ВІДГУК

офіційного опонента, доктора технічних наук, професора,
професора кафедри спеціалізованих комп'ютерних систем
Західноукраїнського національного університету
Возної Наталії Ярославівни
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 дисертації

Корпоративні мережі залишаються привабливим об'єктом для атак зловмисників. Для забезпечення їх захисту від комп'ютерних атак (КА) та зловмисного програмного забезпечення (ЗПЗ) наявні багато методів і засобів. Але проблема захисту від комп'ютерних атак зберігається. Мотивами атак є як прагнення отримати вигоду, так і недоліки існуючих систем захисту, які часто сприймаються зловмисниками як відносно прості для подолання. Інформацію про засоби безпеки вони отримують з відкритих джерел або шляхом розвідки, під час якої вивчають структуру та роботу корпоративних систем. Засоби захисту зазвичай реагують на атаки повторюваними відповідями з обмеженим набором команд, що дає змогу ідентифікувати їхні особливості й слабкі місця. Тому, виникає потреба у створенні систем, здатних формувати різні варіанти відповідей на однакові впливи, або однакові відповіді, але різними методами. Це ускладнює розуміння логіки роботи захисту та підвищує його ефективність. Додатково такі системи можуть включати приманки та пастки для заплутування зловмисників і дослідження їхньої поведінки. Водночас навіть сучасні комерційні рішення не гарантують повного захисту, що підтверджується практикою експлуатації корпоративних мереж. Тому, потрібно

застосовувати комплексні підходи, адже зловмисники постійно вдосконалюють інструменти, моделі та техніки атак, використовуючи відомості про типову поведінку адміністраторів і стандартні протоколи дій.

У таких умовах перспективним напрямом є використання обманних систем, які імітують роботу справжніх сервісів і водночас ускладнюють роботу зловмисників, змушуючи їх витрачати додаткові ресурси. Проте такі системи мають швидко реагувати на атаки та забезпечувати повноцінну імітацію, інакше зловмисники зможуть виявити їх і використати у власних цілях. Отже, вони повинні бути адаптивними, самоорганізованими, реагувати нестандартно та діяти автономно, без залучення адміністратора.

Разом із цим виникає протиріччя: обманні мультикомп'ютерні системи мають змінювати власну архітектуру та центри прийняття рішень, узгоджуючи її з архітектурою приманок і пасток, що містять інтелектуальні компоненти та мають підтримувати зв'язки між собою. Проблема полягає в можливих розбалансуваннях дій: система може підготувати певні відповіді, тоді як її автономні частини реагуватимуть інакше. Це знижує ефективність виявлення та протидії ЗПЗ і КА.

У зв'язку з цим сформульовано актуальну науково-прикладну проблему: забезпечення злагодженого функціонування мультикомп'ютерних систем антивірусних комбінованих приманок і пасток, здатних до перебудови архітектури й узгодження дій усіх компонентів, аби заплутувати зловмисників, реагувати на повторювані атаки різними варіантами та приймати рішення автономно, без участі адміністратора.

Зв'язок з науковими програмами, планами і 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.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі

Наукові положення, висновки та рекомендації, представлені у дисертаційній роботі, спираються на комплексне використання сучасних теоретичних і прикладних методів. Це забезпечує їх високий рівень наукової обґрунтованості. Достовірність підтверджується коректним застосуванням математичного апарату, успішною програмною реалізацією розробленої мультикомп'ютерної системи антивірусних комбінованих приманок і пасток для виявлення ЗПЗ і КА у корпоративних мережах, а також результатами ефективного практичного впровадження на підприємствах. Це впровадження продемонструвало узгодженість теоретичних напрацювань із фактичними результатами їх використання.

3. Наукова новизна отриманих в дисертації результатів

В дисертаційній роботі авторкою отримано результати, наукова новизна яких полягає у 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.

4. Зв'язок матеріалів кандидатської дисертації з докторською дисертацією

Наукові положення, результати, висновки, рекомендації та інші матеріали наукових досліджень, представлені та захищені здобувачкою у кандидатській дисертації, не стали предметом розгляду та не були використані в дослідженнях, представлених у поданій до захисту докторській дисертації Каштальян Антоніни Сергіївни.

5. Повнота викладення результатів досліджень в наукових публікаціях за темою докторської дисертації

Наукові положення, результати, висновки та рекомендації, представлені у дисертаційному дослідженні та подані до захисту, опубліковані в необхідному обсязі.

За темою дисертації опубліковано 38 наукових праць, з них: 17 статей у наукових виданнях, включених до переліку наукових фахових видань України; 4 статті у наукових періодичних журналах, індексованих у базах даних Web of Science Core Collection та/або Scopus, в тому числі 1 публікація у виданні, віднесеному до третього квартилю (Q3) відповідно до класифікації SCImago Journal and Country Rank, що згідно із Наказом МОН України №1220 від 23.09.2019 р. прирівнюються до двох публікацій та 1 публікація у виданні, віднесеному до другого квартилю (Q2), що прирівнюється до трьох публікацій; 16 публікацій, які засвідчують апробацію матеріалів дисертації (у тому числі 13 індексованих у науко метричних базах Scopus та/або Web of Science); 1 свідоцтво про реєстрацію авторського права на твір.

