«ЗАТВЕРДЖУЮ»
Проректор з НР ХНУ
Олег СИНЮК
«29» 07 2025 року

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

Каштальян Антоніни Сергіївни

на тему: «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах»,

поданої на здобуття наукового ступеня доктора технічних наук
з галузі знань 12 – інформаційні технології
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Фаховий семінар для апробації докторської дисертації проведений на кафедрі комп'ютерної інженерії та інформаційних систем «30» червня 2025 року, протокол №24.

1. Актуальність теми дослідження. 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., Феng 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.

2. 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.

3. Наукова новизна отриманих результатів полягає у розробленні елементів теорії та практики створення мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА.

У дисертації отримано такі нові наукові результати:

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. Теоретичне та практичне значення результатів дисертації.

Теоретичне значення полягає 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 ЗПЗ і КА, розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик, 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.

Теоретичну значущість результатів дослідження вказано також у пункті 3 Висновку «Наукова новизна отриманих результатів».

У результаті виконаного дисертаційного дослідження розроблено архітектуру і компоненти мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для виявлення ЗПЗ та КА в корпоративних мережах, здійснено їх реалізацію. Результати експериментальних досліджень підтверджують ефективність розроблених засобів, а також правильність наукових положень теорії розподілених систем, оскільки впровадження мультикомп'ютерної системи дозволяє підвищити достовірність виявлення на 3–9 % порівняно з відомими аналогами за мультиплікативним та адитивним

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

5. Використання результатів роботи.

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.).

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі.

Дисертаційна робота виконана на кафедрі комп’ютерної інженерії та інформаційних систем Хмельницького національного університету, науковий консультант – доктор технічних наук, професор, професор кафедри комп’ютерної інженерії та інформаційних систем Савенко О.С.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Каштальян А.С. є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Дисертаційну роботу Каштальян А.С. перевірено на плагіат програмним засобом «StrikePlagiarism». Відсоток текстових збігів за «StrikePlagiarism» (українська) – 4.78%, «StrikePlagiarism» (англійська) – 4.17%. Визначено, що робота містить окремі збіги з власними публікаціями, термінологією, посиланнями на джерела літератури, а також загальновживаними фразами. Використані результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

Матеріали та наукові положення кандидатської дисертації Каштальян А.С. у її докторській дисертації не використовувались.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За темою дисертації з викладенням основних її результатів опубліковано 38 наукових праць, з них: ***17 статей*** у наукових виданнях, включених до Переліку наукових фахових видань України категорії Б; ***4 статті*** у наукових періодичних журналах, індексованих у базах даних Web of Science Core Collection та/або Scopus, зокрема три з них в журналі категорії А, який включено до Переліку наукових фахових видань України; 16 публікацій, які засвідчують апробацію матеріалів дисертації (у тому числі 13 індексованих у наукометричних базах Scopus та/або Web of Science); 1 свідоцтва про реєстрацію авторського права на твір.

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.

Список публікацій здобувача

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

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення та комп'ютерних атак на основі аналізу поведінкових патернів системи.

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

Здобувачем розроблено методи для організації прийняття рішень та функціонування обманних систем на основі попереднього досвіду функціонування та різних варіантів виконання завдань.

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

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення та комп'ютерних атак мультикомп'ютерними системами на основі впровадження антивірусних комбінованих приманок та пасток.

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/

Здобувачем розроблено комплексний метод захисту комп'ютерної мережі шляхом створення мережі приманок, що забезпечує ефективне виявлення зловмисного трафіку та аналіз патернів нових атак.

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

Здобувачем розроблено концептуальну модель архітектури мультикомп’ютерних систем з приманками та пастками для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам.

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.

Здобувачем розроблено критерій оперативності щодо наступного варіанту центру системи в архітектурі системи для забезпечення її перебудови.

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

Здобувачем розроблено правила формування потенційно можливих варіантів централізації в архітектурі мультикомп’ютерних систем, яку задано моделлю множин її елементів та графа зв’язків між компонентами системи.

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

Здобувачем розроблено принцип синтезу мультикомп’ютерних систем, які є одним з класів deception-систем, з комбінованих антивірусних приманок і пасток та контролеру прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам

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

Здобувачем розроблено моделі характерних властивостей централізації для використання їх в методі визначення наступного варіанту центру в архітектурі мультикомп’ютерних систем попередження, виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам.

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

Здобувачем розроблено концептуальну модель мультикомп'ютерних систем, зокрема самоорганізовану систему прогнозування зловмисної активності в комп'ютерній мережі згідно алгоритмів глибокого навчання.

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

Здобувачем розроблено метод знаходження схожих зловмисників в мережі приманок за їх поведінковими характеристиками.

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

Здобувачем розроблено модель та концепцію побудови мережі інтелектуальних приманок, розгорнутої в комп'ютерній мережі.

