МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

КАШТАЛЬЯН АНТОНІНА СЕРГІЇВНА

УДК 004.7:004.75:004.49:004.62

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

05.13.05 – комп'ютерні системи та компоненти

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Хмельницький – 2025

Дисертацією є рукопис.

Робота виконана в Хмельницькому національному університеті Міністерства освіти і науки України.

Науковий консультант:

доктор технічних наук, професор
Савенко Олег Станіславович,
професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету, м. Хмельницький;

Офіційні опоненти:

доктор технічних наук, професор
Мухін Вадим Євгенійович,
завідувач кафедри системного проектування Національного технічного університету України "Київський політехнічний інститут ім. Ігоря Сікорського", м. Київ;

доктор технічних наук, професор
Коваленко Андрій Анатолійович,
завідувач кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки;

доктор технічних наук, професор
Возна Наталія Ярославівна,
професор кафедри спеціалізованих комп'ютерних систем Західноукраїнського національного університету, м. Тернопіль.

Захист відбудеться «17» жовтня 2025 р. о 11^{00} годині на засіданні спеціалізованої вченої ради Д 70.052.06 у Хмельницькому національному університеті (29016, м. Хмельницький, вул. Кам'янецька, 112, ауд. 1-210 першого корпусу).

З дисертацією можна ознайомитися у бібліотеці Хмельницького національного університету (29016, м. Хмельницький, вул. Кам'янецька, 110/1).

Реферат оприлюднено «16» вересня 2025 р.

Вчений секретар
спеціалізованої вченої ради
к.т.н., доцент А.О. Нічепорук

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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., Бісвас Д., Ванг К., Віола В., Гнатюк С., Дудикевич В., Занг Ю., Золфахарі Ш., Ефенді М., Карпінський М., Кларк А., Кемпвел Р., Коваленко А., Корченко А., Корченко О., Летичевський О., Мілов О., Мухін В., Парк К., Ров Н., Сардана А., Саченко А., Сохор Т., Харченко В., Хофер В., Хохлачова Ю., Фенг М., Фергюсен-Вальтер К., Франко Д., Євсєєв С. 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. Метою дисертаційної роботи 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.

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.

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.

Наукова новизна одержаних 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.

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.

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: [8] - розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень; [4, 5] - розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик; [6, 7, 9] - розроблені математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для вибору наступних варіантів централізації; [2] - розроблено метод організації функціонування контролера прийняття рішень; [27] - метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками; [2] - розроблено метод організації функціонування мультикомп'ютерних систем; [3, 4] - 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: [15, 16, 20, 30, 31, 33, 34,] – запропонована концепція вирішення науково-прикладної проблеми; [20] - розроблено принцип і метод синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень; [10, 21, 32, 37] - розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик; [19] - розроблені математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи для вибору наступних варіантів централізації; [18] - розроблено метод визначення варіанту централізації в мультикомп'ютерних системах для вибору наступного варіанту централізації; [20, 21] - розроблено метод організації функціонування контролера прийняття рішень; [20, 21] - розроблено метод організації функціонування мультикомп'ютерних систем; [11, 12, 13, 14, 23, 28, 29,] - метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками; [1, 17, 22, 24, 25, 26, 35, 36] - розроблено метод виявлення ЗПЗ і КА; [38] – 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 [1 - 21], з яких 4 статті опубліковані в двох наукових журналах та індексовані у наукометричній базі Scopus [18 - 21,], 17 статей у фахових наукових виданнях України категорії Б [1 - 17]. Апробація засвідчена публікаціями 16 праць в матеріалах зарубіжних та українських конференцій [22 - 37], з яких 13 публікацій індексовано у наукометричній базі Scopus. Опубліковано одне свідоцтво про реєстрацію

авторського права на твір (програму) [38].

Структура дисертації. Дисертаційна робота складається з анотації, переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел та десяти додатків. Повний обсяг роботи містить 487 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.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, визначено об'єкт та предмет, мету і завдання дослідження, сформульовано науково-прикладну проблему, визначено наукову новизну та практичну цінність отриманих результатів. Вказано зв'язок роботи з науковими програмами та науково-дослідними роботами за місцем виконання роботи. Надано інформацію щодо кількості публікацій та апробації результатів дисертації.

У **першому розділі** проведено аналіз і дослідження обманних систем, мультикомп'ютерних систем антивірусних приманок та пасток та ефективності їх роботи.

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 пасками 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.

У **другому розділі** представлено концепцію, принцип синтезу МКС з АКПП та контролером прийняття рішень, концептуальну модель МКС з АКПП.

Згідно з аналізом поставленої задачі та сформованих вимог для вирішення проблеми з покращення функціонування МКС АКПП виявлення ЗПЗ і КА для забезпечення безпеки та захисту корпоративних мереж було розроблено концепцію, принцип синтезу та концептуальну модель таких систем

Концепція вирішення проблеми, що розглядається, 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 зловмисного програмного забезпечення та комп'ютерних атак 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.

Принцип синтезу МКС з АКПП та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА позначено символом $\mathfrak{P}$. Ним як відображенням з усієї множини мультикомп'ютерних систем $\mathfrak{C}$ сформовано підмножину систем $\mathfrak{S}$, для яких буде виконуватись вимога принципу $\mathfrak{P}$. Тобто, задане відображення формулою $\mathfrak{C} \overset{\mathfrak{P}}{\rightarrow} \mathfrak{S}$ формує клас систем із заданими принципом $\mathfrak{P}$ вимогами і потрібно деталізувати компоненти таких систем для подальшого їх синтезу.

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:

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

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. 1.