Аналіз внеску авторки в публікаціях з питань, висвітлених в дисертації, показав, що внесок Каштальян А.С. є вирішальним, усі основні наукові результати та основні матеріали докторської дисертації опубліковані в наукових публікаціях здобувачки.

Зазначений перелік відповідає вимогам МОН України до опублікування результатів дисертації на здобуття наукового ступеня доктора наук.

6. Практичне значення результатів дисертаційної роботи.

У дисертаційному дослідженні розроблено архітектуру та компоненти мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для виявлення зловмисного програмного забезпечення (ЗПЗ) та комп'ютерних атак (КА) у корпоративних мережах, а також здійснено їх практичну реалізацію. Експериментальні дослідження підтвердили

ефективність запропонованих рішень і достовірність наукових положень теорії розподілених систем. Зокрема, впровадження розробленої системи забезпечило підвищення точності виявлення на 3–9 % порівняно з відомими аналогами за мультиплікативним і адитивним критеріями, що враховують як системні метрики, так і показники помилкових спрацювань.

Показано, що вже на початкових етапах роботи система з контролером прийняття рішень демонструє інтегрований показник стійкості та рівноваги понад 65 %, і цей показник зростає зі збільшенням часу експлуатації. Для критеріїв оперативності, стабільності, цілісності та безпеки відхилення між крайніми значеннями цільової функції у штатному режимі не перевищує 3 %, а при зовнішньому впливі на один із параметрів сягає максимуму 7 %, після чого система відновлює стабільність завдяки перебудові центру управління. Встановлено, що при наявності контролера прийняття рішень значення цільової функції для всіх досліджуваних варіантів централізації зменшується на 50 % у порівнянні з варіантом без нього, що дозволяє досягти приблизно 10 % приросту вдалого вибору рішень та скорочення часу на їх реалізацію.

Додатково розроблені правила визначення наступних варіантів виконання завдань і централізації забезпечують стабільність функціонування системи. Завдяки застосуванню поліморфних відповідей на події з урахуванням попереднього досвіду було встановлено, що дисперсія відхилень між системою з контролером і без нього становить близько 60 % на користь варіанту з контролером. Середній рівень достовірності виявлення для всіх класів ЗПЗ із метаморфним функціоналом дорівнює TPR = 75,46 % для тієї множини вірусів, які залишалися невиявленими після проходження через стандартні антивірусні системи та системи виявлення вторгнень. Водночас відхилення між окремими класами не перевищує 3 %, що у сукупності забезпечує підвищення точності багаторівневого виявлення до 98,8 % для всієї множини ЗПЗ з метаморфними характеристиками.

7. 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 підвищення ефективності функціонування мультикомп'ютерних систем антивірусних комбінованих приманок і пасток, призначених для виявлення зловмисного програмного забезпечення та комп'ютерних атак з метою забезпечення захисту корпоративних мереж. Досягнення цього запропоновано за рахунок інтеграції в архітектуру системи властивостей приховування власної присутності, варіативності відповідей на повторювані дії зловмисників та здатності до автономного прийняття рішень без залучення адміністратора. Також висвітлено зв'язок тематики дослідження з міжнародними науковими напрямами у цій сфері, наведено ключові результати роботи, їх практичну значущість, а також перелік підприємств та установ, де здійснено впровадження отриманих напрацювань.

У першому розділі здійснено комплексний аналіз предметної області, розглянуто методи побудови обманних мультикомп'ютерних систем з приманками і пастками, виконано класифікацію таких систем, проведено дослідження методів моделювання зловмисних загроз за допомогою приманок, а також розглянуто підходи до організації функціонування обманних систем та методи виявлення зловмисного програмного забезпечення й атак з використанням приманок і пасток. За результатами огляду підведено підсумки та сформульовано постановку науково-прикладної задачі.

Другий розділ присвячено розробці концепції вирішення окресленої проблеми, яка полягає у вдосконаленні теоретичних і практичних засад побудови мультикомп'ютерних систем з комбінованими антивірусними

приманками і пастками, а також контролера прийняття рішень, що підвищує ефективність виявлення зловмисного програмного забезпечення та комп'ютерних атак у корпоративних мережах. Запропоновано принцип синтезу архітектури таких систем, побудовано концептуальну модель, особливістю якої є визначальна характеристика для реалізації контролю прийнятих рішень та механізм синтезу решти характеристик через замкнений маршрут у графі визначальних параметрів.

У третьому розділі представлено нові математичні моделі, що описують критерії оперативності, стійкості, цілісності та безпеки центру системи. Ці моделі використано для визначення оптимального варіанта централізації архітектури системи. Розроблено аналітичні вирази, які враховують специфіку різних типів централізації (централізованої, частково централізованої, частково децентралізованої та децентралізованої) і дозволяють здійснювати вибір за комплексними критеріями.

