ВІДГУК

офіційного опонента, доктора технічних наук, професора,
завідувача кафедри системного проектування
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Мухіна Вадима Євгенійовича
про дисертаційну роботу Каштальян Антоніни Сергіївни
«Елементи теорії та практики створення мультикомп'ютерних систем
комбінованих антивірусних приманок і пасток в корпоративних мережах»,
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми дослідження та зв'язок з науковими програмами, планами та темами.

В сучасних умовах стрімкого розвитку цифрових технологій корпоративні мережі залишаються одним із привабливих об'єктів для здійснення цілеспрямованих атак з боку зловмисників. Основною метою таких дій є отримання несанкціонованого доступу до інформаційних ресурсів, завдання економічної або репутаційної шкоди, а також викрадення конфіденційних даних. Попри активне впровадження методів, засобів та систем для протидії комп'ютерним атакам та зловмисному програмного забезпеченню, ефективне забезпечення безпеки корпоративних мереж залишається актуальною та складною задачею. Однією з основних причин збереження вразливості корпоративних мереж є передбачуваність дій засобів захисту, які зазвичай реагують на атаки з використанням типових сценаріїв або команд. Це дозволяє зловмисникам на етапі розвідки ідентифікувати захисні механізми, які використовуються, виявити їх слабкі місця та обійти системи захисту. Додаткову складність становить використання відкритих джерел інформації, з яких зловмисники отримують відомості про загальні

принципи функціонування захисних систем, а також швидкий розвиток інструментарію атак.

Для підвищення ефективності захисту корпоративних мереж застосовуються обманні системи, зокрема приманки, пастки, хибні цілі та інші обманні об'єкти, призначені для збору даних про дії зловмисинка та введення зловмисника в оману, викривляючи його уявлення про архітектуру мережі. Такі системи спрямовані на збільшення витрат ресурсів та часу зловмисника, одночасно зменшуючи ймовірність успішного завершення атаки. Разом з тим ефективність обманних систем значною мірою залежить від їх здатності імітувати реальне функціонування систем, залишаючись при цьому непомітними. Такі системи повинні діяти автономно, без постійного втручання адміністратора, бути адаптивними, самоорганізованими, здатними реагувати нестандартно на події, що відбуваються в мережі.

Зазначені особливості обумовлюють складність побудови архітектури таких систем. Зокрема, виникає протиріччя між необхідністю динамічного перебудовування архітектури системи захисту та збереженням узгодженості дій автономних компонентів. З огляду на це особливої актуальності набуває проблема розробки мультикомп'ютерних обманних систем, які б мали здатність до самоналаштування, забезпечували узгоджене прийняття рішень та імітацію багатоваріантної поведінки у відповідь на атаки.

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.

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.

2. **Ступінь обґрунтованості 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 зловмисного програмного забезпечення та компютерних атак в корпоративних мережах, ефективним практичним впровадженням результатів дисертаційного дослідження на підприємствах, що експлуатують корпоративні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

3. Наукова новизна результатів дослідження. Наукова новизна результатів дослідження полягає у розробленні елементів теорії та практики створення мультикомп'ютерних систем з комбінованими приманками і

пастками та контролером прийняття рішень для виявлення та протидії зловмисного програмного забезпечення та комп'ютерних атак.

До найбільш суттєвих і науково нових результатів дисертаційної роботи можна віднести:

1) вперше запропоновано концепцію вирішення науково-прикладної проблеми, що полягає у синтезі та поєднанні 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;

2) вперше розроблено принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та компютерним атакам, особливістю якого є вставновлені вимоги щодо включення до архітектури систем контролера прийняття рішень та спеціалізованого функціоналу, що забезпечує можливість впливу на рішення систем відносно їх наступних кроків та модифікації архітектури, що ускладнює для зловмисників розуміння функціонування таких систем за рахунок формування різних наступних кроків системи при однакових початкових станах і покращить виявлення та протидію зловмисному програмного забезпеченню та комп'ютерним атакам в корпоративних мережах;

