РЕЦЕНЗІЯ

рецензента, д.т.н., доцента, Мілевського Станіслава Валерійовича

на дисертаційну роботу **Звєрцевої Наталії Віталіївни**

«Моделі оцінки безпеки комп'ютерних систем»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 122 – Комп'ютерні науки

Детальний аналіз дисертаційної роботи Звєрцевої Н.В. на тему «Моделі оцінки безпеки комп'ютерних систем» що представлена для захисту на здобуття наукового ступеня доктора філософії у Національному технічному університеті «Харківський політехнічний інститут», дає змогу зробити комплексний висновок щодо її актуальності, ступеня обґрунтованості наукових положень, висновків, рекомендацій, достовірності та значущості отриманих результатів, наукової новизни, теоретичної та практичної цінності, надати загальну оцінку дисертації.

1. Ступінь актуальності теми дисертаційної роботи

Дисертаційна робота присвячена актуальній проблемі – формалізованому оцінюванню рівня безпеки комп'ютерних систем у контексті трансформації сучасного кіберпростору та зростання складності інформаційних загроз.

В умовах глобальної цифровізації, стрімкого розвитку технологій Інтернету речей, хмарних обчислень, штучного інтелекту та мобільних комунікацій, питання забезпечення надійного та адаптивного кіберзахисту постає як ключове. Зокрема, поява гібридних, мультивекторних атак, що поєднують соціальну інженерію, шкідливе програмне забезпечення та уразливості інфраструктурного рівня, вимагає нових підходів до аналізу рівня безпеки.

Окрему загрозу становить можливість практичного використання квантових комп'ютерів, які потенційно здатні зруйнувати основи традиційної

криптографії, що унеможливлює використання класичних моделей оцінювання безпеки в постквантовому середовищі.

У зв’язку з цим зростає потреба в побудові нових науково обґрунтованих моделей, здатних комплексно враховувати різнорідні фактори загроз, у тому числі економічні, технологічні, організаційні та соціальні.

Розробка системи формалізованої оцінки рівня безпеки комп’ютерних систем із використанням синергетичних метрик та логіки гібридних загроз має важливе значення як для теорії кібербезпеки, так і для її практичного застосування в умовах зростання складності та динамічності кіберзагроз.

2. Зв’язок роботи з науковими програмами, планами, темами

Дисертаційне дослідження здійснювалося в межах наукової спеціальності 122 «Комп’ютерні науки» та виконувалося на базі кафедри програмної інженерії та інтелектуальних технологій управління НТУ «ХПІ».

Проведена робота безпосередньо пов’язана з кафедральною темою науково-дослідної діяльності університету «Розробка моделей, методів та інформаційних технологій оцінювання складних багатоознакових об’єктів і систем» (державний реєстраційний номер 0125U001121).

3. Наукова новизна одержаних результатів

Наукова новизна здобутих результатів полягає у теоретичному узагальненні та запропонуванні нового підходу до вирішення актуальної наукової проблеми – оцінювання рівня безпеки комп’ютерних систем з урахуванням гібридного характеру сучасних загроз та їх синергетичної дії. У межах дисертаційного дослідження отримано такі основні науково обґрунтовані результати:

1. Вперше запропоновано метод безперервного функціонування безпеки комп’ютерної системи, що дозволяє формувати контур безпеки безперервних бізнес-процесів комп’ютерної системи та забезпечити

своєчасне формування превентивних заходів проти цільових (змішаних) атак.

2. Вперше розроблено модель оцінки поточного стану рівня захищеності комп’ютерної системи, що дозволяє враховувати складові безпеки та ознаки гібридності та синергізму загроз на комп’ютерні системи.

3. Вперше запропоновано модель визначення рівня безпеки на основі комплексування різних метрик з метою одержання об'єктивної оцінки поточного стану рівня захищеності соціокіберфізичних систем, з урахуванням не лише обчислювальних та фінансових витрат зловмисника на реалізацію цільової атаки, а й рівня таємності.