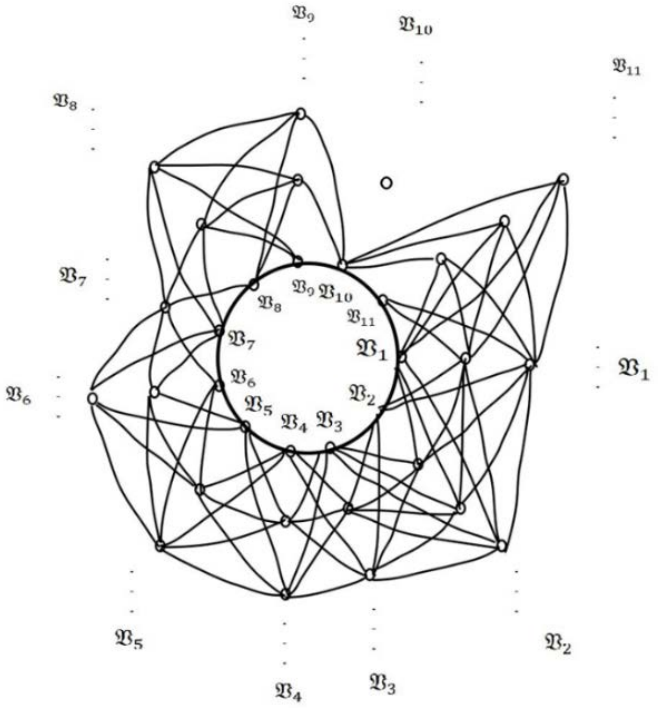

Рисунок 1 - Граф відображення визначальних характеристик
в архітектурі систем типу $\mathfrak{S}$

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.

В концептуальній моделі МКС з АКПП та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, архітектура якої віднесена до класу систем $\mathfrak{S}$, відображені елементи та компоненти, як складові частини архітектури.

Тому, введено підмножини для таких елементів та компонентів в архітектурі системи і задано загальну множину $\mathfrak{M}_{\mathfrak{S}}$ для них таким чином:

$$\mathfrak{M}_{\mathfrak{S}} = \bigcup_{i=1}^{n_{\mathfrak{M}_{\mathfrak{S}}}} \mathfrak{M}_i, \qquad (2)$$

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.

Введено 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. Таким чином, буде справедливе функційне відображення в множині підмножин $\mathfrak{P}(\mathfrak{M}_\mathfrak{S})$:

$$\mathfrak{P}(\mathfrak{M}_\mathfrak{S}) \xrightarrow{\mathfrak{F}} \mathfrak{P}(\mathfrak{M}_\mathfrak{S}). \quad (3)$$

Співвідношення, яке задане формулою (3), 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. 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:

$$\mathfrak{P}_\mathfrak{f}(\mathfrak{M}_\mathfrak{S}) \in \mathfrak{P}(\mathfrak{M}_\mathfrak{S}), \quad (4)$$

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)-(4) задано архітектуру мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень алгебраїчною системою типу $\tau = (\alpha, \beta)$ так:

$$\mathfrak{A}_\mathfrak{S} = \langle \mathfrak{P}(\mathfrak{M}_\mathfrak{S}), \mathfrak{F}, \mathfrak{P}_\mathfrak{M} \rangle, \quad (5)$$

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 $\tau = (\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_\mathfrak{S})}, 1)$; $\mathfrak{n}_{\mathfrak{P}(\mathfrak{M}_\mathfrak{S})}$ – кількість елементів в множині $\mathfrak{P}(\mathfrak{M}_\mathfrak{S})$.

Згідно принципу синтезу $\mathfrak{P}$ систем класу $\mathfrak{S}$, деталізації множин і їх елементів, обмежень на елементи в множинах, що випливають з вимог принципу синтезу $\mathfrak{P}$, та згідно визначень і відображень концептуальну модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ архітектури МКС з АКПП та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА задано так:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$9)\ \forall\ \mathfrak{g}_1,\mathfrak{g}_2\colon\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{g}_1}\cap\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{E},\mathfrak{K},\mathfrak{T},\mathfrak{g}_2}=\emptyset;\ \mathfrak{g}_1=1,2,3,4;\ \mathfrak{g}_2=1,2,3,4;\ \mathfrak{g}_1\neq\mathfrak{g}_2,\ (6)$$

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; $\mathfrak{M}_{\mathrm{i}_1}$ - i_1 – та підмножина для певних елементів та компонентів в архітектурі системи; $\mathrm{i}_1=1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathfrak{S}}}$ – кількість підмножин; $\mathfrak{m}_{\mathrm{i}_1,\mathrm{I}}$ – i_1-елемент $\mathfrak{M}_{\mathrm{i}_1}$ підмножини; $\mathrm{I}=1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathrm{i}_1}}$; $\mathfrak{n}_{\mathfrak{M}_{\mathrm{i}_1}}$ – кількість елементів підмножини $\mathfrak{M}_{\mathrm{i}_1}$; $\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$ – множина векторів; елемент $\mathfrak{w}_{\mathrm{j}}\in\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})$; $\mathrm{j}=1,2,\dots,\mathfrak{n}_{\mathfrak{W}(\mathfrak{M}_{\mathfrak{S}})}$; $\mathfrak{w}_{\mathrm{j},\mathrm{i}_2}$ – $(\mathrm{j},\mathrm{i}_2)$ – координата вектору $\mathfrak{w}_{\mathrm{j}}$; $\mathrm{i}_2=1,2,\dots,\mathfrak{n}_{\mathfrak{M}_{\mathfrak{v}}}$; $\mathfrak{G}_2$ – 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 $\mathfrak{S}$; $\mathfrak{m}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1,\mathrm{I}_2}$ – I_2-елемент множини типових компонент $\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}$; $\mathrm{I}_2=1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{K},\mathfrak{T},1}}$ – 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; $\mathfrak{v}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K},\mathfrak{l}_3,1}$ - значення номеру компоненти за списком системи; $\mathfrak{l}_3 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$; $\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},\mathfrak{E},\mathfrak{K}}}$ – 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 $\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3} = \left\{\mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,1}, \mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,2}, \dots, \mathfrak{f}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3,\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}}}\right\}$; $\mathfrak{l}_4 = 1,2,\dots,\mathfrak{n}_{\mathfrak{M}^{\mathfrak{S}}_{\mathfrak{V},2,3}}$; $\mathfrak{n}_{\mathfrak{F}^{\mathfrak{S},\mathfrak{V}}_{\mathfrak{V},2,3}}$ - 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 (6) 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 (6) 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. Розглянутоо 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 (6)) подано на рис. 2.

