трафік, немає збігів з множиною

патернів, тощо. На основі рішень приманка виконує відповідну дію/дії з множини дій $A = \{a_1, a_2, \dots, a_n\}$. Приклади дій: a_1 – продовжити виконання процесу; a_2 – призупини процес для подальшого аналізу; a_3 – зупинити процес, тощо.

Таким чином, функціонування приманки розглядатимемо як функцію так:

$$S^* \to D \to A, \tag{5.2}$$

де A - множина дій; D - множина рішень; S^* - множина послідовностей станів.

Рішення приймаються на основі досвіду, який враховує власний досвід. На основі власного досвіду приманки можливі таки варіанти рішень: оптимальне рішення на основі власного досвіду; неоптимальне рішення на основі власного досвіду; неможливо прийняти будь-яке рішення на основі власного досвіду. Кожній окремій приманці, як агенту, може не вистачати досвіду (набору знань), яким вона володіє для прийняття оптимального рішення, або рішення взагалі. Тому, доцільна взаємодія з іншими приманками мереж.

Важливо визначити кінцеву ціль, якої повинна досягати приманка. Оптимальним рішенням та оптимальною дією є ті, які підвищують функцію винагороди приманки. Цільова функція винагороди відображає те, що приманка як агент функціонує в оптимальний спосіб. В процесі роботи на кожному кроці функція винагороди є числом R_t. Робота приманки оптимізується таким чином, щоб забезпечити максимум цільової функції винагороди при тривалій роботі приманки. Приріст функції винагороди має відображати кінцевий результат роботи приманки (наприклад, виявлення аномального трафіку). Інтегральна функція винагороди на тривалому проміжку роботи приманки отримується з цільових функцій винагороди на кожному кроці. Для інтеграції можуть бути використані різні способи, зокрема усереднена адитивна інтегральна функція винагороди:

$$C_R = \frac{R_{t+1} + R_{t+2} + \cdots + R_{t+n}}{n} = \frac{1}{n}\sum_{i=1}^{n} R_{t+i}, \tag{5.3}$$

де R_{t+i} – значення функції винагороди на i-ому кроці; n – кількість кроків, на яких визначається інтегральна цільова функція винагороди.

Цільова функція винагороди визначає кількісно внесок приманки в підвищення захищеності комп’ютерної мережі та повинна враховувати такі чинники:

1) виявлення зловмисного трафіку та зупинка процесу призводить до збільшення функції винагороди;

2) виявлення хибно-позитивного зловмисного трафіку призводить до зменшення функції винагороди;

3) збільшення часу виявлення зловмисного трафіку призводить до зменшення функції винагороди.

Після виявлення аномалія o_i порівнюється з множиною заданих патернів P. Якщо аномалія збігається з патерном, то цільова функція винагороди збільшується на число $k_r r$, де r – винагорода, k_r – коефіцієнт, який враховує час виявлення. Якщо аномалія не збігається з жодним патерном, то функція винагороди залишається незмінною, а дані аномалії зберігаються для подальшого аналізу адміністратором (в режимі адміністратора чи змішаному режимі) або самою приманкою з появою додаткової інформації. Такою додатковою інформацією є оновлення патернів атак. Якщо такий додатковий аналіз дозволяє підтвердити аномалію, то функція винагороди збільшується. Якщо аномалія визначається як нормальний трафік, то функція винагороди зменшується на число w. Таким чином, на кожному кроці цільова функція винагороди визначається як:

$$R_t = p_r \cdot k_r r - p_w \cdot w, \tag{5.4}$$

де p_r – ймовірність винагороди; p_w – ймовірність стягнення; r – винагорода; k_r – коефіцієнт, який враховує час виявлення; w – число, на яке зменшується винагорода.

Архітектура приманки як інтелектуального агенту описує дані, рішення, які приймає приманка, та дії, які виконує приманка (рис. 5.2).

За наявності скінченого переліку трійок «стан середовища – рішення – дія» приманка навчається оптимальній стратегії поведінки, яка приводить до зростання інтегральної функції винагороди. Але в умовах реального мережевого трафіку множина послідовностей станів S^* містить велику кількість послідовностей та є невизначеною, тому немає можливості отримати чітку відповідність $S^* \to D$. Крім того, для генерації оптимальних стратегій необхідні провести значні обсяги обчислень, що є ще одним суттєвим обмеженням в умовах онлайн режиму роботи приманки. Тому, для отримання функцій залежності $D(S^*)$ необхідно

використовувати апроксимацію за допомогою моделей виявлення аномалій. Модель виявлення аномалій мережевого трафіка, як правило, є моделлю, яка навчається з підкріпленням.

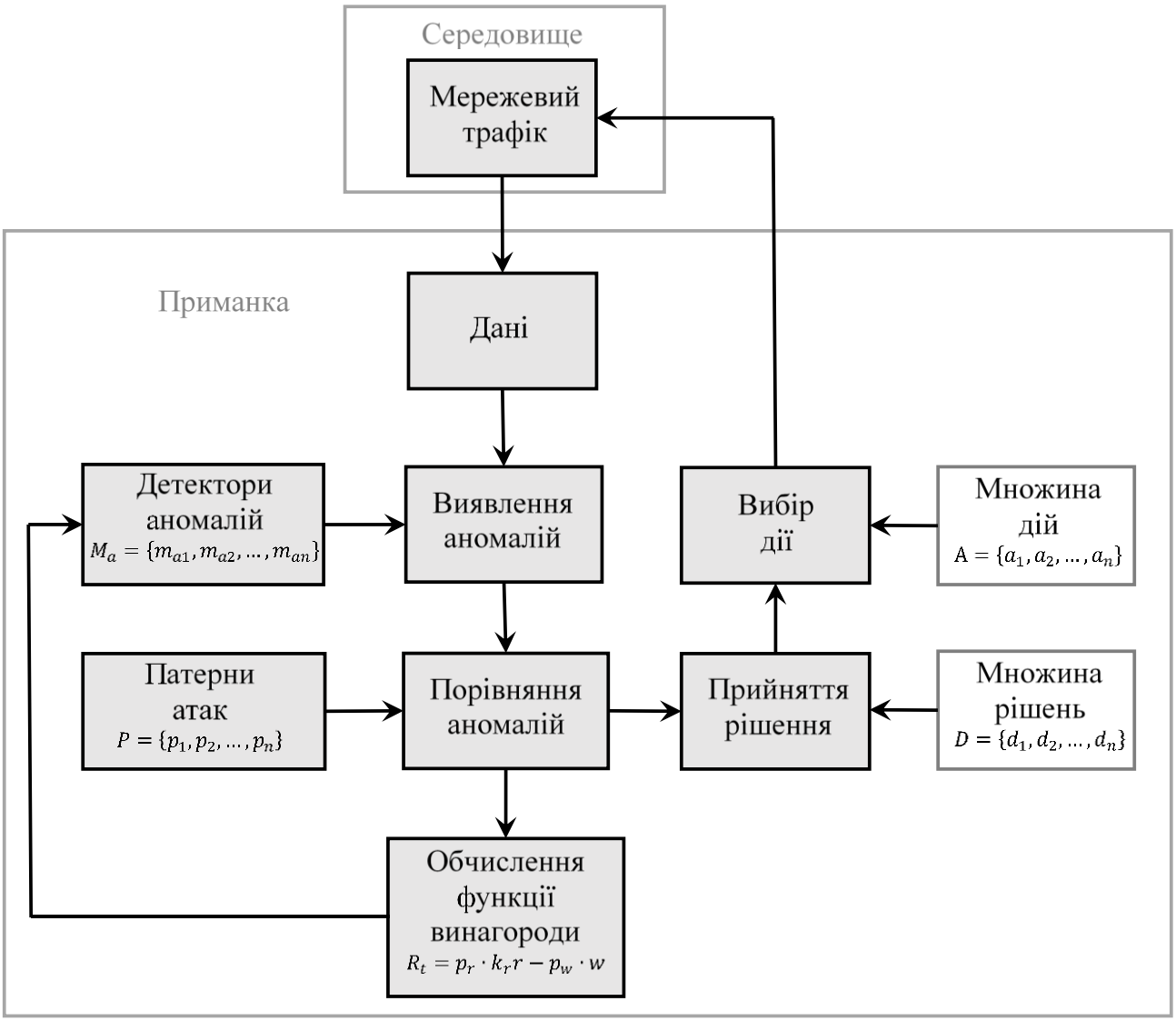


Рисунок 5.2 - Архітектура приманки як інтелектуального агента

Таким чином, встановлено особливості застосування приманок в контексті зловмисних дій та здійснено їх формальне подання, які відображені в розроблених моделях зловмисних дій та приманок. В архітектурі приманок виділено інтелектуальну складову частину, яка виконує завдання із здійснення аналізу трафіку. Архітектура приманок розроблена для можливості їх функціонування як інтелектуальних агентів, що можуть взаємодіяти з рештою приманок, але з урахуванням координації в мультикомп’ютерних системах.

5.2. Моделі приманок в корпоративних мережах з врахуванням типів зловмисних атак

Моделі приманок потребують деталізації на основі типових комп'ютерних атак, архітектурних особливостей приманок та з врахуванням архітектури мультикомп'ютерних систем з приманками та пастками. Для побудови моделей приманок згрупуємо і узагальнимо їх характеристики. З цією метою враховуватимемо рівні роботи приманок з урахуванням її функцій: виявлення; аналізу; реагування; виконання. На цих рівнях здійснюється збір інформації щодо вторгнень в роботу сервісу, визначається із зафіксованої активності зловмисна активність та визначається рівень її небезпеки для мережі, формуються правила попередження та виявлення атак. А на останньому рівні відбувається поєдання двох основних функції. На етапі виявлення за відомими сигнатурами виявляються атаки мережі на основі статичних патернів. На етапі попередження ці атаки блокуються як зловмисні. Тоді модель приманки, яка враховуватиме функції з яких вона формуватиметься, задамо так:

$$\mathfrak{W}_{\text{p}} = \langle \text{P}, \Omega_{\text{I}} \rangle, \tag{5.5}$$

де P–множина, яка позначає сукупність функцій приманки; Ω_{I}–множину предикатів на множині P.

Розроблені моделі приманок, мереж приманок та аналіз особливостей типів приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки. Моделі приманок та мереж приманок є основою для розробки принципово нових методів виявлення зловмисного втручання в функціонування корпоративних мереж. Це досягається за рахунок конфігурування різних типів приманок та їх інтеграції не тільки з іншими системами забезпечення рівня безпеки корпоративних мереж, а також і за рахунок їх представлення в мультикомп'ютерних системах, які за своєю архітектурою будуть здійснювати ефективну реакцію на зловмисні події. Для виявлення атаки та визначення її типу потрібно визначити характерні ознаки певного типу атаки. Приманка повинна забезпечувати: порти та

сервіси, на які здійснюються атаки; організацію збирання, зберігання та опрацювання даних мережного трафіку приманки; взаємодію з мережею приманок. Порти та сервіси, які розгорнуті на приманці, залежить від типу/типів атак, які перехоплює приманка. Організація збирання та зберігання даних може бути реалізована однаково для різних типів атак. Розглянемо типові архітектури приманок з урахуванням типових атак в корпоративних мережах. Атака «поштова бомба» направлена на електронну поштову скриню або на поштовий сервер. Основною метою цієї атаки є навмисне запобігання поштової комунікації та зниження продуктивності роботи мережі. В залежності від інтенсивності «поштової бомби» вплив атаки може бути від незручностей у використані до повної відмови в обслуговуванні. До типових атак «поштова бомба» можна віднести: масова розсилка, тобто цілеспрямоване відправлення великої кількості випадкового поштового трафіку на цільові електронні поштові адреси; посилання на список, тобто внесення електронних поштових адрес, визначених для атаки, в численні списки підписок, таким чином використовуючи сторонні джерела для надсилання поштового трафіку на ці цільові адреси; архівна бомба, тобто надсилання дуже великого заархівованого файлу на електронну поштову адресу, яку визначено для атаки; вкладення, тобто надсилання повідомлень з вкладеннями значних розмірів, що має на меті перевищення обсягу пам’яті, доступної на поштовому сервері. Характерними ознаками атаки «поштова бомба» є значний обсяг поштового трафіку. Цей поштовий трафік може бути сформований у різні способи так: одне повідомлення великого обсягу; значна кількість повідомлень невеликого обсягу, які направлені на одну електронну поштову адресу; значна кількість повідомлень невеликого обсягу, які направлені на різні поштові електронні адреси, розташовані на одному сервері тощо. Зловмисний поштовий трафік може надходити від одного джерела або бути розподіленим, наприклад, у випадку атаки типу «посилання на список». Для виявлення атаки типу «поштова бомба» необхідно розгорнути на приманці SMTP-сервіс для імітації поштового серверу (рис. 5.3). Дані, які фіксує приманка: IP-адреса/IP-префікс джерела повідомлення; ім’я домена/ URL/тип URL джерела повідомлення; ID користувача/користувачів; обсяг повідомлення, що надсилається. На основі цих даних проводиться аналіз активності на SMTP-сервісі приманки, визначаються порогові значення обсягу

повідомлення/повідомлень та швидкості їх надходження. Порогові значення використовуються для визначення поштового трафіку як зловмисного та такого, що потребує аналізу.

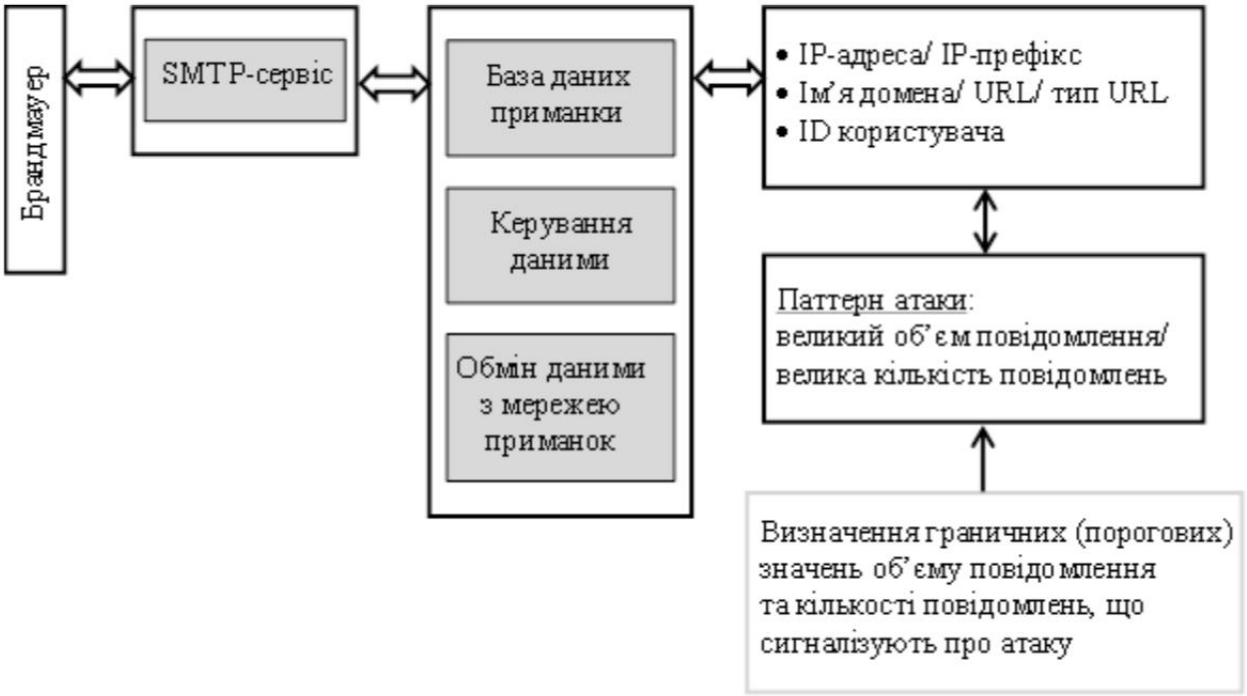


Рисунок 5.3 - Структурна схема приманки для атаки «поштова бомба» (mailbomb)

Атаку Neptune можна охарактеризувати як напіввідкрита TCPSYN атака. Для успішної реалізації атаки зловмисник використовує особливості попереднього встановлення з'єднання в TCP протоколі, постійно надсилаючи велику кількість SYN пакетів (запитів на встановлення зв'язку) безпосередньо на TCP сервер. Сервер надсилає у відповідь SYN/ACK пакет і чекає на ACK пакет від клієнта, який зловмисник не надсилає, і з'єднання залишається «напіввідкритим». Оскільки TCP сервер має обмежену кількість з'єднань, то відбувається переповнення, і робота сервера блокується. Для виявлення атаки Neptune на приманці повинен бути розгорнутий сервіс, який працює за TCP протоколом, наприклад HTTP та FTP сервіси (рис. 5.4). Дані, які фіксує приманка: IP-адреса/IP-префікс джерела запиту; ім'я домена/URL/тип URL джерела запиту; кількість «напіввідкритих» запитів. З кількості «напіввідкритих» запитів формується часовий ряд активності зловмисників на серверах даної приманки, оскільки у випадку розподіленої атаки запити можуть надходити з різних джерел. В результаті аналізу мережний трафік класифікуємо як

незловмисний/зловмисний та визначаємо граничне значення кількості запитів та швидкості їх надходження.

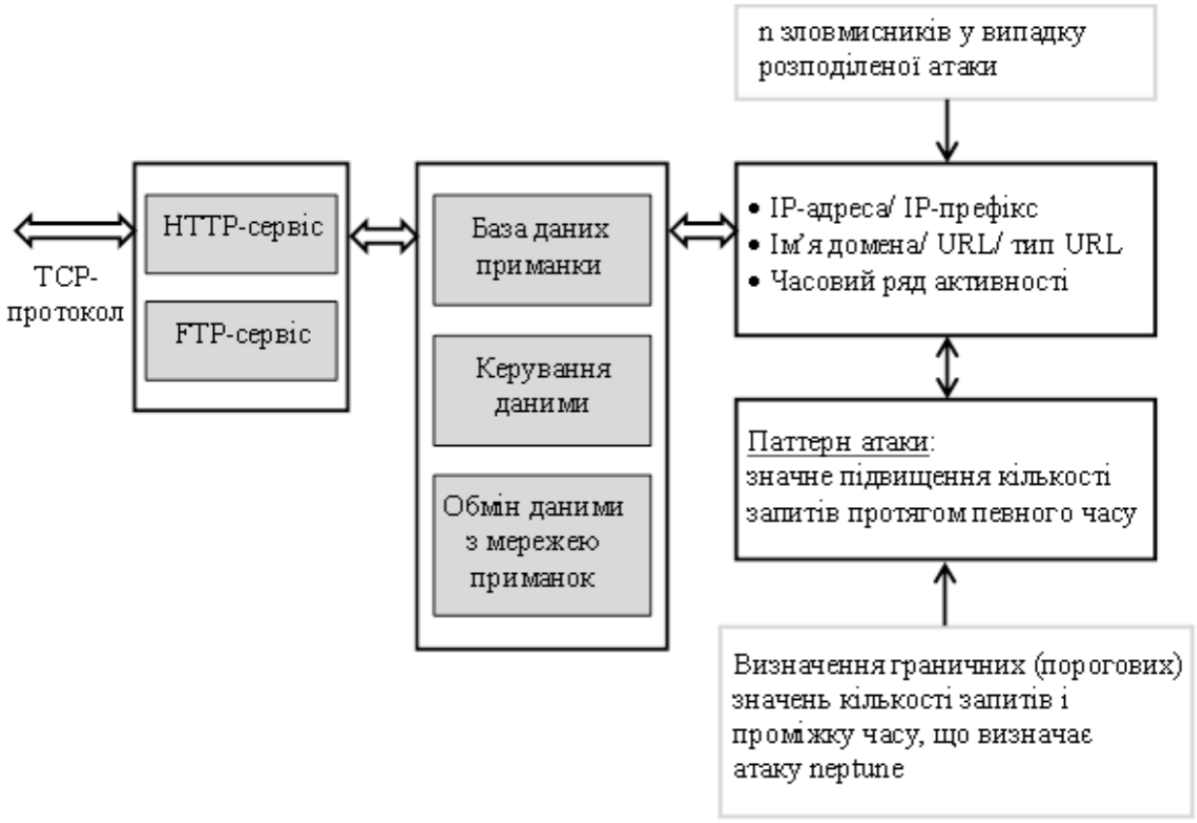


Рисунок 5.4 - Структурна схема приманки для мережної атаки neptune

Атака portsweep (рис. 5.5) передбачає, що зловмисник сканує значну кількість портів цільового серверу з метою визначення сервісів, які на ньому використовуються. Для виявлення цієї атаки на приманці має бути реалізована значна кількість портів, які можуть бути фізичні і віртуальні та відповідають портам реального сервісу. Дані, які збирає приманка такі: IP-адреса/IP-префікс; ім'я домена/URL/тип URL; наявність звернення до портів. Кількість звернень до портів формує часовий ряд активності зловмисника (зловмисників у разі розподіленої атаки). Аналіз цього ряду дає можливість класифікувати активність як зловмисну.

Розглянемо типи розповсюджених приманок для виявлення зловмисних дій в корпоративних мережах. Побудуємо моделі приманок на основі групування і узагальнення їх характеристик з метою створення мереж приманок в корпоративних мережах для покращення рівнів безпеки в них. В табл. 5.1 подано рівні роботи приманок з урахуванням її функцій.

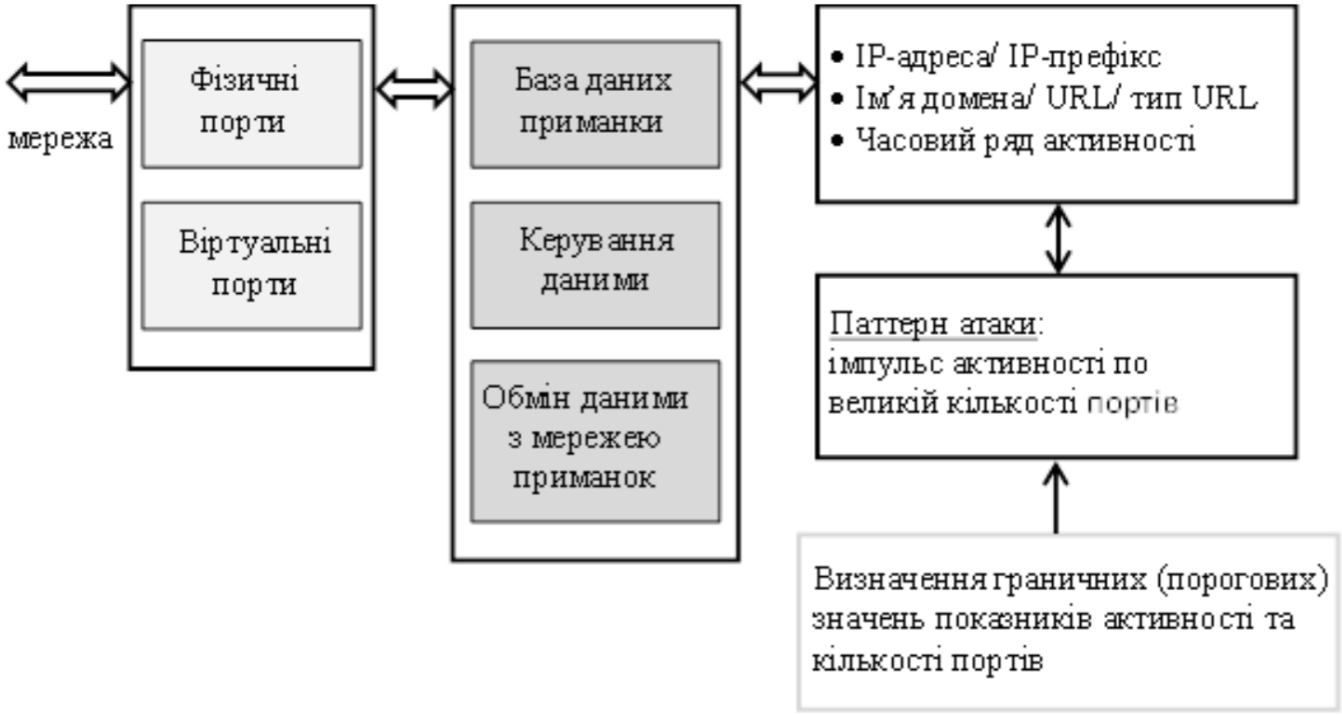


Рисунок 5.5 - Структурна схема приманки для мережної атаки portsweep

Таблиця 5.1

Рівні роботи приманок

Рівні	Виконувані функції
Виявлення	Збір мережного трафіку, повідомлення виявлення приманки зловмисником
Аналізу	Аналіз та оцінка дій зловмисника, аналіз виявалення приманки зловмисником
Реагування	Реагування на дії зловмисника
Виконання	Виявлення атак, попередження зловмисних дій

Рівень виявлення забезпечує збір інформації щодо вторгнень в роботу сервісу. До цієї інформації відносяться дані щодо виявлення приманки зловмисником, виявлення портів, що прослуховують сервер, виявлення неавторизованих облікових записів, виявлення файлів, заміщених зловмисником тощо.

На рівні аналізу зібрана інформація аналізується, визначається яка саме зафіксована активність є зловмисною та визначається рівень її небезпеки для мережі. Рівень небезпеки зловмисних дій асоціюється з рівнем шкоди, що може бути завдана

мережі. Наприклад, чи були зафіксовані дії неавторизованих користувачів, модифікації файлів тощо.

На рівні реагування формуються правила попередження та виявлення атак, сформовані на основі зібраної та проаналізованої інформації, які надалі використовуються мережею.

Рівень виконання поєднує дві основних функції. На етапі виявлення за відомими характеристиками (сигнатурами) виявляються атаки мережі на основі статичних патернів. На етапі попередження ці атаки блокуються як зловмисні.

Процес збору та аналізу інформації та реагування є неперервним. Правила виявлення динамічно оновлюються на основі інформації рівня виявлення та аналізу, що дозволяє постійно реагувати на нові види зловмисних дій та їх модифікації.

Розроблені моделі приманок для типових атак можуть бути застосовними для побудови мереж приманок в корпоративних мережах і бути включеними в мультикомп'ютерні системи антивірусних комбінованих приманок та пасток. Це дозволить їх використовувати в залежності від типів атак. Для організації функціонування такої мережі приманок необхідно використовувати методи теорії прийняття рішень з метою визначення динамічної зміни архітектури мережі приманок.

5.3. Метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками

Комплексний аналіз атак, які зафіксовані мережею приманок, передбачає пошук подібних зловмисників, пошук трендів в поведінці зловмисників, аналіз викидів, які відображають підвищення активності окремих зловмисників, сумарний аналіз викидів, що відображає підвищення сумарної активності, прогнозування активності зловмисників.

Пошук подібних зловмисників можна здійснювати на основі кластеризації їх поведінки, тобто часових рядів атак, які належать зловмисникам. Кластеризація часових рядів здійснюється різними методами, серед яких кластеризація на основі інформаційних критеріїв, кластеризація на основі гаусівських змішаних,

кластеризація на основі прихованих марківських моделей, кластеризація на основі нейронних мереж. Основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації.

Представлення даних часового ряду має на меті виконання таких задач: значне зменшення розмірів даних, виділення основних глобальних та локальних характеристик; можливість відновлення ряду з отриманого представлення. Серед методів зменшення розмірності використовуються метод сингулярного спектрального аналізу, перетворення Фур'є, вейвлет-перетворення, поліноміальні перетворення, використання авторегресивного рухомого середнього тощо.

Визначення відстані між рядами, що відображає подібність, є критичним етапом для виконання подальшої кластеризації. При порівнянні поведінки зловмисників практично немає можливості застосовувати оцінки відстані, які застосовуються в класичних методах кластеризації. Необхідно застосовувати функції порівняння часових рядів, які враховують такі особливості часових рядів як можливі шуми, часові зсуви, масштабування в часі і за амплітудою, лінійні зсуви, неоднорідності та розриви. Функції порівняння часових рядів враховують подібність у часі, формі та динаміці.

Для кластеризації часових рядів активності зловмисників використовуються різні методи кластеризації, зокрема графові (алгоритм виділення зв'язаних компонент, алгоритм FOREL, функціонали якості кластеризації), ієрархічні (агломеративні та ієрархічні алгоритми) та статистичні (EM-алгоритм, метод k-середніх), чіткі та нечіткі. У випадку чіткої кластеризації один зловмисник відноситься до одного кластеру. Аналіз активності зловмисників показує, що дії одного зловмисника можуть відноситися до декількох кластерів, тому доцільно поряд з чіткими методами кластеризації використовувати методи нечіткої кластеризації. Серед методів нечіткої кластеризації варто виділити метод с-середніх, нейромережеві (самоорганізуючі карти Кохонена тощо) та генетичні алгоритми.

Для визначення та аналізу трендів активності зловмисників здебільшого використовуються статистичні підходи, які досить широко застосовуються в економетриці. Тренд відображає загальну тенденцію зростання, спадання або

стабільність активності окремого зловмисника та групи зловмисників. Зазвичай під трендом мається на увазі глобальна довготермінова середня тенденція поведінки часового ряду. Але у випадку аналізу активності зловмисників доцільно також розглядати короткотермінові тренди в межах певного періоду, відповідно до якого приймати рішення про стан захисту мережі та подальші дії. Часовий ряд містить систематичну та несистематичну складові. В сучасних підходах до аналізу та моделювання часових рядів вважається, що часовий ряд містить три систематичних складових (рівень, тренд, періодичні коливання) та одну несистематичну (шум). Розглядаються дві моделі часових рядів, які враховують ці чотири складових: адитивна та мультиплікативна. Реальні дані можуть містити як адитивні, так і мультиплікативні складові. Для виділення тренду як однієї складової необхідно розкласти часовий ряд на складові. Одним з класичних методів є декомпозиція методом рухомого середнього, а також застосування обчислення рухомого середнього до рухомого середнього та зваженого рухомого середнього. Також поширеним методом декомпозиції є застосування поліноміальної регресії.

Аналіз викидів в одномірних та багатомірних часових рядах дозволяє проаналізувати аномально високу та аномальну низьку активність зловмисників. Це також дає інформацію про те, чи є атака розподіленою. Викиди можуть бути точковими та послідовними. Точковим викидом є точка спостереження в певний момент часу, яка відрізняється від сусідніх точок ряду (локальний викид) або від усіх точок ряду (глобальний викид). Послідовним викидом є послідовність точок, поведінка та/або значення яких відрізняються від сусідніх точок або точок ряду, при цьому окремі точки цієї послідовності можуть не бути викидами. У випадку, якщо для визначення викидів використовуються дані всього ряду, то викиди будуть глобальними, а у випадку використання сусідніх точок (часового вікна) викиди будуть локальними. Особливо доцільними для аналізу атак є методи визначення викидів, які працюють з потоками даних, тому що вони дозволяють визначати, чи є дані викидами одразу після їх надходження в реальному часі.

До методів визначення точкових викидів в одномірному та багатомірному часових рядах відносяться методи, які ґрунтується на моделях, які базуються на густині та гістограмі. Найбільш популярним визначенням точкового викиду є точка,

що суттєво відхиляється від очікуваного значення, визначення викиду на основі такого припущення ґрунтується на моделі часового рядку. Для побудови моделі часового ряду використовується ряд методів, серед яких вже згадані моделі рухомого середнього, декомпозиції часових рядів, штучних нейронних мереж. В процесі визначення викидів в потоках даних моделі періодично довчаються таким чином, щоб адаптуватися до надходження нових даних. Методи, що базуються на густині, визначають викиди на основі кількості сусідніх точок щодо потенційного викиду. Гістограмний метод ґрунтується на пошуку точок, видалення яких призводить до зменшення похибки гістограмного представлення часового ряду. У випадку багатомірного ряду точковий викид може стосуватися як однієї змінної ряду, так і декількох одночасно.

Для пошуку викидів в багатомірних рядах засовуються одномірні та багатомірні підходи. В одномірному підході багатомірний часовий ряд розглядається як сукупність одномірних рядів, до кожного з яких застосовується пошук викидів. Недоліком цього є не враховані кореляційні залежності багатомірного ряду, що в результаті може призвести до втрати інформації. Для уникнення цього та водночас використання одномірного підходу можуть застосовуватися методи зменшення розмірності багатомірного часового ряду. З одного боку це дозволяє зменшити кількість даних для аналізу і підвищити швидкість аналізу, з іншого боку врахувати кореляційні залежності. Серед таких методів метод головних компонент, аналіз незалежних компонент, T-розподілене вкладення стохастичної близькості. При багатомірному підході пошук точкових викидів здійснюється із використанням одразу всіх вихідних даних без їх попереднього перетворення та розділення.

Для знаходження послідовних викидів використовуються характеристики послідовності точок одномірного або багатомірного часового ряду. До таких характеристик відносяться довжина та періодичність. В більшості випадків визначаються послідовності викидів фіксованої довжини, але можливе також одночасне визначення послідовностей різної довжини. Порівняння послідовностей є більш складною задачею ніж порівняння точок, тому багато методів порівняння послідовностей для визначення викидів ґрунтуються не на оригінальних значення часового ряду, а на різних його представленнях. Зокрема з цією метою часто

використовується дискретизація значень часового рядку. Періодичність послідовністних викидів враховується у порівнянні з періодичністю нормальних значень часового ряду.

Прогнозування активності зловмисників передбачає раннє виявлення зловмисних дій та визначення ймовірності атак та їх характеристик на основі поточного стану та попередньо виявлених паттернів. Аналіз дій зловмисників дозволяє отримати патерни атак. Атаки можуть бути короткі та тривалі, інтенсивні та відносно непомітні. Вивчення цих патернів дозволяє вживати заходів підвищення безпеки мережі задля послаблення впливу зловмисників та зменшення втрат від втручань. Для прогнозування одномірних та багатомірних часових рядів розроблено значну кількість методів, більшість яких може бути застосована та адаптована до прогнозування різних типів атак, зокрема в мережі приманок.

До традиційних методів прогнозування часових рядів відноситься ряд методів, які ґрунтуються на авторегресії, рухомому середньому та згладжуванні. Класичні методи прогнозування часових рядів передбачають оцінку періодичності (сезонності), тренду та стаціонарності ряду, тобто передбачають певні характеристики механізму генерації значень ряду. Але в багатьох випадках, в тому числі це стосується поведінки атак, механізм генерації подій є досить складним і попередньо невідомим. В цьому випадку генеровані дані не можуть бути описані аналітичними рівняннями. В часових рядах, які описують зловмисні дії, може бути відсутній або неявний тренд. Так само період може бути відсутній або відповідати складній залежності. В цьому випадку застосування традиційних методів аналізу та прогнозування часових рядів може не привести до бажаних результатів. Натомість сучасні методи машинного та глибокого навчання не передбачають, що часовий ряд має відповідати певним характеристикам, і дозволяє прогнозувати поведінку ряду навіть якщо механізм його генерації невідомий. На сьогоднішній день розроблено ряд нейромережевих методів прогнозування одномірних та багатомірних часових рядів, які ґрунтуються на використанні різної архітектури нейронних мереж, серед яких нейронні мережі прямого розповсюдження (авторегресивні нейронні мережі, авторегресивні нейронні мережі з зовнішніми входами), рекурентній нейронні мережі (нейронні мережі Елмана та Джордана, LSTM та GRU нейронні мережі), згорткові

нейронні мережі. Методи глибокого навчання постійно вдосконалюються, розробляються нові механізми підвищення точності та ефективності нейронних мереж, нові комбінації архітектури (наприклад, рекурентні згорткові мережі).

Для знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками розробимо метод, який може бути імплементований в архітектурі мультикомп'ютерних систем антивірусних комбінованих приманок та пасток. Метод буде позиціонуватись як один з варіантів вирішення завдання щодо знаходження схожих зловмисників в мережі приманок.

Розглянемо спочатку частотні характеристики джерел атак. Інформація, яку збирає приманка, описує характеристики зловмисників. Серед таких характеристик важливе місце займають частотні характеристики, серед яких кількість джерел атак за одиницю часу, кількість нових джерел, що додаються за одиницю часу, кількість джерел атак в певній IP-агломерації, кількість джерел на кількість атак, кількість запитів за одиницю часу, кількість переданих пакетів за одиницю часу. Частотні характеристики атак в багатьох випадках дозволяють визначити тип атаки, а отже дають можливість її прогнозувати. А також на основі частотних характеристик можна визначити рівень небезпеки зловмисника в реальному часі та вжити відповідних заходів.

Відношення джерел атак до приманок можна описати як багато до багатьох, оскільки один зловмисник здійснює атаки на різні цілі і так само одна приманка піддається впливу атак з багатьох джерел. Якщо розглядати відношення один до багатьох (одне джерело атаки, багато приманок), то отримаємо профіль зловмисника. Якщо розглядати відношення багато до одного (багато джерел атак, одна приманка), то отримаємо характеристики розподіленої атаки, а також профіль вразливостей приманки. Профіль зловмисника, який може атакувати певну кількість приманок, може бути розглянутий як інтегральний профіль, що складається з профілів один до одного (одне джерело атаки, одна приманка). Для отримання інтегрального профілю зловмисника необхідно отримати характеристики атак на приманки з точки зору відношення один до одного. Якщо розглядати всі атаки на приманку в межах заданого часового інтервалу, то вони в загальному випадку можуть бути результатом різних типів атак.

Розглянемо в якості поведінкової характеристики зловмисника часовий ряд, що представляє собою кількість запитів від одного джерела атаки до однієї приманки за інтервал часу в одну секунду. Припустимо, що всі запити є зловмисною активністю.

Часовий ряд кількості запитів від i-го джерела атаки до j-ї приманки за одиницю часу задамо так:

$$X^{ij} = \{x_1^{ij}, x_2^{ij}, x_3^{ij}, \dots, x_k^{ij}\}, \quad (5.6)$$

де x_k^{ij} – кількість запитів від i-го джерела до j-ї приманки за 1 сек.; k – тривалість досліджуваного часового вікна; i=1, 2, 3, …, m, m – кількість джерел атак; j=1,2,3,…n; n – кількість приманок.

Здійснимо вибір інформаційних критеріїв для кластеризації. Завдання кластеризації часових рядів передбачає виявлення патернів, для подання часового ряду. Особливість кластеризації часових рядів полягає в тому, що ознаки змінюються в часі. Методи кластеризації часових рядів поділяють на три типи: методи, в яких використовуються безпосередньо необроблені дані; методи, які використовують вилучені ознаки; методи, які базуються на моделях часових рядів.

Методи, що ґрунтуються на моделях, передбачають попередню трансформацію даних часових рядів шляхом визначення параметрів моделі. Використовують для цього моделі різного типу, зокрема: динамічна регресія; ARMA, ARIMA, ARFIMA; GARCH, NGARCH; нейромережеві моделі. Метою використання параметрів моделі часового ряду замість його значень є перехід до простору ознак, в якому можна виконати кластеризацію. Для визначення відстаней між параметрами моделей часових рядів використаємо такі інформаційні критерії, як інформаційний критерій Акаіке [11], модифікований критерій Акаіке, інформаційний критерій Кульбака [12], Байєсівський інформаційний критерій [13].

Розглянемо більш детально визначення інформаційного критерію як міри подібності двох часових рядів на основі байєсівського інформаційного критерію. Нехай задані два часових ряди, які представлені векторами $X = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_{n_x}\}$ та $Y = \{\boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_{n_y}\}$. Необхідно оцінити наступні дві гіпотези [14]:

$$H_1: x_1, x_2, \dots, x_{n_x}, y_1, y_2, \dots, y_{n_y} - N(\mu, \Sigma), \quad (5.7)$$

$$H_2: \quad x_1, x_2, \dots, x_{n_x} - N(\mu_X, \Sigma_X); \\ y_1, y_2, \dots, y_{n_y} - N(\mu_Y, \Sigma_Y). \tag{5.8}$$

Гіпотеза H_1 передбачає, що X та Y отримані з однієї моделі, гіпотеза H_2 означає, що X та Y формуються двома моделями. Нехай $Z = X \cup Y$ та $n = n_x + n_y$. Тоді, різниця між величинами байєсівського критерію для двох гіпотез може бути визначена так:

$$\Delta BIC(X,Y) = BIC(H_1, Z) - BIC(H_2, Z) =$$

$$= log\, p\left(X|\hat{\mu}_X, \hat{\Sigma}_X\right) + log\, p\left(Y|\hat{\mu}_Y, \hat{\Sigma}_Y\right) - log\, p\left(Z|\hat{\mu}, \hat{\Sigma}\right) - \frac{1}{2}\lambda\left(d + \frac{1}{2}d(d+1)\right) log\, n =$$

$$= \frac{n}{2} log\left|\hat{\Sigma}\right| - \frac{n_x}{2} log\left|\hat{\Sigma}_X\right| - \frac{n_y}{2} log\left|\hat{\Sigma}_Y\right| - \frac{1}{2}\lambda\left(d + \frac{1}{2}d(d+1)\right) log\, n, \tag{5.9}$$

де $\hat{\mu}$, $\hat{\mu}_X$ та $\hat{\mu}_Y$ - вектори середніх значень вибірок Z, X та Y відповідно; $\hat{\Sigma}$, $\hat{\Sigma}_X$ та $\hat{\Sigma}_Y$ - коваріаційні матриці вибірок; d – розмірність вектора ознак [15]. Чим менша величина ΔBIC, тим більш схожими є два часових ряди. За умови $\lambda = 0$ відстань ΔBIC є еквівалентною відношенню правдоподібності.

Процедура кластеризації часових рядів, які характеризують профілі зловмисників, ґрунтується на процедурі агломеративної кластеризації та включає такі кроки:

1. Визначення початкових кластерів.

На першому етапі кластеризації кожний часовий ряд представляє собою кластер. Відповідно множина кластерів має такий вигляд:

$$C = \{C_1, C_2, C_3, \dots, C_l\}, \tag{5.10}$$

де $C_1 = \{X^{11}\}$,$C_2 = \{X^{12}\}$, $C_3 = \{X^{13}\}$, і так далі, $C_l = \{x^{mn}\}$; $l = m \times n$ - кількість початкових кластерів.

2. Визначення відстаней між парами кластерів, які визначають на основі одного з інформаційних критеріїв, наведених вище.

Якщо в якості такого інформаційного критерію використовується байєсівський інформаційний критерій, то відстань між двома кластерами $C_i = \{X_1, X_2, X_3, \dots, X_m\}$ та $C_j = \{Y_1, Y_2, Y_3, \dots, Y_n\}$ визначається як

$$D_{ij} = \Delta BIC(C_i, C_j) = \frac{\sum_{a=1}^{m}\sum_{b=1}^{n}\Delta BIC(X_a, Y_b)}{|C_i \times C_j|}, a \neq b, \quad (5.11)$$

де m – кількість об'єктів (часових рядів) в кластері C_i; n – кількість об'єктів (часових рядів) в кластері; $i=1,2,3…l$; $j=1,2,3…l$; l – кількість кластерів поточної ітерації процесу кластеризації.

3. Визначення з множини відстаней $D = \{D_{12}, D_{13}, \dots, D_{ij}, \dots, D_{l-1,l}\}$ мінімальної для поточної ітерації $D_{min\,iter} = min(D) = D_{ij}$, вибір відповідної пари кластерів C_i та C_j та об'єднання множин об'єктів цих двох кластерів в один кластер $C_{join(ij)} = C_i \cup C_j$.

4. Визначення інтегрального критерію відстаней між об'єктами всередині кластера.

Інтегральний критерій визначається на основі одного з інформаційних критеріїв. Якщо цей критерій визначається на основі байєсівського інформаційного критерію, то його визначимо так:

$$J = \frac{\sum_{i=1}^{l}\Delta BIC(C_i)}{l}, \quad (5.12)$$

де $\Delta BIC(C_i)$ - відстань між об'єктами всередині одного кластеру; i=1,2,3,…,l; l – кількість кластерів. Ця відстань для кластера $C_i = \{X_1, X_2, X_3, \dots, X_m\}$ визначається за співвідношенням:

$$\Delta BIC(C_i) = \frac{\sum_{a=1}^{m}\sum_{b=a}^{m}\Delta BIC(X_a, X_b)}{m}. \quad (5.13)$$

5. Перевірка умови зупинки процесу об'єднання кластерів.

Якщо умова виконана, отримують остаточну множину кластерів $C_{res} = \{C_1, C_2, C_3, \dots, C_{lres}\}$, де lres – остаточна кількість кластерів. Виконання пунктів 2-5 повторюється до тих пір, поки умова зупинки не буде виконана.

Для зупинки процесу об'єднання кластерів використовується один з трьох таких критеріїв:

1. Кількість кластерів. Наявна вимога щодо задання кількості кластерів, що може потребувати попередньої оцінки. В загальному випадку кількість кластерів профілів зловмисників не є попередньо відомою. Тому, необхідно застосовувати цей критерій зупинки для задачі визначення рівня небезпеки зловмисника.

2. Абсолютний мінімум функції залежності інтегрального критерію від числа ітерацій об’єднання кластерів $min\big(J(k)\big)$, де k – кількість ітерацій. У цьому випадку обирається множина кластерів, що відповідає ітерації, на якій спостерігається мінімум *J(k)* (рис. 5.6 (1)). Цей критерій зупинки забезпечує максимально чистоту отриманих кластерів. Недоліком є те, що частина кластерів може бути неповною, і зловмисників одного типу може містити більше ніж один кластер.

3. Градієнтний критерій. У цьому випадку визначається стрибок функції залежності відносного градієнта $\nabla J(k)/J(k)$ від кількості ітерацій та обирається множина кластерів, відповідна цій ітерації (рис. 5.6 (2)).

4. Результати кластеризації зловмисників

Для проведення експериментальних досліджень було використано датасет мережі приманок [16]. З датасету були відібрані часові ряди кількості запитів за 1 секунду від одного джерела атаки до однієї приманки, які сформували набір часових рядів для кластеризації. Кластеризація проводилася із використанням трьох

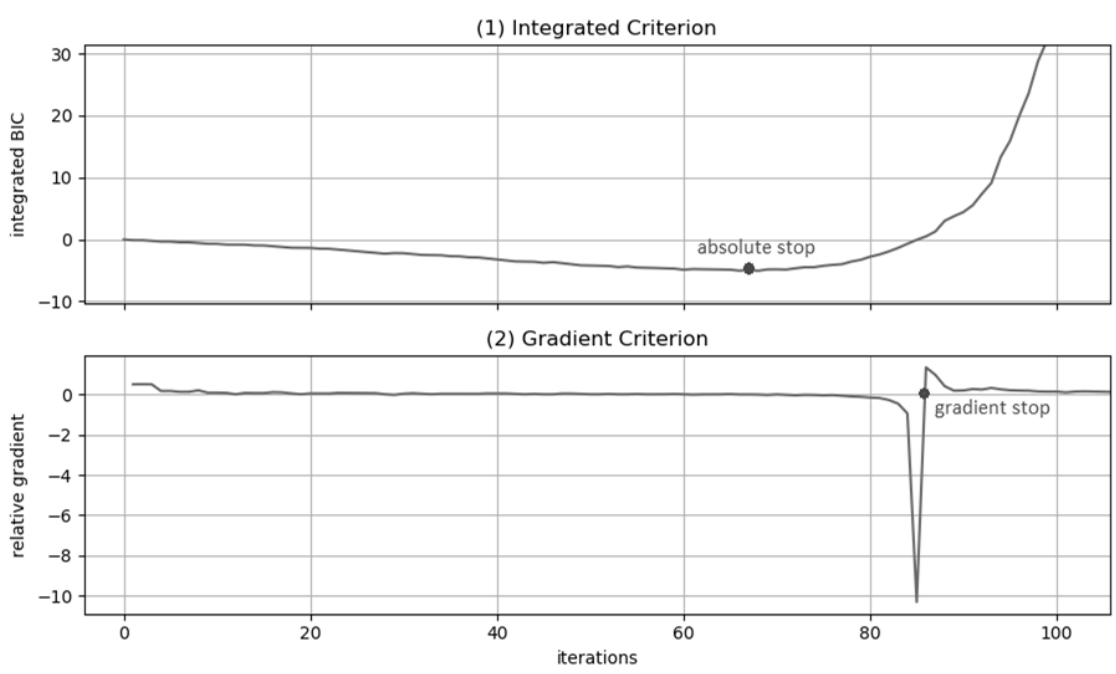


Рисунок 5.6 - Критерії зупинки процесу об’єднання кластерів: (1) - залежність інтегрального критерію відстаней між об’єктами всередині кластера від кількості ітерацій J(k); (2) - залежність відносного градієнту функції $\nabla J(k)/J(k)$від кількості ітерацій інформаційних критеріїв (AIC, KIC, BIC), також з використанням двох критеріїв зупинки процесу кластеризації (абсолютний мінімум та відносний градієнт)

Найвищі показники точності показала кластеризація на основі BIC критерію із зупинкою за відносним градієнтом. Точність кластеризації перевищила 80%, а зупинка за відносним градієнтом забезпечила оптимальне співвідношення чистоти кластерів та їх повноти. Також, було проведено кластеризацію з числом кластерів 3 для визначення відносного рівня небезпеки зловмисника: високого, середнього та низького (рис. 5.7).

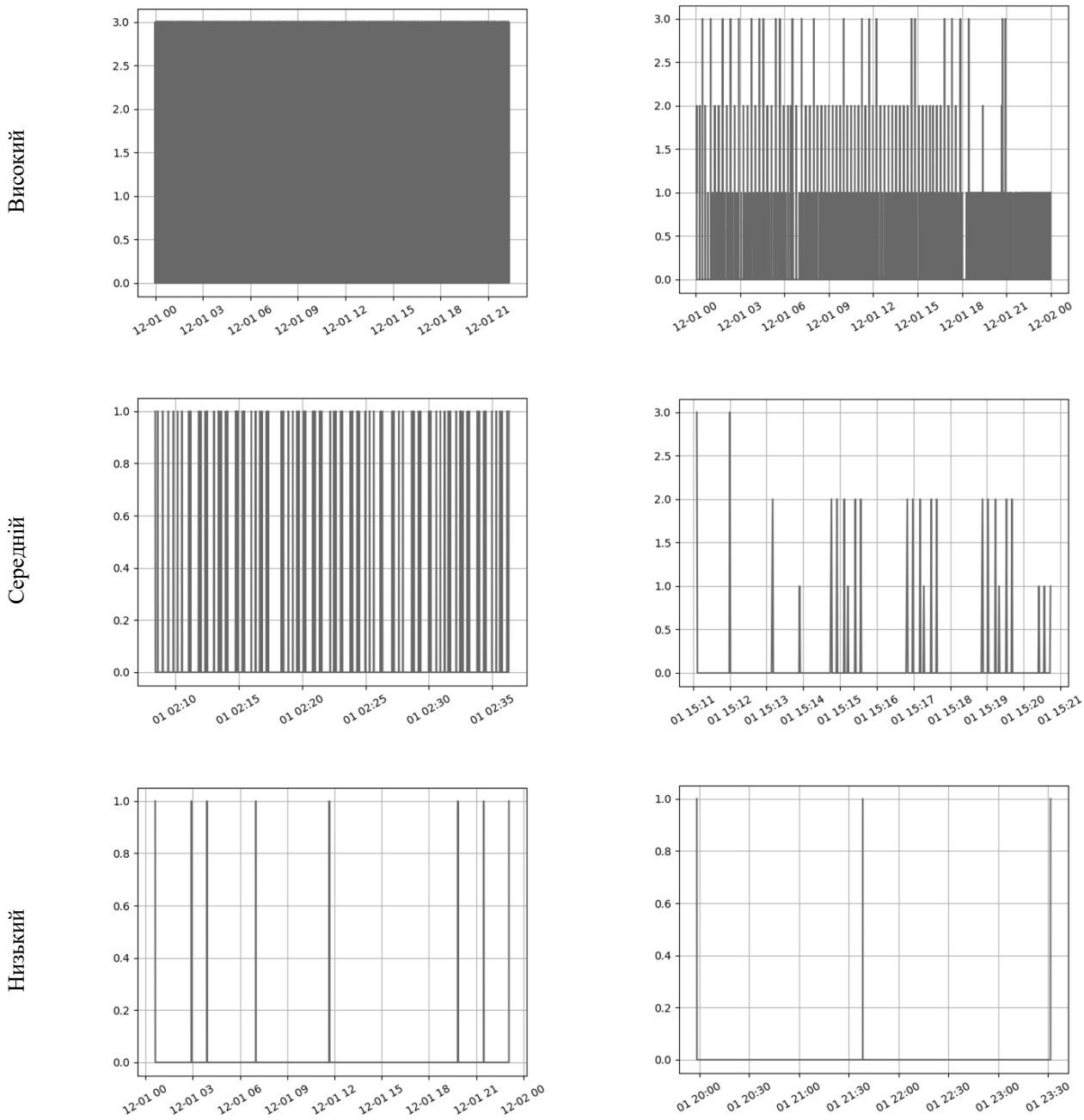


Рисунок 5.7 - Приклади частотних характеристик зловмисників з різними рівнями загрози

Збір та аналіз приманками поведінкових характеристик зловмисників дозволяє виявляти та групувати нові типи атак, що є надзвичайно важливим для систем виявлення вторгнень. Розроблений метод дозволяє проводити неперервний пошук подібних зловмисників з врахуванням їх динамічних характеристик. Запропонована процедура агломеративної кластеризації на основі інформаційних критеріїв дозволяє отримати достатню точність кластеризації та визначити рівень небезпеки зловмисника.

Розглянемо два різних підходи до кластеризації.

В першому підході використаємо нейромережевий автоенкодер (рекурентний) з подальшою кластеризацією на основі k- means.

В другому підході використаємо нейромережевий автоенкодер (згортковий) з подальшою агломеративною кластеризацією.

Кількість підходів має бути значною і різноманітною для формування різних варіантів виконання завдань.

Атаки різного типу, в тому числі DoS атаки, мають характерну поведінку в часі, тому доцільно виявляти патерни атак в динаміці, що передбачає аналіз багатомірних часових рядів, сформованих з даних приманок. Мережа приманок представляє собою розподілену мережу, яка складається з приманок різного типу: фізичних та віртуальних приманок; приманок низького, середнього та високого рівня взаємодії; спеціалізованих приманок різних сервісів.

Виявлення патернів атак включає ряд етапів (рис. 5.8).

Для виявлення патернів в багатомірному часовому ряді необхідно розбити його на сегменти. Є значна кількість підходів до сегментації, починаючи від простого використання вікна, що зсувається по осі часу до більш складних та якісних алгоритмів, таких як [23]. Для виявлення патернів в часових рядах важко обрати однозначний підхід, оскільки для різних типів даних різні алгоритми та міри подібності можуть давати різні кінцеві результати. Тому, важливо обрати з існуючих такі, які забезпечать найкраще групування вихідних даних [24]. А також необхідно використовувати відповідне представлення часових рядів, основною властивістю якого є те, що схожі часові ряди мають схожі представлення.

Представлення часових рядів отримується з використанням нейромережного згорткового автоенкодера, який забезпечує зменшення розмірності та виявлення ознак часового ряду, необхідних для кластеризації.

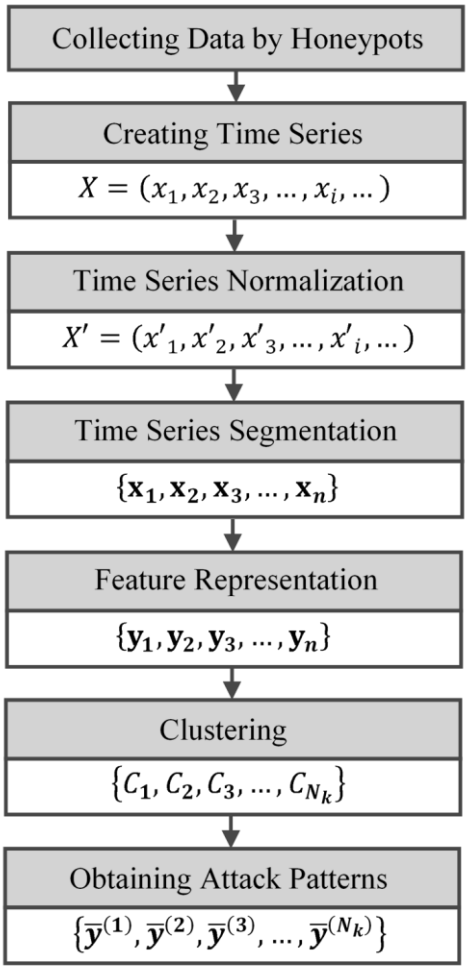


Рисунок 5.8 – Етапи атак

Попередня обробка часових рядів виконується на основі нейромережного згорткового автоенкодера (рис. 5.9). Автоенкодер складається з згорткового енкодера та згорткового декодера. Згортковий енкодер складається з стеку згорткових блоків. Згортковий блок включає згорковий шар, випрямляючий лінійний шар (relu), шар об'єднання (pooling) та шар нормалізації. Згортковий шар перетворює карту ознак розміру $d_1^{(l-1)} \times d_1^{(l-1)} \times d_1^{(l-1)}$ в іншу карту ознак розміром $d_1^{(l)} \times d_1^{(l)} \times d_1^{(l)}$. Вихід $X_i^{(l)}$ шару l містить $d_1^{(l)}$ карт ознак (число фільтрів) розміру $d_2^{(l)} \times d_3^{(l)}$. Відповідно до розміру фільтру згортка відбувається тільки по осі часу.

Шар об’єднання призначений для зменшення розмірів карт ознак та виділення точок, які передають в наступні шари більш важливу інформацію та ігнорують несуттєву. Об’єднання виконується тільки по осі часу.

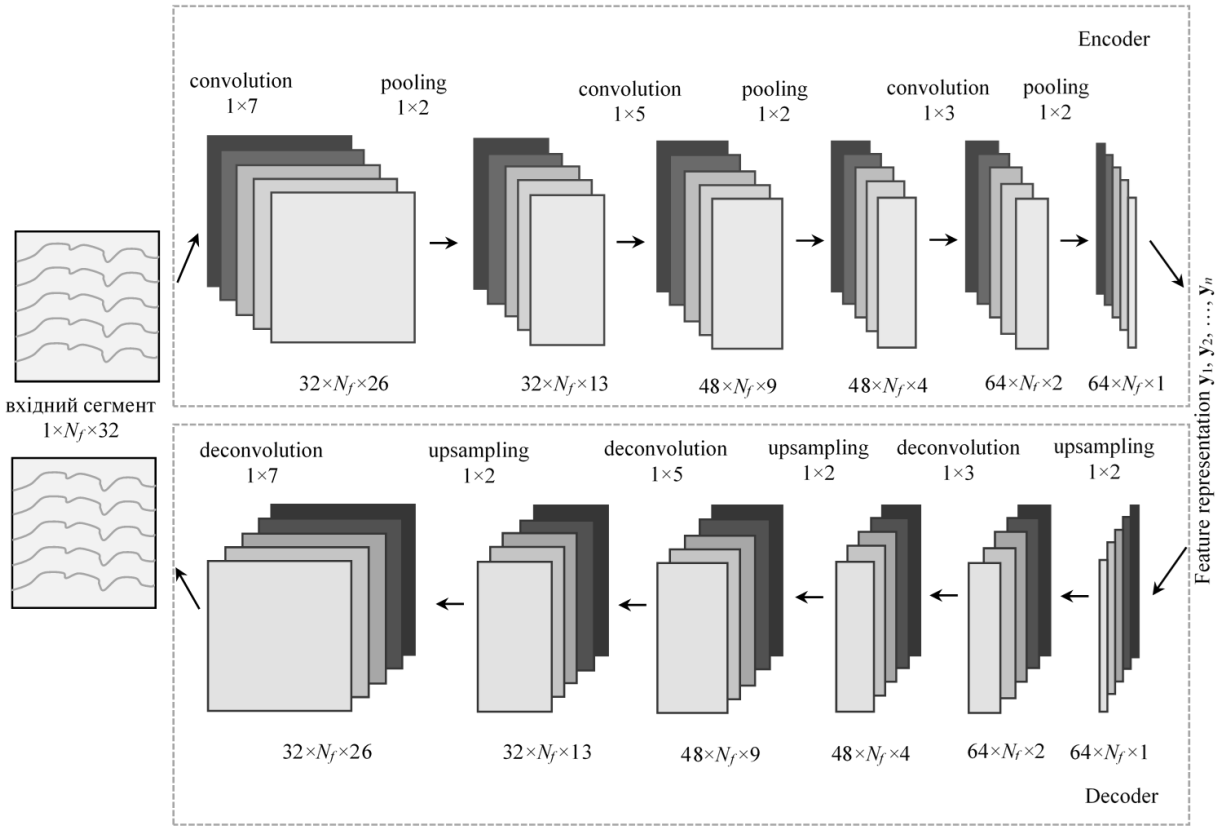


Рисунок 5.9 – Розподіл шарів

В якості екземплярів даних для навчання згорткового автоенкодера використовуються сегменти багатомірного часового ряду, отриманого за допомогою вікна, яке ковзається. Таким чином, розмір одного сегменту $1 \times N_f \times l_w$, де N_f – число ознак багатомірного часового ряду, l_w – довжина вікна, 1 – глибина сегменту. Для отримання наступних екземплярів вікно зсувається по осі часу із заданим кроком.

Функція втрат навчання автоенкодера містить дві складових: функцію відновлення згорткового декодера та функцію, яка відображає відстань між об’єктами всередині кластерів:

$$L(\theta) = L_r(\theta) + L_c(\theta). \tag{5.14}$$

Функцію відновлення декодером пропонується обирати з функцій втрат, які використовуються для задач регресії, зокрема це: середньоквадратична похибка, середня абсолютна похибка, функція втрат Хубера.

Функцію, що відображає відстань між об'єктами всередині кластера, характеризує інтегральний критерій, наведений нижче. Розрахунок цього критерію ґрунтується на використанні відстаней, тобто мір подібностей між сегментами. Ознаки отримані із використанням згорткового енкодера також представляють собою часові ряди, тому доцільно для їх кластеризації використовувати міри подібності, придатні для порівняння послідовностей [25]. Використаємо такі міри подібності:

1) відстань, отримана за алгоритмом динамічної трансформації часової шкали (DTW) [26];

2) відстань, отриману за алгоритмом Global Alignment Kernel (GAK) [27];

3) відстань отриману за уніфікованим алгоритмом (soft-DTW) [28].

Аналіз та кластеризація даних, які характеризують зловмисні дії, включає такі кроки:

1) формування часового ряду з даних, зібраних мережею приманок та їх нормалізація;

2) сегментація часового ряду на окремі сегменти з використанням вікна, що ковзається або відповідно до обраного алгоритму;

3) перший етап навчання згорткового автоенкодера з використанням однієї складової функції втрат $L(\theta)$ – функції відновлення згорткового декодера $L_r(\theta)$;

4) процесінг сегментів часових рядів згортковим енкодером та отримання ознак сегментів;

5) процедура агломеративної кластеризації, яка відповідає такій послідовності:

а) визначення початкових кластерів; на першій ітерації кластеризації кожний сегмент представляє собою кластер; відповідна множина кластерів $C = \{C_1, C_2, \ldots, C_{N_{k1}}\}$, де $C_1 = \{\mathbf{y}_1\}$, $C_1 = \{\mathbf{y}_2\}$, …, $C_{N_{k1}} = \{\mathbf{y}_n\}$.

б) визначення відстаней між парами кластерів $\{d_{12}, d_{13}, \ldots, d_{ij}, \ldots\}$, вибір пари кластерів C_i та C_j з мінімальною відстанню та їх об'єднання $C_{join(ij)} = C_i \cup C_j$; відстань між двома кластерами $C_i = \{\mathbf{y}_{i1}, \mathbf{y}_{i2}, \ldots \mathbf{y}_{im}\}$ та $C_j = \{\mathbf{y}_{j1}, \mathbf{y}_{j2}, \ldots \mathbf{y}_{jm}\}$:

$$d_{ij} = d(C_i, C_j) = \frac{\sum_{a=1}^{m}\sum_{b=1}^{n} d(\mathbf{y}_{ia}, \mathbf{y}_{jb})}{|C_i \times C_j|}, \ a \neq b. \tag{5.15}$$

в) визначення інтегрального критерію відстаней між об'єктами всередині кластера:

$$J = \frac{\sum_{i=1}^{l} d(C_i)}{l}, \tag{5.16}$$

де l – кількість кластерів, $d(C_i) = \sum_{a=1}^{m}\sum_{b=1}^{m} d(\mathbf{y}_a, \mathbf{y}_b) \Big/ l$ - відстань для кластера C_i.

г) перевірка умови зупинки об'єднання кластерів; виконання пунктів (б)-(г) повторюється до досягнення мінімуму інтегрального критерію, що є умовою зупинки.

6) виділення патернів зловмисних дій; патерн атаки відображається усередненим сегментом кластера; усереднені сегменти отримуємо на основі алгоритму динамічного перетворення часової шкали [29]; серед сегментів k-го кластеру $\{\mathbf{y}_1^{(k)}, \mathbf{y}_2^{(k)}, \ldots \mathbf{y}_n^{(k)}\}$ обирається медоід $\bar{\mathbf{x}}^{(k)}$, який задовольняє умові:

$$\arg\min_{\mathbf{x} \in E} \sum_{i=1}^{n} d_{dtw}^2 \left(\bar{\mathbf{y}}^{(k)}, \mathbf{y}_i^{(k)}\right). \tag{5.17}$$

В умовах значної кількості об'єктів у кластері використовується задане число ітерацій пошуку метоіда, що дозволяє отримати компроміс між об'ємом обчислень та точністю. Множина медоідів $\{\bar{\mathbf{y}}^{(1)}, \bar{\mathbf{y}}^{(2)}, \ldots \bar{\mathbf{y}}^{(N_k)}\}$ є множиною патернів атак.

7) тюнінг (другий етап) навчання згорткового автоенкодера із функцією втрат $L(\theta)$, що містить дві складових – функцію відновлення згорткового декодера та функцію, яка відображає відстань між об'єктами в кластерах;

8) використання патернів для виявлення атак в режимі реального часу.

Результати експериментального аналізу подано в п. 6.2.5.

Таким чином, метод агломеративної кластеризації зловмисних дій, представлених часовими рядами активності зловмисників. Препроцесінг початкових часових рядів виконується згортковим енкодером, який дозволяє виділити характерні ознаки активності та знизити розмірність даних для кластеризації. Поєднання функції втрат відновлення декодером та функції, що відображає відстань між об'єктами в

кластерах, дозволяє отримати більше репрезентативне представлення часових рядів для кластеризації, і підвищити точність кластеризації в цілому.

Кластеризація даних, які змінюються в часі є ускладненою в зв'язку з непрозорістю міри подібності порівняно із статичними даними. Крім того часові ряди можуть мати різну розмірність і взаємозв'язки між ними часто мають неявну природу. Безпосередня кластеризація часових рядів потребує використання даних високої розмірності та часто не в змозі виявити приховані взаємозв'язки між об'єктами. Тому, в більшості випадків потребує попередньої екстракції ознак, тобто перетворення до простору ознак, придатного для коректної кластеризації.

Збір даних мережею приманок. Мережа приманок, частину якої подано на рис. 1, представляє собою багаторівневу множину інтелектуальних приманок, які виконують постійний моніторинг мережі. Мережа включає зовнішні приманки, приєднані до мережі інтернет перед брандмауером; приманки, розташовані в зоні ДМЗ; внутрішні приманки, розташовані всередині мережі. Мережа приманок поряд із статичними, містить віртуальні приманки. Важливою перевагою такої мережі приманок є можливість відслідковувати розповсюдження розподілених атак та виявляти їх паттерни. Цей процес в більшості випадків розбивається на три етапи: а) вибір і вилучення ознак та представлення паттернів; б) визначення мір подібності, придатних до виявлення паттернів; в) групування схожих патернів.

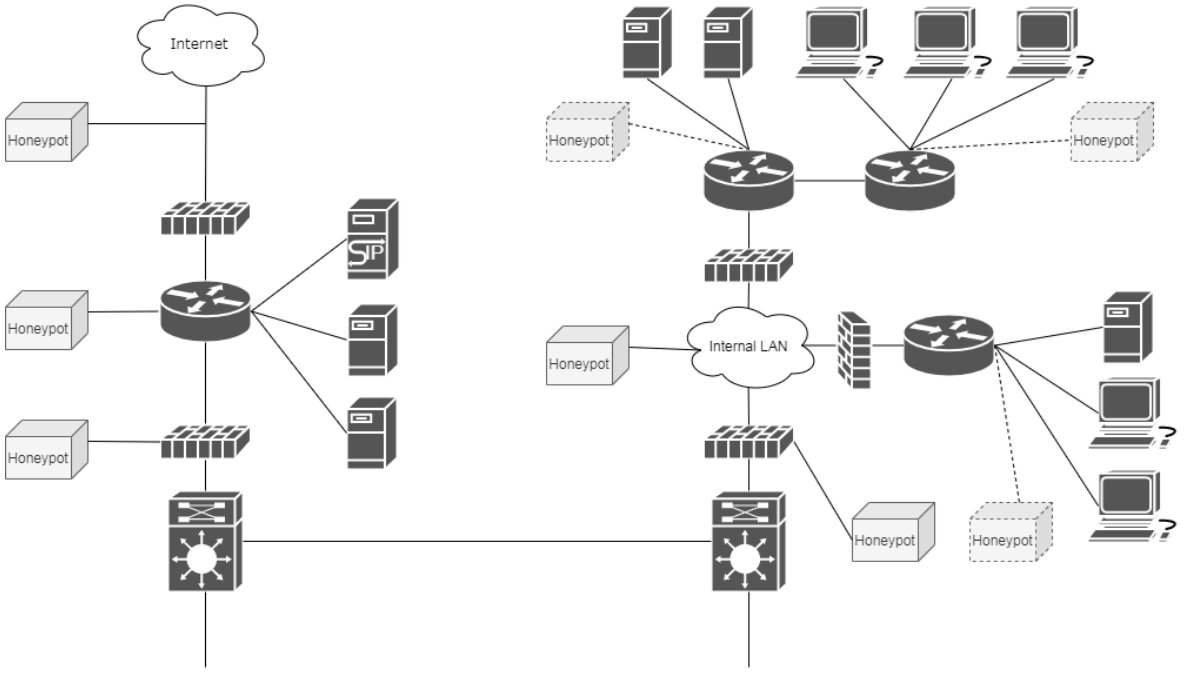


Рисунок 5.10 – Частина системи з приманками

Перший крок передбачає вилучення з масиву даних певних ознак, що відображають відповідні характеристики зловмисних дій. Дані, які збирає мережа приманок та дані, які можна отримати на основі їх аналізу: кількість зловмисних джерел за одиницю часу; кількість нових зловмисних джерел за одиницю часу; кількість зловмисних джерел в певній IP-агрегації; кількість зловмисних джерел відносно кількості атак; кількість пакетів, прийнятих за одиницю часу; обсяг даних, прийнятих за одиницю часу; кількість пакетів, відправлених за одиницю часу; обсяг даних, відправлених за одиницю часу; кількість електронних повідомлень, отриманих за одиницю часу; обсяг даних на одне повідомлення; кількість сесій за одиницю часу; тривалість сесії; час між сесіями; час функціонування зловмисного джерела. Ці дані формують часові ряди зловмисної активності на приманках:

$$X^1 = \mathrm{x}_1^1, \mathrm{x}_2^1, \dots, \mathrm{x}_t^1, X^2 = \mathrm{x}_1^2, \mathrm{x}_2^2, \dots, \mathrm{x}_t^2, \dots X^n = \mathrm{x}_1^n, \mathrm{x}_2^n, \dots, \mathrm{x}_t^n, \quad (5.18)$$

де n - кількість приманок в мережі, t- тривалість часового вікна. Часове вікно зсувається в часі з кроком, величина якого залежить від часу, необхідного для проведення обчислень.

Дані ознак є числовими, значення різних ознак знаходяться в різних діапазонах, тому потребують попереднього масштабування. Доцільно використовувати масштабування до діапазону [0, 1] кожної ознаки. Числовий ряд кожної ознаки $\{x_1, x_2, \dots, x_n\}$ перетворюється до часового ряду $\{x'_1, x'_2, \dots, x'_n\}$ відповідно до співвідношення $x' = \frac{x - x_{min}}{x_{max} - x_{max}}$.

Дані, які збирає мережа приманок, представляють собою часові ряди фактично неперервні в часі. Для кластеризації та виявлення пат тернів необхідно обрати часове вікно, в межах якого буде проводитися аналіз. Для вибору тривалості вікна можна відокремити два підходи: 1) часове вікно фіксованої тривалості t_w, яке зсувається в часі з кроком t_s; 2) часове вікно, отримане на основі попередньої сегментації. Перший підхід є простими і потребує тільки визначення двох величин. Для отримання часового вікна на основі сегментації може бути застосований Bayesian Change Point Analysis. Слід враховувати, що сегментація багатомірних часових рядів є окремою задачею, та її вирішення виходить за межі розгляду даної роботи.

Виявлення патернів не передбачає однозначної процедури для будь-яких типів даних. Різні методи кластеризації забезпечують різне розділення груп, більше того один і той же метод кластеризації може привести до різних результатів за різної початкової ініціалізації. Тому, надзвичайно важливо із множити існуючих методів кластеризації та мір подібності обрати ті, які найкращим чином згрупують наявні дані. Це одна з причин використання багатьох підходів до виявлення паттернів та їх групування у мережах приманок.

Розглянемо архітектуру автоенкодера. Попередня обробка часових рядів виконується на основі нейромережного рекурентного автоенкодера (рис. 5.11).

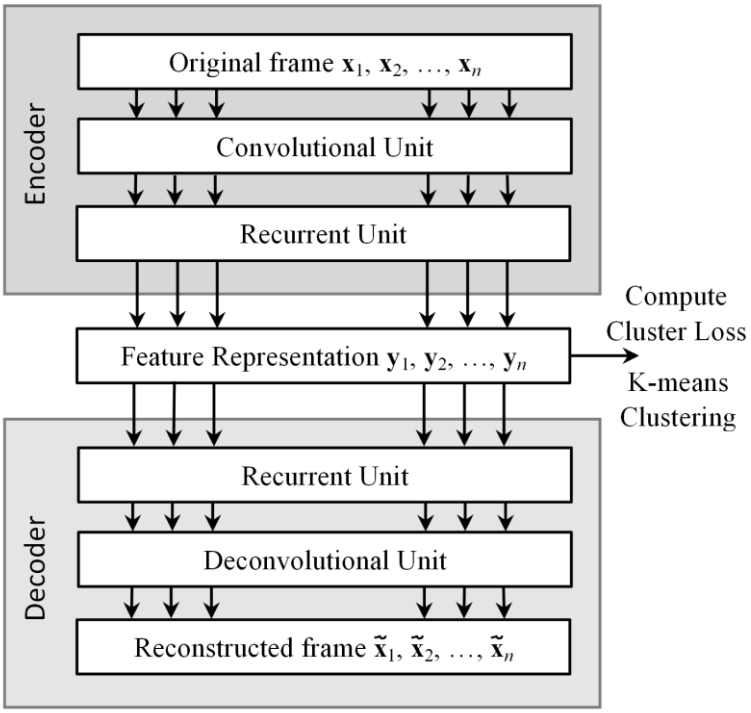


Рисунок 5.11 – Архітектура рекурентного автоенкодера

Автоенкодер складається з рекурентного енкодера та рекурентного декодера. Рекурентний енкодер в свою чергу складається з згорткового блоку та рекурентного блоку. Згортковий блок включає згортковий шар з ядром згортки 1×1, згортковий шар з ядром згортки n×1 (n=3, 5, 7 – розмір ядра по осі часу, таким чином згортка виконується по осі часу) шар MaxPool з ядром 2×1 (2 – розмір ядра по осі часу) та шар BatchNormalization. Шар MaxPool використовується у випадку, якщо кількість відліків необхідно зменшити перед обробкою рекурентним блоком. При використанні ядра 2×1 кількість точок по осі часу зменшується вдвічі.

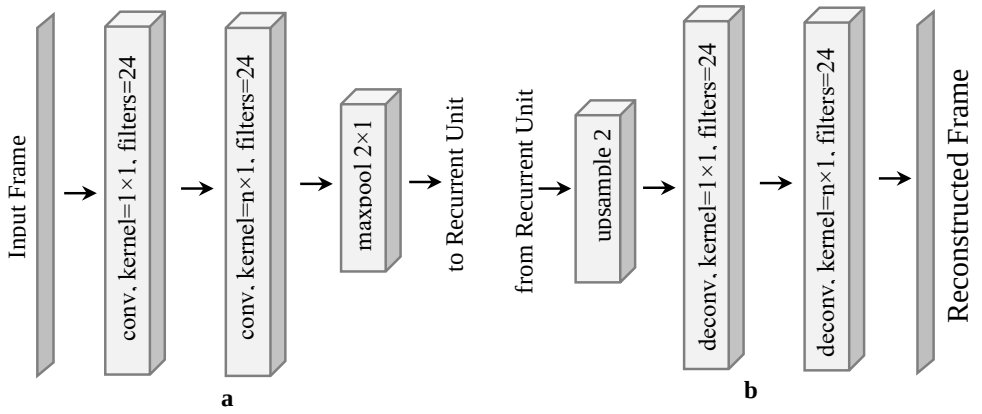


Рисунок 5.12 – Архітектура рекурентного енкодера та рекурентного декодера

Рекурентний блок представляє собою стек *m* LSTM-шарів з residual зв'язками (рис. 5.12). LSTM представляє собою модифікацію RNN архітектури, яку доцільно використовувати для моделювання даних послідовностей. Навчання RNN для врахування довготермінових залежностей є досить непростою задачею в зв'язку з проблемою зникаючого та «вибухаючого градієнту». Одним з рішень, для усунення проблеми «вибухаючого» градієнту є використання clipping градієнту, тобто зменшення градієнту, який перевищує встановлене порогове значення. Додавання residual зав'язків додає гнучкості мережі для уникнення зникаючого або exploding градієнту. Оскільки градієнт передається через шари, це дозволяє збільшити кількість шарів в рекурентному блоці та покращити представлення ознак на його виході. На виході останнього шару цього стеку отримуємо представлення ознак початкового часового ряду.

Це представлення на рис. 5.13 відображає характеристики початкового часового ряду і використовується для подальшої кластеризації, а також для розрахунку складової функції втрат кластеризації.

Функція втрат автоенкодера. Функція втрат для навчання енкодера складається з двох частин: функції втрат відновлення вхідного сигналу декодером; функції втрат кластеризації. Функція втрат відновлення декодером $L_r(\theta)$ належить до функцій втрат, які використовують для задач регресії. Функції, які пропонується використовувати для навчання рекурентного автоенкодера: середньоквадратична похибка; середня абсолютна похибка; функція втрат Хубера; функція логарифму гіперболічного косинусу.

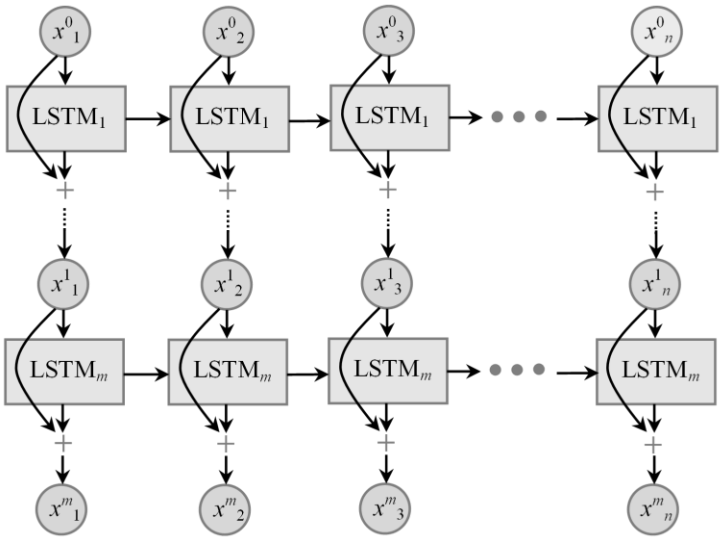


Рисунок 5.13 – Характеристики початкового часового ряду

Так само функція втрат відновлення функція втрат кластеризації $L_c(\theta)$ може бути обрана з певного переліку в залежності від методу кластеризації та характеру міри подібності між об'єктами. В якості методу кластеризації обрано k-means кластеризацію завдяки порівняній простоті його реалізації та швидкості обчислень, які може забезпечити цей метод. Попередній препроцесінг вихідних часових рядів рекурентним автоенкодером та використання відповідної міри подібності забезпечує коректне виявлення взаємозв'язків між часовими рядами даних, зібраних мережею приманок. Основний недолік методу k-means кластеризації полягає у необхідності мати попередню інформацію про кількість кластерів. Однак точної інформації про кількість типів атак, які мають або матимуть місце в мережі, немає. Тому в процесі кластеризації необхідно також визначити кількість кластерів.

Функція втрат для k-means кластеризації:

$$L_c(\theta) = \sum_{j=1}^{N} \sum_{k=1}^{K} s_{jk} \cdot d(x_j, \mu_k), \tag{5.19}$$

де x_j- об'єкт; μ_k- центроїда кластера k; s_{jk}- булева величина, що відображає приналежність обєкта x_j до кластера з центроїдою μ_k; $d(x_j, \mu_k)$- міра подібності між об'єктом x_j та центроїдою μ_k.

До мір подібності, які використовують для кластеризації часових рядів, відносять: евклідову відстань; коефіцієнт кореляції Пірсона; відстань Махаланобіса; відстань, отримана за алгоритмом динамічної трансформації часової шкали.

Кластеризація часових рядів, які представляють дані приманок із використанням рекурентного автоенкодера включає такі етапи:

1) збір та попередня обробка даних, що включає власне збір даних мережею приманок, вибір тривалості часового вікна та масштабування;

2) навчання рекурентного автоенкодера, яке складається з двох етапів: початкового навчання та тюнінгу; початкове навчання автоенкодера передбачає навчання моделі без врахування кінцевої мети кластеризації і має на меті сформувати початкові представлення ознак часових рядів; функція втрат (1) на 1-ому етапі навчання має тільки одну складову – функцію відновлення рекурентного декодера, яка обирається з (2)-(5):

$$L(\theta) = L_r(\theta); \tag{5.20}$$

тюнінг автоенкодера з врахуванням функції втрат кластеризації, використовується одна з мір подібності; для обчислення функції втрат кластеризації використовується представлення ознак $\mathbf{y} = y_1, y_2, \cdots y_m$, отримане на виході енкодера; тюнінг моделі представляє собою процес постійного (періодичного) донавчання моделі, враховує поточні зміни у датасеті;

3) для отримання представлення ознак використовується енкодер рекуррентного автоенкодера;

4) процедура кластеризації, яка передбачає такий порядок дій:

а) провести розрахунок алгоритму кластеризації для різних значень кількості кластерів NC від 1 до NCmax;

б) розрахувати для кожного NC інтегральний критерій відстані між об'єктами всередині кластеру $J = \sum_{i=1}^{l} d(C_l)/l$, де $d(C_i)$- відстань між об'єктами всередині одного кластеру; $i = 1,2,\ldots,l$; l- кількість кластерів; ця відстань для кластера $C_i = \{X_1, X_2, \ldots, X_m\}$ визначається за співвідношенням $d(C_i) = \sum_{a=1}^{m} \sum_{b=1}^{m} d(X_a, X_b)/m$, де $d(X_a, X_b)$- відстань між двома об'єктами, яка визначається за одним із співвідношень (6)-(9) в залежності від того, яка міра подібності була обрана для кластеризації.

в) вибір з множини розрахованих інтегральних критеріїв $\{J_{NC1}, J_{NC2}, \ldots\}$ мінімуму, відповідного йому числа кластерів NC та відповідних центроїд $\boldsymbol{\mu}^1\{\mu_1^1, \mu_2^1, \cdots \mu_n^1\}$, …,

$\boldsymbol{\mu}^{Nc}\left\{\mu_1^{Nc},\mu_2^{Nc},\cdots\mu_n^{Nc}\right\}$; центроїди кластерів відображають патерни атак, які діють в мережі приманок.

Процес кластеризації періодично повторюється для постійного оновлення патернів атак. Відповідно повторюється виконання етапів 1-4 процедури кластеризації. З процедури можливе виключення початкового навчання автоенкодера, а випадку критичних вимог до часу обчислень це виключення є доцільним.

Використання приманок та мереж приманок для збору та аналізу характеристик активності зловмисників дозволяє виявляти крім відомих також нові атаки, знаходити серед них атаки із схожими характеристиками, та відповідно виявляти патерни нових атак. Правильно побудована мережа приманок дозволяє відслідковувати зловмисні дії в усіх точках робочої комп'ютерної мережі. Інформація, яку надає така мережа приманок разом з відповідним аналізом дозволяє в реальному часі відслідковувати зловмисні дії, кластеризувати їх, отримувати патерни атак, яким піддається мережа, а отже підвищує захищеність комп'ютерної мережі в цілому.

Для виявлення патернів атак використовувати часові ряди активності зловмисників, які формуються на основі даних, зібраних мережею приманок. Для отримання представлення ознак багатомірних часових рядів пропонується використати рекурентний автоенкодер, який побудовано на основі згорткового та рекурентного блоків. Перевага застосування рекурентного блоку полягає в тому, що він ефективно опрацьовує ознаки багатомірних часових рядів. Рекурентний блок представляє собою стек LSTM шарів з residual зв'язками, що сприяє уникненню зникаючого та вибухаючого градієнту при оптимізації вагових коефіцієнтів. Для оптимізації рекурентного автоенкодера разом з функцією втрат автоенкодера використовується функція втрат кластеризації, що в загальному підвищує точність кластеризації. Завдяки такому препроцесінгу часових рядів рекурентним автоенкодером можна використовувати не тільки міри подібності звичні для часових рядів (dynamic time warping, коефіцієнт кореляції Пірсона), а також евклідову відстань та відстань Махаланобіса.

Розроблено метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснено збір даних та кластеризацію

схожих зловмисників з використанням мультикомп’ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА.

5.4. Метод виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток

Мережа приманок здійснює комплексний захист корпоративної мережі. Вона включає приманки, які моніторять тільки зловмисний трафік, тому може забезпечити максимально швидке його виявлення, а також виявлення патернів нових атак. Мультикомп’ютерна система антивірусних комбінованих приманок та пасток представляє собою множину приманок та пасток різних типів.

Приманки системи є інтелектуальними, мають ознаки інтелектуального агенту, володіють автономною та гнучкою поведінкою, що передбачає наявність таких характеристик: реактивність; проактивність; соціальні можливості.Інтелектуальна приманка здатна сприймати середовище, в якому вона працює, та своєчасно реагувати на зміни, які в ньому відбуваються, відповідно до цілей функціонування. Іінтелектуальна приманка здатна проявляти цілеспрямовану поведінку, що передбачає прояв ініціативи, відповідно до цілей функціонування. Інтелектуальна приманка здатна взаємодіяти з іншими приманками (та іншими пристроями) системи відповідно до цілей функціонування.

Мультиагентна система приманок володіє колективною поведінкою, яка передбачає, що приманки, як інтелектуальні агенти, схильні до кооперування. Кожна приманка мережі відслідковує мережний трафік (кількість запитів, відкритих з’єднань, спроб несанкціонованого доступу, обсяг переданих пакетів тощо). Операційне середовище, в якому функціонують приманки, зображено на рис. 5.14.

Сумарний мережний трафік приманок складається з трафіку індивідуальних приманок і представляє собою середовище, в якому функціонує мережа приманок. Для формування сумарного трафіку передбачається взаємодія між приманками.

Тобто, приманка фіксує мережний трафік, який надходить на неї, а далі передає його мережі та використовує локально (рис. 5.15).