3) вперше розроблено концептуальну модель мультикомп’ютерних систем, особливістю якої є введена визначальна характеристика, що відповідає за контроль прийнятих рішень, а також інші визначальні характеристики, які в процесі функціонування систем формують архітектуру системи, самостійно синтезуючи множину окремих визначальних характеристик в архітектурі систем, а також виділено спеціалізований функціонал, що забезпечує варіативність відповідей при впливах зловмисників, комп'ютерних атак і функціонуванні зловмисного програмного забезпечення, а також забезпечує стійкість систем при вилученні окремих вузлів в корпоративних мережах та при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії зловмисному програмному забезпеченню та комп'ютерним атакам;

4) розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки щодо центру системи, які на відміну від відомих моделей оцінювання центрів систем для вибору наступних варіантів централізації, подані у вигляді аналітичних виразів, в яких враховані особливості типів централізації в архітектурі систем, а також 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 дозволяє формувати поліморфні відповіді системи на події, 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, 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.

4. **Зміст дисертації та відповідність встановленим вимогам.**

Дисертаційна робота складається з анотації, вступу, шести розділів, висновків, списку використаних джерел та десяти додатків. Робота містить 325 сторінок основного тексту. Список використаних літературних джерел містить 317 найменувань. Зміст дисертації відповідає меті та завданням дослідження, характеризується повнотою викладення, логічністю та завершеністю.

У вступі наведено обґрунтування актуальності науково-прикладної проблеми покращення ефективності функціонування мультикомп’ютерних систем антивірусних комбінованих приманок і пасток для виявлення зловмисного програмного забезпечення та комп’ютерних атак з метою забезпечення захисту й безпеки корпоративних мереж за рахунок синтезу в їх архітектурі властивостей приховування власної присутності, варіативності відповідей на повторювані дії зловмисника, а також здатності до самостійного прийняття рішень без участі адміністратора. Також, висвітлено зв’язок тематики дослідження з напрямами наукових робіт у цій сфері у світовій практиці, подано основні наукові результати, визначено їх практичне значення, наведено перелік підприємств та установ, де впроваджено здобуті результати.

У першому розділі проведено аналіз предметної області дослідження, розглянуто методи синтезу обманних мультикомп’ютерних систем із

приманками та пастками, здійснено їх класифікацію, а також досліджено підходи до моделювання зловмисних загроз із використанням приманок. Проаналізовано методи організації функціонування обманних систем і методів виявлення зловмисного програмного забезпечення та комп'ютерних атак за допомогою приманок і пасток. Також, підведено підсумки проведеного аналізу та здійснено постановку науково-прикладної проблеми дослідження.

У другому розділі запропоновано концепцію вирішення науково-прикладної проблеми, що полягає у розвитку елементів теорії і практики створення мультикомп'ютерних систем із комбінованими антивірусними приманками, пастками та контролером прийняття рішень з метою підвищення ефективності виявлення зловмисного програмного забезпечення й комп'ютерних атак у корпоративних мережах. Запропоновано принцип синтезу таких систем із використанням комбінованих приманок, пасток і контролера прийняття рішень для забезпечення виявлення та протидії загрозам. Розроблено концептуальну модель мультикомп'ютерних систем, особливістю якої є наявність визначальної характеристики, що відповідає за контроль прийнятих рішень, а також сукупності інших характеристик, які в процесі функціонування системи мають формувати її архітектуру шляхом самостійного синтезу множини окремих характеристик відповідно до замкненого маршруту в графі визначальних характеристик архітектури систем.

У третьому розділі розроблено нові математичні моделі для критеріїв оперативності, стійкості, цілісності та безпеки відносно центру системи, що необхідні для вибору подальших варіантів централізації, які подані у вигляді аналітичних виразів, у яких враховано особливості різних типів централізації в архітектурі систем, а також показники оперативності, стійкості, цілісності та безпеки щодо центру. Запропоновано новий метод визначення варіанта централізації в системах, у якому вибір наступного варіанта здійснюється за сукупністю критеріїв оперативності, стійкості, цілісності та безпеки з

урахуванням поділу архітектури на централізовану, частково централізовану, частково децентралізовану та децентралізовану.