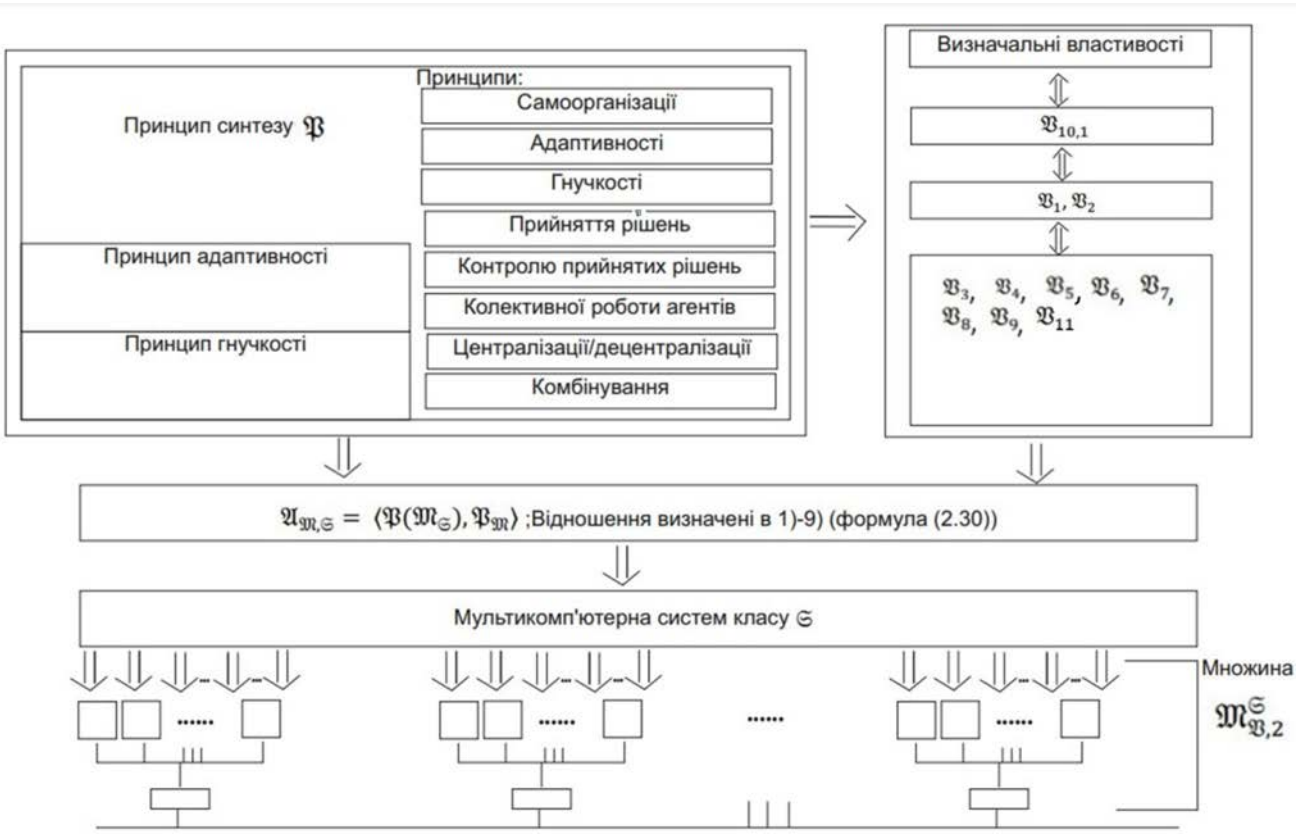

Рисунок 2 – Співвіднесення елементів та компонентів концептуальної моделі $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$, мультикомп’ютерних систем класу $\mathfrak{S}$ та середовища функціонування систем

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 контролеру 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 ефективності 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.

У **третьому розділі** визначено математичні моделі та критерії оцінювання варіантів централізації в архітектурі МКС, метод та правила визначення наступного варіанту ценалізації в архітектурі МКС.

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.

Правила формування варіантів централізації для мультикомп'ютерних систем задано множиною правил:

$$M_{Pr} = \left\{ m_{Pr,1}, m_{Pr,2}, \dots, m_{Pr,N_{M_{Pr}}} \right\}, \quad (7)$$

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}.

