

ВІДГУК

офіційного опонента на дисертаційну роботу Полуциганової Вікторії Ігорівни на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах», представлену на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації.

Безпека кіберсистем різних державних і приватних установ має велике значення, особливо в умовах воєнного стану, оскільки будь-яке порушення їх цілісності або доступу до конфіденційної інформації може призвести до небажаних наслідків. Подібні ситуації трапляються в хмарних середовищах і системах критичної інфраструктури, де вони можуть завдати значної шкоди фінансової сфери та репутації. Усі такі системи мають певні типи вразливостей, які створюють загрози різного ступеня серйозності, починаючи від втрати доступу даних до повного знищення системи. Атаки на різні кіберсистеми по всьому світу підтверджують це.

На сьогоднішній день існуючі методи та методики, розроблені інформаційні технології та програмне забезпечення моделювання та дослідження безпеки кіберсистем не завжди забезпечують високі показники адекватності та якісної оцінки ризиків. Тому проблеми розробки процедур оцінки ризиків, удосконалення та впровадження нових методів кібербезпеки потребують вивчення та впровадження у критичній інфраструктурі.

Оцінювання ризиків при реалізації вразливостей є актуальною задачею для створення систем захисту кіберсистем. Запропонований метод включає урахування впливу структурних особливостей у взаємозалежності між вразливостями та загрозами та допомагає точніше оцінити рівень ризику та зрозуміти його природу та характер. Тому подане авторкою дослідження, спрямоване на створення ефективного методу для аналізу ризиків, має безумовну актуальність.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- вперше побудовано модель зв'язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;

- вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;

– вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;

– розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

Достовірність отриманих результатів забезпечується коректним застосуванням понять і математичного апарату структурного аналізу, теорії ймовірностей, теорії ризику, адекватність і ефективність яких підтверджується великим досвідом їх використання. Аналіз досліджених у роботі прикладів підтверджує як можливість практичного застосування, так і ефективність розробленого методу оцінювання ризику та відповідних обчислювальних процедур.

Наукові дослідження були виконані здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського в рамках НДР «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» державний реєстраційний номер 0124U001957 під керівництвом доцентом кафедри інформаційної безпеки, к.ф.-м.н., с.н.с. Смирновим Сергієм Анатолійовичем.

Наукові напрацювання дисертаційного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК. Теоретичні та практичні результати наукового дослідження використані для вдосконалення державної політики з питань національної безпеки у сфері забезпечення кібербезпеки, насамперед щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем об'єктів критичної інфраструктури, зокрема паливно-енергетичного сектору.

Теоретичні та практичні результати застосовуються у навчальному процесі кафедри інформаційної безпеки НТУУ «КПІ ім. Ігоря Сікорського» при підготовці та викладанні курсів «Рішення в умовах невизначеності та ризику», «Проблеми кібербезпеки критичної інфраструктури», «Математичні моделі кібербезпеки».

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Полуциганової В. І. повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та напрямкам досліджень відповідно до освітньої програми Кібербезпека.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям 12 Інформаційні технології.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Полуциганової Вікторії Ігорівни є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагиату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Матеріал дисертаційної роботи повністю відповідає вимогам щодо грамотності та стилю викладення результатів. Автор роботи при викладенні матеріалу дотримується сучасної загальноприйнятої у даній сфері науки термінології.

Дисертація складається з вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 207 сторінок.

У вступі підтверджується актуальність теми дисертаційного дослідження, вказується на зв'язок з науковим планом, програмою і темою, викладається мета і завдання дослідження. Також описано наукову новизну та практичне значення отриманих результатів та надано відомості про впровадження, затвердження та публікацію результатів.

Розділ 1 охоплює поточний стан методів оцінки ризиків, структурний аналіз складних кіберсистем, аналіз уразливості та загроз в кібербезпеці, а також описує поточний стан досліджень питань, подібних до тих, що обговорюються в цій статті. Узагальнено основні методи структурного аналізу, розроблені в дисертаційному дослідженні, а саме Q-аналіз, топологічний аналіз і симпліціальний аналіз. Проаналізовано основні етапи життєвого циклу вразливості кіберсистеми. Розглянуто основні методи оцінки ризику на основі методів Вальда та Байєса.

