ВІДГУК

офіційного опонента, доктора технічних наук, професора, завідувача кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки Коваленка Андрія Анатолійовича на 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

АКТУАЛЬНІСТЬ ТЕМИ

Для захисту корпоративних мереж від атак зловмисників застосовуються різні методи, засоби та системи протидії комп'ютерним атакам (КА) і зловмисному програмному забезпеченню (ЗПЗ). Проте проблеми зберігаються, адже зловмисників мотивує вигода та недосконаліть існуючих систем безпеки. Інформацію про захист вони отримують як з відкритих джерел, так і під час розвідки, вивчаючи поведінку засобів безпеки. Оскільки системи часто реагують стандартними діями, зловмисники можуть визначити їхні можливості та слабкі сторони. Тому необхідно створювати адаптивні системи, здатні варіювати відповіді на однакові впливи, що ускладнюватиме розуміння їх функціонування. Перспективним напрямом є використання приманок і пасток для введення зловмисників в оману та дослідження їхньої поведінки.

Незважаючи на розвиток технологій, повного захисту корпоративних мереж не забезпечують наявні комерційні рішення, що підтверджує практика експлуатації. Адміністратори зазвичай застосовують відомі підходи й алгоритми, що відкриває додаткові можливості для атак. Тому, необхідно розвивати комплексні системи безпеки, зокрема з використанням обманних

механізмів. Однак вони мають діяти автономно, бути непомітними, самоорганізованими та нестандартно реагувати на події, інакше зловмисники швидко виявлять їх. Такі властивості можна закласти безпосередньо в архітектуру систем.

При цьому виникає протиріччя: обманні мультикомп'ютерні системи складаються з розподілених компонентів і автономних засобів, що не завжди узгоджено реагують із центром прийняття рішень. Це призводить до розбалансування дій, коли система й окремі її частини по-різному реагують на однакові впливи. Тому, актуальною науково-прикладною проблемою є забезпечення узгодженої роботи таких систем антивірусних приманок і пасток, здатних змінювати власну архітектуру, синхронізувати рішення без участі адміністратора та ефективно заплутувати зловмисників.

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.

СТРУКТУРА, ЛОГІКА ТА ЗМІСТ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

Дисертація складається з анотації, вступу, шести розділів, висновків, списку використаних джерел із 317 найменувань, десяти додатків та охоплює 325 сторінок основного тексту.

У вступі розкрито суть, структуру й актуальність науково-прикладної проблеми, пов’язаної з підвищенням ефективності функціонування мультикомп’ютерних систем антивірусних приманок і пасток для виявлення ЗПЗ і КА у корпоративних мережах. Обґрунтовано потребу синтезу в архітектурі таких систем властивостей приховування, змінюваності реакцій, автономного прийняття рішень без участі адміністратора. Подано взаємозв’язок тематики дослідження зі світовими науковими напрямами, основні результати, їх практичну значущість та організації, де впроваджено напрацювання.

У першому розділі здійснено аналіз предметної області, методів побудови обманних мультикомп’ютерних систем, їх класифікацію, підходи до моделювання загроз та організації функціонування, а також методів виявлення ЗПЗ і КА. Узагальнено результати аналізу та сформульовано постановку проблеми.

Другий розділ присвячено концепції розв’язання поставленої проблеми. Запропоновано принципи синтезу систем із комбінованими приманками та пастками й контролером прийняття рішень. Побудовано концептуальну модель мультикомп’ютерних систем, у якій архітектура формується на основі множини визначальних характеристик, що взаємодіють у замкненому графі.

У третьому розділі подано нові математичні моделі та аналітичні вирази для критеріїв оперативності, стійкості, цілісності й безпеки щодо центру системи. Розроблено метод вибору варіанта централізації, що враховує комплексні показники та поділ архітектур на різні типи.

Четвертий розділ містить новий метод організації роботи контролера прийняття рішень для вибору оптимального варіанта виконання завдань із урахуванням попереднього досвіду, рівня безпеки та зв’язків між компонентами. Розроблено метод функціонування мультикомп’ютерних систем із можливістю самостійної зміни властивостей і структури залежно від стану кібербезпеки в корпоративних мережах.

У п’ятому розділі представлено метод кластеризації зловмисників за поведінковими характеристиками в мережі приманок та метод виявлення ЗПЗ і КА, реалізований у багаторівневій архітектурі систем з інтелектуальними агентами. Запропонований підхід забезпечує адаптивність, багатоваріантність реагування та ускладнює розуміння логіки роботи системи з боку зловмисників.

Шостий розділ присвячений постановці експериментів і перевірці ефективності розроблених методів у межах створеної системи.

У висновках узагальнено наукові та практичні результати. У додатках наведено наукові публікації, акти впровадження, лістинги програмного забезпечення та результати експериментів.

Структура, обсяг і оформлення відповідають вимогам чинних нормативних документів. Текст викладено послідовно із використанням загальноприйнятої термінології, а всі залучені положення мають відповідні посилання.

