РЕЦЕНЗІЯ

офіційного рецензента професора кафедри інформаційних технологій та програмної інженерії Національного університету «Чернігівська політехніка», доктора технічних наук, професора Дорош Марії Сергіївни
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 12 – Інформаційні технології
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми дисертації

Актуальність теми дисертаційного дослідження зумовлена стрімким розширенням екосистеми Інтернету речей (IoT), яка охоплює критичну інфраструктуру, промисловість, енергетику, охорону здоров'я, транспорт та побутову сферу. Велика гетерогенність пристроїв, протоколів і архітектур суттєво розширює поверхню атаки та ускладнює застосування традиційних підходів до забезпечення інформаційної безпеки. Інциденти останніх років, зокрема масштабні ботнет-атаки на IoT-пристрої та компрометація систем промислового й критичного призначення, підтверджують, що вразливості IoT можуть призводити не лише до витоку даних, а й до фізичних наслідків, економічних збитків і загроз національній безпеці.

За таких умов особливої ваги набуває саме управління ризиками інформаційної безпеки, яке дозволяє перейти від реактивного реагування на інциденти до системного, науково обґрунтованого виявлення, оцінювання та мінімізації загроз на всіх етапах життєвого циклу IoT-систем. Існуючі методики та стандарти (зокрема ISO/IEC 27005, NIST SP 800-30, NIST IR 8228) не повною мірою враховують специфіку IoT: динамічність топології, обмежені ресурси пристроїв, взаємозалежність компонентів та кіберфізичний характер наслідків.

Отже, розроблення інформаційних технологій, які поєднують нові та вдосконалені моделі та методи оцінки ризиків інформаційної безпеки в галузі IoT є важливим науково-прикладним завданням, що має суттєве теоретичне й практичне значення.

Зв’язок роботи з науковими програмами, планами і темами

Дослідження виконано в Національному університеті «Чернігівська політехніка». У дисертації зазначено його зв’язок із науково-дослідними темами «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). Результати роботи узгоджуються з цими напрямами в частині моделювання загроз, оцінювання ризиків і підтримки аналізу стану безпеки.

Наукова новизна та практичне значення дослідження

Основний науковий внесок автора охоплює три взаємопов’язані результати.

Вперше розроблено модель формування контекстно-ризикового профілю IoT-пристрою за результатами інтелектуально-контекстної класифікації. У моделі використано п’ять критеріїв: рівень вбудованого інтелекту, характеристики безпеки, архітектуру взаємодії, функціональний контекст і динамічність середовища. Результати класифікації зберігаються за окремими критеріями без зведення до одного числового показника. Профіль використовують разом із даними про поточний стан безпеки, щоб визначати та пояснювати параметри оцінювання ризику.

Удосконалено метод контекстно-адаптивного оцінювання ризиків інформаційної безпеки IoT-середовищ на основі нечіткого логічного виведення типу Мамдані. Метод спільно враховує критичність активу, рівень загрози, рівень вразливості, можливості потенційного порушника, імовірність реалізації загрози, тяжкість її наслідків та попередньо сформований показник BackdoorRisk. Контекстно залежні параметри уточнюються з використанням профілю та відомостей про стан безпеки. Нечіткі правила забезпечують визначення показника RiskLevel і змістове пояснення отриманого результату.

Набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків. У цьому підході профіль пристрою та дані про стан безпеки використовують для підготовки вхідних параметрів нечіткого оцінювання. На цій основі визначено багаторівневу архітектуру, функціональні компоненти та інформаційні потоки. Передбачено оновлення вхідних

параметрів і повторне оцінювання у разі зміни характеристик пристрою або середовища.

Практичне значення результатів полягає у створенні програмного прототипу ризикового модуля в MATLAB із використанням Fuzzy Logic Toolbox. Реалізовано систему Мамдані із сімома вхідними змінними, виходом RiskLevel і 40 продукційними правилами. Окремо досліджено процедуру класифікації мережевих подій, яка може використовуватися для отримання відомостей про активність у середовищі.

У дисертації наведено матеріали про впровадження результатів у діяльність ТОВ «ЛЮМ'ЄР ЕЛЕКТРО», ТОВ «АРКАДА ФІНАНС», ТОВ «АТРІЯ КОМПАНІ» та в освітній процес Національного університету «Чернігівська політехніка».

Ступінь обґрунтованості наукових положень і висновків

Наукові положення та висновки дисертації є верифікованими й належно обґрунтованими, оскільки спираються на грунтовний аналіз праць українських і зарубіжних дослідників, ретельному огляді існуючих сучасних технологій та підтверджуються експериментами, які можуть бути відтворені, що забезпечує достовірність отриманих результатів. Наукові результати дисертації були апробовані, доповідались на міжнародних науково-практичних конференціях та підтверджуються довідками про впровадження. Наукове завдання дослідження виконано повністю, здобувач повною мірою оволодів методологією наукової роботи.

Повнота викладення основних результатів в опублікованих працях

Результати дослідження опубліковано в 11 наукових працях: п'яти статтях у фахових виданнях України та шести публікаціях у матеріалах наукових конференцій.

У наведених публікаціях повно й корректно подані результати дисертаційної роботи, а порушень академічної доброчесності в них не виявлено.