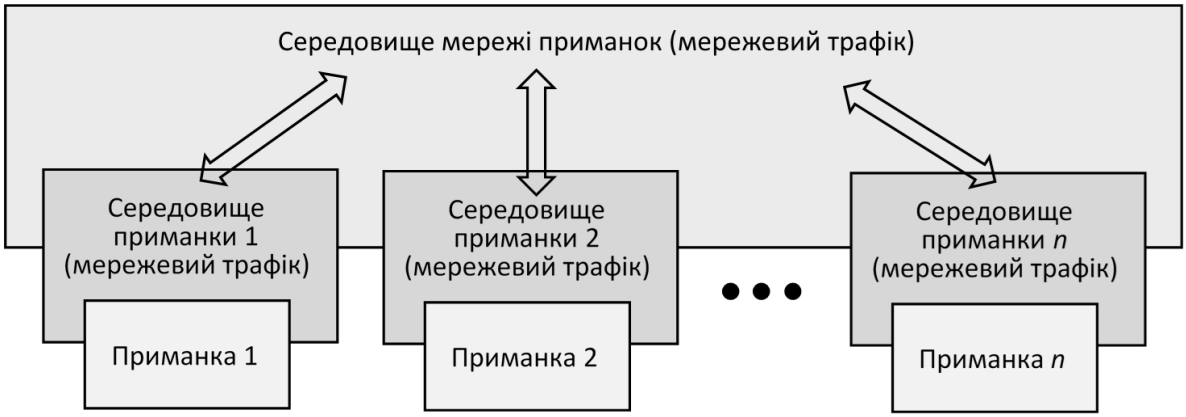


Рисунок 5.14 - Операційне середовище приманок

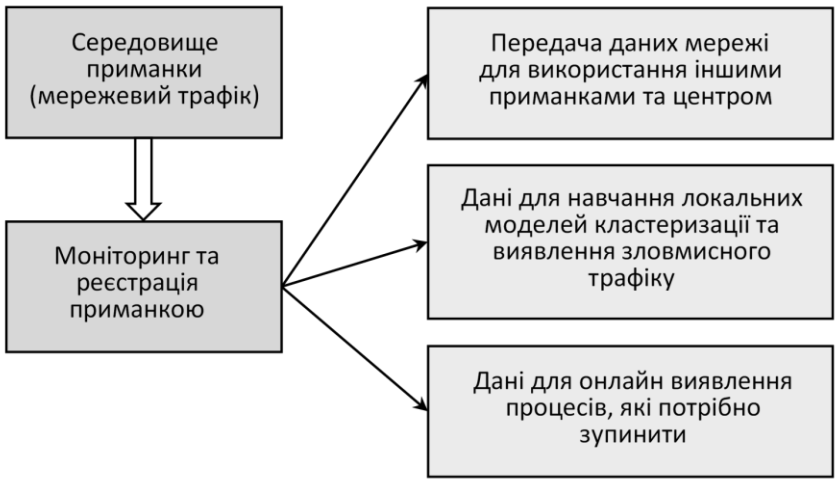


Рисунок 5.15 - Схема проходження трафіку із застосуванням приманки

Локальне використання даних мережного трафіку: навчання моделей кластеризації патернів атак; навчання моделей виявлення процесів, які необхідно зупинити; онлайн виявлення процесів, які потрібно зупинити. Тобто, приманка сама визначає критерії, коли процес потрібно зупинити. Мультиагентна система приманок може бути як централізована, децентралізована, частково-централізована, частково-децентралізована. У випадку централізованої архітектури в поточний момент часу мультиагентної системи приманок мережний трафік передається на центральний пристрій мережі (рис. 5.16). В центральному пристрої виконується організація і аналіз даних, в тому числі статистичний. Ці дані використовуються для навчання моделей, які працюють з даними всієї мережі.

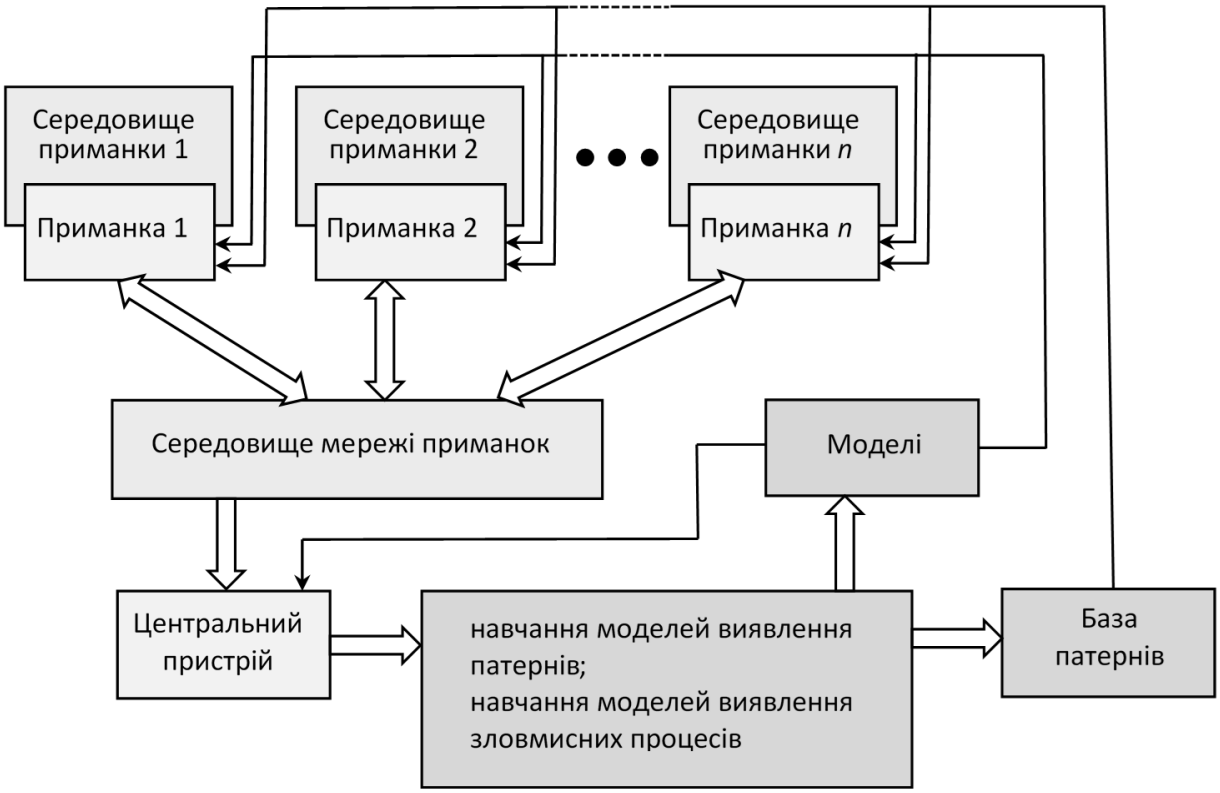


Рисунок 5.16 - Схема проходження трафіку для централізованої архітектури системи

Цілі функціонування мережі приманок визначаються при її проектуванні. У випадку автономної роботи (роботи без втручання оператора) робота приманки характеризується інтегральною цільовою функцією, яка відображає стан приманки. Кожна подія, яка відбувається в середовищі, впливає на цю цільову функцію. Інтегральна цільова функція (функція винагороди) розраховується згідно набору показників. Наприклад, інтегральна функція у вигляді вектору, яка враховує ряд показників:

$$R_H = (N_d, N_i, t_d, t_i, M, P), \tag{5.21}$$

де N_d - кількість виявлених зловмисних подій; N_i- кількість ідентифікованих зловмисних подій; t_d - середній час виявлення зловмисної події; t_i- середній час ідентифікації зловмисної події; M - пам'ять, яка використовується приманкою, для виявлення зловмисної події; P - потужність процесора, яка використовується приманкою, для виявлення зловмисної події.

Функціонування приманки повинно бути ефективним, тому необхідно витримувати компроміс між кількістю виявлених подій та споживаними ресурсами.

При визначені набору показників потрібно, також, враховувати ступень захищеності комп'ютерної мережі, якого необхідно досягти. Критично важливі сервіси та збереження конфіденційності інформації потребують високого ступеню захищеності комп'ютерної мережі, тому витрати надлишкових обчислювальних ресурсів виправдані.

Цільова функція мережі приманок формується на основі цільових функцій окремих приманок:

$$R_{NH} = R_{H1} + R_{H1} + \dots R_{Hn}, \tag{5.22}$$

де R_{NH} - цільова функція мережі, R_{Hn} - цільова функція *n*-ої приманки.

Цільова функція кожної приманки в мультикомп'ютерній системі формується таким чином, щоб сумарна цільова функція була максимальна.

Кількість приманок мережі та їх тип може змінюватися, але конфігурування системи відбувається відповідно до цільової функції. Конфігурування системи відбувається на всіх етапах функціонування та передбачає визначення:

- кількості активних приманок системи;
- типів активних приманок системи;
- конфігурацію зв'язків між приманками.

Задачі, які ставляться перед приманкою: збір та аналіз виключно зловмисного трафіку на приманці; робота в режимі тіньової приманки, тобто аналіз трафіку робочого сервісу. Мережа містить приманки, які виконують ці функції. Одна приманка може виконувати тільки одну з цих функцій або всі. Частина приманок є активними постійно, частина активується за певних умов, відповідно до індикаторів мережі приманок.

Функціонування мережі приманок відбувається відповідно до цільової функції, яка включає набір індикаторів. До цих індикаторів (табл. 5.2) входять такі, що відображають ступінь захищеності системи (кількість виявлених зловмисних дій, швидкість їх виявлення тощо), а також рівень небезпеки середовища (трафіку, відсоток кількості зловмисних запитів відносно нормальних, швидкість надходження зловмисних запитів тощо).

Множина індикаторів (табл. 5.2) приманки, яка відображає рівень загрози середовища включає ряд показників, зокрема $R_{H_{at}} = \{N_{at}, t_{at}, \dots\}$, де N_{at} – кількість

зловмисних запитів в трафіку приманки, t_{at} – середній час надходження зловмисного запиту. Ця множина є підмножиною цільової функції приманки R_H. Для кожного індикатора встановлюються порогові рівні, досягнення яких потребує відповідних дій приманки.

Таблиця 5.2

Індикатори мережі приманок

Індикатори рівня небезпеки середовища	
N_{at_s}	Кількість зловмисних джерел
N_{at_ns}	Кількість нових зловмисних джерел
$N_{at_ns_IP}$	Кількість зловмисних джерел в певній IP агрегації
N_{at_r}	Кількість зловмисних запитів
N_{at_p}	Кількість пакетів, прийнятих від зловмисних джерел
N_{at_em}	Кількість електронних повідомлень, отриманих від зловмисних джерел
V_{at_em}	Обсяг електронного повідомлення, отриманого від зловмисного джерела
N_{at_sess}	Кількість сесій зловмисного джерела
t_{at_sess}	Тривалість сесії зловмисного джерела
t_{at_l}	Час «життя» зловмисного джерела
t_{at_p}	Кількість атакованих портів
Індикатори рівня захищеності системи	
$N_{id_at_s}$	Кількість виявлених зловмисних джерел
$t_{id_at_s}$	Час виявлення зловмисного джерела
Індикатори споживання ресурсів	
L_{cpu}	Завантаження центрального процесора
L_{gpu}	Завантаження графічного процесора
V_m	Обсяг пам’яті, що використовується

Для виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток розробимо відповідний метод, в якому буде враховано виявлення саме мультикомп’ютерниими системами, до складу яких потрібно залучати множину приманок різної архітектури та призначення і, при цьому, частина з них можуть взаємодіяти між собою як інтелектуальні агенти, а також залучення приманок до складу мультикомп’ютерних систем повинно бути здійснено на основі їх поділу між завданнями системи. Для виконання певного завдання можуть

бути залучені приманки різних типів, тобто частина приманок може мати декілька функцій і виконувати декілька завдань. Крім того, певна частина приманок для виконання завдань може здійснювати комунікацію між собою з інформуванням центру системи та опрацювання подій сумісно.

Основні кроки методу виявлення ЗПЗ та КА мультикомп'ютерними системи антивірусних комбінованих приманок та пасток

1) активізація приманок після увімкнення комп'ютерних станцій;

2) встановлення зв'язків з компонентами мультикомп'ютерної системи;

3) включення приманок до складу мультикомп'ютерної системи;

4) ідентифікація та поділ приманок на групи за їх призначенням;

5) ідентифікація та поділ приманок на групи за їх типами внутрішньої архітектури;

6) визначення групи приманок, які можуть взаємодіяти між собою та мати функції інтелектуальних агентів;

7) встановлення відповідності між завданнями мультикомп'ютерної системи і приманками та їх групами;

8) отримання зовнішніх та внутрішніх впливів на приманки з групи, в якій приманки можуть опрацьовувати такі події, і надсилання інформації про події до центру мультикомп'ютерної системи;

9) виконання кроку 8) методу організації функціонування мультикомп'ютерних систем з вибору приманки чи приманок для виконання завдань із обов'язковим врахуванням їх функцій винагороди;

10) фіксування мультикомп'ютерною системою подій, які не зафіксовані приманками, їх опрацювання і виконання кроку 9) із залученням приманок з групи тіньових приманок;

11) отримання зовнішніх та внутрішніх впливів на приманки з групи, в якій приманки можуть опрацьовувати такі події, і надсилання інформації про події до центру мультикомп'ютерної системи та опрацювання подій самостійно з повідомленням в центр системи або із залученням певних приманок та інформуванням про це центр системи;

12) повідомлення в центр системи про неможливість виконати завдання в зв’язку з вимкненням комп’ютерної станції чи пристрою;

13) повідомлення в центр системи про неможливість виконати завдання приманкою;

14) повідомлення в центр системи про вимкнення комп’ютерної станції чи пристрою і, відповідно, від’єднання приманки з мультикомп’ютерної системи.

Суть методу виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток полягає в тому, що до складу мультикомп’ютерних систем залучається множина приманок різної архітектури та призначення і, при цьому, частина з них можуть взаємодіяти між собою як інтелектуальні агенти, а також залучення приманок до складу мультикомп’ютерних систем здійснюється на основі їх поділу між завданнями системи, для виконання яких можуть бути залучені приманки різних типів, тобто частина приманок може мати декілька функцій і виконувати декілька завдань. Частина приманок в процесі виконання завдань з опрацювання подій в системі може здійснювати комунікацію між собою з інформуванням центру системи та опрацювання подій сумісно. В результаті такої конфігурації при опрацюванні подій застосовується трьохетапний аналіз подій, який включає опрацювання на першому етапі безпосередньо приманкою, на другому етапі – групою приманок, на третьому етапі – системою з приманками. Це дає змогу системі здійснити різні обманні дії щодо зловмисних дій, зловмисного програмного забезпечення та комп’ютерних атак завдяки урізноманітненню варіантів відповідей.

Таким чином, розроблено новий метод виявлення зловмисного програмного забезпечення та комп’ютерних атак, який реалізується в архітектурі мультикомп’ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення. Вони можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій, зокрема на рівні окремої приманки, групи приманок та всієї системи. Це забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, підвищує ефективність протидії.

5.5. Висновки до п’ятого розділу

Визначено застосування приманок для встановлення зловмисних дій та здійснено їх формальне подання, які відображені в розроблених моделях зловмисних дій та приманок. В архітектурі приманок виділено інтелектуальну складову частину. Вона виконує завдання із здійснення аналізу трафіку. Архітектура приманок розроблена для можливості їх функціонування як інтелектуальних агентів, що можуть взаємодіяти з рештою приманок, але з урахуванням координації в мультикомп’ютерних системах. Розроблені моделі приманок для типових атак можуть бути застосовними для побудови мереж приманок в корпоративних мережах і бути включеними в мультикомп’ютерні системи антивірусних комбінованих приманок та пасток.

Розроблено метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснено збір даних та кластеризацію схожих зловмисників з використанням мультикомп’ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА.

Розроблено метод виявлення ЗПЗ та КА, особливістю якого є його імплементація в архітектуру мультикомп’ютерних систем комбінованих антивірусних приманок і пасток різної архітектури та функціонального призначення. Вони можуть функціонувати як інтелектуальні агенти, виконувати одночасно декілька різних завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи При цьому, також реалізовується трирівнева модель аналізу подій: на рівні окремої приманки; групи приманок; всієї системи. Це забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, покращує протидію ЗПЗ та КА.

Основні наукові результати опубліковані в працях [10, 92, 96, 145, 146, 147, 171, 172, 204, 286, 288, 296, 297, 298, 299, 303, 312, 314].

РОЗДІЛ 6.
МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК І РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТІВ

6.1. Методика оцінювання ефективності мультикомп'ютерних систем антивірусних комбінованих приманок та пасток

Важливими характеристиками в контексті синтезованих систем певного класу та призначення є їх стійкість та рівновага. Оскільки, розглядуваний клас систем охоплює комп'ютерні станції корпоративної мережі, а зв'язок між ними формується за рахунок проміжного програмного забезпечення, що створює мультикомп'ютерну систему, тобто розподілену систему, то стійкість таких систем та їх рівновага є важливими характеристиками і потребують дослідження. Крім того, для аналізу цих двох характеристик потрібно досліджувати час як показник впливу на них і на результат виконання завдання спеціалізованим функціоналом системи.

Введемо три цільові функції $\mathfrak{F}_i^{\mathfrak{E}}$ $(i = 1,2,3)$, які будуть характеризувати відповідно стійкість, рівновагу та результат виконання завдання спеціалізованим функціоналом системи. Результат виконання кожної з цих функцій буде відображено в проміжок [0;1]. Середньоарифметичні значення цих трьох функцій будуть встановлювати три коефіцієнти для характеристики системи:

$$\mathfrak{k}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}} = \frac{\sum_{j=1}^{\mathfrak{n}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}} \mathfrak{F}_i^{\mathfrak{E}}(t_j)}{\mathfrak{n}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}}, \tag{6.1}$$

де t_j – час від початку функціонування системи; j – індекс для часу, що відображає j – тий момент фіксування часу в системі; $j = 1,2,\dots,\mathfrak{n}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$; $\mathfrak{n}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$ – кількість фіксувань часу, які було здійснено системою; $\mathfrak{F}_i^{\mathfrak{E}}(t_j)$ $(i = 1,2,3)$ - функції, які характеризують стійкість, рівновагу та результат виконання завдання спеціалізованим функціоналом системи; $\mathfrak{k}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$ $(i = 1,2,3)$ - коефіцієнти, які характеризують рівні стійкості, рівноваги та результату виконання завдання спеціалізованим функціоналом системи.

Введемо інтегрований показник характеристики системи, в якому будуть відображені коефіцієнти рівнів стійкості, рівноваги та результату виконання завдання спеціалізованим функціоналом системи, а також кількість компонентів системи, так:

$$\mathfrak{k}_{\mathfrak{J}}^{\mathfrak{E}} = \frac{\sum_{j=1}^{n_{\mathfrak{J}}^{\mathfrak{E}}} \mathfrak{k}_{\mathfrak{F}_i}^{\mathfrak{E}}}{n_{\mathfrak{J}}^{\mathfrak{E}}} \cdot \frac{n_1}{n_2}, \tag{6.2}$$

де $n_{\mathfrak{J}}^{\mathfrak{E}}$ – кількість коефіцієнтів; $\mathfrak{F}_i^{\mathfrak{E}}(t_j)$ $(i = 1,2,\dots,n_{\mathfrak{J}}^{\mathfrak{E}})$ - функції, які характеризують стійкість, рівновагу та результат виконання завдання спеціалізованим функціоналом системи; $\mathfrak{k}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$ $(i = 1,2,\dots,n_{\mathfrak{J}}^{\mathfrak{E}})$ – значення коефіцієнтів; n_1 – кількість компонентів в системі; n_2 – кількість комп'ютерних станцій в корпоративній мережі.

Для проведення експерименту з системою, яку побудовано згідно запропонованої моделі за формулою (2.30), було здійснено запуск системи та забезпечено її функціонування протягом 180 годин. Також, для залучення спеціалізованого функціоналу було активовано п'ять штучних комп'ютерних атак. Для опрацювання подій пов'язаних з ними були використані приманки. Кількість фіксованих часових значень за увесь час функціонування становив 50, тобто за увесь час функціонування системи було отримано 50 значень усіх характеристичних показників. Результати значень інтегрального коефіцієнту, трьох коефіцієнтів та проміжних величин такі: $\mathfrak{k}_{\mathfrak{F}_1^{\mathfrak{E}}}^{\mathfrak{E}} = 0{,}78452$; $\mathfrak{k}_{\mathfrak{F}_2^{\mathfrak{E}}}^{\mathfrak{E}} = 0{,}69433$; $\mathfrak{k}_{\mathfrak{F}_3^{\mathfrak{E}}}^{\mathfrak{E}} = 0{,}91521$; $n_1 = 100$; $n_2 = 120$; $n_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}} = 50$. Значення інтегрального коефіцієнту $\mathfrak{k}_{\mathfrak{J}}^{\mathfrak{E}} = 0{,}66502$. Такі результати отримано саме для систем з наявним контролером. При використанні систем без контролера при проведенні такого ж есперименту було отримано таке значення інтегрального коефіцієнту $\mathfrak{k}_{\mathfrak{J}}^{\mathfrak{E}} = 0{,}64892$. Тобто, певна ефективність в таких системах з контролером досягнута. Вона зростатиме при інтенсивнішому і тривалішому їх використанні. Тоді, кількість оброблюваних подій зростатиме, що вимагатиме постійного використання контролера, який надає переваги системам порівняно з системами без контролера. Крім того, на результат впливає, також, і кількість розміщених в корпоративній мережі компонент системи. Якщо їх кількість менша за кількість комп'ютерних станцій, то тоді ефективність такої системи буде меншою.

Визначення ефективності систем з контролером за формулами (6.1) та (6.2) потребує подальшої деталізації та проведення експериментів щодо стійкості, безпеки, цілісності і оперативності системи конкретно за кожним критерієм. Важливим напрямом щодо оцінювання ефективності мультикомп'ютерних систем антивірусних комбінованих приманок та пасток є встановлення досягнення мети дослідження, яка полягає в покращенні функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

6.2. Експериментальні дослідження запропонованих рішень

Згідно розроблених методів синтезу мультикомп'ютерних систем антивірусних комбінованих приманок та пасток було розроблено прототип системи [294], який підтверджує можливість реалізації запропонованих рішень, а також їх належну деталізацію для здійснення відтворюваності. Крім того, прототип системи необхідний для проведення експериментальних досліджень, щоб підтвердити можливість практичного застосування розроблених методів синтезу в контексті досягнення мети дослідження. Враховуючи складність розробленої системи згідно методів синтезу, а також окремих приманок та пасток і їх поєднання, здійснимо експериментальні дослідження системи за окремими параметрами, які відображають певні реалізовані методи в архітектурі системи, і експериментальні дослідження щодо функціонування системи для виконання завдань з виявлення ЗПЗ та КА. Експерименти будемо проводити з урахуванням визначеної мети, постановки та обгрунтування коректності експерименту, визначенням серій експерименту, вибором альтернатив та крайніх випадків для подальшого порівняння.

6.2.1 Перший експеримент та результати

Перший експеримент проведемо для аналізу впливу та адекватності критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи.

Метою експерименту було дослідження критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для встановлення відповідності їх значень реальним станам при функціонуванні системи в моменти зміни варіантів централізації в архітектурі системи та адекватності обраним для них параметрів.

Постановка експерименту. Експеримент було проведено протягом 90 діб для різних випадків в контексті визначених для характеристики системи критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи. Перша серія експериментів полягала у дослідженні системи у випадку її штатного функціонування без виникнення у ній та операційному середовищі її функціонування критичних для неї подій. Решта серій експерименту була спрямована на дослідження системи за критеріями оперативності, стійкості, цілісності та безпеки щодо центру системи при виникненні у ній та операційному середовищі її функціонування критичних для неї подій. Для досягнення повноти щодо результатів експерименту серії проводились окремо для випадків критичної зміни у показниках одного з критеріїв, причому для показників, які характерні виняткова для окремо взятого критерію. Також, серії експерименту проводились у випадках впливу на декілька критеріїв одночасно через спільні для них показники.

Перша серія першого експерименту. За час функціонування система здійснила 100 разів зміну свого центру за різними варіантами. Для визначення наступного варіанту централізації в архітектурі системи було здійснено розрахунок значень критеріїв оперативності, стійкості, цілісності та безпеки за аналітичними виразами, які визначено за формулами (3.32), (3.36), (3.40) і (3.42). Результати першої серії першого експерименту подано фрагментом в табл. 6.1 (всі значення результатів експерименту в табл. Є.1-Є.2, Додаток Є). Всі отримані значення належать відрізку [0; 0.65]. Це відповідає вимогам до розроблених аналітичних виразів для чотирьох критеріїв, які задано загальною формулою (3.31). При цьому дотримано обмеження щодо належності отриманих значень кожного критерію відрізку [0;1].

Таблиця 6.1

Результати першої серії експерименту

Номер перебудови	Час, с	Значення функцій				
		Оператив-ність, $f_{1,kr}^{centr}$	Стійкість, $f_{2.kr}^{centr}$	Цілісність, $f_{3.kr}^{centr}$	Безпека, $f_{4,kr}^{centr}$	Цільова функція, F_{kr}^{centr}
1	0	0.060488135	0.061778165	0.058117959	0.064065555	0.061112454
2	$7.94 \cdot 10^3$	0.062151894	0.05770008	0.061963435	0.062740473	0.06113897
3	$1.59 \cdot 10^4$	0.061027634	0.06235194	0.058777518	0.058331452	0.060122136
4	$2.38 \cdot 10^4$	0.060448832	0.064621885	0.056796037	0.055811014	0.059419442
…	…	…	…	…	…	…
99	$7.78 \cdot 10^6$	0.0632894	0.055580292	0.064729195	0.055163285	0.059690543
100	$7.96 \cdot 10^6$	0.055046955	0.059344166	0.064608347	0.056852323	0.058962948

Аналіз результатів першої серії першого експерименту, графіки функцій для чотирьох критеріїв та цільової функції подано в додатку В (деталізація першого експерименту).

Значення всіх функцій першого експерименту подано фрагментом в табл. 6.2, в якій відображено відхилення за кожним параметром окремо (всі значення результатів експерименту в табл. Є.1-Є.2, Додаток Є). Таким чином, задані функціями чотири критерії адекватно відображають поведінку системи.

Адекватність опису аналітичними виразами критеріїв підтверджена не суттєвим відхиленнями їх графіків функцій. У випадках суттєвих відхилень на певних часових проміжках в процесі функціонування системи, досягнення результату з визначення варіантів централізації досягається. Аналітичні вирази для цільової функції у всіх випадках, які отримані теоретичним способом, теж підтверджують можливість отримання прийнятного результату. Відхилення між крайніми значеннями цільової функції при штатному функціонуванні мультикомп’ютерної системи становить 3%. При впливі на параметри одного з чотирьох критеріїв максимальне відхилення дорівнює 7% в момент впливу, але в подальшому система функціонує стабільно при виконанні перебудови центру. Це досягається за рахунок врахування попереднього досвіду з вибору варіанту централізації та відповідності введеної цільової функції.

Таблиця 6.2

Значення всіх функцій першого експерименту

Номер перебудови	Час, с	Значення функції				
		Оперативність $f_{1.kr}^{centr}$	Стійкість $f_{2.kr}^{centr}$	Цілісність $f_{3.kr}^{centr}$	Безпека $f_{4.kr}^{centr}$	Цільова функція F_{kr}^{centr}
…	…	…	…	…	…	…
17	$1.27 \cdot 10^6$	0.061176355	0.058599781	**0.024556127**	0.064518745	0.052212752
18	$1.35 \cdot 10^6$	0.056187277	0.057378928	**0.031408288**	0.058068101	0.050760649
19	$1.43 \cdot 10^6$	0.057961402	0.064194826	**0.033481409**	0.061956254	0.054398473
20	$1.51 \cdot 10^6$	0.061924721	0.060722519	**0.034404319**	0.056594145	0.053411426
21	$1.59 \cdot 10^6$	0.055710361	0.063480082	**0.033818294**	0.057835188	0.052710981
…	…	…	…	…	…	…
23	$1.75 \cdot 10^6$	**0.063209932**	0.057487531	0.057817301	0.059304024	0.059454697
24	$1.83 \cdot 10^6$	**0.027444256**	0.059287687	0.060883171	0.06403984	0.052913738
25	$1.91 \cdot 10^6$	**0.023918779**	0.062142413	0.063621915	0.062567786	0.053062723
26	$1.99 \cdot 10^6$	**0.024218483**	0.057239247	0.055978445	0.063605512	0.050260422
27	$2.06 \cdot 10^6$	**0.062392636**	0.060722519	0.063638556	0.060361775	0.061778871
…	…	…	…	…	…	…
42	$3.18 \cdot 10^6$	0.061531083	**0.049575421**	0.061874883	0.05589603	0.057219354
43	$3.26 \cdot 10^6$	0.064636628	**0.049754205**	0.064903389	0.057400203	0.059173606
44	$3.34 \cdot 10^6$	0.059236548	**0.038600776**	0.061699165	0.062786954	0.055580861
45	$3.41 \cdot 10^6$	0.064883738	**0.033778165**	0.062980468	0.064589827	0.05655805
46	$3.49 \cdot 10^6$	0.064786183	**0.037965466**	0.056856359	0.062740473	0.055587121
…	…	…	…	…	…	…
73	$5.64 \cdot 10^6$	0.058154284	0.06230122	0.0587417	**0.034605388**	0.053450648
74	$5.72 \cdot 10^6$	0.063209932	0.056354741	0.061874883	**0.033997959**	0.053859379
75	$5.80 \cdot 10^6$	0.056182744	0.060699649	0.058834639	**0.033720478**	0.052359378
76	$5.88 \cdot 10^6$	0.0632894	0.059287687	0.064774951	**0.033720478**	0.055268129
77	$5.96 \cdot 10^6$	0.061048455	0.062220556	0.062851529	**0.041288984**	0.056852381
…	…	…	…	…	…	…

Тестове середовище, включаючи параметри топології мережі, кількість вузлів та варіанти тестування, в усіх серіях першого експерименту було однаковим. Для проведення експерименту було встановлено компоненти системи в 60 комп'ютерних станцій. Корпоративна мережа поділена на 8 сегментів. Демілітаризована зона складена з трьох комп'ютерних станцій в одному сегменті корпоративної мережі.

Тестування щодо конкретних типів комп'ютерних атак не досліджувалось. Впливи здійснювались на окремі параметри, які впливають на значення критеріїв і здійснювались в окремих серіях першого експерименту.

Вплив попереднього досвіду з використання певного варіанту централізації можна проаналізувати за точками на графіках цільових функцій оцінювання, в яких відбувається зміна тренду кривої лінії. Також, вдалий підбір наступного варіанту централізації в архітектурі і перехід в нього відображені невеликим відхиленням точок кривої від кривої тренду.

Результати різних серій першого експерименту підтвердили те, що система може виконувати завдання при зміні її параметрів для різних критеріїв. Відхилення за кожним критерієм не створювало критичних проблем для її функціонування. Таким чином, система показала стабільність своєї роботи. В отриманих аналітичних виразах для критеріїв оцінювання в достатній мірі враховано параметри, що забезпечило повноту опису процесів, які відбуваються в ній.

Всі параметри чотирьох критеріїв при дослідженні можна розглядати в їх крайніх значеннях. При максимальних крайніх значеннях результатом обчислення функцій для критеріїв будуть значення, які дорівнюють одиниці в параметрах цільової функції. Але всі одночасно параметри та всі чотири критерії не можуть мати максимальні крайні числові значення, бо тоді система оцінить такий варіант як варіант з низьким рівнем безпеки і відхились його. Якщо ж значення параметрів будуть дорівнювати нулеві або будуть такими, згідно яких значення функцій для критеріїв будуть близькими до нуля в цільовій функції, тоді такі варіанти централізації будуть розглядатись системою як варіанти для наступного переходу до них.

Розроблена цільова функція (формула (3.28)) оцінювання варіантів централізації може бути використана в системах, які передбачають перебудову своєї архітектури самостійно, без залучення адміністратора. Такі системи в сфері кібербезпекти активно розробляються. Підхід з використанням цільової функції оцінювання може бути адаптований для оцінювання наступних кроків системи. Перехід до наступного варіанту централізації є лише одним із можливих кроків системи, які вона може виконати без залучення адміністратора. Узагальнене подання цільової функції оцінювання може бути інтегровано в існуючі механізми безпеки корпоративних мереж, зокрема обманних систем, включно з приманками та пастками.

6.2.2 Другий експеримент та результати

Для розробленого методу визначення варіанту централізації в системах класу $\mathfrak{S}$ здійснимо постановку другого експерименту. Завданнями експерименту будуть такі: встановлення наступного варіанту централізації протягом визначеного часу функціонування системи; час витрачений на визначення наступного варіанту централізації та перехід до нього; кількість вдалих спроб переходу до наступного варіанту централізації; кількість невдалих спроб переходу до наступного варіанту централізації; значення цільової функції та показників з правил; номери правил використані для визначення наступних варіантів централізації. Отриманні результати виконання завдань експерименту дадуть змогу оцінити можливість реалізації розробленого методу в системах класу $\mathfrak{S}$ та врахування попереднього досвіду щодо вибору варіанту централізації.

Для проведення експерименту було реалізовано мультикомп'ютерну систему з функціоналом, який дозволяє приймати впливи ззовні і зсередини корпоративної мережі. В архітектурі системи виділено окремо центр системи та контролер прийняття рішень. Центр системи готує п'ять варіантів виконання завдання, яке є відповіддю на подію викликану впливами. Контролер прийняття рішень затверджує один варіант виконання завдання із запропонованих п'яти варіантів. Мультикомп'ютерна система функціонувала в корпоративній мережі 90 діб. В табл. 6.3 подано фрагмент результатів (всі значення результатів експерименту в табл. Ж.1, Додаток Ж) її функціонування за такими показниками:

1) загальної кількості варіантів перебудови центру системи протягом часу функціонування (стовпець 1);

2) час початку перебудови центру системи (стовпець 2);

3) п'ять варіантів для наступного варіанту централізації в архітектурі системи (нумерація п'яти рядків, стовпець 3);

4) десять характерних властивостей з формули (1) для кожного варіанту централізації (стовпці 4-13);

5) номер затвердженого варіанту централізації в архітектурі системи (стовпець 14);

6) час завершення перебудови центру системи (стовпець 15);

7) час виконання перебудови центру системи (стовпець 16);

8) результат щодо успішного виконання перебудови центру системи (вдала спроба – «1», невдала спроба – «0», стовпець 17);

9) номер варіанту використаного правила при виборі наступного варіанту централізації в архітектурі системи (стовпець 18);

10) цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації (формула (3.28), стовпець 19);

11) номер варіанту централізації, з яким відбулось повторне затвердження такого ж варіанту (стовпець 20);

12) номер варіанту правила («1» - 1..4, «2» - 5, «3» - 6) за трьома групами (стовпець 21).

Друга серія другого експерименту стосувалась цієї ж системи, але в ній контролера прийняття рішень не було. Тобто, окремо контролер прийняття рішень і окремо центр системи не функціонували. В системі був тільки центр системи, в якому здійснювались оцінювання п’яти варіантів централізації і обирався варіант централізації, для якого цільова функція була найменшою. Результати проведеної другої серії другого експерименту подані фрагментом в табл. 6.4 (всі значення результатів експерименту в табл. Ж.2, Додаток Ж). В табл. 6.4 враховано ті ж параметри, що і в табл. 6.3.

Зведемо результати функціонування мультикомп’ютерної системи у варіанті з контролером прийняття рішень в табл. 6.5 та без контролера прийняття рішень в табл. 6.6 і отримаємо загальну кількість перебудов центру системи за час її функціонування (стовпець 1), кількість використаних варіантів для кожної характерної властивості (стовпці 4-13), відомості про успішність/неуспішність виконання перебудови центру системи (стовпець 17), значення цільової функції (найменше, затверджене, найбільше серед п’яти варіантів, стовпець 19), кількість варіантів централізації за номерами, з яким відбулось повторне затвердження такого ж варіанту (стовпець 20), кількість номерів варіантів правила («1» - 1..4, «2» - 5, «3» -

6) за трьома групами (стовпець 21).

Таблиця 6.3

Фрагмент результатів функціонування мультикомп’ютерної системи (перша серія другого експерименту)

Загальна кількість варіантів перебудови центру системи протягом часу функціонування	Час початку перебудови центру системи	П’ять варіантів для наступного варіанту централізації в архітектурі системи	Десять характерних властивостей з формули (1) для кожного варіанту централізації										Номер затвердженого варіанту централізації в архітектурі системи	Час завершення перебудови центру системи	Час виконання перебудови центру системи	Результат щодо успішного виконання перебудови центру системи (вдала спроба – «1», невдала спроба – «0»	Номер варіанту використаного правила при виборі наступного варіанту централізації в архітектурі системи	Цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації (формула (3.28)	Номер варіанту централізації, з яким відбулось повторне затвердження такого ж варіанту	Номер варіанту правила («1» - 1..4, «2» - 5, «3» - 6) за трьома групами
			1-4	1-2	1-3	1 -4	1-5	1-3	1-2	1-3	1-3	1-3								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19,00	20	21
		1	1	1	2	2	4	1	1	1	1	1						0,0336		
		2	2	1	1	4	4	1	1	1	2	1						0,0268		
1	29054	3	3	2	2	3	3	1	1	1	1	3	3	29059	5	1	3	0,0366		1
		4	4	2	1	4	5	1	2	3	3	2						0,0725		
		5	1	1	2	1	2	3	1	2	1	2						0,0393		
		1	1	1	1	2	2	1	1	3	2	1						0,0922		
		2	2	1	1	2	3	1	1	2	3	2						0,0181		
2		3	3	1	1	2	1	2	1	3	3	2						0,0674		
	54775	4	4	2	2	1	1	3	2	1	1	2	4	54779	4	1	4	0,0645		1
		5	1	2	1	3	3	3	2	2	3	3						0,0893		
		1	1	1	1	4	1	2	2	1	1	3						0,0507		
	80055	2	2	1	1	4	4	1	1	1	1	3	2	80060	5	1	2	0,0179		1
3		3	3	1	2	1	5	3	2	2	3	2						0,0876		
		4	4	2	1	1	2	2	2	1	1	1						0,0863		
		5	3	1	2	3	4	3	2	1	3	3						0,0179		
		1	1	2	2	1	5	2	1	1	1	1						0,0159		
		2	2	1	2	3	1	3	1	2	1	2						0,0349		
4	103211	3	3	2	1	1	4	2	2	1	3	2	3	103214	3	1	3	0,0579		1
		4	4	2	2	2	1	2	2	1	1	1						0,0827		
		5	1	2	2	3	3	3	2	1	2	2						0,0569		
		1	1	2	1	2	3	1	2	1	3	3						0,0964		
	127542	2	2	2	1	2	4	1	2	2	3	1	2	127547	5	1	2	0,0945		1
5		3	3	1	1	2	1	1	1	1	1	1						0,0178		
		4	4	2	1	3	4	1	2	1	1	1						0,0856		
		5	4	2	2	1	5	3	2	2	1	2						0,0306		

Таблиця 6.4

Фрагмент результатів функціонування мультикомп’ютерної системи (друга серія другого експерименту)

Загальна кількість варіантів перебудови центру системи протягом часу функціонування	Час початку перебудови центру системи	П’ять варіантів для наступного варіанту централізації в архітектурі системи	Десять характерних властивостей з формули (1) для кожного варіанту централізації										Номер затвердженого варіанту централізації в архітектурі системи	Час завершення перебудови центру системи	Час виконання перебудови центру системи	Результат щодо успішного виконання перебудови центру системи (вдала спроба – «1», невдала спроба – «0»	Номер варіанту використаного правила при виборі наступного варіанту централізації в архітектурі системи	Цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації (формула (3.28)	Номер варіанту централізації, з яким відбулось повторне затвердження такого ж варіанту	Номер варіанту правила («1» - 1..4, «2» - 5, «3» - 6) за трьома групами
			1-4	1-2	1-3	1-4	1-5	1-3	1-2	1-3	1-3	1-3								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
		1	1	1	1	1	5	3	2	2	2	1						0,5084		
	27619	2	2	1	2	3	3	2	1	2	3	3	2	27623	4	1	2	0,4194		1
1		3	3	2	1	3	5	3	1	1	2	3						0,4601		
		4	4	1	1	2	4	3	2	2	1	1						0,5579		
		5	4	2	2	2	5	1	2	3	2	2						0,5888		
		1	1	2	1	1	3	3	2	2	1	1						0,5845		
		2	2	2	2	4	2	3	2	3	2	1						0,3045		
2		3	3	2	2	4	2	2	1	2	1	1						0,4785		
		4	4	2	1	1	5	2	1	3	1	2						0,348		
	56213	5	3	2	2	3	5	3	1	1	2	1	5	56218	5	1	3	2,78E-04		1
		1	1	1	2	2	4	3	1	2	2	2						0,5299		
		2	2	2	1	2	2	2	1	3	3	2						0,19		
3	81992	3	3	1	2	2	1	3	1	2	3	1	3	81995	3	1	3	0,0426		1
		4	4	1	2	4	2	3	2	3	3	1						0,6311		
		5	3	2	1	2	1	3	2	1	2	3						0,4833		
		1	1	2	2	3	5	3	1	2	3	3						0,2666		
		2	2	2	2	2	1	1	1	2	3	1						0,08		
4	106505	3	3	2	1	3	2	3	1	1	3	3	3	106510	5	1	3	0,0644		1
		4	4	1	1	3	1	2	1	3	1	2						0,4541		
		5	2	2	1	3	2	2	1	3	1	3						0,7091		
		1	1	2	1	1	5	3	2	2	1	3						0,4118		
		2	2	1	2	1	5	1	2	1	1	3						0,61		
5	136331	3	3	2	1	2	2	3	2	2	2	3	3	136334	3	0	3	0,198		1
		4	4	1	1	1	3	1	1	1	2	2						0,4333		
		5	1	1	2	3	2	1	1	3	2	2						0,3701		

Таблиця 6.5

Зведені значення результатів першої серії другого експерименту

Загальна кількість варіантів перебудови центру системи протягом часу функціонування	Час початку перебудови центру системи	П'ять варіантів для наступного варіанту централізації в архітектурі системи	Десять характерних властивостей з формули (1) для кожного варіанту централізації										Номер затвердженого варіанту централізації в архітектурі системи	Час завершення перебудови центру системи	Час виконання перебудови центру системи	Результат щодо успішного виконання перебудови центру системи (вдала спроба – «1», невдала спроба – «0»	Номер варіанту використаного правила при виборі наступного варіанту централізації в архітектурі системи	Цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації (формула (3.28)	Номер варіанту централізації, з яким відбулось повторне затвердження такого ж варіанту	Номер варіанту правила («1» - 1..4, «2» - 5, «3» - 6) за трьома групами
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
307			1:	1:	1:	1:	1:	1:	1:	1:	1:	1:				1:	1:	Aver:	53, 84	1:
			388	756	740	381	283	517	764	505	510	511			1404	296	70	0,0547	190, 301	245
			2:	2:	2:	2:	2:	2:	2:	2:	2:	2:				0:	2:	Aver_f_zaty:	214, 250	2:
			381	779	795	390	315	497	771	517	522	519				11	74	0.0530		16
			3:			3:	3:	3:		3:	3:	3:					3:			3:
			384			393	322	521		513	503	505					82			17
			4:			4:	4:										4:			4:
			382			371	317										81			18
							5:													5:
							298													10
																				6:
																				1

Таблиця 6.6

Зведені значення результатів другої серії другого експерименту

Загальна кількість варіантів перебудови центру системи протягом часу функціонування	Час початку перебудови центру системи	П'ять варіантів для наступного варіанту централізації в архітектурі системи	Десять характерних властивостей з формули (1) для кожного варіанту централізації										Номер затвердженого варіанту централізації в архітектурі системи	Час завершення перебудови центру системи	Час виконання перебудови центру системи	Результат щодо успішного виконання перебудови центру системи (вдала спроба – «1», невдала спроба – «0»	Номер варіанту використаного правила при виборі наступного варіанту централізації в архітектурі системи	Цільова функція F_{kr}^{centr} оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації (формула (3.28)	Номер варіанту централізації, з яким відбулось повторне затвердження такого ж варіанту	Номер варіанту правила («1» - 1..4, «2» - 5, «3» - 6) за трьома групами
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
337			1:	1:	1:	1:	1:	1:	1:	1:	1:	1:				1:		Aver:	71,212	1:
			422	817	853	398	335	549	839	540	570	569			2062	291		0,3553		236
			2:	2:	2:	2:	2:	2:	2:	2:	2:	2:				0:				2:
			414	868	832	438	344	550	846	579	565	571				46				17
			3:			3:	3:	3:		3:	3:	3:						Aver_f_min:		3:
			432			411	359	586		566	550	545						0,1149		16
			4:			4:	4:													4:
			417			438	331													22
							5:													5:
							316													45
																				6:
																				1

Проведений другий експеримент в першій серії підтверджує стійкість системи. Зокрема, система не змогла завершити перебудову свого центру з 330 разів 35 разів. Але в 34 випадках завершення відбулось з другої оновленої спроби, а в одному випадку потрібна була третя спроба, виконання якої здійснювалось за шостим правилом. Також, значення цільової функції для всіх п'яти варіантів, які були підготовлені центром системи, перебували в інтервалі 0-0,25. Для випадку вдалої перебудови центру системи верхня межа інтервалу не перевищувала 0,1, а для випадку з повторним підбором варіантів перебудови через проблеми із завершенням перебудови центру системи – 0,25. Ці значення в контексті цільової функції підтверджують адекватність підбору варіантів для вибору контролером прийняття рішень і використанні для наступного варіанту централізації в архітектурі системи.

Детальніше аналіз другого експерименту подано в додатку Г (деталізація другого експерименту).

Друга серія другого експерименту з системою була проведена за тими ж вимогами, що і перша серія другого експерименту. Але в другій серії другого експерименту контролера прийняття рішень в системі не було. Центр системи готував варіанти централізації, обчислював значення цільової функції для них і обирав наступним варіантом централізації той, в якому значення цільової функції було мінімальним. За результатами другої серії другого експерименту було встановлено, що значення цільової функції перебували переважно в інтервалі 0-0,72, що є достатньо великими і вказують на певну розбалансованість при виборі варіанту централізації.

Таким чином, результати другого експерименту при використанні у складі системи контролера прийняття рішень для вибору наступного варіанту централізації при перебудові архітектури системи підтверджують ефективність розробленого правила та методу вибору наступного варіанту централізації. Зокрема, у випадку використання контролера прийняття ріщень, значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера. За рахунок використанння контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання.

6.2.3 Третій експеримент та результати

Завдання третього експерименту. Оскільки метою роботи було покращення прийняття рішень мультикомп’ютерними системами з комбінованими антивірусними приманками та пастками щодо подальших кроків за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування систем, то сфокусуємо постановку третього експерименту щодо дослідження таких показників:

1) врахування попереднього досвіду функціонування системи та застосування варіантів виконання при формуванні поліморфних відповідей на події;

2) стійкість системи;

3) оперативність системи;

4) цілісність системи;

5) безпека системи;

6) оцінювання прийнятих рішень.

Показники щодо стійкості, оперативності, цілісності, безпеки системи є загальноприйнятими при дослідженні систем в корпоративних мережах. Зокрема, критерій щодо стійкості системи буде відображати спроможність системи функціонувати тривалий час без суттєвої деградації її компонентів під зовнішніми та внутрішніми впливами. Оскільки система є розподіленою, то перевірка відповідності критерію щодо оперативності прийняття рішень та виконання завдань в компонентах системи та в ній в цілому є важливою її характеристикою. Під час функціонування системи в корпоративній мережі система повинна зберігати цілісність, на характеристику якої впливає не тільки вихід з ладу певних компонент, але й втрата зв’язків між ними. Тому, забезпечення цілісності системи є важливою характеристикою в контексті функціонування систем та виконання ними завдань. Безпека системи потребує оцінювання та врахування, оскільки система спрямована на виконання завдань попередження, виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам. Значення показників щодо стійкості, оперативності, цілісності, безпеки системи визначимо за формулою (4.7) як значення критеріїв.

Враховуючи особливість синтезу мультикомп’ютерних систем в частині прийняття рішень, то потрібно дослідити врахування попереднього досвіду функціонування системи та застосування варіантів виконання при формуванні поліморфних відповідей на події. Ці особливості в архітектурі систем повинні забезпечити її стійке функціонування та заплутування зловмисників при дослідженні систем в корпоративних мережах. За результатами третього експерименту потрібно встановити обсяг врахованого попереднього досвіду функціонування системи та його вплив на зміну варіантів виконання завдань системою. Також, потрібно визначити спроможність системи формувати варіанти виконання завдань та оцінювати їх з врахуванням попереднього досвіду їх застосування.

Рішення прийняті системою та реалізовані як виконані завдання потрібно оцінити. Тобто, за результатами всього третього експерименту потрібно виконати оцінювання прийнятих рішень. Це оцінювання здійснюватиме сама система. Вони формуватимуть попередній досвід щодо застосування варіантів виконання завдань та будуть враховувати показники стійкості, оперативності, безпеки та цілісності. Згідно такого оцінювання можна отримати прогноз щодо прийнятих рішень. Оцінювання варіантів виконання завдань будемо обчислювати як значення цільової функції оцінювання за формулою (4.6).

Постановка третього експерименту. Для дослідження відповідності показників згідно запропонованих рішень проведемо окремо експерименти з прототипом мультикомп’ютерної системи. Експерименти будемо проводити для двох випадків (серій): варіант системи, в якому реалізовано контролер прийняття рішень; варіант системи з одним центром без контролера прийняття рішень.

В першому випадку (першій серії) центр системи буде готувати п’ять варіантів виконання завдання. Після підготовки, вони будуть оцінені контролером прийняття рішень з врахуванням попереднього досвіду їх застосування і з них буде обрано один варіант.

В другому випадку (другій серії) центр системи буде обирати один варіант виконання завдання. Цей варіант виконання завдання буде обиратись постійно один і той же. Решта варіантів виконання цього ж завдання застосовуватись не будуть. Обраний варіант виконання завдання по завершенні буде оцінюватись за тими ж критеріями і кожного разу буде обчислюватись значення цільової функції оцінювання. Таким чином, в цьому випадку буде отримано такий самий набір статичних даних, що і для першого випадку. Їх можна буде порівняти на предмет оцінювання прийнятих рішень.

В обох випадках зловмисні дії будуть повторюватись, тобто будуть однаковими. Крім них, система буде вирішувати завдання щодо свого функціонування, тобто за результатами її функціонування буде сформовано траєкторію її станів. При повторюваності зловмисних дій важливою відмінністю першого випадку від другого повинні бути різні варіанти відповіді та інтервал часу між ними. Ці показники потрібно порівняти для обох випадків.

Проведення третього експерименту. Для проведення експерименту було обрано корпоративну мережу, в якій наявні сімдесят п’ять комп’ютерних станцій, два сервери, демілітаризована зона з чотирма комп’ютерними станціями, вісім сегментів. В кожну комп’ютерну станцію було встановлено компоненти системи, тобто компонент системи разом сімдесят п’ять. На початку роботи системи всі комп’юерні станції були увімкнені. В подальшому при проведенні експерименту у двох випадках кількість увімкнених комп’ютерних станцій, тобто наявність компонент в системі, змінювалась, але для обох випадків однаково в кількісному та часовому вимірах. Таким чином, експеримент проводився в типовій корпоративній мережі. Тривалість експерименту в двох окремих випадках становила по дев’яносто діб для кожного. Результати обчислень, які здійснювала система щодо оцінювання варіантів виконання завдань разом з проміжними даними, зокрема кількість компонент в поточний час функціонування систем, номери компонент з центром в поточні періоди часу, номери завдань для виконання, номери варіантів виконання завдань, фіксувались в окремому файлі-протоколі роботи системи.

Згідно опрацювання даних з файлу-протоколу було підготовлено таблиці (Додаток З) і побудовано графіки функцій. Результати третього експерименту. В табл. 6.7 подано дані фрагментом результатів експерименту для першого випадку та загальним підсумком в табл. 6.8. Всі результати першої серії третього експерименту подано в табл. З.1 та табл. З.2 (Додаток З).

Таблиця 6.7

Фрагмент результатів експерименту для першого випадку

№	Час вибору варіантів виконання завдань	Час завершення виконання завдань	Час виконання	Номер завдання	Варіанти виконання завдання	*Критерій* $f_{j,kr}^{m_{pz,i}}$				*Значення цільової функції оцінювання* $F_{kr}^{m_{pz,i}}$	Номер варіанту 1-5	Номер повтору варіанту	Попереднє значення цільової функції	Час виконання	Стратегія	Правило
						с	о	ц	б							
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*
1	1,54E-01	5,99E-01	4,45E-01	1	1	0,0003	0,0657	0,0484	0,0149	0,0323					8	1.1
	1,90E-01	3,46E-01	1,56E-01		2	0,0294	0,0391	0,0011	0,0429	0,0281					5	3.1
	1,56E-01	5,68E-01	4,12E-01		3	0,0672	0,0294	0,0289	0,0551	0,0451	3				4	2.3
	1,68E-01	3,63E-01	1,95E-01		4	0,0696	0,0633	0,0161	0,0056	0,0386					11	2.3
	1,53E-01	3,50E-01	1,97E-01		5	0,0402	0,0234	0,0162	0,0625	0,0356					2	2.2
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
34	1,36E-01	5,93E-01	4,57E-01	3	1	0,0294	0,0563	0,0353	0,0418	0,0407			0,0281	2,26E-01	3	2.1
	1,54E-01	5,19E-01	3,65E-01		2	0,0181	0,0304	0,0031	0,0226	0,0185		2	0,0398	3,03E-01	6	2.2
	1,27E-01	5,59E-01	4,32E-01		3	0,0143	0,0154	0,0237	0,0368	0,0226	3		0,0427	1,73E-01	4	2.3
	1,84E-01	4,73E-01	2,89E-01		4	0,0437	0,0005	0,0673	0,0390	0,0376			0,0238	3,50E-01	8	2.3
	1,47E-01	4,36E-01	2,89E-01		5	0,0497	0,0227	0,0090	0,0419	0,0308			0,0364	4,08E-01	4	2.3
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
100	1,43E-01	5,45E-01	4,02E-01	7	1	0,0536	0,0437	0,0352	0,0371	0,0424	1		0,0243	2,63E-01	14	3.1
	1,02E-01	4,60E-01	3,58E-01		2	0,0300	0,0397	0,0473	0,0670	0,0460			0,0107	3,46E-01	8	1.1
	1,66E-01	5,49E-01	3,83E-01		3	0,0011	0,0029	0,0563	0,0152	0,0188			0,0308	3,95E-01	5	2.2
	1,04E-01	3,67E-01	2,63E-01		4	0,0503	0,0113	0,0580	0,0122	0,0330		4	0,0305	1,77E-01	1	1.1
	1,34E-01	4,35E-01	3,01E-01		5	0,0525	0,0014	0,0355	0,0082	0,0244			0,0330	2,15E-01	3	2.3

Таблиця 6.8

Узагальнені показники

Середній час виконання	Номер завдання	Розподіл завдань по варіантах*	Середнє значення стійкості	Середнє значення оперативності	Середнє значення цілісності	Середнє значення безпеки	Середнє значення цільової функції	Номер варіанту 1-5	Номер повтору варіанту	Кількість обраних правил	Кількість обраних стратегій
1,56E+02	1 - 22 2 - 8 3 - 16 4 - 14 5 - 24 6 - 9 7 - 7	6-3-5-2-6 0-3-1-2-2 4-1-6-3-2 5-2-0-4-3 7-3-5-2-7 1-3-1-1-3 0-2-1-3-1	0,0683	0,0368	0,0389	0,0361	0,0359	1 - 18 2 - 22 3 - 35 4 - 5 5 - 20	1 - 18 2 - 22 3 - 34 4 - 5 5 - 20	1 - 47 2 - 33 3 - 39 4 - 28 5 - 42 6 - 55 7 - 36 8 - 31 9 - 24 10 - 38 11 - 41 12 - 29 13 - 19 14 - 37	1,1 - 83 2,1 - 47 2,2 - 92 2,3 - 56 3,1 - 104 3,2 - 118

*Примітка формат запису 1-2-3-4-5 означає для *i*-го завдання розподіл кількості обраних варіантів 1,..,5 у цьому завданні

В табл. 6.7 для подання результатів першої серії третього експерименту зібрано такі характеристичні показники:

1) номер події, яка потребує реакції системи (стовпець 1);

2) час вибору варіантів виконання завдань для реагування на події (стовпець 2);

3) час завершення виконання завдань (стовпець 3);

4) час виконання (стовпець 4);

5) номер завдання, яке відподає за реагування на вказану подію (стовпець 5);

6) варіанти виконання завдання, яке визначено для опрацювання події (стовп. 6);

7) значення функції для критерію стійкості (стовпець 7);

8) значення функції для критерію оперативності (стовпець 8);

9) значення функції для критерію цілісності (стовпець 9);

10) значення функції для критерію безпеки (стовпець 10);

11) значення цільової функції оцінювання варіантів виконання завдання, яке визначено для опрацювання події (стовпець 11);

12) номер обраного варіанту виконання завдання, яке визначено для опрацювання події (стовпець 12);

13) номер повтору варіанту виконання завдання при опрацюванні повторюваних подій через певні проміжки часу в процесі функціонування системи (стовпець 13);

14) попереднє значення цільової функції для того ж варіанту виконання завдання, який повторився при повторному настанні тієї ж події (стовпець 14);

15) час виконання варіанту виконання завдання, який повторився при повторному настанні тієї ж події, на попередньому кроці по відношенню до поточного вибору цього ж варіанту (стовпець 15);

16) номер стратегії, яка була застосована для обраного варіанту виконання завдання (стовпець 16);

17) номер правила, яке було застосоване для обраного варіанту виконання завдання (стовпець 17).

В табл. 6.7 подано фрагмент результатів роботи системи, а також зведені результати (табл. 6.8) для всіх подій, які відбулись за досліджуваний період. В стовпці 5 наявні дані про кількість повторень завдань при їх викликах для опрацювання подій. Зокрема, завдання 1 викликалось 22 рази, завдання 2 – 8 разів, завдання 3 – 16 разів, завдання 4 – 14 разів, завдання 5 – 24 рази, завдання 6 – 9 разів, завдання 7 – 7 разів.

В стовпці 12 подано номер варіанту затвердженого контролером прийняття рішень при виборі одного з п’яти варіантів, які підготовлено центром системи для вибору. Тобто, для кожного завдання обрано один з п’яти можливих варіантів.

Стовпці 13-15 містять інформацію про попередні варіанти виконання завдання, які вже застосовувались при виникненні цієї ж події в процесі функціонування системи. Ця інформація в стовпцях 13-15 є частиною інформації від інформації про попередній досвід функціонування системи для прийняття рішення про наступний крок системи.

В стовпці 17 подано номер правила, яке було застосоване для вибору наступного варіанту виконання завдання.

Критерій щодо стійкості системи подано значеннями в стовпці 7, критерій щодо оперативності системи – в стовпці 8, критерій щодо цілісності системи – в стовпці 9, критерій щодо безпеки системи – в стовпці 10. Значення цільової функції оцінювання подано в стовпці 11. Згідно значень цільової функції для різних варіантів виконання завдання контролером прийняття рішень було обрано варіант з врахуванням

попереднього досвіду функціонування системи та застосування варіантів виконання при формуванні поліморфних відповідей на події. Наприклад, значення цільової функції для кроку 100 для всіх п’яти варіантів різні і обрано було не найменше і не найбільше із отриманих значень контролером прийняття рішень, а значення 0,0424.

Також, повторювані події вимагають виклику тих самих завдань для їх опрацювання. Кожне завдання має п’ять варіантів опрацювання подій. Обчислені значення цільової функції на кожному кроці повтору події для тих самих варіантів виконання завдання є різними. Наприклад, завдання 1 – номери варіантів повторились (табл. 6.9) 18 разів.

Детальніше аналіз подано в Додатку Д (перша частина).

Аналогічно до першого випадку з контролером прийняття рішень в системі було проведено експеримент для другого випадку (другої серії) без контролера прийняття рішень в системі. В табл. 6.9 подано дані з результатів експерименту для другого випадку.

Таблиця 6.9

Фрагмент результатів експерименту для першого випадку

№	Час вибору варіантів виконання завдань	Час завершення виконання завдань	Час вико-нання	Номер завдання	Варіанти виконання завдання	*Критерій* $f_{j,kr}^{m_{pz.i}}$				*Значення цільової функції оцінювання* $F_{kr}^{m_{pz.i}}$	Номер варіанту 1-5	Номер повтору варіанту	Попереднє значення цільової функції	Час вико-нання	Стра-тегія	Правило
						с	о	ц	б							
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*
1	1,09E-01	3,12E-01	2,03E-01	1	1	0,1901	0,2463	0,1256	0,1727	0,1837	1				4	2.1
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
34	1,45E-01	3,17E-01	1,72E-01	6	1	0,2024	0,1207	0,1932	0,1980	0,1786	1	1	0,1733	3,78E-01	12	2.1
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
100	1,56E-01	4,71E-01	3,15E-01	7	1	0,2164	0,1572	0,1659	0,2536	0,1983	1	1	0,1227	3,41E-01	6	3.1

В табл. 6.10 подано узагальнені показники з табл. 6.9. Всі результати другої серії третього експерименту подано в табл. З.3 та табл. З.4 (Додаток З).

В табл. 6.9 аналогічно до табл. 6.7 так само подано дані в сімнадцяти стовпцях. В табл. 6.9 для кожного завдання, яке може виконувати система є тільки один варіант виконання завдання (табл. 6.10). А для першого випадку в табл. 6.7 таких варіантів є п’ять для кожного.

Детальніше аналіз подано в Додатку Д (друга частина).

В результаті проведення третього експерименту було встановлено, що розроблені аналітичні вирази для критеріїв щодо стійкості, оперативності, цілісності, безпеки та цільової функції адекватно описують процеси та об’єкти в розробленій

системі і можуть бути використані для вибору варіантів виконання завдання щодо оперативності, стійкості, безпеки, цілісності оцінювання в мулькомп'ютерних системах та корпоративних мережах.

Таблиця 6.10

Узагальнені показники

Середній час виконання	Номер завдання	Середнє значення стійкості	Середнє значення оперативності	Середнє значення цілісності	Середнє значення безпеки	Середнє значення цільової функції	Номер варіанту 1-5	Номер повтору варіанту	Кількість обраних правил	Кількість обраних стратегій
2,48E-01	1 - 18 2 - 12 3 - 15 4 - 13 5 - 20 6 - 11 7 - 11	0,2049	0,1966	0,1964	0,1916	0,1974	1 - 100	1 - 99	1 - 8 2 - 6 3 - 9 4 - 4 5 - 7 6 - 10 7 - 8 8 - 6 9 - 4 10 - 7 11 - 9 12 - 5 13 - 3 14 - 13	1,1 - 13 2,1 - 11 2,2 - 14 2,3 - 9 3,1 - 16 3,2 - 37

Метод організації функціонування мультикомп'ютерних систем дає змогу розробляти обманні системи, які самостійно без залучення адміністраторів систем можуть приймати рішення щодо свої подальших кроків та опрацювання подій, що виникатимуть в корпоративних системах. Особливістю запропонованого рішення є то, що центр поділено на дві частини. В одній частині, яку було названо центром системи, опрацьовуються події і визначається номер завдання, яке може опрацювати подію, що викликана зовнішніми і внутрішніми впливами. В другій частині, яку було названо контролером прийняття рішень, здійснюється вибір одного з п'яти варіантів виконання завдання з опрацювання події на основі попереднього досвіду функціонування систем та з урахуванням різних стратегій вибору варіанту. Це дало змогу розробляти та здійснювати такими системами різні варіанти відповідей на повторювані зловмисниками дії та оцінювати їх результат на безпосереднє функціонування систем для врахування в наступних кроках систем. Крім того, така конструкція в архітектурі систем спрямована на забезпечення подальшої їх стабільності роботи. Згідно експериментальних досліджень встановлено, що дисперсія відхилень між двома випадками експерименту становить приблизно 60%.

Тому, виокремлення контролера прийняття рішень та включення в його механізм функціонування попереднього досвіду дає змогу покращити функціонування систем.

6.2.4 Четвертий експеримент та результати

Розроблений прототип мультикомп’ютерної системи може бути використано для виявлення прояву метаморфних вірусів. Для цього в її архітектурі можуть перебувати комп’ютерні станції, в яких буде здійснюватись емулювання команд виконуваної програми, причому процес емулювання здійснюватиметься з певним ступенем паралелізму та із зміненими параметрами ізольованих середовищ емулювання. Тобто, ця система може виконувати завдання пісочниці для отримання відбитків програмного коду та подальшого їх аналізу на предмет виявлення метаморфного коду.

Постановка четвертого експерименту. В розробленій мультикомп’ютерній системі наявні в кожній компоненті файли, в яких міститься інформація про виконувані дії та запущені функції виконання певних завдань, а також про події, які впливатимуть на систему безпосередньо та спонукатимуть реагувати її на них певним чином. Ці файли будуть постійно доповнюватись, а за певними критеріями з них вилучатиметься застаріла інформація. Крім того, згідно цих файлів системою будуть сформовані окремі таблиці, в яких на задані впливи буде зберігатись інформація про реакції системи протягом тривалого часу. Така інформація надаватиме змогу центру системи напрацьовувати варіанти рішень щодо подальших кроків системи, рейтингувати їх та погоджувати з контролером. Контролер для остаточного затвердження рішення щодо подальших кроків системи згідно одного впливу буде використовувати інформацію з відповідної таблиці впливу. Таким чином, у внутрішніх таблицях компонентів системи буде міститись інформація про попередні рішення системи як рішення на визначені впливи. Тобто, розроблена мультикомп’ютерна система буде позиціонуватись як система з елементами пам’яті. Оскільки на початковому етапі її функціонування відомостей про попередні події не має, то розглядатимемо її в першому експерименті як таку, що не містить повнофункційного контролера прийнятих рішень. В такому випадку контролер буде

погоджувати рішення центру системи згідно рейтингу (за найвищим) запропонованих варіантів. Відповідно для кожної серії першого етапу четвертого експерименту умови проведення будуть однакові.

Другим важливим фактором при проведенні четвертого експерименту є метаморфні віруси та їх різноманітність. Виділимо в них такі особливості: запис повністю у виконуваний PE-файл із збереженням обсягу початкового файлу, тобто заміщенням частини бітів і, відповідно, втратою функціоналу початкового файлу та збереженням частини бітів початкового файлу без їх використання; запис повністю у виконуваний PE-файл без збереженням обсягу початкового файлу, тобто доповнення частини бітів метаморфного вірусу до початкового файлу і, відповідно, збереження функціоналу початкового файлу і отримання доступу на виконання першої команди вірусу при запуску інфікованого PE-файлу; заміна початкового PE-файлу на метаморфний вірус із зміною або збереженням обсягу файлу в бітах шляхом доповнення неактивними командами; записування метаморфного вірусу у початковий PE-файл і копіювання та зберігання цього початкового файлу під іншим іменем з можливістю його виклику на виконання після виконання команд вірусу. Ці особливості є основою формування чотирьох підмножин метаморфних вірусів. Виділення саме цих підмножин є визначальним в контексті дослідження їх коду згідно результатів попереднього експерименту щодо отримання дизасембльованих команд та логіки досліджуваних програм. Наприклад, якщо вірус втілено у файл так, що точкою входу в програму є перша команда вірусу і після цього відбувається безумовний перехід через декілька команд, то такий механізм вірусу формує один шаблон. А при відсутності безумовного переходу буде сформовано другий шаблон. Тому, ці особливості повинні враховуватись при виявленні метаморфного коду вірусів. Позначимо підмножини метаморфних вірусів так: $\mathfrak{H}_1$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), відсутність функції збереження початкового PE-файлу в окремому файлі; $\mathfrak{H}_2$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі з можливістю

його виклику на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_3$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі без виклику його на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_4$ – заміщення бітів, обсяг початкового файлу в бітах не збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), відсутність функції збереження початкового PE-файлу в окремому файлі; $\mathfrak{H}_5$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі з можливістю його виклику на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_6$ – заміщення бітів, обсяг початкового файлу в бітах не збережено, втрата функціоналу початкового PE-файлу, наявність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі без виклику його на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_7$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), відсутність функції збереження початкового PE-файлу в окремому файлі; $\mathfrak{H}_8$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі з можливістю його виклику на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_9$ – заміщення бітів, обсяг початкового файлу в бітах збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі без виклику його на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_{10}$ – заміщення бітів, обсяг початкового файлу в бітах не збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), відсутність функції збереження початкового PE-файлу в окремому файлі; $\mathfrak{H}_{11}$ – заміщення бітів, обсяг початкового файлу в бітах

збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі з можливістю його виклику на виконання після виконання команд метаморфного вірусу; $\mathfrak{H}_{12}$ – заміщення бітів, обсяг початкового файлу в бітах не збережено, втрата функціоналу початкового PE-файлу, відсутність безумовного переходу на початку PE-файлу (з точки входу у файл), збереження початкового PE-файлу в окремому файлі без виклику його на виконання після виконання команд метаморфного вірусу.

Таким чином, в множині метаморфних вірусів виділимо 12 підмножин розділених за певними критеріями і ці підмножини включають переважну кількість типів метаморфних вірусів, але їх об'єднання не є вичерпною множиною метаморфних вірусів. Для проведення експерименту будемо користуватись цим поділом на 12 підмножин і кожна з підмножин обов'язково буде задана елементом чи елементами в четвертому експерименті. Задамо множину метаморфних вірусів так:

$$\mathfrak{H} = \bigcup_{\mathfrak{f}=1}^{12} \mathfrak{H}_{\mathfrak{f}}. \qquad (6.1)$$

Кількість елементів в множині $\mathfrak{H}$ позначимо $\mathfrak{N}_{\mathfrak{H}}$ і аналогічно для підмножин $\mathfrak{H}_{\mathfrak{f}}$ позначимо $\mathfrak{N}_{\mathfrak{H}_{\mathfrak{f}}}$ ($\mathfrak{f} = 1,2, \dots, 12$). Ці позначення будуть використані при опрацюванні результатів експерименту і будуть позначати кількість метаморфних вірусів певної підмножини та множини в цілому, які було взято для проведення експериментальних досліджень.

Метою першого етапу четвертого експерименту є встановлення достовірності виявлення метаморфних вірусів розробленою мультикомп'ютерною системою виявлення ЗПЗ із метаморфним функціоналом за умови відсутності інформації в елементах пам'яті за попередні кроки та, відповідно, без залучення контролера. Тобто, на першому етапі четвертого експерименту з системою для прийняття рішення про виявлення метаморфного вірусу буде залучено тільки центр системи. На відміну від хостових систем, в розробленій мультикомп'ютерній системі виявлення ЗПЗ із метаморфним функціоналом буде досягнення покращення ефективності за рахунок збільшення обчислювальних ресурсів, використання спроможності комп'ютерної мережі і особливостей в архітектурі самої мультикомп'ютерної системи. Метаморфні

віруси можуть бути виявлені хостовими системами без залучення решти обчислювальних ресурсів мережі, а також можуть бути виявлені компонентами мультикомп’ютерної системи без залучення частини всієї системи та центру системи. В такому випадку самі компоненти системи та їх сенсори будуть виконувати функції прийняття рішень. Таким чином, на першому етапі четвертого експерименту буде здійснено перевірку самої мультикомп’ютерної системи щодо виявлення метаморфних вірусів із позиціонуванням її як єдиної цілісної системи без контролера.

Метою наступних етапів четвертого експерименту є встановлення достовірності виявлення метаморфних вірусів розробленою мультикомп’ютерною системою виявлення ЗПЗ із метаморфним функціоналом за умови наявності інформації в елементах пам’яті за попередні кроки та, відповідно, із залученням контролера. Другий етап четвертого експерименту буде включати можливості розробленої мультикомп’ютерної системи з використання попереднього досвіду із виявлення метаморфних вірусів, але це досвід, який сформовано на відомостях у елементах пам’яті, буде незначним. Тому, доцільно провести певну кількість етапів експериментів для досягнення сталої достовірності виявлення метаморфних вірусів. Достатньою кількістю етапів буде така кількість етапів, при якій результати достовірності виявлення вже не будуть покращуватись. При проведенні експериментальних досліджень цю кількість етапів потрібно буде визначити. На неї буде впливати особливість архітектури контролера і закладений в ньому механізм затвердження рішення центру системи.

Детальніше аналіз подано в Додатку Е (перша частина). Результати серій експериментальних досліджень подано в табл. И.1 та табл. И.2 (Додаток И). Приклади для 1-го і 21-го результатів серії експериментальних досліджень (всього 46 етапів) представлені в табл. 6.11.

Експеримент зупинено після повного завершення кроку 46, тому що значення, отримані на кроках 44-46, близькі і вони відображають підвищення надійності виявлення в порівнянні з попередніми кроками. Тобто вимоги щодо зупинки експерименту були виконані. Для оброблення результатів експериментальних досліджень було використано методику ROC-аналізу.

Таблиця 6.11

Результати дослідження достовірності виявлення метаморфних вірусів на окремих етапах з врахуванням всіх особливостей штучно створених екземплярів класів

Етап	Результат виявлення	Клас метаморфних вірусів												Підсумок
		1	2	3	4	5	6	7	8	9	10	11	12	
1	TP	11	10	13	13	12	12	13	12	12	12	11	12	143
	FN	4	5	2	2	3	3	2	3	3	3	4	3	37
	FP	34	27	20	20	19	33	35	32	29	21	28	27	325
	TN	326	333	340	340	341	327	325	328	331	339	332	333	3995
...														
21	TP	10	13	13	11	11	12	10	11	9	13	13	12	138
	FN	5	2	2	4	4	3	5	4	6	2	2	3	42
	FP	33	21	34	22	32	19	36	42	40	26	28	25	358
	TN	327	339	326	338	328	341	324	318	320	334	332	335	3962
	FN	4	4	3	6	2	4	2	3	2	4	6	4	44
...														

Приклади результатів аналізу для 1-го та 21-го етапів (всього 46 етапів) наведені окремо в табл. 6.12.

Таблиця 6.12

Приклади результатів аналізу для 1-го та 21-го етапів (всього 46 етапів)

Етап	TPR	FPR	S_P	$Precision$	$Recall$	$F1$	MCC
1	79.44	7.52	92.48	0.31	0.79	0.44	0.46
...							
21	76.67	8.29	91.71	0.28	0.77	0.41	0.43
...							

У табл. 6.12 наведена оцінка величини МКК. Отриманий результат у табл. 6.12 підтверджує відповідний рівень розробленого класифікатора метаморфних вірусів.

Детальніше аналіз подано в Додатку Е (друга частина). Зведемо всі результати, отримані на всіх етапах, в єдину таблицю значень з 1-46 етапів. В результаті отримуємо для кожного класу метаморфних вірусів суму значень за показниками ROC-аналізу. На перших етапах ці значення були меншими, а на останніх – більшими. Це дозволило оцінити якість досліджуваних зразків класів метаморфних вірусів. Це було досягнуто шляхом порівняння відхилення результатів показника від середнього значення. Якщо відхилення значне, то необхідно провести аналіз екземплярів

метаморфних вірусів того класу, в якому виявлено відхилення, або доопрацювати відповідну підсистему мультикомп'ютерної системи. У табл. 6.13 наведені всі зведені значення результатів четвертого експерименту.

Середнє арифметичне значення достовірності виявлення для всіх класів і всіх серій і етапів експерименту дорівнює $TPR = 75.46\%$ для тієї множини вірусів, які залишались невиявленими в досліджуваному операційному середовищі після їх проходження через системи виявлення вторгнень та антивірусні засоби. Відхилення від цього значення всіх значень дванадцяти класів не перевищує 3%, тому створені екземпляри класів метаморфних вірусів корелюють між собою. Таким чином, за результатами проведеного четвертого експерименту було встановлено, що наявність контролера в мультикомп'ютерній системі забезпечує покращення виявлення метаморфних вірусів зі збільшенням числа разів його застосування.

Таблиця 6.13

Результати дослідження окремих типів штучно створених екземплярів класів на всіх етапах

Результат виявлення	Класи метаморфних вірусів												Підсумок
	1	2	3	4	5	6	7	8	9	10	11	12	
TP	510	520	519	511	517	515	535	519	520	540	501	541	6248
FN	180	170	171	179	173	175	155	171	170	150	189	149	2032
FP	1132	1151	1167	1115	1096	1214	1132	1228	1161	1164	1178	1117	13855
TN	15428	15409	15393	15445	15464	15346	15428	15332	15399	15396	15382	15443	184865
TPR	73.91	75.36	75.22	74.06	74.93	74.64	77.54	75.22	75.36	78.26	72.61	78.41	75.46
FPR	6.84	6.95	7.05	6.73	6.62	7.33	6.84	7.42	7.01	7.03	7.11	6.75	6.97
$Precision$	0.31	0.31	0.31	0.31	0.32	0.30	0.32	0.30	0.31	0.32	0.30	0.33	0.31
$Recall$	0.74	0.75	0.75	0.74	0.75	0.75	0.78	0.75	0.75	0.78	0.73	0.78	0.75
$F1$	0.44	0.44	0.44	0.44	0.45	0.43	0.45	0.43	0.44	0.45	0.42	0.46	0.44
MCC[61]	0.45	0.45	0.45	0.45	0.46	0.44	0.47	0.44	0.45	0.47	0.43	0.48	0.45

Основною метою четвертого експерименту була перевірка ефективності виявлення метаморфних вірусів за допомогою розробленої мультикомп'ютерної системи. Детальніше аналіз подано в Додатку Е (третя частина).

Таким чином, досліджено ефективність виявлення метаморфного коду вірусів мультикомп'ютерною системою та встановлено покращення ефективності детектування.

6.2.5 П’ятий експеримент та результати

Для експериментального аналізу підходу щодо кластеризації схожих зловмисників використано дані мережі приманок [30, 146, 147], яка містить приманки з різними операційними системами та сервісами. Із зібраних даних було сформовано часові ряди з такими початковими ознаками зловмисних дій: кількість зловмисних джерел за одиницю часу; кількість нових зловмисних джерел за одиницю часу; обсяг даних, відправлених за одиницю часу; обсяг даних, прийнятих за одиницю часу; обсяг даних на одне повідомлення; кількість сесій за одиницю часу; тривалість сесії; час життя зловмисного джерела. Фрагмент кластеризованого багатомірного часового ряду подано на рис. 6.1.

Для розбиття часового ряду на сегменти було використано сегментацію вікном, яке зсувається в часі, та розділення на відрізки за алгоритмом. При навчанні згорткового автоенкодера використовувались запропоновані функції втрат відновлення декодером та запропоновані міри подібності сегментів часових рядів.

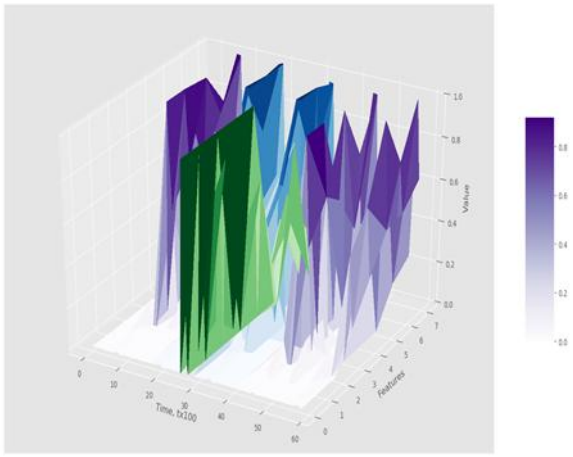


Рисунок 6.1 - Фрагмент кластеризованого багатомірного часового ряду

Результати експериментів відображені в табл. 6.14, для визначення показників точності кластеризації використано попередньо розмічені сегменти.

Результати показують, що всі три міри подібності дають близький результат Rand statistics, однак забезпечують різний час виконання кластеризації. Швидкодія трьох метрик від найвищої до найнижчої розташовується таким чином: soft-DTW, GAK, DTW. Порівняння з показниками точності підходу [31, 146, 147] показує, що досягнуто дещо кращих показників Rand Statistics, а також більш стабільних

результатів. Швидкодія запропонованого підходу потребує більш детального дослідження імплементації мір подібності, оскільки час виявлення атаки в процесі її реалізації є критично важливим.

Таблиця 6.14

Результати експериментів

Decoder Loss Function	Time Series Similarity Measure		
	DTW	GAK	Soft-DTW
MSE	83	84	84
MAE	84	85	84
Huber Loss	85	85	84
Log-Cosh Loss	83	84	83

Виявлення патернів нових атак та модифікованих існуючих є важливою перевагою використання приманок та їх мереж. Мережі приманок дають змогу в реальному часі аналізувати зловмисні дії та із використанням відповідних алгоритмів надавати інформацію, необхідну для реагування на ці дії.

Проведемо експеримент для другого випадку. Проведено аналіз даних мережі приманок. Для аналізу був сформований датасет, який містив часові ряди даних: кількість зловмисних джерел за одиницю часу; кількість нових зловмисних джерел за одиницю часу; обсяг даних, прийнятих за одиницю часу; обсяг даних, відправлених за одиницю часу; обсяг даних на одне повідомлення; кількість сесій за одиницю часу; тривалість сесії; час функціонування зловмисного джерела. Для визначення довжини часових рядів використовувалось вікно фіксованого розміру та вікно, отримане на основі попередньої сегментації. Було проведено кластеризацію з використанням різних комбінацій функції втрат відновлення автоенкодера та міри подібності кластеризації. Отримані результати були порівняні з попередньо розміченими патернами та наведені в табл. 6.15.

Найкращі результати серед мір подібності показує dynamic time warping distance, що є цілком логічним, оскільки ця відстань є більш інваріантною до деяких зміщень порівняно з іншими мірами подібності. Однак за використання цієї міри подібності час обчислень є найбільшим, що слід співвідносити з вимогами до швидкодії.

Таблиця 6.15

Значення точності кластеризації

Міра подібності кластеризації / Функція втрат автоенкодера	Евклідова відстань	Коефіцієнт кореляції Пірсона	Відстань Махаланобіса	Dynamic Time Warping Distance
Середньоквадратична похибка	69	79	71	83
Середня абсолютна похибка	69	80	70	83
Функція втрат Хубера	70	82	71	84
Функція логарифму гіперболічного косинусу	67	81	69	81

Використання приманок та мереж приманок для збору та аналізу характеристик активності зловмисників дозволяє виявляти, крім відомих, також нові атаки, знаходити серед них атаки із схожими характеристиками, та відповідно виявляти патерни нових атак. Правильно побудована мережа приманок дозволяє відслідковувати зловмисні дії в усіх точках робочої комп'ютерної мережі. Інформація, яку надає така мережа приманок разом з відповідним аналізом дозволяє в реальному часі відслідковувати зловмисні дії, кластеризувати їх, отримувати патерни атак, яким піддається мережа, а отже підвищує захищеність комп'ютерної мережі в цілому.

6.2.6 Шостий експеримент та результати

Оцінювання ефективності мультикомп'ютерних систем антивірусних комбінованих приманок та пасток необхідне для встановлення досягнення мети дослідження, яка полягає в покращенні функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Мультиикомп’ютерні системи антивірусних комбінованих приманок і пасток повинні виявляти спроби вторгнення, відволікати й затримувати зловмисника, збирати інформацію про його інструменти та тактику. Щоб оцінити ефективність таких систем, визначимо критерії оцінювання обманних технологій, які наявні в системах. При цьому будемо оцінювати обманні спроможності систем не тільки за кількістю приманок і пасток, але також з врахуванням витрат часу і ресурсів зловмисника. Розглянемо основні з них такі:

1) правдоподібність хибних об’єктів атак;

2) тривалість взаємодії зловмисника з хибними об’єктами атак;

3) спроможність зловмисника протягом певного часу встановити, що він взаємодіє з приманками;

4) ступінь інтеграції приманок в різні сегменти мережі;

5) повнота фіксування дій зловмисника чи ЗПЗ.

Введемо метрики оцінювання обманних технологій, які наявні в системах:

1) q_1 – кількість приманок, які не відрізняються від справжніх об’єктів в мережах (імітація логінів, документів, бази даних), крім тіньових приманок;

2) q_2 – кількість приманок, які демонструють реалістичну активність;

3) q_3 – частка часу на встановлення зловмисником чи ЗПЗ того, що він взаємодіє з приманками чи перебуває в штучному ізольованому середовищі, до загального оціночного часу, який необхідно для виявлення такої взаємодії;

4) q_4 – частка кроків проходження атаки в приманці і пастці до всіх передбачених кроків;

5) q_5 – частка дій зловмисника чи ЗПЗ, які фіксуються системою, до кількості всіх дій;

6) q_6 – загальна кількість приманок;

7) q_7 – кількість тіньових приманок;

8) q_8 – кількість комп’ютерних станцій в корпоративній мережі;

9) q_9 – кількість сегментів в корпоративній мережі;

10) $q_{10,i}$ – кількість приманок в i – тому сегменті мережі, $i = 1, 2, \dots N_{q_{10}}$, $N_{q_{10}}$ – кількість сегментів в корпоративній мережі;

11) $q_{11,i}$ – кількість комп'ютерних станцій та серверів в i – тому сегменті мережі, $i = 1, 2, \dots N_{q_{10}}$, $N_{q_{10}}$ – кількість сегментів в корпоративній мережі;

12) q_{12} – частка приманок по відношенню до кількості комп'ютерних станцій та серверів в корпоративній мережі;

13) $q_{13,i}$ – частка приманок по відношенню до кількості комп'ютерних станцій та серверів в i – тому сегменті мережі, $i = 1, 2, \dots N_{q_{10}}$, $N_{q_{10}}$ – кількість сегментів в корпоративній мережі;

14) q_{14} – кількість зібраних унікальних індикаторів компрометації під час взаємодії із зловмисниками;

15) q_{15} – загальна кількість зібраних індикаторів компрометації під час взаємодії із зловмисниками;

16) q_{16} – частка часу на розгортання нової приманки чи пастки порівняно з максимальним часом, який було витрачено на розгортання приманок і пасток при розгортанні всієї системи;

17) q_{17} – частка сценаріїв, які автоматично передають тривогу з пастки у SIEM/SOAR, тобто ступінь інтеграції з SIEM/SOAR.

Задамо формулу оцінювання ефективності обманних систем на основі мультиплікативного критерію так:

$$E_m = \frac{q_2}{q_1} \cdot q_3 \cdot q_4 \cdot q_5 \cdot \frac{q_1+q_7}{q_6} \cdot \frac{q_6}{q_8} \cdot D_{i=1}^{N_{q_{10}}} q_{13,i} \cdot q_{12} \cdot \frac{q_{14}}{q_{15}} \cdot q_{16} \cdot q_{17}. \qquad (6.3)$$

Аналогічно задамо формулу оцінювання ефективності обманних систем на основі адитивного критерію так:

$$E_a = \frac{1}{11} \cdot \left(\frac{q_2}{q_1} + q_3 + q_4 + q_5 + \frac{q_1+q_7}{q_6} + \frac{q_6}{q_8} + D_{i=1}^{N_{q_{10}}} q_{13,i} + q_{12} + \frac{q_{14}}{q_{15}} + q_{16} + q_{17}\right). \qquad (6.4)$$

Для порівняння розробленої системи з відомими обманними системами було здійснено їх дослідження в корпоративній мережі зі 103 хостів (робочі станції, сервери). Сегменти мережі: робочі групи; файловий сервер; принтери; демілітаризована зона. Кількість сегментів в корпоративній мережі $N_{q_{10}} = q_9 = 4$.

Результати експерименту подано в табл. 6.16 з врахуванням кількості розгорнутих приманок і пасток для систем.

Таблиця 6.16

Порівняльна характеристика

№ з/п	Назва системи	Загальна кількість приманок і пасток q_6	Значення критерію $E_m \cdot 10^{11}$	Значення критерію E_a
1	Acalvio ShadowPlex	4	0, 1374	0,4138
2	Acalvio ShadowPlex	15	0,6739	0,8537
3	TrapX DeceptionGrid	15	0,7824	0,8219
4	Zscaler Deception (Smokescreen IllusionBLACK)	15	0,5913	0,9002
5	Мультикомп’ютерна система	4	0,2418	0,4387
6	Мультикомп’ютерна система	15	0,8496	0,9325

За результатами експерименту встановлено, що із збільшенням кількості приманок та пасток покращується функціонування систем щодо протидії зловмисникам та ЗПЗ. Оптимальною кількістю приманок та пасток залежно від кількості хостів в корпоративній мережі повинно бути приблизно 15 відсотків. Для розглядуваних в експерименті систем ця кількість становить приблизно 15 відсотків. Крім того, мультикомп’ютерна система порівняно з аналогами має кращі показники ефективності в середньому на 3-6,5 % за обома критеріями, які враховують метрики щодо систем та хибних об’єктів атак.

Загалом експеримент підтвердив гіпотезу про ефективність використання мережі комбінованих приманок та пасток. Запропонована архітектура дозволяє не лише виявляти загрози з високою точністю, а й здійснювати ефективне управління реагуванням завдяки скоординованій роботі елементів системи, здатних до обміну інформацією і прийняття рішень в умовах невизначеності.

6.3 Етичні аспекти та методичні рекомендації для застосування мультикомп’ютерних систем антивірусних комбінованих приманок і пасток

Розглянемо етичні принципи використання технологій приманок та пасток у корпоративних мережах. Приманки і пастки створюються з метою виявлення і фіксації несанкціонованої активності, аналізу спроб вторгнення та збору даних для

вдосконалення систем кіберзахисту. Приманка завжди передбачає наявність вбудованих пасток, що фіксують дії порушника/зловмисника і дозволяють отримати докази спроб зламу. Зловмисник цілеспрямовано здійснює спроби отримання доступу в корпоративну мережу і може бути легальним користувачем з певною роллю в системі, а може і не бути. Порушник може здійснити певні дії несвідомо і не мати за мету виконання зловмисних дій, але може діяти як зловмисник. При цьому він розглядається як легальний користувач.

Технології приманок із вбудованими пастками впроваджуються виключно для оборонних цілей — моніторингу, збору інформації про загрози та підвищення рівня безпеки корпоративної мережі. Забороняється використання приманок для активного втручання у зовнішні мережі чи провокування порушників на вчинення незаконних дій. Будь-яке використання приманок повинно відповідати політиці інформаційної безпеки підприємства.

Використання приманок здійснюється у відповідності до чинного законодавства про захист персональних даних, комерційної та конфіденційної інформації. Працівники підприємства обов’язково інформуються про існування механізмів моніторингу та збору даних у мережі шляхом ознайомлення з внутрішніми нормативними актами. Збір даних має бути обґрунтованим і використовуватися винятково для гарантування кібербезпеки.