У четвертому розділі вперше розроблено метод організації роботи контролера прийняття рішень, що забезпечує вибір одного з можливих варіантів виконання завдання з урахуванням попереднього досвіду системи, рівня безпеки її компонентів, їх кількості та зв'язків. Запропоновано новий метод організації функціонування мультикомп'ютерних систем, який забезпечує здатність до автономної зміни властивостей, структури та взаємозв'язків компонентів відповідно до поточного стану функціональної та кібербезпеки. Особливу увагу приділено виокремленню контролера прийняття рішень та центру системи.

П'ятий розділ містить метод визначення груп схожих зловмисників у мережі приманок за поведінковими характеристиками. Запропоновано алгоритм збору даних і кластеризації часових рядів активності зловмисників, що дозволяє формувати варіативні відповіді на повторювані дії, збільшуючи витрати зловмисників і тривалість атак. Крім того, розроблено метод виявлення зловмисного програмного забезпечення та атак, що реалізується в архітектурі мультикомп'ютерних систем з комбінованими приманками і пастками різного функціонального призначення. Такі системи здатні діяти

як інтелектуальні агенти, одночасно виконувати кілька завдань, взаємодіяти між собою та центром, а також реалізовувати трирівневу модель аналізу подій (на рівні окремої приманки, групи приманок і всієї системи), що підвищує адаптивність та ускладнює розуміння логіки їх роботи для зловмисників.

У шостому розділі описано постановку та проведення експериментів для апробації реалізованого прототипу мультикомп'ютерних систем з комбінованими приманками і пастками, зокрема перевірку ефективності запропонованих методів у різних конфігураціях архітектури.

У висновках підсумовано основні наукові та практичні результати дослідження.

У додатках наведено наукові публікації, що відображають здобуті результати, акти впровадження, програмні коди, а також таблиці з даними проведених експериментів.

Дисертаційна робота відповідає 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».

8. Зауваження та дискусійні питання.

Даючи загальну позитивну оцінку науковим положенням, результат, рекомендаціям, наведеним у дисертаційній роботі, та рівню їх обґрунтування, слід відзначити наступні зауваження та дискусійні питання:

1. У роботі недостатньо розкрито механізми врахування передісторії функціонування системи під час прийняття рішень контролером. Потребує деталізації опис того, яким чином відбувається збереження, накопичення та подальше використання цього досвіду для підвищення ефективності прийнятих рішень.

2. Недостатньо проаналізовано питання забезпечення стійкості архітектури у випадках цілеспрямованих атак на центральний вузол або контролер прийняття рішень. Відсутній детальний розгляд механізмів

резервування, децентралізації функцій чи впровадження відмовостійких протоколів, які здатні гарантувати безперервність функціонування системи навіть за умови компрометації окремих критичних компонентів.

3. У представлених підходах спостерігається обмежене використання сучасних методів глибокого навчання та штучного інтелекту. Доцільно було б розширити дослідження шляхом інтеграції моделей глибоких нейронних мереж, алгоритмів самоорганізації чи адаптивних інтелектуальних агентів, що дозволило б підвищити рівень адаптивності, точність класифікації подій та якість прогнозування поведінки системи.

4. У роботі відсутній повноцінний аналіз продуктивності архітектури при масштабуванні системи. Не розглянуто вплив зростання кількості агентів, до сотень чи навіть тисяч, на швидкодію, час відгуку та ефективність взаємодії між компонентами. Потребує дослідження питання оптимізації обчислювальних ресурсів, пропускної здатності мережі та забезпечення стабільності системи при різних режимах навантаження.

5. Не в повній мірі деталізована поведінка мультикомп'ютерної системи як мережі взаємодіючих агентів. Зокрема, не розкрито механізми розподілу завдань між агентами, методи виявлення та вирішення конфліктів, а також підходи до координації їх спільної роботи. Аналіз зазначених аспектів надав би змогу краще зрозуміти властивості колективної взаємодії агентів та вплив цих процесів на ефективність функціонування всієї системи.

6. Недостатньо проаналізовано відомі технології та методи збереження і використання передісторії функціонування системи.

7. Пункти наукової новизни, з точки зору формулювання, є громіздкими та переобтяженими другорядними поясненнями.

9. 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, в якому вирішено актуальну науково-прикладну проблему забезпечення безпеки та захисту корпоративних мереж.

Представлені в дисертаційній роботі наукові положення мають відповідне теоретичне обґрунтування та належним чином підтверджені на практиці. Одержані результати мають як наукову новизну, так і практичну цінність у галузі інформаційних технологій. Дисертаційна робота повністю відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти.

Взявши до уваги ступінь актуальності теми, обґрунтованість наукових положень, висновків і рекомендацій дисертаційної роботи, її наукову новизну, практичну корисність отриманих результатів, повноту викладення результатів у наукових публікаціях, вважаю, що дисертаційна робота відповідає кваліфікаційним вимогам до дисертаційних робіт на здобуття наукового ступеня доктора наук, зокрема, пп. 6, 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженому постановою Кабінету Міністрів України № 1197 від 17 листопада 2021 р., 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, професор кафедри
спеціалізованих комп'ютерних систем
Західноукраїнського національного
університету Наталія ВОЗНА

29 вересня 2025 р.