ВІДГУК

офіційного опонента

доктора технічних наук, професора Смірнова Олексія Анатолійовича

на дисертаційну роботу Звєрцевої Наталії Віталіївни

«Моделі оцінки безпеки комп'ютерних систем»,

представлену на здобуття наукового ступеня доктора філософії

за спеціальністю 122 – Комп'ютерні науки

Актуальність теми.

У світовій практиці безпека інформаційних технологій поступово переходить від локального технічного питання до стратегічного чинника національної та міжнародної безпеки. Стрімке впровадження цифрових сервісів, систем зі штучним інтелектом, автономних платформ, а також повсюдна присутність IoT-компонентів створюють надскладні гібридні комп'ютерні системи, уразливість яких стає дедалі критичнішою.

У цьому контексті стає очевидною потреба у науково обґрунтованих підходах до оцінювання стійкості таких систем до сучасних і перспективних загроз. Перехід до постквантової епохи лише загострює ці виклики, адже злам традиційних криптографічних алгоритмів стане лише питанням часу. Це висуває нові вимоги до моделей безпеки, методів їх оцінювання та адаптивності захисту до швидкоплинних змін технологічного середовища.

Таким чином, обрана здобувачем тематика є вкрай актуальною і цілком відповідає світовим пріоритетам у сфері кібербезпеки, оскільки поєднує фундаментальні дослідження з прикладними потребами цифрового суспільства..

Дисертаційна робота Звєрцевої Наталії Віталіївни присвячена вирішенню актуального науково-технічного завдання – забезпеченню підвищеного рівня кібербезпеки комп'ютерних систем шляхом розробки моделей оцінювання захищеності із застосуванням комплексованих метрик. Запропоновані рішення дозволяють здійснювати глибокий аналіз стану безпеки, ідентифікувати потенційні вразливості та своєчасно реагувати на загрози, що, у свою чергу, підвищує ефективність функціонування систем кіберзахисту та сприяє формуванню стійких до атак інформаційних середовищ.

Дисертаційна робота виконана на кафедрі програмної інженерії та інтелектуальних технологій управління НТУ «ХПІ» у межах ініціативної науково-дослідної роботи К8018 «Розробка моделей, методів та інформаційних технологій оцінювання складних багатоознакових об'єктів і систем» (№ДР 0125U001121), де здобувач був виконавцем розділу.

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

Положення та висновки, наведені в дисертаційній роботі Звєрцевої Н.В., в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні теорії ймовірностей і математичної статистики, використаних для дослідження моделей та методів оцінки комп'ютерних систем.

Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірені шляхом проведення практичних експериментів, що підтверджує обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Достовірність результатів досліджень.

Достовірність результатів теоретичних досліджень підтверджується результатами відповідних експериментальних перевірок, проведених у рамках моделювання та аналізу рівня захищеності комп'ютерних систем.

Отримані наукові результати реалізовані у вигляді прототипу інтегрованої системи оцінювання безпеки з використанням комплексованих метрик та механізмів аналізу гібридних загроз.

До основних нових наукових результатів дисертації слід віднести наступне:

1. Розроблено нову модель оцінювання поточного стану захищеності комп'ютерної системи, яка враховує комплексні характеристики безпеки, а також прояви гібридності та синергетичної взаємодії загроз, що підвищує точність оцінки рівня безпеки в умовах складного загрозового середовища.

2. Запропоновано метод забезпечення безперервного функціонування системи безпеки, що орієнтований на захист критичних бізнес-процесів у реальному часі та дозволяє своєчасно формувати превентивні заходи у відповідь на змішані та цілеспрямовані кібератаки.

3. Розроблено модель визначення рівня безпеки на основі інтеграції різнорідних метрик, яка забезпечує об'єктивну оцінку стану соціокіберфізичних систем, враховуючи не лише технічні та фінансові ресурси зловмисника, а й рівень конфіденційності атакованих активів.

4. Удосконалено математичний апарат побудови класифікатора загроз, що базується на врахуванні їх гібридного характеру, синергетичного ефекту та критичності впливу на інфраструктуру комп'ютерної мережі, що дозволяє покращити ефективність систем виявлення загроз.

Значимість отриманих результатів для науки і практичного використання.

Практична цінність полягає у використанні результатів досліджень:

1) у ТОВ «НІКС СОЛЮШЕНС ЛТД» (м. Харків) – ІТ-компанії, що займається розробкою програмного забезпечення;

2) на кафедрі програмної інженерії та інтелектуальних технологій управління в НТУ «ХПІ» (м. Харків) при підготовці бакалаврів за спеціальністю 122 Комп'ютерні науки та 121 Інженерія програмного забезпечення

Повнота викладення результатів досліджень в опублікованих працях.

У відкритому друці за темою дисертації опубліковано 15 наукових праць, з них: 5 статей, з яких 2 статті включено до наукометричної бази Scopus та/або Web of Science Core Collection, 3 статті – в збірниках наукових праць, що входять до переліку фахових Міністерства освіти і науки України; 10 публікацій – тези доповідей на конференціях.

Участь здобувача у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та

скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44.

Оцінка змісту дисертаційної роботи.

Дисертаційна робота Звєрцевої Наталії Віталіївни складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, 4 додатків.