При застосуванні мультикомп’ютерних систем антивірусних приманок та пасток обов’язково потрібно дотримуватись принципу мінімізації даних. Приманки та пастки повинні збирати тільки мінімально необхідні дані для виявлення і протидії спробам вторгнення. Персональні дані співробітників та користувачів не повинні фіксуватися без обґрунтованої потреби. У випадку збору такі дані обов’язково знеособлюються або шифруються. Дані зберігаються лише протягом часу, необхідного для аналізу загроз і реагування на інциденти.

Доступ до інформації, яка зібрана системою з приманками і пастками, повинні мати тільки уповноважені працівники підрозділу інформаційної безпеки або IT-відділу. Забороняється передача цих даних третім особам без належних підстав і погодження керівництва. Усі співробітники з доступом до таких даних зобов’язані підписати угоди про конфіденційність.

Системи з приманки і пастками повинні бути належним чином ізольовані від основної корпоративної мережі, щоб унеможливити використання їх зловмисниками як точки проникнення. Відповідальні співробітники регулярно повинні перевіряти стан системи з приманками і пастками, своєчасно оновлювати їх та усувати потенційні вразливості. Усі дії виконуються відповідно до затверджених внутрішніх регламентів і процедур безпеки.

Для працівників, які залучені до розгортання і обслуговування системи з приманками та пастками, повинна бути встановлена персональна відповідальність за дотримання етичних норм. На підприємстві потрібно встановлювати та здійснювати регулярний контроль у формі внутрішніх аудитів для перевірки дотримання етичних норм і ефективності роботи систем з приманками і пастками.

Мультикомп’ютерна система антивірусних комбінованих приманок і пасток це цілісна обманна система, що повинна функціонувати проти зовнішніх і внутрішніх загроз. При цьому вона повинна містити протоколи роботи для дослідження інцидентів та результатів її функціонування протягом тривалого часу, а також пояснень того, на основі чого нею приймались рішення.

Крім етичних аспектів з використання таких систем, розглянемо методичні рекомендації щодо впровадження мультикомп’ютерної системи антивірусних комбінованих приманок і пасток у корпоративній мережі.

Стратегічна мета застосування мультикомп’ютерної системи антивірусних комбінованих приманок і пасток у корпоративній мережі полягає у покращенні безпеки та захисту мережі та її ресурсів на основі встановлення комплексної обманної інфраструктури. Її основне призначення спрямоване на введення в оману потенційних зловмисників, що діють як ззовні, так і зсередини корпоративної мережі, а також ЗПЗ. Вона імітує реальні сервіси та ресурси організації, фіксує спроби несанкціонованого доступу та аналізує дії атакуючих або ЗПЗ.

Принцип роботи: основна частина системи є загальною і в ній приймаються остаточні рішення щодо наступних кроків системи та реагування на події, також з неї здійснюється керування приманками і пастками як периферійними обманними об’ктами. Збір технічних доказів активності зловмисників здійснюється осовною частиною системи та окремими її засобами. Приманки та пастки копіюють реальні

сервіси (сервери баз даних, файлові ресурси, облікові записи, порти) і створюють ілюзію справжньої робочої інфраструктури. Зловмисник, взаємодіючи з такою системою, залишає сліди своїх дій, тактики і використовуваних експлойтів або ЗПЗ. При розгортанні системи потрібно встановити комп'ютерні станції, в які будуть встановлені компоненти для підтримки основної частини системи. Також, кількість та тип приманок і пасток та здійснення вибору вузлів для них потребують врахування того, чи допускають вони виконання роботи персоналом на тих комп'ютерних станціях та розміщення в них компонентів основної частини системи.

Перед встановленням системи потрібно здійснити облік потенційних загроз на виявлення яких будуть долучені в систему приманки та пастки. Система призначена для виявлення та протидії: зовнішнім атакам з Інтернету (сканування, спроби вторгнення, експлуатація вразливостей); внутрішнім загрозам (недобросовісні працівники, випадкові або навмисні порушення); автоматизованим атакам (комп'ютерні віруси, трояни, бот-мережі).

Система має динамічну структуру, що дозволяє змінювати топологію мережі, запускати або вимикати окремі приманки і пастки, тому центр системи та контролер прийняття рішень можуть переміщатись між вузлами для уникнення компрометації та продовження роботи у випадку атаки на окремий вузол. В зв'язку з цим на початку розгортання системи повинні бути визначенні вузли для встановлення компонент, що підтримують основну частину системи. Система сама визначить місця перебування центру системи та контролеру прийняття рішень. Вузли обманної системи розподілені у різних сегментах мережі для контролю різних точок доступу, якщо корпоративна мережа поділена на сегменти.

Приманки і пастки потрібно розміщувати поруч із критично важливими ресурсами, імітуючи їх зовнішній вигляд. Вони повинні мати мінімальні зв'язки з реальною мережею, тобто тільки для фіксації даних і передачі логів до аналітичного вузла.

Система має механізми для безпечного ізольованого запуску підозрілих файлів у середовищі приманок та пасток (пісочниці). Вона містить компоненти, які підтримують технологію розподіленої пісочниці. Ці компоненти для формування

післчниці система визначає сама, оцінюючи вузли мережі згідно критеріїв їх завантаженості та безпеки.

Частина приманок і пасток інтегрується у внутрішню корпоративну мережу для відстеження дій працівників, які можуть порушувати політики безпеки. Такі вузли в корпоративній мережі потрібно визначити адміністраторам з кібербезпеки. Рекомендовано їх кількість максимізувати, а сама система буде їх активувати за потреби.

Усі дії атакуючого зловмисника журналюються і захищаються від зміни або видалення. Дані зберігаються централізовано у вузлах-логерах з багаторівневим резервуванням. Адміністратори системи не володіють інформацією щодо місць розміщення файлів аудиту та типу шифрування, а мають лише доступ для зчитування такої інформації із встановленого вузла.

Мультикомп’ютерна система антивірусних комбінованих приманок та пасток є активним елементом пасивного захисту, що створює оману для зловмисника та перетворює спробу злому на джерело безцінної інформації для служб кібербезпеки. Виходячи з цього, рекомендується включити таку систему в загальну ієрархію рівнів захисту корпоративної мережі.

Таким чином, етичні аспекти та методичні рекомендації з розгортання та експлуатації таких систем повинні бути враховані адміністраторами та власниками корпоративних мереж.

6.4 Висновки до шостого розділу

Таким чином, було встановлено досягнення мети дослідження, яка полягала в покращенні функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Для оцінювання ефективності в контексті синтезованих систем певного класу та призначення було розглянуто їх стійкість та рівновагу. Крім того, для аналізу цих

двох характеристик також досліджувався час як показник впливу на них і на результат виконання завдання спеціалізованим функціоналом системи. Результати підтверджують доцільність застосування контролеру прийняття рішень в системах. Було встановлено, що з початку функціонування системи її інтегрований показник становить більше 65% та зростає з часом її експлуатації.

Дослідження критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи для встановлення відповідності їх значень реальним станам при функціонуванні системи в моменти зміни варіантів централізації в архітектурі системи та адекватності обраним для них параметрів показало, що відхилення між крайніми значеннями цільової функції при штатному функціонуванні мультикомп'ютерної системи становить 3%, а при впливі на параметри одного з чотирьох критеріїв максимальне відхилення дорівнює 7% в момент впливу, але в подальшому система функціонує стабільно при виконанні перебудови центру.

При визначенні варіанту централізації в системах щодо встановлення наступного варіанту централізації протягом визначеного часу функціонування системи, витраченого часу на визначення наступного варіанту централізації та переходу до нього, кількості вдалих спроб переходу до наступного варіанту централізації, кількості невдалих спроб переходу до наступного варіанту централізації, значення цільової функції та показників з правил при використанні у складі системи контролера прийняття рішень значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера, тобто за рахунок використанння контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання.

Встановлено покращення функціонування системи щодо її подальших кроків за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування і було отримано дисперсію відхилень між двома випадками з наявним контролером прийняття рішень і без нього, яка становить приблизно 60% на користь системи з контролером, тому виокремлення контролера прийняття рішень та включення в його механізм функціонування попереднього досвіду дає змогу покращити функціонування систем.

Встановлення достовірності виявлення метаморфних вірусів розробленою мультикомп’ютерною системою виявлення ЗПЗ із метаморфним функціоналом з наявним контролером прийняття рішень за умови відсутності інформації в елементах пам’яті за попередні кроки забезпечує покращення виявлення метаморфних вірусів зі збільшенням кількості разів його застосування. При цьому середнє арифметичне значення достовірності виявлення для всіх класів і всіх серій і етапів експерименту дорівнює $TPR = 75.46\%$ для тієї множини вірусів, які залишались невиявленими в досліджуваному операційному середовищі після їх проходження через системи виявлення вторгнень та антивірусні засоби, а відхилення від цього значення всіх значень розроблених дванадцяти класів не перевищує 3%, що загалом дає змогу досягти достовірності виявлення при багатоетапній перевірці до 98,8 % для всієї множини ЗПЗ з метаморфним функціоналом.

Встановлено, що залежно від кількості хостів в корпоративній мереж оптимальною кількістю приманок та пасток є приблизно 15 відсотків. Крім того, мультикомп’ютерна система порівняно з аналогами має кращі показники функціонування в середньому на 3-9 % за мультиплікативним та адитивним критеріями, які враховують метрики сукупно щодо систем та хибних об’єктів атак.

Основні результати розділу опубліковані у працях [92, 96, 107, 145, 164, 165, 170, 186, 201, 203, 228, 286, 287, 288, 294, 295, 303, 312, 313, 314].

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну проблему щодо неефективного функціонування та прогнозування зловмисниками поведінки мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж в частині зміни архітектури систем та їх центрів прийняття рішень з врахування попереднього досвіду із виконання таких змін для узгодження дій щодо заплутування зловмисників з архітектурою окремих засобів, які є частиною систем, для уникнення подій, при яких система готує певні відповіді, а її автономні частини при впливах на вузли в мережах, в яких вони розміщені, реагують на ці ж події по різному, тобто наявність розбалансування дій, а також забезпечення різних варіантів відповідей на повторювані зловмисні дії узгодженням дій всіх частин систем і прийняття рішень без залучення адміністратора. Вирішення даної проблеми має важливе значення в усіх галузях, де активно застосовуються корпоративні мережі.

При цьому отримано такі основні наукові та практичні результати:

1. Досліджено особливості функціонування мультикомп’ютерних систем антивірусних комбінованих приманок та пасток виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж та проаналізовано ефективність роботи сучасних обманних систем з приманками та пастками, а також їх архітектуру і компоненти, що дало змогу встановити недоліки в архітектурі таких систем, а також недоліки в організації функціонування систем з приманками різних рівнів взаємодії та визначено стратегії щодо усунення недоліків.

2. Запропоновано концепцію вирішення науково-прикладної проблеми, яка полягає у поєднанні та синтезі в системах таких визначальних властивостей, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних

приманок і пасток в системі, що дало змогу синтезувати мультикомп’ютерні системи антивірусних комбінованих приманок і пасток в корпоративних мережах, які будуть автономними, складними в прогнозуванні їх наступних кроків та розуміння їх принципів функціонування зловмисниками, для покращення виявлення та протидії ЗПЗ і КА.

3. Розроблено принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, який містить дві визначальні вимоги щодо наявності в архітектурі систем контролера та спеціалізованого функціоналу, що дало змогу впливати на рішення систем щодо їх наступних кроків та зміни архітектури і в результаті це ускладнило для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах та покращило ефективність виявлення та протидії ЗПЗ і КА в корпоративних мережах.

4. Розроблено концептуальну модель мультикомп’ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також забезпечує стійкість систем при вилученні певних вузлів в корпоративних мережах та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА.

5. Розроблено математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дали змогу сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах. Для критеріїв отримані

значення різниці між крайніми значеннями цільової функції при штатному функціонуванні мультикомп’ютерної системи, які становлять 3%, а при впливі на параметри одного з чотирьох критеріїв максимальна різниця дорівнює 7% в момент впливу і в подальшому система продовжує функціонувати стабільно при виконанні перебудови центру.

6. Розроблено метод визначення варіанту централізації в мультикомп’ютерних системах, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, і який дав змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і обрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі, зокрема при визначенні варіанту централізації з використанням у складі системи контролера прийняття рішень значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера, тобто за рахунок використанння контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання, при цьому використано розроблені правила дають змогу забезпечити стабільність функціонування системи без залучення адміністратора.

7. Розроблено метод організації функціонування контролера прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв’язків між ними, що дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах.

8. Розроблено метод організації функціонування мультикомп’ютерних систем, який на відміну від відомих, дає змогу забезпечити можливості систем до самостійної

зміни своїх властивостей, організації елементів та компонентів і встановлення зв’язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролера прийняття рішень та центру систем, що забезпечило багатоваріантність при опрацюванні відповіді на події, які викликані зовнішніми та внутрішніми впливами на системи в корпоративних мережах. При практичному застосуванні методу встановлено, що з початку функціонування системи її інтегрований показник щодо стійкості та рівноваги становить більше 65% та зростає з часом її експлуатації, а при забезпеченні її подальших кроків за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування було отримано дисперсію відхилень між двома випадками з наявним контролером прийняття рішень і без нього приблизно 60% на користь системи з контролером.

9. Розроблено метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснено збір даних та кластеризацію схожих зловмисників з використанням мультикомп’ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА.

10. Розроблено метод виявлення ЗПЗ і КА, який реалізується в архітектурі мультикомп’ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи), що забезпечує адаптивне, варіативне реагування, прийняття рішень як на рівні приманок, так і центрів системи, ускладнює зловмисникам розуміння логіки її функціонування та, відповідно, підвищує ефективність протидії. При практичному застосуванні методу встановлено, що середнє арифметичне значення достовірності виявлення для всіх класів ЗПЗ з метаморфним функціоналом дорівнює 75.46% для тієї множини вірусів, які залишались невиявленими в досліджуваному операційному

середовищі після їх проходження через системи виявлення вторгнень та антивірусні засоби, а відхилення від цього значення всіх значень розроблених дванадцяти класів не перевищує 3%, що загалом дає змогу досягти достовірності виявлення при багатоетапній перевірці до 98,8 % для всієї множини ЗПЗ з метаморфним функціоналом.

11. Розроблено мультикомп’ютерну систему антивірусних комбінованих приманок та пасток, яка продемонструвала покращення функціонування на 3-9% за мультиплікативним та адитивним критеріями, які враховують метрики сукупно щодо систем та хибних об’єктів атак, а також виявлення та протидії ЗПЗ та КА з наявним контролером прийняття рішень порівняно з системами без нього, для підтвердження реалізації запропонованих принципу та методів синтезу таких систем, підтвердження спроможності їх практичного створення та використання в експериментальних дослідженнях для порівняння з відомими системами виявлення і впровадити розроблену систему в корпоративних мережах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A comprehensive survey on cyber deception techniques to improve honeypot performance / A. Javadpour et al. *Computers & security*. 2024. P. 103792. URL: https://doi.org/10.1016/j.cose.2024.103792 (date of access: 08.05.2025).

2. A cost-effective security management for clouds: a game-theoretic deception mechanism / M. T. Adili et al. *2017 IFIP/IEEE symposium on integrated network and service management (IM)*, Lisbon, Portugal, 8–12 May 2017. 2017. URL: https://doi.org/10.23919/inm.2017.7987269 (date of access: 05.05.2025).

3. A deep learning assisted personalized deception system for countering web application attacks / W. B. Shahid et al. *Journal of information security and applications*. 2022. Vol. 67. P. 103169. URL: https://doi.org/10.1016/j.jisa.2022.103169 (date of access: 06.05.2025).

4. A detection of malware embedded into web pages using client honeypot / M. Veena et al. *Computer security threats*. 2020. URL: https://doi.org/10.5772/intechopen.89646 (date of access: 05.05.2025).

5. A distributed cloud honeypot architecture / J. X. Huang et al. *2021 IEEE 45th annual computers, software, and applications conference (COMPSAC)*, Madrid, Spain, 12–16 July 2021. 2021. URL: https://doi.org/10.1109/compsac51774.2021.00162 (date of access: 05.05.2025).

6. A first look: using linux containers for deceptive honeypots / A. Kedrowitsch et al. Proceedings of the 2017 workshop on automated decision making for active cyber defense (safeconfig ’17). association for computing machinery, New York, NY, USA. 2017. P. 15–22. URL: https://doi.org/10.1145/3140368.3140371.

7. A highly interactive honeypot-based approach to network threat management / X. Yang et al. *Future internet*. 2023. Vol. 15, no. 4. P. 127. URL: https://doi.org/10.3390/fi15040127 (date of access: 05.05.2025).

8. A honeypot proxy framework for deceiving attackers with fabricated content / J. Papalitsas et al. *Advances in information security*. Cham, 2018. P. 239–258. URL: https://doi.org/10.1007/978-3-319-73951-9_12 (date of access: 04.05.2025).

9. A mathematical model for analyzing honeynets and their cyber deception techniques / A. Javadpour et al. *2023 27th international conference on engineering of complex computer systems (ICECCS)*, Toulouse, France, 14–16 June 2023. 2023. URL: https://doi.org/10.1109/iceccs59891.2023.00019 (date of access: 08.05.2025).

10. A method for detecting botnets in IT infrastructure using a neural network / D. Denysiuk et al. *CEUR workshop proceedings*. 2024. Vol. 3736. P. 282–292. URL: https://ceur-ws.org/Vol-3736/paper21.pdf.

11. A model of an intelligent clustering system with an external module for the architecture of RTOS with intensive changes of states regarding their flexibility and balancing / O. Kozelskiy et al. *CEUR workshop proceedings*. 2025. Vol. 3899. P. 234–243. URL: https://ceur-ws.org/Vol-3899/paper21.pdf.

12. A new method of cyber deception defense / C. Liu et al. *2024 IEEE symposium on computers and communications (ISCC)*, Paris, France, 26–29 June 2024. 2024. P. 1–7. URL: https://doi.org/10.1109/iscc61673.2024.10733695 (date of access: 08.05.2025).

13. A novel deception defense-based honeypot system for power grid network / M. Feng et al. *Lecture notes in computer science*. Cham, 2022. P. 297–307. URL: https://doi.org/10.1007/978-3-030-97774-0_27 (date of access: 04.05.2025).

14. A security framework for the detection of targeted attacks using honeypot / P. Subhash et al. *Proceedings of fifth international conference on computer and communication technologies*. Singapore, 2024. P. 183–192. URL: https://doi.org/10.1007/978-981-99-9704-6_16 (date of access: 06.05.2025).

15. A scalable high-interaction physical honeypot framework for programmable logic controller / J. You et al. *2020 IEEE 92nd vehicular technology conference (vtc2020-fall)*, Victoria, BC, Canada, 18 November – 16 December 2020. 2020. URL: https://doi.org/10.1109/vtc2020-fall49728.2020.9348483 (date of access: 05.05.2025).

16. A survey of deception defense: approaches used to counter malicious behavior / H. Yi et al. *2023 IEEE 12th international conference on cloud networking (cloudnet)*, Hoboken, NJ, USA, 1–3 November 2023. 2023. URL: https://doi.org/10.1109/cloudnet59005.2023.10490043 (date of access: 04.05.2025).

17. A survey on honeypot software and data analysis / M. Nawrocki et al. 2016. URL: https://doi.org/10.48550/arXiv.1608.06249.

18. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems / J. Franco et al. *IEEE communications surveys & tutorials*. 2021. P. 1. URL: https://doi.org/10.1109/comst.2021.3106669 (date of access: 05.05.2025).

19. A survey of moving target defenses for network security / S. Sengupta et al. *IEEE communications surveys & tutorials*. 2020. Vol. 22, no. 3. P. 1909–1941. URL: https://doi.org/10.1109/comst.2020.2982955 (date of access: 05.05.2025).

20. A web-based honeypot in ipv6 to enhance security / K. Wang et al. *Information*. 2020. Vol. 11, no. 9. P. 440. URL: https://doi.org/10.3390/info11090440 (date of access: 27.04.2025).

21. *Acalvio ShadowPlex. Autonomous Deception*. URL: https://www.acalvio.com/product/ (date of access: 06.08.2023).

22. ACyDS: an adaptive cyber deception system / C.-Y. J. Chiang et al. *MILCOM 2016 - 2016 IEEE military communications conference (MILCOM)*, Baltimore, MD, USA, 1–3 November 2016. 2016. P. 800–805. URL: https://doi.org/10.1109/milcom.2016.7795427 (date of access: 06.05.2025).

23. Active security control approach against dos attacks in cyber-physical systems / T. Li et al. *IEEE transactions on automatic control*. 2020. Vol. 66, no. 9. P. 4303–4310. URL: https://doi.org/10.1109/tac.2020.3032598 (date of access: 06.05.2025).

24. ADAPT: adaptive camouflage based deception orchestration for trapping advanced persistent threats / P. V. S. Charan et al. *Digital threats: research and practice*. 2024. Vol. 5, no. 3. 21. URL: https://doi.org/10.1145/3651991 (date of access: 06.05.2025).

25. AHEAD: a new architecture for active defense / F. De Gaspari et al. *Association for computing machinery*. P. 11–16. URL: https://doi.org/10.1145/2994475.2994481.

26. Agrawal N., Tapaswi S. The performance analysis of honeypot based intrusion detection system for wireless network. *International journal of wireless information networks*. 2017. Vol. 24, no. 1. P. 14–26. URL: https://doi.org/10.1007/s10776-016-0330-3 (date of access: 06.05.2025).

27. Aggarwal P. D., Singh K., González C. Decoys in cybersecurity: an exploratory study to test the effectiveness of 2-sided deception. *ArXiv*. URL: https://arxiv.org/abs/2108.11037 (date of access: 26.04.2025).

28. Aggarwal P., Gonzalez C., Dutt V. Cyber-Security: role of deception in cyber-attack detection. *Advances in intelligent systems and computing*. Cham, 2016. P. 85–96. URL: https://doi.org/10.1007/978-3-319-41932-9_8 (date of access: 27.04.2025).

29. Al-Shaer E. A cyber mutation: metrics, techniques and future directions. *Proceedings of the 2016 ACM workshop on moving target defense (MTD '16). association for computing machinery*, New York. 2016. URL: https://doi.org/10.1145/2995272.2995285.

30. Almeshekah M. H., Spafford E. H. Cyber security deception. *Cyber deception*. Cham, 2016. P. 23–50. URL: https://doi.org/10.1007/978-3-319-32699-3_2 (date of access: 26.04.2025).

31. Almeshekah M. H., Spafford E. H. Planning and integrating deception into computer security defenses. *The 2014 workshop*, Victoria, British Columbia, Canada, 15–18 September 2014. New York, New York, USA, 2014. URL: https://doi.org/10.1145/2683467.2683482 (date of access: 27.04.2025).

32. Amal M., Venkadesh P. Review of cyber attack detection: honeypot system. *Webology*. 2022. Vol. 19, no. 1. P. 5497–5514. URL: https://doi.org/10.14704/web/v19i1/web19370 (date of access: 04.05.2025).

33. An adaptive honeypot deployment algorithm based on learning automata / Y. Zhang et al. *2017 IEEE second international conference on data science in cyberspace (DSC)*, Shenzhen, China, 26–29 June 2017. 2017. URL: https://doi.org/10.1109/dsc.2017.52 (date of access: 05.05.2025).

34. An adaptive honeypot using Q-Learning with severity analyzer / S. Suratkar et al. *Journal of ambient intelligence and humanized computing*. 2021. URL: https://doi.org/10.1007/s12652-021-03229-2 (date of access: 05.05.2025).

35. An analysis of worm dynamics with honeypot feedback in scale-free networks / J. Xue et al. *IAENG international journal of computer science*. 2025. Vol. 52, no. 1. P. 90–102.

36. An IoT honeynet based on multiport honeypots for capturing IoT attacks / W. Zhang et al. *IEEE internet of things journal*. 2020. Vol. 7, no. 5. P. 3991–3999. URL: https://doi.org/10.1109/jiot.2019.2956173 (date of access: 05.05.2025).

37. An innovative honeypot architecture for detecting and mitigating hardware trojans in iot devices / A. H. E. Omar et al. *IoT*. 2024. Vol. 5, no. 4. P. 730–755. URL: https://doi.org/10.3390/iot5040033 (date of access: 05.05.2025).

38. Antonioli D., Agrawal A., Tippenhauer N. O. Towards High-Interaction Virtual ICS Honeypots-in-a-Box. *The 2nd ACM workshop*, Vienna, Austria, 28 October 2016. New York, New York, USA, 2016. URL: https://doi.org/10.1145/2994487.2994493 (date of access: 05.05.2025).

39. Anwar A. H., Kamhoua C. A. Cyber deception using honeypot allocation and diversity: a game theoretic approach. *2022 IEEE 19th annual consumer communications & networking conference (CCNC)*, Las Vegas, NV, USA, 8–11 January 2022. 2022. URL: https://doi.org/10.1109/ccnc49033.2022.9700616 (date of access: 25.04.2025).

40. Anwar A. H., Kamhoua C., Leslie N. Honeypot allocation over attack graphs in cyber deception games. *2020 international conference on computing, networking and communications (ICNC)*, Big Island, HI, USA, 17–20 February 2020. 2020. URL: https://doi.org/10.1109/icnc47757.2020.9049764 (date of access: 25.04.2025).

41. Arifianto R. M., Sukarno P., Jadied E. M. An SSH honeypot architecture using port knocking and intrusion detection system. *2018 6th international conference on information and communication technology (icoict)*, Bandung, 3–5 May 2018. 2018. URL: https://doi.org/10.1109/icoict.2018.8528787 (date of access: 04.05.2025).

42. Approaches for preventing honeypot detection and compromise / M. Tsikerdekis et al. *2018 global information infrastructure and networking symposium (GIIS)*, Thessaloniki, Greece, 23–25 October 2018. 2018. URL: https://doi.org/10.1109/giis.2018.8635603 (date of access: 04.05.2025).

43. Autonomous cyber deception: reasoning, adaptive planning, and evaluation of honeythings / C. Wang et al. Springer, 2019. 247 p. URL: https://doi.org/10.1007/978-3-030-02110-8 (date of access: 26.04.2025).

44. A survey on deception techniques for securing web application / A. I. M. Efendi et al. 2019 IEEE 5th intl conference on big data security on cloud (bigdatasecurity), IEEE intl conference on high performance and smart computing, (HPSC) and IEEE intl conference on intelligent data and security (IDS), Washington, DC, USA, 27–29 May 2019.

2019. URL: https://doi.org/10.1109/bigdatasecurity-hpsc-ids.2019.00066 (date of access: 27.04.2025).

45. Automatic identification of honeypot server using machine learning techniques / C. Huang et al. *Security and communication networks*. 2019. Vol. 2019. P. 1–8. URL: https://doi.org/10.1155/2019/2627608 (date of access: 08.05.2025).

46. Automated honeynet deployment strategy for active defense in container-based cloud / T. Kong et al. 2020 IEEE 22nd international conference on high performance computing and communications; IEEE 18th international conference on smart city; IEEE 6th international conference on data science and systems (hpcc/smartcity/dss), Yanuca Island, Cuvu, Fiji, 14–16 December 2020. 2020. P. 483–490. URL: https://doi.org/10.1109/hpcc-smartcity-dss50907.2020.00059 (date of access: 06.05.2025).

47. Baykara M., Das R. A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of information security and applications*. 2018. Vol. 41. P. 103–116. URL: https://doi.org/10.1016/j.jisa.2018.06.004 (date of access: 06.05.2025).

48. Baykara M., Daş R. A survey on potential applications of honeypot technology in intrusion detection systems. *International journal of computer networks and applications (IJCNA)*. 2015. Vol. 2, no. 5. P. 203–211.

49. Baykara M., Daş R. SoftSwitch: a centralized honeypot-based security approach usingsoftware-defined switching for secure management of VLAN networks. *Turkish journal of electrical engineering & computer sciences*. 2019. Vol. 27, no. 5. P. 3309–3325. URL: https://doi.org/10.3906/elk-1812-86 (date of access: 08.05.2025).

50. Behan L., Sevcik L., Voznak M. Development of a distributed voip honeypot system with advanced malicious traffic detection. *Lecture notes in electrical engineering*. Cham, 2019. P. 409–419. URL: https://doi.org/10.1007/978-3-030-14907-9_40 (date of access: 05.05.2025).

51. Behavioral study of users when interacting with active honeytokens / A. Shabtai et al. *ACM transactions on information and system security*. 2016. Vol. 18, no. 3. P. 1–21. URL: https://doi.org/10.1145/2854152 (date of access: 27.04.2025).

52. Biswas J. Analysis of client honeypots. *(IJCSIT) international journal of computer science and information technologies*. 2014. Vol. 5, no. 4. P. 5776–5780. URL: https://ijcsit.com/docs/Volume%205/vol5issue04/ijcsit20140504209.pdf.

53. Breeden J. Buyer's guide: 5 top deception tools and how they ensnare attackers. *CSO*. URL: https://www.csoonline.com/article/570063/5-top-deception-tools-and-how-they-ensnare-attackers.html

54. Bringer M. L., Chelmecki C. A., Fujinoki H. A survey: recent advances and future trends in honeypot research. *International journal of computer network and information security*. 2012. Vol. 4, no. 10. P. 63–75. URL: https://doi.org/10.5815/ijcnis.2012.10.07 (date of access: 08.05.2025).

55. CamDec: Advancing Axis P1435-LE video camera security using honeypot-based deception / L. F. Sikos et al. *Journal of computer virology and hacking techniques*. 2023. URL: https://doi.org/10.1007/s11416-023-00463-4 (date of access: 04.05.2025).

56. Game theory for adaptive defensive cyber deception / K. Ferguson-Walter et al. *The 6th annual symposium*, Nashville, Tennessee, 1–3 April 2019. New York, New York, USA, 2019. URL: https://doi.org/10.1145/3314058.3314063 (date of access: 08.05.2025).

57. Campbell R. M., Padayachee K., Masombuka T. A survey of honeypot research: trends and opportunities. *2015 10th international conference for internet technology and secured transactions (ICITST)*, London, United Kingdom, 14–16 December 2015. 2015. URL: https://doi.org/10.1109/icitst.2015.7412090 (date of access: 04.05.2025).

58. Gao C., Wang Y., Xiong X. A cyber deception defense method based on signal game to deal with network intrusion. *Security and communication networks*. 2022. Vol. 2022. P. 1–17. URL: https://doi.org/10.1155/2022/3949292 (date of access: 06.05.2025).

59. Gao Y., Zhang G., Xing C. A multiphase dynamic deployment mechanism of virtualized honeypots based on intelligent attack path prediction. *Security and communication networks*. 2021. Vol. 2021. P. 1–15. URL: https://doi.org/10.1155/2021/6378218 (date of access: 05.05.2025).

60. Catuogno L., Castiglione A., Palmieri F. A honeypot system with honeyword-driven fake interactive sessions. *2015 international conference on high performance*

computing & simulation (HPCS), Amsterdam, Netherlands, 20–24 July 2015. 2015. URL: https://doi.org/10.1109/hpcsim.2015.7237039 (date of access: 05.05.2025).

61. Chicco D., Jurman G. The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. *BioData mining*. 2023. Vol. 16, no. 1. URL: https://doi.org/10.1186/s13040-023-00322-4 (date of access: 25.04.2025).

62. Chovancová E., Ádám N. A clustered hybrid honeypot architecture. *Acta polytechnica hungarica*. 2019. Vol. 16, no. 10. P. 173–189. URL: https://doi.org/10.12700/aph.16.10.2019.10.11 (date of access: 04.05.2025).

63. Chouhan P. K., Aujla G. S. Deception technology for active defence: background and opportunities. *2024 IEEE international conference on communications workshops (ICC workshops)*, Denver, CO, USA, 9–13 June 2024. 2024. P. 1183–1188. URL: https://doi.org/10.1109/iccworkshops59551.2024.10615759 (date of access: 04.05.2025).

64. Client honeypot based malware program detection embedded into web pages / S. Kaur et al. 2013. URL: https://api.semanticscholar.org/CorpusID:35982505.

65. Gokhale S., Dalvi A., Siddavatam I. Industrial control systems honeypot: a formal analysis of conpot. *International journal of computer network and information security*. 2020. Vol. 12, no. 6. P. 44–56. URL: https://doi.org/10.5815/ijcnis.2020.06.04 (date of access: 05.05.2025).

66. Combining markov and semi-markov modelling for assessing availability and cybersecurity of cloud and iot systems / V. Kharchenko et al. *Cryptography*. 2022. Vol. 6, no. 3. P. 44. URL: https://doi.org/10.3390/cryptography6030044 (date of access: 10.05.2025).

67. Compression of network traffic parameters for detecting cyber attacks based on deep learning / M. Komar et al. *2018 IEEE 9th international conference on dependable systems, services and technologies (DESSERT)*, Kyiv, Ukraine, 24–27 May 2018. 2018. P. 44–48. URL: https://doi.org/10.1109/dessert.2018.8409096 (date of access: 10.05.2025).

68. CONCEAL: a strategy composition for resilient cyber deception-framework, metrics and deployment / Q. Duan et al. *2018 IEEE conference on communications and network security (CNS)*, Beijing, 30 May – 1 June 2018. 2018. URL: https://doi.org/10.1109/cns.2018.8433196 (date of access: 06.05.2025).

69. Concealing cyber-decoys using two-sided feature deception games / M. S. Miah et al. *Hawaii international conference on system sciences*. 2020. URL: https://doi.org/10.24251/hicss.2020.235 (date of access: 04.05.2025).

70. Gopireddy S. R. AI-Augmented honeypots for cloud environments: proactive threat. *European journal of advances in engineering and technology*. 2019. Vol. 6(12). P. 85–89. URL: https://ejaet.com/PDF/6-12/EJAET-6-12-85-89.pdf.

71. *Counter Craft Security*. URL: https://www.countercraftsec.com/ (дата звернення: 06.08.2023).

72. Cutting edge trends in deception based intrusion detection systems–a survey / O. U. Oluoha et al. *Journal of information security*. 2021. Vol. 12, no. 04. P. 250–269. URL: https://doi.org/10.4236/jis.2021.124014 (date of access: 06.05.2025).

73. Cyber deception: virtual networks to defend insider reconnaissance / S. Achleitner et al. Proceedings of the 8th ACM CCS international workshop on managing insider security threats (MIST '16). association for computing machinery, New York. 2016. P. 57–68. URL: https://doi.org/10.1145/2995959.2995962.

74. Cybersecurity deception experimentation system / J. C. Acosta et al. *2020 IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 28–30 September 2020. 2020. URL: https://doi.org/10.1109/secdev45635.2020.00022 (date of access: 06.05.2025).

75. Dahbul R. N., Lim C., Purnama J. Enhancing honeypot deception capability through network service fingerprinting. *Journal of physics: conference series*. 2017. Vol. 801. P. 012057. URL: https://doi.org/10.1088/1742-6596/801/1/012057 (date of access: 08.05.2025).

76. Dasent S. Dynamic honeypots. *Wellington faculty of engineering symposium*. 2023. URL: https://ojs.wgtn.ac.nz/wfes/article/view/8364.

77. Data mining in long-term honeypot data / D. Fraunholz et al. *2017 IEEE international conference on data mining workshops (ICDMW)*, New Orleans, LA, 18–21 November 2017. 2017. URL: https://doi.org/10.1109/icdmw.2017.92 (date of access: 05.05.2025).

78. Datasheet. *Labyrinth Deception Platform*. URL: https://labyrinth.tech/assets/media/pdf/labyrinth-data-sheet.pdf (date of access: 06.08.2023).

79. De Faveri C., Moreira A., Amaral V. Multi-paradigm deception modeling for cyber defense. *Journal of systems and software*. 2018. Vol. 141. P. 32–51. URL: https://doi.org/10.1016/j.jss.2018.03.031 (date of access: 08.05.2025).

80. Deceptive attack and defense game in honeypot-enabled networks for the internet of things / Q. D. La et al. *IEEE internet of things journal*. 2016. Vol. 3, no. 6. P. 1025–1035. URL: https://doi.org/10.1109/jiot.2016.2547994 (date of access: 26.04.2025).

81. Deceiving network reconnaissance using sdn-based virtual topologies / S. Achleitner et al. *IEEE transactions on network and service management*. 2017. Vol. 14, no. 4. P. 1098–1112. URL: https://doi.org/10.1109/tnsm.2017.2724239 (date of access: 27.04.2025).

82. Deceiving cyber adversaries: a game theoretic approach / A. Schlenker et al. Proceedings of the 17th international conference on autonomous agents and multiagent systems (AAMAS '18). international foundation for autonomous agents and multiagent systems, Richland, SC. P. 892–900. URL: https://dl.acm.org/doi/10.5555/3237383.3237833.

83. Deceptive routing in relay networks / A. Clark et al. *Lecture notes in computer science*. Berlin, Heidelberg, 2012. P. 171–185. URL: https://doi.org/10.1007/978-3-642-34266-0_10 (date of access: 27.04.2025).

84. Decepti-SCADA: a cyber deception framework for active defense of networked critical infrastructures / N. Cifranic et al. *Internet of things*. 2020. Vol. 12. P. 100320. URL: https://doi.org/10.1016/j.iot.2020.100320 (date of access: 06.05.2025).

85. Deception-Based game theoretical approach to mitigate dos attacks / H. Çeker et al. *Lecture notes in computer science*. Cham, 2016. P. 18–38. URL: https://doi.org/10.1007/978-3-319-47413-7_2 (date of access: 26.04.2025).

86. Deception attack detection of isolated DC microgrids under consensus- based distributed voltage control architecture / D. Shi et al. *IEEE journal on emerging and selected topics in circuits and systems*. 2021. Vol. 11, no. 1. P. 155–167. URL: https://doi.org/10.1109/jetcas.2021.3050784 (date of access: 05.05.2025).

87. Deception in network defences using unpredictability / J. Happa et al. *Digital threats: research and practice*. 2021. Vol. 2, no. 4. P. 1–26. URL: https://doi.org/10.1145/3450973 (date of access: 05.05.2025).

88. Demystifying deception technology: a survey / D. Fraunholz et al. 2018. URL: https://doi.org/10.48550/arXiv.1804.06196.

89. Design thinking for cyber deception / D. Ashenden et al. *Hawaii international conference on system sciences*. 2021. URL: https://doi.org/10.24251/hicss.2021.240 (date of access: 04.05.2025).

90. Designing and evaluating a flexible and scalable HTTP honeypot platform: architecture, implementation, and applications / M. Rabzelj et al. *Electronics*. 2023. Vol. 12, no. 16. P. 3480. URL: https://doi.org/10.3390/electronics12163480 (date of access: 04.05.2025).

91. Detecting targeted attacks using shadow honeypots / K. G. Anagnostakis et al. *Proceedings of the conference on USENIX security symposium*. 2005. P. 9–23.

92. Detection of computer attacks based on sonification of network traffic / B. Semeniuk et al. CEUR workshop proceedings. 2025. Vol. 3963. P. 252-263. URL: https://ceur-ws.org/Vol-3963/paper21.pdf

93. Development of a concept for building a critical infrastructure facilities security system / S. Yevseiev et al. *Eastern-European journal of enterprise technologies*. 2021. Vol. 3, no. 9(111). P. 63–83. URL: https://doi.org/10.15587/1729-4061.2021.233533 (date of access: 10.05.2025).

94. Dhanalakshmi K. S., BabyShalini V. Medium interaction honeypot for network security to detect cyber attacks. *3C Tecnología_Glosas de innovación aplicadas a la pyme*. 2021. P. 397–409. URL: https://doi.org/10.17993/3ctecno.2021.specialissue8.397-409 (date of access: 05.05.2025).

95. DiPot: a distributed industrial honeypot system / J. Cao et al. *Lecture notes in computer science*. Cham, 2018. P. 300–309. URL: https://doi.org/10.1007/978-3-319-73830-7_30 (date of access: 06.05.2025).

96. Distributed system for predicting malicious activity in computer networks / D. Liubinetskyi et al. *CEUR workshop proceedings*. 2023. Vol. 3373. P. 401–410. URL: https://ceur-ws.org/Vol-3373/paper26.pdf.

97. DodgeTron: towards autonomous cyber deception using dynamic hybrid analysis of malware / M. S. I. Sajid et al. *2020 IEEE conference on communications and network*

security (CNS), Avignon, France, 29 June – 1 July 2020. 2020. URL: https://doi.org/10.1109/cns48642.2020.9162202 (date of access: 06.05.2025).

98. Dodson M., Beresford A. R., Vingaard M. Using global honeypot networks to detect targeted ICS attacks. *2020 12th international conference on cyber conflict (cycon)*, Estonia, 26–29 May 2020. 2020. P. 275–291. URL: https://doi.org/10.23919/cycon49761.2020.9131734 (date of access: 06.05.2025).

99. Dowling S., Schukat M., Barrett E. Improving adaptive honeypot functionality with efficient reinforcement learning parameters for automated malware. *Journal of cyber security technology*. 2018. P. 1–17. URL: https://doi.org/10.1080/23742917.2018.1491460 (date of access: 06.05.2025).

100. Dynamic distributed honeypot based on blockchain / L. Shi et al. *IEEE access*. 2019. Vol. 7. P. 72234–72246. URL: https://doi.org/10.1109/access.2019.2920239 (date of access: 06.05.2025).

101. Dynamic forensics based on intrusion tolerance / L. Chen et al. *2009 IEEE international symposium on parallel and distributed processing with applications*, Chengdu, Sichuan, China, 10–12 August 2009. 2009. P. 469–473. URL: https://doi.org/10.1109/ispa.2009.66 (date of access: 08.05.2025).

102. Dynamic virtual network honeypot / B. Park et al. *2019 international conference on information and communication technology convergence (ICTC)*, Jeju Island, Korea (South), 16–18 October 2019. 2019. URL: https://doi.org/10.1109/ictc46691.2019.8939791 (date of access: 05.05.2025).

103. Ellouh M., Ghaleb M., Felemban M. IoTZeroJar: towards a honeypot architecture for detection of zero-day attacks in iot. *2022 14th international conference on computational intelligence and communication networks (CICN)*, Al-Khobar, Saudi Arabia, 4–6 December 2022. 2022. URL: https://doi.org/10.1109/cicn56167.2022.10008323 (date of access: 05.05.2025).

104. Enabling an anatomic view to investigate honeypot systems: a survey / W. Fan et al. *IEEE systems journal*. 2018. Vol. 12, no. 4. P. 3906–3919. URL: https://doi.org/10.1109/jsyst.2017.2762161 (date of access: 05.05.2025).

105. Enabling defensive deception by leveraging software defined networks / I. Belalis et al. *INTERNET 2020 the twelfth international conference on evolving internet*. P. 7–16. URL: https://hdl.handle.net/11250/2685618.

106. Enabling defensive deception in distributed system environments / N. Soule et al. *2016 resilience week (RWS)*, Chicago, IL, USA, 16–18 August 2016. 2016. P. 73–76. URL: https://doi.org/10.1109/rweek.2016.7573310 (date of access: 06.05.2025).

107. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits / A. Kashtalian et al. *Radioelectronic and computer systems*. 2025. Vol. 2025, no. 1. P. 264–297. URL: https://doi.org/10.32620/reks.2025.1.18 (date of access: 08.05.2025).

108. Evaluating deception and moving target defense with network attack simulation / D. Reti et al. *CCS '22: 2022 ACM SIGSAC conference on computer and communications security*, Los Angeles CA USA. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3560828.3564006 (date of access: 08.05.2025).

109. Fan W., Fernández D., Du Z. Adaptive and flexible virtual honeynet. *Mobile, secure, and programmable networking*. Cham, 2015. P. 1–17. URL: https://doi.org/10.1007/978-3-319-25744-0_1 (date of access: 06.05.2025).

110. Ferguson-Walter, K., Fugate, S., Mauger, J., & Major, M. Game theory for adaptive defensive cyber deception. 2019. DOI:10.1145/3314058.3314063.

111. *Fidelis Security*. URL: https://fidelissecurity.com/fidelis-elevate/ (дата звернення: 06.08.2023).

112. Fraunholz D., Zimmermann M., Schotten H. D. An adaptive honeypot configuration, deployment and maintenance strategy. *2017 19th international conference on advanced communication technology (ICACT)*, Pyeongchang, Kwangwoon Do, South Korea, 19–22 February 2017. 2017. URL: https://doi.org/10.23919/icact.2017.7890056 (date of access: 05.05.2025).

113. Han X., Kheir N., Balzarotti D. Evaluation of deception-based web attacks detection. *CCS '17: 2017 ACM SIGSAC conference on computer and communications security*, Dallas Texas USA. New York, NY, USA, 2017. URL: https://doi.org/10.1145/3140549.3140555 (date of access: 08.05.2025).

114. Han X., Kheir N., Balzarotti D. Deception techniques in computer security. *ACM computing surveys*. 2018. Vol. 51, no. 4. P. 1–36. URL: https://doi.org/10.1145/3214305 (date of access: 06.05.2025).

115. Hetzler C., Chen Z., Khan T. M. Analysis of SSH honeypot effectiveness. *Lecture notes in networks and systems*. Cham, 2023. P. 759–782. URL: https://doi.org/10.1007/978-3-031-28073-3_51 (date of access: 05.05.2025).

116. HoneyBug: personalized cyber deception for web applications / A. Niakanlahiji et al. *Hawaii international conference on system sciences*. 2020. URL: https://doi.org/10.24251/hicss.2020.233 (date of access: 06.05.2025).

117.30. HoneyDOC: an efficient honeypot architecture enabling all-round design / W. Fan et al. *IEEE journal on selected areas in communications*. 2019. Vol. 37, no. 3. P. 683–697. URL: https://doi.org/10.1109/jsac.2019.2894307 (date of access: 04.05.2025).

118. HoneyIoT: adaptive high-interaction honeypot for iot devices through reinforcement learning / C. Guan et al. *WiSec '23: 16th ACM conference on security and privacy in wireless and mobile networks*, Guildford United Kingdom. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3558482.3590195 (date of access: 05.05.2025).

119. HoneyMix: toward sdn-based intelligent honeynet / W. Han et al. *Proceedings of the 2016 ACM international workshop on security in software defined networks*, New Orleans. 2016. P. 1–6. URL: https://doi.org/10.1145/2876019.2876022.

120. HoneyProxy: Design and implementation of next-generation honeynet via SDN / S. Kyung et al. *2017 IEEE conference on communications and network security (CNS)*, Las Vegas, NV, 9–11 October 2017. 2017. URL: https://doi.org/10.1109/cns.2017.8228653 (date of access: 05.05.2025).

121. Honeypot allocation for cyber deception under uncertainty / A. H. Anwar et al. *IEEE transactions on network and service management*. 2022. P. 1. URL: https://doi.org/10.1109/tnsm.2022.3179965 (date of access: 25.04.2025).

122. Honeypot allocation for cyber deception in dynamic tactical networks: a game theoretic approach / M. A. Sayed et al. *Lecture notes in computer science*. Cham, 2023. P. 195–214. URL: https://doi.org/10.1007/978-3-031-50670-3_10 (date of access: 25.04.2025).

123. Honeypot and cyber deception as a tool for detecting cyber-attacks on critical infrastructure / D. Morozov et al. *CEUR workshop proceedings*. 2023. P. 81–96.

124. Honeypot-Based cyber deception against malicious reconnaissance via hypergame theory / A. H. Anwar et al. *GLOBECOM 2022 - 2022 IEEE global communications conference*, Rio de Janeiro, Brazil, 4–8 December 2022. 2022. P. 3393–3398. URL: https://doi.org/10.1109/globecom48099.2022.10000813 (date of access: 06.05.2025).

125. Honeypots deployment for the analysis and visualization of malware activity and malicious connections / I. Koniaris et al. *ICC 2014 - 2014 IEEE international conference on communications*, Sydney, NSW, 10–14 June 2014. 2014. URL: https://doi.org/10.1109/icc.2014.6883587 (date of access: 05.05.2025).

126. Honeypot-based intrusion detection system: a performance analysis / J. R. Kondra et al. *2016 3rd international conference on computing for sustainable global development (indiacom)*, New Delhi. 2016. P. 2347–2351.

127. HoneyVP: a cost-effective hybrid honeypot architecture for industrial control systems / J. You et al. *ICC 2021 - IEEE international conference on communications*, Montreal, QC, Canada, 14–23 June 2021. 2021. URL: https://doi.org/10.1109/icc42927.2021.9500567 (date of access: 04.05.2025).

128. Horák K., Zhu Q., Bošanský B. Manipulating adversary's belief: a dynamic game approach to deception by design for proactive network security. *Lecture notes in computer science*. Cham, 2017. P. 273–294. URL: https://doi.org/10.1007/978-3-319-68711-7_15 (date of access: 27.04.2025).

129. Hybrid cyber defense strategies using Honey-X: a survey / X. Qin et al. *Computer networks*. 2023. P. 109776. URL: https://doi.org/10.1016/j.comnet.2023.109776 (date of access: 04.05.2025).

130. Huang L., Zhu Q. Duplicity games for deception design with an application to insider threat mitigation. *IEEE transactions on information forensics and security*. 2021. Vol. 16. P. 4843–4856. URL: https://doi.org/10.1109/tifs.2021.3118886 (date of access: 25.04.2025).

131. Identification and classification of cyber threats through SSH honeypot systems / J. M. Jorquera Valero et al. *Handbook of research on intrusion detection systems*. 2020.

P. 105–129. URL: https://doi.org/10.4018/978-1-7998-2242-4.ch006 (date of access: 26.04.2025).

132. Identifying attack propagation patterns in honeypots using markov chains modeling and complex networks analysis / A. Bar et al. *2016 IEEE international conference on software science, technology and engineering (SWSTE)*, Beer Sheva, Israel, 23–24 June 2016. 2016. URL: https://doi.org/10.1109/swste.2016.13 (date of access: 08.05.2025).

133. Implementation of insider threat detection system using honeypot based sensors and threat analytics / M. M. Yamin et al. *Lecture notes in networks and systems*. Cham, 2019. P. 801–829. URL: https://doi.org/10.1007/978-3-030-12385-7_56 (date of access: 27.04.2025).

134. Implementation of a modern security systems honeypot Honey Network on wireless networks / H. Wafi et al. *2017 international young engineers forum (YEF-ECE)*, Almada, 5 May 2017. 2017. P. 91–96. URL: https://doi.org/10.1109/yef-ece.2017.7935647 (date of access: 06.05.2025).

135. Influence of network size on adversarial decisions in a deception game involving honeypots / H. Katakwar et al. *Frontiers in psychology*. 2020. Vol. 11. URL: https://doi.org/10.3389/fpsyg.2020.535803 (date of access: 06.05.2025).

136. Intelligent deception techniques against adversarial attack on the industrial system / S. Kumari et al. *International journal of intelligent systems*. 2021. Vol. 36, no. 5. P. 2412–2437. URL: https://doi.org/10.1002/int.22384 (date of access: 08.05.2025).

137. IoT honeypot: a review from researcher's perspective / M. F. Razali et al. *2018 IEEE conference on application, information and network security (AINS)*, Langkawi, Malaysia, 21–22 November 2018. 2018. URL: https://doi.org/10.1109/ains.2018.8631494 (date of access: 04.05.2025).

138. Islam M. M., Al-Shaer E. Active deception framework: an extensible development environment for adaptive cyber deception. *2020 IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 28–30 September 2020. 2020. P. 41–48. URL: https://doi.org/10.1109/secdev45635.2020.00023 (date of access: 06.05.2025).

139. Jay D. Deception technology based intrusion protection and detection mechanism for digital substations: A game theoretical approach. *IEEE access*. 2023. P. 1. URL: https://doi.org/10.1109/access.2023.3279504 (date of access: 04.05.2025).

140. Jiang K., Zheng H. Design and implementation of A machine learning enhanced web honeypot system. *2020 13th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI)*, Chengdu, China, 17–19 October 2020. 2020. P. 957–961. URL: https://doi.org/10.1109/cisp-bmei51763.2020.9263640 (date of access: 08.05.2025).

141. Joshi R.C., Sardana A. Science Honeypots. A new Paradigm to Information Security. *Publishers, P.O.* Box 699, Enfi eld, NH 03748, USA, 2011. – 323p. https://doi.org/10.1201/b10738 (date of access: 06.08.2023).

142. Juels A., Rivest R. L. Honeywords: making password-cracking detectable. Proceedings of the 2013 ACM SIGSAC conference on computer & communications security (CCS '13). association for computing machinery, New York. 2013. P. 145–160. URL: https://doi.org/10.1145/2508859.2516671.

143. Kaghazgaran P., Takabi H. Toward an insider threat detection framework using honey permissions. *Journal of internet services and information security (JISIS)*. Vol. 5, no. 3. P. 19–36. URL: https://isyou.info/jisis/vol5/no3/jisis-2015-vol5-no3-02.pdf.

144. Karpinski M., Kuznetsov O., Oliynykov R. Security, privacy, confidentiality, and trust in the blockchain: from theory to applications. *Electronics*. 2025. Vol. 14, no. 3. P. 581. URL: https://doi.org/10.3390/electronics14030581 (date of access: 10.05.2025).

145. Kashtalian A. Honeypots models in computer networks according to mailcious attacs types. *Proceedings of VII international conference "Information technology and interactions" (it&i-2020)*, Kyiv, 2–4 December 2020. P. 71–73. URL: http://iti.fit.univ.kiev.ua/wp-content/uploads/ITI_Satellite_2020_Conference-Proceedings.pdf.

146. Kashtalian A., Savenko O., Sachenko A. Agglomerative clustering of data collected by honeypots. 2021 11th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), Cracow, Poland, 22–25 September 2021. 2021. URL: https://doi.org/10.1109/idaacs53288.2021.9661027 (date of access: 10.05.2025).

147. Kashtalian A., Sochor T. K-Means clustering of honeynet data with unsupervised representation learning. International workshop on intelligent information

technologies & systems of information security. CEUR workshop proceedings. vol. 2853. 2021. P. 539–549. URL: https://ceur-ws.org/Vol-2853/paper48.pdf.

148. Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems, *Cryptography*, 2022, vol. 6, no. 44. DOI:10.3390/cryptography6030044.

149. Kharchenko, V. CONCEPTUAL FUNDAMENTALS OF DEPENDABLE ARTIFICIAL INTELLIGENCE SYSTEMS. *Reports of the National Academy of Sciences of Ukraine*. 2025.№ 2, Pp. 11–23. https://doi.org/10.15407/dopovidi2025.02.011

150. Kechao L., Xinli X. OpenHIP random host hopping in network layer. *International conference on education, management and information technology (ICEMIT 2019)*. 2019. P. 300–309. URL: https://webofproceedings.org/proceedings_series/ESSP/ICEMIT%202019/ICEMIT19048.pdf.

151. Khoroshko V., Khokhlachova Y., Vyshnevska N. Decomposition of computer network technology in their design. *Ukrainian scientific journal of information security*. 2023. Vol. 29, no. 3. P. 130–137. URL: https://doi.org/10.18372/2225-5036.29.18072.

152. Khoroshko V., Khokhlachova Y., Vyshnevska N. Choice of indicators for forecasting cyber protection of computer systems. *Ukrainian scientific journal of information security*. 2023. Vol. 29, no. 1. P. 41–47.

153. Kumar S., Janet B., Eswari R. Multi platform honeypot for generation of cyber threat intelligence. *2019 IEEE 9th international conference on advanced computing (IACC)*, Tiruchirappalli, India, 13–14 December 2019. 2019. URL: https://doi.org/10.1109/iacc48062.2019.8971584 (date of access: 04.05.2025).

154. Kilinc H. H., Acar O. F. Analysis of attack and attackers on VoIP Honeypot environment. *2018 26th signal processing and communications applications conference (SIU)*, Izmir, Turkey, 2–5 May 2018. 2018. URL: https://doi.org/10.1109/siu.2018.8404331 (date of access: 05.05.2025).

155. Komar, M., Sachenko, A., Golovko, V., Dorosh, V. Compression of Network Traffic Parameters for Detecting Cyber Attacks Based on Deep Learning, *Proceedings of*

the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2018), Kyiv, Ukraine, 2018 (pp. 44-48).

156. *Labyrinth Deception Platform*. URL: https://labyrinth.tech/platform (дата звернення: 06.08.2023).

157. Leveraging computational intelligence techniques for defensive deception: a review, recent advances, open problems and future directions / P. V. Mohan et al. *Sensors*. 2022. Vol. 22, no. 6. P. 2194. URL: https://doi.org/10.3390/s22062194 (date of access: 08.05.2025).

158. Letychevskyi O., Peschanenko V. Applying algebraic virtual machine to cybersecurity tasks. *2022 IEEE 9th international conference on sciences of electronics, technologies of information and telecommunications (SETIT)*, Hammamet, Tunisia, 28–30 May 2022. 2022. URL: https://doi.org/10.1109/setit54465.2022.9875895 (date of access: 10.05.2025).

159. Lightweight on-demand honeypot deployment for cyber deception / J. C. Acosta et al. *Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering*. Cham, 2022. P. 294–312. URL: https://doi.org/10.1007/978-3-031-06365-7_18 (date of access: 06.05.2025).

160. Li Y., Shi L., Feng H. A game-theoretic analysis for distributed honeypots. *Future internet*. 2019. Vol. 11, no. 3. P. 65. URL: https://doi.org/10.3390/fi11030065 (date of access: 27.04.2025).

161. Lobanchykova N., Pilkevychb I., Korchenko O. Analysis of attacks on components of IoT systems and cybersecurity technologies. *QuaInT+ doors, CEUR-WS*. 2021. Vol. 2850. P. 83–96. URL: https://ceur-ws.org/Vol-2850/paper6.pdf.

162. López P. B., Pérez M. G., Nespoli P. Cyber deception: state of the art, trends and open challenges. 2024. URL: https://doi.org/10.48550/arXiv.2409.07194.

163. Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. *Communications in Computer and Information Science*. 2019. Vol. 1039. PP. 127-143, ISSN: 1865-0929.

164. Malware detection by distributed systems with partial centralization / B. Savenko et al. 2023 IEEE 12th international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), Dortmund, Germany, 7–9 September 2023. 2023. P. 265–270. URL: https://doi.org/10.1109/idaacs58523.2023.10348773 (date of access: 10.05.2025).

165. Malware detection tool based on emulator state analysis / P. Rehida et al. 2023 IEEE 12th international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), Dortmund, Germany, 7–9 September 2023. 2023. P. 135–140. URL: https://doi.org/10.1109/idaacs58523.2023.10348678 (date of access: 10.05.2025).

166. Matin I. M. M., Rahardjo B. Malware detection using honeypot and machine learning. *7th international conference on cyber and IT service management (CITSM)*, Jakarta. 2019. P. 1–4. URL: https://doi.org/10.1109/CITSM47753.2019.8965419.

167. Mathematical model for heterogeneous databases parameters estimation in distributed systems with dynamic structure / V. Mukhin et al. *2020 IEEE 2nd international conference on advanced trends in information theory (ATIT)*, Kyiv, Ukraine, 25–27 November 2020. 2020. P. 158–161. URL: https://doi.org/10.1109/atit50783.2020.9349331 (date of access: 10.05.2025).

168. Measuring the effectiveness of network deception / S. Sugrim et al. *2018 IEEE international conference on intelligence and security informatics (ISI)*, Miami, FL, 9–11 November 2018. 2018. P. 142–147. URL: https://doi.org/10.1109/isi.2018.8587326 (date of access: 06.05.2025).

169. Mehresh R., Upadhyaya S. J. Deception-Based survivability. *Secure system design and trustable computing*. Cham, 2016. P. 521–537. URL: https://doi.org/10.1007/978-3-319-14971-4_17 (date of access: 06.05.2025).

170. Method and rules for determining the next centralization option in multicomputer system architecture / A. Kashtalian et al. *International journal of computing*. 2025. Vol. 24(1). P. 35–51. URL: https://doi.org/10.47839/ijc.24.1.3875 (date of access: 08.05.2025).

171. Method for detecting steganographic changes in images using machine learning / D. Denysiuk et al. *2023 13th international conference on dependable systems, services and*

technologies (DESSERT), Athens, Greece, 13–15 October 2023. 2023. P. 1–6. URL: https://doi.org/10.1109/dessert61349.2023.10416453 (date of access: 10.05.2025).

172. Methods for detecting software implants in corporate networks / D. Denysiuk et al. *CEUR workshop proceedings*. 2024. Vol. 3675. P. 270–284. URL: https://ceur-ws.org/Vol-3675/paper20.pdf.

173. Method for detecting malicious commands transmitted via images using steganography/ D. Denysiuk et al. CEUR workshop proceedings. 2025. Vol. 3963. P. 340–350. URL: https://ceur-ws.org/Vol-3963/paper27.pdf

174. Mimic defense: a designed-in cybersecurity defense framework / H. Hu et al. *IET information security*. 2018. Vol. 12, no. 3. P. 226–237. URL: https://doi.org/10.1049/iet-ifs.2017.0086 (date of access: 04.05.2025).

175. Model-driven deception for control system environments / W. Hofer et al. *2019 IEEE international symposium on technologies for homeland security (HST)*, Woburn, MA, USA, 5–6 November 2019. 2019. URL: https://doi.org/10.1109/hst47167.2019.9032927 (date of access: 04.05.2025).

176. Mohammadzadeh H. A survey on dynamic honeypots. *International journal of information and electronics engineering*. 2012. URL: https://doi.org/10.7763/ijiee.2012.v2.89 (date of access: 27.04.2025).

177. Mohssen M. Honeypots and Routers: Collecting Internet Attacks/ Mohssen Mohammed, Habib-ur Rehman – CRC Press, *Taylor & Francis Group LLC*, 2016. - 197p.

178. Moreira A., Amaral V., De Faveri C. Goal-Driven deception tactics design. *2016 IEEE 27th international symposium on software reliability engineering (ISSRE)*, Ottawa, ON, 23–27 October 2016. 2016. P. 264–275. URL: https://doi.org/10.1109/issre.2016.44 (date of access: 08.05.2025).

179. Moskalenko, V., Kharchenko, V., Moskalenko, A., & Kuzikov, B. Resilience and resilient systems of artificial intelligence: Taxonomy, models and methods, *Algorithms*, 2023, vol. 16, 165. DOI: 10.3390/a16030165.

180. Mphago B. Deception in web application honeypots: case of glastopf. *International journal of cyber-security and digital forensics*. 2017. Vol. 6, no. 4. P. 179–185. URL: https://doi.org/10.17781/p002304 (date of access: 04.05.2025).

181. MTDCD: an MTD enhanced cyber deception defense system / C. Gao et al. *2021 IEEE 4th advanced information management, communicates, electronic and automation control conference (IMCEC)*, Chongqing, China, 18–20 June 2021. 2021. URL: https://doi.org/10.1109/imcec51613.2021.9482133 (date of access: 06.05.2025).

182. Muhamad Malik Matin, Iik & Rahardjo, Budi. (2019). Malware Detection Using Honeypot and Machine Learning. 1-4. 10.1109/CITSM47753.2019.8965419. – без номера

183. Mukhin V., Kornaga Y., Zavgorodnii V., Bazaka Y., Zavgorodnya A., Mukhin O., Method of Data Processing System Synthesis for Heterogeneous Distributed Databases Based on Network-Centric Control. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, pp. 607-612, URL: https://doi.org/ 10.1109/IDAACS58523.2023.10348667.

184. Mukti F. S., Sukmawan R. M. Integration of low interaction honeypot and ELK stack as attack detection systems on servers. *Jurnal penelitian pos dan informatika*. 2021. Vol. 11, no. 1. URL: https://doi.org/10.17933/jppi.v11i1.336 (date of access: 27.04.2025).

185. Mudgal A., Bhatia S. Big data with machine learning enabled intrusion detection with honeypot intelligence system on apache Flink (BDML-IDHIS). *Journal of computer virology and hacking techniques*. 2025. Vol. 21, no. 1. URL: https://doi.org/10.1007/s11416-024-00545-x (date of access: 08.05.2025).

186. Multi-computer malware detection systems with metamorphic functionality / A. Kashtalian et al. *Radioelectronic and computer systems*. 2024. Vol. 2024, no. 1. P. 152–175. URL: https://doi.org/10.32620/reks.2024.1.13 (date of access: 08.05.2025).

187. Nassar M., State R., Festor O. VoIP honeypot architecture. *2007 10th IFIP/IEEE international symposium on integrated network management*, Munich, Germany, 21–25 May 2007. 2007. URL: https://doi.org/10.1109/inm.2007.374775 (date of access: 05.05.2025).

188. Nasr M., Zolfaghari H., Houmansadr A. The waterfall of liberty: decoy routing circumvention that resists routing attacks. *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*. 2017. URL: https://dl.acm.org/doi/pdf/10.1145/3133956.3134075.

189. Qasem M., Almohri H. M. J. An efficient deception architecture for cloud-based virtual networks. 2020. URL: https://doi.org/10.48550/arXiv.2004.06933.

190. Onaolapo J., Mariconti E., Stringhini G. What happens after you are pwnd: understanding the use of leaked webmail credentials in the wild. *Proceedings of the 2016 internet measurement conference (IMC '16)*, New York. 2016. P. 65–79. URL: https://doi.org/10.1145/2987443.2987475.

191. On defensive cyber deception: A case study using SDN / C.-Y. J. Chiang et al. *MILCOM 2018 - 2018 IEEE military communications conference (MILCOM)*, Los Angeles. 2018. P. 110–115. URL: https://doi.org/10.1109/MILCOM.2018.8599755.

192. Online cyber deception system using partially observable monte-carlo planning framework / M. A. R. A. Amin et al. *Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering*. Cham, 2019. P. 205–223. URL: https://doi.org/10.1007/978-3-030-37231-6_11 (date of access: 08.05.2025).

193. Optimally blending honeypots into production networks: hardness and algorithms / M. M. U. Zaman et al. *Science of cyber security*. Cham, 2023. P. 285–304. URL: https://doi.org/10.1007/978-3-031-45933-7_17 (date of access: 08.05.2025).

194. Optimal network security hardening using attack graph games / K. Durkota et al. *Intl. joint conf. on artificial intelligence*. P. 526–532. URL: https://dl.acm.org/doi/10.5555/2832249.2832322.

195. Papazis K., Chilamkurti N. Detecting indicators of deception in emulated monitoring systems. *Service oriented computing and applications*. 2019. Vol. 13, no. 1. P. 17–29. URL: https://doi.org/10.1007/s11761-018-0252-2 (date of access: 05.05.2025).

196. Patil L., Desai S., Singh A. Honeypot based secure network system. *International research journal of engineering and technology (IRJET)*. 2021. Vol. 8, no. 3. P. 2014–2016.

197. Pawlick J., Colbert E., Zhu Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM computing surveys*. 2019. Vol. 52, no. 4. P. 1–28. URL: https://doi.org/10.1145/3337772 (date of access: 27.04.2025).

198. Pingree L. Emerging technology analysis : deception techniques and technologies create security technology business opportunities. URL: https://api.semanticscholar.org/CorpusID:53491340 (date of access: 27.04.2025).

199. Podhradsky A. L., Casey C., Ceretti P. The Bluetooth honeypot project. *2012 wireless telecommunications symposium (WTS 2012)*, London, United Kingdom, 18–20 April 2012. 2012. URL: https://doi.org/10.1109/wts.2012.6266078 (date of access: 05.05.2025).

200. Prathapani A., Santhanam L., Agrawal D. P. Intelligent honeypot agent for blackhole attack detection in Wireless Mesh Networks. *2009 IEEE 6th international conference on mobile adhoc and sensor systems (MASS)*, Macau, China, 12–15 October 2009. 2009. P. 753–758. URL: https://doi.org/10.1109/mobhoc.2009.5336925 (date of access: 08.05.2025).

201. Principle and method of deception systems synthesizing for malware and computer attacks detection / A. Kashtalian et al. *Radioelectronic and computer systems*. 2023. No. 4. P. 112–151. URL: https://doi.org/10.32620/reks.2023.4.10 (date of access: 08.05.2025).

202. Priya V. S. D., Chakkaravarthy S. S. Containerized cloud-based honeypot deception for tracking attackers. *Scientific reports*. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-28613-0 (date of access: 04.05.2025).

203. Prodeus M., Nicheporuk A., Kashtalian A., Kapustian M., Sochor T. Honeypot-based monitoring, detection, response, and information protection framework. *Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 329-339. URL: https://ceur-ws.org/Vol-3963/paper26.pdf

204. Proof-of-Activity consensus protocol based on a network's active nodes / R. Belfer et al. *CEUR-WS*. 2020. Vol. 2623. P. 239–251. URL: https://ceur-ws.org/Vol-2623/paper21.pdf.

205. Proof: pre-training model of malware family classification based on active defense / S. Guo et al. *IEEE transactions on sustainable computing*. 2025. P. 1–12. URL: https://doi.org/10.1109/tsusc.2025.3529752 (date of access: 08.05.2025).

206. *Proofpoint Identity Threat Defense*. URL: https://www.proofpoint.com/us/illusive-is-now-proofpoint (date of access: 06.08.2023).

207. Pour M. S., Khoury J., Bou-Harb E. HoneyComb: a darknet-centric proactive deception technique for curating iot malware forensic artifacts. *NOMS 2022-2022*

IEEE/IFIP network operations and management symposium, Budapest. 2022. P. 1–9. URL: https://doi.org/10.1109/NOMS54207.2022.9789827.

208. Random host and service multiplexing for moving target defense in software-defined networks / D. P. Sharma et al. *ICC 2019 - 2019 IEEE international conference on communications (ICC)*, Shanghai, China, 20–24 May 2019. 2019. URL: https://doi.org/10.1109/icc.2019.8761496 (date of access: 05.05.2025).

209. Ravi A., Sharma B., Mukherjee A. A cloud-native honeynet automation and orchestration framework. 2023. URL: https://doi.org/10.31219/osf.io/xkqzr.

210. Resilience and resilient systems of artificial intelligence: taxonomy, models and methods / V. Moskalenko et al. *Algorithms*. 2023. Vol. 16, no. 3. P. 165. URL: https://doi.org/10.3390/a16030165 (date of access: 10.05.2025).

211. Rethinking the honeypot for cyber-physical systems / S. Litchfield et al. *IEEE internet computing*. 2016. Vol. 20, no. 5. P. 9–17. URL: https://doi.org/10.1109/mic.2016.103 (date of access: 05.05.2025).

212. Rowe N. C. Honeypot deception tactics. *Autonomous cyber deception*. Cham, 2019. P. 35–45. URL: https://doi.org/10.1007/978-3-030-02110-8_3 (date of access: 26.04.2025).

213. Rrushi J. Cyber deception engineering. *Encyclopedia of cryptography, security and privacy*. Berlin, Heidelberg, 2023. P. 1–4. URL: https://doi.org/10.1007/978-3-642-27739-9_1790-1 (date of access: 04.05.2025).

214. Rrushi J. L. NIC displays to thwart malware attacks mounted from within the OS. *Computers & security*. 2016. Vol. 61. P. 59–71. URL: https://doi.org/10.1016/j.cose.2016.05.002 (date of access: 27.04.2025).

215. Sadasivam G. K., Hota C. Scalable honeypot architecture for identifying malicious network activities. *2015 international conference on emerging information technology and engineering solutions (EITES)*, Mahashtra, India, 20–21 February 2015. 2015. URL: https://doi.org/10.1109/eites.2015.15 (date of access: 04.05.2025).

216. Sandnet: towards high quality of deception in container-based microservice architectures / A. Osman et al. *ICC 2019 - 2019 IEEE international conference on communications (ICC)*, Shanghai, China, 20–24 May 2019. 2019. URL: https://doi.org/10.1109/icc.2019.8761171 (date of access: 04.05.2025).

217. Saputro E. D., Purwanto Y., Ruriawan M. F. Medium interaction honeypot infrastructure on the internet of things. *2020 IEEE international conference on internet of things and intelligence system (iotais)*, BALI, Indonesia, 27–28 January 2021. 2021. URL: https://doi.org/10.1109/iotais50849.2021.9359711 (date of access: 05.05.2025).

218. Saravanan T., Saravanakumar S. Privacy preserving using enhanced shadow honeypot technique for data retrieval in cloud computing. *2021 3rd international conference on advances in computing, communication control and networking (ICAC3N)*, Greater Noida, India, 17–18 December 2021. 2021. URL: https://doi.org/10.1109/icac3n53548.2021.9725712 (date of access: 05.05.2025).

219. Saud Z., Islam M. H. Towards proactive detection of advanced persistent threat (APT) attacks using honeypots. *SIN '15: the 8th international conference on security of information and networks*, Sochi Russia. New York, NY, USA, 2015. URL: https://doi.org/10.1145/2799979.2800042 (date of access: 06.05.2025).

220. Secure cyber deception architecture and decoy injection to mitigate the insider threat / K. Park et al. *Symmetry*. 2018. Vol. 10, no. 1. P. 14. URL: https://doi.org/10.3390/sym10010014 (date of access: 04.05.2025).

221. Security and availability models for smart building automation systems / V. Kharchenko et al. *International journal of computing*. 2017. Vol. 16(4). P. 194–202. URL: https://doi.org/10.47839/ijc.16.4.907 (date of access: 10.05.2025).

222. Selvaraj R., Kuthadi V. M., Marwala T. Honey pot: a major technique for intrusion detection. *Advances in intelligent systems and computing*. New Delhi, 2015. P. 73–82. URL: https://doi.org/10.1007/978-81-322-2523-2_7 (date of access: 05.05.2025).

223. *SentinelOne*. URL: https://www.sentinelone.com/surfaces/identity/ (date of access: 06.08.2023).

224. Seo S., Kim D. IoDM: a study on a iot-based organizational deception modeling with adaptive general-sum game competition. *Electronics*. 2022. Vol. 11, no. 10. P. 1623. URL: https://doi.org/10.3390/electronics11101623 (date of access: 06.05.2025).

225. Sever D., Kisasondi T. Efficiency and security of docker based honeypot systems. *2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO)*, Opatija, 21–25 May 2018. 2018. URL: https://doi.org/10.23919/mipro.2018.8400212 (date of access: 05.05.2025).

226. Schindler S., Schnor B., Scheffler T. Hyhoneydv6: a hybrid honeypot architecture for ipv6 networks. *International journal of intelligent computing research*. 2015. Vol. 6, no. 2. P. 562–570. URL: https://doi.org/10.20533/ijicr.2042.4655.2015.0071 (date of access: 04.05.2025).

227. SDN-Based cyber deception deployment for proactive defense strategy using honey of things and cyber threat intelligence / N. H. Khoa et al. *Intelligence of things: technologies and applications*. Cham, 2023. P. 269–278. URL: https://doi.org/10.1007/978-3-031-46749-3_26 (date of access: 06.05.2025).

228. Self-Organized distributed anomaly detection system in computer systems based on the principal components method / B. Savenko et al. *CEUR workshop proceedings*. 2022. Vol. 3156. P. 329–351. URL: https://ceur-ws.org/Vol-3156/paper25.pdf

229. Sharma S., Kaul A. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. *Vehicular communications*. 2018. Vol. 12. P. 138–164. URL: https://doi.org/10.1016/j.vehcom.2018.04.005 (date of access: 06.05.2025).

230. Shimanaka T., Masuoka R., Hay B. Cyber deception architecture: covert attack reconnaissance using a safe SDN approach. *Hawaii international conference on system sciences*. 2019. URL: https://doi.org/10.24251/hicss.2019.876 (date of access: 06.05.2025).

231. Shinde A., Doshi P., Setayeshfar O. Cyber attack intent recognition and active deception using factored interactive pomdps. *Proceedings of the 20th international conference on autonomous agents and multiagent systems (AAMAS '21)*. Richland, SC, 2021. P. 1200–1208.

232. Shukla R., Singh M. PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems. *2014 3rd international conference on reliability, infocom technologies and optimization (ICRITO) (trends and future directions)*, Noida, India, 8–10 October 2014. 2014. URL: https://doi.org/10.1109/icrito.2014.7014753 (date of access: 04.05.2025).

233. Shokri R. Privacy games: optimal user-centric data obfuscation. *Proceedings on privacy enhancing technologies*. 2015. Vol. 2015, no. 2. P. 299–315. URL: https://doi.org/10.1515/popets-2015-0024 (date of access: 27.04.2025).

234. Sochor T., Zuzcak M. High-Interaction linux honeypot architecture in recent perspective. *Computer networks*. Cham, 2016. P. 118–131. URL: https://doi.org/10.1007/978-3-319-39207-3_11 (date of access: 04.05.2025).

235. SODA: a system for cyber deception orchestration and automation / M. S. I. Sajid et al. *ACSAC '21: annual computer security applications conference*, Virtual Event USA. New York, NY, USA, 2021. URL: https://doi.org/10.1145/3485832.3485918 (date of access: 04.05.2025).

236. Sri Latha P., Prasanth Vaidya S. Multi-purpose web application honeypot to detect multiple types of attacks and expose the attacker's identity. *Computational vision and bio-inspired computing*. Singapore, 2022. P. 279–287. URL: https://doi.org/10.1007/978-981-16-9573-5_21 (date of access: 05.05.2025).

237. Steingartner W., Galinec D., Kozina A. Threat defense: cyber deception approach and education for resilience in hybrid threats model. *Symmetry*. 2021. Vol. 13, no. 4. P. 597. URL: https://doi.org/10.3390/sym13040597 (date of access: 27.04.2025).

238. Strategic honeypot game model for distributed denial of service attacks in the smart grid / K. Wang et al. *IEEE transactions on smart grid*. 2017. Vol. 8, no. 5. P. 2474–2482. URL: https://doi.org/10.1109/tsg.2017.2670144 (date of access: 27.04.2025).

239. Surber J. G., Zantua M. Intelligent interaction honeypots for threat hunting within the internet of things. *Journal of the colloquium for information systems security education*. 2022. Vol. 9, no. 1. P. 5. URL: https://doi.org/10.53735/cisse.v9i1.147 (date of access: 06.05.2025).

240. Survey of cyber moving targets second edition / B. C. Ward et al. 2018. URL: https://api.semanticscholar.org/CorpusID:70305693.

241. Survey of contemporary open-source honeypots, frameworks, and tools / N. Ilg et al. *Journal of network and computer applications*. 2023. P. 103737. URL: https://doi.org/10.1016/j.jnca.2023.103737 (date of access: 04.05.2025).

242. Sutharsan M., Logeshwaran J. Design intelligence data gathering and incident response model for data security using honey pot system. *International journal for research & development in technology*. 2016. Vol. 5, no. 5. P. 310–314.

243. Svanadze V., Gnatyuk S. Challenges and solutions for cybersecurity and information security management in organizations. *CEUR-WS*. 2024. Vol. 3654. P. 497–504. URL: https://ceur-ws.org/Vol-3654/short20.pdf.

244. Tamas K. Lengyel, Justin Neumann, Steve Maresca, Bryan D. Payne, and Aggelos Kiayias. 2012. Virtual machine introspection in a hybrid honeypot architecture. In Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test (CSET'12). USENIX Association, USA, 5.

245. Taxonomy and survey of collaborative intrusion detection / E. Vasilomanolakis et al. *ACM computing surveys*. 2015. Vol. 47, no. 4. P. 1–33. URL: https://doi.org/10.1145/2716260 (date of access: 06.05.2025).

246. Technologies to enable cyber deception / V. E. Urias et al. *2017 international carnahan conference on security technology (ICCST)*, Madrid, 23–26 October 2017. 2017. URL: https://doi.org/10.1109/ccst.2017.8167793 (date of access: 04.05.2025).

247. Thonnard O., Dacier M. A framework for attack patterns' discovery in honeynet data. *Digital investigation*. 2008. Vol. 5. P. 128–139. URL: https://doi.org/10.1016/j.diin.2008.05.012 (date of access: 08.05.2025).

248. Titarmare N., Hargule N., Gupta A. An overview of honeypot systems. *International journal of computer sciences and engineering*. 2019. Vol. 7, no. 2. P. 394–397.

249. Tounsi W. Cyber deception, the ultimate piece of a defensive strategy - proof of concept. *2022 6th cyber security in networking conference (csnet)*, Rio de Janeiro, Brazil, 24–26 October 2022. 2022. URL: https://doi.org/10.1109/csnet56116.2022.9955605 (date of access: 04.05.2025).

250. Towards intelligent cyber deception systems / F. De Gaspari et al. *Autonomous cyber deception*. Cham, 2019. P. 21–33. URL: https://doi.org/10.1007/978-3-030-02110-8_2 (date of access: 06.05.2025).

251. Towards self-adaptive cyber deception for defense / J. Landsborough et al. *Hawaii international conference on system sciences*. 2021. URL: https://doi.org/10.24251/hicss.2021.244 (date of access: 05.05.2025).

252. Trassare S. T. A technique for presenting a deceptive dynamic network topology. 2013. URL: http://hdl.handle.net/10945/32911 (date of access: 06.05.2025).

253. *The Commvault Data Protection Platform*. URL: https://www.commvault.com/ (дата звернення: 06.08.2023).

254. Two-layer deception model based on signaling games against cyber attacks on cyber-physical systems. / P. C. Kamdem et al. *IEEE access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3478808 (date of access: 05.05.2025).

255. Underbrink A. J. Effective cyber deception. *Cyber deception*. Cham, 2016. P. 115–147. URL: https://doi.org/10.1007/978-3-319-32699-3_6 (date of access: 04.05.2025).

256. Valeros V., Rigaki M., Garcia S. Attacker profiling through analysis of attack patterns in geographically distributed honeypots. 2023. URL: https://doi.org/10.48550/arXiv.2305.01346 (date of access: 08.05.2025).

257. Viola V. From honeypots to distributed deception platforms: theory and testing of emerging technologies for IT security. 2019. URL: https://api.semanticscholar.org/CorpusID:226826721.

258. Virtual machine introspection in a hybrid honeypot architecture / T. K. Lengyel et al. Proceedings of the 5th USENIX conference on cyber security experimentation and test (CSET'12), USENIX association. 2012. P. 5.

259. Virtual USB honeypot / R. B. Yehuda et al. *SYSTOR '19: the 12th ACM international systems and storage conference*, Haifa Israel. New York, NY, USA, 2019. URL: https://doi.org/10.1145/3319647.3325843 (date of access: 05.05.2025).

260. Wang M., Santillan J., Kuipers F. ThingPot: an interactive Internet-of-Things honeypot. 2018. URL: https://doi.org/10.48550/arXiv.1807.04114.

261. Webb S., Caverlee J., Pu C. Social honeypots: making friends with a spammer near you. *International conference on email and anti-spam*. 2008. URL: https://api.semanticscholar.org/CorpusID:55307 (date of access: 08.05.2025).

262. Wegerer M., Tjoa S. Defeating the database adversary using deception - A mysql database honeypot. *2016 international conference on software security and assurance (ICSSA)*, St. Pölten, Austria, 24–25 August 2016. 2016. URL: https://doi.org/10.1109/icssa.2016.8 (date of access: 04.05.2025).

263. Wang H., Wu B. SDN-based hybrid honeypot for attack capture. *2019 IEEE 3rd information technology, networking, electronic and automation control conference*

(ITNEC), Chengdu, China, 15–17 March 2019. 2019. URL: https://doi.org/10.1109/itnec.2019.8729425 (date of access: 06.05.2025).

264. Walter E. C., Ferguson-Walter K. J., Ridley A. D. Incorporating deception into cyberbattlesim for autonomous defense. 2021. URL: https://doi.org/10.48550/arXiv.2108.13980.

265. Xiao F., Chen E., Xu Q. S7commTrace: A high interactive honeypot for industrial control system based on S7 protocol. *Information and communications security*. Cham, 2018. P. 412–423. URL: https://doi.org/10.1007/978-3-319-89500-0_36 (date of access: 05.05.2025).

266. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Prokopenko, O., Sievierinov, O., & Chopenko, D. Development of a concept for building a critical infrastructure facilities security system, *Eastern-European Journal of Enterprise Technologies*, 2021, vol. 3, pp. 63–83. DOI:10.15587/1729-4061.2021.233533

267. Yu T., Xin Y., Zhang C. HoneyFactory: container-based comprehensive cyber deception honeynet architecture. *Electronics*. 2024. Vol. 13, no. 2. P. 361. URL: https://doi.org/10.3390/electronics13020361 (date of access: 06.05.2025).

268. Zemene M. S., Avadhani P. S. Implementing high interaction honeypot to study SSH attacks. *2015 international conference on advances in computing, communications and informatics (ICACCI)*, Kochi, India, 10–13 August 2015. 2015. URL: https://doi.org/10.1109/icacci.2015.7275895 (date of access: 05.05.2025).

269. Zhang L., Thing V. L. L. Three decades of deception techniques in active cyber defense - Retrospect and outlook. *Computers & security*. 2021. Vol. 106. P. 102288. URL: https://doi.org/10.1016/j.cose.2021.102288 (date of access: 06.05.2025).

270. Zhuo Z., Wang C., Zhao S. Cyber deception for computer and network security: survey and challenges. 2020. URL: https://doi.org/10.48550/arXiv.2007.14497.

271. Zielinski D., Kholidy H. A. An analysis of honeypots and their impact as a cyber deception tactic. 2022. URL: https://doi.org/10.48550/arXiv.2301.00045.

272. Zobal L., Kolar D., Fujdiak R. Current state of honeypots and deception strategies in cybersecurity. *2019 11th international congress on ultra modern telecommunications and control systems and workshops (ICUMT)*, Dublin, Ireland, 28–30

October 2019. 2019. URL: https://doi.org/10.1109/icumt48472.2019.8970921 (date of access: 04.05.2025).

273. ДСТУ ISO/IEC 2382:2017. Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT). Вид. офіц.

274. ДСТУ ISO/IEC 25001:2016. Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Планування та керування (ISO/IEC 25001:2014, IDT). Вид. офіц.

275. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Вид. офіц.

276. ДСТУ ISO/IEC TR 24774:2016. Інженерія систем і програмних засобів. Керування життєвим циклом. Настанови щодо опису процесу (ISO/IEC TR 24774:2010, IDT). Вид. офіц.

277. ДСТУ ISO/IEC 15026-4:2018. Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 4. Гарантування в життєвому циклі (ISO/IEC 15026-4:2012, IDT). Вид. офіц.

278. ДСТУ ISO/IEC 15026-3:2018. Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 3. Рівні цілісності системи (ISO/IEC 15026-3:2015, IDT). Вид. офіц.

279. ДСТУ ISO/IEC/IEEE 16326:2015. Розроблення систем та програмного забезпечення. Процеси життєвого циклу. Керування проектами (ISO/IEC/IEEE 16326:2009, IDT). Вид. офіц.

280. ДСТУ ISO/IEC 15026-2:2018. Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 2. Сценарій гарантування (ISO/IEC 15026-2:2011, IDT). Вид. офіц.

281. ДСТУ ISO/IEC 16085:2016. Інженерія систем і програмних засобів. Процеси життєвого циклу. Керування ризиками (ISO/IEC 16085:2006, IDT). Вид. офіц.

282. ДСТУ ISO/IEC 27034-1:2017. Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT). Вид. офіц.

283. ДСТУ ISO/IEC 30111:2016. Інформаційні технології. Методи захисту. Процеси оброблення вразливостей (ISO/IEC 30111:2013, IDT). Вид. офіц.

284. ДСТУ ISO/IEC 33001:2016. Інформаційні технології. Оцінювання процесу. Поняття та термінологія (ISO/IEC 33001:2015, IDT). Вид. офіц.

285. Дудикевич В., Микитин Г., Ребець А. Квінтесенція інформаційної безпеки кіберфізичної системи. *Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі*. 2018. № 887. С. 58–68.

286. Каштальян А. С. МЕТОД ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК МУЛЬТИКОМП'ЮТЕРНИМИ СИСТЕМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК. *Herald of Khmelnytskyi National University. Technical Sciences*, 2025, № *349*(2), С. 346-352. https://doi.org/10.31891/2307-5732-2025-349-50

287. Каштальян А. Методи організації функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток в корпоративних мережах. *Measuring and computing devices in technological processes*. 2025. № 1. С. 160–171. URL: https://doi.org/10.31891/2219-9365-2025-81-19

288. Каштальян А. Мультикомп'ютерна система з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп'ютерних атак на основі мультиагентних технологій. *Herald of Khmelnytskyi National University. Technical sciences*. 2025. Т. 347, № 1. С. 535–542. URL: https://doi.org/10.31891/2307-5732-2025-347-73

289. Каштальян А. Концептуальна модель архітектури мультикомп'ютерних систем із приманками та пастками для виявлення та протидії зловмисному програмному забезпеченню та комп'ютерним атакам. *Information technology: computer science, software engineering and cyber security*. 2023. № 3. С. 22–31. URL: https://doi.org/10.32782/it/2023-3-3

290. Каштальян А. Критерій оперативності щодо варіантів централізації в архітектурі мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп'ютерних атак. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Т. 345, № 6(2). С. 172–178. URL: https://doi.org/10.31891/2307-5732-2024-345-6-26

291. Каштальян А. Особливості правил формування варіантів централізації для мультикомп’ютерних систем в корпоративних мережах. *Measuring and computing devices in technological processes*. 2024. № 4. С. 386–393. URL: https://doi.org/10.31891/2219-9365-2024-80-46

292. Каштальян А. Принцип синтезу мультикомп’ютерних систем з комбінованих антивірусних приманок і пасток та контролеру прийняття рішень для виявлення зловмисного програмного забезпечення та комп’ютерних атак. *Measuring and computing devices in technological processes*. 2023. № 4. С. 265–272. URL: https://doi.org/10.31891/2219-9365-2023-76-35

293. Каштальян А. Характерні властивості централізації в архітектурі мультикомп’ютерних систем антивірусних комбінованих приманок і пасток. *Information technology: computer science, software engineering and cyber security*. 2024. № 4. С. 114–124. URL: https://doi.org/10.32782/it/2024-4-14

294. Каштальян А.С., Авсієвич В.Р., Нічепорук А.О., Савенко О.С. А. с. 124518, Україна. Комп'ютерна програма «Проміжне програмне забезпечення мультикомп’ютерних систем спеціалізованого призначення». Дата реєстрації 11.03.2024.