У четвертому розділі вперше розроблено метод організації функціонування контролера прийняття рішень, що забезпечує вибір одного з варіантів виконання завдання серед підготовлених і поданих на розгляд центром системи, з урахуванням попереднього досвіду використання різних варіантів, рівнів безпеки компонентів системи, їх кількості та взаємозв'язків. Також розроблено новий метод організації функціонування мультикомп'ютерних систем, який дозволяє забезпечити їх здатність до самостійної зміни власних властивостей, організації елементів і компонентів та формування зв'язків між ними з урахуванням стану функціональної та кібербезпеки. Окремо виокремлено контролер прийняття рішень та центр системи.

У п'ятому розділі запропоновано метод виявлення схожих зловмисників у мережі приманок на основі їх поведінкових характеристик, який передбачає збір даних та кластеризацію подібних зловмисників із застосуванням мультикомп'ютерних систем з антивірусними комбінованими приманками й пастками. Основними етапами пошуку подібних часових рядів активності є представлення рядів, вимірювання відстані між ними, застосування алгоритму кластеризації та забезпечення різних варіантів відповідей на повторювані події, що підвищує витрати зловмисників та збільшу тривалість атаки. Також розроблено метод виявлення зловмисного програмного забезпечення та комп'ютерних атак, реалізований в архітектурі мультикомп'ютерних систем із комбінованими антивірусними приманками й пастками різного типу та функціонального призначення, що можуть діяти як інтелектуальні агенти, виконувати кілька завдань одночасно, взаємодіяти під час обробки подій із інформуванням центру системи та реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок і всієї системи), що забезпечує адаптивне та варіативне реагування й прийняття рішень як на рівні приманок, так і на рівні центрів системи,

ускладнює зловмисникам розуміння логіки функціонування системи та, відповідно, підвищує ефективність протидії.

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

У висновках представлено отримані наукові та практичні результати дослідження.

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

Обсяг, структура, оформлення матеріалів досліджень в цілому відповідають вимогам «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого Постановою КМУ №1197 від 17 липня 2021 р., та вимогам наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Наукові результати, отримані Каштальян А.С. в дисертації на здобуття наукового ступеня кандидата технічних наук, не виносяться у представлену до захисту докторську дисертацію.

Усі основні положення та найбільш важливі результати дисертації, подані до захисту, опубліковані в необхідному обсязі у фахових наукових виданнях України та закордонних виданнях, пройшли відповідну апробацію на міжнародних науково-технічних конференціях. За результатами проведених досліджень основні наукові результати опубліковано у 21 науковій праці, з яких 4 статті опубліковані в двох наукових журналах та індексовані у наукометричній базі Scopus, 17 статей у фахових наукових виданнях України категорії Б. Апробація засвідчена публікаціями 16 праць в матеріалах зарубіжних та українських конференцій, з яких 13 публікацій

індексовано у наукометричній базі Scopus. Опубліковано одне свідоцтво про реєстрацію авторського права на твір (програму).

Загальна кількість публікацій та їх зміст в достатній мірі висвітлюють результати дисертаційної роботи. Результати аналізу публікацій здобувача за темою дисертаційної роботи вказують на повноту викладу основних наукових положень та дотримання здобувачем принципів академічної доброчесності у процесі підготовки докторської дисертації.

Дисертація за змістом та отриманими результатами повністю відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти

5. Практичне значення результатів дисертаційної роботи.

У результаті виконаного дисертаційного дослідження розроблено архітектуру та компоненти мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для виявлення зловмисного програмного забезпечення та комп'ютерних атак у корпоративних мережах, а також здійснено їх практичну реалізацію. Експериментальні дослідження підтвердили ефективність розроблених засобів і коректність 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 щодо систем у цілому та хибних об'єктів атак. Встановлено, що з початку функціонування системи з контролером прийняття рішень її інтегрований показник стійкості та рівноваги перевищує 65% і зростає з часом експлуатації. Для критеріїв оперативності, стабільності, цілісності та безпеки щодо центру системи відхилення між крайніми значеннями цільової функції при штатному режимі роботи становить 3%, а при впливі на параметри одного з чотирьох критеріїв максимальне відхилення сягає 7% у момент впливу; надалі система стабільно функціонує, виконуючи перебудову центру. За наявності у складі системи контролера прийняття рішень значення цільової функції для всіх варіантів централізації на 50% менше порівняно з системою без контролера, що забезпечує приблизно на