Наукові результати, отримані Каштальян А.С. у кандидатській дисертації, не включені до представленої докторської роботи.

Академічного плагіату, фабрикації чи фальсифікації в дисертаційні роботі не виявлено.

НАУКОВА НОВИЗНА РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

У дисертаційній роботі наведено розв’язання актуальної науково-прикладної проблеми розроблення 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.

При цьому отримано ряд наукових результатів, що мають переваги над існуючими:

1) вперше запропонована концепція вирішення науково-прикладної проблеми, яка полягає у поєднанні та синтезі в системах таких визначальних

властивостей, як варіативності типу архітектури системи, варіативності типу та кількості центрів системи, адаптивності системи при зміні зовнішніх умов, характерних змін в центрі системи, самоорганізації системи, гнучкості системи, самостійності щодо прийняття рішень, допустимої варіативності впливу на систему, варіативності щодо наявності агентів в системі для прийняття рішень, контролю щодо прийнятих рішень в системі, особливості спеціалізованого функціоналу щодо комбінованих антивірусних приманок і пасток в системі, що дає змогу синтезувати мультикомп'ютерні системи антивірусних комбінованих приманок і пасток в корпоративних мережах, які будуть автономними, складними в прогнозуванні їх наступних кроків та розуміння їх принципів функціонування зловмисниками, для покращення виявлення та протидії ЗПЗ і КА;

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

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

при поєднанні спеціалізованого функціоналу із основною частиною системи формує цілісну систему, що в цілому покращує ефективність протидії ЗПЗ та КА;

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

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

6) вперше розроблено метод організації функціонування контролера прийняття рішень, особливістю якого є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дало змогу формувати

поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах;

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

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

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

ПРАКТИЧНЕ ЗНАЧЕННЯ РЕЗУЛЬТАТІВ РОБОТИ ТА ПОВНОТА ЇХ ВИКЛАДУ В НАУКОВИХ ПУБЛІКАЦІЯХ

У ході дисертаційного дослідження розроблено архітектуру та компоненти мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, а також здійснено їх практичну реалізацію. Експериментальні результати підтвердили ефективність створених засобів і коректність наукових положень теорії розподілених систем. Встановлено, що впровадження таких систем дозволяє підвищити достовірність виявлення на 3–9 % порівняно з відомими аналогами за мультиплікативним і адитивним критеріями, які враховують сукупні метрики щодо системи та хибних об'єктів атак.

Показано, що на початковому етапі роботи системи з контролером прийняття рішень її інтегрований показник стійкості та рівноваги перевищує 65 % і надалі зростає в процесі експлуатації. Для критеріїв оперативності, стабільності, цілісності та безпеки відхилення між крайніми значеннями цільової функції при штатному режимі становить 3 %, а під час впливу на один із чотирьох критеріїв максимальне відхилення дорівнює 7 %. Після перебудови центру система функціонує стабільно. Водночас, за наявності контролера прийняття рішень значення цільової функції при виборі варіантів централізації зменшується на 50 % у порівнянні з системою без контролера, що забезпечує приблизно на 10 % ефективніший підбір рішень та скорочує час їх реалізації. Розроблені правила вибору наступних варіантів завдань і централізації сприяють стабільності функціонування системи.

Додатково встановлено, що завдяки формуванню поліморфних відповідей на події з урахуванням попереднього досвіду дисперсія відхилень між системою з контролером і без нього становить близько 60 % на користь першої. Середнє значення достовірності виявлення для всіх класів ЗПЗ із метаморфним функціоналом досягає TPR = 75,46 % для тих вірусів, які залишалися невиявленими після проходження через системи виявлення

вторгнень та антивірусні засоби. Відхилення між дванадцятьма розробленими класами не перевищує 3 %, що в комплексі дозволяє досягти рівня достовірності виявлення до 98,8 % під час багатоетапної перевірки.

Наукові та практичні результати дисертаційної роботи достатньо повно висвітлені у 38 наукових працях здобувача, серед яких 4 статті опубліковані в двох наукових журналах та індексовані у наукометричній базі Scopus, 17 статей у фахових наукових виданнях України категорії Б, 13 публікацій у матеріалах зарубіжних та українських конференцій, які індексуються у науко метричній базі Scopus, 3 публікації в матеріалах українських конференцій, 1 публікація, яка додатково відображає наукові результати дисертації.

Згідно п.2 Наказу МОН України № 1220 від 23.09.2019 р. (із змінами внесеними згідно з Наказами Міністерства освіти і науки № 496 від 27.05.2022, № 285 від 08.03.2024) щодо наукових публікацій у виданнях, які віднесено до першого і другого квартилів (Q1 і Q2) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports, публікація прирівнюється до трьох публікацій, у виданні, віднесеному до третього квартиля (Q3),- до двох публікацій. Основні результати дисертації опубліковані в 21 науковій статті, з яких одна стаття в науковому журналі з квартилем Q2, одна стаття - з квартилем Q3, тому прирівнених публікацій за темою дисертації – 24.