295. Каштальян А., Любінецький Д. Розподілена самоорганізована система прогнозування зловмисної активності в комп’ютерних мережах. *Measuring and computing devices in technological processes*. 2022. № 4. С. 49–57. URL: https://doi.org/10.31891/2219-9365-2022-72-4-5

296. Каштальян А., Савенко О., Бельфер Р. Моделі приманок в корпоративних комп'ютерних мережах з врахуванням типів зловмисних атак. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2020. № 1. С. 104–110. URL: https://doi.org/10.31891/2219-9365-2020-65-1-16.

297. Каштальян А., Савенко О., Грибинчук В. Моделі та типи приманок для зловмисних атак в корпоративних комп’ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*. 2020. № 5. С. 45–50.

298. Каштальян А., Савенко О. Кластеризація зловмисників у комп'ютерних мережах за їх поведінковими характеристиками. *Вісник Хмельницького національного*

університету, технічні науки. 2020. № 6. С. 22–27. URL: https://doi.org/10.31891/2307-5732-2020-291-6-22-27.

299. Каштальян А., Савенко О. Покращення безпеки та модель антивірусних інтелектуальних приманок в корпоративних комп'ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*. 2020. Т. 1, № 4. С. 33–38. URL: https://doi.org/10.31891/2307-5732-2020-287-4-33-38.

300. Концепція застосування розподілених систем для аналізу поліморфних вірусів / П. Регіда та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Т. 331, № 1. С. 38–43. URL: https://doi.org/10.31891/2307-5732-2024-331-4

301. Корченко, А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень: автореф. дис. … д-ра техн. наук : 05.13.21. Київ, 2019. 40 с.

302. Летичевський О. О. Сучасні наукові проблеми кібербезпеки. *Visnik Nacional noi academii nauk Ukraini*. 2023. № 2. С. 12–20. URL: https://doi.org/10.15407/visn2023.02.012

303. Метод виявлення зловмисного програмного забезпечення на основі аналізу поведінкових патернів системи / Д. Денисюк та ін. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: технічні науки*. 2024. Т. 35(74), № 5. С. 124–129. URL: https://doi.org/10.32782/2663-5941/2024.5.1/19.

304. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами : Наказ від 29.05.2023 № 463. URL: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text.

305. Лисенко С. М. Методологічні основи та інформаційна технологія забезпечення резильєнтності комп’ютерних систем в умовах кіберзагроз: дис. … д-ра техн. наук : 05.13.06. Львів. 2020. 409 с.

306. Лукова-Чуйко Н.В. Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз: автореферат дис. … д-ра техн. наук: 05.13.06. Київ. 2018. с. 40.

307. Про захист інформації в інформаційно-комунікаційних системах : Закон від 05.07.1994 № 80/94-ВР : станом на 16 груд. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

308. Продеус М.С., Нічепорук А. О., Каштальян А. С. Система моніторингу, виявлення, реагування та захисту інформації на основі Honeypot-файлів. *Central Ukrainian Scientific Bulletin. Technical Sciences.* 2025. Issue 11(42), Part I. Pp. 56-67. URL: https://mapiea.kntu.kr.ua/pdf/11(42)_I/8.pdf

309. Регіда П. Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах : дис. … д-ра філософії в галузі техн. наук : 123. Хмельницький, 2025. 245 с. URL: https://nauka.khmnu.edu.ua/wp-content/uploads/dysertatsiia-savenko.pdf.

310. Савенко Б. О. Метод синтезу математичних моделей рівнів безпеки для частково централізованих розподілених систем виявлення зловмисного програмного забезпечення. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2023. № 3. Ч. 1. С. 217-227. DOI: https://doi.org/10.32782/2663-5941/2023.3.1/34

311. Савенко Б. Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах : дис. … д-ра філософії в галузі техн. наук : 123. Хмельницький, 2024. 245 с. URL: https://nauka.khmnu.edu.ua/wp-content/uploads/dysertatsiia-savenko.pdf.

312. Савенко Б., Каштальян А. Модель антивірусних інтелектуальних приманок в комп'ютерній мережі. Збірник наукових праць за матеріалами XII всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2020», м. Хмельницький. 2020. С. 257–260. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/3-7-35.pdf.

313. Савенко Б., Каштальян А., Петляк Н. Розподілені системи виявлення worm-вірусів. *2023 itsec: безпека інформаційних технологій: матеріали XII міжнар. наук.-техн. конф*, м. Ужгород, 2–4 трав. 2023 р. Київ, 2023. С. 37–39. URL: http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf.

314. Семенюк, Б., Каштальян, А. Виявлення комп'ютерних атак із використанням 2D-CNN та соніфікації мережевого трафіку. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2025. № 1. С. 193–201, doi: https://doi.org/10.32782/IT/2025-1-26

315. Тимошик Н. П. Вдосконалення принципів побудови та функціонування приманок в задачах захисту комп"ютерних систем та мереж : автореф. дис. … канд. техн. наук : 05.13.05. Львів, 2010. 20 с.

316. Ткачов В.М., Коваленко А.А., Кучук Г.А., Ні Я.С. Метод забезпечення живучості високомобільної комп’ютерної мережі. *Сучасні інформаційні системи*. Харків: НТУ «ХПІ», 2021. Т. 5., No 2. С. 159-165. DOI: https://doi.org/10.20998/2522-9052.2021.2.24

317. Ткачов В.М., Коваленко А.А., Фесенко Т.Г. Оптимізація мережного алгоритму функціонування комп'ютерних мереж підвищеної живучості на мобільній платформі на етапі їх проектування. *Системи управління, навігації та зв’язку. Збірник наукових праць*. Полтава: ПНТУ, 2021. Т. 3 (65). С. 143-147. DOI: https://doi.org/10.26906/SUNZ.2021.3.143

ДОДАТКИ

ДОДАТОК А.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України, або у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

1. Kashtalian A., Lysenko S., Kysil T., Sachenko A., Savenko O., Savenko B. Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*, 2025. *24*(1), 35-51. DOI: https://doi.org/10.47839/ijc.24.1.3875 (***Scopus***)

2. Kashtalian A., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*, 2025. № 1. Pp. 264-297. DOI: https://doi.org/10.32620/reks.2025.1.18 (категорія А, ***Scopus***)

3. Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil T. Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems*, 2023. № 4. Pp. 112-151. DOI: https://doi.org/10.32620/reks.2023.4.10 (категорія А, ***Scopus***, Q3)

4. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., & Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024. № 1. Pp. 152-175. DOI: https://doi.org/10.32620/reks.2024.1.13 (категорія А, ***Scopus***, Q2)

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

5. Денисюк Д.О., Савенко Б.О., Каштальян А.С., Іванченко О.В. Метод виявлення зловмисного програмного забезпечення на основі аналізу поведінкових патернів системи. *Вчені записки Таврійського національного університету імені В.І.*

Вернадського. Серія: технічні науки. Том 35(74), №5. 2024. Ч.1. С.124-129. DOI: https://doi.org/10.32782/2663-5941/2024.5.1/19

6. Каштальян А. С. Методи організації функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток в корпоративних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*. 2025. № 1. С. 160–171. https://doi.org/10.31891/2219-9365-2025-81-19

7. Каштальян А. С. МЕТОД ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК МУЛЬТИКОМП'ЮТЕРНИМИ СИСТЕМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК. *Herald of Khmelnytskyi National University. Technical Sciences*, 2025, № *349*(2), С. 346-352. https://doi.org/10.31891/2307-5732-2025-349-50

8. Каштальян А. С. Мультикомп'ютерна система з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп'ютерних атак на основі мультиагентних технологій. *Вісник Хмельницького національного університету. Серія: Технічні науки* 2025, № *347* (1). С. 535-542. https://doi.org/10.31891/

9. Каштальян А. С. Концептуальна модель архітектури мультикомп'ютерних систем із приманками та пастками для виявлення та протидії зловмисному програмному забезпеченню та комп'ютерним атакам. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, №3, С. 22-31 https://doi.org/10.32782/IT/2023-3-3

10. Каштальян А. С. Критерій оперативності щодо варіантів централізації в архітектурі мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток для виявлення зловмисного програмного забезпечення та комп'ютерних атак. *Herald of Khmelnytskyi National University. Technical sciences, [S. l.]*, v. 345, n. 6(2), p. 172–178, 2024. DOI: 10.31891/. Disponível em: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/995.

11. Каштальян А. С. Особливості правил формування варіантів централізації для мультикомп'ютерних систем в корпоративних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, [S. l.]*, n. 4, p. 386–393,

2024. DOI: 10.31891/2219-9365-2024-80-46. DOI: https://doi.org/10.31891/2219-9365-2024-80-46

12. Каштальян А. С. Принцип синтезу мультикомп’ютерних систем з комбінованих антивірусних приманок і пасток та контролеру прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*, 2023. № 4, С. 265–272. https://doi.org/10.31891/2219-9365-2023-76-35

13. Каштальян А. С. Характерні властивості централізації в архітектурі мультикомп’ютерних систем антивірусних комбінованих приманок і пасток. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2024, № 4, С. 112-124. DOI: https://doi.org/10.32782/IT/2024-4-14

14. Каштальян, А., Любінецький, Д. Розподілена самоорганізована система прогнозування зловмисної активності в комп’ютерних мережах. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*. 2022. №4. С. 49–57. https://doi.org/10.31891/2219-9365-2022-72-4-5

15. Каштальян А.С., Савенко О.С. Кластеризація зловмисників у комп'ютерних мережах за їх поведінковими характеристиками. *Вісник Хмельницького національного університету, технічні науки*, 2020, №6, С. 22-27. DOI: 10.31891/2307-5732-2020-291-6-22-27

16. Каштальян А.С., Савенко О.С. Покращення безпеки та модель антивірусних інтелектуальних приманок в корпоративних комп'ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*, 2020, №4, том 1, С. 33-38 DOI: https://www.doi.org/10.31891/2307-5732-2020-287-4-33-38

17. Каштальян А.С., Савенко О.С., Бельфер Р.Е. Моделі приманок в корпоративних комп'ютерних мережах з врахуванням типів зловмисних атак. *Вимірювальна та обчислювальна техніка в технологічних процесах*, 2020, №1, С.104-110. DOI: 10.31891/2219-9365-2020-65-1-16

18. Каштальян А.С., Савенко О.С., Грибинчук В.І. Моделі та типи приманок для зловмисних атак в корпоративних комп’ютерних мережах. *Вісник Хмельницького національного університету, технічні науки*, 2020, №5, С. 45-50.

19. Продеус М.С., Нічепорук А. О., Каштальян А. С. Система моніторингу, виявлення, реагування та захисту інформації на основі Honeypot-файлів. *Central Ukrainian Scientific Bulletin. Technical Sciences.* 2025. Issue 11(42), Part I. Pp. 56-67. URL: https://mapiea.kntu.kr.ua/pdf/11(42)_I/8.pdf

20. Регіда П.Г., Бармак О.В., Каштальян А.С., Манзюк Е.А. Концепція застосування розподілених систем для аналізу поліморфних вірусів. *Herald of Khmelnytskyi National University. Technical Sciences. 2024. № 331*(1). С. 38-43. https://doi.org/10.31891/2307-5732-2024-331-4

21. Семенюк, Б., Каштальян, А. Виявлення комп'ютерних атак із використанням 2D-CNN та соніфікації мережевого трафіку. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2025. № 1. С. 193–201, doi: https://doi.org/10.32782/IT/2025-1-26

Праці, які засвідчують апробацію матеріалів дисертації

22. Belfer R., Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes. *CEUR-WS*. – 2020. Vol. 2623. – Pp. 239-251. URL: https://ceur-ws.org/Vol-2623/paper21.pdf (Scopus)

23. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece. 2023. Pp. 1-6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416453 (Scopus)

24. Denysiuk D., Sochor T., Kapustian M., Kashtalian A., Drozd A. A method for detecting botnets in IT infrastructure using a neural network. CEUR Workshop Proceedings. 2024, 3736. Pp. 282–292. URL: https://ceur-ws.org/Vol-3736/paper21.pdf (Scopus)

25. Denysiuk D., Sochor T., Kapustian M., Kashtalian A., Savenko O. Methods for detecting software implants in corporate networks. CEUR Workshop Proceedings. 2024. 3675. Pp. 270–284. URL: https://ceur-ws.org/Vol-3675/paper20.pdf (Scopus)

26. Liubinetskyi D., Kashtalian A., Sochor T., Selskyi A., Klein O. Distributed System for Predicting Malicious Activity in Computer Networks. *CEUR Workshop Proceedings*. 2023. Vol. 3373. Pp. 401–410. URL: https://ceur-ws.org/Vol-3373/paper26.pdf (Scopus)

27. Kashtalian A. Honeypots Models in Computer Networks According to Mailcious Attacs Types. *Proceedings of VII International conference "Information Technology and Interactions" (IT&I-2020)*, 02-04 December 2020. – Taras Shevchenko National University, Kyiv. Pp. 71-73. URL: http://iti.fit.univ.kiev.ua/wp-content/uploads/ITI_Satellite_2020_Conference-Proceedings.pdf

28. Kashtalian A., Savenko O., Sachenko A. Agglomerative Clustering of Data Collected by Honeypots. *2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Cracow, Poland, 2021. Pp. 504-509. DOI: https://doi.org/10.1109/IDAACS53288.2021.9661027 (Scopus)

29. Kashtalian A., Sochor T. K-Means Clustering of Honeynet Data with Unsupervised Representation Learning. *International Workshop on Intelligent Information Technologies & Systems of Information Security*. *CEUR Workshop Proceedings*. 2021. Vol. 2853. Pp. 439–449. URL: https://www.semanticscholar.org/paper/K-means-Clustering-of-Honeynet-Data-with-Learning-Kashtalian-Sochor/ca7f4a13249eb5624f7df585f840a1e24f2e6ef4#citing-papers (Scopus)

30. Prodeus M., Nicheporuk A., Kashtalian A., Kapustian M., Sochor T. Honeypot-based monitoring, detection, response, and information protection framework. *Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 329-339. URL: https://ceur-ws.org/Vol-3963/paper26.pdf (Scopus)

31. Rehida, P., Savenko, O., Kashtalian, A., Sachenko, A. Malware Detection Tool Based on Emulator State Analysis. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023. Pp. 135-140. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348678 (Scopus)

32. Kozelskiy O., Kashtalian A., Stetsyuk V., Martiniuk D., Sachenko A. A model of an intelligent clustering system with an external module for the architecture of RTOS with intensive changes of states regarding their flexibility and balancing. *CEUR Workshop Proceedings*. 2025. 3899. Pp. 234–243. URL: https://ceur-ws.org/Vol-3899/paper21.pdf (Scopus)

33. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023. Pp. 265-270. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348773 (Scopus)

34. Savenko B., Kashtalian A., Sochor T., Nicheporuk A. Self-Organized Distributed Anomaly Detection System in Computer Systems Based on The Principal Components Method. *CEUR Workshop Proceedings*. 2022. Vol. 3156. Pp. 329–351. URL: https://ceur-ws.org/Vol-3156/paper25.pdf (Scopus)

35. Semeniuk B., Kashtalian A., Martiniuk D., Drozd A., Abdel-Badeeh M. Salem. Detection of computer attacks based on sonification of network traffic *Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 252-263. URL: https://ceur-ws.org/Vol-3963/paper21.pdf (Scopus)

36. Савенко Б.О., Каштальян А.С. Модель антивірусних інтелектуальних приманок в комп'ютерній мережі. *Актуальні проблеми комп'ютерних наук. Збірник наукових праць за матеріалами XII всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2020»*. Хмельницький: ХНУ, 2020. С. 257-260. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/3-7-35.pdf

37. Савенко Б., Каштальян А., Петляк Н. Розподілені системи виявлення worm-вірусів. *2023 ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф.*, м. Ужгород, 2-4 трав. 2023 р. / НАУ, м. Київ, 2023. С. 37-39. http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

Публікації, які додатково відображають наукові результати дисертації

38. Каштальян А.С., Авсієвич В.Р., Нічепорук А.О., Савенко О.С. А. с. 124518, Україна. Комп'ютерна програма «Проміжне програмне забезпечення мультикомп'ютерних систем спеціалізованого призначення». Дата реєстрації 11.03.2024

ДОДАТОК Б.
АКТИ ВПРОВАДЖЕННЯ

«Затверджую»
Генеральний директор
ПП «Нолт Технолоджис»
Олександр МЕЛЬНИЧЕНКО
«21» квітня 2025 р.

АКТ
про впровадження результатів дисертаційної роботи
Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток»

Результати дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Каштальян А. впроваджені на ПП «Нолт Технолоджис» та відповідають напрямам діяльності щодо розроблення сучасних інформаційних технологій та систем для різних предметних областей.

При розробленні мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора, були використані на ПП «Нолт Технолоджис» такі результати, які одержані Каштальян А. особисто:

1) вперше запропонована концепція вирішення науково-прикладної проблеми, яка полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем з комбінованих антивірусних приманок і пасток та контролеру прийняття рішень для покращення ефективності виявлення ЗПЗ та КА в корпоративних мережах, що базується на поєднанні таких виділених визначальних властивостей та їх синтезу в системах, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних приманок і пасток в системі;

2) вперше розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА містить дві визначальні вимоги щодо наявності в архітектурі систем контролера та спеціалізованого функціоналу, що дає змогу впливати на рішення систем щодо їх наступних кроків та зміни архітектури і в результаті це ускладнить для зловмисників розуміння функціонування таких

систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращить ефективність виявлення та протидії ЗПЗ і КА в корпоративних мережах;

3) вперше розроблено концептуальну модель мультикомп'ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, який сумісно з загальною частиною системи формує систему як єдиний сенсор, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також дає змогу не тільки урізноманітнити систему через її різну архітектуру, але й забезпечує її стійкість при вилученні певних вузлів в корпоративній мережі та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

Виконані дослідження включають принципи, моделі, методи та засоби покращення ефективності функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Отримані результати забезпечують підвищення достовірності виявлення ЗПЗ та КА порівняно з відомими аналогічними рішеннями в середньому на 8–11%.

Цей акт не є підставою для фінансових розрахунків.

Генеральний директор Олександр МЕЛЬНИЧЕНКО

«Затверджую»
Директор ТОВ «ІТТ»
_____ Сімогук В.С.
«_10_» квітня 2025 р.

АКТ
про впровадження результатів дисертаційної роботи
докторантки кафедри комп'ютерної інженерії та інформаційних систем
Хмельницького національного університету Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем
комбінованих антивірусних приманок і пасток»

Результати дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Антоніни КАШТАЛЬЯН впроваджені на ТОВ «ІТТ». При здійсненні забезпечення захисту корпоративної мережі були використані на ТОВ «ІТТ» такі результати, які одержані Антоніною КАШТАЛЬЯН особисто:

1) концептуальна модель мультикомп'ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, який сумісно з загальною частиною системи формує систему як єдиний сенсор, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також дає змогу не тільки урізноманітнити систему через її різну архітектуру, але й забезпечує її стійкість при вилученні певних вузлів в корпоративній мережі та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

2) метод організації функціонування мультикомп'ютерних систем, особливістю якого є забезпечення можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролеру прийняття рішень та центру системи, що забезпечило багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі.

3) метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, в якому здійснено збір даних та кластеризацію схожих зловмисників з використанням мультикомп'ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних

ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА;

4) метод виявлення зловмисного програмного забезпечення та комп'ютерних атак, який реалізується в архітектурі мультикомп'ютерних систем з комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати одночасно кілька завдань, взаємодіяти між собою у процесі обробки подій з інформуванням центру системи, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок та всієї системи).

У результаті впровадження наукового доробку Антоніни КАШТАЛЬЯН було впроваджено мультикомп'ютерну систему комбінованих антивірусних приманок і пасток в корпоративну мережу. Результати експериментальних досліджень підтвердили ефективність запропонованих рішень та дозволили підвищити достовірність виявлення комп'ютерних атак на 6–9 % порівняно з відомими аналогами.

Цей акт не є підставою для фінансових розрахунків.

Заступник директора _____ Іванов О.В.

Системний адміністратор_____Веремеєнко В.А.

ДОВІДКА

про впровадження результатів дисертаційної роботи
докторантки кафедри комп'ютерної інженерії та інформаційних систем
Хмельницького національного університету Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем
комбінованих антивірусних приманок і пасток»

Результати дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Антоніни КАШТАЛЬЯН впроваджені у Приватному підприємстві «Авіві».

При здійсненні захисту корпоративної мережі були використані такі результати:

1) метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками;

2) метод виявлення зловмисного програмного забезпечення та комп'ютерних атак комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення.

Використання наведених наукових результатів Антоніни КАШТАЛЬЯН дало змогу впровадити мультикомп'ютерну систему комбінованих антивірусних приманок і пасток в корпоративну мережу. Результати досліджень з встановленою системою дозволили підвищити достовірність виявлення комп'ютерних атак на 7–9 % порівняно з відомими аналогами.

18.06.2025 р.

Директор ПП «Авіві» _____ В. В. Аскеров

«Затверджую»
Директор ТОВ «ЮКС++»
Юрій КЛЬОЦ
«_17_» червня 2025 р.

АКТ
про впровадження результатів дисертаційної роботи
докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток»

Результати дисертаційної роботи Антоніни КАШТАЛЬЯН докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету впроваджені на ТОВ «ЮКС++».

При розробленні мультикомп'ютерної системи комбінованих антивірусних приманок і пасток були використані на ТОВ «ЮКС++» такі результати, які отримані Антоніною КАШТАЛЬЯН особисто:

1) метод організації функціонування контролера прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

2) метод організації функціонування мультикомп'ютерних систем, який на відміну від відомих, дає змогу забезпечити можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролера прийняття рішень та центру системи, що забезпечило багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі;

3) метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, особливістю якого є збір даних та кластеризація схожих зловмисників з використанням мультикомп'ютерних систем з антивірусними комбінованими приманками і пастками, основними етапами пошуку подібних часових рядів активності зловмисників є представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації та забезпечення різних варіантів відповідей на повторювані події, що збільшує витрати зловмисників та тривалість КА.

Отриманні результати дозволили покращити ефективність функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток виявлення зловмисного програмного забезпечення і комп'ютерних атак для забезпечення безпеки та захисту корпоративних мереж за рахунок синтезу в їх архітектурі властивостей із приховування своєї присутності, змінюваності відповідей на повторювані зловмисником дії, самостійного прийняття рішень без залучення адміністратора.

Цей акт не є підставою для фінансових розрахунків.

Товариство з обмеженою відповідальністю «ЮКС++» Код 39587947 Україна м.Хмельницький

_____ Юрій КЛЬОЦ

ДОВІДКА

про впровадження результатів дисертаційної роботи
Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток»

В діяльності відділу протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції Національної поліції України при забезпеченні захисту корпоративної мережі були використані результати дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Антоніни КАШТАЛЬЯН.

Зокрема, було використано такі результати дисертаційної роботи:

- концептуальна модель мультикомп'ютерних систем антивірусних комбінованих приманок і пасток;
- метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками;
- метод виявлення зловмисного програмного забезпечення та комп'ютерних атак комбінованими антивірусними приманками і пастками різної архітектури та функціонального призначення.

У відділі протидії кіберзлочинам в Хмельницькій області розгорнута в корпоративній мережі мультикомп'ютерна система антивірусних приманок і пасток дала змогу проводити дослідження зловмисних впливів та покращила її безпеку та захист. Використання наукових результатів Антоніни КАШТАЛЬЯН дало змогу підвищити достовірність виявлення комп'ютерних атак приблизно на 8 % порівняно з використанням попередніх аналогів.

24.06.2025 р.

Т.в.о. начальника
відділу протидії кіберзлочинам
в Хмельницькій області
Департаменту кіберполіції
Національної поліції України _____ Дереновський А.В.

«Затверджую»
Проректор з науково-педагогічної роботи
_____ Віктор ЛОПАТОВСЬКИЙ
«16» квітня 2025 р.

АКТ

про впровадження в навчальний процес Хмельницького національного університету результатів дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Каштальян Антоніни Сергіївни «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток»

Ми, комісія в складі: декана факультету інформаційних технологій, професора кафедри комп'ютерної інженерії та інформаційних систем, д.т.н., професора Говорущенко Т. О. (голова комісії), професора кафедри комп'ютерної інженерії та інформаційних систем, д.т.н., професора Лисенка С.М., доцента кафедри комп'ютерної інженерії та інформаційних систем, к.т.н., доцента Капустян М. В. склала акт про те, що результати дисертаційної роботи Каштальян А.С. впроваджені та використовуються в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності 123 Комп'ютерна інженерія, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Теорія і технології проєктування спеціалізованих операційних систем», «Безпека та захист комп'ютерних систем».

При викладанні цих дисциплін викладачами кафедр використовувалися наступні матеріали досліджень, отримані Каштальян А.С. особисто:

1) принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА містить дві визначальні вимоги щодо наявності в архітектурі систем контролера та спеціалізованого функціоналу, що дає змогу впливати на рішення систем щодо їх наступних кроків та зміни архітектури і в результаті це ускладнить для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращить ефективність виявлення та протидії ЗПЗ і КА в корпоративних мережах;

2) концептуальна модель мультикомп'ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за здійснення контролю прийнятих рішень, та решту визначальних характеристик, які в процесі функціонування систем повинні формувати архітектуру системи самостійно синтезуючи множину окремих визначальних характеристик згідно замкненого маршруту в графі визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, який сумісно з загальною частиною системи

формує систему як єдиний сенсор, що дає змогу забезпечити урізноманітнення варіантів відповідей при впливах зловмисників, КА і функціонуванні ЗПЗ, а також дає змогу не тільки урізноманітнити систему через її різну архітектуру, але й забезпечує її стійкість при вилученні певних вузлів в корпоративній мережі та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

3) математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих математичних моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані аналітичними виразами, в яких враховані особливості типів централізації в архітектурі систем, показники оперативності, стійкості, цілісності та безпеки щодо центру системи і дають змогу сформувати на їх основі цільову функцію для оцінювання наступних варіантів централізації в системах, особливістю яких є приховування компонент з центром системи від його виявлення зловмисниками;

4) метод визначення варіанту централізації в системах класу $\mathfrak{S}$, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури на централізовану, частково централізовану, частково децентралізовану і децентралізовану, що дає змогу згідно правил вибору варіанта централізації здійснити оцінювання кожного з обраних варіантів в залежності від кількості активних компонентів систем в поточний момент часу та критеріїв і підібрати з великої кількості варіантів наступний варіант без здійснення оцінювання всіх варіантів, що забезпечує швидкодію та уникнення повного чи значного часткового перебору всіх варіантів в постійно змінюваному середовищі;

5) метод організації функціонування контролеру прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах.

Отримані матеріали досліджень дозволили розробити навчальний матеріал для лекційних курсів та лабораторних занять з розроблення та застосування мультикомп'ютерних систем комбінованих антивірусних приманок і пасток.

Говорущенко Т. О.
Лисенко С.М.
Капустян М. В.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
(НУВГП)
вул. Соборна, 11, м. Рівне, 33028, тел. (0362) 63 30 98, факс (0362) 63 32 09,
e-mail: mail@nuwm.edu.ua, web: https://nuwm.edu.ua
код ЄДРПОУ 02071116

Від 14.03.2025 № 011 – 07 На № _____ від _____

ДОВІДКА
про використання у навчальному процесі
Національного університету водного господарства та природокористування
результатів досліджень і розробок, одержаних при виконанні дисертаційної роботи
Каштальян Антоніни Сергіївни
на здобуття наукового ступеня доктора технічних наук за спеціальністю
05.13.05 «Комп'ютерні системи та компоненти»

Використання у навчальному процесі Національного університету водного господарства та природокористування науково-методичних розробок та результатів досліджень докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету, що викладені в її дисертації «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток», забезпечують набуття теоретичних знань і практичних навичок щодо методів виявлення зловмисного програмного забезпечення та комп'ютерних атак, методів знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками, математичного моделювання та формалізації критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи та сприяють розвитку у майбутніх фахівців творчого, науково-дослідницького мислення під час викладання таких освітніх компонент:

- при викладанні навчальної дисципліни «Основи кібербезпеки» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності F5 Кібербезпека та захист інформації, ОПП «Інформаційна безпека»: Тема 2. Вступ до кібербезпеки; Тема 12. Методики побудови комбінованих антивірусних систем на основі приманок;
- при викладанні навчальної дисципліни «Комплексні системи захисту інформації» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності F5 Кібербезпека та захист інформації, ОПП «Інформаційна безпека»: Тема 11. Аналіз і класифікація зловмисного програмного забезпечення за допомогою пасток; Тема 12. Типологія та архітектура антивірусних пасток і приманок;
- при викладанні навчальної дисципліни «Виявлення вразливостей та тестування безпеки інформаційних систем» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності F5 Кібербезпека та захист інформації, ОПП «Інформаційна безпека»: Тема 12 Сучасні тренди: використання AI/ML у кібербезпеці.

Матеріали досліджень Антоніни КАШТАЛЬЯН дозволили включити їх в методичні вказівки та завдання до лабораторних занять із застосування антивірусних приманок і пасток, а також застосування штучних нейронних мереж для задач із виявлення комп'ютерних атак.

Проректор з наукової роботи
та міжнародних зв'язків,
д.е.н., професор Наталія САВІНА

Виконавець: Сидор А.І. +380961983[illegible]

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної роботи
Західноукраїнського національного університету
_____ Віктор ОСТРОВЕРХОВ
«16» 06 2025 р.

АКТ

про впровадження в навчальний процес Західноукраїнського національного університету результатів дисертаційної роботи докторантки кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Каштальян Антоніни Сергіївни «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток»

Комісія в складі декана факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету, к.т.н., доцента Якименка Ігоря Зіновійовича (голова комісії), заступника завідувача кафедри кібербезпеки, к.т.н., доцента Івасьєва Степана Володимировича, професора кафедри кібербезпеки, д.т.н., професора Касянчука Михайла Миколайовича склала акт про те, що результати дисертаційної роботи Антоніни КАШТАЛЬЯН впроваджені та використовуються в навчальному процесі при викладанні дисциплін на кафедрі кібербезпеки Західноукраїнського національного університету для спеціальності 125 Кібербезпека та захист інформації, зокрема в курсах «Дослідження і проектування систем захисту інформації» та «Безпека комп'ютерних та кіберфізичних систем». При викладанні цих дисциплін викладачами кафедри використовувалися такі наукові результати, отримані Антоніною КАШТАЛЬЯН особисто:

1) принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам;

2) математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи;

3) метод визначення варіанту централізації в системах визначеного класу, в якому вибір наступного варіанту централізації здійснюється за комплексними критеріями оперативності, стійкості, цілісності, безпеки та з врахуванням поділу типу архітектури.

Вказані результати використані при розробці відповідних лекційних курсів.

Декан факультету комп'ютерних інформаційних технологій, к.т.н., доцент — Ігор ЯКИМЕНКО

Заступник завідувача кафедри кібербезпеки к.т.н., доцент — Степан ІВАСЬЄВ

Професор кафедри кібербезпеки, д.т.н., професор — Михайло КАСЯНЧУК

ДОДАТОК В.
ДЕТАЛІЗАЦІЯ ПЕРШОГО ЕКСПЕРИМЕНТУ

Перша серія першого експерименту була проведена за штатного функціонування системи. Чотири графіки дискретних функцій зображено на рис. В.1, які відображають по сто точок для кожного з чотирьох критеріїв. Проблемних подій в системі протягом часу її функціонування не відбулось. Зображені графіки відображають значення в діапазоні від 0 до 0,065, що відповідає заданим в аналітичних виразах обмеженнях для визначених критеріїв щодо оперативності, стійкості, цілісності та безпеки. Всі точки на графіках відповідають значенням функцій, які отримані під час підготовки наступного варіанту централізації в системі. Задані критерії переважно не мають спільних показників і, тому, отримані значення згідно їх аналітичних виразів не є корельованими.

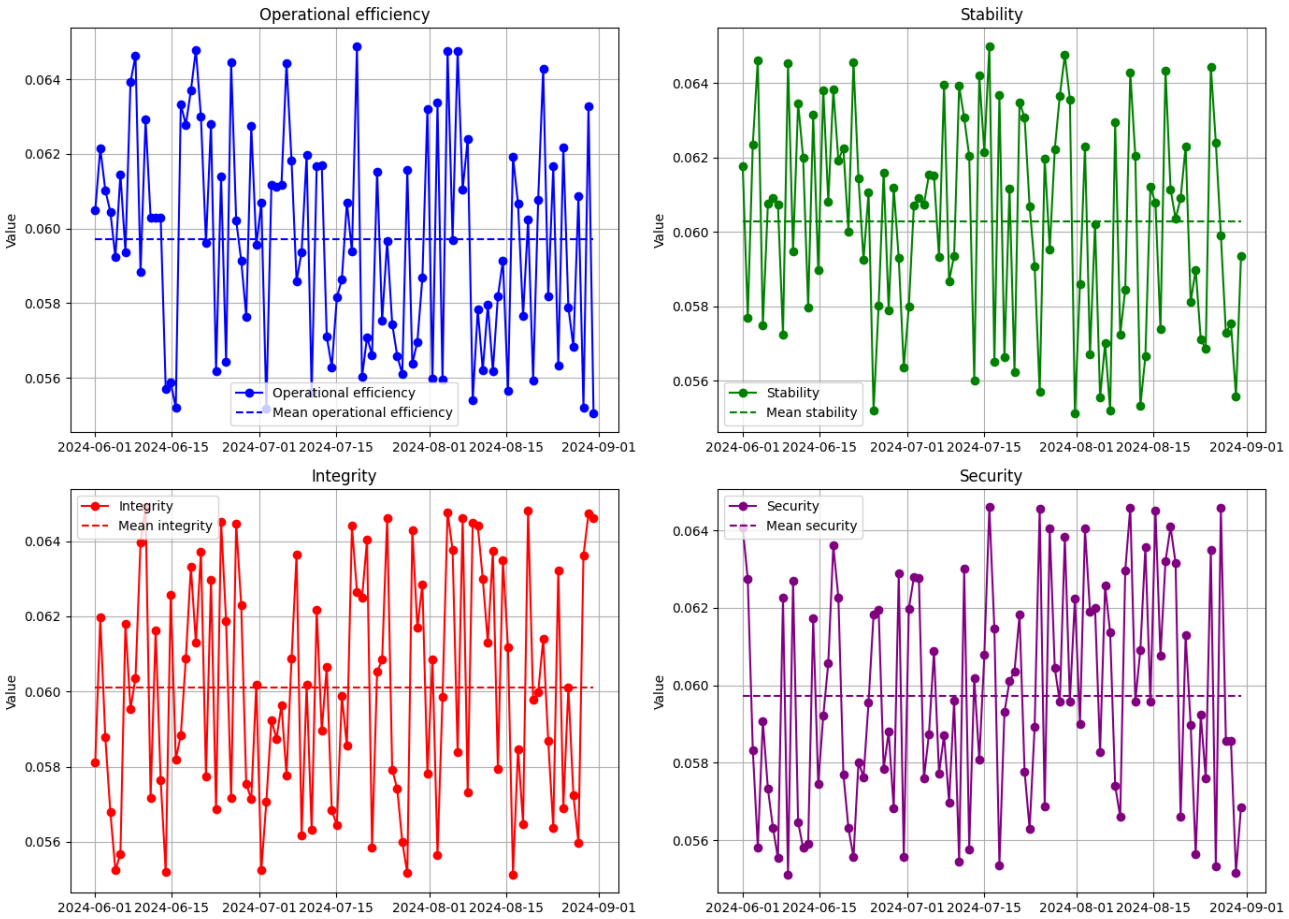


Рисунок В.1 - Графіки функцій для чотирьох критеріїв першої серії першого експерименту

Побудуємо графік для цільової функції за отриманими значеннями для критеріїв за формулою (3.28). Обчислимо її значення як середньоарифметичне значення усіх чотирьох критеріїв. Хоча за потреби її значення може бути визначено як середньозважене значення, якщо більший вплив певного критерію буде встановлено або зазначено. Графік цільової функції для першої серії експерименту, який зображено на рис. В.2, показує допустимі значення для переходів до наступних варіантів централізації в архітектурі системи протягом часу проведення експерименту. Крім того, на основі значень цільової функції було побудовано графік теоретичної кривої, яка відображає та визначає можливі подальші значення цільової функції при визначенні наступних варіантів централізації. Відхилення між теоретичною кривою і експериментально отриманими значеннями згідно методу найменших квадратів перебувають в допустимих межах. Зокрема, різниця між максимальним (мінімальним) значенням з експерименту та значенням відповідної точки теоретичної кривої дорівнює приблизно 0,03, тобто становить 3%. Це наслідок підбору вдалих варіантів централізації. Отримана теоретична крива, для якої визначено аналітичний вираз, задана півпараболою з поступовим низхідним трендом. Це відображає врахування попереднього досвіду при кожному новому варіанті вибору. Оскільки, система працювала тривалий час, то це є показником її вдалого самонавчання і, відповідно, визначення цільової функції для штатного випадку функціонування системи.

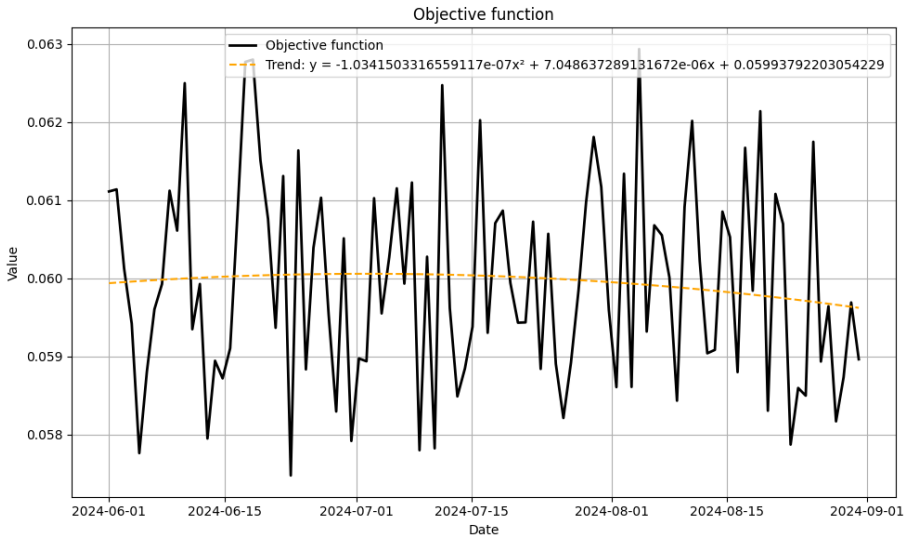


Рисунок В.2 - Графік цільової функції для першої серії першого експерименту

Наступні серії першого експерименту для дослідження системи щодо застосування критеріїв були здійснені для випадків окремих впливів на показники критеріїв, причому кожен критерій досліджувався окремо.

Друга серія першого експерименту була проведена з урахуванням зміни показників, які впливали на значення критерію щодо оперативності. Було встановлено протягом часу функціонування системи суттєві відхилення в отриманих значеннях протягом трьох часових періодів. Графіки всіх чотирьох функцій в цьому випадку зображено на рис. В.3.

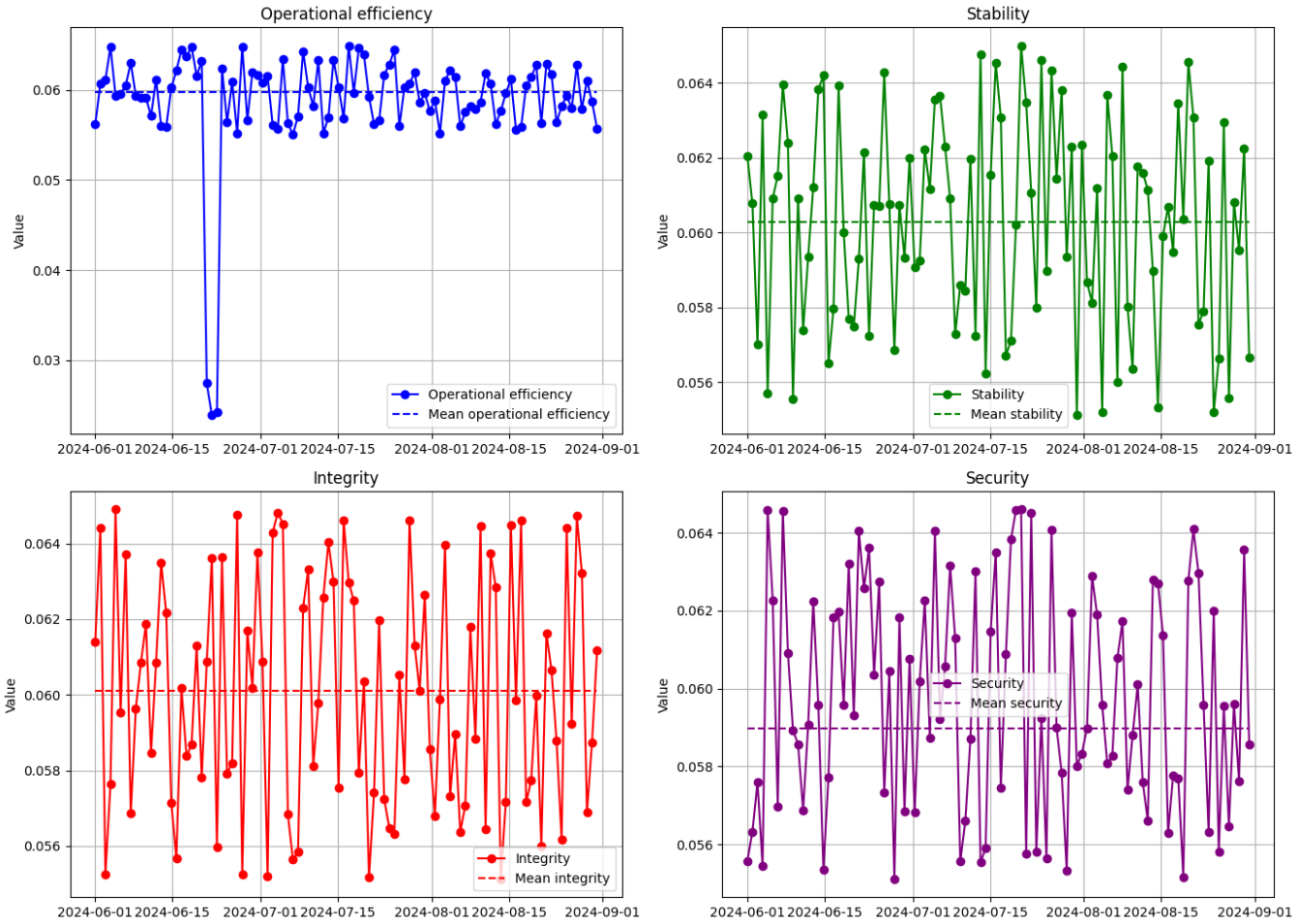


Рисунок В.3 - Графіки функцій другої серії першого експерименту для чотирьох критеріїв

Отримані значення з урахуванням суттєвих відхилень частини значень для критерію щодо оперативності є допустимими для продовження функціонування системи. Тобто стабільність роботи системи не була порушена в результаті подій, які

вплинули на значення для критерію щодо оперативності. Цільова функція, яку зображено графіком на рис. В.4, отримана емпіричним способом теж підтверджує спроможність системи продовжувати функціонування та визначення наступного варіанту централізації. В цьому випадку оцінені варіанти централізації згідно визначення цільової функції будуть мати більші значення і серед них для затвердження пріоритетним буде менше з цих значень.

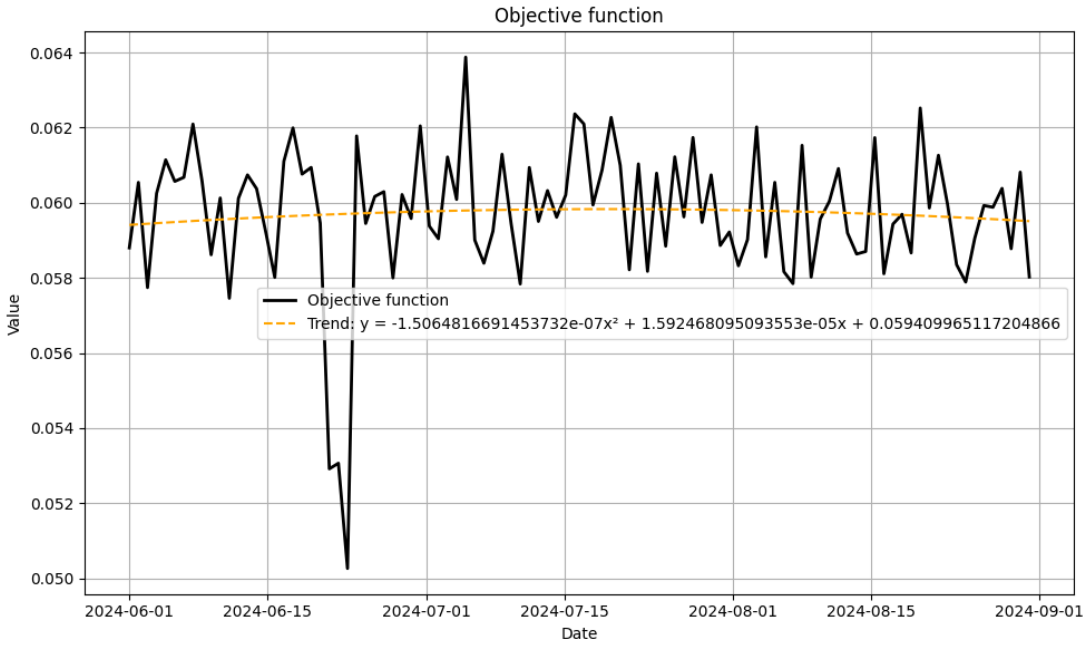


Рисунок В.4 - Графік цільової функції другої серії першого експерименту

Цільова функція, яку визначено теоретичним способом, підтверджує спроможність системи визначати наступний варіант її централізації.

Аналогічно для критеріїв щодо стійкості (графіки на рис. В.5 і рис. В.6), цілісності (графіки на рис. В.7 і рис. В.8) та безпеки (графіки на рис. В.9 і рис. В.10) отримуємо підтвердження щодо допустимості виконання завдання визначення наступного варіанту централізації в архітектурі системи. Тренд теоретичної кривої цільової функції для критерію щодо впливу на стійкість (рис. В.6) є висхідним, а для теоретичних кривих цільової функції для критеріїв щодо оперативності, безпеки та цілісності є низхідними. При цьому всі значення цільових функцій при зміні всіх критеріїв окремо менше 7%, що є допустим для функціонування роботи. На графіках для цих випадків подальші кроки системи з перебудови центру є стабільними.

Значення всіх функцій першого експерименту подано фрагментом в табл. 6.2, в якій відображено відхилення за кожним параметром окремо (всі значення результатів експерименту в табл. Є.1-Є.2, Додаток Є). Таким чином, задані функціями чотири критерії адекватно відображають поведінку системи.

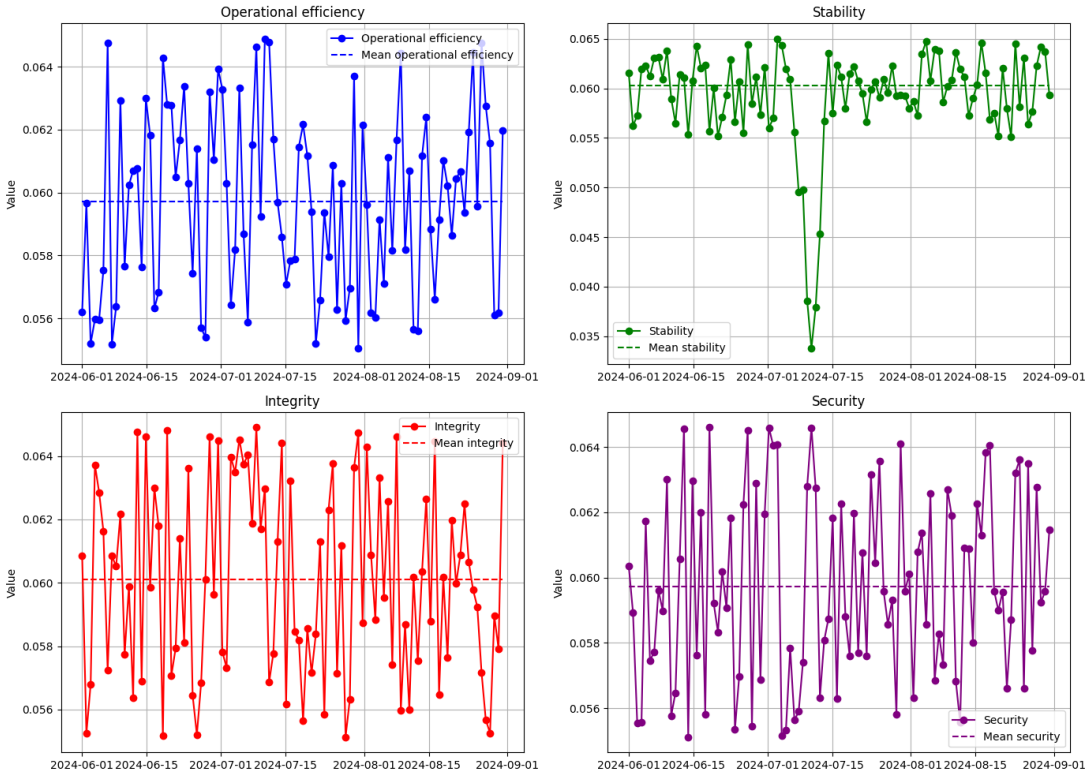


Рисунок В.5 - Графіки функцій третьої серії першого експерименту для чотирьох критеріїв

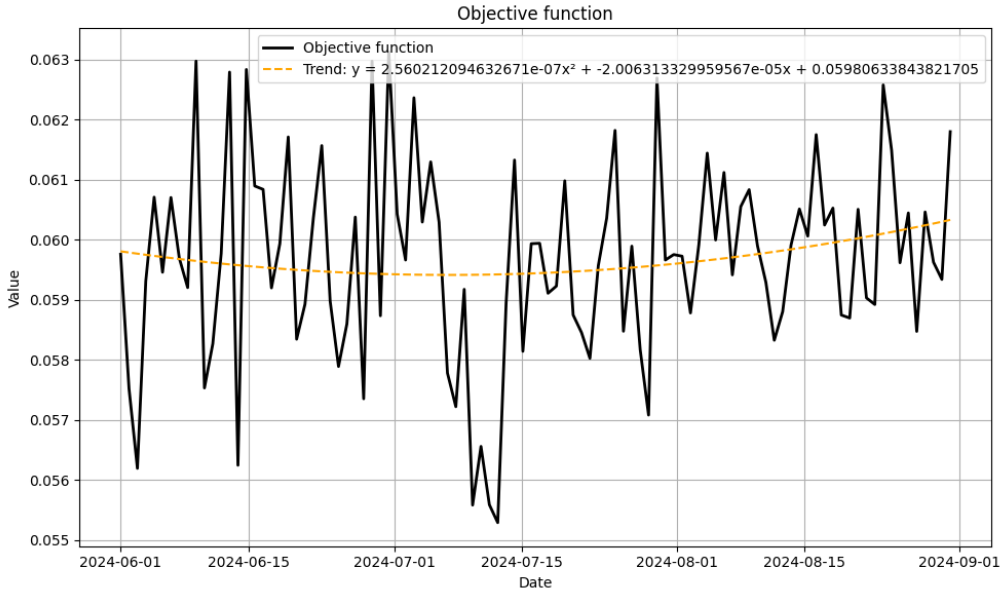


Рисунок В.6 - Графік цільової функції третьої серії першого експерименту

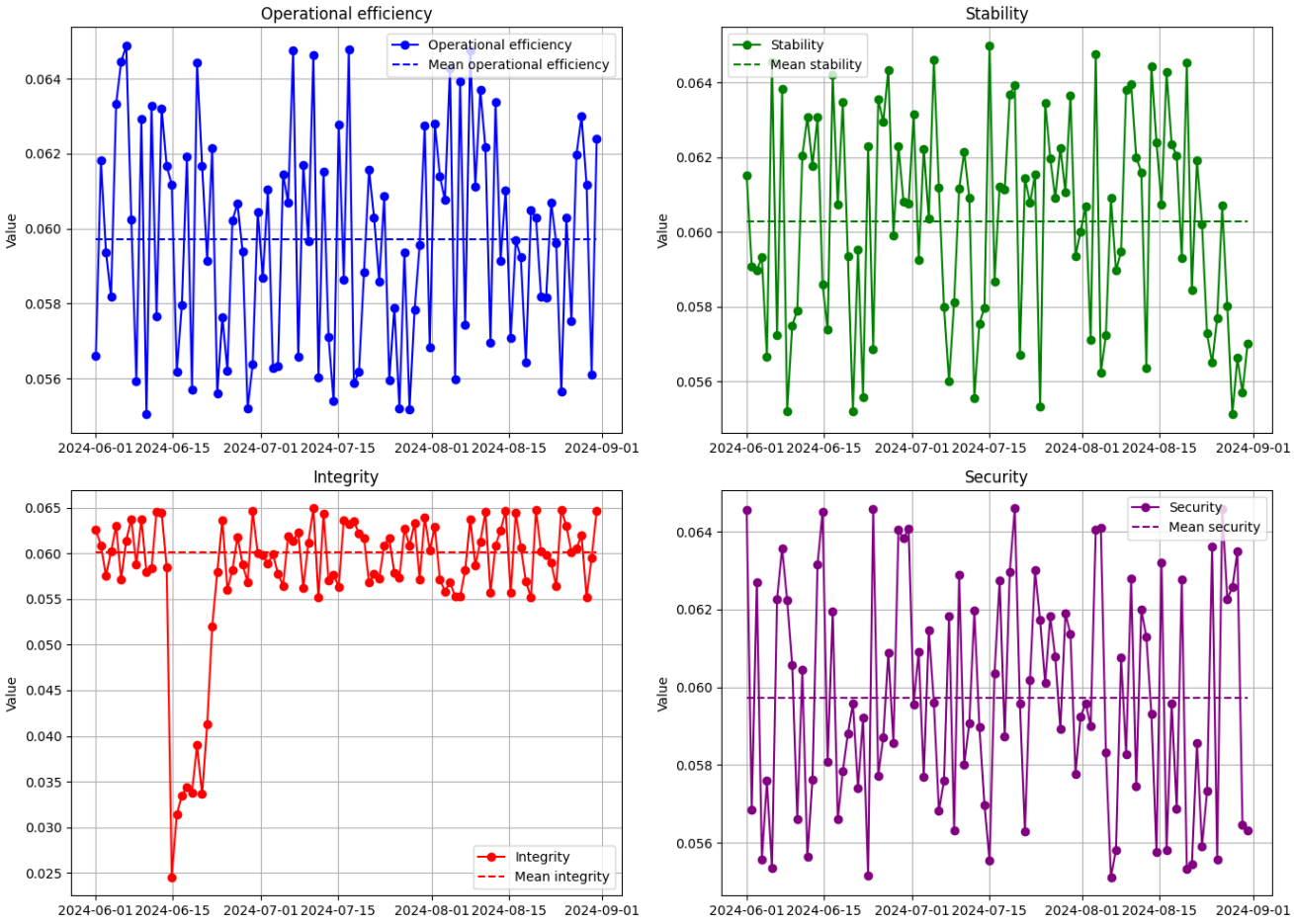


Рисунок В.7 - Графіки функцій четвертої серії експерименту для чотирьох критеріїв

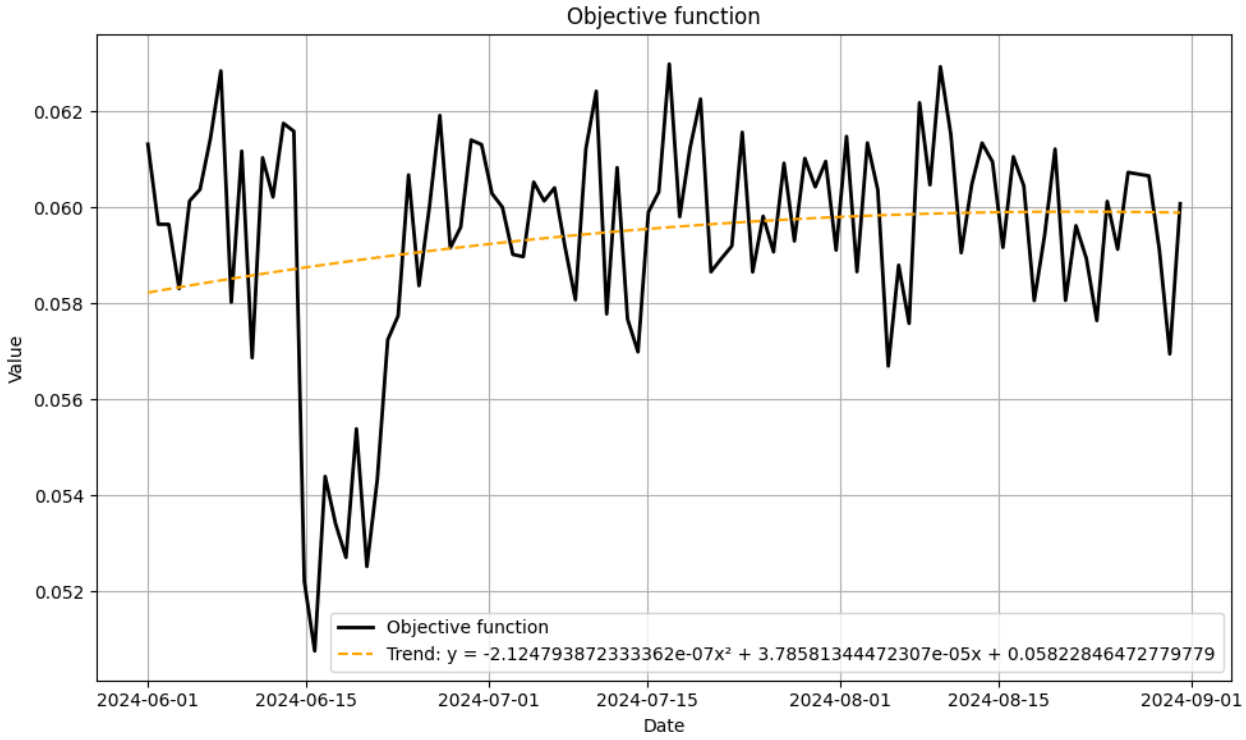


Рисунок В.8 - Графік цільової функції четвертої серії експерименту

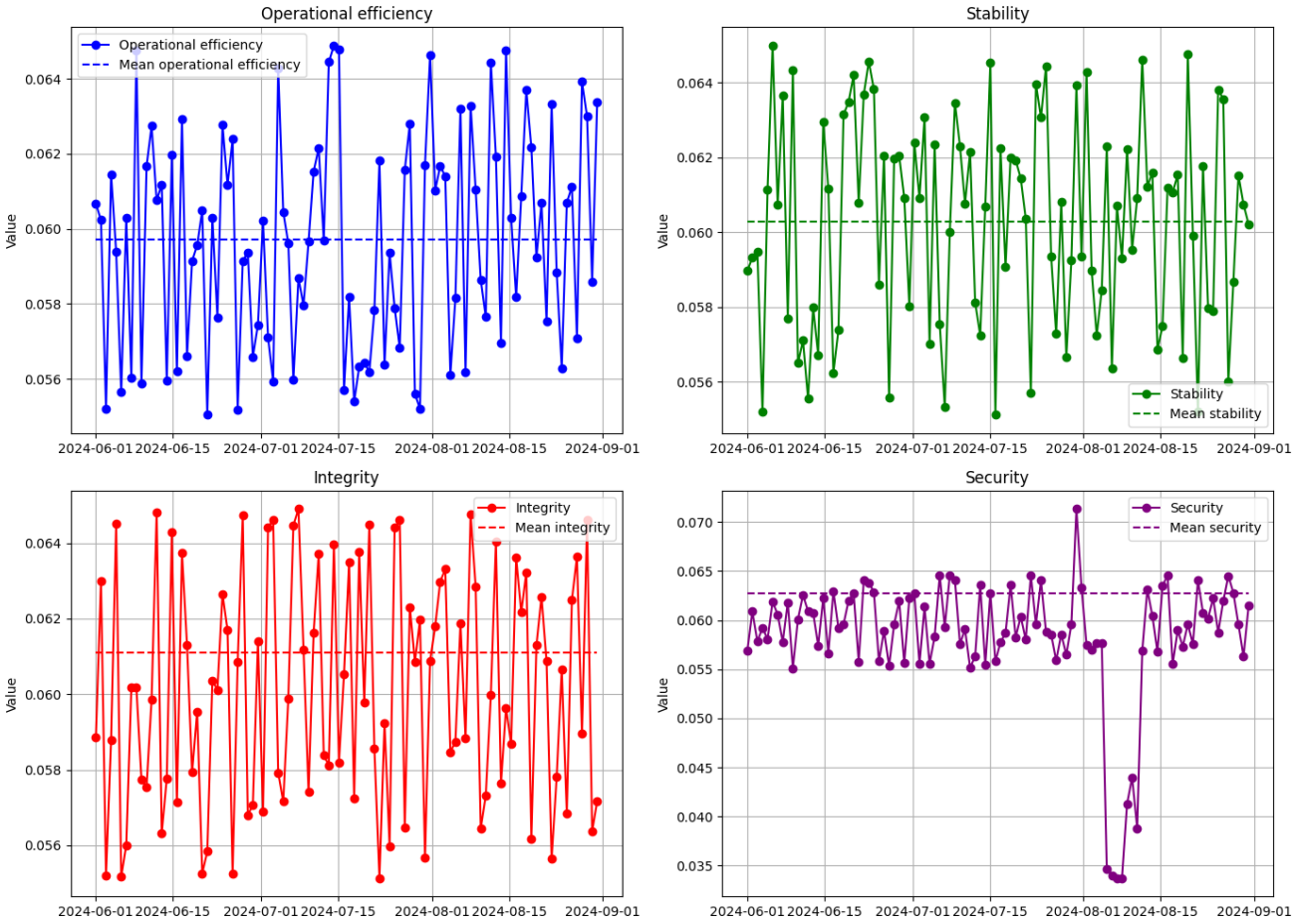


Рисунок В.9 - Графіки функцій п’ятої серії експерименту для чотирьох критеріїв

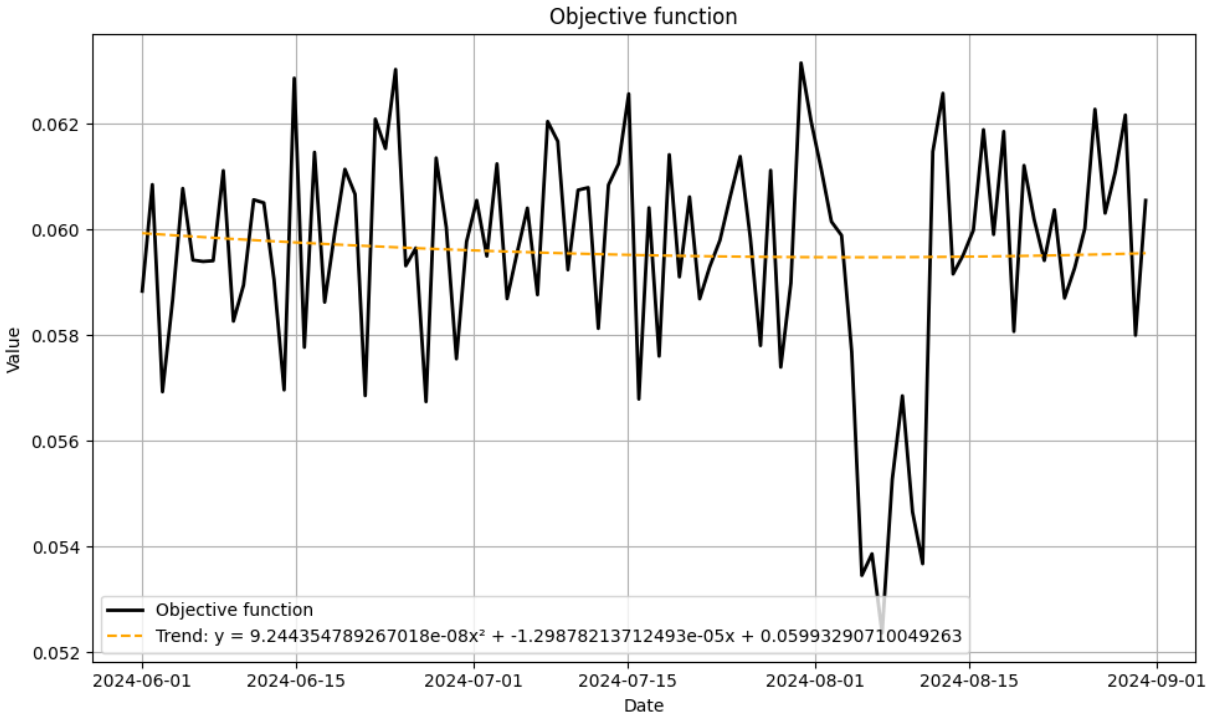


Рисунок В.10 - Графік цільової функції п’ятої серії першого експерименту

ДОДАТОК Г.
ДЕТАЛІЗАЦІЯ ДРУГОГО ЕКСПЕРИМЕНТУ

Графік залежності часу перебудови та значень цільової функції зображено на рис. Г.1.

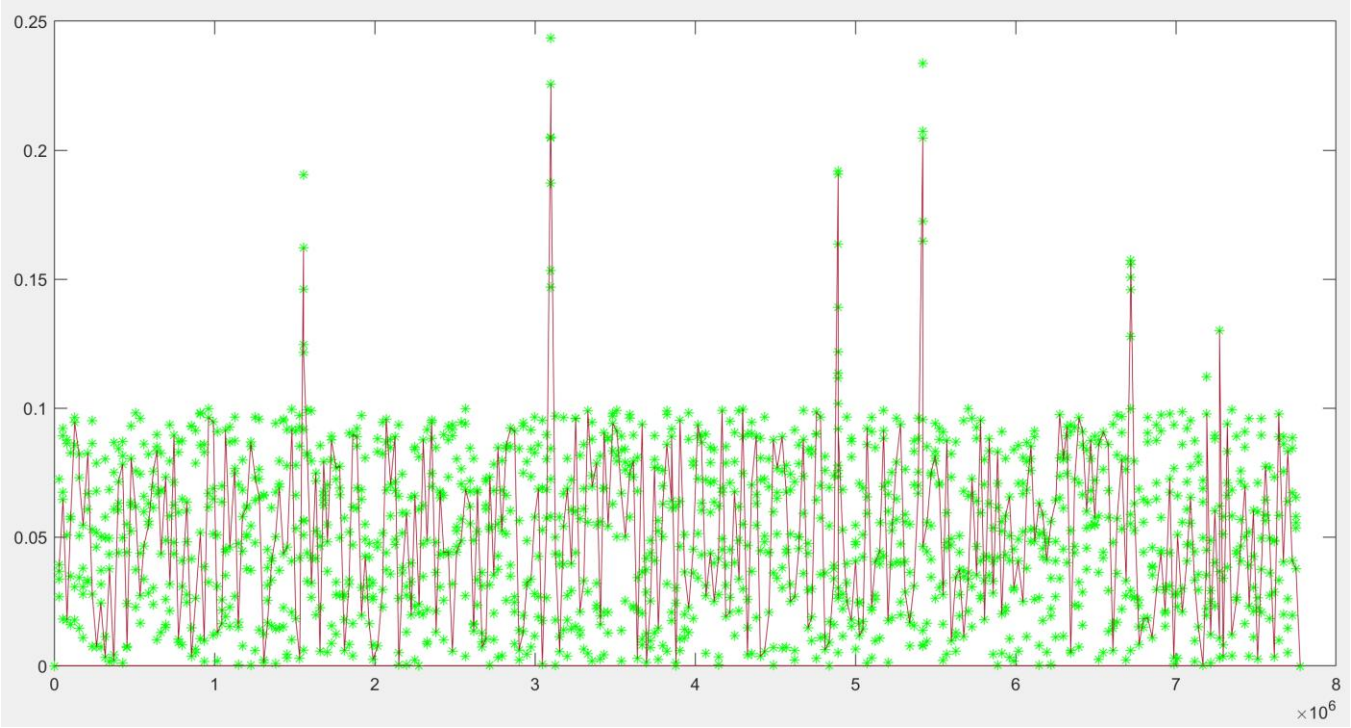


Рисунок Г.1 - Графік залежності значень цільової функції від часу функціонування системи та часу перебудови центру системи для першої серії другого експерименту

В графіку на рис. Г.1 зображено навпроти певного часу п’ять значень цільової функції. Графік є дискретним. Неперервною лінією поєднані значення варіантів, які затверджені контролером прийняття рішень системи.

Друга серія другого експерименту з системою була проведена за тими ж вимогами, що і перша серія другого експерименту. Але в другій серії другого експерименту контролера прийняття рішень в системі не було. Центр системи готував варіанти централізації, обчислював значення цільової функції для них і обирав наступним варіантом централізації той, в якому значення цільової функції було мінімальним. Результати експерименту зображено на рис. Г.2.

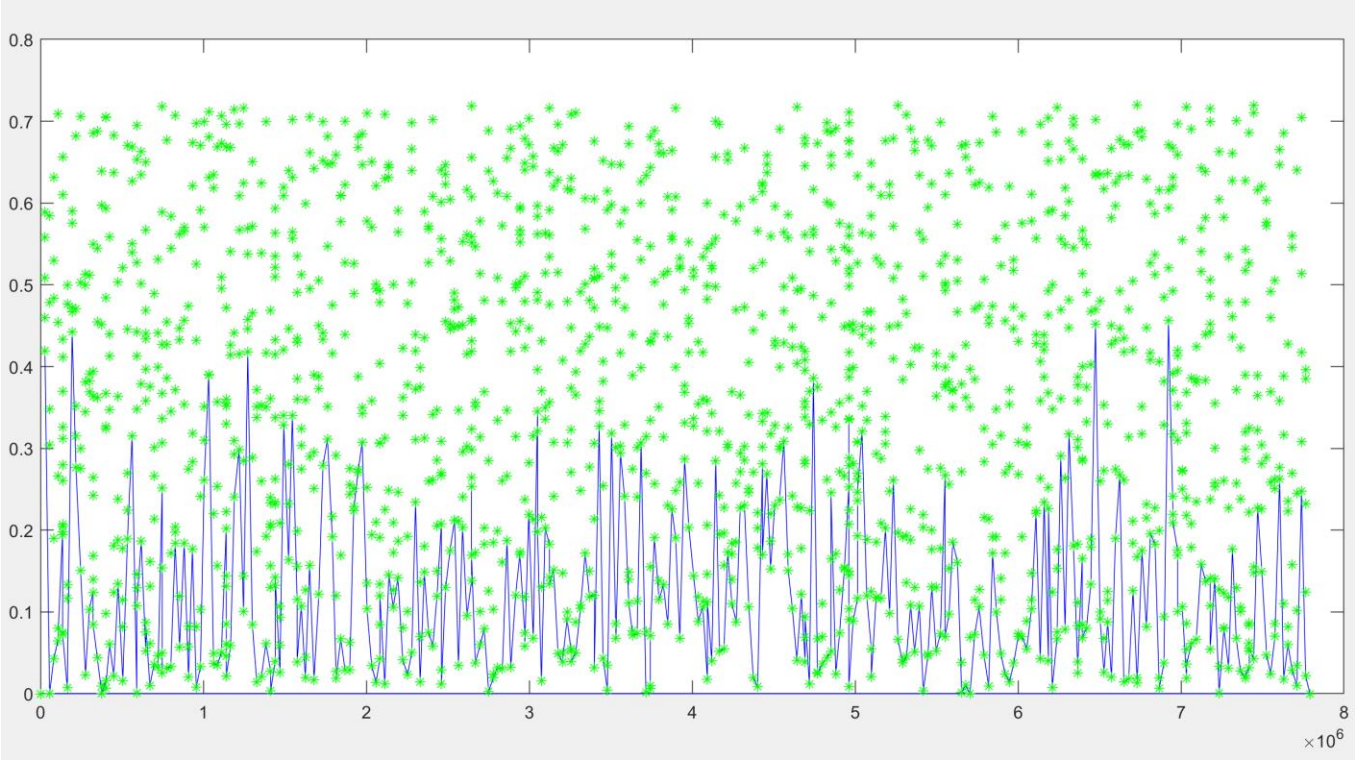


Рисунок Г.2 - Графік залежності значень цільової функції від часу функціонування системи та часу перебудови центру системи для другої серії другого експерименту

За результатами другої серії другого експерименту було встановлено, що значення цільової функції перебували переважно в інтервалі 0-0,72, що є достатньо великими і вказують на певну розбалансованість при виборі варіанту централізації. Порівняння двох серій другого експерименту показано на рис. Г.3 і рис. Г.4. Графіки для затверджених варіантів централізації відрізняються тим, що у першому експерименті значення цільової функції може обиратись не обов’язково найменше, а в другому експерименті – тільки найменше значення. Це впливатиме на подальші кроки системи з вибору варіантів централізації в архітектурі системи та її функціонування. Також, це впливатиме на формування попереднього досвіду у використанні різних параметрів для вибору наступного варіанту централізації.

Таким чином, для першої серії лругого експерименту значення цільової функції порівняно з результатами другої серії другого експерименту відображають кращу стійкість та перебування в межах інтервалу 0-0,25 протягом всього часу функціонування, незалежно від того, що наступні варіанти централізації обирались

не обов’язково з найменших значень цільової функції. У другій серії другого експерименту вибір наступних варіантів централізації проводився з обранням лише мінімальних значень цільової функції і результати функціонування характеризуються недостатньою стійкістю системи та збільшенням значення цільової функції порівняно з результатами першої серії другого експерименту на 0,5, що є достатньо великим відхиленням.

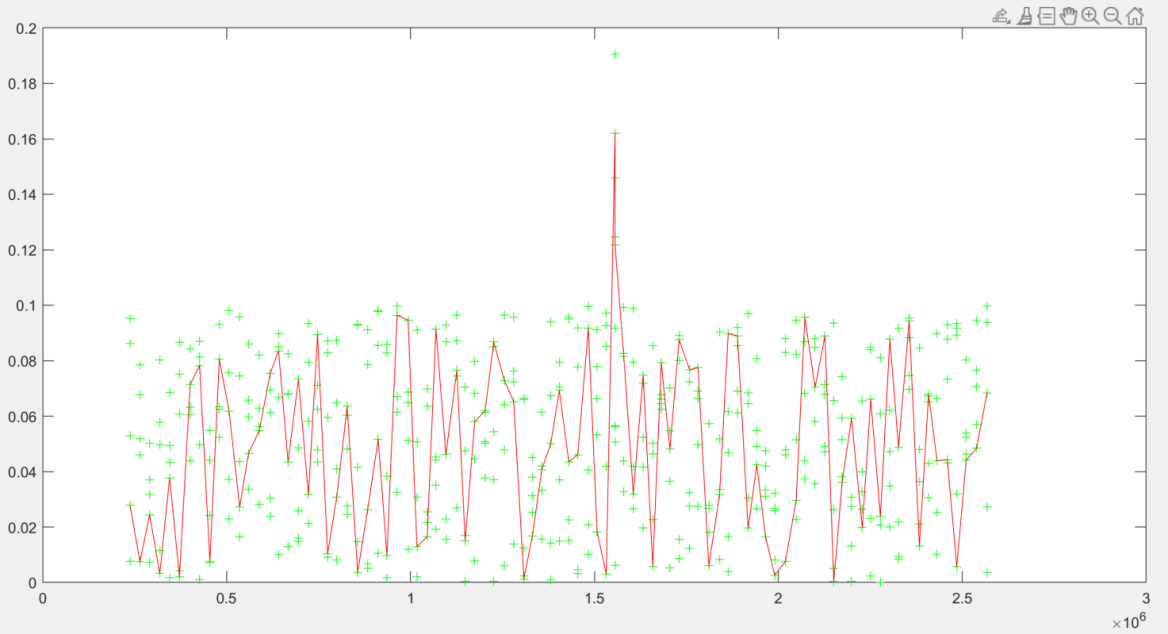


Рисунок Г.3 - Фрагмент графіку цільової функції для першої серії другого експерименту(10-100 кроки)

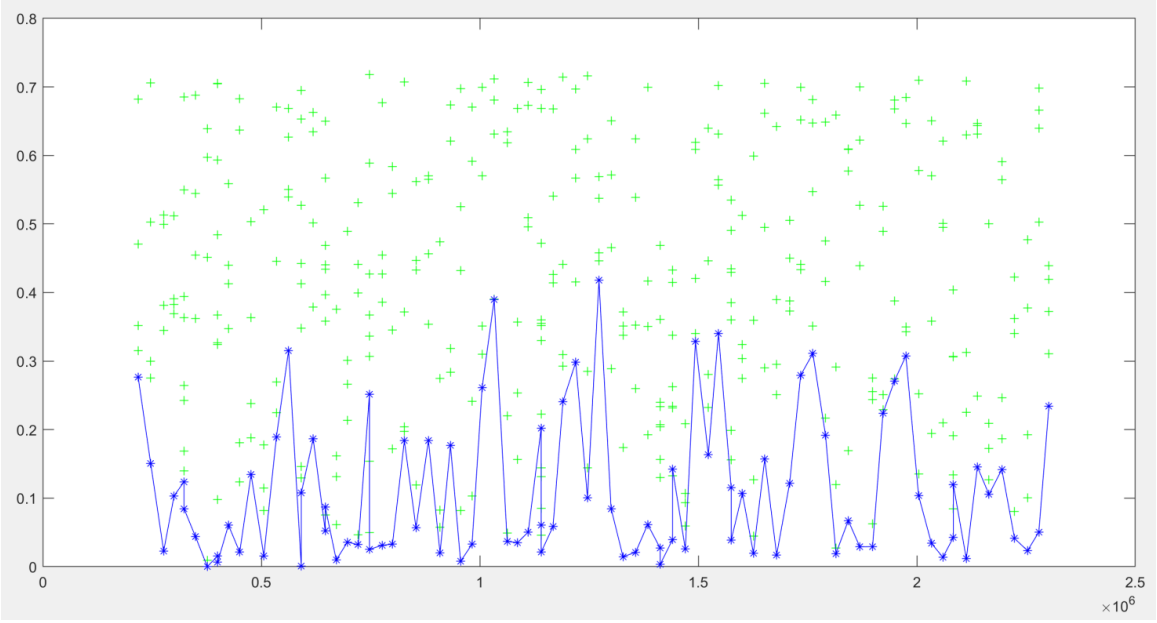


Рисунок Г.4 - Фрагмент графіку цільової функції для другої серії другого експерименту (10-100 кроки)

Кількість невдалих спроб при переході на наступного варіанту централізації у першому випадку становить одинадцять, а в другому - сорок шість. Це підтверджує кращий вибір у першому експерименті і перевагу у використанні контролера прийняття рішень. Підібрані варіанти централізації в архітектурі систем у першому випадку є більш адаптованими в контексті спроможності переходу до них. Відсоток невдалих спроб порівняно з усіма спробами в першому варіанті становить 3,2%, в другому випадку – 13,6%. Тобто, за рахунок застосування контролера прийняття рішень для визначення наступного варіанту централізації в архітектурі систем досягнуто підвищення ефективності щодо переходу системи до наступного визначеного варіанту централізації на 10%.

Час, який витрачався на здійснення переходу до наступного варіанту централізації в архітектурі систем для обох експериментів є приблизно однаковим. Але в другій серії другого експерименту через велику кількість невдалих спроб переходу до наступного варіанту централізації витрати часу є більшими, оскільки час витрачено на невдалі спроби, виконання яких із зміненими варіантами в подальшому потрібно знову повторити. При цьому було додатково витрачено час на їх реалізацію, що становило приблизно 10,5% від загального часу, який було витрачено на всі спроби зміни варіанту централізації в архітектурі системи.

При виборі наступного варіанту централізації в архітектурі систем в першій серії другого експерименту п’яте правило було застосоване десять разів, шосте правило – один раз. Це означає, що при повторній спробі перейти до наступного варіанту централізації в архітектурі системи було дві невдалі спроби і, тому було застосоване шосте правило. Для другої серії другого експерименту п’яте правило було застосоване сорок п’ять разів, шосте правило – один раз. Це є аналогічним до першого експерименту в контексті двох невдалих спроб підряд при здійсненні переходу. Крім того, застосування п’ятого правила сорок п’ять разів підтверджує аналіз витрат часу, який було використано на невдалі спроби.

Вибір наступного варіанту централізації в архітектурі мультикомп’ютерних систем з використанням контролера прийняття рішень забезпечує подальшу стабільну роботу системи. Це відображається значеннями цільової функції, дисперсія яких перебуває в малому інтервалі. Результати експерименту підтверджують

коректність та адекватність використання розробленої цільової функції для оцінювання наступного варіанту централізації в архітектурі систем. Різниця між дисперсіями в обох варіантах експериментів становить приблизно 50%. Це дає змогу однозначно виокремити використання контролера прийняття рішень як доцільну складову частину систем при виборі наступного варіанту централізації.

ДОДАТОК Д.
ДЕТАЛІЗАЦІЯ ТРЕТЬОГО ЕКСПЕРИМЕНТУ

Перша частина

Графіки дискретних функцій для всіх чотирьох критеріїв (стійкість, оперативність, цілісність, безпека) зображено на рис. Д.1 – рис. Д.4 за увесь час функціонування системи. Значення функцій для критеріїв позначено точками. На їх основі визначено графік кривої тренду.

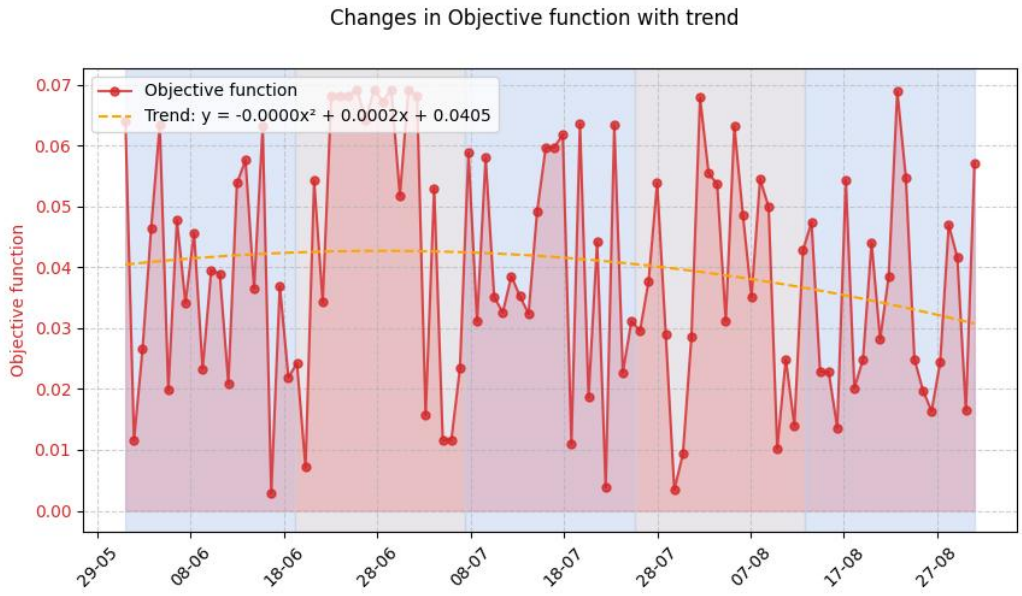


Рисунок Д.1 – Графік функції для критерію стійкості

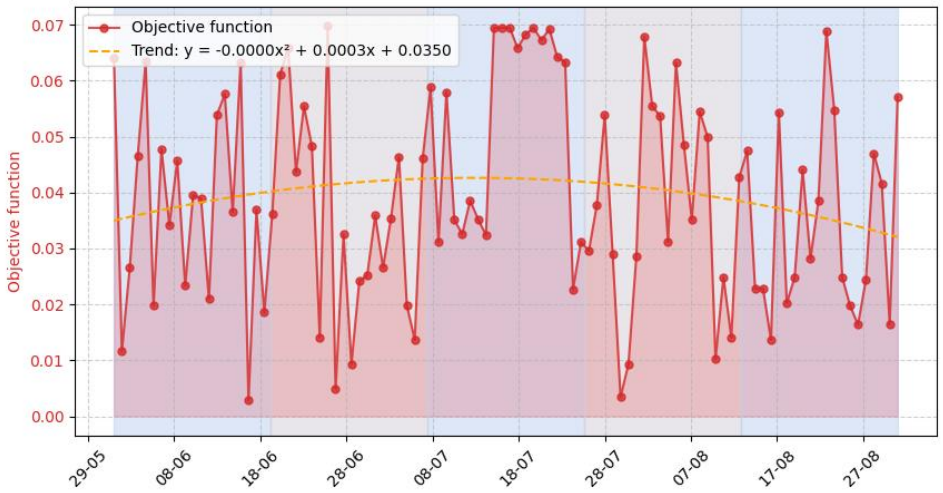


Рисунок Д.2 – Графік функції для критерію оперативності для першого випадку

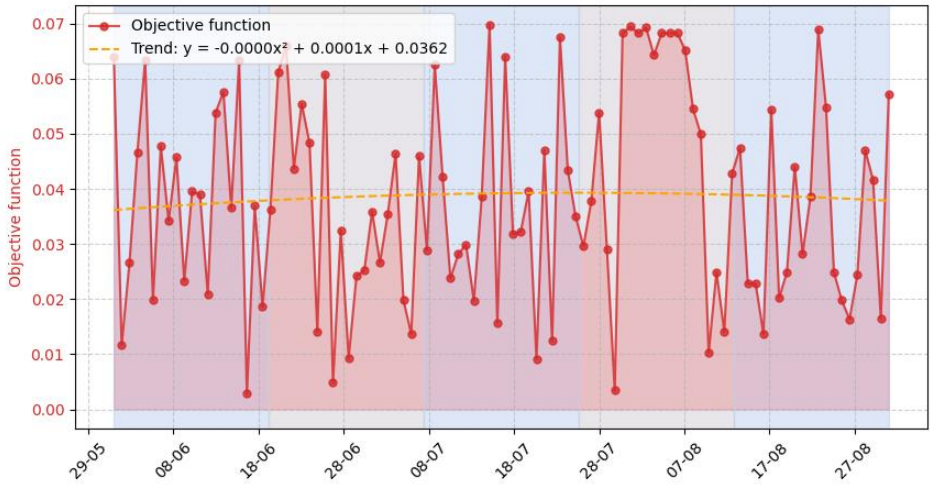


Рисунок Д.3 – Графік функції для критерію цілісності для першого випадку

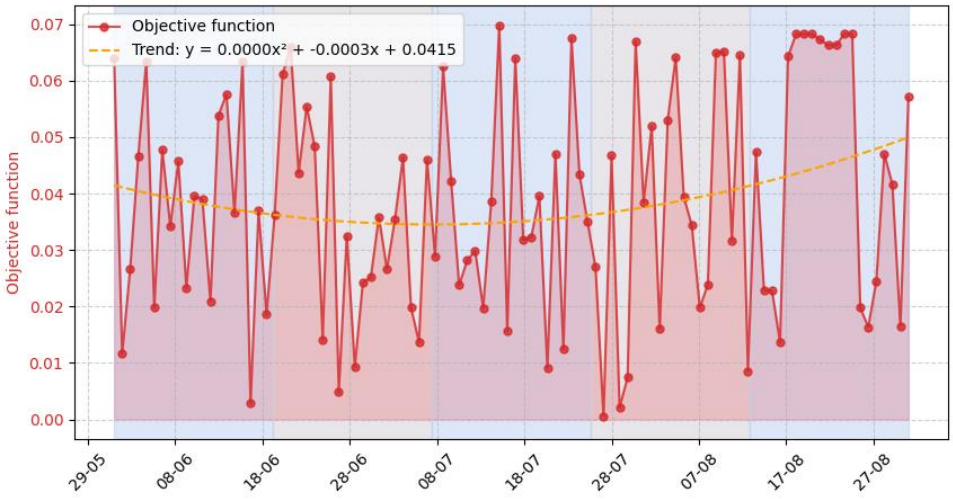


Рисунок Д.4 – Графік функції для критерію безпеки для першого випадку

Під час функціонування системи було досліджено її спроможність до продовження в умовах внутрішніх і зовнішніх впливів. Для дослідження такої спроможності увесь час функціонування системи було розділено на п’ять приблизно однакових проміжків. На першому проміжку система функціонувала в штатному режимі. На другому проміжку було здійснено вплив на значення критерію стійкості, яке було суттєво віддалено від його значення в штатному режимі, тобто його значення перебувало в критичній зоні. Аналогічно на наступних проміжках: третій проміжок – критерій оперативності; четвертий проміжок – критерій цілісності; п’ятий проміжок – критерій безпеки.

Графік цільової функції для першого випадку зображено на рис. Д.5.

