ВІДГУК

офіційного опонента
доктора технічних наук, професора Хлапоніна Юрія Івановича
на дисертаційну роботу Підлісного Юрія Івановича
на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ»,
подану на здобуття наукового ступеня доктора філософії
до разової спеціалізованої вченої ради
Національного університету «Чернігівська політехніка»
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми дисертації

IoT-середовища складаються з пристроїв, які відрізняються призначенням, обчислювальними можливостями, засобами захисту та способами взаємодії. Під час експлуатації змінюються їх конфігурація, зв'язки й умови роботи. Через це оцінювання ризиків потребує врахування не лише загроз і вразливостей, а й ролі конкретного пристрою та можливих наслідків порушення його функціонування.

Для аудиту важливо поєднати ці відомості з даними про поточний стан безпеки. Частина оцінок при цьому має якісний характер, а дані можуть бути неповними. Водночас результат має залишатися зрозумілим для фахівця, який приймає рішення щодо заходів захисту. Це визначає потребу в моделях подання контекстної інформації та методах її використання під час оцінювання ризику.

У дисертації Підлісного Юрія Івановича запропоновано формувати контекстно-ризиковий профіль IoT-пристрою та на його основі уточнювати параметри нечіткого оцінювання. Такий підхід пов'язує характеристики пристрою з результатом аналізу ризику й дає змогу пояснювати оцінку через вхідні параметри та правила. Вважаю тему роботи актуальною для розвитку засобів аудиту інформаційної безпеки IoT-середовищ.

Мета, об'єкт і предмет дослідження

Метою дослідження є розроблення моделі формування контекстно-ризикового профілю IoT-пристрою та удосконалення методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням характеристик пристрою, поточного стану безпеки й попередньо сформованого показника ризику прихованої компрометації в процесі аудиту.

Об'єктом дослідження є процеси оцінювання ризиків інформаційної безпеки IoT-середовищ під час аудиту в умовах гетерогенності компонентів,

динамічності структури й функціонування та невизначеності параметрів середовища.

Предмет дослідження охоплює модель формування контекстно-ризикового профілю, метод оцінювання ризиків на основі нечіткого виведення типу Мамдані з урахуванням попередньо сформованого показника ризику прихованої компрометації та підхід до побудови інформаційної технології їх узгодженого застосування.

Наукова новизна результатів дисертаційної роботи

Науковий внесок автора визначають три взаємопов'язані результати.

1. Вперше розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Модель враховує рівень вбудованого інтелекту, характеристики безпеки, архітектуру взаємодії, функціональний контекст та динамічність середовища. Її особливістю є збереження результатів класифікації за окремими критеріями без зведення їх до одного числового показника. Це забезпечує змістову основу для визначення та інтерпретації параметрів оцінювання ризику.

2. Удосконалено метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані. Метод спільно враховує критичність активу, рівні загрози та вразливості, можливості потенційного порушника, імовірність реалізації загрози, тяжкість наслідків і попередньо сформований показник BackdoorRisk. Контекстно залежні параметри уточнюються з урахуванням профілю пристрою та поточного стану безпеки. Інтегральний показник RiskLevel визначається за допомогою функцій належності та бази нечітких правил, що дає змогу пояснювати отриманий результат.

3. Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків. Підхід установлює порядок узгодженого застосування моделі формування профілю та методу нечіткого оцінювання, використання поточних даних про безпеку й повторного визначення ризику в разі зміни характеристик пристрою або середовища. На його основі визначено архітектуру технології, функціональні компоненти та інформаційні потоки між ними.

Практична цінність одержаних результатів

Практичним результатом роботи є програмний прототип ризикового модуля, створений у MATLAB із використанням Fuzzy Logic Toolbox. Реалізовано FIS-модель Мамдані із сімома входами, виходом RiskLevel і базою з 40 унікальних продукційних правил. Модуль обробляє попередньо

підготовлені параметри та визначає інтегральну оцінку і відповідну категорію ризику.

Окремо досліджено класифікацію мережевих подій як засіб отримання відомостей про активність у середовищі. Результати цього дослідження та перевірки FIS мають різне призначення й обґрунтовано оцінюються окремо. Показник BackdoorRisk надходить до ризикового модуля як готовий вхід; його використання не означає, що модуль самостійно виявляє приховану компрометацію.

У дисертації наведено матеріали про впровадження результатів у ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС», ТОВ «АТРІЯ КОМПАНІ» та в освітній процес Національного університету «Чернігівська політехніка». Розроблені рішення можуть використовуватися для підтримки аудиту, порівняння ризиків і визначення пріоритетів заходів захисту.

Методи дослідження

Для аналізу IoT-середовищ та зв'язків між їх компонентами автор використав системний аналіз та інформаційне моделювання. Апарат нечітких множин і нечіткого логічного виведення застосовано для побудови методу оцінювання. Програмне й сценарне моделювання використано для реалізації прототипу та перевірки його поведінки. Порівняльний і статистичний аналіз дозволили кількісно оцінити результати. У дослідженні мережевих подій окремо застосовано методи машинного навчання.

Обґрунтованість наукових положень, висновків і рекомендацій

Завдання роботи сформульовано відповідно до її мети. Автор показує, які обмеження відомих підходів зумовили потребу у формуванні профілю та як цей профіль використовується для уточнення параметрів ризику. Теоретичні положення доповнено програмною реалізацією та експериментами.

Роботу FIS перевірено аналізом спрацьовування правил, поверхонь виведення та покомпонентної монотонності для опорної конфігурації. Під час порівняння контекстних конфігурацій функції належності, база правил і механізми виведення залишалися незмінними. Це дозволяє пов'язувати відмінності результатів зі зміною входів моделі.

Сценарну вибірку обсягом 100 000 записів розподілено на валідаційну частину з 60 000 сценаріїв і незалежну тестову частину з 40 000 сценаріїв. Порогові значення визначено на валідаційній частині за критерієм максимізації F1-міри, а остаточні показники отримано на тестовій. Для запропонованої FIS-моделі наведено Accuracy = 0,971175, F1-міру = 0,982012 та FPR = 0,078250. Порівняно із семипараметричною зваженою моделлю

Accuracy збільшилася на 0,018675, F1-міра – на 0,011565, а FPR зменшилася на 0,058750.

Експеримент із почерговою фіксацією контекстно залежних параметрів дозволив оцінити їхній внесок. Найбільше зниження F1-міри спостерігалося для ThreatLevel, Vulnerability та ImpactSeverity. Одночасна фіксація п'яти параметрів на рівні 5 спричинила віднесення всіх тестових сценаріїв до ризикового класу. Цей результат характеризує саме обрану контрольну конфігурацію та підтверджує значення контекстної варіативності в межах сформованої вибірки; його не слід поширювати на всі можливі моделі без контекстного уточнення.

Окреме дослідження класифікації мережевих подій виконано з використанням даних BoT-IoT, TON_IoT та Edge-IIoTset. На незалежній тестовій частині з 4105 записів для XGBoost отримано Accuracy = 0,9481, F1-міру = 0,9374 та FPR = 0,0238. Ці показники належать до завдання класифікації мережевих подій і обґрунтовано розглядаються окремо від результатів сценарного оцінювання ризиків.

Додаткові експерименти із фіксацією BackdoorRisk та пропущеними значеннями розкривають чутливість моделі. Зокрема, фіксація BackdoorRisk на рівні 5 змінила категорію ризику у 7,7025 % тестових сценаріїв. За 30 % пропущених значень із медіанним заміщенням середня абсолютна зміна RiskLevel становила 0,577, а зміна категорії ризику спостерігалася у 23,96 % контрольних комбінацій. Ці результати дають підстави оцінити межі стійкості моделі та необхідність контролю якості вхідних даних.

Наведені показники підтверджують результативність запропонованих рішень в умовах проведених експериментів. Водночас сценарна перевірка не охоплює всіх умов експлуатації реальних IoT-середовищ. Для перенесення методу в конкретну систему потрібні налаштування вхідних оцінок та додаткова перевірка, що узгоджується з обмеженнями, зазначеними автором.

Зв'язок роботи з науковими програмами, планами і темами

Дослідження виконано в Національному університеті «Чернігівська політехніка» та пов'язане з науково-дослідними роботами «Методологія побудови захищеного кіберпростору» (державний реєстраційний номер 0124U004485), «Моделі та методи забезпечення безпеки й довіри в кіберпросторі з урахуванням клептографічних загроз» (0126U001352) та «Методи й моделі забезпечення цілісності даних у каналах керування БпЛА в умовах застосування засобів РЕБ» (0125U001728). Наведений у дисертації зв'язок із цими темами узгоджується з дослідженням контекстно залежних ризиків, прихованих загроз і засобів підтримки аналізу безпеки.

Оцінка змісту дисертації та її завершеності

Дисертація містить вступ, чотири розділи, висновки, список використаних джерел та додатки. Її побудова відповідає послідовності розв'язання поставленого наукового завдання.

У вступі обґрунтовано актуальність теми, визначено мету, завдання, об'єкт і предмет дослідження, наведено методи, наукову новизну, практичне значення, відомості про апробацію та особистий внесок здобувача.

У першому розділі проаналізовано загрози, вразливості та особливості захисту IoT-середовищ, сучасні методи класифікації, оцінювання ризиків і аудиту. Виявлені обмеження слугують підставою для подальшого врахування функціонального контексту та невизначеності даних.

У другому розділі викладено модель формування контекстно-ризикового профілю, визначено склад і зміст параметрів оцінювання, обґрунтовано застосування нечіткого виведення типу Мамдані. Розділ містить основні теоретичні положення роботи та описує зв'язок між класифікаційними характеристиками пристрою й оцінюванням ризику.

У третьому розділі розглянуто побудову інформаційної технології, її архітектуру, функціональні компоненти, інформаційні потоки та порядок взаємодії в процесі аудиту. Запропонована організація пов'язує формування профілю з підготовкою вхідних даних і повторним оцінюванням ризику.

У четвертому розділі наведено реалізацію програмного прототипу та експериментальні результати. Досліджено класифікацію мережевих подій, результативність FIS-моделі, вплив контекстного уточнення, варіативності BackdoorRisk і пропущених даних. Висвітлено часові характеристики нечіткого виведення та обмеження застосування результатів.

Загальні висновки узгоджуються з поставленими завданнями й основними результатами розділів. Робота є завершеним дослідженням, у якому теоретичні положення доповнено програмною реалізацією та кількісним оцінюванням.

Повнота висвітлення основних результатів у наукових публікаціях

За наведеними в дисертації відомостями, результати дослідження висвітлено в 11 наукових працях, зокрема у п'яти статтях у фахових виданнях України та шести публікаціях апробаційного характеру. Тематика праць охоплює класифікацію IoT-середовищ, аудит, захист приватності, побудову правил нечіткого оцінювання та врахування прихованих загроз. Сукупність представлених публікацій відображає основні напрями дисертаційного дослідження.

У вступі зазначено особистий внесок здобувача у розроблення моделі, удосконалення методу, побудову інформаційної технології та проведення

експериментів. Представлені в роботі результати утворюють цілісне дослідження, а відомості про апробацію свідчать про їх обговорення на наукових заходах.

Мова та оформлення дисертації

Дисертацію написано українською мовою. Матеріал викладено послідовно: від аналізу проблеми до формалізації, архітектури технології та експериментальної перевірки. Таблиці й рисунки допомагають зіставити запропоновані рішення та їх результати. Анотації українською й англійською мовами відображають основний зміст роботи.

Дотримання принципів академічної доброчесності

У тексті наведено посилання на використані джерела, описано власні результати та особистий внесок здобувача. Оцінку академічної доброчесності під час офіційного розгляду роботи слід також узгодити з результатами перевірки, проведеної університетом.

Зауваження щодо змісту дисертації та її оформлення

Загалом робота заслуговує на позитивну оцінку. Водночас вважаю за потрібне звернути увагу на такі питання.

1. Для практичного використання моделі варто докладніше подати процедуру переходу від характеристик профілю та поточних даних безпеки до числових значень AC, TL, V, L та IS. Зокрема, корисними були б приклади для пристроїв із різним призначенням і пояснення дій у разі суперечливих вхідних даних.

2. У роботі реалізовано 40 унікальних нечітких правил. Доцільно детальніше пояснити їх добір, порядок експертного погодження та налаштування функцій належності. Додаткова перевірка за інших параметрів цих функцій допомогла б оцінити чутливість результатів до налаштування FIS.

3. Контрольна конфігурація без контекстного уточнення сформована шляхом одночасної фіксації п'яти параметрів на рівні 5. Такий експеримент показує вплив обраного способу усунення контекстної варіативності. Варто докладніше обґрунтувати саме цей контроль та пояснити межі поширення отриманого порівняння на інші способи формування вхідних оцінок.

4. BackdoorRisk надходить до системи як попередньо сформований показник. Для застосування методу поза сценарним експериментом потрібно уточнити джерела цієї оцінки, її нормалізацію та перевірку достовірності. Важливо також пояснити, як помилки BackdoorRisk можуть впливати на підсумкову категорію ризику.

5. Наведений середній час нечіткого виведення 0,0543 мс для одного запису характеризує роботу ризикового модуля. Для оцінювання швидкодії всієї технології необхідно додатково враховувати час збирання даних, формування профілю та підготовки вхідних параметрів.

6. Повторне визначення ризику передбачено в архітектурі технології. Було б корисно конкретизувати умови запуску такого оцінювання: які зміни характеристик пристрою або стану безпеки потребують негайного перегляду, а які можуть враховуватися під час чергового аудиту.

Зауваження стосуються деталізації процедур, меж експериментального оцінювання та подальшого практичного розвитку технології. Вони не ставлять під сумнів основні результати й не змінюють позитивної оцінки дисертації.

Висновки

Дисертаційна робота Підлісного Юрія Івановича «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ» є завершеною кваліфікаційною науковою працею. У ній розв'язано актуальне наукове завдання розроблення моделі формування контекстно-ризикового профілю IoT-пристрою та удосконалення методу оцінювання ризиків у процесі аудиту. На основі моделі й методу створено інформаційну технологію їх узгодженого застосування.

За актуальністю, науковою новизною, обґрунтованістю результатів і практичним значенням дисертація відповідає вимогам до робіт на здобуття ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. Основні результати висвітлено у наукових публікаціях та перевірено експериментально.

Вважаю, що автор роботи, Підлісний Юрій Іванович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки галузі знань 12 – Інформаційні технології.

Офіційний опонент:

професор кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету

доктор технічних наук, професор Юрій ХЛАПОНІН

«02» листопада 2026 року

Підпис Юрія Хлапоніна засвідчую

Начальник відділу кадрів Н. Шевченко