Розділ 2 визначає та аналізує основні показники вразливостей кіберсистеми та описує структуру системи загроз. Встановлено, що основними ознаками, достатніми для однозначної ідентифікації (і відновлення) структури складних систем, є локальні карти, структурні дерева та структурні графи. У цьому розділі описані алгоритми переходу від матриці інцидентності уразливостей та загроз до побудови матриці симпліціального комплексу та інших складних структурних характеристик. Наведено класифікацію та структурний аналіз вразливих систем, що значно допомагає у запобіганні та подоланні несприятливих наслідків, викликаних реалізацією загроз.. Було створено алгоритм для класифікації типів загроз на основі сумісності вразливостей.

Розділ 3 розробляє підхід до оцінки ризику на основі складної структурованої інформації про залежності вразливостей, загроз і втрат під час інциденту. Щоб розглянути вплив існуючих взаємозв'язків між уразливими місцями, використовується модель взаємодії вразливості та загрози на основі побудови симпліційного комплексу. У ході дослідження

були уточнені оцінки відповідних ймовірностей і втрат. У цьому документі розроблено метод оцінки ризику, заснований на складній структурі ідентифікованих загроз і вразливостей кіберсистеми. Визначено, що цей метод розрахунку будь-яких адитивних властивостей комплексу за його структурними компонентами буде коректним за умови дотримання процедури синтезу комплексу та врахування включення-виключення вкладів компонентів.

Розділ 4 проводить прикладне дослідження на основі методу, розробленого у дисертації. Розглянуто загрози та вразливі місця для інформаційних підсистем критичної інфраструктури. Вони пов'язані з потенційно вразливими компонентами, які можуть стати об'єктами кібератак. Для виявлення можливих сумісних реалізацій загроз було проведено структурний аналіз, який проявляється складними взаємозалежностями між вразливими місцями та загрозами. Уразливості класифіковано на основі параметрів системи загроз у вибраній системі критичної інфраструктури. Отримана оцінка ризику була проаналізована на основі ймовірності виникнення загрози (визначається обставинами атаки на систему) та оцінки втрат від її реалізації за допомогою експертів.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких: 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України.

Також результати дисертації були апробовані на 8 наукових фахових конференціях.

Усі публікації здобувачки мають високий науковий рівень. У них детально розкриваються основні наукові результати виконаного дослідження. Особистий внесок здобувачки до публікацій за співавторством вагомий, особливо у описі експериментальних частин роботи. Принципів академічної доброчесності у жодній з публікацій не порушено.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. При описі алгоритмів, розроблених на основі Q-аналізу, не наведені характеристики їх складності. Доцільно було провести аналіз залежності роботи алгоритмів від кількості елементів симплекційного комплексу.

2. В роботі детально розібрано приклад оцінки ризику на основі сиплекційного комплексу вразливостей, але не розглянуто симплекційний комплекс загроз.

3. Використання складного ілюстративного матеріалу в тексті дисертації, які доречніше було винести у додатки.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Полудиганової Вікторії Ігорівни на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах», виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для Інформаційних технологій. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «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 р. № 44.

Здобувач Полудиганова Вікторія Ігорівна заслуговує на присудження ступеня доктора філософії в галузі знань Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

ОФІЦІЙНИЙ ОПОНЕНТ:

професор кафедри кібербезпеки та
захисту інформації

КНУ ім. Тараса Шевченка

д.т.н., професор

/  /

Сергій ТОЛЮПА

М.П. «___» _____ 20__ року

Підпис професора Толюпи С.В. засвідчую.

Заступник декана факультету інформаційних
технологій з наукової роботи
кандидат технічних наук наук





Григорій ГНАТІЄНКО