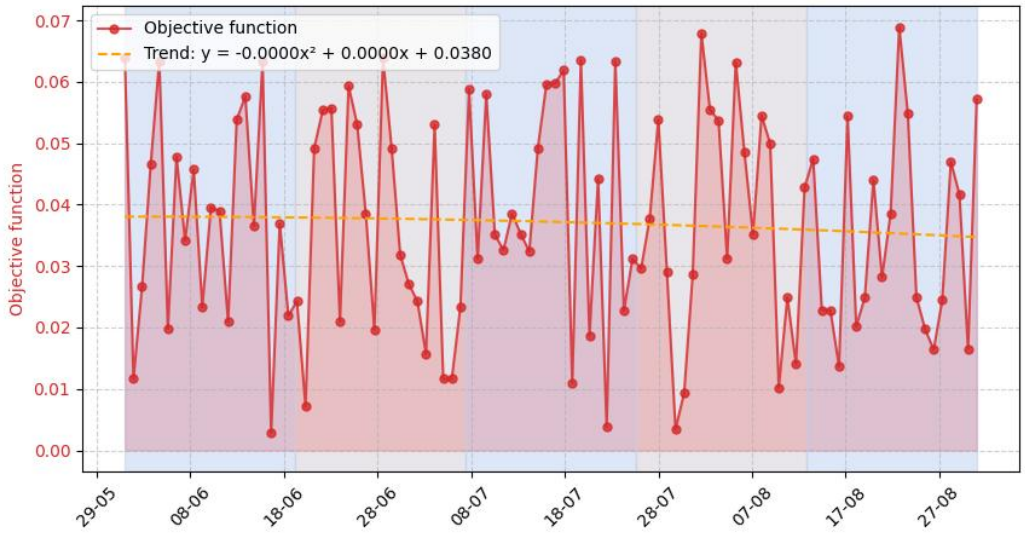


Рисунок Д.5 – Графік цільової функції для першого випадку

На всіх графіках з рис. Д.1 – рис. Д.5 найбільші відхилення від нульового значення є такими, що можуть бути критичними значеннями. Тобто, чим більші значення тим критичнішою є робота системи. І навпаки, якщо значення функцій наближені до нульового значення, то робота системи є кращою. Для кожного графіку, який визначено точками з реального експерименту, побудовано теоретичну криву тренду для оцінювання системи на наступних кроках та для порівняння їх між собою. Порівняння теоретичних кривих тренду підтверджує спроможність функціонування системи в штатному режимі незалежно від внутрішніх та зовнішніх впливів. Тобто, наявність контролера прийняття рішень, який враховує попередній досвід функціонування системи, дає змогу системі зберігати належний стан функціонування.

Друга частина

Аналогічно до першого випадку для другого випадку, також, побудовано графіки функцій для критеріїв стійкості, оперативності, цілісності та безпеки на рис. Д.6 – рис. Д.10 відповідно. Для всіх критеріїв, аналогічно, до першого випадку було розподілено на п’ять часових проміжків функціонування системи і внесено впливи за кожним критерієм окремо, щоб уникнути впливу на два і більше критеріїв в один і той же проміжок часу. Цим забезпечено якість експерименту. Для деяких критеріїв

вплив на параметри одного з них все-таки призводить до впливу на ті ж параметри другого критерію, але таких спільних параметрів небагато. При цьому кожен критерій розроблено з врахування великої кількості параметрів, щоб уникнути великої кореляції між ними. Тому, вплив на спільні параметри є несуттєвим. Це було підтверджено графіками на рис. Д.1 - рис. Д.4. Вплив на один критерій в певному проміжку часу не було видно на решті графіків з суттєвим відхиленням від нульового значення.

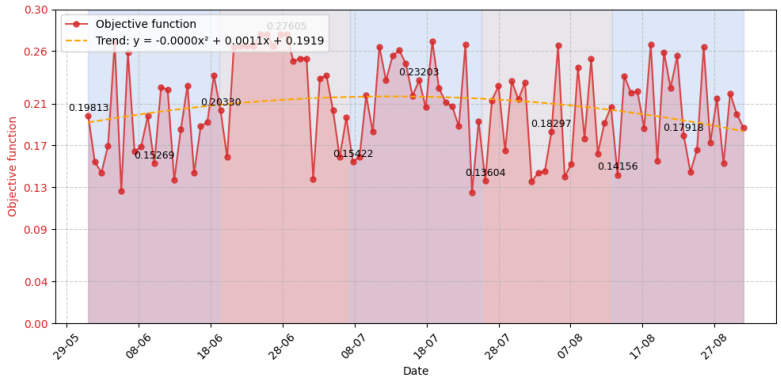


Рисунок Д.6 – Графік функції для критерію стійкості для другого випадку

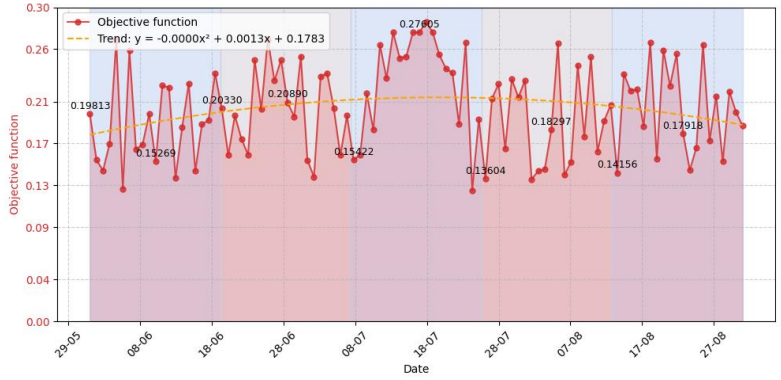


Рисунок Д.7 – Графік функції для критерію оперативності для другого випадку

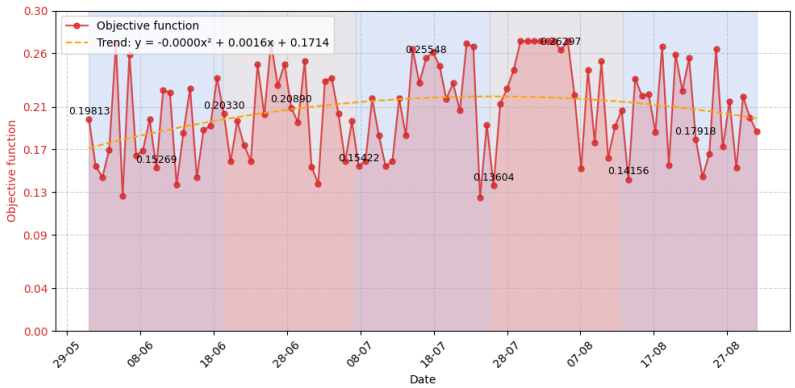


Рисунок Д.8 – Графік функції для критерію цілісності для другого випадку

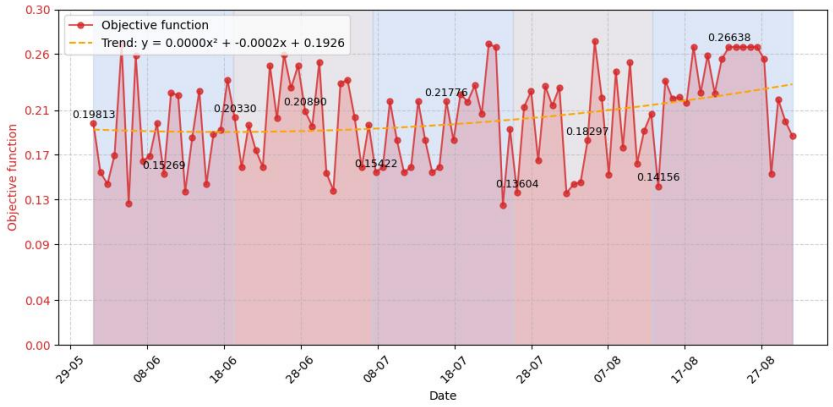


Рисунок Д.9 – Графік функції для критерію безпеки для другого випадку

Графік цільової функції для другого випадку зображено на рис. Д.10. Також зображено на рис. Д.6 – рис. Д.9 теоретичну криву тренду.

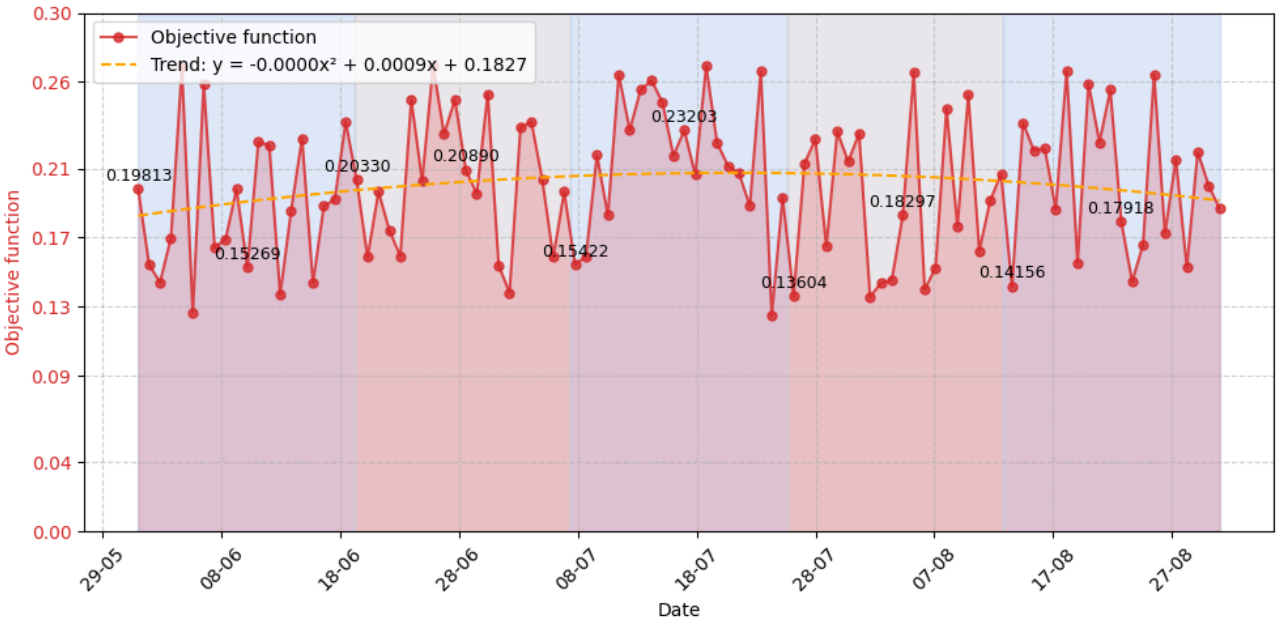


Рисунок Д.10 – Графік цільової функції для другого випадку

Результати для другого випадку відображають погіршення значень функцій для критеріїв і цільової функції зокрема. Тобто, для випадку функціонування системи без контролера прийняття рішень, а лише з вибором одного варіанту для опрацювання події, функціонування системи на протязі певного часу погіршується та деградує.

Загальний аналіз результатів третього експерименту. В результаті проведеного експерименту з системою в двох випадках з контролером прийняття рішень та без нього, встановлено покращення функціонування мультикомп’ютерної системи у

випадку функціонування з контролером. Такий результат підтверджено значеннями цільової функції, які є оцінками потенційних варіантів виконання завдань. В першому випадку з контролером прийняття рішень значення цільової функції знаходяться в межах інтервалу [0,002; 0,07], що відповідають цільовій меті функції. В другому випадку значення цільової функції, які обчислені без врахування попереднього досвіду функціонування системи та при цьому не було використано контролер прийняття рішень, для кожного окремого варіанту виконання завдань знаходяться в інтервалі [0,11; 0,28]. Такіці значення суттєво відхиляються нуля, тобто від цільового значення. Ці значення з другого випадку, також, суттєво відрізняються від значень для першого випадку. Це відхилення становить приблизно 17 відсотків. Все це впливає на стабільність функціонування системи в другому випадку.

Врахування попереднього досвіду функціонування системи при виборі варіантів виконання завдання зображено в табл. 6.7 в стовпцях 13-15. Для розглянутих даних значення цільової функції оцінювання на наступних кроках функціонування системи є меншим від значення попереднього використаного варіанту, що вказує на спроможність системи до покращення свого функціонування за рахунок врахування попереднього досвіду функціонування.

ДОДАТОК Е.
ДЕТАЛІЗАЦІЯ ЧЕТВЕРТОГО ЕКСПЕРИМЕНТУ

Перша частина

Контролер при проведенні експерименту буде налаштований так, що кожного третього і шостого етапу при повторенні впливів буде вибирати відповідь другу за рейтингом, а кожного дев'ятого разу третю відповідь за рейтингом. Тоді, мінімальна кількість етапів експериментів від початкового повинна дорівнювати десять, бо включатиме і перший етап. Для продовження дослідження після десятого етапу потрібно провести дев'ять експериментів, щоб забезпечити відповідність етапам з другого по десятий, тобто виконати повну ітерацію. Але кількість етапів може дорівнювати не обов'язково десять, дев'ятнадцять, двадцять вісім тощо. Вона може бути іншою і визначатись тим, що на двох сусідніх етапах чи трьох сусідніх етапах в залежності від сформованих вимог буде досягнуто належного рівня достовірності виявлення метаморфних вірусів.

Важливою складовою частиною четвертого експерименту є набір тестових зразків метаморфних вірусів та коректне їх використання, оскільки всі вони мають функціонал, який передбачає втілення у виконувані PE-файли. Для проведення експерименту виберемо для кожної з підмножин $\mathfrak{H}_{\mathfrak{k}}$ ($\mathfrak{k} = 1,2, \dots, 12$) по п'ять різних, але при цьому таких, що мають характерні ознаки класу, метаморфних вірусів. Їх конструювання було здійснено щтучно без включення зловмисного функціоналу. Таким чином, кількість зразків різних метаморфних вірусів для проведення експерименту буде дорівнювати шістдесят. Загальною моделлю всіх шістдесяти метаморфних вірусів буде пошук виконуваного PE-файлу та його інфікування за типом, що визначає один з класів $\mathfrak{H}_{\mathfrak{k}}$ ($\mathfrak{k} = 1,2, \dots, 12$) і він повинен бути такого типу як запущений на виконання метаморфний вірус.

Корисні програми, тобто програми користувача, повинні теж виконуватись при проведенні четвертого експерименту. Виберемо в корпоративній мережі двадцять п'ять комп'ютерних станцій, які будуть знаходитись мінімум в трьох її сегментах. Решту комп'ютерних станцій вимкнемо. Встановимо в кожну з них компоненти

системи і проведемо її первинні налаштування та запуски. При проведенні серій експериментів на різних етапах дії із встановлення компонентів системи будемо повторювати, щоб забезпечити їх незалежність, для всіх окремих дванадцяти типів метаморфних вірусів, які задані відповідними класами $\mathfrak{H}_{\mathfrak{k}}$ ($\mathfrak{k} = 1,2, \dots, 12$). Для кожного типу метаморфних вірусів мультикомп'ютерна система перевстановлюватись не буде. Вона буде накопичувати знання в елементах пам'яті для використання їх контролером. Таким чином, незалежність експерименту буде стосуватись винятково класів $\mathfrak{H}_{\mathfrak{k}}$ ($\mathfrak{k} = 1,2, \dots, 12$). В кожному з двадцяти п'яти вузлів, в які встановлені компоненти мультикомп'ютерної системи, будуть запущені тільки системні процеси та по одному досліджуваному процесу. В двадцяти чотирьох вузлах будуть запущені на виконання різні двадцять чотири процеси, які будуть орієнтовані на використання введення-виведення для забезпечення тривалості виконання. Після повного виконання заданого користувацького процесу буде повторення його виконання до завершення серії експерименту за встановленим часом. В одному з вузлів буде запускатись метаморфний вірус. Час для проведення серії четвертого експерименту буде визначено з врахуванням часу витраченого на виконання метаморфного вірусу та обробки подій, які пов'язані з ним, в мультикомп'ютерній системі. Час для всіх серій експерименту буде однаковим і визначений експериментальним шляхом під час попередніх серій експерименту. Для визначеного набору початкових даних планованого експерименту встановимо час проведення серії експериментів тривалістю 30 хвилин. Для метаморфного вірусу приманками будуть використовуватись однакові виконувані PE-файли, як об'єкти його атак для подальшого інфікування. Ці файли-приманки для конкретного вузла будуть однаковими за набором біт, але різними за найменуваннями. Вони будуть розміщуватись в усіх каталогах та корневому каталозі.

Проведення четвертого експерименту та результати експериментальних досліджень. Для проведення експериментальних досліджень з розробленою мультикомп'ютерною системою в кожному визначеному вузлі корпоративної мережі було здійснено запуск заданих виконуваних програм в однаковий час. Для цього було використано однакову програму запуску із встановленим в ній часом запуску. Всі дослідження проведені в ізольованому середовищі корпоративної мережі. Результати

всіх серій четвертого експерименту було збережено окремо разом з файлами-логами та таблицями елементів пам’яті. Мультикомп’ютерна система досліджувала всі виконувані процеси, які намагались здійснити пошук в комп’ютерній станції виконуваних PE-файлів та дослідити місце їх точки входу. Такі функції були у всіх запущених програмах-приманках. Тільки в одній з них буде метаморфний вірус, який на відміну від решти програм міг втілювати програмний код в програму-приманку. Метаморфних вірусів певного типу було п’ять екземплярів класу і з кожним було окремо проведено серії експериментів. Серій кожного етапу експерименту було проведено по три. Таким чином, разом загальна кількість базових експериментальних досліджень за серіями становила сто вісімдесят повторень для одного етапу.

Аналіз результатів експериментальних досліджень з розробленою мультикомп’ютерною системою було проведено за двома критеріями: дослідження достовірності виявлення метаморфних вірусів на окремих етапах з врахуванням всіх особливостей штучно створених екземплярів класів; дослідження окремих типів штучно створених екземплярів класів на всіх етапах. Для другого випадку кількість етапів буде збіжною з встановленою експериментально кількість потрібних етапів першого випадку. Аналіз першого випадку буде відображати вплив на систему в явному вигляді контролера. В другому випадку наявність контролера буде відображатись в неявному вигляді через накопичення результатів і їх усереднення в числовому ряді. Але великі відхилення за типами екземплярів класів від отриманого результуючого значення з першого випадку буде відображувати особливості їх архітектури. Тому, якщо відхилення будуть невеликі, то потрібно буде ускладнювати архітектуру тих екземплярів класу і проводити експериментальні дослідження повторно. Таким чином, другий випадок буде верифікувати якість тестових зразків.

Для оцінювання ефективності підходу виявлення були використані метрики TPR – True Positive Rate, FPR – False Positive Rate, Precision, Recall, F1-score та MCC [61]:

$$FPR = \frac{TP}{TP+FN} * 100\,. \tag{E.1}$$

$$FPR = \frac{FP}{TN+FP} * 100. \tag{E.2}$$

$$S_P = \frac{TN}{TP+FN} * 100. \tag{E.3}$$

$$Precision = \frac{TP}{TP+FP}. \quad \text{(E.4)}$$

$$Recall = \frac{TP}{TP+FN}. \quad \text{(E.5)}$$

$$F1 = \frac{2*Recall*Precision}{Recall+Precision}. \quad \text{(E.6)}$$

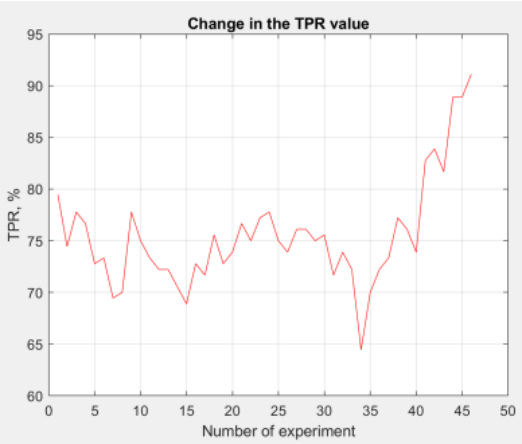
$$MCC = \frac{TP*TN-FP*FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}. \quad \text{(E.7)}$$

МКК (коефіцієнт кореляції Метьюза) [61] визначається від -1 до 1, де ±1 означає повну згоду або незгоду, а нульове значення означає відсутність зв'язку. Коефіцієнт кореляції має максимальне значення, яке визначається розподілом двох змінних, якщо одна або обидві змінні можуть приймати більше двох значень.

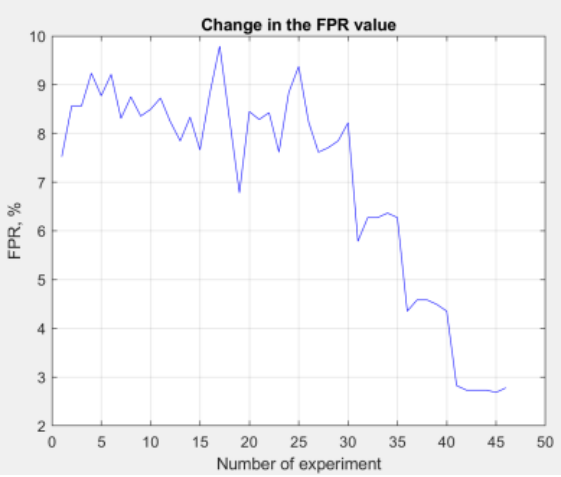
Друга частина

Зміну значень основних показників аналізу при виконанні 46 етапів зображено на рис. Е.1. На рис. Е.1а) графік функції показує зростання значення достовірності виявлення метаморфічних вірусів в процесі наповнення системи інформацією про її попередні кроки. Результат виявлення розробленої мультикомп'ютерної системи досяг 90 відсотків, що є достатнім базовим показником. На рис. Е.1б) зображено графік для частоти помилкових спрацьовувань і графік є спадним, демонструючи поліпшення класифікації системи програм, які не містять метаморфного функціоналу. Відсоток помилкових спрацьовувань становить 3% і він покращився приблизно на 6%, що підтверджує необхідність використання інформації про результати попередніх етапів виявлення метаморфічних вірусів.

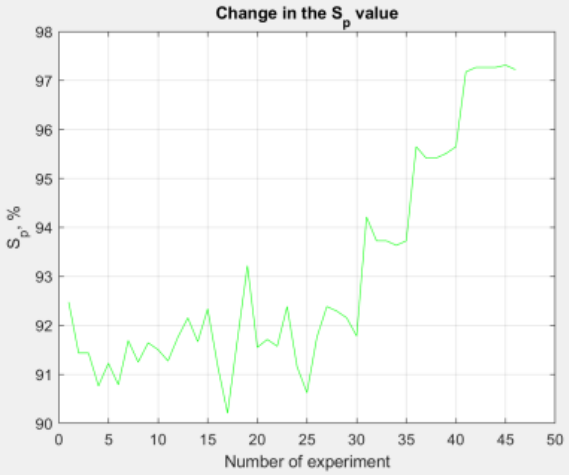
Аналогічно на рис. Е.1б) і рис. Е.1в) показаний результат класифікації програм без метаморфного функціоналу і результат становить близько 97%, що прийнятно для подальших удосконалень розроблюваної мультикомп'ютерної системи.



а)



б)



с)

Рисунок Е.1 - Графіки для функцій з табл. 6.12

Третя частина

Експеримент включав в себе серію тестів, в кожному з яких метаморфні віруси запускались на одному з компонентів (ініціаторі завдання) системи. Щоразу на

компоненті-ініціаторі запускалася процедура аналізу цього файлу за методом виявлення метаморфних вірусів.

За допомогою дизасемблера було розібрано метаморфний вірус та отримано зразок коду для виконання в ізольованому віртуальному середовищі (у вигляді списку кодів операцій та набору функцій API). Щоб отримати зразок коду, після виконання він був запущений в ізольованому середовищі. Після виконання виконуваного файлу в ізольованому середовищі було проведено його повторне розбирання. Далі було проведено формування вектору ознак схожості кодового зразка з метаморфним вірусом на основі реалізованого методу формування вектору ознак схожості кодового зразка з метаморфним вірусом. Потім за допомогою вбудованої в запропоновану систему нечіткого висновку було проведено ідентифікацію метаморфного вірусу.

Якщо показник «Рівень подібності до метаморфічного вірусу» отримував значення Medium (тобто однозначно ідентифікувати приналежність тестового зразка до одного з класів метаморфних вірусів засобами одного хоста не вдавалося), то тестовий зразок відправлявся на інші компоненти мультикомп'ютерної системи з метою їх запуску в ізольованих середовищах і прояву метаморфних властивостей.

На рис. Е.2 зображено приклад двох списків кодів операцій для одного екземпляру виконуваної прогарми з метаморфним функіоналом, отриманих після запуску і дизасемблювання на різних хостах системи. Модифіковані блоки маркуються червоними квадратами.

```
endbr64
push   %rbp
mov    %rsp,%rbp
push   %rbx
sub    $0x218,%rsp
mov    %fs:0x28,%rax
mov    %rax,-0x18(%rbp)
xor    %eax,%eax
lea    0xd99(%rip),%rax        # 0x2008
mov    %rax,%rsi
lea    0x2dc7(%rip),%rax        # 0x4040 <_ZSt4cout@GLIBCXX_3.4>
mov    %rax,%rdi
call   0x10f0 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
lea    -0x220(%rbp),%rax
mov    $0x10,%edx
lea    0xd7c(%rip),%rcx        # 0x2010
mov    %rcx,%rsi
mov    %rax,%rdi
call   0x1100 <_ZNSt14basic_ofstreamIcSt11char_traitsIcEEC1EPKcSt13_Ios_Openmode@plt>
lea    -0x220(%rbp),%rax
mov    %rax,%rdi
call   0x10d0 <_ZNSt14basic_ofstreamIcSt11char_traitsIcEE7is_openEv@plt>
test   %al,%al
je     0x12f5 <main+172>
lea    -0x220(%rbp),%rax
lea    0xd60(%rip),%rdx        # 0x2020
mov    %rdx,%rsi
mov    %rax,%rdi
call   0x10f0 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
lea    -0x220(%rbp),%rax
mov    %rax,%rdi
call   0x1120 <_ZNSt14basic_ofstreamIcSt11char_traitsIcEE5closeEv@plt>
lea    0xd5f(%rip),%rax        # 0x2040
mov    %rax,%rsi
lea    0x2d55(%rip),%rax        # 0x4040 <_ZSt4cout@GLIBCXX_3.4>
mov    %rax,%rdi
call   0x10f0 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
jmp    0x1315 <main+204>
lea    0xd7c(%rip),%rax        # 0x2078
mov    %rax,%rsi
lea    0x2e5a(%rip),%rax        # 0x4160 <_ZSt4cerr@GLIBCXX_3.4>
```

а)

```
endbr64
push   %rbp
mov    %rsp,%rbp
sub    $0x10,%rsp
mov    %fs:0x28,%rax
mov    %rax,-0x8(%rbp)
xor    %eax,%eax
lea    0xddc(%rip),%rax        # 0x2017
mov    %rax,%rsi
lea    0x2dfb(%rip),%rax        # 0x4040 <_ZSt4cout@GLIBCXX_3.4>
mov    %rax,%rdi
call   0x10c0 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
lea    -0x10(%rbp),%rax
mov    $0x0,%ecx
lea    -0x74(%rip),%rdx        # 0x11e9 <_Z14threadFunctionPv>
mov    $0x0,%esi
mov    %rax,%rdi
call   0x10f0 <pthread_create@plt>
mov    -0x10(%rbp),%rax
mov    $0x0,%esi
mov    %rax,%rdi
call   0x10b0 <pthread_join@plt>
mov    $0x0,%eax
mov    -0x8(%rbp),%rdx
sub    %fs:0x28,%rdx
je     0x1294 <main+123>
call   0x10d0 <__stack_chk_fail@plt>
leave
ret
```

б)

Рисунок Е.2 - Два списки кодів операцій досліджуваної виконуваної прогарми після запуску та розбирання на різних хостах системи: а) хост 1; б) ведучий 3

Після виконання аналогічних симетричних дій над кожним з компонентів системи результати аналізу були відправлені в компоненту-ініціатор. Фрагмент журналу на компоненті ініціатора зображено на рис. Е.3. Після додаткової перевірки за допомогою інших компонентів системи було проведено остаточне формування висновку.

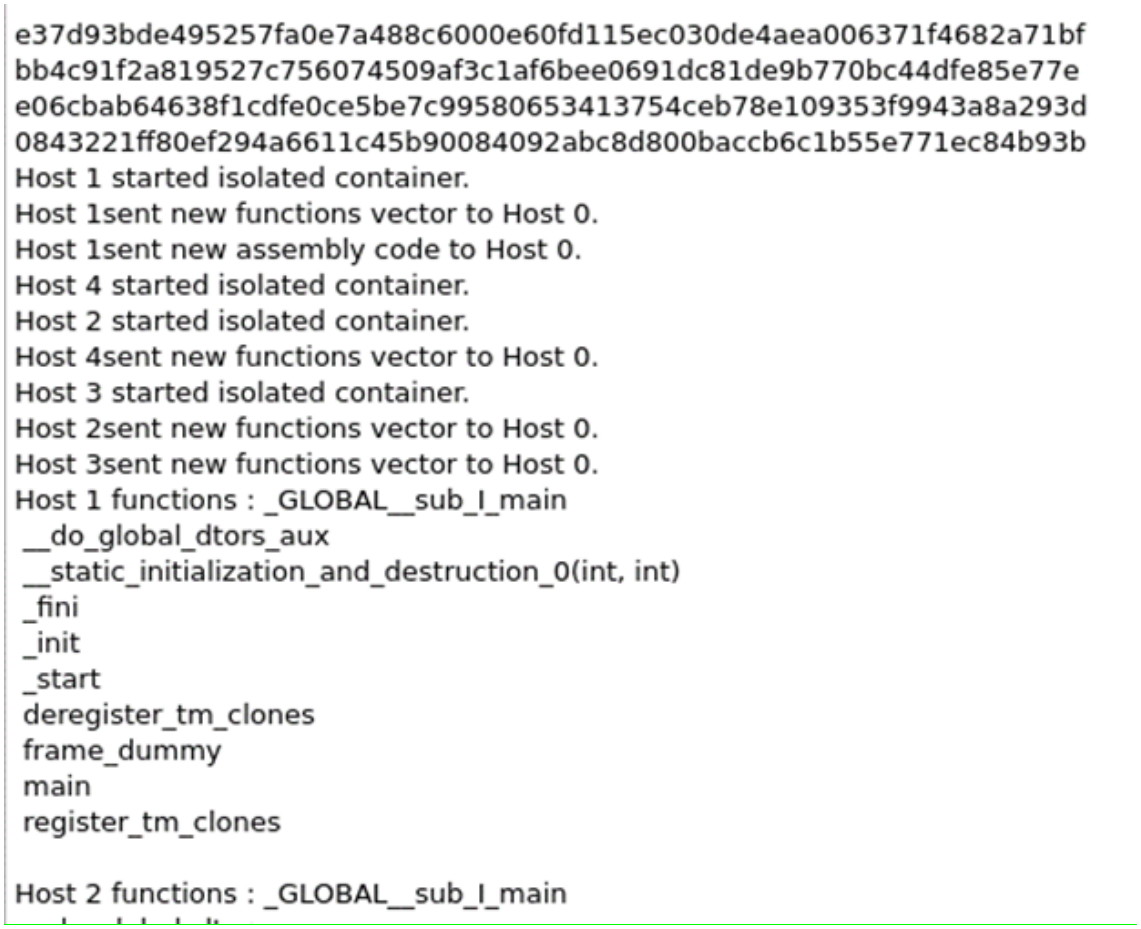


Рисунок Е.3 - Фрагмент журналу, що ілюструє прийом списку функцій API компонентом Host0 від решти компонентів мультикомп'ютерної системи

ДОДАТОК Є.

РЕЗУЛЬТАТИ ПЕРШОГО ЕКСПЕРИМЕНТУ

Таблиця Є.1

Перша серія експериментів

№	Час, с	Оперативність	Стійкість	Цілісність	Безпека	Цільова функція
1	2	3	4	5	6	7
1	0,00E+00	0,060488135	0,061778165	0,058117959	0,064065555	0,061112454
2	7,94E+04	0,062151894	0,05770008	0,061963435	0,062740473	0,06113897
3	1,59E+05	0,061027634	0,06235194	0,058777518	0,058331452	0,060122136
4	2,38E+05	0,060448832	0,064621885	0,056796037	0,055811014	0,059419442
5	3,18E+05	0,059236548	0,057487531	0,055246787	0,059072412	0,05776082
6	3,97E+05	0,061458941	0,060761573	0,055672496	0,057322341	0,058803838
7	4,77E+05	0,059375872	0,060920419	0,061793928	0,056324876	0,059603774
8	5,56E+05	0,06391773	0,060722519	0,059536968	0,055534272	0,059927872
9	6,35E+05	0,064636628	0,057230816	0,060365792	0,062255944	0,061122295
10	7,15E+05	0,058834415	0,06452749	0,063966713	0,055114275	0,060610723
11	7,94E+05	0,06291725	0,059471254	0,064903389	0,062705807	0,062499425
12	8,74E+05	0,060288949	0,063464087	0,05716897	0,056469466	0,059347868
13	9,53E+05	0,060288949	0,061994793	0,061630782	0,055795221	0,059927436
14	1,03E+06	0,060288949	0,05797437	0,057633224	0,05589603	0,057948143
15	1,11E+06	0,055710361	0,063137978	0,05520651	0,061720478	0,058943832
16	1,19E+06	0,055871293	0,058965057	0,062583787	0,057453672	0,058718452
17	1,27E+06	0,055202184	0,063811032	0,058200172	0,059205395	0,059104696
18	1,35E+06	0,063326198	0,060812729	0,058834639	0,060573688	0,060886814
19	1,43E+06	0,062781568	0,063817354	0,060883171	0,063605512	0,062771901
20	1,51E+06	0,063700121	0,061925316	0,063310485	0,062270443	0,062801591
21	1,59E+06	0,064786183	0,062252543	0,061289818	0,057703279	0,061507956
22	1,67E+06	0,062991586	0,060013244	0,063726507	0,056314828	0,060761541
23	1,75E+06	0,059614794	0,064560836	0,05773542	0,055553743	0,059366198
24	1,83E+06	0,062805292	0,061439902	0,062980468	0,058015986	0,061310412
25	1,91E+06	0,056182744	0,05923855	0,056856359	0,057621181	0,057474709
26	1,99E+06	0,06139921	0,061063932	0,064527917	0,059561406	0,061638116
27	2,06E+06	0,056433533	0,055191932	0,061874883	0,061832813	0,05883329
28	2,14E+06	0,064446689	0,058015748	0,057155077	0,061956254	0,060393442
29	2,22E+06	0,060218483	0,061601735	0,064473706	0,057835188	0,061032278
30	2,30E+06	0,059146619	0,057900776	0,062308558	0,05879927	0,059538806
31	2,38E+06	0,057645556	0,061180154	0,057539416	0,05681151	0,058294159
32	2,46E+06	0,062742337	0,059287687	0,05713312	0,062885455	0,06051215
33	2,54E+06	0,059561503	0,056354741	0,060182007	0,055568481	0,057916683
34	2,62E+06	0,060684339	0,057982823	0,055256627	0,061969972	0,058973441
35	2,70E+06	0,055187898	0,060699649	0,057074701	0,062786954	0,0589373
36	2,78E+06	0,061176355	0,060908728	0,059246855	0,062774076	0,061026503
37	2,86E+06	0,061120957	0,060743252	0,0587417	0,057594226	0,059550034
38	2,94E+06	0,06116934	0,061532008	0,059635754	0,058738131	0,060268808
39	3,02E+06	0,064437481	0,061521033	0,057776287	0,060875996	0,061152699
40	3,10E+06	0,061818203	0,059314184	0,060867843	0,057728219	0,059932112

Продовження таблиці Є.1

1	2	3	4	5	6	7
41	3,18E+06	0,058595079	0,063965466	0,063638556	0,058708528	0,061226907
42	3,26E+06	0,05937032	0,058675619	0,056175319	0,056970543	0,05779795
43	3,34E+06	0,061976312	0,059358649	0,060173791	0,059598559	0,060276828
44	3,41E+06	0,055602255	0,063919234	0,056320681	0,055446123	0,057822073
45	3,49E+06	0,061667667	0,06306194	0,062168597	0,062997959	0,062474041
46	3,57E+06	0,061706379	0,062038886	0,058960597	0,055769564	0,059618857
47	3,65E+06	0,057103826	0,056002269	0,060654213	0,060188351	0,058487165
48	3,73E+06	0,056289263	0,064194826	0,056832798	0,058068101	0,058846247
49	3,81E+06	0,058154284	0,062142413	0,056448478	0,060775429	0,059380151
50	3,89E+06	0,058637108	0,06498847	0,059880563	0,064594333	0,062025118
51	3,97E+06	0,060701968	0,056494483	0,058556127	0,061455702	0,05930207
52	4,05E+06	0,059386015	0,063681261	0,064404319	0,055353624	0,060706305
53	4,13E+06	0,064883738	0,056624929	0,062653253	0,059304024	0,060866486
54	4,21E+06	0,056020448	0,061155596	0,062486636	0,060100169	0,059940712
55	4,29E+06	0,057088768	0,0562382	0,064037197	0,060361775	0,059431485
56	4,37E+06	0,056613095	0,063480082	0,055834224	0,061813925	0,059435332
57	4,45E+06	0,061531083	0,06307319	0,060521925	0,057775961	0,06072554
58	4,53E+06	0,057532916	0,060691007	0,060844761	0,056288606	0,058839322
59	4,61E+06	0,059663108	0,059071833	0,064619364	0,058926757	0,060570265
60	4,69E+06	0,057444256	0,05569167	0,057921475	0,064564057	0,058905365
61	4,77E+06	0,056589696	0,061974288	0,057408288	0,056871309	0,058210895
62	4,84E+06	0,056103751	0,059535427	0,056002939	0,06403984	0,058920489
63	4,92E+06	0,061563296	0,062220556	0,055164296	0,06043806	0,059846552
64	5,00E+06	0,05638183	0,063663823	0,064295293	0,059569114	0,060977515
65	5,08E+06	0,056965824	0,064755215	0,061699165	0,063820414	0,061810155
66	5,16E+06	0,058687252	0,063558033	0,062851529	0,05958604	0,061170713
67	5,24E+06	0,063209932	0,055117141	0,057817301	0,062241676	0,059596513
68	5,32E+06	0,055971013	0,058599781	0,060864102	0,058990253	0,058606287
69	5,40E+06	0,063379449	0,062299906	0,055639553	0,064040444	0,061339838
70	5,48E+06	0,055960984	0,056716297	0,059856276	0,06190025	0,058608452
71	5,56E+06	0,064764595	0,060210366	0,064774951	0,061996221	0,062936533
72	5,64E+06	0,059686512	0,05554338	0,063765052	0,058277204	0,059318037
73	5,72E+06	0,064767611	0,056999965	0,05838159	0,062567786	0,060679238
74	5,80E+06	0,061048455	0,055185218	0,064615702	0,061360611	0,060552496
75	5,88E+06	0,062392636	0,062936977	0,057317016	0,057400203	0,060011708
76	5,96E+06	0,055391878	0,057239247	0,064493188	0,056605388	0,058432425
77	6,04E+06	0,05782807	0,058453517	0,064413777	0,062963915	0,06091482
78	6,12E+06	0,056201966	0,064280813	0,062992026	0,064591666	0,062016618
79	6,19E+06	0,057961402	0,062044144	0,061304479	0,059581388	0,060222853
80	6,27E+06	0,056187277	0,055318389	0,06374288	0,060909842	0,059039597
81	6,35E+06	0,058179832	0,056646942	0,057930203	0,063577226	0,059083551
82	6,43E+06	0,05914263	0,061214784	0,063489436	0,059572235	0,060854771
83	6,51E+06	0,055641475	0,060772286	0,061178767	0,064518745	0,060527818
84	6,59E+06	0,061924721	0,057378928	0,055132369	0,060757512	0,058798382
85	6,67E+06	0,060666015	0,06434214	0,058472335	0,063207671	0,06167204
86	6,75E+06	0,057653895	0,06113966	0,056481409	0,064088437	0,05984085

Кінець таблиці Є.1

1	2	3	4	5	6	7
87	6,83E+06	0,060232481	0,060356328	0,064818294	0,063155238	0,062140585
88	6,91E+06	0,055939405	0,0608991	0,059783703	0,056594145	0,058304088
89	6,99E+06	0,060759465	0,06230122	0,059973914	0,061288984	0,061080896
90	7,07E+06	0,064292962	0,05811945	0,061394725	0,058984343	0,06069787
91	7,15E+06	0,05818569	0,058982211	0,058685846	0,05562713	0,057870219
92	7,23E+06	0,061674104	0,057098437	0,056369003	0,059240323	0,058595467
93	7,31E+06	0,056317979	0,05686193	0,063221177	0,057586841	0,058496982
94	7,39E+06	0,062163272	0,064443724	0,056898479	0,063490383	0,061748965
95	7,47E+06	0,057894061	0,062395508	0,06011319	0,055333046	0,058933951
96	7,54E+06	0,056831914	0,059904588	0,05724317	0,064589827	0,059642375
97	7,62E+06	0,060865129	0,057274146	0,055978445	0,058553688	0,058167852
98	7,70E+06	0,055201075	0,057543565	0,063621915	0,058567069	0,058733406
99	7,78E+06	0,0632894	0,055580292	0,064729195	0,055163285	0,059690543
100	7,86E+06	0,055046955	0,059344166	0,064608347	0,056852323	0,058962948

Таблиця Є.2

Друга серія експериментів

№	Час, с	Оперативність	Стійкість	Цілісність	Безпека	Цільова функція
1	2	3	4	5	6	7
1	0,00E+00	0,056187277	0,055568481	0,062044144	0,061394725	0,058798657
2	7,94E+04	0,060666015	0,056324876	0,060772286	0,064404319	0,060541874
3	1,59E+05	0,061120957	0,057586841	0,056999965	0,055256627	0,057741098
4	2,38E+05	0,064786183	0,055446123	0,063137978	0,057633224	0,060250877
5	3,18E+05	0,059386015	0,064589827	0,05569167	0,064903389	0,061142725
6	3,97E+05	0,059561503	0,062270443	0,060908728	0,059536968	0,060569411
7	4,77E+05	0,060488135	0,056970543	0,061521033	0,063726507	0,060676554
8	5,56E+05	0,062991586	0,064564057	0,063965466	0,056856359	0,062094367
9	6,35E+05	0,05937032	0,060909842	0,062395508	0,059635754	0,060577856
10	7,15E+05	0,059146619	0,058926757	0,05554338	0,060844761	0,058615379
11	7,94E+05	0,05914263	0,058567069	0,060920419	0,061874883	0,06012625
12	8,74E+05	0,057103826	0,056871309	0,057378928	0,058472335	0,057456599
13	9,53E+05	0,06116934	0,059072412	0,059358649	0,060864102	0,060116126
14	1,03E+06	0,056020448	0,062241676	0,061214784	0,063489436	0,060741586
15	1,11E+06	0,055939405	0,059569114	0,063817354	0,062168597	0,060373617
16	1,19E+06	0,060232481	0,055353624	0,064194826	0,05713312	0,059228513
17	1,27E+06	0,062151894	0,057728219	0,056494483	0,055672496	0,058011773
18	1,35E+06	0,064437481	0,061832813	0,05797437	0,060173791	0,061104614
19	1,43E+06	0,063700121	0,061969972	0,063919234	0,05838159	0,061992729
20	1,51E+06	0,064764595	0,05958604	0,060013244	0,058685846	0,060762431
21	1,59E+06	0,061563296	0,063207671	0,05770008	0,061289818	0,060940216
22	1,67E+06	0,063209932	0,059304024	0,057487531	0,057817301	0,059454697
23	1,75E+06	**0,027444256**	0,06403984	0,059287687	0,060883171	0,052913738
24	1,83E+06	**0,023918779**	0,062567786	0,062142413	0,063621915	0,053062723
25	1,91E+06	**0,024218483**	0,063605512	0,057239247	0,055978445	0,050260422

Продовження таблиці Є.2

1	2	3	4	5	6	7
26	1,99E+06	0,062392636	0,060361775	0,060722519	0,063638556	0,061778871
27	2,06E+06	0,056433533	0,062740473	0,060699649	0,057921475	0,059448783
28	2,14E+06	0,060865129	0,057322341	0,064280813	0,058200172	0,060167114
29	2,22E+06	0,055201075	0,06043806	0,060761573	0,064774951	0,060293915
30	2,30E+06	0,064767611	0,055114275	0,05686193	0,055246787	0,057997651
31	2,38E+06	0,056613095	0,061813925	0,060743252	0,061699165	0,06021736
32	2,46E+06	0,061976312	0,056852323	0,059314184	0,060182007	0,059581207
33	2,54E+06	0,061667667	0,060757512	0,061994793	0,063765052	0,062046256
34	2,62E+06	0,060759465	0,05681151	0,059071833	0,060867843	0,059377663
35	2,70E+06	0,061531083	0,060188351	0,05923855	0,05520651	0,059041124
36	2,78E+06	0,056103751	0,062255944	0,062220556	0,064295293	0,061218886
37	2,86E+06	0,055641475	0,058738131	0,061155596	0,064818294	0,060088374
38	2,94E+06	0,063379449	**0,026425592**	0,063558033	0,064527917	0,054472748
39	3,02E+06	0,056317979	**0,024785492**	0,063663823	0,056832798	0,050400023
40	3,10E+06	0,055046955	**0,025218483**	0,06230122	0,055639553	0,049551553
41	3,18E+06	0,057088768	**0,025318483**	0,0608991	0,055834224	0,049785144
42	3,26E+06	0,064292962	0,061288984	0,057274146	0,062308558	0,061291163
43	3,34E+06	0,060288949	0,055553743	0,058599781	0,063310485	0,059438239
44	3,41E+06	0,058179832	0,056594145	0,058453517	0,058117959	0,057836363
45	3,49E+06	0,0632894	0,058708528	0,061974288	0,059783703	0,06093898
46	3,57E+06	0,055202184	0,062997959	0,057230816	0,062583787	0,059503686
47	3,65E+06	0,056965824	0,055534272	0,064755215	0,064037197	0,060323127
48	3,73E+06	0,063326198	0,05589603	0,0562382	0,062992026	0,059613114
49	3,81E+06	0,060288949	0,061455702	0,061532008	0,057539416	0,060204019
50	3,89E+06	0,056831914	0,063490383	0,06452749	0,064615702	0,062366372
51	3,97E+06	0,064883738	0,057453672	0,06307319	0,062980468	0,062097767
52	4,05E+06	0,059686512	0,060875996	**0,027444256**	0,062486636	0,05262335
53	4,13E+06	0,064636628	0,063820414	**0,023918779**	0,057930203	0,052576506
54	4,21E+06	0,06391773	0,064591666	**0,023918875**	0,060365792	0,053198516
55	4,29E+06	0,059236548	0,064594333	**0,021258779**	0,055164296	0,050063489
56	4,37E+06	0,056201966	0,055769564	**0,024561878**	0,057408288	0,048485424
57	4,45E+06	0,056589696	0,064518745	0,061063932	0,061963435	0,061033952
58	4,53E+06	0,061674104	0,055795221	0,057982823	0,05724317	0,05817383
59	4,61E+06	0,062805292	0,059240323	0,064621885	0,056481409	0,060787227
60	4,69E+06	0,064446689	0,05562713	0,058982211	0,056320681	0,058844178
61	4,77E+06	0,055960984	0,064065555	0,06434214	0,060521925	0,061222651
62	4,84E+06	0,060288949	0,058990253	0,061439902	0,057776287	0,059623848
63	4,92E+06	0,060684339	0,057835188	0,063811032	0,064619364	0,061737481
64	5,00E+06	0,061924721	0,055333046	0,059344166	0,061304479	0,059476603
65	5,08E+06	0,058595079	0,061956254	0,062299906	0,06011319	0,060741107
66	5,16E+06	0,059663108	0,058015986	0,055117141	0,062653253	0,058862372
67	5,24E+06	0,057645556	0,058331452	0,06235194	0,058556127	0,059221269
68	5,32E+06	0,058834415	0,058984343	0,058675619	0,056796037	0,058322603
69	5,40E+06	0,055187898	0,062885455	0,05811945	0,059880563	0,059018341
70	5,48E+06	0,061027634	0,06190025	0,061180154	0,063966713	0,062018688
71	5,56E+06	0,062163272	0,059572235	0,055185218	0,057317016	0,058559435

Кінець таблиці Є.2

1	2	3	4	5	6	7
72	5,64E+06	0,061458941	0,058068101	0,063681261	0,058960597	0,060542225
73	5,72E+06	0,055971013	0,058277204	0,062038886	0,056369003	0,058164026
74	5,80E+06	0,057532916	0,060775429	0,056002269	**0,022422002**	0,049183154
75	5,88E+06	0,058154284	0,061720478	0,064443724	**0,024918779**	0,052309316
76	5,96E+06	0,05782807	0,057400203	0,058015748	**0,023918875**	0,049290724
77	6,04E+06	0,058637108	0,05879927	0,056354741	**0,021258779**	0,048762474
78	6,12E+06	0,061818203	0,060100169	0,061778165	**0,024561878**	0,052064604
79	6,19E+06	0,060701968	0,057594226	0,061601735	0,06374288	0,060910202
80	6,27E+06	0,056182744	0,056605388	0,06113966	0,062851529	0,05919483
81	6,35E+06	0,057653895	0,062786954	0,058965057	0,055132369	0,058634569
82	6,43E+06	0,059614794	0,062705807	0,055318389	0,05716897	0,05870199
83	6,51E+06	0,061176355	0,061360611	0,059904588	0,064493188	0,061733685
84	6,59E+06	0,055602255	0,056288606	0,060691007	0,059856276	0,058109536
85	6,67E+06	0,055871293	0,057775961	0,059471254	0,064608347	0,059431714
86	6,75E+06	0,060448832	0,057703279	0,063464087	0,057155077	0,059692819
87	6,83E+06	0,06139921	0,055163285	0,060356328	0,05773542	0,058663561
88	6,91E+06	0,062781568	0,062774076	0,064560836	0,059973914	0,062522598
89	6,99E+06	0,056289263	0,064088437	0,06306194	0,056002939	0,059860645
90	7,07E+06	0,06291725	0,062963915	0,057543565	0,061630782	0,061263878
91	7,15E+06	0,061706379	0,059581388	0,057900776	0,060654213	0,059960689
92	7,23E+06	0,05638183	0,056314828	0,061925316	0,058777518	0,058349873
93	7,31E+06	0,05818569	0,061996221	0,055191932	0,056175319	0,05788729
94	7,39E+06	0,059375872	0,055811014	0,056624929	0,064413777	0,059056398
95	7,47E+06	0,057961402	0,059561406	0,062936977	0,059246855	0,05992666
96	7,54E+06	0,062742337	0,056469466	0,055580292	0,064729195	0,059880322
97	7,62E+06	0,057894061	0,059598559	0,060812729	0,063221177	0,060381631
98	7,70E+06	0,061048455	0,057621181	0,059535427	0,056898479	0,058775886
99	7,78E+06	0,058687252	0,063577226	0,062252543	0,0587417	0,06081468
100	7,86E+06	0,055710361	0,058553688	0,056646942	0,061178767	0,058022439

ДОДАТОК Ж.
РЕЗУЛЬТАТИ ДРУГОГО ЕКСПЕРИМЕНТУ

Таблиця Ж.1

Результати першої серії другого експерименту

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
		1	1	1	2	2	4	1	1	1		1	1						0,0336		
		2	2	1	1	4	4	1	1	1		2	1						0,0268		
1	29054	3	3	2	2	3	3	1	1	1		1	3	3	29059	5	1	3	0,0366		1
		4	4	2	1	4	5	1	2	3		3	2						0,0725		
		5	1	1	2	1	2	3	1	2		1	2						0,0393		
		1	1	1	1	2	2	1	1	3		2	1						0,0922		
		2	2	1	1	2	3	1	1	2		3	2						0,0181		
2		3	3	1	1	2	1	2	1	3		3	2						0,0674		
	54775	4	4	2	2	1	1	3	2	1		1	2	4	54779	4	1	4	0,0645		1
		5	1	2	1	3	3	3	2	2		3	3						0,0893		
		1	1	1	1	4	1	2	2	1		1	3						0,0507		
	80055	2	2	1	1	4	4	1	1	1		1	3	2	80060	5	1	2	0,0179		1
3		3	3	1	2	1	5	3	2	2		3	2						0,0876		
		4	4	2	1	1	2	2	2	1		1	1						0,0863		
		5	3	1	2	3	4	3	2	1		3	3						0,0179		
		1	1	2	2	1	5	2	1	1		1	1						0,0159		
		2	2	1	2	3	1	3	1	2		1	2						0,0349		
4	103211	3	3	2	1	1	4	2	2	1		3	2	3	103214	3	1	3	0,0579		1
		4	4	2	2	2	1	2	2	1		1	1						0,0827		
		5	1	2	2	3	3	3	2	1		2	2						0,0569		
		1	1	2	1	2	3	1	2	1		3	3						0,0964		
	127542	2	2	2	1	2	4	1	2	2		3	1	2	127547	5	1	2	0,0945		1
5		3	3	1	1	2	1	1	1	1		1	1						0,0178		
		4	4	2	1	3	4	1	2	1		1	1						0,0856		
		5	4	2	2	1	5	3	2	2		1	2						0,0306		
		1	1	2	1	1	4	1	1	3		2	3						0,0146		
	154931	2	2	1	2	1	5	1	2	2		3	1	2	154936	5	0	2	0,0820		2
6		3	3	1	1	4	4	3	1	1		2	3						0,2315		
		4	4	1	2	3	2	2	2	3		3	1						0,0343		
		5	4	2	1	2	3	2	1	2		2	3						0,0504		
	154936	1	1	2	2	4	4	2	2	3		3	2	1	154953	17	1	1	0,0729		5
		2	2	1	1	3	4	1	2	1		2	3						0,1623		
7		3	3	2	2	4	3	1	2	2		3	2						0,2111		
		4	4	1	2	3	4	2	1	1		3	2						0,2058		
		5	3	1	1	4	1	3	1	3		2	2						0,1561		
		1	1	2	2	1	1	1	1	1		2	1						0,0379		
		2	2	2	2	3	4	1	2	2		2	2						0,0306		
8		3	3	2	1	4	2	3	1	1		2	2						0,0110		
	180388	4	4	1	2	3	1	2	2	2		1	3	4	180392	4	1	4	0,0546		3
		5	2	1	1	4	1	2	1	3		3	1						0,0279		
		1	1	2	2	4	2	1	1	1		2	3						0,0323		
		2	2	1	1	1	2	2	1	1		1	3						0,0669		
9		3	3	2	1	2	5	1	2	2		2	2						0,0608		
	209565	4	4	2	2	3	3	2	2	3		1	2	4	209570	5	1	4	0,0825		1
		5	2	1	2	1	5	1	2	2		2	1						0,0333		
		1	1	1	1	1	1	1	1	1		3	3						0,0862		
		2	2	2	1	4	3	2	2	3		3	1						0,0076		
10		3	3	2	1	2	3	2	2	3		1	3						0,0530		
		4	4	1	2	4	3	2	2	3		2	3						0,0951		
	237221	5	3	2	1	1	2	1	2	1		2	3	5	237225	4	1	3	0,0279		1
		1	1	1	1	4	1	3	2	2		1	1						0,0460		
		2	2	1	1	4	5	3	1	3		2	2						0,0518		
11		3	3	2	1	3	1	2	2	3		2	2						0,0678		
		4	4	2	2	1	5	2	2	2		3	2						0,0785		
	264345	5	4	1	1	3	5	3	1	2		3	2	5	264350	5	1	4	0,0075		1
		1	1	1	1	3	4	3	1	3		3	1						0,0073		
		2	2	2	2	2	5	3	2	2		3	1						0,0501		
12	290719	3	3	2	1	1	2	3	1	3		3	3	3	290723	4	1	3	0,0244		2
		4	4	1	2	4	4	3	2	2		1	3						0,0317		
		5	1	2	2	1	4	1	2	2		3	2						0,0371		
		1	1	1	1	1	2	2	2	1		3	2						0,0577		
		2	2	1	1	1	1	3	2	2		3	3						0,0802		
13	318241	3	3	1	1	2	2	2	2	3		2	1	3	318244	3	1	3	0,0033		1
		4	4	1	2	3	5	1	1	1		3	3						0,0114		
		5	4	1	2	3	1	3	2	3		2	2						0,0497		
		1	1	1	1	4	3	2	1	1		1	3						0,0685		
	345140	2	2	1	2	2	2	1	1	2		1	1	2	345145	5	1	2	0,0376		1
14		3	3	2	2	3	3	1	2	2		1	1						0,0017		
		4	4	1	2	4	5	3	2	2		3	1						0,0494		
		5	3	1	2	4	5	3	2	3		3	2						0,0433		
	371788	1	1	1	2	1	1	3	1	1		1	1	1	371791	3	1	1	0,0021		1
		2	2	2	2	3	4	2	2	2		2	2						0,0751		
15		3	3	1	2	1	2	2	2	3		2	1						0,0608		
		4	4	1	1	3	5	1	2	1		3	1						0,0867		
		5	1	1	2	4	3	3	1	3		2	2						0,0043		
		1	1	1	1	4	2	2	2	1		1	1						0,0605		
		2	2	1	2	4	1	2	1	1		2	2						0,0631		
16		3	3	1	1	1	1	1	2	3		1	2						0,0843		
	400815	4	4	2	2	1	2	2	1	1		3	3	4	400818	3	1	4	0,0714		4
		5	3	2	2	2	4	3	1	2		1	3						0,0439		
		1	1	2	2	1	2	1	2	2		1	1						0,0010		
	426573	2	2	1	1	3	4	3	2	2		2	2	2	426577	4	1	2	0,0782		1

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
17		3	3	2	1	3	4	3	2	1		2	1						0,0870		
		4	4	2	1	1	3	2	2	3		3	3						0,0813		
		5	2	2	2	1	4	2	1	2		2	3						0,0497		
		1	1	1	2	4	2	1	2	2		1	1						0,0549		
	454475	2	2	2	2	1	3	3	2	2		2	2	2	454480	5	1	2	0,0076		1
18		3	3	2	2	1	2	1	2	3		2	1						0,0440		
		4	4	2	1	1	5	3	1	1		3	3						0,0242		
		5	1	1	1	2	2	1	2	1		1	2						0,0071		
		1	1	1	1	1	3	2	1	1		3	2						0,0932		
	480209	2	2	1	1	1	5	3	1	3		1	2	2	480213	4	1	2	0,0805		1
19		3	3	1	2	3	2	3	2	1		3	1						0,0624		
		4	4	1	1	3	4	1	1	3		2	1						0,0523		
		5	2	1	2	3	1	2	1	2		2	1						0,0634		
		1	1	1	2	2	2	2	2	2		3	1						0,0229		
		2	2	1	2	3	2	1	1	3		3	2						0,0981		
20	506679	3	3	2	1	4	3	2	2	3		2	1	3	506684	5	1	3	0,0618		2
		4	4	1	2	3	5	3	2	1		2	3						0,0372		
		5	1	2	2	2	4	3	1	3		2	2						0,0755		
		1	1	2	2	4	2	3	2	2		2	1						0,0165		
		2	2	2	1	3	5	2	1	1		3	3						0,0436		
21	535512	3	3	2	2	4	5	3	2	2		1	3	3	535517	5	1	3	0,0272		1
		4	4	2	2	4	2	3	2	1		3	2						0,0958		
		5	3	1	1	3	1	3	1	1		3	3						0,0745		
		1	1	1	1	2	3	1	1	3		1	3						0,0658		
	559598	2	2	1	1	1	1	1	1	1		2	2	2	559602	4	1	2	0,0465		1
22		3	3	1	1	1	1	3	2	3		2	2						0,0597		
		4	4	2	1	1	1	2	2	3		1	2						0,0860		
		5	1	2	2	4	3	2	2	2		3	3						0,0336		
		1	1	2	2	2	5	2	2	1		2	2						0,0561		
		2	2	1	1	4	2	3	2	2		2	3						0,0820		
23	588740	3	3	1	1	3	2	1	2	2		1	3	3	588744	4	1	3	0,0548		1
		4	4	2	1	1	2	3	2	1		3	3						0,0630		
		5	3	1	1	4	1	3	2	1		2	2						0,0282		
		1	1	1	2	1	1	3	1	2		2	2						0,0613		
		2	2	2	1	2	5	1	2	3		3	2						0,0303		
24		3	3	2	2	1	5	3	2	2		2	1						0,0693		
		4	4	2	2	1	1	2	2	2		2	1						0,0238		
	618421	5	1	2	1	2	1	1	1	2		2	3	5	618424	3	1	1	0,0755		1
		1	1	2	1	1	3	3	1	2		2	1						0,0101		
		2	2	2	2	3	2	1	1	1		1	2						0,0897		
25	641171	3	3	1	1	2	5	2	1	2		2	1	3	641174	3	1	3	0,0835		1
		4	4	2	2	2	2	2	1	3		3	3						0,0850		
		5	4	1	2	3	3	1	2	2		1	3						0,0668		
		1	1	1	1	1	5	3	2	1		2	2						0,0678		
		2	2	2	2	3	1	1	2	1		1	3						0,0129		
26		3	3	2	1	1	3	1	1	1		3	3						0,0824		
		4	4	2	2	1	2	3	1	2		3	2						0,0681		
	667045	5	3	2	2	2	4	1	2	3		1	1	5	667048	3	1	3	0,0435		1
		1	1	1	2	4	4	2	1	2		2	1						0,0486		
		2	2	2	2	1	3	2	1	1		3	3						0,0258		
27	695322	3	3	1	2	4	2	2	2	1		2	3	3	695326	4	1	3	0,0733		4
		4	4	2	1	4	2	3	2	1		3	1						0,0159		
		5	4	2	2	1	1	1	1	3		1	2						0,0149		
		1	1	2	2	4	5	1	2	2		1	3						0,0935		
	722341	2	2	1	1	2	2	2	2	2		2	2	2	722345	4	1	2	0,0316		1
28		3	3	2	1	4	1	3	2	2		2	3						0,0581		
		4	4	1	1	4	4	2	2	3		1	3						0,0794		
		5	1	1	1	1	2	1	2	3		2	2						0,0213		
		1	1	2	1	3	1	2	1	2		2	3						0,0478		
		2	2	2	1	1	3	1	1	3		1	3						0,0711		
29		3	3	2	1	1	2	3	2	3		1	1						0,0434		
	747268	4	4	1	1	4	2	3	2	3		1	2	4	747271	3	1	4	0,0894		1
		5	4	1	1	4	2	1	1	3		2	3						0,0623		
		1	1	1	2	4	4	3	2	3		1	1						0,0871		
		2	2	1	1	2	4	3	1	2		2	1						0,0596		
30	774631	3	3	1	2	3	2	3	2	2		3	3	3	774634	3	1	3	0,0104		1
		4	4	1	2	2	2	2	2	1		2	3						0,0828		
		5	2	2	2	1	2	1	2	2		3	3						0,0091		
		1	1	2	2	4	5	1	2	2		3	3						0,0082		
	799403	2	2	2	2	2	5	1	1	1		2	2	2	799408	5	1	2	0,0308		1
31		3	3	1	1	4	5	1	2	1		1	3						0,0648		
		4	4	1	2	4	2	1	2	3		3	1						0,0408		
		5	1	1	2	4	5	2	1	2		3	1						0,0873		
		1	1	2	1	1	4	3	1	1		1	2						0,0245		
		2	2	1	2	2	3	1	2	1		3	2						0,0480		
32		3	3	2	2	1	3	2	2	1		3	3						0,0276		
	827664	4	4	1	1	1	3	2	1	1		1	1	4	827668	4	1	4	0,0635		1
		5	4	2	1	4	3	1	2	1		1	1						0,0603		
		1	1	2	1	1	2	1	2	3		3	2						0,0931		
	856192	2	2	2	1	3	3	2	1	1		1	2	2	856196	4	1	2	0,0036		1
33		3	3	1	2	1	2	1	1	2		2	2						0,0928		
		4	4	1	2	2	5	2	2	1		3	2						0,0415		
		5	2	1	2	4	1	2	2	1		1	2						0,0147		
		1	1	2	2	1	4	2	2	2		2	3						0,0066		
		2	2	1	1	3	4	2	1	3		3	1						0,0051		
34		3	3	1	1	2	3	2	2	1		2	2						0,0912		
	883432	4	4	2	1	1	3	3	1	2		2	3	4	883436	4	1	4	0,0262		4
		5	4	2	2	4	4	3	1	2		3	2						0,0786		
		1	1	2	1	1	1	2	2	2		3	2						0,0977		
		2	2	1	1	1	3	2	1	3		3	2						0,0856		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
35	912067	3	3	1	1	2	3	2	2	2		2	1	3	912071	4	1	3	0,0516		1
		4	4	2	1	2	4	3	1	2		2	1						0,0106		
		5	1	2	2	4	4	1	2	3		1	2						0,0982		
		1	1	1	1	2	3	2	1	2		1	2						0,0828		
		2	2	2	2	2	3	3	2	2		2	1						0,0017		
36		3	3	1	1	3	3	3	1	1		3	1						0,0859		
	935917	4	4	2	2	4	5	2	2	2		2	3	4	935921	4	1	4	0,0098		3
		5	1	1	2	2	2	3	2	2		2	2						0,0384		
		1	1	2	2	4	4	1	2	2		2	3						0,0670		
		2	2	2	1	2	5	1	2	2		3	2						0,0996		
37		3	3	1	2	2	2	2	2	3		3	3						0,0615		
	963427	4	4	1	1	2	4	3	2	3		1	1	4	963430	3	1	4	0,0963		1
		5	1	1	2	3	2	2	2	3		2	1						0,0325		
		1	1	2	1	4	2	1	2	2		2	2						0,0511		
	993296	2	2	1	1	4	2	1	2	3		3	1	2	993299	3	1	2	0,0946		1
38		3	3	2	2	1	3	2	1	2		2	3						0,0687		
		4	4	1	1	2	5	2	2	2		3	1						0,0648		
		5	1	2	1	4	5	1	2	2		1	1						0,0120		
	1017410	1	1	2	1	2	5	1	1	1		1	1	1	1017413	3	1	1	0,0129		2
		2	2	2	1	2	2	2	1	1		3	3						0,0909		
39		3	3	2	2	4	1	3	1	1		2	3						0,0507		
		4	4	2	1	1	4	1	1	3		2	2						0,0308		
		5	4	1	2	2	1	1	1	3		3	2						0,0019		
	1045325	1	1	1	1	3	5	3	2	3		1	3	1	1045330	5	1	1	0,0165		1
		2	2	1	1	2	4	1	1	2		2	1						0,0255		
40		3	3	2	1	4	1	2	2	3		3	1						0,0697		
		4	4	1	1	2	1	1	2	2		3	2						0,0636		
		5	3	2	1	3	2	3	2	1		3	3						0,0216		
		1	1	2	2	3	5	1	2	1		1	2						0,0442		
		2	2	1	2	1	4	2	1	1		3	3						0,0192		
41		3	3	1	2	2	1	3	1	2		1	2						0,0452		
		4	4	1	2	3	2	2	1	3		2	1						0,0350		
	1068913	5	3	1	2	2	1	1	1	2		2	1	5	1068918	5	1	3	0,0914		1
		1	1	2	2	3	3	1	1	2		3	1						0,0228		
		2	2	2	2	2	4	1	2	1		2	1						0,0928		
42	1096228	3	3	1	1	4	5	1	2	2		2	2	3	1096232	4	1	3	0,0461		1
		4	4	2	2	2	1	2	2	2		2	2						0,0869		
		5	2	2	2	3	4	2	1	3		3	1						0,0154		
	1125876	1	1	1	2	4	3	2	2	3		2	2	1	1125881	5	1	1	0,0765		1
		2	2	2	1	3	2	2	2	1		3	1						0,0269		
43		3	3	2	2	4	2	2	2	2		1	2						0,0745		
		4	4	1	2	2	4	2	1	3		2	1						0,0872		
		5	3	1	2	4	5	3	2	3		3	3						0,0965		
	1148607	1	1	2	1	4	2	2	1	2		1	2	1	1148610	3	1	1	0,0150		1
		2	2	2	2	4	1	1	1	1		3	1						0,0475		
44		3	3	1	1	1	5	1	2	3		3	2						0,0170		
		4	4	2	2	2	2	1	1	2		1	2						0,0704		
		5	3	1	1	1	5	3	2	2		1	2						0,0005		
		1	1	2	2	1	4	1	1	2		3	2						0,0682		
		2	2	1	2	2	1	3	2	1		3	2						0,0078		
45		3	3	1	2	4	1	2	2	1		1	3						0,0445		
	1174391	4	4	1	2	1	1	3	1	3		3	1	4	1174394	3	1	4	0,0580		1
		5	2	2	1	3	2	2	1	3		1	2						0,0798		
	1202560	1	1	1	2	1	4	1	1	1		3	1	1	1202563	3	1	1	0,0619		1
		2	2	1	1	2	3	1	2	1		2	2						0,0502		
46		3	3	1	2	1	3	1	2	2		3	3						0,0613		
		4	4	1	1	4	5	3	1	3		3	2						0,0377		
		5	2	2	2	3	1	3	1	1		2	2						0,0509		
		1	1	2	1	2	5	2	2	3		2	2						0,0543		
	1226313	2	2	2	1	3	4	1	2	3		2	3	2	1226316	3	1	2	0,0868		1
47		3	3	1	2	4	2	1	2	1		2	3						0,0850		
		4	4	1	2	2	3	3	2	1		1	1						0,0003		
		5	1	1	2	2	1	3	2	2		3	2						0,0371		
	1254759	1	1	1	1	2	5	1	1	2		3	1	1	1254762	3	1	1	0,0729		1
		2	2	2	2	2	3	1	1	1		3	3						0,0477		
48		3	3	2	1	3	5	3	2	2		2	3						0,0965		
		4	4	1	2	2	1	2	2	3		1	2						0,0060		
		5	4	2	2	2	5	1	1	2		1	2						0,0642		
		1	1	1	1	2	4	3	2	3		1	1						0,0723		
		2	2	1	1	3	4	2	1	3		3	1						0,0762		
49	1280509	3	3	2	2	3	2	3	1	2		1	3	3	1280513	4	1	3	0,0652		4
		4	4	2	2	2	3	1	2	2		1	2						0,0956		
		5	1	1	2	2	4	1	2	3		1	1						0,0140		
		1	1	1	1	2	3	3	2	1		1	1						0,0124		
	1308028	2	2	1	1	3	2	3	2	1		1	3	2	1308032	4	1	2	0,0012		1
50		3	3	2	2	3	1	3	1	2		1	1						0,0664		
		4	4	1	2	1	3	2	2	2		1	2						0,0023		
		5	3	2	2	3	4	3	2	2		1	2						0,0659		
		1	1	2	1	4	5	2	2	3		2	2						0,0312		
		2	2	1	1	3	2	2	1	3		1	3						0,0380		
51	1331351	3	3	1	2	3	1	2	2	2		3	2	3	1331356	5	1	3	0,0168		1
		4	4	2	2	1	1	2	1	2		2	2						0,0253		
		5	2	2	2	2	4	1	1	2		2	1						0,0450		
		1	1	1	2	3	4	2	1	2		1	1						0,0332		
		2	2	1	1	3	5	2	2	1		1	3						0,0614		
52		3	3	1	2	2	4	1	1	1		1	1						0,0420		
	1356893	4	4	2	2	1	4	1	2	3		3	3	4	1356898	5	1	4	0,0407		1
		5	4	1	2	1	5	3	1	3		1	1						0,0157		
	1381196	1	1	1	2	2	3	2	1	3		1	1	1	1381200	4	1	1	0,0501	84	1
		2	2	1	2	1	2	1	2	3		1	2						0,0673		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
53		3	3	1	2	3	1	1	1	3		3	1						0,0143		
		4	4	1	1	2	3	2	1	3		3	2						0,0941		
		5	1	2	2	3	3	3	2	2		1	1						0,0010		
		1	1	2	1	3	4	1	2	1		1	2						0,0370		
		2	2	2	2	2	1	2	1	1		2	2						0,0706		
54		3	3	2	1	3	2	1	1	2		2	3						0,0149		
		4	4	1	1	2	3	2	1	2		1	2						0,0794		
	1404478	5	3	1	1	1	4	2	2	3		3	3	5	1404482	4	1	3	0,0693		1
		1	1	2	1	4	4	3	1	1		1	2						0,0153		
		2	2	1	1	3	3	1	1	3		1	2						0,0956		
55		3	3	1	1	2	1	3	1	3		2	2						0,0225		
	1430355	4	4	1	1	1	2	3	2	2		1	3	4	1430358	3	1	4	0,0435		1
		5	4	2	2	3	4	3	2	2		3	1						0,0950		
		1	1	2	1	2	4	2	2	1		3	1						0,0777		
	1454733	2	2	1	1	1	3	2	1	3		2	1	2	1454736	3	1	2	0,0461		1
56		3	3	2	1	2	5	1	1	1		3	3						0,0918		
		4	4	2	2	2	5	3	1	1		3	1						0,0031		
		5	1	1	1	4	1	2	1	3		2	1						0,0046		
		1	1	2	1	1	3	3	1	3		2	1						0,0101		
		2	2	1	1	3	3	3	2	1		1	2						0,0995		
57	1483290	3	3	1	1	3	4	2	1	1		1	2	3	1483294	4	1	3	0,0917		1
		4	4	2	2	2	3	1	2	3		1	1						0,0406		
		5	3	1	1	3	3	1	1	2		3	2						0,0207		
	1507248	1	1	2	2	4	5	1	1	1		3	1	1	1507253	5	1	1	0,0183		1
		2	2	1	1	2	5	2	1	3		2	3						0,0778		
58		3	3	1	2	4	4	2	2	1		2	3						0,0912		
		4	4	1	1	1	1	1	2	3		3	3						0,0662		
		5	2	2	1	4	1	3	2	3		2	3						0,0533		
		1	1	1	2	1	4	3	1	1		1	3						0,0927		
		2	2	2	2	3	3	3	2	3		3	3						0,0419		
59	1532084	3	3	1	1	3	5	1	2	2		2	2	3	1532087	3	1	3	0,0030		4
		4	4	1	2	1	1	1	1	3		1	1						0,0972		
		5	4	1	1	3	4	1	2	2		2	2						0,0852		
		1	1	2	1	2	3	2	2	3		1	1						0,0506		
	1556020	2	2	1	1	4	5	3	1	3		1	3	2	1556024	4	0	2	0,1621		1
60		3	3	1	1	1	5	1	2	3		2	3						0,1245		
		4	4	2	1	3	1	1	1	1		1	1						0,0565		
		5	3	2	1	3	4	2	2	3		2	3						0,0561		
	1556024	1	1	1	2	2	4	2	1	3		2	2	1	1556049	25	1	1	0,1216		5
		2	2	2	2	1	1	3	2	3		2	1						0,0062		
61		3	3	2	1	2	1	1	2	3		3	3						0,1905		
		4	4	1	1	3	2	1	2	1		2	1						0,1460		
		5	4	2	1	2	5	2	2	1		1	1						0,0916		
		1	1	1	1	3	2	3	2	2		2	2						0,0327		
	1579746	2	2	2	1	4	1	1	2	2		1	3	2	1579750	4	1	2	0,0815		1
62		3	3	1	1	2	5	3	2	2		3	1						0,0826		
		4	4	2	2	1	5	3	1	3		1	3						0,0992		
		5	2	1	2	3	2	3	1	2		2	2						0,0438		
		1	1	1	2	1	4	1	1	2		2	2						0,0265		
		2	2	2	1	4	3	2	2	1		3	2						0,0988		
63		3	3	1	2	1	5	1	1	2		1	2						0,0795		
		4	4	1	2	4	5	1	1	2		1	3						0,0418		
	1605620	5	2	2	2	2	2	1	2	1		2	3	5	1605625	5	1	2	0,0319		1
		1	1	2	2	2	1	3	1	3		1	2						0,0718		
		2	2	2	1	4	5	3	2	1		1	2						0,0197		
64	1632453	3	3	1	2	3	2	1	1	2		2	1	3	1632456	3	1	3	0,0748		1
		4	4	2	1	2	2	3	1	1		3	1						0,0417		
		5	3	2	1	4	1	3	2	2		3	3						0,0522		
		1	1	2	1	4	4	2	2	3		3	3						0,0227		
	1658563	2	2	2	2	1	2	1	1	3		3	2	2	1658568	5	1	2	0,0058		1
65		3	3	2	2	4	3	2	1	2		3	1						0,0854		
		4	4	2	2	4	5	3	2	1		3	1						0,0464		
		5	3	2	2	2	5	2	1	3		2	1						0,0502		
		1	1	2	2	4	5	1	2	1		2	2						0,0644		
	1681530	2	2	2	2	1	5	3	1	1		1	1	2	1681535	5	1	2	0,0793		1
66		3	3	1	2	4	4	3	1	2		1	2						0,0661		
		4	4	1	2	2	5	1	2	2		2	3						0,0623		
		5	3	1	1	4	4	1	1	1		3	2						0,0677		
		1	1	1	1	4	5	2	1	2		1	3						0,0053		
		2	2	1	1	3	1	1	1	1		3	3						0,0366		
67		3	3	2	1	2	4	1	1	2		2	3						0,0547		
		4	4	2	1	3	5	3	2	3		2	2						0,0701		
	1705271	5	3	1	2	1	4	1	1	3		1	3	5	1705274	3	1	3	0,0481		2
		1	1	2	2	3	4	3	2	2		2	2						0,0087		
	1730095	2	2	2	2	2	5	3	1	1		3	3	2	1730098	3	1	2	0,0876		3
68		3	3	2	2	4	2	3	1	1		3	2						0,0156		
		4	4	1	1	4	4	3	1	1		1	1						0,0801		
		5	3	2	1	4	1	3	2	3		2	3						0,0891		
		1	1	1	2	3	1	2	2	3		2	2						0,0723		
	1758713	2	2	2	2	2	3	1	1	1		3	2	2	1758716	3	1	2	0,0768		1
69		3	3	2	1	2	5	3	2	3		1	3						0,0324		
		4	4	1	1	1	1	1	2	2		2	3						0,0276		
		5	1	2	2	1	2	2	2	1		3	1						0,0123		
	1781599	1	1	2	2	1	4	2	1	1		2	1	1	1781604	5	1	1	0,0775		1
		2	2	1	1	3	3	3	1	2		3	1						0,0497		
70		3	3	1	2	3	4	2	2	2		2	2						0,0663		
		4	4	1	2	4	4	3	1	2		2	1						0,0690		
		5	4	2	2	1	5	1	2	3		2	3						0,0274		
		1	1	1	2	4	5	3	1	2		1	2						0,0268		
		2	2	2	2	2	4	2	1	1		2	3						0,0573		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
71		3	3	2	2	1	2	1	2	2		1	2						0,0279		
		4	4	2	2	3	4	3	1	2		2	3						0,0181		
	1810919	5	2	2	1	3	3	1	2	3		1	3	5	1810923	4	1	2	0,0060		1
	1840093	1	1	2	1	4	5	3	1	2		2	3	1	1840098	5	1	1	0,0317		4
		2	2	2	1	4	4	2	2	2		1	2						0,0083		
72		3	3	1	2	2	2	1	2	3		3	1						0,0335		
		4	4	2	1	4	1	2	2	1		3	1						0,0903		
		5	1	2	1	1	2	3	1	1		2	2						0,0518		
		1	1	1	2	3	5	2	2	2		1	2						0,0468		
		2	2	2	1	3	2	3	2	2		3	3						0,0165		
73		3	3	2	2	4	5	3	1	1		2	1						0,0615		
		4	4	2	2	2	5	3	1	3		2	3						0,0040		
	1863598	5	3	1	2	4	3	2	1	1		3	3	5	1863602	4	1	3	0,0897		1
		1	1	1	1	2	3	3	2	2		1	2						0,0853		
		2	2	2	1	3	2	2	2	1		2	3						0,0690		
74		3	3	2	1	2	2	2	2	1		3	2						0,0612		
		4	4	2	1	3	2	3	1	2		1	3						0,0920		
	1888959	5	1	2	1	4	1	3	1	3		2	1	5	1888963	4	1	1	0,0890		1
		1	1	2	1	4	3	3	1	3		3	3						0,0646		
	1917834	2	2	1	2	2	2	2	1	1		1	3	2	1917838	4	1	2	0,0196		1
75		3	3	2	2	2	3	3	2	2		3	1						0,0684		
		4	4	1	1	3	1	3	2	3		1	2						0,0970		
		5	4	2	1	1	3	1	2	1		1	2						0,0304		
		1	1	1	1	3	5	2	1	2		3	2						0,0490		
		2	2	1	1	2	4	3	1	1		2	2						0,0548		
76		3	3	2	1	1	4	3	2	3		3	2						0,0265		
		4	4	2	1	3	1	1	2	2		2	1						0,0807		
	1941350	5	1	2	1	2	1	2	1	1		3	3	5	1941355	5	1	1	0,0425		1
		1	1	1	1	3	1	1	2	3		3	2						0,0334		
	1965193	2	2	1	2	4	1	3	1	1		1	3	2	1965197	4	1	2	0,0164		1
77		3	3	1	1	4	2	1	2	3		3	3						0,0311		
		4	4	2	1	2	1	1	2	1		2	3						0,0474		
		5	4	1	1	2	1	3	2	2		2	3						0,0421		
		1	1	1	1	2	2	2	1	1		3	1						0,0323		
		2	2	2	2	4	2	3	1	2		3	1						0,0259		
78		3	3	1	2	1	1	1	1	2		2	2						0,0268		
		4	4	2	1	1	1	2	2	3		1	2						0,0081		
	1989927	5	1	2	2	1	1	3	2	2		1	2	5	1989932	5	1	1	0,0026		1
		1	1	2	1	2	3	1	2	3		2	1						0,0478		
		2	2	1	1	4	2	3	2	3		1	3						0,0460		
79		3	3	2	2	3	3	3	2	1		2	3						0,0830		
	2019079	4	4	2	2	3	1	2	1	2		2	1	4	2019082	3	1	4	0,0076		1
		5	2	2	1	4	4	2	2	1		1	1						0,0880		
	2048463	1	1	2	2	4	1	1	2	1		3	2	1	2048466	3	1	1	0,0296		1
		2	2	2	1	3	1	2	2	3		1	2						0,0945		
80		3	3	1	1	4	1	3	2	2		1	3						0,0228		
		4	4	1	1	3	2	3	2	2		1	3						0,0823		
		5	3	2	1	4	5	3	1	1		2	2						0,0514		
		1	1	1	1	3	4	1	2	3		2	2						0,0440		
	2071993	2	2	2	2	2	4	2	1	2		3	1	2	2071996	3	1	2	0,0957		1
81		3	3	2	2	3	4	1	2	2		3	1						0,0373		
		4	4	2	1	4	1	2	2	1		1	2						0,0869		
		5	2	2	2	4	3	3	2	1		2	3						0,0682		
		1	1	1	1	4	5	3	2	1		1	3						0,0847		
		2	2	1	2	1	4	1	1	3		2	1						0,0357		
82	2099760	3	3	2	2	4	4	2	1	1		1	3	3	2099764	4	1	3	0,0704		1
		4	4	1	2	1	2	3	2	3		1	3						0,0879		
		5	1	1	1	1	2	2	1	1		3	3						0,0581		
		1	1	1	1	2	3	2	2	1		3	3						0,0471		
	2126571	2	2	2	2	3	1	1	2	3		3	2	2	2126575	4	1	2	0,0889		1
83		3	3	1	1	1	4	3	1	2		1	1						0,0679		
		4	4	1	2	1	4	2	1	1		2	3						0,0490		
		5	4	2	1	1	3	3	1	3		1	3						0,0715		
	2150682	1	1	1	2	2	3	2	1	3		1	1	1	2150686	4	1	1	0,0005	53	1
		2	2	2	2	2	2	1	1	1		2	2						0,0263		
84		3	3	1	2	1	1	1	2	3		2	2						0,0051		
		4	4	2	2	1	1	1	1	1		3	1						0,0935		
		5	3	2	2	2	5	1	1	1		1	3						0,0657		
		1	1	1	2	1	3	2	2	2		3	3						0,0515		
		2	2	2	2	3	2	3	1	2		1	3						0,0594		
85	2173325	3	3	1	2	4	4	3	2	1		1	2	3	2173328	3	1	3	0,0361		1
		4	4	1	2	1	1	1	1	1		1	1						0,0744		
		5	1	1	1	2	3	1	2	1		1	3						0,0381		
		1	1	2	2	2	4	1	1	1		1	3						0,0308		
		2	2	2	1	3	5	2	1	3		2	1						0,0275		
86	2198675	3	3	1	2	1	3	1	1	1		3	1	3	2198678	3	1	3	0,0591		1
		4	4	2	2	3	3	1	2	1		1	3						0,0004		
		5	4	2	1	4	5	2	2	1		2	1						0,0131		
	2228156	1	1	2	1	2	5	3	1	3		1	2	1	2228159	3	1	1	0,0198		1
		2	2	2	2	3	3	1	2	2		2	3						0,0654		
87		3	3	1	1	1	4	1	1	3		3	2						0,0265		
		4	4	1	1	3	3	3	1	1		2	3						0,0326		
		5	4	2	1	4	1	3	1	3		3	3						0,0399		
		1	1	2	1	1	4	1	2	3		3	3						0,0231		
		2	2	1	1	1	5	3	2	2		3	1						0,0840		
88		3	3	1	2	4	1	3	2	2		3	1						0,0848		
	2251094	4	4	2	2	3	1	1	2	1		3	2	4	2251097	3	1	4	0,0660		1
		5	2	2	1	4	4	1	1	2		3	3						0,0023		
	2277399	1	1	2	1	2	3	2	1	1		1	2	1	2277403	4	1	1	0,0238		1
		2	2	2	1	2	5	3	1	1		3	2						0,0206		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
89		3	3	1	1	2	4	1	1	3		3	3						0,0810		
		4	4	2	2	1	3	3	2	1		2	3						0,0608		
		5	4	2	2	2	1	3	2	3		3	1						0,0000		
		1	1	1	1	4	2	2	2	3		2	3						0,0472		
		2	2	1	2	4	2	3	2	3		1	2						0,0347		
90		3	3	2	1	1	2	1	2	1		2	1						0,0621		
		4	4	2	2	2	4	3	1	2		1	1						0,0200		
	2303043	5	3	1	1	1	2	2	1	2		2	3	5	2303046	3	1	3	0,0877		1
		1	1	2	1	2	4	3	1	2		1	2						0,0094		
	2326855	2	2	1	1	3	2	2	1	2		3	2	2	2326859	4	1	2	0,0488		1
91		3	3	1	2	2	3	3	2	2		3	2						0,0085		
		4	4	2	2	4	1	1	2	2		2	2						0,0218		
		5	4	2	2	1	4	2	1	3		1	2						0,0917		
	2355599	1	1	2	2	1	1	2	1	3		1	3	1	2355603	4	1	1	0,0944		1
		2	2	2	2	1	5	3	2	3		1	1						0,0883		
92		3	3	1	2	3	3	2	1	1		3	3						0,0746		
		4	4	2	2	3	3	3	2	1		1	1						0,0697		
		5	2	1	1	2	5	3	1	2		3	2						0,0953		
		1	1	2	1	3	2	2	1	1		2	2						0,0479		
	2383367	2	2	2	1	3	5	1	2	3		2	3	2	2383371	4	1	2	0,0131		1
93		3	3	2	2	2	2	1	2	3		1	1						0,0363		
		4	4	1	2	3	2	2	1	1		2	1						0,0846		
		5	1	1	1	2	4	1	1	3		3	1						0,0212		
		1	1	1	1	2	4	2	2	1		1	2						0,0652		
	2408415	2	2	1	1	3	4	1	2	1		1	2	2	2408420	5	1	2	0,0679		1
94		3	3	1	1	1	4	2	2	3		2	1						0,0672		
		4	4	1	1	2	1	3	1	2		1	2						0,0430		
		5	4	1	1	3	1	2	1	1		2	1						0,0305		
		1	1	2	1	2	2	1	2	3		3	1						0,0102		
	2431337	2	2	2	2	4	3	3	1	2		1	1	2	2431341	4	1	2	0,0439		1
95		3	3	1	2	3	2	3	2	2		1	2						0,0253		
		4	4	1	2	1	1	2	1	2		1	2						0,0662		
		5	3	1	2	1	2	3	1	1		1	1						0,0897		
		1	1	2	2	1	5	3	2	3		2	3						0,0432		
	2459469	2	2	1	2	3	5	3	2	3		1	2	2	2459474	5	1	2	0,0442		3
96		3	3	2	2	4	5	2	1	2		1	3						0,0877		
		4	4	2	2	4	4	1	1	2		2	2						0,0929		
		5	1	1	2	3	1	3	2	3		2	2						0,0733		
	2484937	1	1	1	1	2	4	2	2	2		1	2	1	2484940	3	1	1	0,0056		2
		2	2	2	2	4	1	3	1	3		1	3						0,0318		
97		3	3	2	1	1	5	1	2	3		3	1						0,0935		
		4	4	2	2	3	3	1	2	3		3	2						0,0917		
		5	4	2	1	2	2	1	1	2		2	3						0,0893		
		1	1	1	2	3	4	3	1	3		3	2						0,0522		
	2510711	2	2	2	2	1	2	1	2	1		2	2	2	2510714	3	1	2	0,0441		1
98		3	3	2	1	3	2	2	2	3		2	2						0,0803		
		4	4	2	1	1	2	2	1	3		2	2						0,0538		
		5	2	1	2	3	4	2	1	3		2	2						0,0463		
		1	1	2	2	3	1	3	2	3		1	3						0,0706		
	2538941	2	2	1	2	4	4	2	2	1		2	1	2	2538946	5	1	2	0,0484		1
99		3	3	2	2	4	5	1	1	1		3	2						0,0945		
		4	4	2	2	1	2	3	2	3		1	3						0,0570		
		5	3	1	1	4	5	2	2	3		1	1						0,0765		
		1	1	2	2	3	5	2	1	2		2	3						0,0037		
		2	2	1	1	2	4	3	1	1		2	3						0,0938		
100	2567278	3	3	2	2	1	2	2	1	3		3	1	3	2567282	4	1	3	0,0683		1
		4	4	2	2	2	3	3	1	1		3	3						0,0997		
		5	3	2	1	2	3	1	1	3		2	3						0,0272		
		1	1	1	2	4	3	2	1	1		1	1						0,0718		
	2594314	2	2	2	2	2	5	1	2	1		1	2	2	2594318	4	1	2	0,0618		1
101		3	3	2	1	2	2	3	1	3		1	1						0,0676		
		4	4	2	1	4	4	1	2	1		1	3						0,0845		
		5	2	1	2	3	4	1	1	3		1	2						0,0551		
		1	1	1	2	4	2	2	1	3		3	3						0,0160		
		2	2	2	1	4	1	3	2	1		1	3						0,0164		
102		3	3	2	2	1	1	3	1	2		3	2						0,0486		
		4	4	2	1	1	5	2	2	3		2	1						0,0805		
	2618016	5	1	1	1	1	4	3	1	1		3	1	5	2618020	4	1	1	0,0136		2
		1	1	1	1	4	1	1	1	2		2	1						0,0673		
		2	2	2	2	4	1	1	1	1		2	1						0,0235		
103	2641499	3	3	2	1	3	3	1	1	1		3	3	3	2641504	5	1	3	0,0682		3
		4	4	1	2	1	3	3	2	2		3	1						0,0521		
		5	2	1	1	2	2	1	2	1		1	3						0,0335		
		1	1	2	2	3	1	2	2	2		2	3						0,0309		
		2	2	1	1	4	2	1	1	1		3	2						0,0363		
104		3	3	1	1	4	3	3	1	2		3	2						0,0093		
	2670700	4	4	2	1	3	1	1	1	1		3	2	4	2670704	4	1	4	0,0073		1
		5	4	2	1	3	1	1	2	3		1	3						0,0128		
		1	1	2	2	3	5	3	1	3		2	3						0,0717		
		2	2	2	2	1	5	2	1	3		3	2						0,0726		
105	2694872	3	3	2	2	4	5	2	2	1		2	3	3	2694875	3	1	3	0,0106		1
		4	4	1	2	2	5	1	2	3		1	2						0,0607		
		5	1	2	2	2	3	1	2	1		1	1						0,0623		
		1	1	2	2	4	3	3	2	2		2	2						0,0538		
		2	2	1	1	2	3	2	2	3		2	2						0,0314		
106	2718752	3	3	1	1	1	4	3	2	3		2	3	3	2718757	5	1	3	0,0732		1
		4	4	2	1	4	4	2	2	3		1	2						0,0531		
		5	3	2	1	4	3	2	2	1		3	1						0,0003		
		1	1	1	2	2	3	1	1	3		1	1						0,0783		
		2	2	1	2	1	1	3	2	1		3	3						0,0204		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
107	2743144	3	3	1	1	2	5	1	1	3		2	3	3	2743148	4	1	3	0,0352		1
		4	4	1	1	4	5	1	2	1		2	2						0,0102		
		5	4	2	2	2	2	1	1	1		2	2						0,0679		
	2769382	1	1	2	2	3	3	2	2	3		2	1	1	2769387	5	1	1	0,0846		1
		2	2	1	1	2	2	3	1	1		2	1						0,0034		
108		3	3	2	2	2	5	1	1	3		3	1						0,0550		
		4	4	1	2	3	4	1	1	2		1	2						0,0375		
		5	2	1	1	3	4	2	1	2		2	3						0,0427		
	2793886	1	1	2	1	1	3	3	1	3		3	1	1	2793891	5	1	1	0,0523		1
		2	2	1	2	1	3	3	1	2		3	3						0,0569		
109		3	3	1	1	3	3	2	1	2		3	3						0,0795		
		4	4	2	2	2	3	2	2	1		3	2						0,0682		
		5	2	2	1	1	5	3	2	2		1	1						0,0039		
		1	1	1	2	2	3	2	1	2		1	1						0,0511		
		2	2	1	1	4	4	1	2	3		2	1						0,0254		
110	2821704	3	3	2	1	4	2	1	2	3		3	2	3	2821707	3	1	3	0,0855		4
		4	4	2	2	2	3	1	2	1		3	3						0,0663		
		5	3	1	1	2	3	2	2	3		2	1						0,0842		
		1	1	2	2	2	4	3	1	2		2	1						0,0851		
		2	2	2	2	2	2	3	1	1		3	1						0,0390		
111		3	3	2	2	3	5	3	2	2		2	2						0,0602		
	2848025	4	4	1	1	1	5	1	1	3		3	1	4	2848028	3	1	4	0,0922		1
		5	2	1	2	4	1	3	1	1		2	3						0,0348		
		1	1	1	1	1	2	1	1	2		1	2						0,0210		
	2873534	2	2	2	1	4	3	3	2	1		2	1	2	2873537	3	1	2	0,0911		1
112		3	3	2	2	3	1	3	2	3		1	2						0,0246		
		4	4	2	2	4	2	1	1	2		2	3						0,0086		
		5	2	2	1	3	3	2	2	2		1	3						0,0269		
		1	1	2	2	4	5	1	1	1		1	2						0,0562		
		2	2	2	2	2	2	3	2	1		2	1						0,0023		
113		3	3	2	2	1	1	1	1	3		3	1						0,0138		
	2901305	4	4	1	2	1	1	3	1	1		3	1	4	2901310	5	1	4	0,0061		1
		5	2	2	2	2	3	3	1	1		3	3						0,0843		
	2926975	1	1	1	1	3	4	3	2	3		2	3	1	2926978	3	1	1	0,0133		1
		2	2	2	1	1	4	2	1	1		2	3						0,0944		
114		3	3	2	1	3	5	1	2	2		3	1						0,0195		
		4	4	2	1	3	3	1	1	3		1	3						0,0932		
		5	1	1	2	1	1	3	1	2		2	2						0,0749		
	2950735	1	1	2	1	1	4	1	1	2		3	3	1	2950739	4	1	1	0,0324		3
		2	2	1	1	2	1	2	1	1		1	2						0,0045		
115		3	3	1	1	3	4	1	2	2		3	2						0,0484		
		4	4	2	1	3	2	1	1	3		2	1						0,0792		
		5	4	1	1	2	5	3	1	3		1	3						0,0312		
		1	1	2	2	4	4	1	1	3		2	1						0,0916		
		2	2	2	2	3	3	1	2	3		2	1						0,0735		
116		3	3	1	1	2	3	3	1	3		2	2						0,0074		
	2975908	4	4	1	1	2	2	3	2	3		3	3	4	2975911	3	1	4	0,0337		1
		5	2	1	1	3	2	3	1	2		3	2						0,0840		
		1	1	2	2	1	2	1	1	2		3	3						0,0116		
	2998715	2	2	2	1	3	2	1	1	2		3	1	2	2998720	5	1	2	0,0578		1
117		3	3	1	1	3	2	1	1	3		3	3						0,0280		
		4	4	2	1	3	3	3	2	1		1	2						0,0965		
		5	4	1	2	4	2	1	1	3		3	3						0,0826		
		1	1	2	1	3	3	1	1	1		1	3						0,0856		
		2	2	2	1	1	1	1	2	1		2	2						0,0190		
118		3	3	1	2	4	2	3	2	1		2	2						0,0425		
		4	4	2	2	2	3	3	2	2		3	1						0,0269		
	3021853	5	2	2	2	4	4	1	2	1		3	3	5	3021858	5	1	2	0,0686		1
		1	1	2	1	4	2	3	1	3		3	3						0,0954		
		2	2	2	2	1	2	3	2	2		3	1						0,0528		
119		3	3	1	2	4	1	2	1	2		3	1						0,0690		
	3046245	4	4	1	2	2	4	2	1	2		2	2	4	3046249	4	1	4	0,0006		1
		5	2	2	1	2	1	2	1	2		2	1						0,0175		
		1	1	2	1	4	1	2	2	2		3	2						0,0264		
		2	2	2	1	1	3	1	2	2		2	3						0,0897		
120		3	3	2	2	4	2	1	1	3		3	1						0,0685		
	3073679	4	4	1	2	1	3	1	1	2		3	2	4	3073683	4	1	4	0,0572		1
		5	3	2	1	4	3	2	1	3		1	2						0,0802		
		1	1	2	2	3	4	1	1	3		3	1						0,1469		
	3099847	2	2	2	2	1	1	3	1	2		2	3	2	3099852	5	0	2	0,2255		1
121		3	3	1	1	2	1	2	1	3		3	1						0,0723		
		4	4	2	2	2	1	1	1	2		2	2						0,1534		
		5	2	1	1	2	2	2	1	1		1	3						0,2435		
		1	1	1	2	2	5	2	1	1		1	1						0,1873		
	3099852	2	2	1	2	4	5	2	1	3		2	1	2	3099876	24	1	2	0,2050		5
122		3	3	2	2	3	3	1	2	2		1	1						0,0842		
		4	4	1	1	2	2	1	2	1		3	3						0,2047		
		5	2	1	2	2	2	3	1	3		2	2						0,0580		
		1	1	2	1	1	2	3	1	1		2	2						0,0004		
		2	2	2	1	3	2	3	1	3		3	3						0,0177		
123		3	3	1	2	3	1	3	1	2		2	1						0,0969		
	3128151	4	4	2	2	1	3	3	1	2		2	2	4	3128156	5	1	4	0,0435		1
		5	3	1	2	2	4	3	2	3		1	1						0,0499		
		1	1	2	1	1	4	3	2	1		3	1						0,0431		
		2	2	2	1	2	1	2	1	3		1	1						0,0114		
124		3	3	2	1	3	5	3	2	1		1	2						0,0394		
	3154453	4	4	2	1	3	3	2	1	3		2	2	4	3154456	3	1	4	0,0055		1
		5	1	1	2	4	2	1	2	2		2	3						0,0578		
		1	1	2	1	3	4	1	1	2		1	2						0,0962		
		2	2	2	2	2	1	2	1	1		1	2						0,0667		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
125		3	3	2	2	4	3	2	1	2		1	2						0,0139		
	3178493	4	4	2	1	1	3	3	1	3		2	2	4	3178498	5	1	4	0,0541		2
		5	3	2	2	2	3	3	1	3		2	2						0,0396		
		1	1	1	2	4	2	2	2	2		1	1						0,0273		
		2	2	2	1	2	2	1	2	3		2	2						0,0178		
126		3	3	1	1	3	3	3	1	3		2	3						0,0038		
		4	4	1	2	3	3	2	1	1		1	2						0,0804		
	3203091	5	2	1	1	3	5	3	2	1		1	3	5	3203094	3	1	2	0,0689		1
	3227212	1	1	2	2	2	2	2	1	1		3	3	1	3227216	4	1	1	0,0396		1
		2	2	1	2	1	2	1	2	3		1	1						0,0143		
127		3	3	2	1	3	1	3	2	2		2	2						0,0605		
		4	4	2	1	3	4	3	1	2		3	2						0,0292		
		5	4	1	2	2	5	3	2	3		2	1						0,0723		
	3254623	1	1	1	2	2	4	2	2	1		2	3	1	3254626	3	1	1	0,0961		1
		2	2	2	2	4	1	3	1	3		1	1						0,0439		
128		3	3	2	2	2	5	2	2	1		1	1						0,0960		
		4	4	2	1	4	5	3	2	2		1	1						0,0600		
		5	4	1	2	3	4	3	1	3		1	1						0,0153		
		1	1	1	2	4	4	3	2	3		2	3						0,0572		
		2	2	1	2	3	3	3	2	3		1	1						0,0140		
129	3280759	3	3	2	2	3	1	2	1	1		1	3	3	3280764	5	1	3	0,0210		1
		4	4	2	2	3	5	1	2	2		3	1						0,0816		
		5	2	2	2	2	4	1	1	1		1	3						0,0119		
	3305314	1	1	1	1	2	3	2	2	3		3	2	1	3305318	4	1	1	0,0331		1
		2	2	2	1	1	3	2	2	2		2	1						0,0065		
130		3	3	1	1	3	4	2	2	3		2	1						0,0859		
		4	4	1	2	3	3	1	1	2		3	1						0,0688		
		5	3	2	1	3	1	3	2	3		2	2						0,0609		
		1	1	2	2	3	4	3	2	3		1	2						0,0288		
		2	2	2	2	4	2	2	1	3		2	2						0,0556		
131	3330438	3	3	2	1	4	2	3	2	3		3	2	3	3330443	5	1	3	0,0988		1
		4	4	2	2	3	3	1	2	2		3	3						0,0047		
		5	2	2	1	4	4	3	2	2		3	2						0,0047		
	3357249	1	1	2	2	4	4	2	2	1		2	1	1	3357253	4	1	1	0,0695		2
		2	2	1	2	2	4	3	2	3		2	1						0,0019		
132		3	3	1	2	3	4	1	1	2		2	1						0,0879		
		4	4	1	2	3	4	1	2	3		1	1						0,0946		
		5	1	1	1	1	1	2	1	3		3	3						0,0738		
		1	1	2	1	4	1	1	1	3		1	1						0,0547		
		2	2	2	2	2	2	1	1	3		2	1						0,0235		
133		3	3	1	2	1	3	3	1	1		3	2						0,0321		
		4	4	1	1	1	1	1	1	1		2	1						0,0221		
	3384785	5	3	2	2	3	5	1	1	2		2	3	5	3384789	4	1	3	0,0787		1
	3409162	1	1	1	1	2	5	1	2	3		2	1	1	3409166	4	1	1	0,0160		1
		2	2	1	2	4	3	2	1	2		3	1						0,0559		
134		3	3	2	2	3	3	1	2	1		3	1						0,0814		
		4	4	1	2	3	3	1	2	3		3	2						0,0027		
		5	2	2	2	4	5	1	1	3		2	2						0,0194		
		1	1	2	1	3	1	1	2	1		2	1						0,0690		
	3431949	2	2	1	2	2	1	1	1	1		3	2	2	3431953	4	1	2	0,0904		1
135		3	3	2	1	3	2	3	1	2		1	1						0,0044		
		4	4	2	1	4	1	1	2	2		3	1						0,0207		
		5	4	2	1	2	2	3	1	3		1	3						0,0688		
		1	1	1	1	4	4	2	2	1		2	3						0,0128		
		2	2	2	2	4	5	2	1	1		1	2						0,0207		
136	3456980	3	3	1	2	2	4	2	2	1		2	3	3	3456983	3	1	3	0,0541		1
		4	4	2	1	1	5	2	1	2		2	2						0,0885		
		5	3	2	2	2	3	2	2	1		2	1						0,0878		
		1	1	1	2	1	5	1	1	2		2	1						0,0969		
		2	2	2	2	1	2	2	2	2		2	1						0,0834		
137		3	3	2	2	2	3	2	1	3		2	2						0,0628		
		4	4	1	2	2	3	3	1	3		2	1						0,0980		
	3485838	5	3	2	1	3	2	2	1	1		3	1	5	3485843	5	1	3	0,0940		1
		1	1	2	2	4	5	2	2	3		1	2						0,0502		
		2	2	2	2	2	3	2	2	1		3	3						0,0794		
138		3	3	2	2	1	5	3	2	1		3	2						0,0815		
		4	4	1	1	2	1	1	1	3		3	1						0,0992		
	3511960	5	4	1	1	3	3	2	1	3		2	2	5	3511964	4	1	4	0,0910		1
		1	1	1	2	3	1	3	2	3		1	3						0,0838		
		2	2	1	1	1	4	1	1	3		2	3						0,0891		
139		3	3	1	2	4	3	2	1	3		1	2						0,0019		
	3539235	4	4	2	1	2	3	2	1	3		2	1	4	3539238	3	1	4	0,0669		1
		5	3	1	1	2	2	3	1	3		3	2						0,0137		
		1	1	1	2	1	2	2	1	2		3	1						0,0840		
		2	2	2	2	3	5	3	1	1		2	2						0,0760		
140		3	3	2	2	3	2	2	1	2		2	3						0,0252		
		4	4	2	1	3	1	2	1	1		2	1						0,0791		
	3564379	5	3	2	1	3	5	3	1	3		3	1	5	3564382	3	1	3	0,0501		1
		1	1	2	1	1	1	2	1	3		3	2						0,0577		
		2	2	1	2	1	4	2	1	3		2	1						0,0777		
141	3590485	3	3	1	2	1	2	2	1	2		2	3	3	3590488	3	1	3	0,0743		1
		4	4	2	1	1	5	3	2	1		2	1						0,0960		
		5	3	1	1	2	3	3	2	1		3	1						0,0976		
		1	1	1	2	3	2	1	1	1		2	1						0,0894		
		2	2	1	1	1	5	3	2	1		1	2						0,0227		
142	3615263	3	3	1	2	1	3	3	1	1		2	2	3	3615267	4	1	3	0,0794		1
		4	4	1	1	3	5	3	1	1		3	3						0,0733		
		5	2	2	1	3	5	2	2	1		2	1						0,0232		
		1	1	2	2	3	5	3	1	1		1	3						0,0342		
	3639318	2	2	1	1	3	5	2	1	1		1	2	2	3639323	5	1	2	0,0029		1

