ВІДГУК

офіційного рецензента на дисертаційну роботу

Підлісного Юрія Івановича

на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ»,

представлену на здобуття ступеня доктора філософії

в галузі знань Інформаційні технології

за спеціальністю 122 – Комп'ютерні науки

Актуальність теми дисертації

Оцінювання ризиків в IoT-середовищах потребує врахування особливостей кожного пристрою. Значення мають його призначення, можливості оброблення даних, засоби захисту та зв'язки з іншими компонентами. Зміна умов роботи IoT-пристрою також може вплинути на ризик, навіть при незмінності технічних характеристик. Тому використання однакових оцінок для різних умов експлуатації не завжди дає достатньо підстав для вибору заходів безпеки. Водночас інтенсифікація гібридних кібератак заснованих на вразливостях "нульового дня" утверджує актуальність теми дисертаційного дослідження, особливо для розвитку інформаційних технологій підтримки аудиту IoT-середовищ.

У дисертації Підлісного Юрія Івановича запропоновано враховувати ці відмінності через контекстно-ризиковий профіль. Він поєднує результати класифікації IoT-пристрою та використовується разом із даними про поточний стан безпеки для уточнення параметрів оцінювання. Такий підхід дозволяє пов'язати оцінку ризику з умовами функціонування конкретного пристрою.

Актуальність роботи визначається також потребою надання прозорої процедури оцінювання та інтерпретації результатів аудиту. Для аудитора важливо розуміти, які чинники вплинули на висновок, що привело до віднесення пристрою до певної ризик-категорії. Зважаючи на особливості предмету дослідження, використання нечіткої логіки у поєднанні з Мамдані-алгоритмом є обґрунтованим вибором для вирішення поставлених задач дослідження.

Зв'язок роботи з науковими програмами, планами, темами

Роботу виконано в Національному університеті «Чернігівська політехніка». У дисертації зазначено її зв'язок із темами «Методологія побудови захищеного кіберпростору» (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).

Дослідження доповнює ці напрями результатами щодо подання характеристик пристроїв та оцінювання ризиків інформаційної безпеки.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукові результати роботи охоплюють модель формування профілю, метод оцінювання ризиків і підхід до їх спільного використання в інформаційній технології.

Вперше розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. Профіль містить характеристики за п’ятьма критеріями: рівнем вбудованого інтелекту, характеристиками безпеки, архітектурою взаємодії, функціональним контекстом і динамічністю середовища. Автор зберігає результати класифікації за кожним критерієм без зведення їх до одного числа. Це дозволяє використовувати зміст окремих характеристик під час визначення та пояснення параметрів ризику.

Удосконалено метод контекстно-адаптивного оцінювання ризиків на основі нечіткого логічного виведення типу Мамдані. У ньому спільно враховано критичність активу, рівень загрози, рівень вразливості, можливості потенційного порушника, імовірність реалізації загрози, тяжкість наслідків та попередньо сформований показник BackdoorRisk. Параметри, що залежать від контексту, уточнюють з урахуванням профілю пристрою і поточного стану безпеки. Результатом є інтегральний показник RiskLevel, який можна інтерпретувати через вхідні значення та правила виведення.

Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків. Автор визначив, як пов’язані формування профілю, підготовка вхідних параметрів і нечітке оцінювання. Описано архітектуру, компоненти та обмін даними між ними. Передбачено повторне визначення ризику, якщо змінюються характеристики пристрою або стан середовища.

Ці результати узгоджені між собою та відповідають поставленому науковому завданню. Їх значення полягає у встановленні зв’язку між контекстними характеристиками IoT-пристрою та процедурою оцінювання ризику в процесі аудиту.

Запропоновані рішення спираються на аналіз відомих методів, формалізований опис профілю та застосування нечіткої логіки. Автор пояснює призначення параметрів, порядок їх використання та зв’язок із результатом оцінювання. Роботу прототипу перевірено аналізом спрацьовування правил і поверхонь виведення. Для опорної конфігурації досліджено покомпонентну монотонність.

Для сценарної перевірки FIS використано 100 000 записів. Пороги конфігурацій визначали на валідаційній частині з 60 000 сценаріїв за найбільшим значенням F1-міри. Остаточне оцінювання виконували на незалежній тестовій частині з 40 000 сценаріїв. Для запропонованої моделі отримано Accuracy = 0,971175, F1-міру = 0,982012 та FPR = 0,078250.

Порівняння із семипараметричною зваженою моделлю показало збільшення Accuracy на 0,018675 і F1-міри на 0,011565 та зменшення FPR на 0,058750. Вплив контексту додатково досліджено шляхом почергової фіксації окремих параметрів. Найбільше зниження F1-міри встановлено для ThreatLevel, Vulnerability та ImpactSeverity. Такі експерименти дозволяють оцінити внесок контекстного уточнення за незмінної структури FIS.

Дослідження не обмежується порівнянням підсумкових показників. Автор перевірив вплив зміни BackdoorRisk, пропусків у даних після медіанного заміщення та виміряв час нечіткого виведення. Це допомагає оцінити, наскільки результат залежить від підготовки вхідних даних.

Для класифікації мережевих подій використано дані BoT-IoT, TON_IoT та Edge-IIoTset. На тестовій частині з 4105 записів XGBoost забезпечив Accuracy = 0,9481, F1-міру = 0,9374 та FPR = 0,0238. Ці показники належать до окремого завдання класифікації та розглядаються окремо від сценарної перевірки RiskLevel.

Загальні висновки відповідають наведеним результатам. При цьому оцінки FIS характеризують сформовану сценарну вибірку. Для застосування в іншому середовищі потрібні підготовка даних, налаштування параметрів і додаткова перевірка, що відповідає зазначеним у роботі обмеженням.

Практичне значення дослідження

Автором розроблено програмний прототип ризикового модуля в MATLAB із використанням Fuzzy Logic Toolbox. Реалізована FIS-модель містить сім вхідних змінних, вихід RiskLevel і 40 унікальних продукційних правил. Прототип дозволяє перевірити правила, проаналізувати поведінку моделі та виконати пакетне оцінювання сценаріїв.

Окремо досліджено класифікацію мережевих подій на основі відкритих наборів даних. Ця частина роботи стосується отримання відомостей про активність у середовищі. FIS-модуль, своєю чергою, визначає рівень ризику за підготовленими вхідними параметрами. Таке розмежування дає чітке уявлення про призначення реалізованих засобів.

У додатках наведено матеріали щодо впровадження результатів у ТОВ «ЛЮМ’ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС», ТОВ «АТРІЯ КОМПАНІ» та в освітній процес Національного університету «Чернігівська політехніка».

Результати роботи можуть використовуватися для підтримки аналізу безпеки, підготовки рекомендацій та навчання фахівців.

Оцінка змісту дисертації, її завершеність та дотримання цінностей, принципів і правил академічної доброчесності

За своїм змістом дисертаційна робота здобувача Підлісного Юрія Івановича повністю відповідає предметній області спеціальності 122 Комп'ютерні науки. Дисертаційна робота є завершеною науковою працею і свідчить про особистий внесок здобувача у науковий напрям Інформаційні технології.

Ознайомлення зі звітом подібності за результатами перевірки дисертаційної роботи на текстові співпадіння дає підстави для заключення, що дисертаційна робота Підлісного Юрія Івановича є результатом самостійних досліджень здобувача, не містить елементів фальсифікації, компіляції, фабрикації та плагіату. Дисертант дотримувався цінностей, принципів і правил академічної доброчесності, норм законодавства про авторське право. У дисертації наявні посилання на відповідні джерела, зазначені у списку використаних джерел.

Мова та стиль викладення результатів

Дисертаційна робота виконана українською мовою. Матеріал викладено структуровано, послідовно та з використанням коректної наукової термінології. Анотації українською та англійською мовами узгоджуються з основними положеннями дисертації.

Структура дисертації є класичною та логічно обґрунтованою, забезпечуючи послідовний перехід від постановки проблеми до її вирішення та верифікації результатів.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. За даними вступу, вона містить 205 сторінок, із них 164 сторінки основного тексту, 24 рисунки, 42 таблиці, 140 найменувань джерел і чотири додатки.

У вступі сформульовано мету та завдання, визначено об'єкт, предмет і методи дослідження, наведено новизну та практичне значення. Наведено відомості про особистий внесок здобувача в розроблення моделі, удосконалення методу, створення технології та проведення експериментів, що висвітлені у публікаціях.

Перший розділ присвячено аналізу загроз, вразливостей і методів захисту IoT-середовищ. Автором встановлено, які обмеження відомих підходів потребують подальшого дослідження.

У другому розділі подано модель формування контекстно-ризикового профілю та метод оцінювання ризиків. Пояснено склад профілю, вхідних параметрів і використання контекстної інформації. Третій розділ присвячено архітектурі інформаційної технології, її компонентам та інформаційним потокам у процесі аудиту.

Четвертий розділ охоплює програмну реалізацію й експерименти: перевірку FIS, порівняння конфігурацій, дослідження впливу контексту, BackdoorRisk і пропущених значень. Окремо наведено результати класифікації мережевих подій. У висновках узагальнено результати відповідно до завдань роботи.

Зміст дисертації відповідає спеціальності 122 – Комп'ютерні науки. Робота поєднує розроблення моделей, методів оброблення даних та інформаційної технології з їх програмною реалізацією. Поставлені завдання розв'язано, а основні положення перевірено експериментально.

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

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені в 11 наукових роботах, у тому числі 5 статтях у фахових виданнях України, 6 публікаціях у матеріалах міжнародних та всеукраїнських конференцій. Праці стосуються класифікації IoT-середовищ, аудиту, приватності, нечіткого оцінювання та прихованих загроз.

Порушень цінностей, принципів і правил академічної доброчесності у публікаціях не виявлено.

Наукові публікації відповідають вимогам п. 8, 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 (зі змінами від 19 травня 2023 р. № 502 та від 03 травня 2024 р. № 507) щодо кількості публікацій, відповідності опублікованих результатів тим, що містяться у дисертації, апробації її основних положень.

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

Зауваження та побажання до дисертаційної роботи

При загальній позитивній оцінці дисертаційної роботи варто виділити такі дискусійні питання та зауваження:

1. У роботі описано використання профілю разом із поточним станом

безпеки. Було б доцільно визначити, які саме дані належать до профілю, які дані надходять із засобів моніторингу, хто відповідає за їх перевірку перед оцінюванням. Це полегшило б практичне використання технології.

2. В тексті роботи використовуються терміни «система нечіткого логічного висновку» та «нечіткого логічного виведення». Було б добре зупинити вибір на єдиному формулюванні.

3. Опис програмного прототипу доцільно розширити відомостями щодо специфікації вхідних даних та процедур перевірки їх валідності. Також додаткове пояснення логіки обробки граничних значень і внутрішньо суперечливих записів суттєво покращило б зрозумілість, що є критично важливим для забезпечення відтворюваності експериментів та подальшої еволюції розробленого інструментарію.

4. Експеримент із пропущеними значеннями демонструє, що попереднє відновлення даних може змінювати категорію ризику. Було б корисно зазначити, як така невизначеність має відображатися в результаті оцінювання для врахування аудитором, та коли таку оцінку потрібно уточнити на підставі отриманих додаткових відомостей.

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 Підлісного Юрія Івановича на тему «Методи та моделі контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ» виконана на високому науковому рівні, не порушує цінностей, принципів і правил академічної доброчесності та є завершеним 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 (зі змінами від 19 травня 2023 р. № 502 та від 03 травня 2024 р. № 507) та «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого Постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (зі змінами та доповненнями).

Здобувач Підлісний Юрій Іванович заслуговує на присудження ступеня доктора філософії в галузі знань Інформаційні технології за спеціальністю 122 «Комп’ютерні науки».

Офіційний рецензент:
Начальник відділу Науково-дослідна частина
Національного університету
«Чернігівська політехніка»
доктор філософії Марія ВОЙЦЕХОВСЬКА