Цільову функцію оцінювання наступних варіантів централізації для вибору одного з варіантів з чотирьох типів централізації задано таким чином:

$$\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}} \left(\mathrm{f}_{1,\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{p}_{1,\mathrm{kr}}^{\mathrm{centr}}\right), \mathrm{f}_{2,\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{p}_{2,\mathrm{kr}}^{\mathrm{centr}}\right), \dots, \mathrm{f}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}},\mathrm{kr}}^{\mathrm{centr}}\left(\mathrm{p}_{\mathrm{N}_{\mathrm{F}_{\mathrm{kr}}^{\mathrm{centr}}},\mathrm{kr}}^{\mathrm{centr}}\right), \mathrm{F}_{\mathrm{var}}^{\mathrm{centr}}(\mathrm{u}), \mathrm{F}_{\mathrm{var}}^{\mathrm{centr}}(\mathrm{v}) \right) \rightarrow \min, \quad (8)$$

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 $\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}} = \left(\mathrm{p}_{1,\mathrm{i,kr}}^{\mathrm{centr}}, \mathrm{p}_{2,\mathrm{i,kr}}^{\mathrm{centr}}, \dots, \mathrm{p}_{\mathrm{N}_{\mathrm{p}_{\mathrm{i,kr}}^{\mathrm{centr}}},\mathrm{i,kr}}^{\mathrm{centr}}, \mathrm{V}_{\mathrm{Pr,u}}, \mathrm{V}_{\mathrm{Pr,v}}, A_{1,u}^{\mathfrak{S}}, A_{1,v}^{\mathfrak{S}}, A_{2,u}^{\mathfrak{S}}, A_{2,v}^{\mathfrak{S}} \right)$, 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; $\mathrm{V}_{\mathrm{Pr,u}}, \mathrm{V}_{\mathrm{Pr,v}}$ – вектори, які задаються координатами; $\mathrm{F}_{\mathrm{var}}^{\mathrm{centr}}(\mathrm{v})$ – функція, значенням якої є номер одного з типів централізації в системі в поточний момент часу або номер досліджуваного типу; $\mathrm{A}_{1,\mathrm{u}}^{\mathfrak{S}}$ – підмножина активних компонент центру системи при u – тому поточному номеру варіанту централізації; $\mathrm{A}_{2,\mathrm{u}}^{\mathfrak{S}}$ – множина компонент системи, які в поточний момент часу не є компонентами центру системи при u – тому поточному номеру варіанту централізації; $\mathrm{A}_{1,\mathrm{v}}^{\mathfrak{S}}$ – підмножина активних компонент центру системи для v – номеру досліджуваного варіанту централізації в системі, який може бути після u – того номеру варіанту централізації; $\mathrm{A}_{2,\mathrm{v}}^{\mathfrak{S}}$ – 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.

Правила з множини правил M_{Pr} розділено 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.

Правила з множини правил $\mathrm{M_{Pr}}$, згідно яких буде визначатись наступний варіант централізації в системах класу $\mathfrak{S}$, з урахуванням показників:

$m_{Pr,s} =$ $(\mathrm{s} = 1, \dots, 4)$ $\forall A^{\mathfrak{S}}$: $((\mathrm{g}_1^{\mathrm{centr}} = \mathrm{true})\ and\ (\mathrm{g}_2^{\mathrm{centr}} = \mathrm{false})\ and\ (\mathrm{g}_3^{\mathrm{centr}} = \mathrm{false}))\ and$ $(\mathrm{V_{Pr,potochn}} \neq \mathrm{V_{Pr,nast}}: \exists\ \mathrm{j}\ \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, \mathrm{potochn}) \neq \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, \mathrm{nast}))\ and$ $(\{\mathrm{m_{\mathfrak{B}_2,centr,v_1},}_{j_1}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_2},}_{j_2}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_3},}_{j_3}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_4},}_{j_4}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_5},}_{j_5}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_6},}_{j_6}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_7},}_{j_7}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_8},}_{j_8}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_9},}_{j_9}\} \cup \{\mathrm{m_{\mathfrak{B}_2,centr,v_{10}},}_{j_{10}}\})$ and $(\mathrm{V_{Pr,potochn}} = \mathrm{V_{Pr,N_{V_{Pr}}}}$, тобто $\forall\ \mathrm{j}: \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, \mathrm{potochn}) = \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, \mathrm{N_{V_{Pr}}}))\ and\ (\{p_{Pr,1}\} \cup \{p_{Pr,2}\} \cup \dots \cup \{p_{Pr,\mathrm{N}_{P_{Pr}}}\})$ and $(\{A_{1,1}^{\mathfrak{S}}, A_{1,2}^{\mathfrak{S}}, \dots, A_{1,N_{1,A^{\mathfrak{S}}}}^{\mathfrak{S}}\} \cup \{A_{2,1}^{\mathfrak{S}}, A_{2,2}^{\mathfrak{S}}, \dots, A_{2,N_{2,A^{\mathfrak{S}}}}^{\mathfrak{S}}\})$ and $(0 \leq \mathrm{F_{kr}^{centr}} \leq 1)\ and$ $(\mathrm{F_{OD}^{centr}}(\mathrm{V_{Pr,nast2}}, M_{\mathrm{V_{Pr}}}, P'_{Pr}) \geq \mathrm{F_{OD}^{centr}}(\mathrm{V_{Pr,nast1}}, M_{\mathrm{V_{Pr}}}, P'_{Pr}))\ and\ (0 \leq \mathrm{F_{OD}^{centr}}(\mathrm{V_{Pr,nast}}, M_{\mathrm{V_{Pr}}}, P'_{Pr}) \leq 1)\ and\ ((\mathrm{F_{OD,t}^{centr}}(\mathrm{V_{Pr,nast}}) = 0)$ or $\frac{t-(\mathrm{F_{OD,t}^{centr}}(\mathrm{V_{Pr,nast}})}{t} \leq e_1^{centr})$ and $((\mathrm{F_{OD,k}^{centr}} = 0)$ or $(\frac{\mathrm{F_{OD,k}^{centr}}}{\mathrm{F_{OD,z}^{centr}}} \leq e_1^{centr}))$ and $(\mathrm{N_A^{centr}} \geq 2)$ and $(\mathrm{F_P^{centr}}(\mathrm{V_{Pr,potochn}}, \mathrm{V_{Pr,nast}}, M_{\mathrm{V_{Pr}}}, P_{Pr}, A^{\mathfrak{S}}) = 1)\ and$ $(\frac{\mathrm{N_A^{centr}}}{\mathrm{N}} \geq e_1^{centr})$ and $((\mathrm{n_{s,potochn}^{centr}} = \mathrm{n_{s,nast}^{centr}})\ or\ ((\mathrm{n_{s,potochn}^{centr}} \neq \mathrm{n_{s',nast}^{centr}}$ and $\mathrm{s} = 1, \dots, 4$ and $s' = 1, \dots, 4\ and\ s' \neq \mathrm{s})\ and\ \mathrm{n_{s',nast}^{centr}}))\ and\ (\frac{\mathrm{k_m}}{\mathrm{N}_{\mathrm{M_{str,nast}^{centr}}} \sum_{m=1} k_m} \leq e_2^{centr})$ $\Rightarrow \mathrm{V_{Pr,nast}}$;