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
143		3	3	2	1	4	4	1	1	2		2	2						0,0679		
		4	4	1	1	3	2	1	2	3		2	1						0,0216		
		5	1	1	1	1	4	3	2	1		1	1						0,0808		
		1	1	2	2	2	4	2	2	1		3	2						0,0203		
		2	2	1	2	3	1	2	1	2		2	1						0,0082		
144		3	3	1	1	1	4	1	2	3		1	1						0,0365		
		4	4	1	1	3	5	3	2	3		2	1						0,0104		
	3669057	5	2	2	2	1	4	1	1	3		2	1	5	3669061	4	1	2	0,0937		1
		1	1	2	1	1	5	2	1	3		2	1						0,0416		
		2	2	1	2	3	4	1	1	2		2	3						0,0125		
145		3	3	1	1	3	1	2	1	3		3	2						0,0372		
	3696487	4	4	2	1	3	4	2	2	2		3	1	4	3696490	3	1	4	0,0013		1
		5	4	1	2	4	2	1	1	1		2	1						0,0285		
		1	1	1	2	3	5	2	1	2		1	2						0,0440		
		2	2	1	2	3	1	2	2	1		3	3						0,0097		
146		3	3	2	2	4	5	3	2	2		2	3						0,0072		
		4	4	1	1	4	4	2	2	1		3	2						0,0487		
	3721260	5	1	1	1	2	1	3	1	1		2	1	5	3721265	5	1	1	0,0252		1
	3746404	1	1	2	2	3	4	1	2	2		1	2	1	3746408	4	1	1	0,0770		1
		2	2	2	1	1	5	3	2	3		3	1						0,0127		
147		3	3	1	1	1	2	2	2	2		1	2						0,0800		
		4	4	2	2	2	5	1	2	3		3	3						0,0408		
		5	4	1	1	2	1	3	1	1		1	3						0,0893		
		1	1	2	1	4	3	3	1	2		2	1						0,0766		
		2	2	1	1	1	3	3	1	2		2	1						0,0564		
148		3	3	2	2	3	4	1	2	3		3	3						0,0025		
	3769859	4	4	2	1	3	4	3	2	3		1	3	4	3769862	3	1	4	0,0145		1
		5	1	1	2	4	2	2	2	3		1	3						0,0522		
		1	1	1	2	2	5	2	1	1		1	2						0,0758		
		2	2	1	2	3	2	2	1	3		2	2						0,0698		
149		3	3	1	2	3	5	1	2	2		3	2						0,0501		
		4	4	1	2	4	5	3	1	3		3	1						0,0078		
	3798528	5	1	2	2	1	5	2	2	2		3	3	5	3798533	5	1	1	0,0628		1
		1	1	2	2	1	1	1	1	3		3	3						0,0976		
	3823477	2	2	2	1	4	2	2	2	3		1	3	2	3823480	3	1	2	0,0859		1
150		3	3	1	1	1	5	3	1	1		3	2						0,0990		
		4	4	2	2	4	1	1	1	3		2	3						0,0319		
		5	1	1	1	2	3	1	2	2		1	3						0,0058		
	3852813	1	1	1	1	1	2	1	1	3		3	2	1	3852817	4	0	1	0,0640		2
		2	2	2	1	2	5	2	2	1		1	3						0,0918		
151		3	3	1	2	3	2	1	2	1		1	3						0,0175		
		4	4	2	2	1	3	1	1	2		1	2						0,1871		
		5	3	2	2	1	5	2	2	3		2	1						0,0614		
		1	1	2	1	4	1	1	2	2		1	3						0,0207		
	3852817	2	2	2	2	3	4	1	1	1		2	1	2	3852836	19	1	2	0,0890		5
152		3	3	2	2	1	5	1	1	3		2	1						0,1014		
		4	4	1	2	4	3	1	2	3		2	3						0,1430		
		5	1	2	1	1	1	2	2	3		1	3						0,1122		
		1	1	1	1	2	5	2	1	3		3	1						0,0243		
	3880454	2	2	2	2	1	4	3	2	1		2	1	2	3880459	5	1	2	0,0012		1
153		3	3	2	1	3	4	2	1	3		1	2						0,0616		
		4	4	1	2	4	1	3	2	1		3	1						0,0001		
		5	1	1	1	2	1	1	2	3		1	1						0,0302		
		1	1	2	1	4	2	2	2	1		3	2						0,0637		
		2	2	1	2	3	4	1	2	1		2	3						0,0059		
154		3	3	2	1	2	4	1	1	3		3	2						0,0463		
		4	4	2	2	4	3	1	1	2		1	1						0,0106		
	3905659	5	2	2	2	4	5	3	1	2		1	1	5	3905662	3	1	2	0,0952		4
		1	1	2	2	3	4	1	1	3		3	2						0,0141		
		2	2	1	1	4	4	2	1	1		1	1						0,0107		
155		3	3	1	2	3	4	2	2	2		2	2						0,0199		
		4	4	2	2	3	2	3	2	2		2	1						0,0509		
	3934612	5	1	2	1	3	3	1	2	3		2	3	5	3934616	4	1	1	0,0365		1
		1	1	1	2	2	4	2	2	1		3	3						0,0129		
		2	2	1	1	2	5	2	1	1		2	3						0,0981		
156		3	3	1	2	4	5	1	1	2		3	1						0,0878		
	3959875	4	4	1	2	2	2	3	1	3		2	1	4	3959880	5	1	4	0,0225		1
		5	1	1	2	4	5	1	1	2		1	2						0,0225		
		1	1	1	1	3	3	1	1	2		3	1						0,0361		
		2	2	2	1	3	2	1	1	1		3	1						0,0777		
157		3	3	2	1	1	1	2	1	1		3	2						0,0184		
		4	4	2	2	3	2	3	2	2		2	2						0,0794		
	3987746	5	4	2	2	4	5	1	2	1		2	3	5	3987751	5	1	4	0,0453		1
		1	1	2	2	2	4	1	2	3		2	1						0,0513		
		2	2	2	2	1	3	3	2	2		1	2						0,0726		
158	4016232	3	3	1	1	2	2	2	1	3		1	3	3	4016235	3	1	3	0,0934		1
		4	4	1	2	2	1	3	2	2		2	3						0,0340		
		5	3	1	2	4	5	1	1	1		3	3						0,0893		
		1	1	1	2	4	2	2	2	2		2	2						0,0604		
		2	2	2	1	1	2	1	1	2		3	3						0,0632		
159		3	3	2	2	3	3	1	1	2		2	3						0,0893		
		4	4	2	1	4	5	2	2	1		1	3						0,0432		
	4039468	5	1	2	2	1	5	1	2	2		3	3	5	4039471	3	1	1	0,0866		1
		1	1	2	2	2	5	3	1	2		2	2						0,0898		
		2	2	2	1	2	3	1	1	3		1	3						0,0721		
160		3	3	2	1	1	1	1	2	3		1	3						0,0048		
		4	4	2	2	1	3	2	2	2		2	2						0,0311		
	4067647	5	1	1	1	4	1	3	1	2		2	2	5	4067650	3	1	1	0,0272		1
		1	1	2	2	3	2	2	1	1		2	2						0,0710		
		2	2	2	1	2	4	2	2	1		1	2						0,0596		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
161		3	3	2	2	1	3	1	2	1		2	1						0,0788		
	4095575	4	4	1	2	3	1	1	2	3		2	1	4	4095578	3	1	4	0,0437		1
		5	1	1	1	4	2	3	2	3		1	1						0,0848		
		1	1	2	2	2	4	2	1	2		2	2						0,0636		
		2	2	2	2	2	2	2	1	2		3	1						0,0399		
162	4118948	3	3	1	2	1	4	2	1	2		3	1	3	4118953	5	1	3	0,0250		1
		4	4	1	1	3	5	3	2	2		1	3						0,0839		
		5	1	2	2	1	3	3	1	3		1	1						0,0716		
		1	1	2	1	1	2	2	2	3		2	3						0,0006		
	4145270	2	2	2	1	1	4	3	1	2		3	1	2	4145275	5	1	2	0,0417		1
163		3	3	1	2	3	5	2	2	1		2	2						0,0620		
		4	4	1	1	1	2	1	1	1		3	3						0,0277		
		5	2	2	1	2	1	2	1	1		1	2						0,0036		
	4168048	1	1	2	1	3	3	3	2	1		2	3	1	4168051	3	1	1	0,0990		1
		2	2	2	1	1	3	1	1	3		2	2						0,0452		
164		3	3	1	2	1	1	1	1	3		1	2						0,0493		
		4	4	1	2	2	5	2	2	3		1	2						0,0673		
		5	4	1	1	2	5	1	2	2		1	3						0,0689		
		1	1	1	1	3	5	3	2	3		1	1						0,0390		
		2	2	1	1	3	3	3	2	2		3	2						0,0786		
165	4190811	3	3	2	2	1	2	1	2	1		2	3	3	4190816	5	1	3	0,0191		1
		4	4	2	2	3	1	1	1	2		3	2						0,0851		
		5	1	2	1	4	3	3	2	2		2	2						0,0313		
		1	1	1	2	2	5	1	1	1		3	1						0,0265		
		2	2	1	1	1	1	3	2	2		2	1						0,0950		
166		3	3	1	1	4	4	2	2	2		3	2						0,0710		
	4216742	4	4	2	2	2	3	3	2	2		2	1	4	4216746	4	1	4	0,0207		1
		5	2	1	1	1	3	2	2	1		2	1						0,0451		
		1	1	2	1	2	3	2	2	3		3	2						0,0905		
		2	2	1	1	2	3	3	1	3		2	1						0,0117		
167		3	3	2	1	4	5	2	1	1		1	2						0,0793		
	4245513	4	4	1	2	3	3	2	1	3		1	3	4	4245518	5	1	4	0,0676		4
		5	3	1	1	3	5	3	2	1		3	2						0,0401		
	4274033	1	1	1	1	1	1	2	2	1		3	2	1	4274036	3	1	1	0,0337		1
		2	2	1	1	3	5	1	1	2		1	2						0,0618		
168		3	3	1	1	2	3	3	2	3		2	3						0,0214		
		4	4	1	1	3	3	2	1	1		3	1						0,0989		
		5	2	2	1	2	4	2	2	1		1	3						0,0486		
		1	1	1	2	2	2	1	2	2		3	2						0,0888		
		2	2	2	1	1	4	2	2	3		2	3						0,0297		
169		3	3	1	2	1	3	3	1	2		3	3						0,0550		
	4297009	4	4	2	1	2	4	2	1	2		2	1	4	4297012	3	1	4	0,0996		1
		5	1	1	1	3	1	3	2	3		1	2						0,0745		
		1	1	1	1	1	2	2	2	2		2	1						0,0468		
		2	2	2	2	4	5	2	2	3		1	1						0,0258		
170		3	3	1	2	1	3	1	2	3		1	2						0,0147		
		4	4	2	1	1	1	1	1	1		3	3						0,0901		
	4326413	5	3	2	1	1	4	1	1	3		2	3	5	4326418	5	1	3	0,0044		1
		1	1	2	2	4	4	1	1	3		2	2						0,0366		
		2	2	1	1	4	4	3	2	3		1	1						0,0048		
171		3	3	2	1	1	4	1	2	2		3	1						0,0900		
	4351966	4	4	2	2	3	3	1	2	2		2	1	4	4351970	4	1	4	0,0702		1
		5	2	1	1	2	1	3	1	3		2	2						0,0946		
	4381276	1	1	2	1	3	2	2	2	2		2	1	1	4381279	3	1	1	0,0890		1
		2	2	1	2	3	1	1	1	1		1	1						0,0545		
172		3	3	1	1	4	2	2	2	3		3	1						0,0189		
		4	4	1	1	2	2	2	1	3		1	2						0,0630		
		5	4	1	1	4	3	1	2	1		3	1						0,0663		
		1	1	1	1	1	5	3	1	2		1	3						0,0722		
		2	2	1	2	2	2	1	1	3		3	2						0,0806		
173		3	3	2	2	3	2	2	1	1		1	2						0,0883		
	4407376	4	4	2	1	4	2	1	2	3		1	2	4	4407381	5	1	4	0,0037		1
		5	4	2	2	1	4	1	1	1		1	1						0,0447		
	4433387	1	1	2	2	2	1	3	2	3		3	2	1	4433391	4	1	1	0,0055		1
		2	2	2	2	4	3	1	2	3		1	2						0,0965		
174		3	3	2	1	4	3	1	1	2		3	3						0,0503		
		4	4	1	2	4	2	2	2	3		3	3						0,0725		
		5	4	1	1	4	5	3	1	1		3	3						0,0481		
		1	1	1	1	3	4	1	2	2		2	1						0,0441		
	4460936	2	2	2	2	3	1	1	1	2		3	2	2	4460939	3	1	2	0,0207		2
175		3	3	2	2	1	5	3	2	1		3	2						0,0694		
		4	4	1	2	2	4	2	1	2		2	3						0,0801		
		5	1	1	2	1	2	2	2	2		3	3						0,0438		
		1	1	1	1	1	1	3	1	1		3	3						0,0072		
		2	2	2	2	2	3	1	1	3		1	2						0,0003		
176		3	3	2	2	2	4	3	1	3		3	2						0,0360		
	4487544	4	4	2	2	2	4	1	2	2		2	1	4	4487549	5	1	4	0,0876		3
		5	1	1	1	1	5	2	1	2		2	2						0,0598		
		1	1	1	2	4	1	2	2	1		2	3						0,0673		
	4512832	2	2	1	1	4	5	3	1	3		3	3	2	4512837	5	1	2	0,0767		1
177		3	3	1	1	4	3	2	1	1		3	3						0,0512		
		4	4	1	2	4	2	1	2	2		2	3						0,0650		
		5	4	2	2	2	4	2	1	2		2	2						0,0340		
	4542672	1	1	2	1	4	4	3	2	3		1	1	1	4542677	5	1	1	0,0889		1
		2	2	2	2	4	1	2	2	1		2	1						0,0380		
178		3	3	2	1	4	3	3	1	1		1	2						0,0069		
		4	4	1	2	4	4	3	2	3		1	2						0,0753		
		5	1	1	2	3	1	2	2	2		3	3						0,0301		
	4568666	1	1	1	1	3	3	1	2	1		2	2	1	4568670	4	1	1	0,0673		1
		2	2	1	2	3	1	2	2	3		3	2						0,0439		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
179		3	3	1	2	4	2	2	2	2		1	2						0,0072		
		4	4	1	2	1	3	1	1	1		1	1						0,0453		
		5	4	1	2	1	3	2	1	2		1	3						0,0779		
		1	1	2	2	4	1	1	1	1		3	3						0,0743		
		2	2	2	1	2	2	2	2	3		2	3						0,0317		
180	4593551	3	3	2	1	4	4	2	1	3		2	1	3	4593555	4	1	3	0,0249		3
		4	4	1	2	1	5	3	1	2		2	3						0,0682		
		5	3	2	1	1	3	2	2	1		3	1						0,0510		
		1	1	2	2	1	3	2	1	2		3	3						0,0715		
		2	2	2	2	1	5	3	1	2		3	1						0,0023		
181		3	3	1	2	1	5	3	1	2		2	1						0,0059		
	4621687	4	4	1	2	1	3	2	2	1		2	2	4	4621691	4	1	4	0,0268		1
		5	1	1	2	2	4	2	1	1		2	1						0,0914		
		1	1	1	1	1	4	1	1	2		3	1						0,0501		
	4647140	2	2	2	2	3	1	3	1	1		1	3	2	4647144	4	1	2	0,0455		1
182		3	3	1	2	1	4	2	2	2		1	2						0,0783		
		4	4	2	2	3	1	1	1	1		1	1						0,0498		
		5	1	2	2	1	5	3	1	1		3	1						0,0856		
		1	1	2	1	3	5	1	2	3		3	3						0,0592		
		2	2	2	2	4	1	2	1	3		2	2						0,0359		
183		3	3	1	1	1	4	2	1	2		2	1						0,0991		
		4	4	2	2	3	1	2	1	2		1	2						0,0736		
	4675085	5	4	1	2	2	5	2	2	3		3	1	5	4675090	5	1	4	0,0878		1
		1	1	1	1	4	3	2	1	1		3	1						0,0474		
		2	2	2	2	3	1	2	1	1		2	3						0,0294		
184		3	3	2	1	2	3	1	1	1		1	3						0,0437		
		4	4	1	1	1	3	2	1	1		2	3						0,0838		
	4704847	5	1	2	2	3	3	3	1	2		1	1	5	4704852	5	1	1	0,0147		1
		1	1	2	1	1	3	2	1	3		3	3						0,0841		
		2	2	1	2	4	5	2	1	1		3	3						0,0298		
185	4727836	3	3	2	1	4	3	3	1	2		3	2	3	4727840	4	1	3	0,0191		1
		4	4	1	2	3	5	2	1	1		2	2						0,0822		
		5	1	1	2	3	1	2	1	1		2	1						0,0097		
		1	1	1	2	2	1	1	2	2		1	3						0,0030		
		2	2	2	1	3	1	2	2	3		1	2						0,0643		
186	4757585	3	3	1	2	4	2	3	2	2		3	2	3	4757590	5	1	3	0,0985		1
		4	4	1	2	1	1	3	1	1		3	2						0,0900		
		5	4	1	1	4	5	1	2	3		1	1						0,0900		
		1	1	1	2	1	4	3	1	2		2	3						0,0110		
		2	2	2	1	2	3	1	2	2		3	3						0,0574		
187		3	3	2	2	4	4	2	2	2		1	1						0,0355		
		4	4	1	2	4	1	1	2	3		2	2						0,0700		
	4782148	5	4	1	1	2	1	1	1	3		3	1	5	4782152	4	1	4	0,0965		1
		1	1	1	2	3	2	1	2	2		1	1						0,0360		
		2	2	2	2	2	3	2	2	1		1	2						0,0813		
188		3	3	2	2	1	3	1	2	3		2	3						0,0113		
		4	4	1	2	1	4	3	1	1		3	2						0,0757		
	4810828	5	4	2	2	3	2	2	1	1		1	3	5	4810832	4	1	4	0,0062		1
		1	1	1	2	2	5	2	2	1		1	2						0,0000		
		2	2	2	2	3	2	1	1	3		2	3						0,0693		
189	4836375	3	3	1	1	2	4	1	2	2		3	2	3	4836378	3	1	3	0,0092		3
		4	4	2	2	1	1	3	2	2		1	2						0,0544		
		5	4	2	1	2	2	2	1	3		2	2						0,0172		
		1	1	2	1	2	3	1	2	2		1	1						0,0161		
		2	2	1	2	1	2	1	2	3		3	3						0,0391		
190	4865717	3	3	1	1	1	4	3	1	2		1	3	3	4865721	4	1	3	0,0338	301	2
		4	4	2	1	2	2	3	2	1		3	1						0,0377		
		5	3	1	2	2	5	3	1	3		1	2						0,0738		
		1	1	2	2	2	4	2	1	2		3	2						0,1136		
		2	2	1	1	1	3	2	1	2		2	1						0,1636		
191		3	3	2	1	3	3	3	2	3		2	3						0,1392		
		4	4	2	1	4	4	3	2	1		1	3						0,1016		
	4892639	5	1	2	1	3	2	2	2	2		3	2	5	4892643	4	0	1	0,1906		1
		1	1	2	2	1	2	3	1	2		2	2						0,1219		
		2	2	1	1	2	3	3	1	1		3	3						0,1918		
192		3	3	2	2	1	3	3	2	3		2	1						0,0302		
	4892643	4	4	1	2	1	5	1	1	2		2	3	4	4892661	18	0	4	0,0277		5
		5	4	1	2	4	4	2	1	3		1	2						0,2454		
		1	1	1	2	4	2	2	2	1		2	1						0,2006		
		2	2	2	2	3	5	1	1	3		1	3						0,1942		
193		3	3	2	2	2	3	1	2	2		2	1						0,2412		
	4892661	4	4	2	1	3	3	2	1	3		1	1	4	4892677	16	0	4	0,0263		5
		5	4	2	1	4	4	2	2	3		2	1						0,0758		
		1	1	2	1	2	1	3	1	2		1	3						0,0052		
		2	2	2	1	2	3	1	1	3		2	2						0,0779		
194	4892677	3	3	1	2	2	3	2	2	3		1	2	3	4892697	20	1	3	0,0918		6
		4	4	1	2	3	5	1	1	2		2	3						0,0735		
		5	2	2	1	4	4	3	2	2		1	3						0,1116		
		1	1	2	2	4	4	3	2	1		2	2						0,0684		
	4919387	2	2	1	2	2	1	3	2	2		3	3	2	4919390	3	1	2	0,0527		1
195		3	3	1	2	4	2	3	2	3		1	1						0,0116		
		4	4	1	1	1	2	2	1	1		1	3						0,0277		
		5	2	2	2	3	2	2	1	1		1	2						0,0222		
		1	1	2	2	1	4	2	2	1		1	1						0,0323		
	4947278	2	2	2	2	1	5	3	1	2		1	3	2	4947281	3	1	2	0,0252		1
196		3	3	1	1	2	1	1	2	2		1	3						0,0396		
		4	4	2	1	2	3	3	1	2		2	2						0,0965		
		5	1	2	2	4	3	1	1	1		3	2						0,0396		
	4974584	1	1	2	1	4	5	3	2	1		3	1	1	4974588	4	1	1	0,0177		1
		2	2	2	2	4	5	1	1	2		2	3						0,0870		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
197		3	3	1	1	3	5	2	1	3		1	2						0,0811		
		4	4	2	1	1	2	2	1	2		1	1						0,0882		
		5	4	2	1	2	4	1	2	1		2	1						0,0153		
		1	1	2	1	4	5	3	1	3		3	1						0,0471		
		2	2	2	2	2	4	3	1	2		3	1						0,0545		
198		3	3	2	2	1	4	3	2	3		3	1						0,0066		
		4	4	2	2	4	4	2	2	1		1	1						0,0482		
	5001145	5	1	1	2	1	1	1	2	3		2	2	5	5001148	3	1	1	0,0407		1
		1	1	2	2	3	2	3	1	2		2	2						0,0166		
		2	2	2	2	1	5	3	1	3		1	3						0,0244		
199	5024813	3	3	1	2	1	4	2	2	2		3	1	3	5024816	3	1	3	0,0117		1
		4	4	1	1	2	2	2	1	2		1	1						0,0708		
		5	4	1	1	4	3	3	2	1		1	3						0,0248		
		1	1	1	2	1	4	3	2	3		3	1						0,0423		
		2	2	2	2	3	1	3	1	3		1	1						0,0172		
200		3	3	2	2	2	1	2	2	3		3	2						0,0509		
	5047421	4	4	1	2	4	4	2	2	1		1	3	4	5047424	3	1	4	0,0143		1
		5	3	1	1	2	1	2	1	2		2	1						0,0690		
	5073155	1	1	2	2	2	5	1	2	2		2	3	1	5073159	4	1	1	0,0922		1
		2	2	2	1	1	3	3	1	3		2	2						0,0858		
201		3	3	1	1	1	5	2	2	3		3	1						0,0012		
		4	4	1	2	3	5	3	1	2		1	3						0,0592		
		5	2	2	1	2	1	1	2	2		3	2						0,0655		
		1	1	2	2	4	2	3	2	3		2	2						0,0963		
		2	2	2	2	2	1	2	2	1		3	1						0,0216		
202		3	3	2	2	1	2	2	2	1		3	1						0,0908		
	5101737	4	4	1	2	2	3	2	2	3		2	3	4	5101742	5	1	4	0,0228		1
		5	4	2	2	4	1	2	1	3		3	3						0,0031		
		1	1	1	1	1	3	2	1	2		1	1						0,0273		
		2	2	2	2	2	2	2	1	1		1	1						0,0097		
203		3	3	1	1	3	2	2	1	2		1	1						0,0847		
	5124392	4	4	2	2	1	2	3	1	3		2	2	4	5124396	4	1	4	0,0404		1
		5	1	1	2	1	1	2	1	1		3	3						0,0257		
		1	1	1	2	4	5	1	1	3		1	2						0,0395		
		2	2	1	1	4	4	1	1	3		1	3						0,0555		
204		3	3	2	1	3	2	3	1	2		1	2						0,0417		
	5152110	4	4	2	1	1	5	2	1	3		1	2	4	5152115	5	1	4	0,0444		1
		5	2	1	2	3	4	1	2	2		2	3						0,0107		
		1	1	1	1	3	1	1	2	2		1	2						0,0992		
		2	2	1	1	4	1	3	1	1		3	2						0,0427		
205	5176369	3	3	1	2	4	4	2	1	1		1	1	3	5176374	5	1	3	0,0912		1
		4	4	2	2	3	1	3	1	2		3	2						0,0696		
		5	3	1	2	2	1	3	2	1		3	3						0,0882		
		1	1	2	2	1	5	3	2	2		1	2						0,0713		
		2	2	1	2	3	5	2	2	1		2	3						0,0014		
206	5203330	3	3	1	1	4	2	3	2	1		2	3	3	5203333	3	1	3	0,0176		1
		4	4	1	2	1	5	2	2	1		1	3						0,0600		
		5	2	2	2	2	3	3	1	2		2	1						0,0665		
		1	1	2	2	3	3	2	2	3		1	2						0,0185		
	5228460	2	2	2	1	1	4	3	1	3		3	1	2	5228463	3	1	2	0,0525		4
207		3	3	1	2	2	2	3	2	3		1	3						0,0392		
		4	4	2	1	4	4	2	1	3		3	2						0,0552		
		5	2	1	1	1	4	1	1	2		1	1						0,0751		
		1	1	2	1	3	5	2	1	1		2	3						0,0647		
		2	2	2	1	3	4	1	2	2		1	1						0,0567		
208	5255296	3	3	1	2	4	1	2	2	2		3	2	3	5255301	5	1	3	0,0791		1
		4	4	2	1	1	4	1	1	1		1	2						0,0961		
		5	3	2	1	1	3	1	2	1		2	3						0,0404		
	5281575	1	1	2	1	4	2	1	1	1		1	3	1	5281579	4	1	1	0,0937		1
		2	2	1	2	4	4	3	1	3		2	3						0,0249		
209		3	3	1	2	3	2	1	1	2		1	3						0,0474		
		4	4	2	2	2	3	2	1	3		3	3						0,0197		
		5	3	2	2	2	1	2	1	2		1	1						0,0400		
		1	1	1	2	3	4	1	1	1		1	1						0,0588		
		2	2	1	2	3	5	1	2	2		3	3						0,0762		
210		3	3	2	1	2	2	2	2	3		1	2						0,0559		
		4	4	1	2	3	5	3	2	1		1	2						0,0406		
	5309901	5	1	2	2	4	3	1	1	2		2	2	5	5309906	5	1	1	0,0287		2
	5339389	1	1	2	2	4	2	3	1	1		3	3	1	5339393	4	1	1	0,0167		1
		2	2	1	1	3	1	2	2	3		3	2						0,0196		
211		3	3	1	1	3	2	1	1	1		2	2						0,0077		
		4	4	1	2	1	3	1	2	3		1	3						0,0548		
		5	3	1	2	2	4	1	1	1		1	3						0,0363		
		1	1	1	1	4	1	1	2	2		3	2						0,0832		
		2	2	1	2	1	1	1	1	3		2	3						0,0155		
212		3	3	2	2	1	5	1	2	3		3	3						0,0702		
		4	4	2	2	1	2	3	2	1		2	2						0,0873		
	5365069	5	3	2	1	1	5	1	2	2		1	1	5	5365073	4	1	3	0,0310		4
		1	1	2	2	3	4	2	1	2		3	3						0,0700		
		2	2	1	1	2	2	2	1	3		1	1						0,0883		
213		3	3	1	1	1	5	3	1	2		2	1						0,0961		
	5391830	4	4	2	2	3	5	1	2	3		2	3	4	5391833	3	1	4	0,0669		1
		5	1	1	2	2	1	1	2	2		3	3						0,0753		
		1	1	1	2	2	5	2	2	3		2	1						0,1648		
		2	2	1	2	1	2	1	1	1		1	3						0,0137		
214		3	3	2	1	1	1	2	1	1		2	3						0,0077		
		4	4	2	1	2	3	3	1	2		1	1						0,1724		
	5421251	5	2	1	2	3	3	3	1	2		2	2	5	5421254	3	0	2	0,2047	250	3
		1	1	1	1	1	2	1	2	3		3	1						0,0081		
		2	2	2	2	2	5	3	2	1		3	2						0,2074		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
215		3	3	2	2	2	2	1	2	3		1	2						0,2336		
	5421254	4	4	2	1	3	4	2	1	1		3	1	4	5421274	20	1	4	0,0462		5
		5	3	2	1	3	2	3	2	2		2	1						0,0955		
		1	1	1	1	1	4	3	2	3		2	1						0,0096		
	5447932	2	2	1	1	1	5	2	1	2		2	3	2	5447936	4	1	2	0,0557		1
216		3	3	2	2	2	2	1	1	1		2	3						0,0850		
		4	4	1	1	2	3	3	2	2		3	2						0,0444		
		5	3	2	1	3	3	3	1	3		3	3						0,0166		
		1	1	2	1	2	3	3	2	1		2	3						0,0344		
		2	2	2	2	3	1	3	1	1		2	2						0,0544		
217	5472831	3	3	1	1	2	1	2	2	2		2	2	3	5472834	3	1	3	0,0749		1
		4	4	1	1	1	2	2	2	1		2	1						0,0412		
		5	2	1	1	4	3	2	1	2		2	2						0,0741		
		1	1	2	2	2	1	2	1	2		2	1						0,0793		
		2	2	2	2	3	5	1	2	1		3	2						0,0832		
218	5497918	3	3	1	2	2	3	1	1	2		3	1	3	5497923	5	1	3	0,0814		1
		4	4	1	1	3	1	3	1	3		3	2						0,0940		
		5	4	2	2	4	1	3	1	3		2	2						0,0263		
	5523982	1	1	1	1	1	4	1	1	2		2	2	1	5523985	3	1	1	0,0702		1
		2	2	1	2	2	2	2	2	2		1	2						0,0709		
219		3	3	2	2	2	1	1	2	2		3	1						0,0879		
		4	4	2	1	4	2	1	1	2		1	1						0,0305		
		5	1	2	2	4	4	2	2	3		2	3						0,0921		
		1	1	2	1	2	2	2	1	3		1	3						0,0319		
		2	2	1	1	3	2	2	1	3		1	1						0,0021		
220		3	3	2	2	2	5	1	2	2		1	1						0,0907		
		4	4	1	2	3	4	3	2	3		3	3						0,0161		
	5547950	5	2	2	1	4	4	3	2	2		2	2	5	5547955	5	1	2	0,0276		1
		1	1	2	2	4	1	1	2	3		2	2						0,0046		
		2	2	2	2	1	3	2	1	3		1	2						0,0459		
221		3	3	1	1	3	3	2	2	1		3	1						0,0479		
		4	4	1	2	3	3	3	2	1		1	2						0,0594		
	5570851	5	3	1	1	4	4	2	1	1		3	3	5	5570855	4	1	3	0,0874		1
		1	1	1	2	1	5	2	2	1		3	3						0,0493		
	5598881	2	2	1	1	2	1	1	2	3		2	1	2	5598884	3	1	2	0,0097		1
222		3	3	1	1	4	1	3	2	3		2	2						0,0732		
		4	4	2	2	1	3	3	1	3		1	3						0,0822		
		5	3	2	2	1	3	2	1	1		3	1						0,0468		
		1	1	1	2	1	3	2	2	2		2	1						0,0114		
		2	2	2	1	4	1	3	2	1		3	3						0,0057		
223		3	3	2	1	3	3	2	2	1		1	3						0,0869		
	5626512	4	4	1	1	1	5	3	2	2		3	1	4	5626517	5	1	4	0,0343		1
		5	2	1	2	3	2	1	1	3		3	3						0,0129		
		1	1	2	1	4	5	1	2	3		3	2						0,0276		
		2	2	1	2	4	4	2	1	2		1	2						0,0442		
224		3	3	1	2	2	5	1	1	1		2	3						0,0195		
	5650410	4	4	1	2	3	5	2	2	3		1	1	4	5650415	5	1	4	0,0374		1
		5	3	2	2	2	1	3	1	3		3	2						0,0505		
		1	1	1	2	4	5	1	1	2		2	2						0,0368		
		2	2	2	2	1	4	3	1	3		3	1						0,0346		
225		3	3	1	1	1	3	2	2	3		1	3						0,0678		
		4	4	1	1	2	2	3	1	1		2	2						0,0952		
	5676665	5	1	2	1	4	4	2	2	3		2	3	5	5676670	5	1	1	0,0114		1
		1	1	2	1	4	1	1	2	1		1	2						0,0657		
		2	2	1	2	1	5	2	1	1		2	2						0,0360		
226	5703972	3	3	1	2	1	4	1	1	3		3	1	3	5703977	5	1	3	0,0336		1
		4	4	2	1	2	2	1	1	2		1	1						0,0213		
		5	2	1	2	3	5	3	2	2		3	1						0,0997		
		1	1	1	1	4	2	2	1	3		2	1						0,0666		
		2	2	2	1	2	5	2	2	2		3	2						0,0306		
227		3	3	2	1	2	3	3	2	3		2	2						0,0961		
		4	4	2	2	3	5	3	2	1		1	3						0,0152		
	5728336	5	4	1	2	3	4	3	2	1		2	2	5	5728340	4	1	4	0,0726		4
		1	1	2	2	4	1	3	2	1		3	2						0,0883		
		2	2	1	1	2	2	2	2	1		2	2						0,0639		
228		3	3	1	2	1	2	1	1	1		3	1						0,0464		
	5756830	4	4	2	2	4	5	2	1	3		3	3	4	5756833	3	1	4	0,0352		1
		5	2	2	2	3	1	2	2	2		1	2						0,0925		
		1	1	1	1	1	2	2	1	3		1	3						0,0593		
		2	2	2	1	3	5	3	1	2		2	1						0,0406		
229		3	3	1	1	4	3	1	2	3		2	1						0,0273		
	5781146	4	4	2	2	4	4	1	2	1		1	1	4	5781149	3	1	4	0,0953		2
		5	3	1	2	3	5	1	2	1		2	1						0,0261		
		1	1	2	2	1	1	3	2	3		2	3						0,0801		
		2	2	1	2	3	3	3	2	3		2	3						0,0704		
230		3	3	1	2	1	1	1	2	2		3	1						0,0331		
	5806352	4	4	2	2	2	1	2	1	1		3	1	4	5806356	4	1	4	0,0180		1
		5	4	2	1	1	2	3	2	3		2	3						0,0424		
		1	1	2	2	3	2	2	1	3		2	3						0,0422		
	5835450	2	2	2	1	4	2	2	2	3		2	1	2	5835454	4	1	2	0,0881		1
231		3	3	2	2	4	5	1	1	3		3	3						0,0834		
		4	4	2	1	4	1	3	1	1		3	1						0,0630		
		5	2	2	2	1	2	3	2	1		1	3						0,0352		
		1	1	2	1	3	3	2	1	2		2	3						0,0404		
		2	2	2	1	3	2	3	2	2		2	3						0,0536		
232	5859875	3	3	2	2	4	5	1	2	1		2	2	3	5859879	4	1	3	0,0282		4
		4	4	2	1	2	2	2	2	3		3	2						0,0328		
		5	1	2	2	1	1	1	2	2		3	1						0,0046		
		1	1	1	1	1	2	1	1	3		1	1						0,0421		
		2	2	1	2	2	4	2	2	2		3	1						0,0614		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
233	5887889	3	3	1	2	3	2	1	2	1		3	2	3	5887893	4	1	3	0,0831		1
		4	4	1	2	4	4	2	1	1		1	3						0,0708		
		5	2	1	2	2	1	3	2	2		2	3						0,0002		
		1	1	1	2	4	4	2	2	3		3	3						0,0908		
		2	2	2	2	3	5	3	1	2		1	1						0,0524		
234	5913215	3	3	2	1	4	3	3	2	1		3	1	3	5913220	5	1	3	0,0202		1
		4	4	1	2	1	4	3	1	3		3	1						0,0559		
		5	4	1	1	2	1	2	2	2		1	3						0,0049		
		1	1	1	2	4	5	3	2	1		1	1						0,0430		
	5937069	2	2	1	2	1	3	1	2	3		1	1	2	5937072	3	1	2	0,0581		1
235		3	3	2	1	4	3	2	1	2		3	3						0,0804		
		4	4	1	1	1	4	2	2	1		2	3						0,0227		
		5	1	2	2	1	2	3	2	2		3	1						0,0212		
		1	1	1	2	3	5	1	2	3		2	1						0,0033		
		2	2	2	1	4	5	2	2	3		3	1						0,0504		
236		3	3	1	1	1	2	3	2	3		3	1						0,0409		
	5961852	4	4	2	2	4	4	2	2	2		3	2	4	5961856	4	1	4	0,0655		1
		5	1	1	2	3	4	1	1	3		3	2						0,0106		
		1	1	2	1	2	3	3	2	1		1	3						0,0297		
		2	2	1	2	2	4	3	2	2		1	1						0,0018		
237		3	3	1	1	2	1	3	1	1		3	2						0,0452		
	5989131	4	4	1	1	4	5	2	1	3		1	1	4	5989136	5	1	4	0,0303		1
		5	2	2	1	1	3	3	1	1		1	1						0,0838		
		1	1	2	1	3	1	1	1	2		1	3						0,0490		
	6016135	2	2	2	1	3	1	1	1	1		3	2	2	6016138	3	1	2	0,0407		1
238		3	3	2	2	4	3	1	1	2		2	3						0,0855		
		4	4	1	2	4	3	2	1	3		2	1						0,0708		
		5	1	2	2	4	2	1	2	2		3	3						0,0056		
		1	1	2	2	1	4	2	2	1		2	2						0,0668		
		2	2	1	2	2	5	2	1	2		2	1						0,0708		
239		3	3	2	1	2	3	2	1	2		2	3						0,0522		
		4	4	2	1	2	4	2	1	2		3	3						0,0807		
	6045964	5	4	1	2	4	4	2	2	2		3	2	5	6045967	3	1	4	0,0249		1
		1	1	1	2	3	2	3	2	2		2	1						0,0113		
		2	2	1	2	3	5	3	1	3		1	1						0,0379		
240		3	3	1	1	2	5	2	2	2		2	3						0,0792		
		4	4	1	2	3	4	1	1	2		1	2						0,0866		
	6069747	5	3	1	1	3	5	2	1	1		1	1	5	6069750	3	1	3	0,0682		1
	6096193	1	1	1	1	3	1	2	2	2		3	2	1	6096198	5	1	1	0,0853		4
		2	2	2	1	1	2	3	1	2		3	1						0,0483		
241		3	3	1	2	1	4	3	1	1		2	2						0,0803		
		4	4	1	1	4	3	3	2	2		3	2						0,0759		
		5	4	2	1	2	2	2	1	3		2	2						0,0530		
		1	1	1	2	4	4	3	1	3		3	3						0,0910		
		2	2	2	1	2	3	3	2	3		2	2						0,0257		
242	6119127	3	3	1	1	2	4	3	1	2		1	1	3	6119132	5	1	3	0,0484		1
		4	4	1	2	4	5	3	1	2		1	3						0,0888		
		5	2	2	1	4	1	1	1	3		3	3						0,0531		
		1	1	2	1	3	2	3	2	3		2	1						0,0509		
		2	2	2	1	1	3	3	2	3		3	3						0,0264		
243		3	3	1	1	3	5	2	2	1		2	2						0,0003		
	6146910	4	4	1	2	3	1	3	2	2		1	2	4	6146915	5	1	4	0,0633		1
		5	3	1	2	1	5	3	2	3		2	1						0,0080		
		1	1	2	1	3	4	2	2	3		1	2						0,0454		
		2	2	2	2	3	1	3	1	2		3	1						0,0176		
244		3	3	1	1	4	2	1	2	3		1	2						0,0517		
		4	4	2	2	1	2	3	2	2		1	3						0,0423		
	6170203	5	1	2	1	4	4	1	1	1		3	2	5	6170208	5	1	1	0,0586		1
		1	1	2	1	2	3	3	2	3		1	2						0,0492		
		2	2	2	2	4	4	3	1	1		3	3						0,0480		
245		3	3	2	2	4	4	1	2	3		3	1						0,0053		
	6193754	4	4	1	1	2	1	1	1	2		1	3	4	6193759	5	1	4	0,0411		1
		5	2	2	1	1	2	1	2	1		1	2						0,0494		
		1	1	1	2	2	1	3	2	1		1	3						0,0194		
		2	2	1	2	2	3	2	1	3		2	1						0,0340		
246		3	3	2	2	2	4	3	2	3		2	2						0,0221		
	6221785	4	4	1	1	4	2	1	1	1		2	1	4	6221789	4	1	4	0,0559		1
		5	4	1	2	1	3	3	1	2		2	3						0,0004		
	6250928	1	1	1	1	2	5	1	1	3		1	1	1	6250932	4	1	1	0,0643		1
		2	2	1	1	2	4	1	1	3		3	3						0,0407		
247		3	3	2	2	3	3	3	1	3		1	1						0,0112		
		4	4	2	1	2	4	1	2	2		3	2						0,0482		
		5	1	2	1	2	3	2	2	2		2	1						0,0268		
		1	1	2	1	2	4	2	2	1		1	1						0,0806		
		2	2	2	1	2	3	3	1	1		3	2						0,0339		
248		3	3	1	1	1	1	1	1	2		3	3						0,0735		
	6275154	4	4	2	1	4	3	3	2	2		1	3	4	6275159	5	1	4	0,0975		1
		5	3	2	1	1	2	2	2	2		3	1						0,0651		
		1	1	2	2	2	4	1	2	3		3	2						0,0116		
	6298796	2	2	1	1	1	3	2	1	1		1	1	2	6298800	4	1	2	0,0800		1
249		3	3	1	1	2	2	2	2	1		3	2						0,0611		
		4	4	1	1	2	1	3	2	2		2	1						0,0822		
		5	4	1	2	1	3	1	2	2		3	3						0,0452		
		1	1	2	1	1	2	3	1	2		2	1						0,0746		
	6321556	2	2	1	2	3	3	3	1	2		2	2	2	6321559	3	1	2	0,0927	214	1
250		3	3	2	1	2	5	2	1	3		2	2						0,0400		
		4	4	1	2	1	4	1	1	3		3	1						0,0808		
		5	2	1	2	2	5	3	2	2		2	3						0,0892		
		1	1	2	2	3	4	1	1	2		1	1						0,0059		
		2	2	1	1	2	4	3	1	2		2	3						0,0906		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
251	6344156	3	3	2	2	3	3	2	2	1		2	2	3	6344159	3	1	3	0,0050		3
		4	4	2	2	2	4	3	1	3		3	1						0,0935		
		5	2	1	1	3	3	1	1	2		1	3						0,0525		
		1	1	1	1	1	4	1	1	3		1	2						0,0463		
	6369027	2	2	2	1	1	5	2	1	1		1	2	2	6369031	4	1	2	0,0723		1
252		3	3	2	1	3	3	1	1	2		2	2						0,0236		
		4	4	2	1	4	5	3	2	3		3	2						0,0925		
		5	1	1	2	1	4	3	1	3		2	1						0,0439		
		1	1	1	2	2	4	2	2	2		1	1						0,0709		
		2	2	2	2	4	5	3	1	3		2	1						0,0231		
253		3	3	2	2	1	1	1	2	2		2	2						0,0324		
		4	4	1	1	3	4	2	2	2		1	1						0,0074		
	6395355	5	1	1	2	3	2	1	2	1		2	3	5	6395358	3	1	1	0,0962		4
		1	1	2	2	2	2	1	1	3		3	3						0,0856		
		2	2	2	1	2	1	1	1	2		1	2						0,0158		
254	6418307	3	3	1	1	3	4	1	2	2		1	3	3	6418312	5	1	3	0,0909		1
		4	4	2	2	3	4	2	2	2		1	1						0,0664		
		5	3	2	1	4	2	1	1	3		3	2						0,0287		
		1	1	1	1	4	3	1	1	1		1	2						0,0534		
		2	2	1	2	1	3	3	1	3		2	3						0,0836		
255		3	3	1	2	4	1	2	1	3		3	1						0,0456		
	6443483	4	4	2	1	3	2	1	1	3		2	3	4	6443486	3	1	4	0,0600		3
		5	3	1	1	4	5	3	1	2		2	1						0,0374		
		1	1	2	1	4	1	1	1	2		1	1						0,0646		
		2	2	1	2	4	3	2	2	1		2	3						0,0804		
256		3	3	2	2	4	3	3	1	1		3	2						0,0545		
	6468772	4	4	2	1	2	4	1	1	3		3	3	4	6468777	5	1	4	0,0875		1
		5	4	2	2	4	4	2	2	2		1	3						0,0680		
	6494032	1	1	2	2	4	1	3	2	1		1	2	1	6494035	3	1	1	0,0574		3
		2	2	2	2	2	2	3	2	2		2	3						0,0545		
257		3	3	2	1	3	3	1	2	2		2	2						0,0720		
		4	4	2	2	3	3	2	2	2		1	3						0,0891		
		5	2	1	2	1	3	3	2	1		2	2						0,0550		
		1	1	2	2	2	2	1	2	3		3	1						0,0026		
		2	2	2	1	2	3	3	1	1		1	1						0,0877		
258	6518914	3	3	2	2	4	5	2	1	3		2	3	3	6518917	3	1	3	0,0859		1
		4	4	1	1	1	5	2	2	3		3	3						0,0582		
		5	2	1	2	3	2	3	2	1		1	1						0,0362		
		1	1	2	1	3	5	2	1	2		3	3						0,0419		
		2	2	1	2	3	5	2	1	3		2	1						0,0052		
259		3	3	2	1	2	5	2	2	3		2	2						0,0441		
		4	4	1	2	3	1	3	2	3		2	3						0,0761		
	6548170	5	3	2	2	3	5	1	2	1		3	3	5	6548174	4	1	3	0,0907		3
		1	1	2	1	2	4	1	1	2		3	3						0,0293		
		2	2	2	2	4	1	1	1	1		1	3						0,0134		
260		3	3	2	2	4	3	3	1	2		1	1						0,0679		
	6577737	4	4	2	2	2	2	3	1	3		3	2	4	6577741	4	1	4	0,0859		1
		5	2	2	2	3	1	1	1	2		1	1						0,0575		
		1	1	1	2	4	1	2	2	3		3	2						0,0145		
	6607438	2	2	2	2	4	2	1	1	2		2	3	2	6607443	5	1	2	0,0059		4
261		3	3	2	1	2	3	1	1	2		1	3						0,0166		
		4	4	2	1	4	1	1	1	3		2	1						0,0937		
		5	2	2	1	2	1	1	2	1		3	3						0,0480		
		1	1	1	1	1	4	3	2	1		3	3						0,0973		
	6633351	2	2	1	2	2	4	2	2	2		1	2	2	6633354	3	1	2	0,0571		1
262		3	3	2	2	1	1	3	1	3		3	2						0,0359		
		4	4	2	1	1	4	1	2	3		1	3						0,0819		
		5	1	1	1	4	2	3	1	1		2	3						0,0170		
		1	1	2	2	4	4	3	1	2		2	3						0,0532		
		2	2	2	2	3	3	2	1	2		3	1						0,0219		
263		3	3	2	2	1	3	3	1	2		3	2						0,0905		
	6662368	4	4	2	2	3	1	3	1	1		1	1	4	6662373	5	1	4	0,0801		1
		5	4	2	2	1	5	2	1	3		1	2						0,0967		
		1	1	1	2	1	5	1	1	1		2	2						0,0802		
		2	2	2	1	2	2	2	1	1		2	2						0,0273		
264		3	3	1	1	3	3	3	2	3		2	3						0,0761		
	6689967	4	4	2	1	3	1	1	2	2		1	3	4	6689970	3	1	4	0,0330		1
		5	3	2	1	3	1	2	1	2		3	2						0,0023		
		1	1	1	1	2	4	3	2	3		1	3						0,1279		
		2	2	2	1	2	4	3	2	1		1	2						0,0997		
265		3	3	1	1	3	5	1	1	3		3	2						0,1556		
		4	4	1	2	2	5	2	1	3		3	3						0,0059		
	6718977	5	3	2	1	2	4	3	2	3		2	1	5	6718981	4	0	3	0,1507		1
		1	1	1	2	3	1	2	2	2		3	2						0,0551		
	6718981	2	2	2	1	4	2	3	1	1		3	2	2	6718996	15	1	2	0,1574		5
266		3	3	2	1	1	2	3	1	2		3	2						0,0291		
		4	4	2	1	3	4	3	1	2		1	2						0,1459		
		5	4	2	1	4	5	1	1	1		1	3						0,0587		
		1	1	1	1	2	1	3	1	1		1	3						0,0263		
		2	2	2	1	1	1	1	1	1		2	3						0,0795		
267		3	3	1	2	4	2	1	1	3		2	3						0,0269		
		4	4	1	1	2	3	3	2	1		2	3						0,0524		
	6741706	5	4	2	1	1	5	2	2	3		3	1	5	6741711	5	1	4	0,0629		1
		1	1	2	2	2	3	3	2	2		3	3						0,0256		
		2	2	2	2	1	5	1	2	2		1	1						0,0233		
268		3	3	1	2	1	3	1	2	2		1	2						0,0685		
		4	4	1	1	4	1	1	2	1		3	2						0,0151		
	6770908	5	4	1	1	4	4	2	2	2		3	2	5	6770912	4	1	4	0,0084		1
		1	1	2	2	4	4	3	2	1		1	1						0,0646		
		2	2	1	2	3	5	3	2	1		3	3						0,0149		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
269		3	3	2	2	3	2	1	2	1		2	3						0,0441		
		4	4	1	1	2	2	3	1	2		3	1						0,0556		
	6798448	5	1	1	2	1	3	1	1	2		1	1	5	6798452	4	1	1	0,0183		1
		1	1	1	1	4	4	3	1	3		1	1						0,0869		
		2	2	1	2	4	4	1	1	1		1	2						0,0963		
270	6824860	3	3	2	2	2	3	1	1	1		1	3	3	6824865	5	1	3	0,0186		4
		4	4	2	1	1	1	2	1	3		3	3						0,0903		
		5	3	2	2	1	3	2	1	3		1	1						0,0634		
	6852270	1	1	2	2	1	4	2	2	1		3	3	1	6852275	5	1	1	0,0110		1
		2	2	1	1	1	2	1	2	3		1	2						0,0386		
271		3	3	1	1	4	3	2	2	1		1	1						0,0382		
		4	4	2	1	4	2	1	1	3		1	3						0,0459		
		5	2	2	2	4	3	1	2	2		2	1						0,0352		
		1	1	1	2	4	3	1	1	3		3	1						0,0709		
		2	2	1	1	4	1	2	2	3		1	1						0,0647		
272		3	3	1	1	3	3	3	2	1		3	1						0,0874		
	6879728	4	4	2	1	4	2	1	2	3		3	1	4	6879731	3	1	4	0,0295		1
		5	3	1	2	3	2	1	1	1		1	2						0,0935		
		1	1	2	1	2	2	3	1	2		2	2						0,0911		
		2	2	1	1	2	3	2	1	2		1	3						0,0576		
273		3	3	1	1	3	3	1	1	3		1	3						0,0448		
	6906666	4	4	2	1	1	4	1	2	1		1	2	4	6906669	3	1	4	0,0436		1
		5	2	1	1	2	5	3	2	3		3	1						0,0973		
		1	1	2	1	3	3	1	2	1		2	1						0,0307		
		2	2	1	2	4	1	3	1	2		3	2						0,0154		
274	6933273	3	3	2	2	3	4	3	2	2		1	3	3	6933278	5	1	3	0,0212		1
		4	4	2	2	3	2	3	1	1		3	3						0,0295		
		5	4	2	1	3	2	2	2	1		3	3						0,0205		
		1	1	1	1	1	5	1	2	1		3	1						0,0675		
		2	2	2	1	2	4	3	2	2		3	1						0,0438		
275		3	3	2	1	3	3	3	1	2		2	1						0,0310		
		4	4	1	1	3	1	1	2	1		2	3						0,0976		
	6961922	5	2	2	1	1	2	1	2	1		1	3	5	6961925	3	1	2	0,0726		1
		1	1	2	1	2	5	2	2	1		3	3						0,0765		
	6987122	2	2	1	2	3	2	1	1	3		2	3	2	6987127	5	1	2	0,0030		1
276		3	3	1	2	3	3	3	2	1		2	1						0,0278		
		4	4	1	1	3	4	2	1	3		3	1						0,0007		
		5	2	1	2	1	1	1	1	1		3	1						0,0936		
		1	1	1	2	2	4	3	2	3		3	1						0,0028		
		2	2	2	1	4	2	1	2	3		3	2						0,0278		
277		3	3	1	1	3	2	3	2	2		2	3						0,0659		
	7010868	4	4	1	1	3	1	3	1	3		3	3	4	7010873	5	1	4	0,0509		1
		5	3	1	2	3	3	3	2	2		1	3						0,0229		
		1	1	1	1	4	2	1	1	1		1	1						0,0859		
		2	2	1	2	1	4	1	2	3		1	3						0,0556		
278		3	3	1	1	1	1	1	2	1		1	1						0,0985		
	7040699	4	4	1	2	2	3	2	2	2		3	3	4	7040704	5	1	4	0,0210		4
		5	3	1	2	2	1	3	2	1		1	3						0,0301		
		1	1	1	2	3	2	2	2	1		3	1						0,0921		
		2	2	1	1	1	3	1	1	3		2	2						0,0713		
279	7068230	3	3	2	1	2	4	3	2	1		2	1	3	7068233	3	1	3	0,0406		3
		4	4	1	2	3	2	3	2	1		2	3						0,0607		
		5	3	1	1	1	4	3	2	3		2	3						0,0471		
		1	1	1	1	3	3	2	1	1		2	2						0,0771		
		2	2	1	1	3	4	1	1	2		1	2						0,0553		
280	7091620	3	3	1	2	2	1	2	1	2		3	1	3	7091623	3	1	3	0,0654		1
		4	4	2	2	2	3	2	1	2		2	3						0,0951		
		5	3	1	1	3	2	1	1	2		1	2						0,0471		
		1	1	1	1	2	5	1	2	3		3	2						0,0442		
		2	2	2	2	4	2	2	1	3		2	2						0,0873		
281		3	3	1	2	4	5	1	1	2		1	1						0,0098		
		4	4	1	2	2	3	3	1	1		1	1						0,0016		
	7116564	5	4	1	2	4	4	1	2	1		1	3	5	7116569	5	1	4	0,0332		1
		1	1	2	2	2	5	2	2	1		1	1						0,0790		
		2	2	1	1	2	3	2	1	1		3	3						0,0293		
282		3	3	1	1	4	3	1	1	3		1	1						0,0812		
		4	4	1	1	4	1	1	1	3		1	3						0,0355		
	7140421	5	4	1	2	1	5	2	1	1		3	2	5	7140424	3	1	4	0,0152		1
		1	1	2	1	4	5	3	2	1		2	2						0,0720		
		2	2	1	1	3	1	3	2	1		1	1						0,0496		
283	7169506	3	3	1	2	1	2	1	2	3		3	3	3	7169509	3	1	3	0,0004		1
		4	4	1	1	3	5	3	2	1		3	2						0,0687		
		5	1	1	2	4	3	3	2	1		2	3						0,0636		
	7193200	1	1	2	2	1	5	2	1	3		3	3	1	7193205	5	0	1	0,0448		1
		2	2	1	2	3	5	3	1	1		1	2						0,1121		
284		3	3	1	2	1	2	3	2	1		3	3						0,1464		
		4	4	1	2	2	3	3	2	2		1	3						0,0197		
		5	3	2	2	4	4	1	2	1		2	3						0,0353		
		1	1	1	2	4	2	3	1	2		2	2						0,1356		
		2	2	2	1	1	1	2	1	2		1	3						0,2356		
285		3	3	2	2	1	3	2	2	1		3	2						0,1627		
	7193205	4	4	2	1	4	1	3	1	2		3	3	4	7193228	23	1	4	0,0978		5
		5	1	1	1	3	1	2	2	3		1	1						0,0221		
		1	1	2	1	1	5	3	2	1		1	1						0,0010		
	7217189	2	2	2	1	3	5	1	1	2		2	2	2	7217192	3	1	2	0,0121		1
286		3	3	2	1	1	5	1	2	2		3	2						0,0250		
		4	4	2	2	2	4	1	2	2		2	3						0,0292		
		5	4	2	2	2	2	3	2	1		3	3						0,0487		
		1	1	1	2	2	1	1	1	1		1	2						0,0880		
		2	2	1	2	4	5	1	2	3		1	2						0,0894		

Продовження таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
287		3	3	1	2	4	5	2	1	3		1	2						0,0233		
		4	4	2	1	2	3	3	1	2		1	3						0,0401		
	7243774	5	2	1	2	1	3	3	2	3		2	1	5	7243779	5	1	2	0,0602		1
		1	1	1	1	4	4	1	2	2		2	1						0,0619		
		2	2	1	1	1	4	2	2	3		3	3						0,0030		
288		3	3	1	1	2	3	1	2	3		2	1						0,2041		
	7272530	4	4	2	2	1	5	2	2	2		2	2	4	7272534	4	0	4	0,0108		1
		5	3	1	2	3	2	3	1	2		3	2						0,1495		
		1	1	1	2	4	2	3	1	1		2	2						0,0367		
		2	2	2	1	1	4	3	1	3		2	2						0,1728		
289	7272534	3	3	1	1	4	5	3	1	1		1	3	3	7272559	25	1	3	0,1300		5
		4	4	2	2	3	3	1	2	1		3	1						0,2345		
		5	1	2	1	3	4	2	2	2		1	3						0,1396		
		1	1	1	2	4	5	2	1	2		1	1						0,0512		
		2	2	1	1	2	2	1	2	1		1	2						0,0080		
290	7295677	3	3	1	1	1	3	1	2	1		1	3	3	7295682	5	1	3	0,0037		1
		4	4	1	1	3	5	2	1	1		1	2						0,0340		
		5	3	2	2	1	5	2	1	1		1	3						0,0580		
		1	1	1	1	4	5	1	2	1		2	3						0,0709		
		2	2	1	2	4	2	3	1	1		1	3						0,0661		
291		3	3	1	2	4	5	1	1	1		3	2						0,0833		
	7321464	4	4	2	2	3	3	2	2	1		2	2	4	7321469	5	1	4	0,0940		1
		5	1	2	1	4	5	3	1	1		1	1						0,0383		
		1	1	1	2	2	5	3	1	1		3	1						0,0582		
		2	2	2	2	1	5	2	2	2		1	1						0,0039		
292		3	3	1	1	2	3	3	2	3		3	1						0,0992		
		4	4	1	2	1	3	3	2	1		3	3						0,0682		
	7348730	5	3	1	2	2	2	3	2	1		3	2	5	7348734	4	1	3	0,0121		1
		1	1	2	1	3	4	2	1	1		1	2						0,0435		
		2	2	1	1	3	5	3	2	2		1	3						0,0265		
293		3	3	2	1	2	4	1	2	2		2	3						0,0448		
		4	4	2	2	1	2	3	1	3		3	3						0,0891		
	7378656	5	1	1	2	1	3	1	1	1		3	3	5	7378659	3	1	1	0,0256		1
	7403898	1	1	1	2	3	1	2	1	2		1	3	1	7403901	3	1	1	0,0465		1
		2	2	2	2	4	4	3	1	2		2	1						0,0407		
294		3	3	1	2	2	4	3	1	1		2	2						0,0755		
		4	4	2	1	4	4	1	2	3		1	2						0,0716		
		5	2	1	2	1	2	1	1	3		2	1						0,0568		
		1	1	2	1	2	4	1	1	2		1	1						0,0163		
		2	2	2	1	3	3	1	1	2		2	3						0,0849		
295	7431828	3	3	1	2	3	5	1	2	2		1	2	3	7431833	5	1	3	0,0696		1
		4	4	2	1	4	5	1	1	1		1	1						0,0502		
		5	4	1	1	4	2	3	2	3		3	2						0,0909		
		1	1	2	1	3	3	3	1	1		3	2						0,0519		
	7457955	2	2	2	2	1	3	1	1	1		2	2	2	7457958	3	1	2	0,0231		1
296		3	3	1	2	1	5	3	1	2		1	1						0,0959		
		4	4	2	2	4	2	2	1	2		2	1						0,0037		
		5	4	1	2	3	4	1	1	1		3	3						0,0392		
		1	1	2	2	1	3	3	1	1		1	2						0,0425		
		2	2	2	1	4	3	3	2	2		1	2						0,0304		
297		3	3	1	1	2	4	3	1	3		3	3						0,0213		
		4	4	2	2	3	1	1	2	1		3	2						0,0111		
	7484081	5	1	1	1	2	5	1	1	1		1	2	5	7484086	5	1	1	0,0602		1
		1	1	1	1	3	2	3	1	2		1	2						0,0598		
		2	2	2	2	4	2	1	2	2		2	2						0,0226		
298		3	3	2	1	1	3	1	2	3		3	1						0,0710		
		4	4	1	1	3	2	3	2	2		1	1						0,0263		
	7510336	5	4	1	1	1	2	2	1	3		3	3	5	7510341	5	1	4	0,0027		3
		1	1	1	2	1	4	2	2	1		2	1						0,0207		
		2	2	2	2	4	1	2	1	1		2	2						0,0494		
299		3	3	1	2	3	4	2	2	3		1	1						0,0895		
		4	4	2	2	2	1	1	1	3		3	3						0,0958		
	7533845	5	1	2	1	3	1	3	1	1		2	1	5	7533848	3	1	1	0,0375		2
	7559266	1	1	2	1	2	4	3	2	2		2	3	1	7559271	5	1	1	0,0773		1
		2	2	1	1	2	3	2	1	2		1	3						0,0584		
300		3	3	1	1	2	3	3	1	3		3	1						0,0563		
		4	4	1	2	2	5	2	1	3		3	1						0,0644		
		5	4	1	1	4	1	1	2	1		1	1						0,0586		
		1	1	2	2	4	4	1	2	2		3	2						0,0185		
		2	2	1	2	2	4	1	2	2		1	3						0,0768		
301	7585211	3	3	1	1	1	4	3	1	2		1	3	3	7585216	5	1	3	0,0496	190	2
		4	4	1	1	1	3	1	2	3		2	2						0,0274		
		5	2	1	2	4	2	1	2	3		2	3						0,0361		
		1	1	1	1	3	2	2	2	3		3	2						0,0285		
		2	2	2	2	1	2	2	2	2		3	2						0,0488		
302	7614904	3	3	1	2	1	2	2	2	3		1	2	3	7614907	3	1	3	0,0035		1
		4	4	2	1	4	1	3	1	1		3	3						0,0732		
		5	3	1	1	3	2	2	2	2		1	3						0,0483		
		1	1	1	1	3	5	3	1	3		2	3						0,0583		
		2	2	2	1	4	2	2	1	1		2	1						0,0099		
303		3	3	2	2	1	2	3	2	2		1	1						0,0889		
	7642376	4	4	1	1	2	1	1	1	3		3	3	4	7642379	3	1	4	0,0978		1
		5	2	1	2	1	3	1	2	3		1	3						0,0332		
	7671190	1	1	1	2	4	3	3	2	1		1	1	1	7671195	5	1	1	0,0403		1
		2	2	1	2	3	1	2	2	2		1	1						0,0755		
304		3	3	2	2	3	4	2	1	3		1	2						0,0199		
		4	4	2	2	3	2	2	1	2		1	2						0,0889		
		5	4	1	1	4	3	2	2	1		3	1						0,0861		
		1	1	1	2	2	3	3	2	2		1	2						0,0052		
	7698982	2	2	1	1	3	4	2	1	1		3	3	2	7698986	4	1	2	0,0832		3

Кінець таблиці Ж.1

1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19	20	21
305		3	3	1	1	3	3	1	1	3		3	3						0,0146		
		4	4	2	2	4	4	2	1	3		2	1						0,0637		
		5	1	2	2	4	1	1	1	2		2	1						0,0260		
		1	1	1	2	1	2	2	2	3		2	1						0,0884		
		2	2	1	1	2	5	1	2	3		1	3						0,0672		
306		3	3	1	1	4	2	2	1	1		2	3						0,0845		
	7726687	4	4	1	2	3	2	2	2	1		3	1	4	7726691	4	1	4	0,0408		1
		5	2	1	2	2	3	1	1	3		3	3						0,0196		
		1	1	1	2	1	1	3	2	1		3	2						0,0654		
		2	2	1	1	1	3	3	2	2		2	1						0,0580		
307	7750045	3	3	2	1	2	5	1	1	1		1	2	3	7750049	4	1	3	0,0376		1
		4	4	2	1	1	4	1	2	1		3	1						0,0556		
		5	4	2	1	2	1	1	2	2		1	1						0,0534		