Задекларований особистий внесок автора у спільних публікаціях відповідає темі, змістові дисертаційної роботи та положенням, що винесені на захист.

ОБҐРУНТОВАНІСТЬ ТА ДОСТОВІРНІСТЬ НАУКОВИХ ПОЛОЖЕНЬ, ВИСНОВКІВ І РЕКОМЕНДАЦІЙ

Вихідні положення дисертації є науково коректними. Сформульовані положення, висновки та рекомендації ґрунтуються на доцільному застосуванні математичного апарату, успішній програмній реалізації мультикомп’ютерної системи антивірусних комбінованих приманок і пасток

для виявлення ЗПЗ та КА в корпоративних мережах, а також на результатах їх практичного впровадження на підприємствах, що експлуатують корпоративні системи. Отримані дані підтвердили відповідність теоретичних досліджень фактичним результатам використання.

Додатковими доказами обґрунтованості та достовірності результатів є їх публікація у фахових наукових виданнях з технічних наук і апробація на міжнародних науково-технічних конференціях.

ЗАУВАЖЕННЯ ЩОДО ПОЛОЖЕНЬ ДИСЕРТАЦІЇ ТА ДИСКУСІЙНІ ПИТАННЯ

1. Попри універсальність архітектури мультикомп’ютерної системи антивірусних приманок і пасток, наведені приклади її застосування обмежуються лише корпоративними мережами. Недостатньо розглянуто потенціал впровадження такої системи в інших галузях, зокрема в критичних інформаційних системах чи промислових мережах, де особливості взаємодії між пристроями та специфіка атак можуть істотно відрізнятися.

2. Потребує поглиблення технічна деталізація реалізації контролера прийняття рішень і конкретних типів антивірусних пасток, які застосовуються у системі. Невизначеним залишається рівень захищеності самого контролера, що може стати потенційною точкою вразливості. Доцільним було б розкрити механізми його захисту від компрометації, резервування чи дублювання функцій для зниження ризиків.

3. Недостатньо висвітленим є аспект стійкості системи до розпізнавання зловмисником. Хоча у роботі згадуються методи маскування, вони описані поверхнево і не дають повного уявлення про рівень їхньої ефективності, обмеження та потенційні сценарії обходу з боку атакуючих.

4. Питання масштабованості та продуктивності системи потребують детальнішого аналізу. Незважаючи на зазначену адаптивність та варіативність архітектури, залишається невизначеним рівень її ефективності при розгортанні на великих мережах із десятками чи сотнями вузлів. Доцільно

було б представити кількісні показники продуктивності, а також моделювання поведінки системи за умов зростання навантаження.

5. Запропонований метод знаходження схожих зловмисників за поведінковими характеристиками поданий без порівняння з альтернативними підходами кластеризації, зокрема DBSCAN, спектральною кластеризацією або сучасними embedding-методами на основі нейронних мереж. Відсутній аналіз помилок класифікації, а також результати перехресної валідації, що знижує достовірність представлених висновків.

6. Робота не містить формалізованої моделі критичної взаємодії системи з адміністратором у надзвичайних ситуаціях. Це створює прогалину у розумінні того, як саме має здійснюватися оперативне втручання людини у випадках збоїв, атак чи некоректної роботи системи.

7. У дослідженні відсутні розрахунки обчислювальних і фінансових витрат, необхідних для впровадження та підтримки мультикомп'ютерної системи антивірусних приманок і пасток. Це обмежує можливості практичної оцінки доцільності використання запропонованого підходу в умовах реальних організацій.

8. У тексті роботи наявні граматичні, орфографічні, синтаксичні та стилістичні неточності, що знижує загальну якість викладу та ускладнює сприйняття матеріалу.

Наведені зауваження в цілому не знижують наукової та практичної цінності виконаного дисертаційного дослідження.

ЗАГАЛЬНИЙ ВИСНОВОК

Дисертаційна робота Каштальян А.С. «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах» є завершеним науковим дослідженням, в якому отримано нові теоретичні та практичні результати. Отримані теоретичні результати є новими, мають належне наукове обґрунтування та

раніше не захищались. Тема та зміст дисертаційної роботи повністю відповідають спеціальності 05.13.05 – комп'ютерні системи та компоненти.

Вважаю, що за обсягом досліджень, актуальністю, науковою новизною і практичним значенням отриманих результатів, їх впровадженням та опублікуванням дисертаційна робота відповідає вимогам чинних нормативних документів, в тому числі пунктам 6, 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженому постановою Кабінету Міністрів України № 1197 від 17 листопада 2021 р. (зі змінами), 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 електронних обчислювальних машин
Харківського національного університету радіоелектроніки

Андрій КОВАЛЕНКО

ПІДПИС ЗАСВІДЧУЮ
Проректор з наукової роботи
Харківського національного університету радіоелектроніки
доктор технічних наук, професор

Юрій РОМАНЕНКОВ

"29" вересня 2025 р.