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

Здобувачем розроблено моделі приманок на основі типових комп'ютерних атак , архітектурних особливостей приманок та з врахуванням архітектури розподіленої системи з приманками.

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.

Здобувачем розроблено моделі приманок, мереж приманок та аналіз особливостей типів приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж.

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

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема системи моніторингу, виявлення, реагування та захисту інформації на основі honeypot-файлів.

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

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема концепцію застосування розподілених систем для аналізу поліморфних вірусів.

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

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення та комп'ютерних атак із використанням 2D-CNN та соніфікації мережевого трафіку

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***)

Здобувачем розроблено метод та правила визначення наступного варіанту централізації в системах, взято участь в розробленні експериментального варіанту системи для проведення експерименту.

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***)

Здобувачем розроблено математичні моделі критеріїв оцінювання варіантів централізації в архітектурі мультикомп'ютерних систем виявлення зловмисного програмного забезпечення та комп'ютерних атак.

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)

Здобувачем розроблено принцип синтезу мультикомп'ютерних систем з комбінованими приманками та пастками, а також контролером прийняття рішень для виявлення та протидії зловмисному програмного забезпеченню та комп'ютерним атакам.

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)

Здобувачем розроблено концептуальну модель мультикомп'ютерних систем виявлення зловмисного програмного забезпечення, взято участь в розробленні реалізації системи виявлення з метаморфним функціоналом.

Публікації, 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)

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак на основі соціально орієнтованого протоколу.

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)

Здобувачем розроблено метод знаходження схожих зловмисників в мережі приманок для виявлення характерних особливостей та закономірностей на зображеннях.

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)

Розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак, зокрема для виявлення ботнет в IT інфрастуктурі з використанням нейромереж.

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)

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак, зокрема для виявлення програмних імплантів у корпоративних мережах.

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)

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак для прогнозування зловмисної активності в комп'ютерних мережах.

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

Здобувачем розроблено моделі приманок в комп'ютерних мережах відповідно типів комп'ютерних атак.

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)

Здобувачем розроблено метод визначення патернів атак на основі інформації зібраної мережею приманок, із використанням агломеративної кластеризації та згорткового автоенкодера.

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)

Здобувачем розроблено метод виділення патернів атак на основі часових рядів, які відображають активність зловмисника, із спільним застосуванням k-means кластеризації та рекурентного автоенкодера.

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)

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема системи моніторингу, виявлення, реагування та захисту інформації на основі приманок.

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)

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема інструменту виявлення шкідливого програмного забезпечення на основі аналізу стану емулятора.

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)

Здобувачем розроблено концептуальну модель мультикомп'ютерних систем на основі визначальних характеристик, зокрема системи інтелектуально кластеризації з зовнішнім модулем для архітектури RTOS з інтенсивними змінами станів.

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)

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема виявлення зловмисного програмного забезпечення розподіленими системами із частковою централізацією.

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)

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема само організованої розподіленої системи виявлення аномалій у комп'ютерних системах на основі методу головних компонентів.

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)

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак, зокрема на основі соніфікації мережевого трафіку.

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

Здобувачем розроблено метод виявлення зловмисного програмного забезпечення і комп'ютерних атак, зокрема із використанням моделі антивірусних приманок в комп'ютерній мережі.

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

Здобувачем запропоновано концепцію вирішення науково-прикладної проблеми, зокрема розподілених систем виявлення worm-вірусів.

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

Здобувачем розроблено програмне забезпечення мультикомп'ютерних систем.

8. Висновок. Ознайомившись із дисертаційним дослідженням Каштальян Антоніни Сергіївни та науковими публікаціями, у яких висвітлені основні наукові результати, а також взявши до уваги підсумки фахового семінару для апробації докторської дисертації, вважаємо, що дисертаційна робота Каштальян А.С. «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, та відповідає спеціальності 05.13.05 – комп'ютерні системи та компоненти.

РЕКОМЕНДУЄМО:

Дисертаційну роботу «Елементи теорії та практики створення мультикомп'ютерних систем комбінованих антивірусних приманок і пасток в корпоративних мережах», подану Каштальян Антоніною Сергіївною на здобуття наукового ступеня доктора технічних наук, до захисту у спеціалізованій вченій раді Д70.052.06 Хмельницького національного університету.

Рецензент, д.т.н., професор,
декан факультету інформаційних
технологій, професор кафедри
комп'ютерної
інженерії та інформаційних систем Тетяна ГОВОРУЩЕНКО

Рецензент, д.т.н., професор,
професор кафедри комп'ютерної
інженерії та інформаційних систем Єлизавета ГНАТЧУК

Рецензент, д.т.н., професор, завідувач кафедри автоматизації,
комп'ютерно-інтегрованих технологій та робототехніки,
професор кафедри комп'ютерної
інженерії та інформаційних систем Валерій МАРТИНЮК

29.07.2025 р.