Таблиця Ж.2

Результати другої серії другого експерименту

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
		1	1	1	1	1	5	3	2	2	2	1						0,5084		
	27619	2	2	1	2	3	3	2	1	2	3	3	2	27623	4	1	2	0,4194		1
1		3	3	2	1	3	5	3	1	1	2	3						0,4601		
		4	4	1	1	2	4	3	2	2	1	1						0,5579		
		5	4	2	2	2	5	1	2	3	2	2						0,5888		
		1	1	2	1	1	3	3	2	2	1	1						0,5845		
		2	2	2	2	4	2	3	2	3	2	1						0,3045		
2		3	3	2	2	4	2	2	1	2	1	1						0,4785		
		4	4	2	1	1	5	2	1	3	1	2						0,348		
	56213	5	3	2	2	3	5	3	1	1	2	1	5	56218	5	1	3	2,78E-04		1
		1	1	1	2	2	4	3	1	2	2	2						0,5299		
		2	2	2	1	2	2	2	1	3	3	2						0,19		
3	81992	3	3	1	2	2	1	3	1	2	3	1	3	81995	3	1	3	0,0426		1
		4	4	1	2	4	2	3	2	3	3	1						0,6311		
		5	3	2	1	2	1	3	2	1	2	3						0,4833		
		1	1	2	2	3	5	3	1	2	3	3						0,2666		
		2	2	2	2	2	1	1	1	2	3	1						0,08		
4	106505	3	3	2	1	3	2	3	1	1	3	3	3	106510	5	1	3	0,0644		1
		4	4	1	1	3	1	2	1	3	1	2						0,4541		
		5	2	2	1	3	2	2	1	3	1	3						0,7091		
		1	1	2	1	1	5	3	2	2	1	3						0,4118		
		2	2	1	2	1	5	1	2	1	1	3						0,61		
5	136331	3	3	2	1	2	2	3	2	2	2	3	3	136334	3	0	3	0,198		1
		4	4	1	1	1	3	1	1	1	2	2						0,4333		
		5	1	1	2	3	2	1	1	3	2	2						0,3701		
		1	1	2	1	2	3	3	1	1	2	1						0,2801		
		2	2	1	2	3	3	1	1	1	3	3						0,6567		
6	136334	3	3	1	2	4	4	2	1	2	2	3	3	136352	18	0	3	0,207		5
		4	4	1	1	1	1	2	2	2	3	1						0,3117		
		5	1	1	2	4	2	3	1	2	2	3						0,3264		
		1	1	1	2	3	3	2	2	2	2	2						0,2605		
		2	2	1	2	2	2	2	2	3	1	1						0,0751		
7	136352	3	3	1	2	1	1	3	1	3	2	1	3	136370	18	1	3	0,073		5
		4	4	1	2	4	5	1	1	3	3	1						0,1945		
		5	3	2	2	3	2	1	1	3	3	2						0,2046		
	165007	1	1	2	2	2	3	1	1	2	2	2	1	165012	5	1	1	0,0071		1
		2	2	2	1	4	2	1	1	1	1	2						0,1336		
8		3	3	2	2	2	1	2	2	3	3	3						0,1164		
		4	4	2	2	1	3	1	1	2	1	2						0,4998		
		5	3	2	2	2	1	2	2	1	1	1						0,4762		
		1	1	2	1	4	2	1	1	1	3	2						0,5754		
	194648	2	2	2	1	3	3	3	1	1	1	3	2	194652	4	1	2	0,4424		1
9		3	3	1	2	2	1	3	1	3	1	2						0,467		
		4	4	1	2	2	5	1	2	3	2	1						0,4722		
		5	2	1	2	4	2	2	1	3	3	1						0,5904		
		1	1	2	2	4	1	3	2	1	2	1						0,3154		
	218153	2	2	1	2	3	3	2	2	3	2	1	2	218158	5	1	2	0,2764		3
10		3	3	2	1	2	3	3	2	1	2	2						0,682		
		4	4	2	1	4	2	1	1	3	2	2						0,3515		
		5	3	1	1	3	4	3	2	3	3	1						0,4707		
		1	1	2	2	4	5	1	2	1	3	3						0,2753		
		2	2	1	2	3	2	3	1	1	1	2						0,7061		
11		3	3	2	1	2	1	3	1	2	2	2						0,2998		
		4	4	1	1	3	5	3	2	1	2	1						0,5025		
	246766	5	4	1	2	1	2	1	1	1	3	2	5	246770	4	1	4	0,1507		1
		1	1	1	1	4	4	2	2	1	1	2						0,513		
		2	2	1	2	4	2	3	2	2	3	2						0,4997		
12		3	3	2	1	3	5	3	1	1	2	2						0,3445		
	276468	4	4	1	2	1	1	3	2	2	2	1	4	276473	5	1	4	0,0228		1
		5	3	1	1	1	3	1	2	2	2	3						0,3811		
		1	1	2	2	1	4	1	2	3	1	1						0,5118		
		2	2	2	2	1	5	2	1	2	3	2						0,3692		
13		3	3	2	2	3	3	3	1	2	1	1						0,3911		
	300332	4	4	2	1	4	2	3	2	2	2	2	4	300335	3	1	4	0,1034		2
		5	1	2	1	3	4	3	1	3	2	2						0,3827		
	322997	1	1	2	1	4	3	2	2	1	1	2	1	323001	4	0	1	0,1238		4
		2	2	1	1	2	4	2	2	1	3	3						0,6854		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
14		3	3	1	1	3	5	1	1	3	2	2						0,1396		
		4	4	2	1	4	3	2	1	3	1	1						0,2642		
		5	3	2	2	4	5	3	2	1	3	1						0,1689		
	323001	1	1	2	2	3	2	3	2	1	1	3	1	323022	21	1	1	0,0848		5
		2	2	2	1	4	4	3	1	3	3	3						0,3632		
15		3	3	2	2	4	4	1	2	2	3	3						0,3939		
		4	4	1	2	4	3	3	2	2	2	1						0,5494		
		5	3	2	1	3	1	1	2	3	2	1						0,2427		
		1	1	2	2	4	1	2	2	3	3	3						0,5447		
		2	2	1	1	4	5	1	1	1	2	2						0,4543		
16	349366	3	3	2	1	2	4	2	2	2	1	1	3	349371	5	1	3	0,0438		1
		4	4	2	2	1	1	2	1	1	2	2						0,3621		
		5	3	2	2	1	2	1	1	1	1	2						0,6881		
		1	1	1	2	1	2	1	1	1	1	1						0,0094		
	376222	2	2	1	1	4	2	3	1	2	2	2	2	376226	4	1	2	2,16E-04		1
17		3	3	1	1	1	1	3	1	3	1	1						0,5971		
		4	4	1	1	3	2	1	1	2	1	2						0,4512		
		5	3	1	2	4	2	2	1	3	3	1						0,6391		
		1	1	2	1	1	4	1	1	2	2	1						0,705		
		2	2	1	1	4	5	3	2	1	1	3						0,3245		
18	400037	3	3	2	1	2	2	3	2	1	3	3	3	400041	4	0	3	0,0156		1
		4	4	1	2	3	1	3	2	1	2	1						0,5933		
		5	1	2	2	2	3	1	2	1	3	1						0,4839		
	400041	1	1	1	2	4	5	1	1	1	1	3	1	400065	24	1	1	0,0067		5
		2	2	2	1	1	2	3	2	1	1	1						0,367		
19		3	3	2	2	2	3	1	2	1	3	2						0,3268		
		4	4	1	1	1	3	1	1	1	3	3						0,7048		
		5	2	2	2	3	2	3	2	2	2	2						0,098		
	424747	1	1	2	1	2	3	3	1	2	2	2	1	424750	3	1	1	0,0607		1
		2	2	2	1	4	1	1	1	2	1	1						0,4125		
20		3	3	1	2	1	4	1	1	3	2	1						0,4399		
		4	4	2	2	2	4	2	1	2	1	1						0,3471		
		5	4	2	1	4	4	3	2	3	3	2						0,5588		
		1	1	2	1	2	3	2	1	3	3	3						0,6828		
	450496	2	2	2	1	4	1	1	2	1	2	3	2	450500	4	1	2	0,0212		1
21		3	3	2	2	1	2	3	2	1	1	2						0,6374		
		4	4	2	2	4	2	3	2	2	2	3						0,181		
		5	1	2	1	2	2	1	2	3	2	1						0,1236		
	476561	1	1	1	2	1	4	1	1	3	2	1	1	476564	3	1	1	0,1346		1
		2	2	1	2	1	4	1	2	1	2	3						0,1879		
22		3	3	1	1	1	4	1	2	2	3	3						0,5035		
		4	4	1	2	4	3	1	1	1	1	2						0,2381		
		5	1	1	2	4	4	2	2	1	1	3						0,3637		
	505738	1	1	1	1	1	1	3	1	1	2	2	1	505743	5	1	1	0,0158		1
		2	2	1	2	2	2	2	2	2	2	3						0,1144		
23		3	3	1	1	4	1	3	1	2	3	1						0,0817		
		4	4	1	1	2	3	2	1	2	2	2						0,1778		
		5	4	1	2	2	4	2	1	2	2	3						0,521		
		1	1	2	2	3	3	3	1	2	2	3						0,2696		
		2	2	2	2	4	2	3	2	3	1	2						0,6704		
24		3	3	2	1	3	3	3	2	2	3	2						0,2248		
	534534	4	4	1	2	4	2	3	1	2	3	2	4	534537	3	1	4	0,1896		1
		5	2	1	1	1	4	3	1	2	2	2						0,4459		
		1	1	2	2	4	3	3	1	3	3	3						0,627		
		2	2	1	2	4	2	2	2	3	3	3						0,5507		
25		3	3	1	1	1	1	2	2	2	1	3						0,6687		
		4	4	1	2	1	1	2	2	3	1	3						0,5391		
	562382	5	2	1	1	3	3	3	1	2	1	2	5	562385	3	1	2	0,3154		1
		1	1	2	1	1	4	3	1	3	2	3						0,6529		
		2	2	1	2	3	3	2	2	1	1	3						0,1292		
26	591400	3	3	2	1	2	4	3	1	1	1	1	3	591405	5	0	3	0,001		2
		4	4	2	1	1	1	2	1	1	3	1						0,5271		
		5	3	1	2	3	5	1	2	2	2	3						0,6947		
		1	1	2	1	1	5	1	1	2	3	2						0,146		
		2	2	1	1	1	3	1	2	1	2	2						0,4128		
27		3	3	1	2	2	1	1	2	3	3	2						0,3481		
		4	4	1	2	3	4	3	1	3	3	3						0,4425		
	591405	5	2	1	1	3	1	2	1	3	1	3	5	591422	17	1	2	0,1078		5
		1	1	1	2	4	1	1	2	2	1	3						0,3789		
	618644	2	2	2	2	1	1	2	2	1	1	2	2	618649	5	1	2	0,1867		4
28		3	3	1	2	1	3	3	1	1	3	2						0,5016		
		4	4	1	2	3	3	2	1	1	1	1						0,6626		
		5	1	2	2	4	3	1	1	1	3	1						0,6345		
		1	1	1	1	4	2	3	2	2	2	1						0,5674		
	646245	2	2	2	2	3	1	1	1	1	3	1	2	646248	3	0	2	0,0524		1
29		3	3	1	2	3	3	1	1	3	2	3						0,0757		
		4	4	1	2	1	4	3	2	2	1	3						0,4341		
		5	2	1	2	3	4	1	1	1	3	1						0,3581		
		1	1	2	2	1	3	2	1	1	3	3						0,397		
		2	2	2	2	4	2	2	2	3	2	3						0,6501		
30		3	3	2	1	1	4	3	1	3	1	2						0,4408		
		4	4	1	2	3	4	2	2	3	3	1						0,4687		
	646248	5	1	1	1	2	4	2	2	1	2	1	5	646268	20	1	1	0,0868		5
		1	1	2	2	1	3	2	2	3	3	3						0,3754		
	671506	2	2	2	2	2	3	1	2	2	1	2	2	671509	3	1	2	0,0098		1
31		3	3	2	1	1	5	2	1	1	1	2						0,0613		
		4	4	2	2	3	5	1	1	1	1	2						0,1312		
		5	1	1	2	3	3	3	2	2	2	1						0,1613		
		1	1	1	1	2	1	1	2	2	1	2						0,2137		
		2	2	2	1	4	4	1	1	2	1	1						0,2663		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
32	696948	3	3	1	2	2	2	2	2	2	1	2	3	696951	3	1	3	0,0359		1
		4	4	2	2	1	2	3	1	2	2	2						0,4894		
		5	1	1	2	1	2	2	1	3	2	1						0,3008		
		1	1	1	1	3	1	2	1	2	3	2						0,4409		
		2	2	1	2	4	4	1	1	3	2	2						0,5309		
33	721752	3	3	2	1	1	3	3	1	1	2	1	3	721757	5	1	3	0,0322		1
		4	4	2	2	2	3	2	1	3	2	3						0,0469		
		5	2	2	1	2	3	2	1	3	2	2						0,3996		
		1	1	1	2	1	4	3	1	3	2	2						0,307		
		2	2	1	2	2	5	2	2	3	3	2						0,5887		
34		3	3	1	2	2	2	1	2	2	1	2						0,3366		
		4	4	2	1	4	2	2	1	3	1	1						0,4268		
	747474	5	3	2	1	4	4	2	2	1	3	2	5	747479	5	0	3	0,2516		2
		1	1	2	2	1	4	1	1	1	3	3						0,7182		
		2	2	1	2	2	5	2	2	1	1	1						0,1542		
35		3	3	2	1	3	5	1	1	3	2	1						0,0496		
	747479	4	4	2	1	1	4	2	2	3	2	1	4	747501	22	1	4	0,0253		5
		5	2	1	1	1	5	1	1	3	2	1						0,367		
		1	1	2	2	1	1	1	2	1	1	2						0,6772		
		2	2	2	1	3	5	1	2	1	1	3						0,4548		
36	776499	3	3	1	2	4	2	1	2	2	2	3	3	776503	4	1	3	0,0313		4
		4	4	1	2	1	5	2	1	3	3	3						0,3856		
		5	4	2	1	1	4	3	1	3	1	1						0,4267		
		1	1	1	2	4	5	2	2	2	1	3						0,5837		
	800036	2	2	1	2	3	4	3	1	1	2	3	2	800040	4	1	2	0,0329		1
37		3	3	2	1	2	2	3	2	2	2	1						0,1716		
		4	4	2	1	2	1	1	2	3	2	1						0,5443		
		5	2	2	2	3	5	2	2	2	2	3						0,3453		
	827286	1	1	1	1	1	2	2	2	1	3	3	1	827291	5	1	1	0,1839		1
		2	2	1	2	3	2	1	1	2	3	1						0,7072		
38		3	3	1	2	1	2	3	2	3	1	1						0,2039		
		4	4	1	1	4	2	1	2	3	1	2						0,3718		
		5	4	1	2	2	3	1	1	1	3	2						0,1973		
	853935	1	1	1	1	2	1	1	1	2	3	2	1	853940	5	1	1	0,0567		4
		2	2	1	1	3	1	3	2	2	3	3						0,4466		
39		3	3	1	1	3	4	3	1	1	3	1						0,4327		
		4	4	1	1	4	1	1	1	2	3	3						0,562		
		5	2	1	2	2	5	3	1	3	1	2						0,1191		
		1	1	2	1	3	4	1	2	1	1	2						0,4564		
		2	2	1	2	2	5	1	1	1	3	1						0,3536		
40		3	3	1	2	4	5	2	1	3	2	2						0,5654		
	882412	4	4	1	1	1	3	3	1	1	1	1	4	882415	3	1	4	0,1841		1
		5	1	1	1	1	2	3	2	1	3	3						0,5703		
		1	1	2	1	4	5	1	2	1	2	1						0,0572		
		2	2	2	1	4	2	2	2	3	1	3						0,4742		
41		3	3	2	2	3	5	3	1	3	3	2						0,2747		
	908968	4	4	1	1	3	4	3	1	1	1	2	4	908971	3	1	4	0,02		1
		5	3	1	2	3	3	2	1	3	2	2						0,0826		
		1	1	2	1	2	4	1	2	3	1	3						0,3185		
	932791	2	2	2	1	4	3	1	1	2	2	1	2	932794	3	1	2	0,1768		1
42		3	3	1	1	2	3	1	1	1	3	3						0,6207		
		4	4	1	1	4	2	1	1	3	2	2						0,2839		
		5	3	1	2	3	4	3	2	3	2	2						0,674		
		1	1	1	2	3	5	3	2	3	1	2						0,525		
		2	2	1	1	2	3	2	2	3	2	3						0,4323		
43	955983	3	3	2	1	2	3	1	1	2	1	3	3	955987	4	1	3	0,008		1
		4	4	2	1	1	5	3	2	3	3	2						0,6975		
		5	2	2	2	4	2	2	2	3	1	2						0,0817		
		1	1	2	1	2	4	1	2	1	2	3						0,1033		
	982233	2	2	1	1	3	4	2	1	1	3	1	2	982236	3	1	2	0,0328		1
44		3	3	2	2	1	2	2	1	1	3	1						0,6708		
		4	4	2	1	1	1	2	1	3	2	1						0,2415		
		5	1	1	2	3	2	1	2	1	2	2						0,5916		
	1005208	1	1	2	2	3	3	2	1	2	1	2	1	1005212	4	1	1	0,2612		1
		2	2	1	1	2	1	2	2	2	2	3						0,31		
45		3	3	2	1	3	3	1	2	3	3	3						0,3513		
		4	4	1	1	4	4	1	1	2	3	3						0,5704		
		5	4	2	2	4	2	1	1	2	1	2						0,6991		
		1	1	1	2	4	3	3	1	1	2	2						0,6312		
		2	2	2	1	3	1	1	1	3	3	3						0,3904		
46	1032833	3	3	1	2	1	5	1	2	2	3	2	3	1032837	4	1	3	0,3896		1
		4	4	1	1	1	5	3	2	3	1	3						0,6809		
		5	4	1	2	3	3	1	2	1	2	3						0,7118		
		1	1	2	2	3	2	1	2	3	3	2						0,2198		
	1062565	2	2	1	1	4	3	2	2	2	1	3	2	1062570	5	1	2	0,0368		1
47		3	3	2	1	3	5	3	1	3	2	2						0,6185		
		4	4	2	2	1	1	3	2	3	1	1						0,6346		
		5	2	2	1	2	3	3	1	2	3	2						0,0491		
	1086518	1	1	2	2	3	3	1	2	2	1	1	1	1086522	4	1	1	0,0352		1
		2	2	2	1	3	5	2	1	3	2	1						0,1564		
48		3	3	2	2	1	5	2	2	3	2	3						0,6685		
		4	4	2	2	4	4	2	1	2	2	2						0,3571		
		5	2	2	2	4	2	3	2	1	2	3						0,2532		
		1	1	2	1	2	1	1	2	2	1	2						0,6728		
		2	2	1	2	2	5	2	1	2	2	3						0,7068		
49		3	3	2	1	1	2	1	2	3	1	1						0,4956		
	1110735	4	4	2	2	4	2	3	2	1	3	1	4	1110739	4	1	4	0,0506		1
		5	3	2	2	3	2	1	2	1	1	1						0,5092		
		1	1	1	2	2	4	1	2	3	1	2						0,2225		
	1140356	2	2	1	1	4	2	2	2	1	3	2	2	1140361	5	0	2	0,2021		1

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
50		3	3	1	1	4	1	2	2	2	3	3						0,6963		
		4	4	2	1	2	5	1	1	2	1	2						0,4719		
		5	4	1	2	2	2	1	1	1	1	2						0,3551		
		1	1	2	2	1	4	3	2	2	3	1						0,3521		
		2	2	2	2	3	1	2	1	2	2	3						0,1314		
51	1140361	3	3	2	2	2	4	3	1	3	3	2	3	1140381	20	0	3	0,0607		5
		4	4	1	2	1	1	2	2	3	1	1						0,0848		
		5	3	1	2	1	1	1	2	2	1	3						0,6684		
	1140381	1	1	2	2	2	4	1	1	2	1	2	1	1140405	24	1	1	0,0213		5
		2	2	1	2	1	5	2	2	3	1	2						0,3601		
52		3	3	2	2	1	2	2	2	2	2	1						0,0461		
		4	4	1	2	1	2	2	1	3	3	1						0,1444		
		5	2	1	1	2	3	1	2	2	3	2						0,3299		
		1	1	1	1	1	2	1	1	3	1	1						0,414		
		2	2	2	2	3	4	3	2	1	3	3						0,5406		
53		3	3	2	2	4	2	2	1	1	2	1						0,6681		
	1167490	4	4	1	2	3	2	3	1	3	1	3	4	1167494	4	1	4	0,0587		1
		5	2	2	2	1	4	3	2	1	3	3						0,4266		
		1	1	2	2	1	4	1	1	1	3	2						0,293		
	1190155	2	2	1	1	3	2	1	1	1	2	1	2	1190160	5	1	2	0,2407		3
54		3	3	2	1	2	5	1	2	2	3	3						0,4409		
		4	4	2	1	2	3	3	2	2	3	1						0,7144		
		5	4	1	1	1	5	2	2	3	3	3						0,3092		
	1219480	1	1	2	1	3	4	2	1	1	1	3	1	1219483	3	1	1	0,2984		1
		2	2	1	2	3	3	3	1	1	3	2						0,5669		
55		3	3	2	2	3	2	2	2	2	1	1						0,6972		
		4	4	2	1	2	3	1	2	1	2	3						0,6091		
		5	3	1	1	2	3	2	2	1	1	1						0,4157		
		1	1	1	2	3	5	2	1	2	1	3						0,6243		
		2	2	2	2	2	5	3	1	3	2	3						0,1441		
56		3	3	1	1	1	2	2	2	2	1	1						0,7161		
	1246418	4	4	1	1	1	1	3	2	3	3	1	4	1246421	3	1	4	0,1005		3
		5	3	1	1	2	3	3	1	3	1	1						0,2853		
		1	1	1	2	4	4	1	1	3	2	1						0,446		
	1272676	2	2	2	2	2	4	3	2	2	1	3	2	1272680	4	1	2	0,4178		1
57		3	3	2	1	3	5	3	1	1	3	3						0,5688		
		4	4	2	2	1	1	2	2	2	2	1						0,5376		
		5	1	1	1	1	1	2	1	3	1	1						0,458		
		1	1	1	1	3	1	2	1	2	1	2						0,6503		
		2	2	1	1	2	2	1	2	1	1	2						0,4656		
58		3	3	1	1	3	5	2	1	2	3	1						0,289		
	1300408	4	4	1	2	3	4	1	2	1	3	2	4	1300411	3	1	4	0,0847		1
		5	4	2	1	3	3	2	1	1	2	2						0,5716		
		1	1	2	2	2	5	3	1	1	1	2						0,3511		
	1327737	2	2	1	1	3	5	1	2	2	1	2	2	1327740	3	1	2	0,0146		1
59		3	3	2	2	1	2	1	2	2	2	3						0,174		
		4	4	2	1	1	3	3	2	2	3	1						0,3715		
		5	1	1	1	3	4	3	1	2	1	3						0,3375		
		1	1	1	1	2	3	2	2	1	2	1						0,5386		
	1356515	2	2	2	1	1	2	1	1	1	1	1	2	1356520	5	1	2	0,0211		1
60		3	3	2	1	1	1	3	1	3	2	2						0,3523		
		4	4	2	1	2	2	3	2	3	3	2						0,6245		
		5	1	2	1	2	1	3	2	1	1	1						0,2598		
	1384091	1	1	1	2	2	1	1	1	2	2	1	1	1384095	4	1	1	0,0616		1
		2	2	2	1	1	3	3	1	1	2	2						0,4167		
61		3	3	1	1	1	4	2	2	2	1	3						0,1923		
		4	4	1	2	4	3	3	2	2	3	2						0,6995		
		5	1	2	1	3	2	3	2	1	2	2						0,3505		
		1	1	2	2	2	3	2	1	1	2	3						0,2402		
		2	2	1	2	2	4	3	1	2	1	3						0,2337		
62	1412787	3	3	2	2	3	5	2	1	2	2	3	3	1412791	4	0	3	0,027		1
		4	4	2	1	2	4	1	2	3	1	2						0,1567		
		5	3	1	2	4	5	3	1	2	1	1						0,4685		
		1	1	2	1	1	1	2	1	2	3	2						0,361		
		2	2	1	1	1	2	1	2	2	1	1						0,13		
63	1412791	3	3	2	1	2	4	1	2	3	3	3	3	1412807	16	1	3	0,0035		5
		4	4	2	1	1	2	2	1	3	2	2						0,2074		
		5	3	1	2	2	1	1	1	2	2	2						0,2038		
		1	1	1	1	1	3	2	2	2	1	2						0,5933		
	1441076	2	2	1	2	4	4	1	2	1	3	3	2	1441079	3	0	2	0,0397		2
64		3	3	1	1	4	5	2	1	3	1	2						0,5102		
		4	4	1	1	2	3	3	1	1	3	2						0,3379		
		5	2	1	1	1	5	3	2	3	3	1						0,1326		
		1	1	2	1	3	4	2	2	3	3	2						0,2317		
	1441079	2	2	1	2	4	2	2	1	1	3	1	2	1441099	20	0	2	0,0397		5
65		3	3	2	2	4	3	3	1	1	3	3						0,4146		
		4	4	1	2	3	5	2	1	3	3	2						0,5633		
		5	4	1	2	3	5	1	2	3	2	3						0,234		
	1441099	1	1	2	2	2	1	2	1	1	2	2	1	1441123	24	1	1	0,1425		5
		2	2	1	2	1	2	3	1	3	1	2						0,5212		
66		3	3	1	2	1	5	3	1	2	2	3						0,4328		
		4	4	2	2	4	5	1	1	3	3	2						0,5352		
		5	3	1	1	2	4	2	2	1	2	1						0,2626		
		1	1	2	1	4	1	1	1	1	1	1						0,2086		
	1470238	2	2	1	2	4	3	2	1	1	2	3	2	1470241	3	1	2	0,0258		1
67		3	3	1	1	1	1	3	1	1	2	1						0,0934		
		4	4	2	1	1	1	1	2	3	2	1						0,0592		
		5	2	2	1	4	3	3	2	2	3	1						0,1068		
		1	1	1	2	2	2	1	2	3	1	3						0,3402		
	1493395	2	2	2	2	4	2	2	1	2	1	3	2	1493400	5	1	2	0,3286		4

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
68		3	3	1	1	3	1	3	2	3	1	2						0,6086		
		4	4	2	2	4	2	3	1	3	1	3						0,4208		
		5	4	1	2	3	2	3	2	3	3	1						0,6193		
		1	1	1	1	1	3	3	2	3	3	2						0,4466		
		2	2	1	1	2	2	1	2	1	3	3						0,232		
69		3	3	1	2	3	4	1	1	1	3	1						0,2808		
		4	4	1	2	1	2	1	1	3	3	3						0,6394		
	1522864	5	1	1	2	4	4	3	1	2	1	3	5	1522868	4	1	1	0,1636		1
	1546102	1	1	2	2	1	1	2	2	3	3	3	1	1546106	4	1	1	0,3403		1
		2	2	1	1	2	4	2	1	2	1	3						0,5646		
70		3	3	2	1	1	4	3	2	1	3	1						0,7023		
		4	4	2	1	4	5	1	2	3	3	1						0,5568		
		5	2	2	2	4	3	3	2	2	3	1						0,6315		
		1	1	2	1	3	3	3	1	2	2	1						0,3603		
		2	2	1	2	1	2	3	1	2	1	3						0,4906		
71		3	3	1	2	2	2	2	2	2	3	2						0,5349		
		4	4	1	2	2	4	2	1	1	3	2						0,156		
	1575221	5	4	1	1	3	5	1	2	3	3	3	5	1575225	4	0	4	0,1152	212	1
		1	1	1	1	1	4	1	1	1	1	3						0,4295		
		2	2	1	1	4	4	2	1	3	1	1						0,4346		
72	1575225	3	3	1	2	3	4	3	2	2	3	3	3	1575249	24	1	3	0,039		5
		4	4	2	1	4	2	3	2	2	1	3						0,3851		
		5	1	2	2	2	3	2	2	2	2	1						0,1991		
		1	1	2	2	4	1	3	2	3	3	2						0,5123		
	1600777	2	2	2	1	3	2	2	1	2	2	2	2	1600782	5	1	2	0,1069		3
73		3	3	1	2	2	2	2	1	3	1	2						0,324		
		4	4	2	2	4	1	1	1	2	3	2						0,2749		
		5	3	2	2	4	3	1	2	1	3	2						0,3034		
		1	1	1	1	1	4	2	1	1	1	3						0,3595		
		2	2	2	1	2	2	3	1	3	3	3						0,1271		
74		3	3	1	2	4	3	3	1	1	3	2						0,599		
	1626024	4	4	2	2	2	2	2	1	1	1	2	4	1626029	5	1	4	0,0197		3
		5	2	1	2	2	5	3	1	2	2	1						0,0446		
		1	1	2	2	2	3	2	2	3	2	2						0,6614		
	1651994	2	2	2	2	1	2	2	2	2	3	1	2	1651998	4	1	2	0,1569		1
75		3	3	2	1	2	5	1	1	1	3	1						0,7051		
		4	4	1	1	3	4	2	2	3	2	3						0,2904		
		5	2	1	2	3	4	2	1	2	3	1						0,495		
	1679244	1	1	2	1	1	5	1	2	2	3	3	1	1679247	3	1	1	0,0173		1
		2	2	1	2	4	4	1	2	1	1	2						0,2508		
76		3	3	2	1	1	4	1	1	1	2	2						0,3897		
		4	4	2	1	2	5	3	1	3	2	3						0,2952		
		5	4	2	1	4	3	3	1	2	1	1						0,6425		
		1	1	2	2	2	3	2	2	1	2	2						0,3879		
		2	2	2	1	3	1	3	2	2	1	1						0,3728		
77		3	3	1	1	3	4	1	2	1	1	3						0,4499		
	1708974	4	4	2	1	1	4	3	1	3	2	2	4	1708978	4	1	4	0,1219		1
		5	2	2	1	2	2	1	2	3	1	3						0,5054		
	1734247	1	1	2	2	2	4	2	2	3	1	2	1	1734250	3	1	1	0,2794		1
		2	2	2	2	1	2	2	2	2	1	2						0,6995		
78		3	3	2	1	4	2	3	1	2	2	2						0,6517		
		4	4	2	2	2	5	1	1	1	3	2						0,4414		
		5	4	1	1	3	1	1	1	3	2	1						0,4333		
		1	1	1	2	2	4	1	2	2	2	2						0,6814		
		2	2	2	1	4	5	1	1	2	1	2						0,6473		
79		3	3	2	1	4	1	2	2	2	2	1						0,3514		
	1762088	4	4	1	1	1	4	3	1	2	2	3	4	1762093	5	1	4	0,3112		1
		5	3	1	1	4	1	1	2	3	3	1						0,5471		
	1791138	1	1	2	2	2	4	2	1	3	1	1	1	1791141	3	1	1	0,1915		2
		2	2	1	2	1	5	1	2	1	1	3						0,4753		
80		3	3	2	1	2	3	1	1	2	1	2						0,6484		
		4	4	2	2	2	1	2	2	3	3	3						0,4164		
		5	4	2	2	3	2	3	1	1	2	3						0,2171		
	1815019	1	1	2	1	4	3	2	2	3	2	3	1	1815022	3	1	1	0,0193		1
		2	2	1	2	3	4	2	2	1	1	2						0,6592		
81		3	3	1	1	2	5	2	1	1	3	3						0,2914		
		4	4	1	1	4	3	1	2	1	3	1						0,1198		
		5	3	1	2	4	5	1	2	1	3	1						0,0272		
		1	1	2	2	2	2	1	2	1	1	1						0,6086		
		2	2	2	2	2	1	2	1	1	2	2						0,5775		
82		3	3	1	1	1	1	2	1	1	1	2						0,6093		
		4	4	2	1	1	5	3	2	2	1	3						0,1692		
	1843208	5	3	2	1	1	1	2	1	3	1	2	5	1843212	4	1	3	0,0674		1
		1	1	1	1	4	4	2	1	2	1	2						0,5269		
		2	2	2	2	3	4	2	2	1	2	2						0,6999		
83		3	3	1	2	2	5	3	2	3	1	2						0,6221		
		4	4	2	1	2	4	1	1	3	2	1						0,439		
	1869539	5	3	2	1	4	5	1	1	3	3	3	5	1869542	3	1	3	0,029		1
		1	1	2	1	1	2	3	1	2	2	3						0,244		
	1898727	2	2	1	2	4	3	3	1	3	2	3	2	1898731	4	1	2	0,0293		1
84		3	3	1	1	1	5	3	1	3	1	2						0,2553		
		4	4	2	1	1	3	2	1	1	3	1						0,0629		
		5	1	2	2	1	4	1	2	2	2	3						0,2754		
		1	1	1	2	4	2	1	2	1	1	1						0,251		
		2	2	2	2	3	1	1	2	2	3	3						0,5261		
85		3	3	2	1	3	1	2	1	1	3	3						0,4896		
	1922639	4	4	2	1	2	1	2	1	3	1	1	4	1922642	3	1	4	0,2242		1
		5	3	2	1	1	2	2	2	1	2	1						0,2293		
	1948911	1	1	2	2	2	3	3	1	2	3	1	1	1948915	4	1	1	0,2711		1
		2	2	2	1	4	2	3	2	1	1	2						0,6808		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
86		3	3	2	1	3	1	1	1	1	3	2						0,668		
		4	4	2	2	4	3	2	2	2	3	1						0,3879		
		5	1	2	1	1	4	1	2	1	3	3						0,2739		
		1	1	1	2	1	2	2	2	3	2	2						0,3496		
		2	2	2	2	2	2	1	1	3	2	3						0,6467		
87		3	3	2	1	2	2	1	2	1	2	1						0,6849		
	1975023	4	4	2	2	1	5	1	1	1	2	2	4	1975028	5	1	4	0,3076		1
		5	4	1	2	3	4	3	2	3	1	2						0,343		
		1	1	1	1	2	2	2	1	3	3	2						0,2525		
	2004041	2	2	1	1	2	5	2	2	2	1	3	2	2004045	4	1	2	0,1037		1
88		3	3	1	1	2	1	3	2	3	3	2						0,1354		
		4	4	1	1	2	1	2	2	3	3	1						0,7096		
		5	2	2	1	1	1	3	2	1	2	2						0,5782		
		1	1	2	2	4	3	2	2	3	1	1						0,1945		
	2033423	2	2	1	1	1	1	1	1	3	3	2	2	2033428	5	1	2	0,0342		1
89		3	3	2	2	2	3	2	2	1	2	1						0,5701		
		4	4	2	2	2	5	1	2	1	1	2						0,358		
		5	4	2	1	3	1	2	2	1	3	2						0,6505		
		1	1	2	2	3	3	1	1	3	1	1						0,6213		
		2	2	2	2	3	5	1	1	2	3	3						0,4949		
90	2059782	3	3	2	1	4	1	1	1	1	3	3	3	2059787	5	1	3	0,0137		1
		4	4	1	1	3	5	1	2	3	3	1						0,2095		
		5	3	1	1	2	2	2	2	3	1	3						0,501		
		1	1	1	2	2	2	1	1	1	1	2						0,0843		
		2	2	2	2	3	2	3	1	1	1	1						0,4925		
91		3	3	2	2	1	5	2	1	3	1	2						0,3065		
		4	4	1	2	4	2	2	2	1	2	3						0,307		
	2083485	5	2	2	2	1	3	2	2	2	3	3	5	2083489	4	0	2	0,0427		1
		1	1	1	2	1	3	3	1	2	1	3						0,4785		
		2	2	2	1	3	5	2	1	3	3	1						0,1343		
92		3	3	1	1	2	1	1	2	1	2	3						0,1914		
		4	4	1	1	2	3	1	2	3	1	1						0,4037		
	2083489	5	2	1	2	2	1	2	1	3	3	3	5	2083504	15	1	2	0,1198		5
	2113311	1	1	2	1	1	5	1	2	2	2	3	1	2113315	4	1	1	0,0116		4
		2	2	1	1	3	1	1	2	2	3	2						0,3124		
93		3	3	1	2	3	1	3	2	1	3	1						0,2254		
		4	4	2	2	4	2	2	1	1	1	3						0,6298		
		5	4	2	2	3	1	1	2	2	1	2						0,7084		
	2138663	1	1	2	1	3	2	2	1	3	3	3	1	2138666	3	1	1	0,1457		4
		2	2	2	1	2	3	1	1	1	2	1						0,6437		
94		3	3	2	1	4	1	2	1	3	3	3						0,6312		
		4	4	1	2	1	1	1	1	2	1	2						0,2489		
		5	1	2	2	1	4	2	1	1	2	2						0,6466		
		1	1	1	2	3	5	1	2	3	2	2						0,5		
		2	2	2	2	4	2	2	2	1	1	3						0,2089		
95		3	3	2	2	3	3	3	1	2	3	3						0,1268		
	2165187	4	4	2	1	3	5	2	1	3	1	3	4	2165191	4	1	4	0,1054		1
		5	1	1	2	3	3	1	2	2	1	2						0,1725		
	2194580	1	1	2	2	3	5	2	2	2	1	3	1	2194584	4	1	1	0,142		3
		2	2	1	1	3	5	3	2	1	1	2						0,5911		
96		3	3	2	1	1	4	2	1	2	2	3						0,1868		
		4	4	2	1	2	4	3	2	3	3	1						0,2467		
		5	2	2	1	4	2	2	1	1	1	3						0,5645		
	2223726	1	1	1	2	3	3	2	1	2	2	3	1	2223730	4	1	1	0,0411		1
		2	2	1	2	3	5	3	2	1	3	1						0,3623		
97		3	3	1	2	3	1	3	2	2	3	2						0,4226		
		4	4	1	2	3	5	3	1	2	3	3						0,3401		
		5	3	1	1	2	1	2	2	3	3	3						0,0805		
		1	1	2	1	4	3	3	2	2	1	2						0,1008		
		2	2	2	1	4	1	2	1	2	2	3						0,4769		
98	2253379	3	3	1	2	4	3	2	2	3	1	1	3	2253382	3	1	3	0,0234		1
		4	4	1	2	2	3	1	2	3	3	2						0,1928		
		5	4	1	2	2	3	1	1	2	1	2						0,3774		
		1	1	2	1	2	2	2	1	3	3	1						0,6979		
		2	2	2	2	2	4	1	1	3	3	3						0,6657		
99		3	3	2	2	1	3	3	1	1	1	1						0,6397		
		4	4	1	1	1	5	1	2	1	1	2						0,5026		
	2279239	5	4	2	1	1	3	1	1	2	1	1	5	2279243	4	1	4	0,0506		1
	2302307	1	1	1	1	4	3	1	2	1	2	1	1	2302311	4	1	1	0,2342		1
		2	2	2	1	1	3	3	1	3	2	3						0,311		
100		3	3	2	1	4	5	3	1	1	1	1						0,4392		
		4	4	2	2	4	1	2	1	3	2	3						0,3722		
		5	2	1	1	3	4	3	2	2	2	2						0,4196		
		1	1	1	1	3	5	2	2	1	3	3						0,3751		
		2	2	1	2	3	3	1	2	3	2	3						0,1362		
101	2330413	3	3	2	2	3	1	3	2	2	2	2	3	2330417	4	1	3	0,0145		1
		4	4	2	2	4	2	1	1	1	1	1						0,0697		
		5	3	1	1	1	3	1	1	3	3	3						0,3989		
	2356258	1	1	2	1	2	3	3	1	2	2	3	1	2356262	4	1	1	0,1485		1
		2	2	2	1	3	5	2	1	3	1	2						0,5894		
102		3	3	2	2	4	3	2	2	2	1	3						0,435		
		4	4	2	2	4	5	1	2	3	3	1						0,3128		
		5	4	1	1	2	4	3	2	3	1	2						0,18		
		1	1	1	1	3	1	2	2	2	2	2						0,5275		
		2	2	2	2	3	2	3	2	3	1	3						0,2597		
103		3	3	2	2	2	1	3	2	2	1	3						0,5718		
		4	4	2	1	4	4	1	2	2	3	1						0,5684		
	2382325	5	1	2	2	3	5	3	2	2	2	1	5	2382328	3	1	1	0,0748		1
		1	1	2	2	3	2	2	1	2	3	2						0,608		
		2	2	1	1	3	1	3	2	2	3	1						0,2613		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
104		3	3	2	1	3	3	2	2	2	2	2						0,7017		
		4	4	1	1	3	1	2	2	2	2	3						0,3412		
	2408772	5	1	2	1	4	3	2	1	3	1	3	5	2408776	4	1	1	0,0583		1
		1	1	2	2	2	1	1	2	1	1	1						0,3467		
		2	2	1	1	2	1	3	1	1	1	3						0,2056		
105		3	3	1	1	4	2	1	2	1	3	3						0,2855		
		4	4	1	2	3	5	3	2	1	1	1						0,15		
	2433681	5	1	1	2	2	4	2	2	2	2	2	5	2433684	3	1	1	0,1193		1
		1	1	2	1	3	2	1	1	1	1	1						0,6012		
	2460985	2	2	1	2	2	4	2	2	1	3	1	2	2460988	3	0	2	0,2079		1
106		3	3	2	2	1	5	3	2	1	2	3						0,6405		
		4	4	2	2	2	5	2	2	3	3	3						0,5408		
		5	1	1	2	3	1	3	2	2	3	2						0,267		
		1	1	2	1	3	4	1	1	1	2	2						0,0292		
	2460988	2	2	1	1	1	4	1	2	2	1	2	2	2461004	16	1	2	0,0118		5
107		3	3	2	2	2	1	2	1	1	2	3						0,2703		
		4	4	2	2	1	3	3	2	1	1	2						0,309		
		5	1	2	2	4	1	3	2	2	3	2						0,5559		
		1	1	1	2	1	4	2	2	3	1	2						0,4549		
		2	2	2	1	4	4	3	1	3	1	3						0,6231		
108		3	3	2	1	2	3	3	1	3	2	2						0,6351		
		4	4	1	2	2	1	1	2	2	1	3						0,6469		
	2487063	5	4	1	1	4	4	2	1	1	3	3	5	2487067	4	1	4	0,13		1
		1	1	2	1	3	1	3	1	2	3	2						0,5291		
		2	2	1	1	3	3	2	2	2	2	3						0,4518		
109		3	3	2	2	4	2	1	1	3	3	3						0,4456		
		4	4	2	1	4	1	2	1	3	1	1						0,6041		
	2513884	5	1	1	2	3	4	2	2	2	3	1	5	2513888	4	1	1	0,1753		1
	2541482	1	1	1	1	3	2	2	1	3	1	2	1	2541487	5	1	1	0,2122		1
		2	2	1	1	2	4	2	1	3	2	3						0,4814		
110		3	3	2	2	4	4	2	1	3	2	3						0,4703		
		4	4	1	2	4	5	1	1	2	1	2						0,4899		
		5	2	1	2	4	1	2	1	2	2	2						0,4481		
	2565613	1	1	2	2	4	5	1	1	2	1	2	1	2565617	4	1	1	0,0347		4
		2	2	1	1	3	4	2	2	1	1	2						0,4728		
111		3	3	2	1	4	1	3	2	1	3	1						0,3467		
		4	4	2	1	4	4	2	1	3	2	1						0,2111		
		5	2	1	2	1	3	1	2	2	2	2						0,4493		
		1	1	1	2	4	1	1	1	1	3	1						0,2408		
		2	2	2	2	2	3	3	2	3	1	2						0,2957		
112		3	3	1	2	1	4	2	2	2	1	2						0,4508		
	2590657	4	4	2	2	1	1	3	1	3	3	1	4	2590661	4	1	4	0,2031		1
		5	3	1	1	3	3	2	1	1	1	2						0,5528		
		1	1	1	1	1	2	2	2	1	2	2						0,6168		
		2	2	2	2	4	3	1	1	2	1	3						0,5612		
113		3	3	2	2	2	5	1	1	2	1	3						0,3025		
		4	4	2	2	2	2	2	1	2	2	2						0,4155		
	2617672	5	4	1	2	3	2	3	2	2	1	1	5	2617676	4	1	4	0,0952		4
		1	1	2	2	1	2	2	2	1	3	2						0,3236		
		2	2	1	1	3	1	2	1	1	3	1						0,4587		
114		3	3	2	2	4	3	3	2	2	3	1						0,2987		
		4	4	2	1	1	3	2	2	1	2	1						0,7189		
	2646112	5	2	2	2	4	1	2	2	3	1	3	5	2646117	5	0	2	0,1383		1
	2646117	1	1	1	2	4	4	1	1	2	1	1	1	2646142	25	0	1	0,2537		5
		2	2	1	2	4	5	1	1	3	1	2						0,5588		
115		3	3	2	1	3	1	3	1	1	2	3						0,656		
		4	4	1	2	4	5	3	1	2	2	3						0,4314		
		5	3	1	2	4	4	2	1	1	2	3						0,4559		
		1	1	1	2	1	1	3	1	2	1	3						0,6072		
		2	2	1	2	2	5	2	2	2	2	2						0,4184		
116		3	3	1	2	3	4	3	1	1	2	3						0,2645		
		4	4	1	1	3	5	2	1	1	1	2						0,5519		
	2646142	5	3	1	2	3	2	3	1	2	2	3	5	2646162	20	1	3	0,1692		5
		1	1	2	2	4	5	3	1	2	2	1						0,3512		
	2668924	2	2	2	2	2	5	1	1	2	2	3	2	2668928	4	1	2	0,0378		1
117		3	3	1	2	4	2	2	2	2	3	2						0,1729		
		4	4	2	1	2	4	2	1	3	1	1						0,5465		
		5	1	1	2	1	1	1	1	3	1	2						0,3563		
		1	1	2	2	3	5	1	1	2	1	2						0,1006		
		2	2	2	1	4	1	2	1	2	2	2						0,3138		
118	2698792	3	3	2	1	3	4	1	1	1	3	3	3	2698795	3	1	3	0,0599		1
		4	4	1	2	4	3	3	2	2	3	1						0,5779		
		5	4	2	1	1	4	3	1	3	3	1						0,5136		
		1	1	1	2	4	3	2	1	1	2	3						0,1827		
		2	2	2	2	4	2	1	1	3	3	2						0,2026		
119		3	3	1	1	3	2	3	2	3	2	1						0,369		
	2723982	4	4	2	1	3	3	3	2	2	1	3	4	2723987	5	1	4	0,0794		1
		5	1	1	2	4	4	2	1	3	2	1						0,4808		
		1	1	2	1	4	1	3	1	3	3	3						0,6884		
	2750799	2	2	2	1	3	5	2	1	2	1	1	2	2750802	3	1	2	0,0028		1
120		3	3	1	2	1	1	3	2	3	2	2						0,2847		
		4	4	1	2	4	4	3	2	3	3	1						0,6388		
		5	3	2	1	1	2	2	2	3	1	1						0,1259		
		1	1	2	1	4	4	3	1	1	2	2						0,0242		
		2	2	2	2	1	2	3	1	1	2	2						0,1845		
121	2779744	3	3	1	1	2	5	2	2	2	3	3	3	2779748	4	1	3	0,0194		1
		4	4	1	1	1	2	1	2	3	1	2						0,1034		
		5	2	1	2	2	5	2	1	1	1	2						0,6269		
		1	1	1	1	3	2	3	2	1	1	2						0,1987		
	2806185	2	2	2	2	3	4	2	1	2	1	3	2	2806189	4	1	2	0,032		1

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
122		3	3	2	2	2	2	1	1	3	3	3						0,6119		
		4	4	1	1	2	2	2	1	2	2	1						0,3347		
		5	1	1	2	3	5	3	1	2	3	1						0,5083		
	2835079	1	1	1	1	1	2	1	1	3	2	3	1	2835084	5	1	1	0,0305		1
		2	2	1	1	1	4	2	1	1	1	2						0,4796		
123		3	3	1	1	1	3	3	2	3	3	3						0,5719		
		4	4	1	1	1	2	3	1	2	2	2						0,1607		
		5	3	1	2	3	5	2	2	1	1	1						0,2606		
		1	1	1	1	3	2	3	2	2	3	1						0,2664		
		2	2	1	1	2	1	1	1	1	1	3						0,6082		
124	2863783	3	3	1	2	4	2	2	1	2	3	2	3	2863788	5	1	3	0,1873		1
		4	4	2	2	1	5	3	1	1	3	2						0,6552		
		5	2	2	2	1	5	2	2	2	3	2						0,3469		
		1	1	2	1	3	1	3	2	2	2	1						0,4185		
	2886826	2	2	1	2	1	4	3	2	2	2	3	2	2886829	3	1	2	0,0321		1
125		3	3	1	1	3	1	3	1	3	1	2						0,4527		
		4	4	1	2	4	1	2	2	1	3	3						0,6904		
		5	1	2	1	1	1	2	1	2	1	2						0,6664		
	2916322	1	1	1	1	2	1	2	1	2	3	1	1	2916327	5	1	1	0,1205		1
		2	2	2	2	2	3	2	1	3	1	3						0,4428		
126		3	3	1	2	1	3	1	2	2	3	3						0,5006		
		4	4	1	2	4	2	3	1	1	1	3						0,3148		
		5	3	2	2	2	4	1	2	2	2	3						0,4965		
		1	1	2	1	3	1	1	1	2	3	3						0,5929		
		2	2	1	2	2	3	3	2	1	2	3						0,5671		
127		3	3	1	2	4	3	2	1	1	2	3						0,5523		
	2942368	4	4	2	1	4	5	3	2	3	2	1	4	2942373	5	0	4	0,1704		1
		5	1	1	1	1	1	1	2	2	1	2						0,5952		
		1	1	2	1	3	2	1	2	1	2	3						0,5614		
	2942373	2	2	1	2	4	1	3	1	3	2	3	2	2942390	17	1	2	0,1729		5
128		3	3	1	1	3	4	2	1	1	1	1						0,4552		
		4	4	2	2	3	5	2	2	2	1	1						0,5036		
		5	4	2	2	4	4	2	2	1	1	1						0,6942		
		1	1	1	1	3	2	2	1	3	1	1						0,6791		
	2972361	2	2	1	1	2	4	3	2	1	1	1	2	2972364	3	0	2	0,0739		1
129		3	3	1	2	1	3	2	2	1	1	2						0,1184		
		4	4	2	1	4	3	1	2	1	1	2						0,2375		
		5	3	1	1	4	1	3	2	1	2	1						0,6486		
		1	1	2	1	2	1	3	2	3	3	1						0,5105		
		2	2	1	2	2	3	1	2	3	3	2						0,4798		
130		3	3	2	2	4	2	1	1	3	3	3						0,4229		
	2972364	4	4	2	1	3	2	1	2	2	2	3	4	2972383	19	1	4	0,058		5
		5	2	1	1	1	5	1	1	3	1	1						0,6404		
		1	1	2	1	3	5	2	1	1	3	1						0,4469		
		2	2	2	2	1	5	2	1	1	1	2						0,703		
131	2996929	3	3	2	2	4	1	1	2	1	3	3	3	2996934	5	1	3	0,2197		1
		4	4	1	2	2	5	2	2	2	2	3						0,6709		
		5	2	1	2	2	2	2	2	1	2	2						0,2826		
	3024579	1	1	1	1	4	4	1	1	3	1	1	1	3024584	5	1	1	0,0677		1
		2	2	1	1	3	3	2	1	2	1	1						0,3152		
132		3	3	1	2	2	3	3	2	1	1	1						0,6448		
		4	4	1	2	1	1	1	2	3	1	3						0,2132		
		5	4	2	1	3	4	1	2	3	3	1						0,6568		
		1	1	2	1	4	3	3	2	2	1	1						0,3965		
		2	2	1	1	4	3	1	2	1	3	1						0,5835		
133		3	3	2	1	4	2	3	2	2	2	3						0,4905		
		4	4	2	1	1	1	2	2	3	2	1						0,5967		
	3051110	5	3	2	2	1	2	1	1	1	2	1	5	3051114	4	0	3	0,3454		1
		1	1	2	2	4	4	3	1	2	2	3						0,3962		
		2	2	2	1	4	5	1	2	1	1	2						0,4819		
134	3051114	3	3	1	1	1	1	1	2	2	1	1	3	3051137	23	1	3	0,1984		5
		4	4	2	2	2	1	1	2	1	3	1						0,562		
		5	3	2	1	3	2	2	1	1	3	3						0,3212		
		1	1	1	1	1	2	2	1	1	3	3						0,3704		
		2	2	1	1	2	3	2	1	3	1	1						0,2159		
135		3	3	2	2	4	5	3	1	1	1	3						0,4316		
	3074651	4	4	2	1	3	3	3	2	2	3	1	4	3074655	4	1	4	0,0159		1
		5	4	2	2	3	3	2	1	3	3	3						0,131		
		1	1	2	2	3	1	3	2	1	2	1						0,3358		
		2	2	1	2	1	5	1	2	3	2	2						0,5142		
136		3	3	2	1	3	4	2	1	3	3	3						0,3501		
		4	4	2	2	2	5	2	1	2	1	3						0,5629		
	3097868	5	4	1	1	1	1	3	2	2	3	3	5	3097873	5	1	4	0,2025		1
		1	1	1	1	4	1	2	1	3	2	1						0,5604		
		2	2	2	1	2	2	2	2	3	3	2						0,356		
137	3124258	3	3	1	1	2	5	3	2	3	1	3	3	3124262	4	0	3	0,1825		1
		4	4	2	2	4	1	1	1	3	2	3						0,476		
		5	1	1	1	2	1	2	1	2	2	3						0,7163		
		1	1	1	1	3	3	3	2	3	3	2						0,5917		
		2	2	2	1	2	1	3	2	2	1	3						0,6371		
138	3124262	3	3	1	1	2	4	1	2	2	2	1	3	3124284	22	1	3	0,1347		5
		4	4	1	2	3	3	3	1	1	1	1						0,1422		
		5	2	2	2	1	5	3	1	1	1	1						0,534		
		1	1	2	1	3	4	3	2	3	1	1						0,3075		
		2	2	2	1	1	1	3	2	3	3	3						0,6673		
139	3149720	3	3	2	1	1	2	1	2	2	2	1	3	3149723	3	1	3	0,1512		1
		4	4	1	1	4	3	3	2	2	3	2						0,6204		
		5	1	1	2	1	1	2	1	1	3	1						0,2411		
		1	1	1	1	3	4	3	2	2	3	3						0,628		
		2	2	1	1	1	3	2	1	1	3	3						0,515		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
140		3	3	2	2	4	3	3	1	3	3	3						0,6961		
		4	4	1	1	2	2	3	2	2	3	3						0,6637		
	3177128	5	2	1	1	3	5	1	1	1	3	1	5	3177133	5	1	2	0,0492		1
		1	1	1	1	3	2	1	2	3	1	1						0,4078		
	3203881	2	2	1	1	3	3	1	2	3	2	1	2	3203886	5	1	2	0,0388		3
141		3	3	2	1	1	2	1	1	2	2	1						0,1477		
		4	4	1	1	2	5	3	2	2	1	1						0,6714		
		5	3	1	1	4	2	2	1	3	2	1						0,0498		
		1	1	2	1	4	1	2	1	1	1	1						0,617		
	3232415	2	2	2	2	2	2	1	1	2	1	2	2	3232420	5	1	2	0,0913		2
142		3	3	2	1	2	3	3	2	3	2	2						0,4797		
		4	4	2	2	2	3	3	2	2	3	2						0,3069		
		5	4	2	2	2	5	2	2	2	2	2						0,1002		
	3255846	1	1	2	2	4	1	1	2	1	3	3	1	3255850	4	0	1	0,0547		1
		2	2	2	2	1	2	1	2	1	1	1						0,2709		
143		3	3	2	1	2	1	3	1	2	1	2						0,6303		
		4	4	2	1	3	3	1	2	3	2	2						0,4477		
		5	1	2	2	3	5	3	2	1	3	2						0,3739		
	3255850	1	1	2	1	3	3	2	1	1	2	2	1	3255867	17	1	1	0,0398		5
		2	2	2	1	1	5	3	1	3	1	1						0,7083		
144		3	3	2	2	2	1	2	1	1	1	1						0,0522		
		4	4	1	2	2	5	2	1	1	1	3						0,6157		
		5	1	2	2	1	3	2	1	2	2	2						0,3228		
		1	1	1	1	2	2	3	2	2	2	3						0,0878		
		2	2	1	2	1	4	1	2	2	3	1						0,3653		
145	3285417	3	3	1	2	4	5	2	1	3	2	1	3	3285421	4	1	3	0,0496		1
		4	4	2	2	1	1	3	1	2	2	1						0,7101		
		5	4	1	2	1	2	2	2	3	1	3						0,3937		
		1	1	1	1	2	2	1	1	1	3	3						0,2483		
		2	2	2	2	3	5	1	2	2	2	1						0,1086		
146		3	3	1	2	1	4	3	2	1	3	2						0,4912		
	3314419	4	4	1	2	4	4	1	1	3	3	2	4	3314422	3	1	4	0,1042		1
		5	3	2	2	3	2	2	1	2	1	3						0,4194		
		1	1	1	1	3	1	2	1	2	2	3						0,6054		
	3343089	2	2	1	2	2	3	3	1	3	1	1	2	3343092	3	1	2	0,1717		1
147		3	3	2	2	3	4	2	1	2	2	1						0,5012		
		4	4	2	1	2	5	3	1	3	3	1						0,4277		
		5	1	1	2	4	2	1	1	1	3	1						0,5684		
	3369977	1	1	1	2	3	2	2	2	2	1	2	1	3369982	5	1	1	0,1188		1
		2	2	2	1	2	1	1	2	2	3	3						0,2776		
148		3	3	2	1	2	1	2	1	3	3	1						0,4364		
		4	4	2	1	1	2	3	1	2	1	3						0,4811		
		5	1	1	1	3	2	1	2	1	3	2						0,15		
		1	1	2	2	4	4	1	2	2	2	3						0,5087		
		2	2	1	1	2	3	3	2	2	3	2						0,5074		
149	3399796	3	3	1	1	2	3	3	1	3	3	3	3	3399800	4	0	3	0,1203		4
		4	4	1	2	1	3	1	1	2	3	3						0,2133		
		5	3	1	1	2	4	3	2	3	2	1						0,6051		
		1	1	1	2	3	2	3	2	2	2	2						0,6758		
	3399800	2	2	2	1	3	1	2	2	2	2	3	2	3399816	16	1	2	0,0318		5
150		3	3	2	1	1	3	3	2	1	3	3						0,5193		
		4	4	1	1	2	4	2	1	3	1	2						0,4718		
		5	4	1	2	3	3	3	1	3	3	1						0,3059		
	3429032	1	1	2	2	4	4	1	2	3	3	2	1	3429036	4	1	1	0,3274		1
		2	2	2	2	3	2	1	1	1	2	1						0,449		
151		3	3	1	1	2	4	2	2	2	1	1						0,3578		
		4	4	2	2	3	2	1	2	2	1	2						0,3457		
		5	2	2	2	4	4	3	2	2	1	2						0,5105		
		1	1	2	2	4	1	2	2	2	2	3						0,6519		
	3453235	2	2	1	2	2	5	2	2	1	3	2	2	3453240	5	1	2	0,0435		1
152		3	3	1	2	3	2	3	1	1	3	1						0,4061		
		4	4	2	2	1	3	3	1	2	3	1						0,2544		
		5	1	2	1	2	3	2	2	1	2	2						0,3818		
		1	1	2	1	1	1	2	2	1	3	1						0,5918		
		2	2	1	1	4	3	3	1	1	2	2						0,6144		
153	3479744	3	3	1	1	2	1	2	2	3	3	3	3	3479747	3	1	3	0,0042		1
		4	4	2	2	3	2	2	2	3	1	1						0,4474		
		5	2	2	2	3	3	1	1	2	2	1						0,035		
		1	1	2	1	1	3	3	2	1	3	3						0,598		
		2	2	1	2	3	2	1	2	1	2	1						0,5377		
154		3	3	2	2	2	1	1	1	1	3	2						0,5221		
	3505230	4	4	1	2	3	2	1	2	3	2	1	4	3505234	4	1	4	0,3187		1
		5	2	2	1	1	1	1	2	3	2	3						0,6477		
		1	1	2	1	2	3	1	1	1	3	3						0,3011		
		2	2	1	2	2	5	3	2	1	1	2						0,4799		
155	3532252	3	3	2	2	4	5	3	1	1	3	3	3	3532256	4	1	3	0,068		1
		4	4	2	1	2	1	3	2	2	1	3						0,4965		
		5	1	2	1	1	1	3	2	2	3	3						0,0858		
		1	1	1	2	3	1	3	1	2	2	3						0,575		
	3559995	2	2	1	2	4	4	3	2	1	2	1	2	3560000	5	1	2	0,2945		1
156		3	3	1	1	4	3	3	1	1	1	1						0,3031		
		4	4	2	2	3	4	2	2	1	3	2						0,6466		
		5	4	2	1	4	3	2	2	1	2	3						0,4169		
		1	1	1	1	3	1	3	2	3	3	3						0,4719		
	3584617	2	2	1	2	1	2	2	2	1	1	2	2	3584621	4	1	2	0,2415		1
157		3	3	2	1	1	3	3	1	2	2	1						0,5087		
		4	4	1	1	3	3	3	1	2	3	2						0,5917		
		5	3	1	2	4	4	2	1	1	1	1						0,3286		
		1	1	1	1	4	3	1	1	2	3	1						0,6936		
		2	2	1	2	4	2	1	1	1	1	1						0,1488		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
158		3	3	1	1	4	5	1	2	1	3	3						0,6723		
		4	4	2	2	2	5	3	2	1	3	2						0,1395		
	3611124	5	2	1	1	3	3	3	1	3	1	1	5	3611129	5	1	2	0,1107		1
		1	1	1	1	3	4	1	1	3	3	1						0,2745		
		2	2	2	1	1	4	2	2	3	1	1						0,3894		
159		3	3	2	2	2	2	1	1	2	2	2						0,0769		
	3635116	4	4	2	2	1	4	3	1	2	1	3	4	3635120	4	1	4	0,0715		1
		5	4	2	1	2	2	3	2	1	1	3						0,4391		
	3662184	1	1	2	2	3	1	3	2	3	3	3	1	3662189	5	1	1	0,0733		4
		2	2	1	1	4	1	2	1	2	2	1						0,555		
160		3	3	2	2	4	4	2	2	1	2	2						0,3008		
		4	4	2	1	3	4	3	1	1	2	3						0,1133		
		5	1	2	1	2	5	2	1	1	2	1						0,2406		
		1	1	1	2	4	4	1	1	1	2	1						0,5308		
	3686574	2	2	1	2	4	4	2	1	3	2	3	2	3686579	5	1	2	0,3068		1
161		3	3	2	2	2	4	3	1	3	1	3						0,3989		
		4	4	1	2	1	2	2	2	3	1	2						0,6001		
		5	3	2	1	3	3	3	2	3	3	3						0,6262		
		1	1	1	1	2	1	2	2	3	3	1						0,6339		
		2	2	1	2	1	4	1	2	3	2	1						0,0764		
162	3716173	3	3	2	1	1	1	2	2	1	1	3	3	3716176	3	1	3	0,0016		1
		4	4	1	2	4	2	2	2	2	3	3						0,2697		
		5	2	2	1	4	5	1	1	3	1	1						0,3148		
		1	1	1	2	2	3	2	2	2	2	1						0,4312		
	3743378	2	2	2	1	2	4	2	2	3	3	1	2	3743382	4	0	2	0,0059		1
163		3	3	2	1	4	3	1	2	2	2	2						0,0103		
		4	4	2	1	2	2	3	2	3	3	3						0,6432		
		5	1	2	2	4	2	2	2	2	3	3						0,6811		
	3743382	1	1	2	1	2	5	3	1	3	3	2	1	3743397	15	1	1	0,0709		5
		2	2	1	1	2	3	2	2	3	3	1						0,4299		
164		3	3	2	1	4	5	3	2	3	1	3						0,1554		
		4	4	1	2	4	4	2	1	1	2	1						0,5473		
		5	1	1	2	4	4	1	2	1	2	1						0,3344		
		1	1	2	2	3	1	2	1	3	1	2						0,2568		
		2	2	2	1	4	5	2	1	1	1	3						0,6885		
165		3	3	2	2	3	2	1	2	2	3	3						0,4399		
		4	4	1	1	2	3	2	2	3	1	2						0,5033		
	3768027	5	1	2	1	4	2	2	2	2	1	2	5	3768031	4	1	1	0,1909		1
		1	1	1	2	3	4	2	1	2	1	2						0,6725		
		2	2	1	2	1	3	3	1	2	1	2						0,1383		
166		3	3	2	2	1	2	3	2	3	3	2						0,3502		
		4	4	1	1	4	3	3	2	3	3	3						0,6616		
	3796695	5	3	1	2	4	1	3	2	3	2	1	5	3796698	3	1	3	0,1151		1
		1	1	2	2	2	3	2	2	1	1	2						0,6608		
		2	2	1	1	4	5	3	2	3	1	1						0,3139		
167		3	3	2	1	4	3	3	1	3	3	2						0,476		
	3823396	4	4	1	1	4	5	3	1	2	2	3	4	3823401	5	1	4	0,1331		1
		5	3	1	2	1	1	3	2	2	2	1						0,5121		
		1	1	2	1	1	5	1	2	1	3	1						0,6075		
		2	2	1	1	1	4	2	2	3	2	3						0,4369		
168		3	3	2	2	1	1	3	2	3	2	1						0,2307		
	3850465	4	4	2	1	1	1	1	1	3	2	3	4	3850469	4	1	4	0,0849		1
		5	3	1	2	4	2	1	1	1	3	1						0,5165		
		1	1	1	2	1	2	3	1	3	3	2						0,6642		
	3875357	2	2	2	2	2	5	3	1	1	3	1	2	3875362	5	1	2	0,2261		2
169		3	3	1	2	3	3	1	1	3	3	1						0,5596		
		4	4	1	1	4	2	3	2	1	2	2						0,5916		
		5	4	1	1	1	4	2	1	3	2	1						0,5555		
	3898476	1	1	2	2	3	1	3	2	1	2	1	1	3898480	4	1	1	0,1904		1
		2	2	2	1	2	3	2	2	1	1	1						0,6078		
170		3	3	1	1	1	3	2	1	2	2	3						0,2481		
		4	4	1	1	1	1	3	2	1	2	1						0,3991		
		5	1	1	2	3	3	2	1	1	1	2						0,7164		
		1	1	1	2	4	3	2	2	1	2	3						0,5203		
		2	2	1	1	2	3	1	1	2	1	3						0,2588		
171		3	3	1	2	2	2	1	2	3	3	3						0,5323		
	3924129	4	4	1	2	1	4	3	2	1	2	1	4	3924133	4	1	4	0,0676		1
		5	2	1	2	3	2	2	2	1	3	3						0,5229		
		1	1	1	2	4	3	1	2	3	2	3						0,3311		
		2	2	2	1	4	4	3	1	1	3	2						0,3768		
172		3	3	1	1	2	1	3	1	2	1	3						0,3685		
		4	4	2	1	1	5	1	1	2	3	3						0,494		
	3953498	5	3	1	2	2	2	2	2	1	3	3	5	3953503	5	1	3	0,287		1
		1	1	2	1	3	1	2	1	3	3	3						0,4528		
		2	2	1	1	4	2	3	1	2	2	1						0,5522		
173		3	3	2	2	2	5	3	2	3	1	1						0,4593		
	3979660	4	4	2	1	1	5	2	2	1	3	1	4	3979663	3	1	4	0,2037		1
		5	3	1	1	2	3	3	1	1	2	1						0,4171		
		1	1	2	2	4	5	3	2	3	3	1						0,5108		
	4008904	2	2	1	1	4	4	3	2	2	1	1	2	4008909	5	1	2	0,1446		1
174		3	3	2	2	1	1	3	2	3	1	3						0,3363		
		4	4	1	1	3	4	3	1	3	3	1						0,5183		
		5	2	2	2	2	3	2	1	2	2	2						0,3272		
		1	1	2	1	1	1	2	2	3	3	1						0,1185		
		2	2	2	1	3	4	3	2	1	2	1						0,2571		
175		3	3	1	2	2	1	1	1	3	1	3						0,3541		
	4036855	4	4	1	1	1	2	1	2	3	1	2	4	4036859	4	1	4	0,0885		1
		5	1	2	1	3	2	3	1	1	1	3						0,4301		
		1	1	2	2	2	2	3	2	2	2	1						0,4173		
		2	2	1	1	1	4	3	1	1	2	3						0,3604		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
176		3	3	2	2	2	3	2	1	1	3	3						0,5346		
	4065418	4	4	2	1	2	3	2	1	3	2	1	4	4065422	4	1	4	0,106		4
		5	2	1	2	3	1	2	2	3	1	2						0,1128		
		1	1	1	1	4	1	1	2	1	1	3						0,4825		
		2	2	2	1	4	1	1	1	2	2	3						0,3581		
177	4093434	3	3	2	1	1	1	2	2	3	3	3	3	4093437	3	0	3	0,0176		1
		4	4	2	1	3	4	2	1	2	2	3						0,2062		
		5	2	2	2	2	3	2	2	2	1	1						0,4989		
	4093437	1	1	1	2	2	2	2	2	3	1	2	1	4093459	22	1	1	0,1119		5
		2	2	1	1	2	3	2	1	2	1	1						0,3212		
178		3	3	2	1	4	3	1	1	2	2	1						0,5448		
		4	4	1	1	1	4	1	1	2	2	2						0,1463		
		5	2	1	2	3	1	1	2	3	2	2						0,5998		
		1	1	2	2	1	5	1	2	3	2	2						0,3427		
		2	2	1	2	4	4	3	1	3	3	2						0,55		
179	4119882	3	3	2	1	3	5	2	1	2	1	3	3	4119887	5	1	3	0,0403		4
		4	4	1	1	4	4	1	1	3	1	2						0,5237		
		5	1	1	2	4	5	1	1	1	2	2						0,5198		
		1	1	2	1	4	3	3	2	3	1	1						0,7003		
	4144722	2	2	1	1	4	1	3	2	1	3	1	2	4144726	4	1	2	0,2852		1
180		3	3	2	1	1	2	2	2	3	3	1						0,5567		
		4	4	1	1	2	1	2	2	3	1	2						0,4977		
		5	3	2	2	3	1	2	2	1	3	2						0,6565		
		1	1	2	1	2	5	3	1	2	1	1						0,3208		
		2	2	1	1	3	2	2	2	1	1	3						0,696		
181	4167441	3	3	2	2	3	1	3	2	3	2	2	3	4167445	4	1	3	0,052		4
		4	4	2	2	2	1	1	2	3	3	3						0,1952		
		5	1	2	2	3	2	2	1	1	2	2						0,2426		
		1	1	1	2	3	5	3	2	2	1	3						0,1962		
		2	2	2	1	4	5	3	2	1	3	2						0,5854		
182		3	3	2	2	1	3	2	1	2	1	2						0,1572		
	4195035	4	4	2	1	3	5	1	1	2	2	2	4	4195038	3	1	4	0,0549		1
		5	4	2	1	4	2	1	2	1	3	2						0,2275		
	4217754	1	1	2	1	1	5	2	2	1	3	3	1	4217757	3	1	1	0,1729		1
		2	2	2	1	1	4	1	1	1	1	2						0,6601		
183		3	3	1	1	3	2	1	2	1	1	1						0,6528		
		4	4	1	2	1	3	1	1	1	1	2						0,3051		
		5	3	1	1	2	4	3	1	3	1	2						0,301		
		1	1	2	2	3	5	3	1	3	1	1						0,1705		
		2	2	1	2	3	2	3	2	2	3	2						0,184		
184		3	3	1	1	4	3	1	2	1	3	1						0,1395		
	4243799	4	4	1	1	1	1	2	1	1	1	3	4	4243803	4	1	4	0,1104		4
		5	2	1	2	4	5	3	1	1	1	3						0,3689		
	4270896	1	1	1	2	2	2	2	2	2	1	2	1	4270901	5	1	1	0,0876		1
		2	2	1	2	2	2	3	2	1	3	3						0,1856		
185		3	3	1	2	4	1	3	1	3	1	2						0,4695		
		4	4	2	2	3	3	3	2	3	3	3						0,2571		
		5	2	2	2	1	4	1	2	2	2	2						0,5782		
		1	1	1	1	4	4	3	2	2	2	1						0,5957		
		2	2	2	1	3	1	3	2	2	3	3						0,2715		
186		3	3	2	2	1	4	3	1	1	1	2						0,2937		
		4	4	1	2	1	5	1	2	2	2	1						0,3652		
	4294905	5	2	2	2	4	3	3	2	3	1	3	5	4294910	5	1	2	0,2269		1
	4320615	1	1	2	2	1	2	2	1	3	2	2	1	4320620	5	1	1	0,2304		1
		2	2	1	1	2	1	1	2	1	1	2						0,6675		
187		3	3	1	1	3	2	1	2	1	1	2						0,4724		
		4	4	2	1	2	4	2	2	3	2	3						0,2856		
		5	4	2	1	4	2	3	2	2	3	3						0,3021		
		1	1	1	1	4	3	1	1	3	2	1						0,2459		
		2	2	1	1	4	1	3	1	3	3	2						0,405		
188		3	3	2	1	2	4	1	2	2	1	2						0,2507		
	4347969	4	4	2	2	4	3	3	1	2	1	2	4	4347972	3	1	4	0,1062		1
		5	3	1	2	3	5	2	2	2	1	1						0,3408		
		1	1	1	1	1	2	2	2	1	1	2						0,4445		
	4375183	2	2	2	1	1	3	1	1	2	1	2	2	4375186	3	1	2	0,0195		2
189		3	3	2	2	3	5	1	1	3	3	2						0,5202		
		4	4	2	1	3	2	3	2	3	3	2						0,2708		
		5	3	1	2	4	2	1	1	1	2	3						0,6043		
		1	1	1	1	1	2	3	2	3	3	3						0,2028		
		2	2	1	1	2	4	2	2	2	1	3						0,2211		
190	4401986	3	3	1	2	1	4	2	1	2	3	1	3	4401991	5	1	3	0,0086		1
		4	4	1	1	4	5	1	2	2	3	2						0,5656		
		5	3	2	2	3	2	3	2	3	1	3						0,1784		
		1	1	1	1	1	3	1	2	3	3	2						0,6138		
	4431325	2	2	1	1	3	2	1	2	2	1	1	2	4431330	5	0	2	0,2809		3
191		3	3	1	2	4	5	3	1	2	1	2						0,3019		
		4	4	1	1	4	4	3	1	1	1	2						0,5275		
		5	1	2	2	3	1	2	1	2	2	1						0,6218		
		1	1	2	1	1	5	1	2	3	1	3						0,4627		
		2	2	2	2	3	1	3	1	3	1	3						0,3429		
192	4431330	3	3	2	2	1	4	3	1	2	2	3	3	4431349	19	1	3	0,1698		5
		4	4	2	1	2	1	1	2	1	3	3						0,3329		
		5	1	2	1	2	5	1	2	3	2	1						0,6242		
	4458270	1	1	2	2	2	5	1	2	3	1	2	1	4458275	5	1	1	0,2692		4
		2	2	2	2	4	5	2	1	1	1	1						0,6474		
193		3	3	2	2	3	4	2	2	3	1	2						0,658		
		4	4	2	1	4	4	3	2	2	3	2						0,6374		
		5	1	2	1	2	4	1	2	2	3	3						0,3432		
		1	1	1	1	1	1	2	1	2	3	1						0,3179		
		2	2	2	2	1	3	2	2	2	2	1						0,5592		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
194	4481125	3	3	1	2	2	4	2	2	1	2	1	3	4481130	5	1	3	0,1529		1
		4	4	2	1	4	3	2	1	3	2	3						0,1867		
		5	3	2	2	2	5	2	2	3	2	1						0,2202		
		1	1	2	2	2	5	1	1	3	3	2						0,426		
		2	2	2	1	2	2	2	2	3	3	3						0,5963		
195	4506685	3	3	1	2	1	4	1	1	1	2	3	3	4506690	5	1	3	0,2302		2
		4	4	1	1	1	2	1	2	2	3	1						0,4315		
		5	3	1	1	2	3	3	1	2	1	3						0,3279		
		1	1	2	2	1	5	3	1	2	1	2						0,3023		
		2	2	1	1	4	4	3	1	3	1	1						0,6906		
196		3	3	1	2	2	1	1	1	1	1	3						0,3991		
	4535804	4	4	1	1	1	3	1	1	1	2	3	4	4535809	5	1	4	0,2367		1
		5	4	2	2	3	5	3	2	3	2	1						0,2993		
		1	1	1	2	4	4	3	1	3	3	1						0,4287		
		2	2	1	2	4	5	2	2	3	2	3						0,4682		
197	4562520	3	3	2	2	3	5	3	1	3	1	3	3	4562523	3	1	3	0,3088		1
		4	4	1	2	4	4	1	1	1	1	3						0,5645		
		5	4	1	1	2	2	3	1	2	3	2						0,4979		
	4589312	1	1	1	1	4	1	1	1	2	1	3	1	4589315	3	1	1	0,1509		1
		2	2	1	1	4	2	1	1	3	3	1						0,1708		
198		3	3	1	2	1	5	2	2	1	2	1						0,5857		
		4	4	2	1	2	3	2	2	3	3	3						0,3254		
		5	3	1	1	3	1	3	1	3	1	3						0,5572		
		1	1	2	2	3	5	1	1	2	2	3						0,5086		
		2	2	2	1	2	3	1	2	2	3	2						0,4236		
199	4614669	3	3	1	2	3	2	2	1	1	3	2	3	4614673	4	1	3	0,1043		1
		4	4	1	1	2	1	3	2	2	2	1						0,2417		
		5	3	1	1	2	5	2	1	1	3	1						0,4483		
	4642520	1	1	1	1	3	1	2	1	1	2	3	1	4642523	3	1	1	0,0407		1
		2	2	2	1	3	3	3	2	1	3	3						0,2283		
200		3	3	1	1	3	1	3	1	3	2	1						0,4038		
		4	4	1	1	4	3	3	2	1	1	1						0,7177		
		5	4	2	1	1	4	1	2	1	1	2						0,4934		
	4670042	1	1	1	1	1	1	2	1	3	1	2	1	4670045	3	1	1	0,1215		1
		2	2	1	2	4	5	2	1	1	2	3						0,1774		
201		3	3	2	1	3	3	2	1	3	2	3						0,4953		
		4	4	2	2	1	2	3	1	1	1	2						0,227		
		5	1	1	1	2	4	2	1	3	1	2						0,4243		
		1	1	2	2	2	1	1	2	3	2	1						0,3508		
	4693076	2	2	2	1	3	4	3	2	3	3	1	2	4693081	5	0	2	0,0391		3
202		3	3	1	2	1	4	1	1	2	3	2						0,2856		
		4	4	1	1	2	3	1	2	3	1	2						0,6453		
		5	2	2	2	3	2	3	1	2	2	3						0,6795		
	4693081	1	1	2	1	2	5	1	2	3	1	3	1	4693099	18	0	1	0,0692		5
		2	2	2	1	3	3	3	1	2	3	1						0,3576		
203		3	3	1	1	1	2	3	2	2	3	2						0,4087		
		4	4	1	1	3	1	1	1	3	1	3						0,3383		
		5	3	2	1	2	3	3	2	2	2	1						0,2814		
		1	1	2	2	3	1	3	2	3	3	2						0,4188		
		2	2	2	1	1	4	1	2	2	3	2						0,5612		
204		3	3	1	1	4	5	2	1	3	2	3						0,6722		
	4693099	4	4	1	2	1	5	2	2	2	1	3	4	4693120	21	1	4	0,094		5
		5	4	1	1	1	3	3	2	2	2	1						0,3956		
		1	1	2	1	4	3	3	2	3	2	2						0,3296		
	4719377	2	2	2	1	2	4	2	1	1	1	1	2	4719380	3	1	2	0,0118		1
205		3	3	2	2	4	3	3	1	3	1	1						0,2238		
		4	4	2	1	2	2	1	2	3	1	2						0,5408		
		5	3	1	1	2	5	3	2	1	2	3						0,3696		
		1	1	2	2	1	4	1	1	3	1	2						0,5679		
		2	2	2	2	3	4	3	2	3	1	3						0,6168		
206	4744132	3	3	1	1	3	4	3	1	2	1	3	3	4744136	4	1	3	0,3856		1
		4	4	1	2	2	1	3	1	1	3	3						0,5614		
		5	1	2	1	4	1	1	1	3	1	2						0,4864		
	4768994	1	1	1	2	1	5	3	1	3	2	1	1	4768998	4	1	1	0,0248		1
		2	2	1	2	1	5	2	1	3	2	3						0,6734		
207		3	3	1	1	4	4	1	1	2	3	1						0,0668		
		4	4	2	2	4	4	1	2	2	3	2						0,3751		
		5	1	1	1	3	2	3	1	3	1	3						0,026		
		1	1	2	2	4	1	3	2	3	2	2						0,3347		
		2	2	2	2	3	4	1	1	1	3	3						0,4607		
208		3	3	1	2	3	5	2	2	2	1	3						0,0696		
		4	4	2	2	4	3	3	2	2	3	1						0,1103		
	4796793	5	3	2	1	4	2	3	1	3	1	2	5	4796796	3	1	3	0,0363		1
		1	1	1	2	2	5	2	2	1	3	1						0,698		
	4825867	2	2	2	1	3	4	3	1	2	3	2	2	4825870	3	1	2	0,0443		1
209		3	3	2	2	3	4	1	1	2	2	2						0,2617		
		4	4	2	1	4	3	2	1	3	1	3						0,6013		
		5	3	2	2	2	1	3	2	1	2	1						0,6886		
		1	1	2	1	2	1	3	1	2	1	2						0,6865		
		2	2	2	2	1	5	1	2	1	1	1						0,1649		
210		3	3	1	2	1	5	3	2	2	1	1						0,5431		
		4	4	2	2	4	1	1	1	2	1	1						0,6581		
	4851882	5	3	1	1	1	3	1	1	3	2	1	5	4851887	5	0	3	0,052		1
	4851887	1	1	1	2	1	1	3	2	1	3	1	1	4851906	19	1	1	0,2456		5
		2	2	1	1	4	4	1	2	2	2	2						0,5977		
211		3	3	1	2	4	5	2	2	3	3	1						0,3439		
		4	4	1	1	3	3	2	1	3	2	2						0,4776		
		5	1	1	2	3	3	2	2	2	2	2						0,6459		
		1	1	1	1	4	1	1	2	1	3	1						0,691		
		2	2	2	1	2	2	1	2	3	3	3						0,5289		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
212		3	3	2	2	3	1	3	1	3	2	3						0,1714	71	
		4	4	1	1	3	1	1	1	1	2	1						0,3263		
	4881325	5	4	1	1	3	5	1	2	3	3	3	5	4881328	3	1	4	0,0241		1
		1	1	1	2	2	1	3	2	1	3	1						0,5756		
		2	2	2	2	3	2	2	1	3	3	1						0,356		
213		3	3	1	1	1	5	1	2	2	3	2						0,127		
	4905000	4	4	2	1	2	5	1	2	2	3	2	4	4905004	4	1	4	0,0744		2
		5	3	2	2	1	3	2	1	1	3	3						0,2714		
		1	1	2	1	2	1	1	2	1	3	1						0,4485		
		2	2	1	2	4	3	3	1	2	2	3						0,2661		
214		3	3	2	2	1	2	3	1	1	1	1						0,1548		
		4	4	1	1	1	4	3	2	2	3	1						0,5456		
	4934151	5	2	1	1	4	5	3	1	3	3	3	5	4934155	4	1	2	0,1526		4
		1	1	2	2	3	1	2	1	2	2	2						0,3364		
		2	2	2	1	3	3	3	2	3	2	3						0,5198		
215		3	3	1	2	4	5	3	1	1	3	3						0,288		
	4961758	4	4	2	2	3	3	1	1	3	3	2	4	4961763	5	0	4	0,253		1
		5	4	2	2	2	2	2	2	3	3	2						0,451		
		1	1	2	1	4	5	2	2	1	3	1						0,5706		
		2	2	1	1	4	2	2	1	3	2	1						0,6766		
216	4961763	3	3	2	2	1	2	1	1	1	3	1	3	4961786	23	0	3	0,3351		5
		4	4	1	2	2	2	2	2	2	2	3						0,5417		
		5	4	2	1	3	2	2	2	3	1	3						0,5602		
		1	1	1	1	2	3	2	1	1	3	3						0,5138		
		2	2	2	1	1	2	1	1	2	1	2						0,3615		
217		3	3	1	2	3	2	2	2	3	2	2						0,698		
		4	4	2	1	3	5	3	2	3	2	1						0,4172		
	4961786	5	1	1	1	4	3	1	2	3	2	3	5	4961801	15	0	1	0,0912		5
		1	1	1	1	3	3	3	1	1	3	2						0,2526		
	4961801	2	2	2	1	2	5	1	1	3	1	2	2	4961824	23	0	2	0,2071		5
218		3	3	2	2	4	2	3	2	3	2	1						0,4981		
		4	4	1	2	1	3	2	2	2	1	3						0,6603		
		5	2	2	2	4	4	3	2	2	3	3						0,7108		
		1	1	2	2	4	4	1	1	3	3	1						0,6757		
		2	2	1	1	4	5	2	2	1	2	1						0,2793		
219		3	3	2	1	4	2	3	2	3	1	1						0,3613		
	4961824	4	4	2	2	2	1	1	1	1	1	1	4	4961835	11	0	4	0,1036		5
		5	4	2	1	1	3	1	2	2	3	3						0,2246		
		1	1	1	1	4	5	1	1	1	3	2						0,387		
		2	2	1	2	3	1	3	2	2	2	2						0,1452		
220		3	3	2	1	2	1	3	2	3	2	1						0,3962		
	4961835	4	4	2	1	1	1	1	1	3	3	2	4	4961856	21	1	4	0,0089		6
		5	3	2	1	3	1	2	1	1	3	1						0,1501		
		1	1	2	1	2	4	1	2	2	2	2						0,4445		
		2	2	1	1	1	4	1	1	2	2	1						0,2812		
221		3	3	2	2	4	3	3	2	1	2	1						0,3987		
		4	4	1	1	2	4	3	1	3	1	2						0,452		
	4987842	5	1	1	1	4	4	3	1	1	1	2	5	4987847	5	1	1	0,0892		4
		1	1	2	1	2	4	1	2	1	1	1						0,2698		
	5014878	2	2	2	1	1	1	1	1	1	2	2	2	5014882	4	0	2	0,1165		1
222		3	3	2	1	4	3	2	1	3	2	1						0,5269		
		4	4	2	1	2	5	2	2	1	2	2						0,1933		
		5	3	2	1	1	5	1	2	2	3	2						0,2361		
		1	1	2	2	1	1	3	1	3	1	3						0,6332		
		2	2	1	2	3	5	1	2	1	2	3						0,3079		
223		3	3	1	1	2	4	3	1	3	2	2						0,2623		
	5014882	4	4	2	2	4	5	1	2	2	1	2	4	5014897	15	1	4	0,2465		5
		5	4	2	2	2	4	3	2	1	2	2						0,3072		
		1	1	2	2	3	1	2	2	2	2	2						0,5637		
		2	2	2	1	2	5	2	1	1	1	3						0,4493		
224	5042418	3	3	1	1	3	3	3	1	2	3	2	3	5042422	4	1	3	0,3209		1
		4	4	1	1	1	5	3	2	1	3	2						0,4388		
		5	3	1	1	2	3	1	1	3	2	1						0,352		
		1	1	2	1	1	4	3	1	1	2	3						0,3696		
		2	2	1	1	3	2	3	2	2	1	3						0,1889		
225	5071369	3	3	2	2	3	5	2	1	2	2	2	3	5071372	3	1	3	0,1197		1
		4	4	2	2	3	3	2	1	1	2	2						0,4669		
		5	3	1	2	4	3	1	2	2	2	3						0,3345		
		1	1	2	1	1	3	3	2	2	2	2						0,4675		
		2	2	2	2	1	3	1	1	3	2	2						0,5847		
226	5099557	3	3	2	1	2	2	2	2	1	3	3	3	5099560	3	0	3	0,0548		1
		4	4	1	1	4	3	2	1	3	1	1						0,429		
		5	2	2	1	4	3	1	2	3	2	1						0,6485		
		1	1	1	1	2	1	3	1	1	2	2						0,5608		
		2	2	2	1	1	2	2	1	3	2	3						0,4465		
227		3	3	1	1	4	5	1	1	2	3	2						0,6198		
		4	4	2	1	2	4	1	1	1	3	3						0,1247		
	5099560	5	4	1	2	4	3	3	2	2	2	2	5	5099576	16	1	4	0,0211		5
		1	1	2	2	3	5	2	2	1	1	2						0,1852		
		2	2	1	1	1	3	3	2	2	2	3						0,1181		
228		3	3	2	2	4	3	3	2	3	1	2						0,2931		
	5129122	4	4	2	1	4	4	1	1	2	1	2	4	5129126	4	1	4	0,1172		1
		5	1	2	2	4	4	3	1	3	2	3						0,5327		
		1	1	2	2	4	3	3	2	1	2	1						0,2875		
		2	2	1	2	4	5	1	1	3	1	1						0,6097		
229		3	3	1	2	3	4	1	1	2	3	2						0,5252		
	5158785	4	4	2	2	4	2	3	1	3	2	3	4	5158789	4	1	4	0,1163		1
		5	2	2	2	2	3	2	2	1	3	1						0,2084		
		1	1	1	2	3	3	2	1	3	1	3						0,3206		
		2	2	1	2	2	5	1	2	2	2	3						0,3054		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
230		3	3	2	1	2	3	1	1	2	1	2						0,3391		
	5186134	4	4	1	2	4	4	2	2	2	1	1	4	5186138	4	1	4	0,2025		1
		5	3	2	1	3	2	1	1	1	2	2						0,6764		
	5211748	1	1	1	1	3	3	3	1	3	3	1	1	5211753	5	1	1	0,0977		1
		2	2	2	2	3	1	2	1	3	1	3						0,6229		
231		3	3	2	2	4	3	3	1	1	1	2						0,6096		
		4	4	2	1	3	5	2	1	1	3	3						0,2475		
		5	4	1	1	2	4	3	1	1	3	1						0,4489		
	5234990	1	1	1	2	4	3	2	1	2	1	3	1	5234994	4	1	1	0,2613		1
		2	2	2	1	1	4	3	1	1	3	2						0,5079		
232		3	3	2	2	3	2	1	2	2	3	1						0,4096		
		4	4	2	1	2	2	1	1	1	2	3						0,5719		
		5	4	2	1	2	5	3	2	1	2	1						0,6787		
		1	1	1	1	1	5	1	2	2	3	3						0,7195		
		2	2	2	1	1	4	3	1	2	2	2						0,1972		
233		3	3	1	2	1	4	3	1	1	1	1						0,4508		
	5262548	4	4	2	2	1	2	3	1	2	3	1	4	5262551	3	1	4	0,0663		1
		5	1	2	1	1	3	3	2	1	3	1						0,5227		
		1	1	2	1	3	5	2	1	2	1	1						0,0418		
		2	2	2	2	2	2	3	1	3	2	3						0,1921		
234	5292307	3	3	1	2	2	3	3	1	1	2	3	3	5292311	4	1	3	0,0378		2
		4	4	2	2	1	1	2	2	3	3	2						0,4822		
		5	4	1	1	1	3	3	1	2	3	2						0,3841		
		1	1	2	2	1	1	3	2	1	3	2						0,1357		
	5315997	2	2	1	1	4	3	3	1	1	3	3	2	5316001	4	1	2	0,046		1
235		3	3	1	1	2	4	3	2	2	3	3						0,4651		
		4	4	2	1	1	4	1	2	1	2	1						0,1933		
		5	4	1	2	1	5	3	2	2	1	2						0,7075		
		1	1	2	2	4	1	1	1	1	1	2						0,1879		
		2	2	1	1	3	3	2	1	1	3	1						0,6901		
236	5340790	3	3	2	1	2	2	3	1	2	3	2	3	5340794	4	1	3	0,1083		1
		4	4	1	2	3	4	3	1	3	1	3						0,4026		
		5	4	2	2	2	5	3	1	3	1	2						0,2261		
		1	1	1	1	2	4	2	2	1	3	3						0,6642		
		2	2	1	2	2	3	2	1	1	2	2						0,1301		
237	5364975	3	3	1	1	1	2	2	1	1	2	2	3	5364978	3	1	3	0,0509		1
		4	4	1	1	3	1	3	2	1	2	3						0,4229		
		5	4	2	1	2	4	1	2	3	2	3						0,6748		
		1	1	2	2	2	5	3	1	3	1	3						0,6337		
		2	2	1	2	2	4	1	2	1	3	2						0,2977		
238	5394155	3	3	1	2	3	3	3	2	3	2	2	3	5394160	5	1	3	0,1071		1
		4	4	2	2	3	2	3	2	3	3	3						0,4233		
		5	1	1	1	2	1	3	1	3	2	1						0,5641		
		1	1	1	2	2	3	1	1	2	3	3						0,2031		
	5418714	2	2	2	2	2	5	3	2	3	3	3	2	5418719	5	1	2	0,0034		1
239		3	3	1	1	4	5	3	2	2	2	3						0,5553		
		4	4	2	2	4	4	2	1	3	2	2						0,2185		
		5	3	2	2	3	3	1	2	1	1	2						0,5107		
		1	1	2	1	1	5	1	1	2	1	3						0,5947		
	5447046	2	2	2	1	2	4	2	1	2	2	1	2	5447051	5	1	2	0,0467		1
240		3	3	2	1	3	3	3	2	3	1	2						0,677		
		4	4	1	2	2	5	2	2	3	2	2						0,0487		
		5	3	1	2	3	4	3	1	2	3	3						0,2748		
		1	1	1	1	2	5	2	1	3	3	1						0,1762		
		2	2	2	1	3	2	1	2	2	1	1						0,6233		
241	5470520	3	3	1	1	3	2	3	1	2	3	1	3	5470525	5	1	3	0,1306		1
		4	4	1	2	3	1	2	1	1	3	3						0,6701		
		5	4	2	1	2	2	1	2	3	2	2						0,2002		
		1	1	2	2	1	5	2	1	3	1	2						0,4006		
		2	2	1	1	4	1	1	2	3	3	1						0,416		
242		3	3	2	2	1	5	3	2	2	1	1						0,364		
		4	4	2	2	3	5	3	2	3	2	1						0,1301		
	5497479	5	4	2	1	1	3	1	1	1	1	2	5	5497484	5	1	4	0,0526		1
		1	1	2	2	2	4	2	1	3	2	2						0,5256		
		2	2	1	2	4	3	3	2	2	1	3						0,2761		
243		3	3	2	2	2	1	3	2	1	1	3						0,6991		
		4	4	1	1	4	3	2	2	1	1	1						0,1775		
	5523820	5	4	1	1	1	5	2	2	1	1	2	5	5523824	4	1	4	0,0734		1
		1	1	2	2	1	5	1	2	2	3	2						0,4997		
		2	2	1	1	3	1	3	1	1	2	3						0,378		
244	5552149	3	3	1	1	1	1	2	1	1	2	2	3	5552152	3	0	3	0,2669		1
		4	4	1	2	3	4	3	1	1	2	1						0,5024		
		5	4	1	2	4	2	3	2	3	2	3						0,4933		
	5552152	1	1	1	2	1	5	1	2	2	1	1	1	5552170	18	1	1	0,0699		5
		2	2	1	2	1	5	1	2	2	1	2						0,6102		
245		3	3	2	2	4	4	1	1	3	1	2						0,5353		
		4	4	1	2	2	1	1	2	3	1	1						0,3996		
		5	1	2	1	3	2	3	1	3	2	2						0,375		
		1	1	1	2	3	4	2	1	1	1	2						0,1532		
		2	2	2	2	4	1	3	1	3	1	2						0,2562		
246		3	3	2	1	4	3	1	1	1	3	2						0,6365		
	5576639	4	4	2	2	2	3	1	2	3	2	2	4	5576642	3	1	4	0,0974		1
		5	1	1	2	2	1	3	1	1	2	2						0,3811		
		1	1	2	1	3	5	2	1	1	3	3						0,3703		
		2	2	2	1	2	1	3	2	3	3	1						0,3715		
247		3	3	2	1	3	1	2	1	3	3	2						0,3504		
	5599307	4	4	2	2	1	4	3	2	2	2	3	4	5599310	3	1	4	0,1853		4
		5	3	2	1	2	2	3	1	1	2	1						0,4121		
	5628838	1	1	2	1	3	5	3	1	3	1	3	1	5628843	5	1	1	0,1603		1
		2	2	2	1	3	1	1	2	2	2	2						0,5049		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
248		3	3	2	1	1	4	2	2	2	3	3						0,4666		
		4	4	2	2	2	1	1	2	3	1	2						0,5742		
		5	3	1	1	1	1	2	2	2	3	2						0,5306		
		1	1	2	1	3	1	3	1	1	1	3						0,3787		
		2	2	2	1	1	3	3	2	3	2	3						0,2712		
249	5653852	3	3	2	2	1	4	1	2	2	3	3	3	5653857	5	1	3	0,0016		2
		4	4	1	2	4	1	1	2	2	2	3						0,0382		
		5	4	2	2	4	2	1	1	1	1	1						0,6696		
		1	1	2	2	2	2	1	2	2	1	2						0,6565		
		2	2	2	2	4	3	1	2	3	1	1						0,4261		
250		3	3	1	1	4	1	1	2	2	2	2						0,672		
		4	4	2	2	2	1	1	2	3	2	3						0,3624		
	5677434	5	4	2	1	4	4	2	2	1	2	2	5	5677438	4	1	4	0,0103		1
	5705311	1	1	1	1	3	2	2	2	1	1	3	1	5705314	3	1	1	2,19E-04		1
		2	2	2	2	1	2	2	2	3	2	1						0,0692		
251		3	3	2	1	3	4	2	1	2	2	3						0,6405		
		4	4	1	2	1	2	3	1	3	2	1						0,3506		
		5	1	2	2	2	4	2	2	3	1	2						0,3969		
		1	1	1	1	4	4	1	1	2	3	1						0,3845		
	5733831	2	2	1	2	3	3	1	1	1	3	1	2	5733836	5	1	2	0,0722		1
252		3	3	2	1	2	3	1	2	2	1	2						0,1144		
		4	4	2	2	3	1	1	2	3	3	2						0,4704		
		5	1	1	2	2	1	3	1	2	3	1						0,6226		
		1	1	2	1	2	4	2	1	3	1	1						0,1273		
	5761455	2	2	2	2	2	1	1	2	3	2	3	2	5761459	4	1	2	0,1061		1
253		3	3	2	2	2	3	3	1	2	2	3						0,6246		
		4	4	1	2	3	2	2	1	1	2	1						0,6735		
		5	4	1	1	3	2	2	2	3	2	2						0,4743		
		1	1	1	1	1	2	2	2	2	2	3						0,2839		
		2	2	2	1	2	1	3	1	1	1	1						0,2156		
254		3	3	1	1	4	1	2	1	1	3	2						0,3244		
	5790410	4	4	1	1	4	4	1	1	1	3	2	4	5790414	4	1	4	0,0475		1
		5	1	1	2	1	1	3	1	2	3	1						0,5069		
		1	1	1	1	4	5	1	2	2	2	1						0,4606		
		2	2	2	2	1	3	2	2	2	3	2						0,6193		
255		3	3	2	1	2	1	3	2	1	3	1						0,2134		
	5819911	4	4	2	1	4	2	3	1	2	2	3	4	5819915	4	1	4	0,0091		1
		5	3	1	2	1	5	1	1	1	2	2						0,4524		
		1	1	1	1	2	2	3	2	3	3	3						0,7056		
		2	2	1	1	4	3	3	1	3	1	1						0,4738		
256		3	3	2	2	4	1	3	1	3	2	2						0,3052		
	5843450	4	4	1	2	1	5	2	2	1	1	3	4	5843454	4	1	4	0,1716		1
		5	3	2	2	2	4	1	2	2	1	1						0,1916		
	5867342	1	1	2	1	2	2	2	2	2	1	1	1	5867346	4	1	1	0,0999		1
		2	2	1	2	2	2	2	1	2	1	3						0,6865		
257		3	3	2	1	2	2	2	1	3	1	1						0,5561		
		4	4	1	1	3	2	3	2	2	3	2						0,3478		
		5	1	1	2	2	3	1	1	2	2	1						0,1919		
		1	1	2	2	1	2	2	1	3	3	1						0,1411		
	5894166	2	2	1	1	1	1	3	2	1	3	1	2	5894171	5	1	2	0,0493		3
258		3	3	1	1	3	5	1	1	3	2	2						0,316		
		4	4	1	1	1	1	3	2	1	2	1						0,1147		
		5	1	2	2	2	4	1	2	2	1	2						0,5236		
		1	1	2	1	4	2	3	1	1	2	2						0,456		
		2	2	1	2	2	3	1	1	1	2	2						0,5726		
259		3	3	1	2	2	5	1	2	3	3	2						0,2699		
	5920576	4	4	1	2	1	2	1	1	1	2	1	4	5920579	3	1	4	0,0241		1
		5	2	2	2	3	5	1	2	2	2	3						0,1717		
		1	1	1	2	2	3	2	1	2	1	1						0,3718		
	5948118	2	2	1	2	4	4	2	1	1	1	1	2	5948122	4	1	2	0,0147		1
260		3	3	1	1	3	5	3	2	3	2	3						0,2782		
		4	4	1	2	4	5	3	2	1	3	1						0,3538		
		5	4	2	2	4	1	3	2	2	1	1						0,6206		
		1	1	2	1	4	3	3	1	3	2	3						0,4728		
		2	2	1	1	4	1	1	2	1	2	3						0,5179		
261		3	3	1	1	1	5	1	2	3	2	2						0,4464		
		4	4	1	2	2	5	1	1	3	1	3						0,5304		
	5973935	5	2	1	1	4	4	1	1	2	2	1	5	5973940	5	1	2	0,0376		1
		1	1	2	1	1	2	1	1	1	3	2						0,4311		
	6001512	2	2	1	2	1	1	2	1	2	3	2	2	6001515	3	1	2	0,0706		1
262		3	3	1	1	4	1	1	1	2	3	1						0,3073		
		4	4	1	2	3	5	1	1	3	1	3						0,0734		
		5	2	2	1	1	5	2	1	2	1	2						0,2681		
		1	1	1	1	3	1	2	2	2	1	2						0,192		
	6024816	2	2	2	2	4	3	1	2	1	3	2	2	6024820	4	1	2	0,0697		1
263		3	3	1	2	3	3	1	1	1	3	2						0,5756		
		4	4	2	2	3	5	1	2	2	2	3						0,6875		
		5	2	2	2	1	1	2	2	1	1	1						0,4617		
		1	1	1	2	2	5	2	2	1	1	2						0,3255		
		2	2	2	1	2	3	2	1	2	1	3						0,304		
264		3	3	1	2	4	5	2	1	1	3	1						0,305		
	6053581	4	4	1	2	4	3	1	2	2	2	1	4	6053586	5	1	4	0,0549		1
		5	1	1	1	2	4	2	2	3	2	3						0,0889		
		1	1	2	2	1	5	2	2	3	2	2						0,6111		
	6082478	2	2	1	1	4	5	2	1	2	1	1	2	6082481	3	1	2	0,104		1
265		3	3	1	2	4	3	3	2	3	2	1						0,1477		
		4	4	2	2	2	5	1	1	2	1	1						0,5782		
		5	3	2	1	2	1	1	2	3	3	2						0,1144		
		1	1	1	1	4	4	1	1	3	2	3						0,557		
	6110162	2	2	2	2	4	3	3	1	2	2	1	2	6110167	5	1	2	0,2209		1