4. Отримав подальший розвиток математичний апарат формування класифікатора загроз на основі врахування їх синергізму та гібридності, а також впливу загроз на критичні точки інфраструктури комп'ютерної мережі.

Вважаю, що дисертаційна робота є вагомим внеском у розвиток математичних моделей та прикладних обчислювальних методів для оцінювання рівня безпеки комп’ютерних систем.

4. Наукова та практична цінність одержаних результатів

Робота має логічно вибудувану структуру, в якій чітко простежується послідовність постановки дослідницьких завдань і шляхів їх реалізації. Результати дослідження підтверджені достатньо обґрунтованими доказами, а обрана математична база відповідає сучасним підходам у сфері комп’ютерної безпеки. Запропоновані автором підходи до оцінювання рівня захищеності комп’ютерних систем порівнювались із відомими методами, продемонстрували аргументовану ефективність на тлі актуальних наукових джерел.

Усі сформульовані в дисертаційній роботі висновки й практичні рекомендації логічно узгоджені з метою дослідження та його актуальністю.

Вони можуть бути використані для практичної реалізації в системах оцінювання кіберзахисту.

Запропоновані в роботі математичні моделі та методи, зокрема підхід до побудови моделі оцінювання рівня безпеки на основі інтеграції множини метрик та врахування синергетичних властивостей гібридних загроз, лягли в основу функціональних компонентів системи оцінки безпеки. Ці компоненти реалізовані у вигляді програмного забезпечення, що дозволяє оцінювати поточний стан захищеності комп'ютерної системи та виявляти потенційні вектори загроз з урахуванням актуальних викликів у сфері кібербезпеки.

Результати дисертації впровадженні та використані в оцінці системи безпеки ТОВ «НІКС СОЛЮШЕНС ЛТД» (м. Харків), а також використовуються в навчальному процесі НТУ «ХПІ».

5. Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором та академічна доброчесність

Результати дослідження представлено у 15 наукових публікаціях, з них: 5 статей, з яких 2 статті індексовано в наукометричній базі Scopus та/або Web of Science Core Collection, при цьому 2 статті опубліковано в журналах, віднесених до третього Q3 квартилю; 3 статті – в збірниках наукових праць, що входять до переліку фахових Міністерства освіти і науки України видань категорії Б; 10 публікацій – тези доповідей на конференціях (з яких 4 роботи видано в закордонних видавництвах).

Дисертація виконана з дотриманням вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи.

6. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

В результаті детального аналізу дисертаційної роботи можна стверджувати, що представлені в ній наукові положення, висновки та практичні рекомендації є вичерпними, логічно послідовними та належним чином обґрунтованими. Авторка об’єднала теоретичні підходи з експериментальною перевіркою, залучивши як українські, так і міжнародні джерела, що підтверджує актуальність і фахову глибину проведеного дослідження.

Достовірність результатів ґрунтується на застосуванні як класичних, так і сучасних методів аналізу, включаючи структуроване вивчення літератури, чітко сформульовані наукові завдання та логічно побудовану аргументацію. Отримані результати були представлені на міжнародних конференціях та опубліковані у спеціалізованих наукових виданнях, що свідчить про їх визнання науковою спільнотою.

Крім того, узгодженість висновків із наявними дослідженнями та ефективне практичне застосування результатів засвідчують їхню надійність. Дослідження повністю реалізувало поставлену мету та вирішило визначені завдання. Структура роботи дозволяє чітко простежити логіку дослідження, а сформульовані висновки надають повне уявлення про зміст кожного етапу. Комплексний підхід до аналізу об’єкта дослідження забезпечив високий рівень достовірності отриманих результатів.

Вищевикладене свідчить про обґрунтованість та достовірність наукових положень, висновків і рекомендацій, що викладено у дисертаційній роботі Звєрцевої Наталії Віталіївни.

7. Оцінка змісту дисертації, її завершеності й оформлення

Робота Звєрцевої Н.В. є завершеною науковою роботою, містить анотацію – українською та англійською мовами, вступ, чотири розділи, висновки, список використаних джерел і чотири додатки.