10% кращий вибір оптимальних варіантів перебудови та скорочення часу на їх реалізацію. Крім того, розроблені правила вибору подальшого варіанта виконання завдання та централізації в системі гарантують стабільність її функціонування. При визначенні наступних кроків системи за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду встановлено, що дисперсія відхилень між випадками з контролером прийняття рішень та без нього становить близько 60% на користь системи з контролером. Середнє значення достовірності виявлення для всіх класів зловмисного програмного забезпечення з метаморфним функціоналом становить TPR = 75,46% для множини вірусів, які залишались невиявленими в досліджуваному операційному середовищі після проходження через системи виявлення вторгнень та антивірусні засоби, а відхилення від цього показника для дванадцяти розроблених класів не перевищує 3%. Загалом це дає можливість досягти достовірності виявлення на рівні до 98,8% при багатоетапній перевірці всієї множини зловмисного програмного забезпечення з метаморфним функціоналом.

6. Зауваження та дискусійні питання.

1. Понятійний апарат потребує уточнення, зокрема терміни «варіативність впливу», «самоорганізація архітектури» та «поліморфні відповіді» не завжди супроводжуються точними визначеннями або прикладами реалізації.

2. Оцінювання ефективності запропонованих моделей базується переважно на відносних приростах, без надання повного порівняння з існуючими стандартами або промисловими рішеннями в умовах реального часу.

3. Відсутній глибокий аналіз ризиків використання приманок і пасток у корпоративних мережах, зокрема щодо ймовірності викриття зловмисником таких компонентів.

4. Не розглянуто питання продуктивності системи в умовах високого навантаження або в ситуаціях масованих атак, наприклад, DDoS.

5. Не розглянуто потенційні конфлікти між агентами системи у децентралізованих конфігураціях, зокрема з точки зору консенсусу щодо дій у разі загрози.

6. Метод визначення варіанту централізації заснований на наборі евристичних критеріїв, але не представлено доказів його оптимальності або асимптотичної поведінки. Відсутні формальні докази коректності алгоритму або порівняння з іншими оптимізаційними підходами (наприклад, генетичними чи градієнтними).

7. Під час розробки моделей для мультикомп'ютерних систем не враховано аспекти масштабованості та витратності, як от обчислювальна складність алгоритмів, потреба в обміні повідомленнями між агентами, затримки тощо — що критично для реального впровадження.

8. Метод організації функціонування мультикомп'ютерної системи передбачає "самостійну зміну архітектури", проте не наведено жодного сценарію або обмежень, за яких система може приймати рішення про зміну своєї структури. Як здійснюється контроль консистентності та безпеки після таких змін — також не висвітлено.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової цінності.

7. Загальні висновки.

Дисертаційна робота Каштальян Антоніни Сергіївни «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах» є завершеним науковим дослідженням, яке виконано самостійно, вирішує актуальну науково-прикладну проблему, має вагоме теоретичне та практичне значення. Отримані теоретичні результати мають належне наукове обґрунтування, є новими та раніше на захищались. Тема та зміст дисертаційної роботи повністю відповідають спеціальності 05.13.05 – комп'ютерні системи та компоненти.

З огляду на актуальність теми дисертаційної роботи, новизну теоретичних положень, практичну цінність отриманих результатів досліджень, рівень висвітлення результатів дослідження у наукових публікаціях, вважаю, що дисертаційна робота «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах», подана на здобуття наукового ступеня доктора технічних наук, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає кваліфікаційним вимогам пп. 6, 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженому постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197, а її авторка, Каштальян Антоніна Сергіївна, заслуговує на присудження їй наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент – доктор технічних наук,
професор, завідувач кафедри
системного проектування
Національного технічного університету України
«Київський політехнічний інститут
ім. Ігоря Сікорського» В.Є. Мухін

«Підпис Мухіна В.Є. засвідчую»:
Вчений секретар
Національного технічного університету України
«Київський політехнічний інститут
ім. Ігоря Сікорського» В.В. Холяво

29 вересня 2025 р.