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
266		3	3	1	1	4	5	3	2	2	1	3						0,4285		
		4	4	1	1	1	1	1	2	2	3	1						0,2242		
		5	4	2	2	1	1	2	2	3	2	1						0,4394		
		1	1	1	1	1	2	2	1	1	3	3						0,6963		
	6136008	2	2	2	2	2	3	3	1	3	1	3	2	6136013	5	1	2	0,0426		1
267		3	3	1	2	2	5	3	1	3	3	2						0,4061		
		4	4	1	2	2	1	3	1	2	1	3						0,263		
		5	1	1	1	2	5	1	1	3	2	2						0,358		
		1	1	1	2	3	1	2	2	3	1	2						0,4207		
		2	2	2	2	4	1	2	1	3	1	3						0,4388		
268		3	3	1	2	2	3	3	1	3	1	3						0,3874		
		4	4	2	1	4	3	1	1	3	3	2						0,4275		
	6160410	5	3	1	1	1	4	1	1	1	2	2	5	6160413	3	1	3	0,2345		3
		1	1	2	2	4	3	1	2	2	3	2						0,2519		
	6186879	2	2	1	2	3	3	3	2	1	3	3	2	6186883	4	0	2	0,0404		1
269		3	3	2	2	2	5	1	2	2	1	1						0,6716		
		4	4	1	2	4	4	2	1	3	2	2						0,4925		
		5	4	1	2	2	2	1	1	1	2	2						0,4627		
		1	1	1	2	2	4	3	2	3	2	1						0,7039		
		2	2	1	1	2	1	2	2	3	3	3						0,589		
270		3	3	1	1	4	4	3	2	2	1	3						0,6516		
	6186883	4	4	2	2	3	3	3	1	2	3	2	4	6186903	20	1	4	0,2263		5
		5	3	1	1	3	3	2	1	3	2	3						0,3679		
		1	1	2	2	1	3	3	2	2	3	2						0,5003		
	6209994	2	2	2	2	1	2	1	1	3	2	2	2	6209999	5	1	2	0,0075		1
271		3	3	1	1	4	4	1	2	1	3	3						0,5917		
		4	4	2	2	2	4	2	1	3	1	1						0,1241		
		5	2	1	1	2	3	1	2	2	1	1						0,3477		
	6238827	1	1	2	2	2	4	1	2	3	3	1	1	6238831	4	1	1	0,0671		1
		2	2	1	2	3	4	3	2	2	2	1						0,1764		
272		3	3	2	1	2	4	1	1	3	3	1						0,7167		
		4	4	2	2	4	3	2	2	3	3	1						0,0756		
		5	3	2	1	3	5	1	1	2	3	1						0,153		
		1	1	2	1	2	1	2	2	2	1	1						0,5564		
		2	2	2	2	1	2	1	2	1	2	1						0,6533		
273	6262347	3	3	2	1	1	2	3	1	2	3	3	3	6262350	3	1	3	0,2907		1
		4	4	1	2	1	1	3	2	3	3	1						0,4692		
		5	4	1	1	4	2	1	1	1	3	2						0,361		
		1	1	1	2	3	3	3	2	1	1	3						0,2639		
	6288674	2	2	2	1	1	4	2	1	1	1	3	2	6288677	3	1	2	0,0789		1
274		3	3	2	1	1	5	2	2	3	1	3						0,5844		
		4	4	1	2	3	5	3	2	1	3	1						0,6186		
		5	4	2	1	3	4	1	2	3	2	3						0,5492		
	6312769	1	1	1	1	1	2	2	2	2	3	1	1	6312772	3	1	1	0,3179		1
		2	2	2	2	4	4	1	1	1	1	3						0,6755		
275		3	3	1	2	4	3	1	1	1	2	3						0,6021		
		4	4	2	1	2	4	3	2	1	1	1						0,4474		
		5	3	1	1	1	5	3	1	3	3	1						0,4817		
		1	1	1	1	4	1	1	1	2	3	1						0,5452		
		2	2	1	2	4	5	2	1	3	1	1						0,6657		
276		3	3	1	1	4	3	1	1	1	1	1						0,7036		
		4	4	2	1	2	3	2	1	2	1	1						0,6957		
	6340120	5	3	2	1	1	5	1	1	1	2	1	5	6340123	3	1	3	0,1807		1
		1	1	1	1	2	5	1	1	1	3	2						0,1828		
	6367437	2	2	2	1	1	3	3	2	1	1	1	2	6367440	3	0	2	0,0255		1
277		3	3	1	2	1	4	1	1	2	3	1						0,3775		
		4	4	2	2	4	2	1	2	1	1	2						0,3106		
		5	4	2	1	2	1	2	1	3	3	1						0,3874		
		1	1	1	1	3	1	3	2	2	2	2						0,3584		
	6367440	2	2	1	1	1	4	1	2	3	3	1	2	6367455	15	1	2	0,0392		5
278		3	3	2	1	4	3	1	1	1	1	3						0,3008		
		4	4	2	1	3	4	3	2	2	1	1						0,0831		
		5	1	1	2	4	1	2	1	1	2	2						0,1117		
		1	1	1	1	4	1	2	2	2	3	2						0,6538		
		2	2	1	1	1	1	2	2	1	2	1						0,5666		
279		3	3	1	2	4	4	1	2	3	2	1						0,2849		
		4	4	2	2	3	5	2	1	1	2	3						0,5562		
	6393921	5	1	2	2	4	2	3	1	2	3	2	5	6393925	4	0	1	0,1653		1
		1	1	2	2	1	2	2	2	1	3	2						0,5137		
		2	2	2	2	4	4	2	2	2	1	3						0,4		
280	6393925	3	3	2	1	3	2	1	1	3	2	2	3	6393948	23	1	3	0,0687		5
		4	4	2	2	1	1	3	1	3	2	3						0,0844		
		5	2	1	2	3	2	1	2	3	3	2						0,287		
		1	1	1	2	2	2	3	2	2	3	2						0,5493		
		2	2	1	2	4	5	2	2	3	1	1						0,4904		
281	6419549	3	3	2	2	2	3	1	1	2	2	1	3	6419553	4	1	3	0,0801		1
		4	4	1	2	4	1	1	2	2	1	2						0,3749		
		5	2	1	1	4	4	3	1	2	3	2						0,3327		
		1	1	1	1	1	1	3	2	3	2	3						0,4028		
		2	2	2	1	2	5	2	1	2	3	3						0,1796		
282		3	3	1	2	2	4	3	2	1	1	1						0,4676		
		4	4	2	1	2	2	1	1	3	2	2						0,1895		
	6446780	5	2	1	1	2	5	1	2	3	2	3	5	6446785	5	1	2	0,1337		2
		1	1	2	1	2	5	3	1	2	2	3						0,6336		
		2	2	2	1	4	1	1	2	2	3	1						0,702		
283		3	3	1	1	2	3	1	1	2	3	3						0,6361		
		4	4	1	1	2	4	3	1	1	3	2						0,4701		
	6475151	5	3	1	2	2	5	1	2	3	1	2	5	6475156	5	1	3	0,4519		1
		1	1	1	2	2	1	1	2	3	1	3						0,2599		
		2	2	2	2	4	5	1	1	1	3	2						0,635		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
284		3	3	1	1	4	5	2	1	2	1	1						0,0997		
		4	4	1	2	4	5	1	1	3	1	2						0,4804		
	6503411	5	1	2	1	4	5	3	1	1	2	3	5	6503415	4	1	1	0,0917		1
		1	1	2	1	2	2	3	2	1	1	2						0,6175		
		2	2	2	1	2	5	3	1	3	2	2						0,2726		
285		3	3	2	1	4	4	3	2	3	1	2						0,0679		
	6527248	4	4	2	2	3	4	3	2	2	3	2	4	6527252	4	1	4	0,0263		3
		5	1	2	1	3	3	1	2	2	3	3						0,3532		
		1	1	1	1	1	4	1	1	3	1	3						0,6363		
		2	2	2	2	4	2	3	2	1	2	3						0,1249		
286		3	3	1	1	4	3	1	2	2	1	3						0,3301		
		4	4	2	2	3	3	2	1	2	1	1						0,1144		
	6549895	5	1	1	1	2	2	3	1	1	1	2	5	6549898	3	1	1	0,0878		1
		1	1	2	1	1	4	1	1	2	2	3						0,4275		
		2	2	2	1	3	5	1	1	3	2	1						0,4504		
287		3	3	2	1	2	5	3	2	3	1	2						0,5817		
	6573632	4	4	1	2	4	5	2	1	3	2	1	4	6573636	4	1	4	0,0201		1
		5	1	1	2	2	5	1	2	3	1	2						0,6667		
	6597383	1	1	2	2	2	5	3	1	1	2	2	1	6597387	4	1	1	0,19		1
		2	2	1	1	3	3	3	2	3	2	2						0,5967		
288		3	3	2	1	2	2	1	2	3	1	3						0,4322		
		4	4	1	2	3	4	3	2	2	2	1						0,2746		
		5	4	2	1	2	5	1	2	2	1	1						0,6248		
	6624153	1	1	2	1	1	5	2	1	1	2	2	1	6624157	4	1	1	0,2673		1
		2	2	1	1	1	4	2	2	3	2	1						0,4462		
289		3	3	1	2	1	5	2	1	1	2	2						0,6774		
		4	4	1	1	2	2	1	1	2	1	1						0,6328		
		5	1	1	1	2	3	1	2	2	2	2						0,4926		
		1	1	1	1	3	5	1	2	1	2	1						0,4181		
		2	2	1	1	4	1	3	2	2	1	2						0,2613		
290		3	3	1	1	1	2	3	1	2	1	1						0,6719		
	6649165	4	4	1	2	3	4	3	1	3	1	1	4	6649170	5	1	4	0,0146		3
		5	3	2	2	1	4	2	2	2	3	2						0,435		
		1	1	2	1	3	4	2	2	2	1	1						0,671		
	6678971	2	2	1	1	1	3	2	2	3	2	1	2	6678974	3	1	2	0,0183		1
291		3	3	2	1	4	2	2	1	1	3	3						0,4699		
		4	4	2	1	4	3	3	2	3	3	2						0,6338		
		5	2	2	2	1	3	3	2	1	2	2						0,3141		
		1	1	2	1	4	4	1	1	1	1	3						0,184		
		2	2	1	2	2	1	2	2	1	2	1						0,5049		
292		3	3	2	2	4	1	1	1	2	3	1						0,2111		
	6705646	4	4	1	1	4	1	3	2	2	2	3	4	6705650	4	1	4	0,1262		1
		5	1	2	1	3	5	2	1	1	1	1						0,4203		
		1	1	1	2	4	4	1	1	1	1	2						0,1673		
		2	2	2	2	2	1	3	2	2	1	3						0,6869		
293		3	3	2	2	4	5	3	1	3	1	2						0,7199		
		4	4	2	1	4	2	2	2	3	3	1						0,0195		
	6731428	5	2	2	2	1	2	3	2	3	3	1	5	6731433	5	1	2	0,0132		1
	6760533	1	1	1	2	4	3	1	1	2	1	3	1	6760538	5	1	1	0,1752		1
		2	2	1	2	2	3	1	1	1	3	3						0,3513		
294		3	3	1	1	1	2	2	2	3	2	1						0,6884		
		4	4	1	2	4	1	2	1	1	3	3						0,3179		
		5	2	2	1	1	3	3	1	3	2	3						0,6805		
		1	1	2	2	2	5	1	2	2	1	1						0,4473		
		2	2	1	2	3	2	1	1	3	1	2						0,2314		
295	6787713	3	3	2	1	2	4	2	1	2	2	3	3	6787716	3	1	3	0,0817		1
		4	4	1	2	4	4	2	2	3	1	3						0,2148		
		5	2	1	2	1	2	2	1	3	3	2						0,6296		
		1	1	1	1	1	3	1	1	1	3	2						0,5266		
		2	2	2	2	4	4	2	1	1	3	3						0,5989		
296		3	3	1	1	2	5	2	2	1	2	2						0,4081		
	6812599	4	4	2	1	2	2	3	1	2	3	2	4	6812602	3	1	4	0,1954		4
		5	2	2	1	1	1	2	2	1	2	1						0,4165		
		1	1	2	1	1	2	1	1	1	1	1						0,5126		
		2	2	1	2	2	1	2	2	1	1	2						0,537		
297	6840879	3	3	2	2	3	3	3	2	2	2	2	3	6840884	5	1	3	0,1828		1
		4	4	2	2	4	1	3	1	2	2	2						0,227		
		5	4	1	2	2	3	1	2	3	2	3						0,5872		
		1	1	1	1	2	2	1	2	3	3	3						0,4055		
		2	2	2	1	3	3	3	1	2	2	2						0,0199		
298		3	3	2	2	3	5	2	1	2	2	1						0,6158		
		4	4	1	2	4	3	3	1	1	2	3						0,1992		
	6866427	5	2	1	2	4	4	3	2	3	1	3	5	6866431	4	1	2	0,0068		1
		1	1	2	2	3	3	3	1	1	1	1						0,3288		
		2	2	2	2	4	2	3	2	2	3	2						0,4845		
299		3	3	2	2	2	1	2	2	2	1	2						0,0941		
	6895511	4	4	2	1	3	4	1	2	2	1	1	4	6895515	4	1	4	0,0373		1
		5	2	1	2	3	4	1	2	3	3	3						0,3822		
		1	1	2	1	2	5	3	1	2	2	2						0,5209		
		2	2	1	1	3	3	2	1	1	3	1						0,6714		
300	6923146	3	3	2	1	2	4	3	2	3	2	1	3	6923151	5	1	3	0,4562		2
		4	4	2	1	2	5	2	1	2	1	1						0,6156		
		5	3	1	1	3	3	3	1	3	2	2						0,5938		
		1	1	1	1	1	2	2	2	3	2	2						0,2415		
		2	2	2	1	3	2	3	1	3	1	3						0,6207		
301		3	3	2	1	1	1	1	1	3	3	1						0,3714		
	6951187	4	4	2	2	3	2	3	1	3	1	1	4	6951190	3	0	4	0,2196		3
		5	4	1	2	3	4	2	1	3	2	1						0,4927		
	6951190	1	1	1	2	2	1	3	2	1	3	1	1	6951209	19	1	1	0,2092		5
		2	2	2	1	2	2	3	1	2	3	3						0,6673		

Продовження таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
302		3	3	1	1	2	3	2	2	3	2	1						0,3916		
		4	4	1	1	3	4	2	1	2	3	2						0,3174		
		5	2	1	1	4	2	2	1	3	2	3						0,6316		
		1	1	2	1	1	2	3	2	2	3	2						0,42		
		2	2	1	2	3	2	1	2	2	1	1						0,3101		
303		3	3	1	2	1	5	3	1	1	1	3						0,3526		
		4	4	2	1	2	1	1	1	3	3	1						0,395		
	6978976	5	1	2	2	3	4	2	2	2	2	1	5	6978980	4	0	1	0,1755		1
	6978980	1	1	2	2	1	1	1	1	3	1	2	1	6978995	15	1	1	0,1005		5
		2	2	2	2	4	4	1	1	2	3	2						0,4137		
304		3	3	1	2	4	5	2	2	2	3	3						0,6587		
		4	4	1	1	4	3	3	1	2	1	3						0,6966		
		5	4	2	1	2	1	3	1	2	3	1						0,1694		
		1	1	2	2	1	1	2	2	1	2	2						0,2719		
		2	2	1	1	4	4	2	2	1	3	3						0,2502		
305		3	3	2	1	4	3	2	2	1	3	2						0,2734		
	7007312	4	4	1	2	1	5	2	1	3	2	3	4	7007316	4	1	4	0,1061		1
		5	4	1	2	4	4	3	1	2	3	1						0,5547		
	7034478	1	1	2	2	2	5	2	1	3	2	2	1	7034483	5	0	1	0,0187		1
		2	2	2	1	3	3	1	1	1	1	2						0,0855		
306		3	3	1	1	1	3	3	1	3	1	2						0,2182		
		4	4	2	2	2	3	3	2	2	1	2						0,7177		
		5	4	1	2	3	2	2	1	2	3	2						0,3188		
		1	1	2	1	2	1	1	1	2	2	1						0,3682		
		2	2	1	2	4	1	1	2	1	2	3						0,2396		
307	7034483	3	3	2	1	3	2	3	2	3	2	3	3	7034505	22	1	3	0,0365		5
		4	4	2	2	3	2	2	1	2	2	1						0,3307		
		5	3	1	1	3	2	1	1	1	2	3						0,0541		
		1	1	2	2	4	2	2	2	2	2	2						0,2081		
		2	2	1	2	3	2	1	1	2	2	1						0,3856		
308		3	3	1	1	1	4	2	1	1	2	1						0,1791		
	7064085	4	4	1	2	2	1	3	1	3	2	1	4	7064088	3	1	4	0,0611		1
		5	2	2	2	3	2	2	2	3	2	1						0,6907		
	7093944	1	1	2	2	1	5	1	2	3	1	1	1	7093949	5	1	1	0,0668		3
		2	2	2	1	4	1	2	2	2	3	3						0,2346		
309		3	3	2	2	3	5	3	2	3	1	3						0,3808		
		4	4	2	2	4	3	1	2	1	1	3						0,3843		
		5	1	1	2	3	3	1	2	3	2	3						0,4244		
	7123646	1	1	1	2	1	5	2	2	1	2	2	1	7123649	3	1	1	0,1586		1
		2	2	2	1	2	4	3	2	1	3	1						0,569		
310		3	3	2	1	3	4	1	1	2	1	2						0,5165		
		4	4	1	2	1	5	3	2	2	3	3						0,5407		
		5	4	1	1	3	1	1	1	2	2	1						0,6432		
		1	1	2	2	4	2	3	2	3	3	2						0,439		
		2	2	1	1	4	5	1	2	2	3	3						0,3831		
311		3	3	2	2	4	4	2	1	2	1	1						0,6386		
	7151211	4	4	2	2	1	1	2	1	3	2	1	4	7151216	5	1	4	0,1373		3
		5	4	2	1	4	3	2	1	3	2	2						0,582		
	7178926	1	1	2	2	1	4	1	1	1	2	3	1	7178931	5	0	1	0,1408		1
		2	2	2	1	4	4	1	2	2	2	3						0,6991		
312		3	3	2	2	2	1	2	2	3	1	1						0,5062		
		4	4	2	2	3	5	1	1	1	1	3						0,2375		
		5	3	2	1	4	1	3	1	3	1	3						0,4861		
		1	1	1	2	3	2	3	1	2	1	1						0,4422		
		2	2	1	2	1	2	2	1	1	2	1						0,4519		
313	7178931	3	3	2	2	4	2	1	2	2	3	3	3	7178946	15	1	3	0,0546		5
		4	4	2	2	4	1	1	2	1	2	2						0,7153		
		5	3	1	2	4	2	3	2	2	2	1						0,1075		
	7206991	1	1	1	1	3	3	3	1	3	1	1	1	7206994	3	1	1	0,1401		1
		2	2	1	2	2	2	3	2	3	3	3						0,253		
314		3	3	1	1	1	4	2	2	1	2	3						0,2577		
		4	4	1	1	1	3	2	1	2	1	2						0,3551		
		5	2	2	2	3	2	1	2	2	1	1						0,3004		
	7234073	1	1	2	1	4	4	3	2	3	1	2	1	7234077	4	1	1	0,0012		1
		2	2	2	2	4	4	2	1	2	3	1						0,1275		
315		3	3	1	1	4	3	1	2	1	1	3						0,604		
		4	4	2	2	1	1	1	1	3	2	3						0,6627		
		5	3	1	2	4	3	1	2	1	2	2						0,0336		
	7263466	1	1	1	1	2	2	3	1	2	3	3	1	7263471	5	1	1	0,0801		1
		2	2	2	2	4	3	1	2	2	3	1						0,0807		
316		3	3	1	1	4	3	3	2	1	3	1						0,2605		
		4	4	2	2	3	1	3	2	2	1	2						0,123		
		5	2	1	1	2	5	2	2	2	1	2						0,5825		
		1	1	1	2	4	1	1	2	3	3	3						0,1179		
	7292366	2	2	1	1	4	2	1	1	1	2	1	2	7292369	3	1	2	0,0313		1
317		3	3	2	1	4	1	1	1	1	1	1						0,5341		
		4	4	1	1	2	1	3	1	3	3	1						0,4785		
		5	2	2	2	2	3	3	2	2	3	2						0,2274		
		1	1	2	2	4	3	2	1	3	3	1						0,6611		
		2	2	1	1	2	4	1	1	2	2	1						0,4362		
318	7315686	3	3	2	2	3	3	2	2	1	1	2	3	7315689	3	1	3	0,1773		2
		4	4	2	2	4	1	3	1	2	3	1						0,6275		
		5	2	2	2	4	4	2	1	2	3	2						0,461		
		1	1	2	2	4	3	2	1	1	2	1						0,1294		
		2	2	2	2	1	4	1	2	1	3	3						0,2574		
319	7338818	3	3	2	2	4	1	2	1	2	3	3	3	7338821	3	1	3	0,0678		1
		4	4	1	1	3	4	1	2	1	1	3						0,7005		
		5	3	2	2	2	2	2	2	2	3	1						0,3718		
		1	1	2	1	4	1	2	1	3	3	2						0,2378		
		2	2	2	1	2	2	3	1	2	3	2						0,1057		

Кінець таблиці Ж.2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
320		3	3	2	1	4	3	2	1	1	1	3						0,4229		
		4	4	1	2	1	3	3	2	1	1	1						0,1003		
	7365099	5	2	2	2	4	5	3	1	3	3	1	5	7365104	5	1	2	0,0279		4
	7394304	1	1	1	2	3	2	2	1	1	3	3	1	7394308	4	0	1	0,019		1
		2	2	1	2	2	3	3	1	1	3	1						0,6278		
321		3	3	2	2	2	1	1	1	2	2	3						0,4793		
		4	4	1	1	2	4	2	1	1	1	3						0,5436		
		5	4	2	2	4	1	3	2	1	2	1						0,39		
	7394308	1	1	1	1	4	4	2	2	1	3	2	1	7394331	23	1	1	0,0223		5
		2	2	2	1	4	5	3	2	3	3	1						0,2991		
322		3	3	1	2	1	3	1	2	2	1	3						0,3205		
		4	4	1	1	1	3	2	1	2	1	2						0,2868		
		5	3	2	2	3	3	2	2	1	3	2						0,5175		
	7418934	1	1	2	1	3	4	2	2	1	1	2	1	7418938	4	0	1	0,0318		2
		2	2	2	2	1	2	2	2	2	2	2						0,0867		
323		3	3	1	1	1	3	1	1	3	3	3						0,6858		
		4	4	2	2	3	3	1	2	1	1	1						0,0617		
		5	3	2	2	2	4	2	1	2	2	3						0,0524		
		1	1	2	1	2	1	1	1	1	1	1						0,0838		
	7418938	2	2	2	2	2	2	1	1	1	3	1	2	7418962	24	1	2	0,0555		5
324		3	3	1	1	1	3	3	2	1	3	2						0,5264		
		4	4	1	1	1	3	2	2	3	1	1						0,2221		
		5	3	1	1	4	2	3	2	2	1	2						0,3246		
	7446488	1	1	1	1	1	3	2	1	3	3	3	1	7446492	4	1	1	0,043		2
		2	2	1	2	3	1	1	2	2	2	3						0,719		
325		3	3	2	2	3	2	1	2	2	1	1						0,1481		
		4	4	2	2	4	4	3	1	3	1	3						0,7103		
		5	2	1	1	3	4	1	2	2	2	1						0,1555		
	7470596	1	1	2	1	2	1	1	1	1	2	1	1	7470600	4	1	1	0,2269		1
		2	2	1	1	3	4	3	2	2	2	1						0,322		
326		3	3	1	1	3	5	3	2	3	3	3						0,389		
		4	4	2	1	2	3	3	2	1	2	3						0,616		
		5	1	1	1	1	4	2	2	3	2	3						0,3644		
	7496610	1	1	2	2	1	3	2	1	2	3	2	1	7496615	5	1	1	0,1492		1
		2	2	1	2	2	4	3	2	2	1	2						0,2259		
327		3	3	2	2	4	2	3	2	3	2	3						0,6207		
		4	4	1	1	2	3	1	1	1	2	2						0,2814		
		5	4	1	1	2	1	2	2	2	2	2						0,3041		
		1	1	1	1	4	1	2	2	1	2	1						0,2888		
		2	2	2	1	1	5	1	2	2	3	3						0,6033		
328		3	3	2	2	3	2	2	1	1	2	3						0,5765		
	7525695	4	4	2	2	3	3	3	2	1	3	3	4	7525700	5	1	4	0,0473		1
		5	4	2	1	2	2	1	1	3	3	2						0,5724		
		1	1	1	2	1	4	1	2	3	1	1						0,3693		
		2	2	2	1	2	4	1	2	2	2	3						0,4918		
329		3	3	2	1	2	2	3	1	1	1	1						0,2583		
		4	4	1	1	1	5	3	1	2	2	2						0,46		
	7549989	5	3	1	1	3	1	2	2	2	3	1	5	7549994	5	1	3	0,0243		1
	7577021	1	1	1	2	1	1	2	2	2	3	1	1	7577026	5	1	1	0,0705		1
		2	2	1	1	1	3	1	2	1	1	2						0,0857		
330		3	3	2	2	2	1	2	2	3	1	2						0,2628		
		4	4	2	2	4	4	1	2	3	2	2						0,251		
		5	1	1	1	3	2	2	1	2	3	2						0,5055		
		1	1	1	1	4	5	1	2	2	2	2						0,3584		
		2	2	1	1	2	3	1	2	2	3	1						0,6466		
331	7605249	3	3	1	2	2	2	3	1	1	1	3	3	7605254	5	1	3	0,2624		1
		4	4	2	1	1	1	3	1	3	2	1						0,2767		
		5	1	2	1	3	3	3	1	3	1	1						0,6651		
		1	1	2	1	4	3	2	1	1	3	3						0,1102		
	7629811	2	2	2	2	4	3	1	1	1	3	1	2	7629814	3	1	2	0,0175		1
332		3	3	1	2	3	4	3	2	1	3	2						0,3886		
		4	4	1	1	1	5	1	1	2	3	2						0,3167		
		5	1	1	1	4	3	3	1	1	2	1						0,6854		
		1	1	1	1	2	2	2	2	2	2	2						0,2234		
		2	2	1	1	3	4	1	2	2	2	1						0,4276		
333		3	3	2	2	4	5	2	1	1	3	3						0,0818		
	7656633	4	4	2	1	1	4	2	2	3	1	1	4	7656637	4	1	4	0,06		1
		5	3	1	1	4	4	3	1	2	1	1						0,2353		
		1	1	1	2	2	2	3	2	2	1	3						0,5601		
		2	2	2	2	1	2	2	2	1	2	3						0,546		
334		3	3	2	1	2	4	1	2	3	2	3						0,1576		
	7682723	4	4	1	2	3	2	2	1	3	3	2	4	7682727	4	1	4	0,0285		1
		5	4	2	2	3	1	1	2	1	2	1						0,2697		
	7711538	1	1	1	1	2	2	1	2	3	2	1	1	7711541	3	1	1	0,0101		1
		2	2	1	2	4	2	1	1	3	1	2						0,102		
335		3	3	2	1	4	1	1	2	2	3	1						0,6402		
		4	4	2	1	3	1	2	1	2	2	2						0,0343		
		5	1	1	2	1	5	3	2	2	1	1						0,245		
		1	1	1	1	3	1	1	1	3	1	1						0,7049		
		2	2	2	2	1	1	3	2	2	3	2						0,4175		
336		3	3	2	2	2	5	3	2	3	1	3						0,5138		
		4	4	1	1	1	5	3	2	1	2	1						0,3084		
	7739621	5	4	2	1	1	2	2	1	3	1	2	5	7739624	3	1	4	0,2476		1
		1	1	1	1	4	3	1	1	2	2	2						0,124		
		2	2	2	1	3	1	2	1	3	3	1						0,2324		
337		3	3	2	1	2	4	2	2	2	2	2						0,3963		
		4	4	2	2	1	4	2	2	1	1	3						0,3849		
	7764839	5	3	2	1	2	1	2	1	2	3	1	5	7764843	4	1	3	0,0223		4

ДОДАТОК З.

РЕЗУЛЬТАТИ ТРЕТЬОГО ЕКСПЕРИМЕНТУ

Таблиця З.1

Повний набір даних для першої серії третього експерименту

Час вибору варіантів виконання завдань	Час завершення виконання завдань	Час виконання	Номер завдання	Варіанти виконання завдання	с	о	ц	б	Значення цільової функції оцінювання	Номер варіанту 1-5	Номер повтору варіанту	Попереднє значення цільової функції	Час виконання	Стратегія	Правило
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1,34E-01	3,67E-01	2,33E-01	4	1	0,0003	0,0657	0,0484	0,0149	0,0323	1				4	2,3
1,69E-01	4,95E-01	3,26E-01		2	0,0294	0,0391	0,0011	0,0429	0,0281					3	2,3
1,72E-01	5,55E-01	3,83E-01		3	0,0672	0,0294	0,0289	0,0551	0,0451					6	2,2
1,09E-01	4,24E-01	3,15E-01		4	0,0696	0,0633	0,0161	0,0056	0,0386					14	2,1
1,15E-01	4,06E-01	2,91E-01		5	0,0402	0,0234	0,0162	0,0625	0,0356					5	3,2
1,10E-01	4,30E-01	3,20E-01	2	1	0,0294	0,0563	0,0353	0,0418	0,0407		1	0,0323	2,33E-01	5	2,2
1,54E-01	3,20E-01	1,66E-01		2	0,0181	0,0304	0,0031	0,0226	0,0185	2		0,0281	3,26E-01	4	2,3
1,65E-01	4,91E-01	3,26E-01		3	0,0143	0,0154	0,0237	0,0368	0,0226			0,0451	3,83E-01	7	2,3
1,95E-01	3,18E-01	1,23E-01		4	0,0437	0,0005	0,0673	0,0390	0,0376			0,0386	3,15E-01	10	2,2
1,07E-01	4,11E-01	3,04E-01		5	0,0497	0,0227	0,0090	0,0419	0,0308			0,0356	2,91E-01	9	2,2
1,31E-01	4,88E-01	3,57E-01	1	1	0,0536	0,0437	0,0352	0,0371	0,0424			0,0407	3,20E-01	3	2,1
1,54E-01	4,64E-01	3,10E-01		2	0,0300	0,0397	0,0473	0,0670	0,0460		2	0,0185	1,66E-01	4	2,1
1,57E-01	4,18E-01	2,61E-01		3	0,0011	0,0029	0,0563	0,0152	0,0188	3		0,0226	3,26E-01	3	2,2
1,97E-01	5,54E-01	3,57E-01		4	0,0503	0,0113	0,0580	0,0122	0,0330			0,0376	1,23E-01	12	3,1
1,86E-01	4,15E-01	2,29E-01		5	0,0525	0,0014	0,0355	0,0082	0,0244			0,0308	3,04E-01	12	2,1
1,97E-01	5,99E-01	4,02E-01	3	1	0,0198	0,0308	0,0019	0,0599	0,0281			0,0424	3,57E-01	3	1,1
1,12E-01	5,23E-01	4,11E-01		2	0,0633	0,0010	0,0315	0,0633	0,0398			0,0460	3,10E-01	2	2,2
1,95E-01	5,67E-01	3,72E-01		3	0,0008	0,0636	0,0678	0,0387	0,0427		3	0,0188	2,61E-01	4	2,1
1,97E-01	4,88E-01	2,91E-01		4	0,0413	0,0025	0,0094	0,0421	0,0238			0,0330	3,57E-01	5	2,3
1,82E-01	5,05E-01	3,23E-01		5	0,0207	0,0396	0,0470	0,0382	0,0364	5		0,0244	2,29E-01	4	2,2
1,31E-01	3,07E-01	1,76E-01	5	1	0,0507	0,0216	0,0548	0,0417	0,0422			0,0281	4,02E-01	7	2,1
1,18E-01	5,57E-01	4,39E-01		2	0,0185	0,0417	0,0337	0,0254	0,0298	2		0,0398	4,11E-01	13	3,2
1,71E-01	5,97E-01	4,26E-01		3	0,0364	0,0254	0,0310	0,0095	0,0256			0,0427	3,72E-01	14	3,2
1,35E-01	5,53E-01	4,18E-01		4	0,0420	0,0095	0,0126	0,0502	0,0286			0,0238	2,91E-01	14	2,3
1,75E-01	3,88E-01	2,13E-01		5	0,0054	0,0502	0,0601	0,0027	0,0296		5	0,0364	3,23E-01	13	3,1
1,83E-01	3,29E-01	1,46E-01	6	1	0,0507	0,0027	0,0548	0,0417	0,0374			0,0422	1,76E-01	7	1,1
1,85E-01	4,03E-01	2,18E-01		2	0,0185	0,0216	0,0337	0,0254	0,0248	2	2	0,0298	4,39E-01	14	1,1
1,85E-01	4,61E-01	2,76E-01		3	0,0364	0,0329	0,0310	0,0095	0,0275			0,0256	4,26E-01	9	2,1
1,35E-01	3,70E-01	2,35E-01		4	0,0420	0,0420	0,0126	0,0502	0,0367			0,0286	4,18E-01	14	2,2
1,79E-01	3,61E-01	1,82E-01		5	0,0054	0,0054	0,0601	0,0027	0,0184			0,0296	2,13E-01	9	2,1
1,80E-01	3,21E-01	1,41E-01	7	1	0,0019	0,0548	0,0548	0,0216	0,0333			0,0374	1,46E-01	11	2,2
1,40E-01	3,82E-01	2,42E-01		2	0,0315	0,0337	0,0337	0,0329	0,0329	2	2	0,0248	2,18E-01	14	3,2
1,84E-01	5,26E-01	3,42E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0275	2,76E-01	5	3,1
1,21E-01	4,35E-01	3,14E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149			0,0367	2,35E-01	14	2,3
1,58E-01	4,16E-01	2,58E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586			0,0184	1,82E-01	1	1,1

Продовження таблиці 3.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1,35E-01	4,41E-01	3,06E-01	7	1	0,0507	0,0216	0,0548	0,0417	0,0422	1		0,0333	1,41E-01	8	3,1
1,03E-01	4,76E-01	3,73E-01		2	0,0185	0,0329	0,0337	0,0254	0,0276		2	0,0329	2,42E-01	14	3,1
1,11E-01	4,78E-01	3,67E-01		3	0,0364	0,0534	0,0310	0,0095	0,0326			0,0458	3,42E-01	1	1,1
1,65E-01	5,99E-01	4,34E-01		4	0,0420	0,0251	0,0601	0,0502	0,0444			0,0149	3,14E-01	9	2,2
1,15E-01	5,44E-01	4,29E-01		5	0,0054	0,0674	0,0548	0,0027	0,0325			0,0586	2,58E-01	8	2,2
1,58E-01	4,70E-01	3,12E-01	5	1	0,0507	0,0507	0,0337	0,0417	0,0442		1	0,0422	3,06E-01	6	1,1
1,32E-01	3,40E-01	2,08E-01		2	0,0185	0,0185	0,0310	0,0254	0,0233			0,0276	3,73E-01	6	2,1
1,73E-01	5,21E-01	3,48E-01		3	0,0364	0,0364	0,0126	0,0095	0,0237			0,0326	3,67E-01	5	2,3
1,98E-01	5,29E-01	3,31E-01		4	0,0420	0,0420	0,0601	0,0502	0,0486			0,0444	4,34E-01	14	3,1
1,90E-01	5,72E-01	3,82E-01		5	0,0054	0,0054	0,0548	0,0027	0,0170	5		0,0325	4,29E-01	12	2,1
1,30E-01	4,00E-01	2,70E-01	3	1	0,0019	0,0548	0,0337	0,0216	0,0280	1		0,0442	3,12E-01	10	3,1
1,18E-01	5,10E-01	3,92E-01		2	0,0315	0,0337	0,0310	0,0329	0,0323			0,0233	2,08E-01	1	3,2
1,35E-01	4,56E-01	3,21E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0237	3,48E-01	12	3,1
1,95E-01	4,64E-01	2,69E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149			0,0486	3,31E-01	14	3,1
1,70E-01	3,39E-01	1,69E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586		5	0,0170	3,82E-01	13	2,3
1,22E-01	5,20E-01	3,98E-01	6	1	0,0019	0,0329	0,0548	0,0216	0,0278			0,0280	2,70E-01	8	2,3
1,17E-01	3,38E-01	2,21E-01		2	0,0315	0,0534	0,0337	0,0329	0,0379	2		0,0323	3,92E-01	1	3,1
1,70E-01	5,91E-01	4,21E-01		3	0,0678	0,0251	0,0310	0,0534	0,0443			0,0458	3,21E-01	1	2,1
1,98E-01	4,53E-01	2,55E-01		4	0,0094	0,0674	0,0126	0,0251	0,0286		3	0,0149	2,69E-01	4	2,1
1,20E-01	3,75E-01	2,55E-01		5	0,0470	0,0216	0,0601	0,0674	0,0490			0,0586	1,69E-01	13	2,3
1,74E-01	3,33E-01	1,59E-01	1	1	0,0019	0,0548	0,0548	0,0216	0,0333			0,0278	3,98E-01	8	3,2
1,76E-01	3,91E-01	2,15E-01		2	0,0315	0,0337	0,0337	0,0329	0,0329		2	0,0379	2,21E-01	14	2,1
1,16E-01	3,89E-01	2,73E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0443	4,21E-01	13	3,2
1,24E-01	4,53E-01	3,29E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149	4		0,0286	2,55E-01	14	2,2
1,56E-01	5,45E-01	3,89E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586			0,0490	2,55E-01	14	2,1
1,56E-01	5,32E-01	3,76E-01	3	1	0,0019	0,0548	0,0601	0,0216	0,0346	1		0,0333	1,59E-01	6	2,1
1,26E-01	4,34E-01	3,08E-01		2	0,0315	0,0337	0,0601	0,0329	0,0396			0,0329	2,15E-01	14	2,1
1,96E-01	5,71E-01	3,75E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0458	2,73E-01	3	3,2
1,23E-01	4,37E-01	3,14E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149		4	0,0149	3,29E-01	6	3,2
1,89E-01	5,07E-01	3,18E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586			0,0586	3,89E-01	14	3,1
1,46E-01	4,95E-01	3,49E-01	5	1	0,0019	0,0548	0,0548	0,0216	0,0333		1	0,0346	3,76E-01	4	2,1
1,49E-01	4,45E-01	2,96E-01		2	0,0315	0,0337	0,0337	0,0329	0,0329			0,0396	3,08E-01	8	3,2
1,94E-01	5,52E-01	3,58E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0458	3,75E-01	8	2,2
1,41E-01	4,37E-01	2,96E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149			0,0149	3,14E-01	3	2,1
1,68E-01	4,92E-01	3,24E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586	5		0,0586	3,18E-01	8	3,1
1,61E-01	3,84E-01	2,23E-01	3	1	0,0019	0,0548	0,0548	0,0216	0,0333	1		0,0333	3,49E-01	5	2,3
1,60E-01	3,90E-01	2,30E-01		2	0,0315	0,0337	0,0337	0,0329	0,0329			0,0329	2,96E-01	1	1,1
1,85E-01	3,57E-01	1,72E-01		3	0,0019	0,0310	0,0310	0,0534	0,0293			0,0458	3,58E-01	2	2,3
1,75E-01	4,14E-01	2,39E-01		4	0,0315	0,0126	0,0126	0,0251	0,0204			0,0149	2,96E-01	3	3,2
1,41E-01	5,43E-01	4,02E-01		5	0,0678	0,0601	0,0601	0,0674	0,0639		5	0,0586	3,24E-01	11	1,1
1,75E-01	5,26E-01	3,51E-01	5	1	0,0094	0,0548	0,0548	0,0216	0,0351		1	0,0333	2,23E-01	4	1,1
1,24E-01	3,62E-01	2,38E-01		2	0,0470	0,0337	0,0337	0,0329	0,0368	2		0,0329	2,30E-01	2	2,3
1,87E-01	5,08E-01	3,21E-01		3	0,0126	0,0310	0,0310	0,0534	0,0320			0,0293	1,72E-01	13	2,3
1,59E-01	3,87E-01	2,28E-01		4	0,0601	0,0126	0,0126	0,0251	0,0276			0,0204	2,39E-01	14	2,1
1,82E-01	5,93E-01	4,11E-01		5	0,0548	0,0601	0,0601	0,0674	0,0606			0,0639	4,02E-01	13	2,1

Кінець таблиці 3.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1,26E-01	3,67E-01	2,41E-01	4	1	0,0337	0,0548	0,0548	0,0216	0,0412			0,0351	3,51E-01	8	2,1
1,83E-01	5,22E-01	3,39E-01		2	0,0310	0,0337	0,0251	0,0329	0,0307	2	2	0,0368	2,38E-01	9	2,3
1,01E-01	4,72E-01	3,71E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0320	3,21E-01	12	3,2
1,22E-01	4,86E-01	3,64E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149			0,0276	2,28E-01	2	1,1
1,22E-01	3,18E-01	1,96E-01		5	0,0470	0,0601	0,0601	0,0674	0,0586			0,0606	4,11E-01	2	1,1
1,66E-01	3,92E-01	2,26E-01	4	1	0,0019	0,0548	0,0548	0,0216	0,0333	1		0,0412	2,41E-01	6	2,3
1,00E-01	5,77E-01	4,77E-01		2	0,0315	0,0337	0,0337	0,0329	0,0329		2	0,0307	3,39E-01	1	3,2
1,53E-01	5,77E-01	4,24E-01		3	0,0678	0,0310	0,0310	0,0534	0,0458			0,0458	3,71E-01	8	2,3
1,61E-01	5,10E-01	3,49E-01		4	0,0094	0,0534	0,0126	0,0251	0,0251			0,0149	3,64E-01	2	3,2
1,82E-01	3,06E-01	1,24E-01		5	0,0470	0,0251	0,0601	0,0674	0,0499			0,0586	1,96E-01	11	1,1
1,90E-01	3,95E-01	2,05E-01	1	1	0,0019	0,0674	0,0548	0,0216	0,0364		1	0,0333	2,26E-01	4	2,1
1,87E-01	3,31E-01	1,44E-01		2	0,0315	0,0216	0,0337	0,0329	0,0299	2		0,0329	4,77E-01	6	3,1
1,23E-01	3,13E-01	1,90E-01		3	0,0678	0,0329	0,0310	0,0534	0,0463			0,0458	4,24E-01	7	1,1
1,84E-01	3,13E-01	1,29E-01		4	0,0094	0,0534	0,0126	0,0251	0,0251			0,0251	3,49E-01	5	1,1
1,64E-01	5,29E-01	3,65E-01		5	0,0470	0,0251	0,0601	0,0310	0,0408			0,0499	1,24E-01	2	2,1
1,20E-01	3,24E-01	2,04E-01	2	1	0,0019	0,0674	0,0548	0,0019	0,0315			0,0364	2,05E-01	6	2,2
1,22E-01	5,72E-01	4,50E-01		2	0,0315	0,0216	0,0337	0,0315	0,0296		2	0,0299	1,44E-01	13	2,1
1,54E-01	5,19E-01	3,65E-01		3	0,0678	0,0329	0,0310	0,0678	0,0499			0,0463	1,90E-01	12	2,3
1,40E-01	3,31E-01	1,91E-01		4	0,0094	0,0126	0,0126	0,0251	0,0149			0,0251	1,29E-01	9	3,1
1,73E-01	5,88E-01	4,15E-01		5	0,0470	0,0601	0,0678	0,0674	0,0606	5		0,0408	3,65E-01	10	3,1

Таблиця 3.2

Середні та зведені значення для першої серії третього експерименту

Середній час виконання	Номер завдання	Розподіл завдань по варіантах*	Середнє значення стійкості	Середнє значення оперативності	Середнє значення цілісності	Середнє значення безпеки	Середнє значення цільової функції	Номер варіанту 1-5	Номер повтору варіанту	Кількість обраних правил	Кількість обраних стратегій
1,55E+02	1 - 3 2 - 2 3 - 4 4 - 3 5 - 4 6 - 2 7 - 2	0-1-1-1-0 0-1-0-0-1 3-0-0-0-1 2-1-0-0-0 0-2-0-0-2 0-2-0-0-0 1-1-0-0-0	0,0319	0,0345	0,0385	0,0362	0,0353	1 - 6 2 - 8 3 - 1 4 - 1 5 - 4	1 - 6 2 - 7 3 - 1 4 - 1 5 - 4	1 - 7 2 - 7 3 - 7 4 - 9 5 - 7 6 - 8 7 - 4 8 - 9 9 - 6 10 - 3 11 - 3 12 - 6 13 - 8 14 - 16	1,1 - 14 2,1 - 24 2,2 - 14 2,3 - 19 3,1 - 15 3,2 - 14

*Примітка формат запису 1-2-3-4-5 означає для *i*-го завдання розподіл кількості обраних варіантів 1,..,5 у цьому завданні

Таблиця 3.3

Повний набір даних для другої серії третього експерименту

№	Час вибору варіантів виконання завдань	Час завершення виконання завдань	Час виконання	Номер завдання	Варіанти виконання завдання	с	о	ц	б	Значення цільової функції оцінювання	Номер варіанту 1-5	Номер повтору варіанту	Попереднє значення цільової функції	Час виконання	Стратегія	Правило
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1,98E-01	3,55E-01	1,57E-01	6	1	0,1901	0,2463	0,1256	0,1727	0,183675	1	1			3	2,3
2	1,37E-01	4,74E-01	3,37E-01	1	1	0,1872	0,2530	0,1972	0,1226	0,190026	1	1	0,183675	1,57E-01	10	2,1
3	1,36E-01	3,25E-01	1,89E-01	1	1	0,2322	0,1779	0,1521	0,1216	0,17095	1	1	0,190026	3,37E-01	3	2,3
4	1,83E-01	3,32E-01	1,49E-01	1	1	0,2032	0,2250	0,1688	0,1773	0,193583	1	1	0,17095	1,89E-01	10	2,3
5	1,90E-01	3,30E-01	1,40E-01	3	1	0,2210	0,1657	0,1852	0,2637	0,208911	1	1	0,193583	1,49E-01	9	3,2
6	1,97E-01	3,23E-01	1,26E-01	6	1	0,2058	0,2354	0,1689	0,1538	0,190984	1	1	0,208911	1,40E-01	12	2,3
7	1,20E-01	3,50E-01	2,30E-01	3	1	0,1402	0,1664	0,1572	0,1836	0,161861	1	1	0,190984	1,26E-01	14	2,3
8	1,30E-01	3,05E-01	1,75E-01	5	1	0,2544	0,2165	0,2353	0,2643	0,24263	1	1	0,161861	2,30E-01	10	2,2
9	1,33E-01	5,47E-01	4,14E-01	7	1	0,1747	0,2121	0,2363	0,1923	0,203847	1	1	0,24263	1,75E-01	13	1,1
10	1,80E-01	3,28E-01	1,48E-01	6	1	0,2643	0,2470	0,2603	0,2433	0,253707	1	1	0,203847	4,14E-01	1	2,2
11	1,40E-01	5,07E-01	3,67E-01	3	1	0,2438	0,2537	0,1961	0,1922	0,221435	1	1	0,253707	1,48E-01	12	2,2
12	1,43E-01	4,12E-01	2,69E-01	2	1	0,2249	0,2689	0,1983	0,1208	0,203225	1	1	0,221435	3,67E-01	11	3,1
13	1,14E-01	3,21E-01	2,07E-01	2	1	0,2250	0,1498	0,2525	0,1523	0,194882	1	1	0,203225	2,69E-01	11	3,2
14	1,97E-01	5,89E-01	3,92E-01	4	1	0,1968	0,1209	0,1382	0,2076	0,165871	1	1	0,194882	2,07E-01	1	2,1
15	1,39E-01	5,60E-01	4,21E-01	2	1	0,2287	0,1783	0,2411	0,2590	0,226772	1	1	0,165871	3,92E-01	1	2,2
16	1,22E-01	5,17E-01	3,95E-01	6	1	0,1964	0,2681	0,2539	0,2681	0,246622	1	1	0,226772	4,21E-01	1	2,1
17	1,04E-01	5,71E-01	4,67E-01	3	1	0,2378	0,1228	0,1691	0,1635	0,17329	1	1	0,246622	3,95E-01	8	1,1
18	1,71E-01	5,96E-01	4,25E-01	1	1	0,1634	0,1821	0,1889	0,2024	0,184229	1	1	0,17329	4,67E-01	3	3,2
19	1,39E-01	4,77E-01	3,38E-01	1	1	0,1391	0,1628	0,1886	0,1521	0,160662	1	1	0,184229	4,25E-01	12	2,1
20	1,98E-01	5,80E-01	3,82E-01	4	1	0,1320	0,1986	0,2548	0,2123	0,199409	1	1	0,160662	3,38E-01	6	2,2
21	1,60E-01	3,30E-01	1,70E-01	7	1	0,2118	0,2491	0,2237	0,2204	0,226229	1	1	0,199409	3,82E-01	2	2,1
22	1,79E-01	4,64E-01	2,85E-01	5	1	0,2159	0,2109	0,2042	0,1461	0,19427	1	1	0,226229	1,70E-01	8	2,1
23	1,64E-01	4,49E-01	2,85E-01	1	1	0,2145	0,1262	0,1532	0,1475	0,16034	1	1	0,19427	2,85E-01	13	2,3
24	1,71E-01	4,14E-01	2,43E-01	2	1	0,1901	0,2463	0,1256	0,1727	0,183667	1	1	0,16034	2,85E-01	12	1,1
25	1,74E-01	5,11E-01	3,37E-01	5	1	0,2024	0,1207	0,1932	0,1980	0,178592	1	1	0,183667	2,43E-01	10	2,2
26	1,12E-01	5,91E-01	4,79E-01	1	1	0,2164	0,1572	0,1659	0,2536	0,198259	1	1	0,178592	3,37E-01	7	1,1
27	1,83E-01	5,45E-01	3,62E-01	1	1	0,1664	0,2237	0,2237	0,2204	0,208534	1	1	0,198259	4,79E-01	11	2,1
28	1,53E-01	4,03E-01	2,50E-01	4	1	0,2165	0,2042	0,2042	0,1461	0,192773	1	1	0,208534	3,62E-01	11	1,1
29	1,52E-01	5,68E-01	4,16E-01	3	1	0,2121	0,1532	0,1532	0,1475	0,166491	1	1	0,192773	2,50E-01	8	3,1
30	1,53E-01	4,96E-01	3,43E-01	6	1	0,2470	0,1256	0,1659	0,2544	0,198211	1	1	0,166491	4,16E-01	14	3,2
31	1,90E-01	5,29E-01	3,39E-01	1	1	0,2537	0,1932	0,2204	0,1747	0,21051	1	1	0,198211	3,43E-01	11	3,1
32	1,76E-01	5,68E-01	3,92E-01	7	1	0,2689	0,1461	0,1461	0,2643	0,206331	1	1	0,21051	3,39E-01	6	1,1
33	1,55E-01	3,23E-01	1,68E-01	3	1	0,1498	0,1475	0,1475	0,2438	0,172132	1	1	0,206331	3,92E-01	6	3,2
34	1,52E-01	3,48E-01	1,96E-01	4	1	0,1209	0,1727	0,1727	0,2249	0,172782	1	1	0,172132	1,68E-01	7	1,1
35	1,23E-01	4,48E-01	3,25E-01	5	1	0,2689	0,1461	0,1461	0,2250	0,196499	1	1	0,172782	1,96E-01	5	3,1
36	1,26E-01	4,53E-01	3,27E-01	6	1	0,1498	0,1475	0,1475	0,1968	0,160376	1	1	0,196499	3,25E-01	2	2,1
37	1,79E-01	4,96E-01	3,17E-01	4	1	0,1228	0,2165	0,1901	0,2287	0,189518	1	1	0,160376	3,27E-01	1	2,2
38	1,69E-01	3,39E-01	1,70E-01	2	1	0,1821	0,2121	0,2024	0,1964	0,198257	1	1	0,189518	3,17E-01	4	2,2
39	1,18E-01	4,40E-01	3,22E-01	1	1	0,1628	0,2470	0,2164	0,2378	0,21598	1	1	0,198257	1,70E-01	4	2,3
40	1,26E-01	3,45E-01	2,19E-01	2	1	0,2249	0,2537	0,1664	0,1634	0,202103	1	1	0,21598	3,22E-01	6	2,3
41	1,58E-01	3,64E-01	2,06E-01	1	1	0,1498	0,2689	0,2165	0,1391	0,193566	1	1	0,202103	2,19E-01	8	2,1
42	1,83E-01	3,48E-01	1,65E-01	4	1	0,1209	0,1498	0,2121	0,1783	0,165243	1	1	0,193566	2,06E-01	8	2,3

Продовження таблиці 3.3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
43	1,74E-01	3,28E-01	1,54E-01	6	1	0,1783	0,1209	0,1228	0,2024	0,15607	1	1	0,165243	1,65E-01	10	1,1
44	1,78E-01	3,02E-01	1,24E-01	4	1	0,2681	0,1783	0,1821	0,2438	0,218065	1	1	0,15607	1,54E-01	1	2,3
45	1,08E-01	3,46E-01	2,38E-01	4	1	0,1228	0,1664	0,1628	0,1727	0,156161	1	1	0,218065	1,24E-01	12	3,1
46	1,58E-01	3,64E-01	2,06E-01	3	1	0,1821	0,2165	0,2353	0,1727	0,201664	1	1	0,156161	2,38E-01	5	2,3
47	1,43E-01	4,83E-01	3,40E-01	7	1	0,1628	0,2121	0,2363	0,1475	0,189658	1	1	0,201664	2,06E-01	2	1,1
48	1,86E-01	5,40E-01	3,54E-01	6	1	0,1986	0,2470	0,2603	0,1727	0,219638	1	1	0,189658	3,40E-01	13	3,1
49	1,30E-01	4,22E-01	2,92E-01	7	1	0,2491	0,2537	0,1961	0,1980	0,224225	1	1	0,219638	3,54E-01	11	1,1
50	1,97E-01	4,41E-01	2,44E-01	4	1	0,2249	0,2689	0,1983	0,2536	0,236413	1	1	0,224225	2,92E-01	7	3,1
51	1,00E-01	3,06E-01	2,06E-01	1	1	0,2250	0,1498	0,2525	0,2165	0,210948	1	1	0,236413	2,44E-01	12	3,1
52	1,27E-01	5,84E-01	4,57E-01	5	1	0,1968	0,1209	0,1382	0,2121	0,166979	1	1	0,210948	2,06E-01	8	2,1
53	1,85E-01	3,43E-01	1,58E-01	5	1	0,2287	0,1783	0,2287	0,1783	0,203464	1	1	0,166979	4,57E-01	8	3,2
54	1,61E-01	3,92E-01	2,31E-01	3	1	0,1964	0,2681	0,2539	0,2536	0,24299	1	1	0,203464	1,58E-01	1	1,1
55	1,54E-01	3,12E-01	1,58E-01	6	1	0,2165	0,2438	0,2537	0,1961	0,227522	1	1	0,24299	2,31E-01	11	2,3
56	1,16E-01	5,42E-01	4,26E-01	7	1	0,2121	0,1664	0,1572	0,1836	0,179826	1	1	0,227522	1,58E-01	3	2,1
57	1,76E-01	4,55E-01	2,79E-01	5	1	0,2470	0,2165	0,2353	0,2643	0,240783	1	1	0,179826	4,26E-01	4	3,1
58	1,50E-01	5,96E-01	4,46E-01	3	1	0,2537	0,2121	0,2363	0,1923	0,223576	1	1	0,240783	2,79E-01	8	1,1
59	1,76E-01	4,07E-01	2,31E-01	3	1	0,2689	0,2470	0,2603	0,2433	0,254849	1	1	0,223576	4,46E-01	13	3,1
60	1,92E-01	4,46E-01	2,54E-01	2	1	0,1498	0,2537	0,1961	0,1922	0,197931	1	1	0,254849	2,31E-01	5	2,1
61	1,80E-01	4,19E-01	2,39E-01	7	1	0,2121	0,2689	0,1983	0,1208	0,20002	1	1	0,197931	2,54E-01	14	2,2
62	1,25E-01	3,37E-01	2,12E-01	5	1	0,1783	0,1498	0,2525	0,1523	0,183204	1	1	0,20002	2,39E-01	8	3,2
63	1,95E-01	4,26E-01	2,31E-01	1	1	0,2536	0,1209	0,1382	0,2076	0,180072	1	1	0,183204	2,12E-01	14	3,1
64	1,84E-01	5,72E-01	3,88E-01	2	1	0,1961	0,1783	0,2411	0,2590	0,218637	1	1	0,180072	2,31E-01	14	2,3
65	1,47E-01	5,50E-01	4,03E-01	1	1	0,1836	0,2681	0,2539	0,2681	0,243406	1	1	0,218637	3,88E-01	4	3,1
66	1,35E-01	3,40E-01	2,05E-01	2	1	0,2643	0,1228	0,1691	0,1635	0,179929	1	1	0,243406	4,03E-01	5	2,1
67	1,60E-01	4,71E-01	3,11E-01	3	1	0,1923	0,1821	0,1889	0,2024	0,19144	1	1	0,179929	2,05E-01	4	3,1
68	1,49E-01	4,62E-01	3,13E-01	5	1	0,2433	0,1628	0,1886	0,1521	0,186708	1	1	0,19144	3,11E-01	13	1,1
69	1,98E-01	4,11E-01	2,13E-01	5	1	0,1922	0,1986	0,2548	0,2123	0,214461	1	1	0,186708	3,13E-01	1	2,1
70	1,38E-01	4,31E-01	2,93E-01	4	1	0,1208	0,2491	0,2237	0,2204	0,203491	1	1	0,214461	2,13E-01	1	2,3
71	1,62E-01	5,41E-01	3,79E-01	4	1	0,1523	0,2109	0,2042	0,1461	0,178371	1	1	0,203491	2,93E-01	8	1,1
72	1,37E-01	5,80E-01	4,43E-01	1	1	0,2076	0,1262	0,1532	0,1475	0,158632	1	1	0,178371	3,79E-01	12	1,1
73	1,38E-01	4,48E-01	3,10E-01	5	1	0,1209	0,2463	0,1256	0,1727	0,166354	1	1	0,158632	4,43E-01	2	2,1
74	1,77E-01	4,36E-01	2,59E-01	2	1	0,2121	0,1532	0,1532	0,1475	0,166491	1	1	0,166354	3,10E-01	1	1,1
75	1,17E-01	3,30E-01	2,13E-01	2	1	0,2470	0,1256	0,1659	0,2544	0,198211	1	1	0,166491	2,59E-01	1	2,3
76	1,84E-01	4,75E-01	2,91E-01	1	1	0,2537	0,1932	0,2204	0,1747	0,21051	1	1	0,198211	2,13E-01	7	2,2
77	1,10E-01	3,39E-01	2,29E-01	4	1	0,2689	0,1461	0,1461	0,2643	0,206331	1	1	0,21051	2,91E-01	12	2,1
78	1,56E-01	5,98E-01	4,42E-01	1	1	0,1498	0,1475	0,1475	0,2438	0,172132	1	1	0,206331	2,29E-01	9	2,1
79	1,17E-01	4,82E-01	3,65E-01	4	1	0,1209	0,1727	0,1727	0,2249	0,172782	1	1	0,172132	4,42E-01	10	2,1
80	1,57E-01	3,27E-01	1,70E-01	6	1	0,2689	0,1461	0,1461	0,2250	0,196499	1	1	0,172782	3,65E-01	1	3,1
81	1,73E-01	4,06E-01	2,33E-01	2	1	0,1498	0,1475	0,1475	0,1968	0,160376	1	1	0,196499	1,70E-01	5	2,2
82	1,96E-01	4,88E-01	2,92E-01	5	1	0,1228	0,2165	0,1901	0,2287	0,189518	1	1	0,160376	2,33E-01	3	3,2
83	1,45E-01	5,25E-01	3,80E-01	2	1	0,1821	0,2121	0,2024	0,1964	0,198257	1	1	0,189518	2,92E-01	8	3,1
84	1,60E-01	3,26E-01	1,66E-01	4	1	0,1628	0,2470	0,2164	0,2378	0,21598	1	1	0,198257	3,80E-01	11	2,3
85	1,82E-01	4,77E-01	2,95E-01	2	1	0,2249	0,2537	0,1664	0,1634	0,202103	1	1	0,21598	1,66E-01	9	1,1
86	1,10E-01	5,81E-01	4,71E-01	5	1	0,1498	0,2689	0,2165	0,1391	0,193566	1	1	0,202103	2,95E-01	10	2,3
87	1,07E-01	3,15E-01	2,08E-01	6	1	0,1475	0,1498	0,2121	0,1783	0,171895	1	1	0,193566	4,71E-01	1	2,3
88	1,79E-01	4,77E-01	2,98E-01	1	1	0,2165	0,2491	0,2237	0,2204	0,227419	1	1	0,171895	2,08E-01	13	3,1

Кінець таблиці 3.3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
89	1,54E-01	4,86E-01	3,32E-01	7	1	0,2121	0,2109	0,2042	0,1461	0,193321	1	1	0,227419	2,98E-01	1	1,1
90	1,81E-01	4,11E-01	2,30E-01	7	1	0,2470	0,1262	0,1532	0,1475	0,168471	1	1	0,193321	3,32E-01	5	3,2
91	1,66E-01	4,29E-01	2,63E-01	3	1	0,2537	0,2463	0,1256	0,1727	0,199549	1	1	0,168471	2,30E-01	12	3,1
92	1,47E-01	3,71E-01	2,24E-01	7	1	0,2689	0,1532	0,1532	0,1475	0,180694	1	1	0,199549	2,63E-01	3	3,2
93	1,95E-01	4,44E-01	2,49E-01	4	1	0,1498	0,1256	0,1659	0,2544	0,173907	1	1	0,180694	2,24E-01	1	3,1
94	1,40E-01	4,92E-01	3,52E-01	5	1	0,1498	0,1932	0,2204	0,1747	0,184535	1	1	0,173907	2,49E-01	2	3,2
95	1,45E-01	3,77E-01	2,32E-01	1	1	0,2689	0,1461	0,1461	0,2250	0,196499	1	1	0,184535	3,52E-01	5	2,3
96	1,86E-01	3,21E-01	1,35E-01	6	1	0,1498	0,1475	0,1475	0,1968	0,160376	1	1	0,196499	2,32E-01	11	2,2
97	1,47E-01	3,27E-01	1,80E-01	4	1	0,1228	0,2165	0,1901	0,2287	0,189518	1	1	0,160376	1,35E-01	5	2,2
98	1,48E-01	5,42E-01	3,94E-01	3	1	0,1821	0,2121	0,2024	0,1964	0,198257	1	1	0,189518	1,80E-01	8	3,1
99	1,47E-01	4,17E-01	2,70E-01	6	1	0,1628	0,2470	0,2164	0,2378	0,21598	1	1	0,198257	3,94E-01	9	3,2
100	1,70E-01	4,72E-01	3,02E-01	1	1	0,2249	0,2537	0,1664	0,1634	0,202103	1	1	0,21598	2,70E-01	7	3,2

Таблиця 3.4

Середні та зведені значення для другої серії третього експерименту

Середній час виконання	Номер завдання	Середнє значення стійкості	Середнє значення оперативності	Середнє значення цілісності	Середнє значення безпеки	Середнє значення цільової функції	Кількість обраних правил	Кількість обраних стратегій
2,85E-01	1 - 20 2 - 14 3 - 13 4 - 16 5 - 14 6 - 13 7 - 10	0,198971	0,19481	0,191822	0,197117	0,19568	1 - 15 2 - 5 3 - 6 4 - 5 5 - 8 6 - 4 7 - 5 8 - 12 9 - 4 10 - 7 11 - 9 12 - 9 13 - 6 14 - 5	1,1 - 18 2,1 - 18 2,2 - 13 2,3 - 19 3,1 - 19 3,2 - 13

ДОДАТОК И.

РЕЗУЛЬТАТИ ЧЕТВЕРТОГО ЕКСПЕРИМЕНТУ

Таблиця И.1

Результати дослідження достовірності виявлення метаморфних вірусів на окремих етапах з врахуванням всіх особливостей штучно створених екземплярів класів

Ета-пи	Detection result	Класи метаморфних вірусів												Total
		1	2	3	4	5	6	7	8	9	10	11	12	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**
1	*TP*	11	10	13	13	12	12	13	12	12	12	11	12	143
	FN	4	5	2	2	3	3	2	3	3	3	4	3	37
	FP	34	27	20	20	19	33	35	32	29	21	28	27	325
	TN	326	333	340	340	341	327	325	328	331	339	332	333	3995
2	*TP*	13	12	12	13	10	9	12	9	11	13	11	9	134
	FN	2	3	3	2	5	6	3	6	4	2	4	6	46
	FP	31	23	27	22	38	38	36	35	30	31	39	20	370
	TN	329	337	333	338	322	322	324	325	330	329	321	340	3950
3	*TP*	12	11	13	9	10	12	13	10	13	13	11	13	140
	FN	3	4	2	6	5	3	2	5	2	2	4	2	40
	FP	20	25	28	39	24	36	26	30	42	35	25	40	370
	TN	340	335	332	321	336	324	334	330	318	325	335	320	3950
4	*TP*	11	11	11	12	12	13	13	13	9	10	13	10	138
	FN	4	4	4	3	3	2	2	2	6	5	2	5	42
	FP	27	39	26	32	40	41	38	34	37	22	25	38	399
	TN	333	321	334	328	320	319	322	326	323	338	335	322	3921
5	*TP*	10	9	9	13	11	13	13	13	9	9	10	12	131
	FN	5	6	6	2	4	2	2	2	6	6	5	3	49
	FP	24	29	41	23	39	31	26	38	42	27	32	27	379
	TN	336	331	319	337	321	329	334	322	318	333	328	333	3941
6	*TP*	12	12	9	9	12	11	13	9	10	13	10	12	132
	FN	3	3	6	6	3	4	2	6	5	2	5	3	48
	FP	39	34	30	41	27	31	25	39	23	38	34	37	398
	TN	321	326	330	319	333	329	335	321	337	322	326	323	3922
7	*TP*	9	10	10	9	10	10	10	13	11	12	11	10	125
	FN	6	5	5	6	5	5	5	2	4	3	4	5	55
	FP	34	31	23	32	26	35	25	36	19	40	29	29	359
	TN	326	329	337	328	334	325	335	324	341	320	331	331	3961
8	*TP*	9	9	9	10	9	12	12	10	10	11	12	13	126
	FN	6	6	6	5	6	3	3	5	5	4	3	2	54
	FP	36	41	26	38	22	39	37	25	22	22	39	31	378
	TN	324	319	334	322	338	321	323	335	338	338	321	329	3942
9	*TP*	13	13	13	11	11	9	13	11	11	13	9	13	140
	FN	2	2	2	4	4	6	2	4	4	2	6	2	40
	FP	22	27	38	26	28	23	26	26	36	36	41	32	361
	TN	338	333	322	334	332	337	334	334	324	324	319	328	3959
10	*TP*	12	13	9	12	11	10	12	9	12	13	10	12	135
	FN	3	2	6	3	4	5	3	6	3	2	5	3	45
	FP	41	27	33	24	26	35	27	23	37	32	38	24	367
	TN	319	333	327	336	334	325	333	337	323	328	322	336	3953

Продовження таблиці И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**
11	TP	12	13	12	12	11	9	12	10	13	9	9	10	132
	FN	3	2	3	3	4	6	3	5	2	6	6	5	48
	FP	28	36	34	35	38	23	35	33	34	23	36	22	377
	TN	332	324	326	325	322	337	325	327	326	337	324	338	3943
12	TP	11	9	11	11	10	10	11	12	13	10	10	12	130
	FN	4	6	4	4	5	5	4	3	2	5	5	3	50
	FP	33	39	33	31	25	23	19	37	27	35	21	33	356
	TN	327	321	327	329	335	337	341	323	333	325	339	327	3964
13	TP	11	12	9	12	13	9	11	9	11	9	11	13	130
	FN	4	3	6	3	2	6	4	6	4	6	4	2	50
	FP	38	19	25	25	39	37	22	21	34	26	20	33	339
	TN	322	341	335	335	321	323	338	339	326	334	340	327	3981
14	TP	9	9	12	9	10	13	12	11	10	13	9	10	127
	FN	6	6	3	6	5	2	3	4	5	2	6	5	53
	FP	35	39	39	19	23	31	29	28	20	34	39	24	360
	TN	325	321	321	341	337	329	331	332	340	326	321	336	3960
15	TP	9	13	12	9	11	10	9	11	11	10	9	10	124
	FN	6	2	3	6	4	5	6	4	4	5	6	5	56
	FP	19	38	19	22	27	19	24	34	39	24	27	39	331
	TN	341	322	341	338	333	341	336	326	321	336	333	321	3989
16	TP	12	12	9	12	10	13	13	9	10	11	11	9	131
	FN	3	3	6	3	5	2	2	6	5	4	4	6	49
	FP	31	32	27	37	27	41	37	37	21	30	40	21	381
	TN	329	328	333	323	333	319	323	323	339	330	320	339	3939
17	TP	9	12	11	10	10	9	12	12	11	10	10	13	129
	FN	6	3	4	5	5	6	3	3	4	5	5	2	51
	FP	42	29	33	31	33	40	34	31	41	37	32	40	423
	TN	318	331	327	329	327	320	326	329	319	323	328	320	3897
18	TP	11	12	12	12	9	10	12	11	13	13	9	12	136
	FN	4	3	3	3	6	5	3	4	2	2	6	3	44
	FP	19	33	41	29	29	39	39	20	28	33	20	28	358
	TN	341	327	319	331	331	321	321	340	332	327	340	332	3962
19	TP	9	9	10	13	12	9	12	11	11	12	11	12	131
	FN	6	6	5	2	3	6	3	4	4	3	4	3	49
	FP	19	27	29	21	19	30	23	29	22	24	24	26	293
	TN	341	333	331	339	341	330	337	331	338	336	336	334	4027
20	TP	11	12	12	9	13	12	10	10	11	12	9	12	133
	FN	4	3	3	6	2	3	5	5	4	3	6	3	47
	FP	21	37	29	34	28	31	29	37	26	34	22	37	365
	TN	339	323	331	326	332	329	331	323	334	326	338	323	3955
21	TP	10	13	13	11	11	12	10	11	9	13	13	12	138
	FN	5	2	2	4	4	3	5	4	6	2	2	3	42
	FP	33	21	34	22	32	19	36	42	40	26	28	25	358
	TN	327	339	326	338	328	341	324	318	320	334	332	335	3962
22	TP	12	11	11	12	13	13	12	12	9	11	10	9	135
	FN	3	4	4	3	2	2	3	3	6	4	5	6	45
	FP	20	29	37	32	20	37	21	39	37	21	40	31	364
	TN	340	331	323	328	340	323	339	321	323	339	320	329	3956

Продовження таблиці И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**
23	TP	11	11	12	11	13	13	13	9	13	9	11	13	139
	FN	4	4	3	4	2	2	2	6	2	6	4	2	41
	FP	29	37	28	23	24	37	29	20	23	34	21	24	329
	TN	331	323	332	337	336	323	331	340	337	326	339	336	3991
24	TP	12	10	13	10	10	13	13	12	10	13	12	12	140
	FN	3	5	2	5	5	2	2	3	5	2	3	3	40
	FP	27	34	29	30	37	33	30	37	23	41	41	20	382
	TN	333	326	331	330	323	327	330	323	337	319	319	340	3938
25	TP	10	13	13	13	10	13	10	9	9	12	11	12	135
	FN	5	2	2	2	5	2	5	6	6	3	4	3	45
	FP	35	19	34	27	34	27	35	36	40	39	41	38	405
	TN	325	341	326	333	326	333	325	324	320	321	319	322	3915
26	TP	9	11	12	13	9	13	10	11	10	13	10	12	133
	FN	6	4	3	2	6	2	5	4	5	2	5	3	47
	FP	27	19	36	23	38	30	41	37	37	22	25	21	356
	TN	333	341	324	337	322	330	319	323	323	338	335	339	3964
27	TP	9	13	13	11	10	10	12	13	9	12	12	13	137
	FN	6	2	2	4	5	5	3	2	6	3	3	2	43
	FP	26	29	34	21	19	31	22	23	38	35	19	32	329
	TN	334	331	326	339	341	329	338	337	322	325	341	328	3991
28	TP	13	9	9	12	13	9	12	13	10	12	13	12	137
	FN	2	6	6	3	2	6	3	2	5	3	2	3	43
	FP	35	24	37	22	19	29	20	26	24	34	30	33	333
	TN	325	336	323	338	341	331	340	334	336	326	330	327	3987
29	TP	12	9	11	12	11	12	13	9	12	13	9	12	135
	FN	3	6	4	3	4	3	2	6	3	2	6	3	45
	FP	32	27	19	39	28	22	33	33	23	31	33	19	339
	TN	328	333	341	321	332	338	327	327	337	329	327	341	3981
30	TP	11	11	12	9	13	11	13	12	13	11	9	11	136
	FN	4	4	3	6	2	4	2	3	2	4	6	4	44
	FP	24	29	21	36	24	34	24	42	34	29	36	22	355
	TN	336	331	339	324	336	326	336	318	326	331	324	338	3965
31	TP	10	12	13	9	9	10	10	9	13	10	11	13	129
	FN	5	3	2	6	6	5	5	6	2	5	4	2	51
	FP	18	19	19	21	24	27	19	20	20	19	26	18	250
	TN	342	341	341	339	336	333	341	340	340	341	334	342	4070
32	TP	9	10	11	12	12	13	12	11	9	13	9	12	133
	FN	6	5	4	3	3	2	3	4	6	2	6	3	47
	FP	26	27	24	21	24	23	19	27	18	18	21	23	271
	TN	334	333	336	339	336	337	341	333	342	342	339	337	4049
33	TP	13	12	9	9	11	9	12	13	13	10	9	10	130
	FN	2	3	6	6	4	6	3	2	2	5	6	5	50
	FP	25	22	20	27	21	20	25	24	18	26	21	22	271
	TN	335	338	340	333	339	340	335	336	342	334	339	338	4049
34	TP	11	10	11	9	10	10	9	9	9	10	9	9	116
	FN	4	5	4	6	5	5	6	6	6	5	6	6	64
	FP	21	19	22	20	19	26	25	28	25	27	21	22	275
	TN	339	341	338	340	341	334	335	332	335	333	339	338	4045

Кінець таблиці И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**
35	TP	9	13	9	9	9	9	9	13	13	13	10	10	126
	FN	6	2	6	6	6	6	6	2	2	2	5	5	54
	FP	25	19	26	25	19	25	25	25	20	20	18	24	271
	TN	335	341	334	335	341	335	335	335	340	340	342	336	4049
36	TP	13	11	10	13	10	9	10	12	10	12	10	10	130
	FN	2	4	5	2	5	6	5	3	5	3	5	5	50
	FP	17	16	17	15	14	16	14	16	14	16	17	16	188
	TN	343	344	343	345	346	344	346	344	346	344	343	344	4132
37	TP	9	12	12	10	13	12	10	9	10	10	12	13	132
	FN	6	3	3	5	2	3	5	6	5	5	3	2	48
	FP	17	18	18	17	15	16	17	15	15	18	17	15	198
	TN	343	342	342	343	345	344	343	345	345	342	343	345	4122
38	TP	12	10	9	10	13	13	11	13	13	12	10	13	139
	FN	3	5	6	5	2	2	4	2	2	3	5	2	41
	FP	15	18	17	18	15	16	17	16	15	17	18	16	198
	TN	345	342	343	342	345	344	343	344	345	343	342	344	4122
39	TP	12	9	12	10	13	10	9	12	13	12	12	13	137
	FN	3	6	3	5	2	5	6	3	2	3	3	2	43
	FP	17	18	18	15	15	18	15	16	15	14	18	15	194
	TN	343	342	342	345	345	342	345	344	345	346	342	345	4126
40	TP	11	9	9	9	9	10	11	13	13	13	13	13	133
	FN	4	6	6	6	6	5	4	2	2	2	2	2	47
	FP	17	15	16	16	18	18	15	15	14	15	14	15	188
	TN	343	345	344	344	342	342	345	345	346	345	346	345	4132
41	TP	13	13	12	12	12	12	12	12	13	13	13	12	149
	FN	2	2	3	3	3	3	3	3	2	2	2	3	31
	FP	8	11	11	10	11	9	8	12	10	9	12	11	122
	TN	352	349	349	350	349	351	352	348	350	351	348	349	4198
42	TP	12	13	12	13	13	12	12	13	13	13	12	13	151
	FN	3	2	3	2	2	3	3	2	2	2	3	2	29
	FP	8	11	12	12	8	8	10	11	8	8	11	11	118
	TN	352	349	348	348	352	352	350	349	352	352	349	349	4202
43	TP	12	12	12	12	13	12	12	13	12	12	13	12	147
	FN	3	3	3	3	2	3	3	2	3	3	2	3	33
	FP	10	10	9	12	11	8	10	10	10	11	9	8	118
	TN	350	350	351	348	349	352	350	350	350	349	351	352	4202
44	TP	13	14	14	13	13	13	13	13	13	14	14	13	160
	FN	2	1	1	2	2	2	2	2	2	1	1	2	20
	FP	9	9	10	8	8	12	12	12	9	9	10	10	118
	TN	351	351	350	352	352	348	348	348	351	351	350	350	4202
45	TP	13	13	13	14	13	13	13	14	13	13	14	14	160
	FN	2	2	2	1	2	2	2	1	2	2	1	1	20
	FP	8	10	9	11	10	8	10	9	10	11	10	10	116
	TN	352	350	351	349	350	352	350	351	350	349	350	350	4204
46	TP	13	13	14	13	14	14	14	14	14	13	14	14	164
	FN	2	2	1	2	1	1	1	1	1	2	1	1	16
	FP	10	9	9	11	12	9	8	12	12	10	10	8	120
	TN	350	351	351	349	348	351	352	348	348	350	350	352	4200

Таблиця И.2

Результати ROC-аналізу для етапів

етап	$TPR = \frac{TP}{TP+FN} \cdot 100\%$	$FPR = \frac{FP}{TN+FP} \cdot 100\%$	$S_p = \frac{TN}{TN+FP} \cdot 100\%$:	$Precision = \frac{TP}{TP+FP}$	$Recall = \frac{TP}{TP+FN}$	$F1 = \frac{2 * Recall * Precision}{Recall + Precision}$	$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN}}$
1	79.44	7.52	92.48	0.31	0.79	0.44	0.46
2	74.44	8.56	91.44	0.27	0.74	0.39	0.41
3	77.78	8.56	91.44	0.27	0.78	0.41	0.43
4	76.67	9.24	90.76	0.26	0.77	0.38	0.41
5	72.78	8.77	91.23	0.26	0.73	0.38	0.40
6	73.33	9.21	90.79	0.25	0.73	0.37	0.39
7	69.44	8.31	91.69	0.26	0.69	0.38	0.39
8	70.00	8.75	91.25	0.25	0.70	0.37	0.38
9	77.78	8.36	91.64	0.28	0.78	0.41	0.43
10	75.00	8.50	91.50	0.27	0.75	0.40	0.41
11	73.33	8.73	91.27	0.26	0.73	0.38	0.40
12	72.22	8.24	91.76	0.27	0.72	0.39	0.40
13	72.22	7.85	92.15	0.28	0.72	0.40	0.41
14	70.56	8.33	91.67	0.26	0.71	0.38	0.39
15	68.89	7.66	92.34	0.27	0.69	0.39	0.40
16	72.78	8.82	91.18	0.26	0.73	0.38	0.39
17	71.67	9.79	90.21	0.23	0.72	0.35	0.37
18	75.56	8.29	91.71	0.28	0.76	0.40	0.42
19	72.78	6.78	93.22	0.31	0.73	0.43	0.44
20	73.89	8.45	91.55	0.27	0.74	0.39	0.41
21	76.67	8.29	91.71	0.28	0.77	0.41	0.43
22	75.00	8.43	91.57	0.27	0.75	0.40	0.42
23	77.22	7.62	92.38	0.30	0.77	0.43	0.45
24	77.78	8.84	91.16	0.27	0.78	0.40	0.42
25	75.00	9.38	90.63	0.25	0.75	0.38	0.40
26	73.89	8.24	91.76	0.27	0.74	0.40	0.41
27	76.11	7.62	92.38	0.29	0.76	0.42	0.44
28	76.11	7.71	92.29	0.29	0.76	0.42	0.44
29	75.00	7.85	92.15	0.28	0.75	0.41	0.43
30	75.56	8.22	91.78	0.28	0.76	0.41	0.42
31	71.67	5.79	94.21	0.34	0.72	0.46	0.46
32	73.89	6.27	93.73	0.33	0.74	0.46	0.46
33	72.22	6.27	93.73	0.32	0.72	0.45	0.45
34	64.44	6.37	93.63	0.30	0.64	0.41	0.40
35	70.00	6.27	93.73	0.32	0.70	0.44	0.44
36	72.22	4.35	95.65	0.41	0.72	0.52	0.52
37	73.33	4.58	95.42	0.40	0.73	0.52	0.52
38	77.22	4.58	95.42	0.41	0.77	0.54	0.54
39	76.11	4.49	95.51	0.41	0.76	0.54	0.54
40	73.89	4.35	95.65	0.41	0.74	0.53	0.53
41	82.78	2.82	97.18	0.55	0.83	0.66	0.66
42	83.89	2.73	97.27	0.56	0.84	0.67	0.67
43	81.67	2.73	97.27	0.55	0.82	0.66	0.66
44	88.89	2.73	97.27	0.58	0.89	0.70	0.70
45	88.89	2.69	97.31	0.58	0.89	0.70	0.70
46	91.11	2.78	97.22	0.58	0.91	0.71	0.71