У *вступі* дисертаційної роботи обґрунтовано актуальність досліджуваної проблематики, чітко визначено мету, об'єкт і предмет дослідження, сформульовано наукову новизну та практичну значущість отриманих результатів. Висвітлено використані наукові методи, подано дані щодо апробації результатів дослідження, а також перелік публікацій автора за темою дисертації.

Перший розділ присвячено огляду сучасного стану інформаційної безпеки комп'ютерних систем. Проведено аналіз існуючих підходів до оцінювання безпеки в умовах технологічного розвитку, зокрема впровадження смарт-систем, зростання обчислювальних ресурсів та викликів постквантового періоду. Розглянуто специфіку гібридних загроз і функціонування систем виявлення атак. Сформульовано ключову наукову проблему, що полягає в необхідності розробки нових моделей оцінки захищеності комп'ютерних систем як основи побудови ефективних систем захисту.

У *другому розділі* подано методологічні засади побудови класифікатора загроз для комп'ютерних систем. Вивчено типологію існуючих метрик безпеки, визначено їх обмеження. Запропоновано новий підхід до об'єднання та інтеграції метрик у єдину комплексовану структуру, яка дозволяє точно відображати рівень ризиків у кіберфізичних системах. В основу розробки покладено інструменти нечіткої логіки та моделей причинно-наслідкових залежностей.

Третій розділ містить результати побудови моделей оцінювання захищеності комп'ютерних систем. Особливу увагу приділено забезпеченню безперервного функціонування системи безпеки в умовах змінного середовища. Запропоновано архітектуру багатоконтурної системи, що враховує специфіку критичних бізнес-процесів, інформаційних активів та характеристик IT-інфраструктури.

У *четвертому розділі* здійснено верифікацію моделей і методів, розроблених у попередніх розділах. Побудовано систему правил досяжності заданого рівня захищеності, яка враховує технічні та організаційні чинники. Представлено архітектуру програмного інструмента, призначеного для автоматизованого аналізу загроз та підтримки прийняття рішень з управління кіберризиками.

У *висновках* підсумовано основні результати дослідження, підтверджено досягнення поставленої мети та ефективність запропонованих рішень. Окреслено перспективи подальших досліджень у напрямі розвитку інтелектуальних систем кіберзахисту та управління інформаційною безпекою.

Висновки до розділів та за результатами роботи сформульовані чітко відповідають змісту дисертаційної роботи.

Список використаних джерел із 130 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

Академічна доброчесність.

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено.

Усі результати, які винесено автором на захист, отримані самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

По дисертаційній роботі можна зробити наступні зауваження:

1. В дисертаційної роботі визначена актуальність дослідження, яка присвячена формуванню моделі побудови системи безпеки критичних бізнес-процесів, в основі якої лежить багатоконтурна система безпеки, але не зрозуміло яким чином соціокіберфізичні системи відносяться до таких систем, та які бізнес-процеси є критичними для них.

2. В роботі п.1.3 визначає системи виявлення кібератак як складову безпеки комп'ютерних систем ,але не зрозуміло яким чином, це враховано при формуванні

об'єктивної оцінки рівня захищеності соціокіберфізичних систем на основі $P_{\text{hacking}}^{\text{average}}$ (стор. 82).

3. На стор. 38 наведений порівняльний аналіз сучасних систем виявлення аномалій, на основі якого SIEM є найбільш комплексним, універсальним рішенням і покриває потреби користувачів, але не зрозуміло чим запропонований підхід виявлення аномалій краще відомих.

4. В п.2.3 роботи наведена методика лінгвістичної класифікації, але не зрозуміло яким чином визначені показники у табл. 2.4 (Набір індикаторів X), табл. 2.5 (Значення показника g), які визначають результат класифікації (табл. 2.8).

5. В дисертаційної роботі у табл. 3.2 визначені залежності послуг безпеки інформаційних ресурсів для стохастичної моделі оцінки рівня захищеності інформаційних активів, але не зрозуміло яким чином враховується рівень «секретності» інформаційних активів та в динаміці забезпечує оцінку поточного стану рівня захищеності.

6. В роботі п. 4.3 запропонована програмна реалізація системи оцінки рівня безпеки системи, але не зрозуміло за який час можливо у динаміці визначати превентивні заходи захисту, та які обмеження є для інтегрування запропонованого програмного рішення до програмних застосунків, які реалізують аналіз комп'ютерних інцидентів та кіберзагроз.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

ВИСНОВОК

На основі критичного вивчення дисертації та праць здобувача, які опубліковані за темою дисертації об'єктивно встановлено:

– дисертаційна робота Звєрцевої Наталі Віталіївни відповідає чинним вимогам, які встановлені у «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого постановою Кабінету Міністрів України від 19 травня 2023 року № 502, та «Порядку присудження ступеня доктора філософії та скасування рішення

разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44;

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертаційна робота Звєрцевої Наталі Віталіївни є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, які дозволяють ефективність систем віддаленої біометричної автентифікації;

– автор дисертації роботи Звєрцева Наталія Віталіївна заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки.

Офіційний опонент

завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук,
професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
“ 24 ” 06 2025 року