$m_{Pr,5} =$ $\forall A^{\mathfrak{S}}$: $((\mathrm{g}_1^{\mathrm{centr}} = \mathrm{false})\ and\ (\mathrm{g}_2^{\mathrm{centr}} = \mathrm{true})\ and\ (\mathrm{g}_3^{\mathrm{centr}} = \mathrm{false}))\ \Rightarrow m_{Pr,s}\ and\ \mathrm{V_{Pr},}_{nast'} \neq \mathrm{V_{Pr,nast}}: \exists\ \mathrm{j}\ \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, nast') \neq \mathrm{F_{Pr}}(\mathrm{m_{\mathfrak{B}_2,centr,v_l,j}}, \mathrm{nast})) \Rightarrow \mathrm{V_{Pr,nast}}$;

$m_{Pr,6} =$ $\forall A^{\mathfrak{S}}$: $((\mathrm{g}_1^{\mathrm{centr}} = \mathrm{false})\ and\ (\mathrm{g}_2^{\mathrm{centr}} = \mathrm{false})\ and\ (\mathrm{g}_3^{\mathrm{centr}} = \mathrm{true}))\ and$ $(e_3^{centr} > 2)$ and $mod\ (m_{Pr,1}\ or\ m_{Pr,2}\ or\ m_{Pr,3}\ or\ m_{Pr,4}\ or\ m_{Pr,5})$, (9)

де g_l^{centr} – група правил ($l = 1,2,3$); $\mathrm{m_{Pr,i}}$ – і-те правило вибору варіанту централізації в мультикомп'ютерних системах; $\mathrm{i} = 1,2, \dots, \mathrm{N_{M_{Pr}}}$; $\mathrm{N_{M_{Pr}}}$ – кількість правил в множині правил $\mathrm{M_{Pr}}$; де l – кількість множин ($l = 1,2, \dots 10$); j_l-тий елемент в множині $M_{\mathfrak{B}_2,centr,l}$; i – номер стану системи; $V_{Pr,potochn}$ – вектор, який задає стан системи в поточний момент часу і наявний в матриці станів $\mathrm{M}_{V_{Pr}}$; $\mathrm{M}_{V_{Pr}}$ – 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.

Основні кроки методу визначення наступного варіанту централізації в системах класу $\mathfrak{S}$: В них враховано розроблены правила, перші 4 правила типові, 5 і 6 для опрацювання виняткових ситуацій, не вирішених першими 4

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 $m_{Pr,s}$ ($\mathrm{s} = 1, \dots, 4$) 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 контролеру 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.

У **четвертому розділі** представлено метод організації функціонування контролера прийняття рішень та метод організації функціонування мультикомп'ютерних систем.

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.

Функціонування контролера прийняття рішень в архітектурі систем класу $\mathfrak{S}$ 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. Розглянуто місце контролера прийняття рішень в архітектурі систем класу $\mathfrak{S}$ та його завдання.

Центр системи взаємодіє з контролером прийняття рішень згідно схеми зображеної на рис. 3.

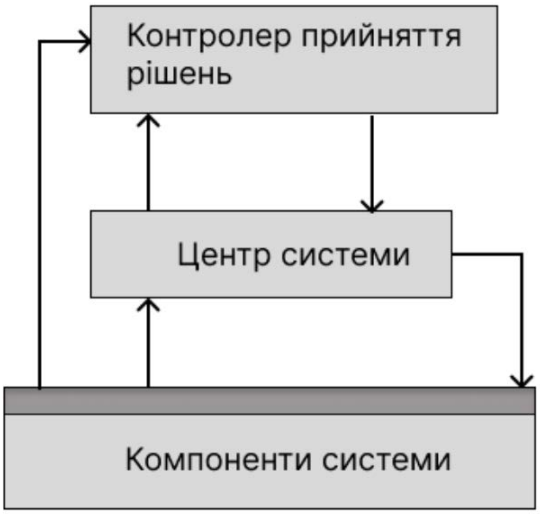

Рисунок 3 - Схема взаємодії контролера прийняття рішень та центру системи

Завдання, які можуть виконувати системи класу $\mathfrak{S}$, задамо множиною завдань системи $M_{pz}^{\mathfrak{S}}$ так:

$$M_{pz}^{\mathfrak{S}} = \left\{ m_{pz,1}^{\mathfrak{S}}, m_{pz,2}^{\mathfrak{S}}, \dots, m_{pz,N_{M_{pz}^{\mathfrak{S}}}}^{\mathfrak{S}} \right\}, \quad (10)$$

де $m_{pz,i}^{\Subset}$ – і-те завдання; $i = 1,2,\dots,N_{M_{pz}^{\Subset}}$; $N_{M_{pz}^{\Subset}}$ – кількість завдань, які може виконувати система.