Дисертація присвячена удосконаленню методів оцінки безпеки комп'ютерних систем у контексті сучасних загроз, зокрема гібридних і постквантових, а також дослідженню практичного застосування запропонованих моделей у соціокіберфізичних системах.

Об'єктом є розробка та використання нових моделей і методів оцінювання рівня безпеки.

У **першому розділі** проведено аналіз стану інформаційної безпеки, класифікації кібератак і систем їх виявлення, визначено недоліки існуючих методів і обґрунтовано потребу в нових підходах.

Другий розділ присвячено методології створення моделей загроз на основі безпекових метрик, аналізу існуючих підходів і вибору оптимальних критеріїв для комплексної оцінки ризиків.

У третьому розділі представлені три розроблені моделі оцінки безпеки: стану захищеності з урахуванням гібридних загроз, забезпечення безперервного функціонування системи безпеки для критичних процесів і інтегрованої оцінки безпеки соціокіберфізичних систем.

Четвертий розділ містить верифікацію моделей, оцінку їх ефективності, а також опис архітектури і програмної реалізації системи автоматизованої оцінки безпеки для підтримки управлінських рішень у змінних умовах.

Висновки підсумовують досягнення дослідження, підтверджуючи виконання поставлених завдань і відповідність вимогам для здобуття наукового ступеня.

Список літератури охоплює широкий спектр джерел, включаючи іноземні, а додатки містять інформацію про практичне впровадження результатів, розширений перелік завдань і публікації автора.

8. Зауваження до дисертаційної роботи

1. В порівняльній таблиці 1.1 (с.38) існуючих систем виявлення та реагування на загрози немає чітких критеріїв оцінювання. Усі

характеристики мають бінарні значення («Так»/«Ні»), але відсутня шкала оцінки ефективності, якості або рівня реалізації функції. Це знижує аналітичну цінність таблиці.

2. На рисунку 3.5 (с.103) зображено зниження часу відновлення функціонування АБС (TOF) за рахунок застосування превентивних планів та заходів захисту, але графік ілюстративний, без вказівки часу в годинах/днях важко оцінити реальну ефективність впроваджених заходів.

3. На рисунку 3.6 (с.107) зображено модель ризику інформаційної безпеки, для якої відсутні позначеня ролей / суб'єктів. Через це не зрозуміло, який суб'єкт виконує дію, який суб'єкт формує вимоги, який суб'єкт проводить обробку ризиків? Це впливає на загальне сприйняття моделі.

4. Було б доцільно доповнити роботу економічним обґрунтуванням доцільності впровадження запропонованої моделі на практиці, зокрема через оцінку витрат на реалізацію та очікуваних вигод (наприклад, зменшення часу простою, зниження втрат від інцидентів тощо). Такий аналіз дозволив би наочно продемонструвати ефективність моделі в умовах реального функціонування інформаційних систем підприємства.

Проте наведені у результаті аналізу роботи зауваження не носять принципового характеру та жодним чином не знижують позитивне враження від роботи та її наукову та практичну цінність.

10. Відповідність дисертації встановленим вимогам і загальні висновки

Дисертаційна робота Звєрцевої Н.В. є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тема дослідження відповідає галузі знань 12 – «Інформаційні технології» та спеціальності 122 – «Комп'ютерні науки».

Отже, враховуючи актуальність теми, отримані результати та визначену практичну значущість вважаю, що дисертаційна робота Звєрцевої

Наталії Віталіївни «Моделі оцінки безпеки комп'ютерних систем» відповідає вимогам 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» від 12.01.2022 р. № 44 та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а сам автор, Звєрцева Наталія Віталіївна, заслуговує присудження їй наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки».

Рецензент:
професор кафедри кібербезпеки
Національного технічного університету
«Харківський політехнічний інститут»,
доктор технічних наук Станіслав МІЛЕВСЬКИЙ

«30» червня 2025р.

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
" " 20 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *