ВІДГУК

офіційного опонента
доктора технічних наук, професора Хоми Володимира Васильовича
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

Розвиток технології Інтернету речей супроводжується невпинним зростанням числа гетерогенних та ресурсно обмежених пристроїв, які функціонують у динамічних середовищах. Внаслідок цього критично розширюється поверхня кіберзагроз, що ускладнює своєчасне виявлення вразливостей і оцінювання пов'язаних з ними ризиків інформаційної безпеки. Традційні статичні моделі з фіксованми наборами параметрів не здатні враховувати оперативні зміни конфігурацій, мережевого оточення та поведінки пристроїв, що зумовлює потребу у розробленні контекстно-адаптивних методів і моделей оцінювання ризиків. Вибір ефективних заходів захисту вимагає врахування функціоналу пристроїв, характеру взаємодії та умов експлуатації, які визначають критичність наслідків їх потенційної компрометації.

Викликом для задачі аналізу ризиків є якісний характер багатьох характеристик IoT-пристроїв та неповннота даних про їх поточний стан. Для вирішення цього науково-прикладного завдання доцільно поєднати формалізовані профілі безпеки з апаратом нечіткої логіки, що дає змогу узгодити різнорідні показники та поєднати кількісні оцінки зі змістовими правилами інтерпретації.

Саме цей зв'язок досліджено у дисертації Підлісного Юрія Івановича. Автором розроблено модель формування контекстно-ризикового профілю, удосконалено метод визначення інтегрального показника RiskLevel та встановлено порядок їх застосування в інформаційній технології аудиту. Така постановка є актуальною для комп'ютерних наук, оскільки охоплює повний цикл розробки систем - від моделювання, оброблення даних, алгоритмізації до програмної реалізації та експериментальних досліджень.

Мета, об’єкт і предмет дослідження

Мета роботи полягає в розробленні моделі формування контекстно-ризикового профілю IoT-пристрою та удосконаленні методу оцінювання ризиків інформаційної безпеки IoT-середовищ з урахуванням характеристик пристрою, поточного стану безпеки й попередньо сформованого в процесі аудиту показника ризику прихованої компрометації.

Об’єкт дослідження – процеси оцінювання ризиків інформаційної безпеки IoT-середовищ під час аудиту за умов неоднорідності компонентів, зміни структури й функціонування та невизначеності параметрів середовища.

Предмет дослідження охоплює модель формування контекстно-ризикового профілю IoT-пристрою, 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 одержаних результатів

Особистий науковий внесок здобувача простежується в трьох взаємопов’язаних результатах, що утворюють логічну послідовність.

Першим науковим результатом є вперше розроблена модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Для профілю використано п’ять критеріїв: рівень вбудованого інтелекту, характеристики безпеки, архітектуру взаємодії, функціональний контекст і динамічність середовища. Принциповим є збереження змісту характеристик за кожним критерієм без їх попереднього зведення до єдиного числового індексу. Завдяки цьому профіль може використовуватися для контекстної інтерпретації параметрів ризику.

Другим результатом є удосконалений метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ. У системі нечіткого виведення типу Мамдані одночасно враховано критичність активу, рівень вразливості, можливості потенційного порушника, ймовірність реалізації загрози, критичність наслідків і показник BackdoorRisk. Профіль та дані про поточний стан безпеки використовуються для уточнення контекстно залежних параметрів. Показник BackdoorRisk включено як окрему попередньо сформовану оцінку ризику прихованої компрометації. Наукове значення методу полягає в узгодженому врахуванні цих чинників за допомогою функцій належності й нечітких правил із визначенням показника RiskLevel.

Третій результат стосується подальшого розвитку підходу до побудови інформаційної технології оцінювання ризиків. Новизна полягає у

комплексному використанні сформованого ризикового профілю пристрою разом із даними про поточний стан безпеки для формування вхідних параметрів нечіткого оцінювання. Цей результат доповнює модель і метод описом умов їх узгодженого застосування в процесі аудиту.

Оцінюючи новизну роботи, слід зазначити, що використання нечіткого виведення саме по собі є відомим. Внесок здобувача визначається конкретною організацією контекстної інформації, складом взаємопов'язаних параметрів, правилами їх опрацювання та узгодженням цих рішень у межах запропонованої технології.

Практична цінність результатів

Практичну реалізацію представлено ризиковим модулем у середовищі MATLAB із використанням Fuzzy Logic Toolbox. Модуль має сім входів, один вихід RiskLevel і базу з 40 унікальних продукційних правил. Він дає змогу виконувати нечітке оцінювання на підготовлених даних та аналізувати зв'язок результату зі спрацьовуванням правил.

Окремою практичною складовою є експериментальне дослідження класифікації мережевих подій. Його результати можуть бути використані для інформаційного забезпечення аналізу активності в IoT-середовищі. При цьому реалізований FIS-модуль та процедура класифікації розглядаються як окремі експериментальні засоби, що забезпечує коректне тлумачення їх функцій і отриманих показників.

У роботі наведено матеріали щодо використання результатів у ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС», ТОВ «АТРІЯ КОМПАНІ», а також в освітньому процесі Національного університету «Чернігівська політехніка». Прикладна цінність полягає у можливості систематизувати характеристики пристроїв, підтримувати оцінювання ризиків і визначати пріоритети подальшого аналізу безпеки.

Методи дослідження

Методологічну основу роботи становлять системний аналіз, інформаційне моделювання, теорія нечітких множин та нечітке логічне виведення. Їх використано для опису характеристик пристроїв, побудови профілю та визначення RiskLevel. Програмне і сценарне моделювання застосовано для перевірки запропонованих рішень, а порівняльний та статистичний аналіз – для оцінювання результатів. Методи машинного навчання використано в задачі класифікації мережевих подій.

Обґрунтованість наукових положень, висновків і рекомендацій

Для досягнення поставленої мети автор застосовує комплексний методологічний апарат, що охоплює системний аналіз, формалізоване подання характеристик пристроїв, нечітке логічне виведення та експериментальне порівняння конфігурацій моделі. Взаємозв'язок обраного інструментарію повністю відповідає логіці дослідження. Валідація розробленої моделі включає аналіз правил, поверхонь виведення й перевірку покомпонентної монотонності для опорної конфігурації.

Суттєвою перевагою експериментального плану є розділення добору порога й остаточного оцінювання. Із 100 000 сценаріїв 60 000 відведено для валідації та 40 000 – для незалежного тестування. Пороги кожної конфігурації визначалися за максимумом F1-міри на валідаційній частині. Для повної FIS-моделі на тестовій частині отримано Accuracy = 0,97, Precision = 0,98, Recall = 0,98 та F1-міру = 0,98. Значення FPR становило 0,078, а Specificity – 0,92.

Порівняно із семипараметричною зваженою моделлю зафіксовано збільшення Accuracy на 0,019 і F1-міри на 0,012 за зменшення FPR на 0,059. Застосування кількох показників дозволяє оцінювати результативність ширше, ніж за однією часткою правильних рішень. Разом із тим отримані значення характеризують умови проведеного сценарного експерименту.

Вплив контекстного профілю досліджено шляхом почергової та одночасної фіксації параметрів AssetCriticality, ThreatLevel, Vulnerability, Likelihood та ImpactSeverity. При цьому структуру нечіткого виведення збережено. Такий прийом дає змогу дослідити чутливість результатів до контекстного уточнення. Найбільше погіршення F1-міри встановлено за фіксації ThreatLevel, Vulnerability та ImpactSeverity. Результат одночасної фіксації п'яти параметрів слід інтерпретувати щодо цього конкретного способу формування контрольних входів.

У дослідженні мережевих подій використано уніфіковану вибірку на основі датасетів BoT-IoT, TON_IoT та Edge-IIoTset. Для XGBoost на тестовій частині обсягом 4105 записів одержано Accuracy = 0,95, F1-міру = 0,94 і FPR = 0,024. Ці результати відображають якість класифікації подій і не підміняють перевірку методу визначення RiskLevel.

Дослідження варіативності BackdoorRisk та пропусків даних доповнюють оцінку моделі. За фіксації BackdoorRisk на рівні 5 категорія ризику змінилася у 7,7 % тестових сценаріїв, а FPR зросла до 0,091. За 30 % пропущених значень із медіанним заміщенням середня абсолютна зміна RiskLevel становила 0,58. Отже, робота містить не лише оцінювання

результативності, а й кількісні оцінки про залежність висновків від якості та варіативності вхідних даних.

Сукупність наведених досліджень підтримує основні висновки дисертації. Подальше перенесення методу в конкретну предметну область потребуватиме налаштування шкал і перевірки на даних відповідного середовища, що узгоджується з описаними автором обмеженнями.

Зв'язок роботи з науковими програмами, планами і темами

Роботу виконано в Національному університеті «Чернігівська політехніка». Згідно з відомостями поданими у дисертації, її результати пов'язані з виконанням тем «Методологія побудови захищеного кіберпростору» (0124U004485), «Моделі та методи забезпечення безпеки й довіри в кіберпросторі з урахуванням клептографічних загроз» (0126U001352), «Методи й моделі забезпечення цілісності даних у каналах керування БпЛА в умовах застосування засобів РЕБ» (0125U001728). Предмет дослідження узгоджується з цією тематикою в частині аналізу загроз, урахування контексту функціонування та підтримки рішень щодо захисту інформації.

Оцінка змісту та завершеності дисертації

Структура дисертації охоплює вступ, чотири розділи, загальні висновки, список використаних джерел та додатки. Матеріал організовано відповідно до переходу від аналізу проблеми до формалізації, технологічної побудови та експериментальної перевірки.

У вступі визначено наукове завдання та очікувані результати, обґрунтовано актуальність, сформульовано мету й завдання, окреслено об'єкт і предмет. Наведено відомості про новизну, практичне застосування, апробацію та внесок здобувача.

Перший розділ формує аналітичну основу роботи. Розглянуто особливості загроз і вразливостей IoT-середовищ, підходи до класифікації та оцінювання ризиків, можливості засобів аудиту. На основі узагальнення обмежень відомих підходів обґрунтовано потребу узгодженого врахування контексту.

У другому розділі обґрунтовано і представлено методологічні засади дослідження. Подано критерії інтелектуально-контекстної класифікації, модель формування профілю та його використання при визначенні параметрів ризику. Розглянуто нечітке оцінювання й принципи побудови відповідної інформаційної технології.

Третій розділ розкриває архітектурне подання технології. Опис функціональних компонентів та інформаційних потоків пояснює, як

результати класифікації й відомості про стан безпеки використовуються в процесі аудиту та повторного визначення рівня ризику.

Четвертий розділ містить програмну реалізацію й експериментальну частину. Представлено перевірку ризикового модуля, порівняння моделей, дослідження контекстних параметрів, BackdoorRisk і пропущених даних. Окремо розглянуто класифікацію мережевих подій та часові характеристики виведення.

Висновки узагальнюють результати відповідно до завдань дослідження. Між розділами наявний логічний зв'язок, а теоретична та експериментальна частини взаємно доповнюють одна одну. Це дає підстави оцінити дисертацію як завершену наукову працю.

Повнота висвітлення результатів у наукових публікаціях

Наведений у дисертації список містить 11 праць за темою дослідження: п'ять статей у фахових виданнях України та шість публікацій, що засвідчують апробацію. Вони охоплюють класифікацію IoT-середовищ, аудит, приватність, нечітке оцінювання та приховані загрози. Зміст публікацій узгоджується з основними напрямами роботи.

Відомості про особистий внесок подано у вступі. Автор пов'язує свій внесок із формуванням моделі профілю, удосконаленням методу, розробленням технології та експериментальним дослідженням. Представлення результатів на наукових заходах забезпечило їх апробацію в межах відповідної фахової тематики.

Мова, оформлення та відповідність анотації

Дисертацію викладено українською мовою. Матеріал подано послідовно, а формалізовані описи, таблиці й рисунки допомагають зрозуміти модель та інтерпретувати експерименти. Анотації українською й англійською мовами узгоджуються з основними положеннями роботи. Окремі терміни та скорочення потребують редакційного узгодження, проте це не змінює змісту наукових результатів.

Дотримання принципів академічної доброчесності

У роботі наведено посилання на джерела та відомості про особистий внесок здобувача. Під час офіційного розгляду оцінку академічної доброчесності слід також узгодити з результатами перевірки дисертації в університеті.

Зауваження щодо змісту дисертації та її оформлення

1. Застосування нечіткого виведення типу Мамдані є обгрунтованим з огляду на вимоги інтерпретованості оцінок. Водночас для більш переконливої аргументації доцільно було зіставити цей вибір з альтернативними схемами (зокрема, Сугено) за критеріями обчислювальних витрат, складності налаштування та пояснюваності в задачах аудиту.

2. Профіль формується за п’ятьма критеріями, проте реальні характеристики пристроїв є різнорідними та частково взаємопов’язаними. У зв’язку з цим потребують додаткового обговорення питання забезпечення однозначності категоризації пристроїв, узгодженості оцінок різних експертів та опрацювання ситуацій із відсутніми (невизначеними) критеріями. Доцільно було б проілюструвати такі випадки на прикладах пристроїв із різним функціональним призначенням.

3. У моделі одночасно поєднуються рівень вразливості, можливості порушника, ймовірність реалізації загрози, а також критичність активу й тяжкість наслідків. Доцільно детальніше обгрунтувати межі застосування цих параметрів і спосіб урахування їх взаємозалежностей у правилах нечіткого виведення. Це дало б змогу чіткіше оцінити, за яких умов пов’язані характеристики взаємно доповнюються, а за яких виникає ризик дублювання (повторного врахування) одного й того самого чинника.

4. Оптимізація порога класифікації за F1-мірою є обгрунтованою для порівняльного експерименту, проте під час реального аудиту критичності пропущеної загрози та хибного спрацювання зазвичай є різними. Доцільно було б проаналізувати, як змінюються рішення за інших критеріїв вибору порога, різного співвідношення ризикових сценаріїв або за заданого допустимого рівня FPR. Крім того, варто чіткіше розмежувати експериментальний поріг прийняття бінарного рішення та градаційні межі категорій шкали RiskLevel.

5. Експериментальна перевірка стійкості до пропущених значень виконувалася із застосуванням медіанного заміщення. Для повнішого дослідження стійкості варто було б розглянути сценарії, коли пропуски є зосередженими в окремих параметрах або пов’язані з поточним станом пристрою. Також доцільно уточнити, яким чином користувач інформаційної технології має враховувати частку заміщених значень та можливу зміну категорії ризику під час прийняття остаточного рішення.

Висловлені зауваження стосуються методичних уточнень, додаткових умов перевірки та перспектив розвитку підходу. Вони не підважують та не

спростовують одержаних результатів, а також не змінюють загальної позитивної оцінки дисертаційної роботи.

Висновки

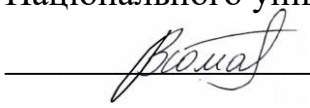
Дисертаційна робота Підлісного Юрія Івановича на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ» є цілісним та завершеним науковим дослідженням, у якому розв’язано актуальне науково-прикладне завдання – формування ризикового профілю IoT-пристрою за результатами інтелектуально-контекстного аналізу та його застосування для підвищення обгрунтованості оцінювання ризиків інформаційної безпеки динамічних IoT-середовищ у процесі аудиту. Отримані наукові результати є новими, обгрунтованими, достатньою мірою висвітленими у публікаціях. Їх достовірність підтверджено програмною реалізацією та експериментальними дослідженнями.

За актуальністю, обсягом виконаних досліджень, науковою новизною і практичною цінністю робота відповідає вимогам до дисертацій на здобуття освітньо-наукового ступеня доктора філософії.

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

Офіційний опонент

доктор технічних наук, професор,я
професор кафедри захисту інформації
Національного університету «Львівська політехніка»



Володимир ХОМА

«27» жовтня 2026 року