Задано 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 задано так:

$$F_{kr}^{m_{pz,i}^{\Subset}}\left(f_{1,kr}^{m_{pz,i}^{\Subset}}\left(p_{1,kr}^{m_{pz,i}^{\Subset}}\right), f_{2,kr}^{m_{pz,i}^{\Subset}}\left(p_{2,kr}^{m_{pz,i}^{\Subset}}\right), \dots, f_{N_{F_{kr}^{m_{pz,i}^{\Subset}}},kr}^{m_{pz,i}^{\Subset}}\left(p_{N_{F_{kr}^{m_{pz,i}^{\Subset}}},kr}^{m_{pz,i}^{\Subset}}\right)\right) \to \min, \qquad (11)$$

де $m_{pz,i}^{\Subset}$ – і-те завдання; $i = 1,2,\dots,N_{M_{pz}^{\Subset}}$; $N_{M_{pz}^{\Subset}}$ – кількість завдань, які може виконувати система; $f_{j,kr}^{m_{pz,i}^{\Subset}}\left(p_{j,kr}^{centr}\right)$ – j - та функція, що задає обчислення значення j – того критерію; $j = 1,2,\dots,N_{F_{kr}^{m_{pz,i}^{\Subset}}}$; $p_{j,kr}^{m_{pz,i}^{\Subset}}$ – вектор, координатами якого є параметри j – того критерію та варіант виконання завдання; $N_{F_{kr}^{m_{pz,i}^{\Subset}}}$ – кількість аргументів функції $F_{kr}^{m_{pz,i}^{\Subset}}$ та кількість векторів $p_{j,kr}^{m_{pz,i}^{\Subset}}$.

Визначено критерії в загальному випадку так:

$$f_{j,kr}^{m_{pz,i}^{\Subset}}\left(p_{1,j,kr}^{m_{pz,i}^{\Subset}}, p_{2,j,kr}^{m_{pz,i}^{\Subset}}, \dots, p_{N_{p_{j,kr}^{m_{pz,i}^{\Subset}}},j,kr}^{m_{pz,i}^{\Subset}}\right) \to [0,1], \qquad (12)$$

де $p_{k,j,kr}^{m_{pz,i}^{\Subset}}$ – k-та координата вектору $p_{j,kr}^{m_{pz,i}^{\Subset}}$ показників для критерію $f_{j,kr}^{m_{pz,i}^{\Subset}}$; $k = 1,2,\dots,N_{p_{j,kr}^{m_{pz,i}^{\Subset}}}$; $N_{p_{j,kr}^{m_{pz,i}^{\Subset}}}$ – кількість координат вектору $p_{j,kr}^{m_{pz,i}^{\Subset}}$ показників для критерію $f_{j,kr}^{m_{pz,i}^{\Subset}}$.

Критерії включають 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 належать числовому відрізку $[0,1]$. Для кожного розглядуваного варіанту цільова функція оцінювання наступних варіантів виконання завдання для вибору одного з варіантів мінімізується за рахунок наявних в критеріях параметрів. Таким чином, отримані цільові функції $F_{kr}^{m_{pz,i}^{\Subset}}$ для оцінювання наступних варіантів виконання завдання визначають значення для варіантів, які розглядатиме контролер прийняття рішень.

Задано правила формування стратегії вибору наступного варіанту виконання завдання контролером прийняття рішень так:

$$P_{str}^{1}: s_{kontr,i}^{\Subset} \wedge s_{kontr,j}^{\Subset} \wedge s_{kontr,k}^{\Subset}, \forall i = 1,2,3,4, j = 5,6,7,8,9,10, k = 11,12,13,14;$$

$$P_{str}^{21}: s_{kontr,i}^{\Subset} \wedge s_{kontr,j}^{\Subset}, \forall i = 1,2,3,4, j = 5,6,7,8,9,10;$$

$$P_{str}^{22}: s_{kontr,i}^{\Subset} \wedge s_{kontr,k}^{\Subset}, \forall i = 1,2,3,4, k = 11,12,13,14;$$

$$P_{str}^{23}: s_{kontr,k}^{\Subset} \wedge s_{kontr,j}^{\Subset}, \forall j = 5,6,7,8,9,10, k = 11,12,13,14;$$

$$P_{str}^{3}: s_{kontr,i}^{\Subset}, \forall i = 1,2,\dots,14, \quad (13)$$

де $.s_{kontr,i}^{\Subset}$ – i-та стратегія з множини стратегій вибору наступного варіанту виконання завдання контролером прийняття рішень; $i = 1,2,\dots,N_{S_{kontr}^{\Subset}}^{str}$; $N_{S_{kontr}^{\Subset}}^{str}$ – загальна кількість стратегій

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 $m_{pz,i}^{\Subset}$ $(i = 1,2,\dots,N_{M_{pz}^{\Subset}}$; $N_{M_{pz}^{\Subset}}$ – кількість завдань, які може виконувати система), j-тий варіант $m_j^{m_{pz,i}^{\Subset}}$ виконання i-того завдання $m_{pz,i}^{\Subset}$ $(j = 1,2,\dots,N_{M_{vvp}^{m_{pz,i}^{\Subset}}}^{\Subset}$; $N_{M_{vvp}^{m_{pz,i}^{\Subset}}}^{\Subset}$ – загальна кількість варіантів виконання i-того завдання $m_{pz,i}^{\Subset})$ (формула (4.2)), k-тий показник $v_{m_j^{m_{pz,i}^{\Subset}},k}^{pdvz}$ характеристики попереднього досвід з використання варіанту $m_j^{m_{pz,i}^{\Subset}}$ виконання завдання $m_{pz,i}^{\Subset}$ $(k = 1,2,\dots,N_{v_{m_j^{m_{pz,i}^{\Subset}}}^{pdvz}}^{\Subset}$; $N_{v_{m_j^{m_{pz,i}^{\Subset}}}^{pdvz}}^{\Subset}$ – загальна кількість показників, які характеризують попередній досвід з використання варіанту $m_j^{m_{pz,i}^{\Subset}}$ виконання завдання $m_{pz,i}^{\Subset})$, множини

$M^{pdvz}_{v^{pdvz}_{M^{m^{\Subset}_{pz}}_{vvp}}}$ попереднього досвіду, значення цільової функції $F^{m^{\Subset}_{pz,i}}_{kr}$ для розглядуваних варіантів виконання завдання, вектор $v^{p^{n^{\Subset}}}_{t}$ врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи, вектор $v^{\Subset}_{t}$стану функційної та кібербезпеки системи, вектор $v^{z^{n^{\Subset}}}_{t}$ подання зв'язків для кожної компоненти, вектор $v^{z^{n^{\Subset}}}_{t,z}$ повноти зв'язків, 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);

6) вибір випадковим чином та застосування одного з правил формування стратегії вибору наступного варіанту виконання завдання контролером прийняття рішень;

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.

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 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 $v^{p^{n^{\Subset}}}_{t}$;

3) отримання даних на виконання вказівок від центру системи та контролера прийняття рішень для формування вектору $v^{p^{n^{\Subset}}}_{t}$ врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи та вектору $v^{\Subset}_{t}$ стану функційної та кібербезпеки системи;

4) отримання даних на виконання вказівок від центру системи та контролера прийняття рішень для формування вектору $v^{z^{n^{\Subset}}}_{t}$ подання зв'язків для кожної компоненти, вектору $v^{z^{n^{\Subset}}}_{t,z}$ повноти зв'язків;

5) виявлення події в корпоративній мережі, яка викликана зовнішніми і внутрішніми впливами, її ідентифікація та здійснення вибору завдань з множини завдань системи $M_{pz}^{\Subset}$ 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 та стану функційної та кібербезпеки системи 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.

У **п'ятому розділі** розроблено методи виявлення ЗПЗ та КА в корпоративних мережах МКС АКПП

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.

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.

Приманка позиціонується як інтелектуальний агент. 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. Робота приманки оптимізується таким чином, щоб забезпечити максимум цільової функції винагороди при тривалій роботі приманки. 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:

$$C_R = \frac{R_{t+1} + R_{t+2} + \dots + R_{t+n}}{n} = \frac{1}{n}\sum_{i=1}^{n} R_{t+i}, \tag{14}$$

де R_{t+i} – значення функції винагороди на i-ому кроці; n – кількість кроків, на яких визначається інтегральна цільова функція 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:

$$R_t = p_r \cdot k_r r - p_w \cdot w, \tag{15}$$

де p_r – ймовірність винагороди; p_w – ймовірність стягнення; r – винагорода; k_r – коефіцієнт, який враховує час виявлення; w – число, на яке зменшується винагорода.

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. В роботі розглянуто типові аріхтектури приманок з урахуванням типових атак в корпоративних мережах.

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 здійснено на основі кластеризації їх поведінки, тобто часових рядів атак, які належать зловмисникам. Виявлення патернів атак включає такі етапи:

1) формування часового ряду з даних, зібраних МКС АКПП 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 Ci та Cj 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 $C_j = \{\mathbf{y}_{j1}, \mathbf{y}_{j2}, \ldots \mathbf{y}_{jm}\}$:

$$d_{ij} = d(C_i, C_j) = \frac{\sum_{a=1}^{m}\sum_{b=1}^{n} d(\mathbf{y}_{ia}, \mathbf{y}_{jb})}{|C_i \times C_j|}, \quad a \neq b \qquad (16)$$

.

в) визначення інтегрального критерію відстаней між об'єктами всередині кластера:

$$J = \frac{\sum_{i=1}^{l} d(C_i)}{l}, \qquad (17)$$

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 Ci.

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; 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:

$$\arg\min_{\mathbf{x} \in E} \sum_{i=1}^{n} d_{dtw}^2 \left(\bar{\mathbf{y}}^{(k)}, \mathbf{y}_i^{(k)}\right) \qquad (18)$$

.

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 $\{\mathbf{y}^{-(1)}, \mathbf{y}^{-(2)}, \cdots \mathbf{y}^{-(N_k)}\}$ 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.

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).

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.

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.

Таким чином, розроблено новий метод виявлення ЗПЗ та КА, 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.

У шостому розділі представлено реалізацію прототипу МКС АКПП, результати її застосування на практиці та методику оцінювання ефективновсті роботи МКС АКПП.

Важливими характеристиками в контексті синтезованих систем певного класу та призначення є їх стійкість та рівновага. Було введено три цільові функції $\mathfrak{F}_i^{\mathfrak{E}}$ $(i = 1,2,3)$, які характеризують відповідно стійкість, рівновагу та результат виконання завдання спеціалізованим функціоналом системи. Результат виконання кожної з цих функцій відображається в проміжку [0;1]. Середньоарифметичні значення цих трьох функцій встановлюють три коефіцієнти для характеристики системи:

$$\mathfrak{k}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}} = \frac{\sum_{j=1}^{n_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}} \mathfrak{F}_i^{\mathfrak{E}}(t_j)}{n_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}}, \tag{19}$$

де t_j – час від початку функціонування системи; j – індекс для часу, що відображає j – тий момент фіксування часу в системі; $j = 1,2,\dots,n_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$; $n_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}$ – 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.

Введено інтегрований показник характеристики системи, в якому відображені коефіцієнти рівнів стійкості, рівноваги та результату виконання завдання спеціалізованим функціоналом системи, а також кількість компонентів системи, так:

$$\mathfrak{k}_{\mathfrak{J}}^{\mathfrak{E}} = \frac{\sum_{j=1}^{n_{\mathfrak{J}}^{\mathfrak{E}}} \mathfrak{k}_{\mathfrak{F}_i^{\mathfrak{E}}}^{\mathfrak{E}}}{n_{\mathfrak{J}}^{\mathfrak{E}}} \cdot \frac{n_1}{n_2}, \tag{20}$$

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 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: $\mathfrak{k}^{\mathfrak{E}}_{\mathfrak{F}^{\mathfrak{E}}_{\mathfrak{d}_1}} = 0{,}78452;\ \mathfrak{k}^{\mathfrak{E}}_{\mathfrak{F}^{\mathfrak{E}}_{\mathfrak{d}_2}} = 0{,}69433;\ \mathfrak{k}^{\mathfrak{E}}_{\mathfrak{F}^{\mathfrak{E}}_{\mathfrak{d}_3}} = 0{,}91521;\ \mathfrak{n}_1 = 100;\ \mathfrak{n}_2 = 120;\ \mathfrak{n}^{\mathfrak{E}}_{\mathfrak{F}^{\mathfrak{E}}_{\mathfrak{d}_i}} = 50.$ Значення інтегрального коефіцієнту $\mathfrak{k}^{\mathfrak{E}}_{\mathfrak{J}} = 0{,}66502.$ 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 $\mathfrak{k}^{\mathfrak{E}}_{\mathfrak{J}} = 0{,}64892.$

Було проведено експеримент для аналізу впливу та адекватності критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи. Результати експерименту підтверджують доцільність застосування контролера прийняття рішень в архітектурі системи. Також, проведено експеримент, завданнями якого були 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. Проведений експеримент підтверджує стійкість системи з контролером прийняття рішень. 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. у випадку використання контролера прийняття ріщень, значення цільової функції для всіх розглядуваних варіантів на 50% менше порівняно з варіантом без контролера. За рахунок використаннння контролера прийняття рішень досягнуто на приблизно 10% підбір вдалих варіантів для перебудови та часу на їх виконання.

Завданнями наступного експерименту було 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. Експерименти було проведено для двох випадків (серій): варіант системи, в якому реалізовано контролер прийняття рішень; варіант системи з одним центром без контролера прийняття рішень. 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.

Експеримент щодо дослідження можливостей використання розробленої МКС для виявлення метаморфних вірусів підтвердив доцільність запропонованого рішення. Також, було проведено експеримент для дослідження розробленого підходу щодо кластеризації схожих зловмисників МКС. Із зібраних даних приманок МКС 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. При навчанні згорткового автоенкодера використовувались запропоновані функції втрат відновлення декодером та запропоновані міри подібності сегментів часових рядів.

Для оцінювання МКС АКПП, необхідного для встановлення досягнення мети дослідження, яка полягає в покращенні функціонування МКС АКПП 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 було проведено експеримент. Ефективність оцінено на основі мультиплікативного E_m та адитивного E_a критеріїв, які включають ряд критеріїв оцінювання обманних технологій, які наявні в системах. 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. 1 з врахуванням кількості розгорнутих приманок і пасток для систем.

Таблиця 1

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.

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.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

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

1. 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.
2. Каштальян А. С. Методи організації функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток в корпоративних мережах. *Measuring and computing devices in technological processes.* № 1. 2025. С. 160–171. DOI: https://doi.org/10.31891/2219-9365-2025-81-19.
3. Каштальян А. С. Метод виявлення зловмисного програмного забезпечення та комп'ютерних атак мультикомп'ютерними системами антивірусних комбінованих приманок та пасток. *Herald of Khmelnytskyi National University. Technical Sciences*. № 349(2). 2025, С. 346-352. https://doi.org/10.31891/2307-5732-2025-349-50.
4. 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/.
5. 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.
6. 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.

7. 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, 2024. p. 386–393, DOI: https://doi.org/10.31891/2219-9365-2024-80-46.

8. 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.* № 4. 2023. С. 265–272. DOI: https://doi.org/10.31891/2219-9365-2023-76-35.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

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:

18. 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***).

19. 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***).

20. 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).

21. 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).

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.

АНОТАЦІЇ

Каштальян А. С. Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах. – *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.

Дисертація присвячена вирішенню актуальної науково-технічної проблеми розроблення елементів теорії та практики синтезу мультикомп'ютерних систем комбінованих антивірусних приманок і пасток для забезпечення безпеки та захисту корпоративних мереж.

В роботі 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 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.

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

Kashtalian A. S. Elements of the Theory and Practice of Creating Multicomputer Systems of Combined Anti-virus Baits and Traps in Corporate Networks. – *On the rights of the Manuscript.*

The thesis 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.

The dissertation is devoted to the solution of the actual scientific and technical problem of development of creating multi-computer systems of combined antivirus baits and traps to ensure the security and protection of corporate networks.

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.

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