Оцінка завершеності роботи та академічної доброчесності

За змістом дослідження належить до спеціальності 122 – Комп'ютерні науки: у ньому розглянуто моделі подання даних, методи їх опрацювання, архітектуру інформаційної технології та програмну реалізацію. Робота є завершеним науковим дослідженням і засвідчує особистий внесок здобувача у науковий напрям «Комп'ютерні науки». Аналіз звіту про подібність

підтверджує, що дисертаційна робота є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату чи некоректних запозичень. Ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Робота є завершеним дослідженням: поставлені завдання розв'язано, результати реалізовано програмно та мають експериментальне підтвердження.

Зміст дисертації

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Згідно з відомостями у вступі, повний обсяг становить 205 сторінок, основний текст – 164 сторінки; робота містить 24 рисунки, 42 таблиці, 140 найменувань джерел і чотири додатки.

У вступі обґрунтовано актуальність, сформульовано мету й завдання, визначено об'єкт, предмет і методи дослідження. Визначено наукову новизну, практичне значення, відомості про апробацію, публікації та внесок здобувача.

У першому розділі проаналізовано сучасні загрози, вразливості й підходи до забезпечення безпеки IoT-середовищ. Розглянуто класифікацію мережевих подій, методи оцінювання ризиків та аудит. Встановлені обмеження обґрунтовують необхідність урахування контексту, взаємозалежності чинників і невизначеності даних.

У другому розділі викладено модель формування контекстно-ризикового профілю та метод нечіткого оцінювання. Визначено критерії класифікації, зміст параметрів ризику та використання профілю для їх контекстної інтерпретації. Розділ містить основні теоретичні результати роботи.

У третьому розділі здійснено проектування інформаційної технології, побудована архітектура, визначені функціональні компоненти та інформаційні потоки. Описано взаємодію засобів формування профілю, підготовки даних і визначення рівня ризику в процесі аудиту.

У четвертому розділі представлено програмний прототип та результати експериментів. Перевірено FIS-модель запропонованого методу, виконано порівняння конфігурацій, досліджено впливи контексту, BackdoorRisk і пропусків даних. Окремо оцінено класифікацію мережевих подій. Наведено кількісні результати та пояснено межі їх застосування.

Дисертацію написано українською мовою. Матеріал викладено послідовно, а таблиці, схеми й графіки допомагають зрозуміти запропоновані рішення та порівняти результати.

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

Відповідність анотації основним положенням дисертації

Анотації українською та англійською мовами відображають актуальність, наукову новизну, практичні результати та ключові слова. Їх зміст узгоджується з основними положеннями та висновками роботи.

Недоліки та зауваження до дисертаційної роботи

Робота заслуговує на позитивну оцінку. Водночас під час ознайомлення з нею виникли такі зауваження та побажання.

1. Формулювання пунктів наукової новизни, на мій погляд, не достатньо точно визначає чим відрізняються запропоновані модель та метод від існуючих. Таке уточнення дало б змогу сфокусувати увагу саме на власному внеску здобувача до існуючих методів та моделей.

2. Визначена вперше розроблена модель побудови контекстно-ризикового профілю IoT пристрою за результатами інтелектуально-контекстної класифікації, відповідно тексту дисертації описує не процес побудови, а скоріше, визначає саму модель. Тому доцільніше було б формувати цей пункт як: «розроблена модель контекстно-ризикового профілю IoT пристрою..» (в задачах так і прописано).

3. В роботі зазначено, що набув подальшого розвитку підхід до побудови інформаційної технології оцінювання ризиків інформаційної безпеки IoT-середовищ. Відповідно тексту дисертаційної роботи виконано порівняльний аналіз підходів до оцінювання ризиків безпеки IoT середовищ, а не до самого процесу побудови. Отже, визначення не зовсім коректне. Натомість, неведені в третьому розділі принципи побудови інформаційної технології контекстно-адаптивного оцінювання ризиків безпеки IoT-середовищ, на мій погляд, можуть бути включені до наукової новизни.

4. Також, на мій погляд, до наукової новизни можна також віднести запропоновану в третьому розділі концептуальну модель інформаційної технології контекстно адаптивного оцінювання ризиків безпеки IoT-середовищ, окільки вона, на відміну від інуючих, передбачає використання контекстно ризикового профілю IoT пристрою разом із даними про поточний стан безпеки.

5. В роботі є недоліки по форматуванню тексту: невідповідні шрифти, відсутнє оформлення продовження таблиць в разі їх перенесення на наступну сторінку та ін.

6. В роботі не завжди спостерігається чіткість та відповідність понять. У різних частинах роботи вжито терміни «формування» і «побудова» профілю та ін.

7. Огляд методів виявлення атак та загроз конфіденційності в першому розділі можна було б скоротити, окільки вони не складають основи для розроблених моделей. Натомість, більше уваги приділити методам та інформаційним системам оцінки ризиків інформаційної безпеки.

8. Наведені в п.п. 2.3.1. Принципи побудови інформаційної технології контекстно адаптивного оцінювання ризиків безпеки IoT-середовищ за назвою відрізняються від зведених на рисунку 3.2.

9. На рис. 3.5.-3.8. наведені різні типи архітектур розробленої інформаційної технології та взаємодії між її компонентами, що, на мій погляд, порушує розуміння єдності запропонованої інформаційної технології. Можливо не всі наведені структрури є архітектурами системи.

10. У четвертому розділі доцільно було б на одному прикладі показати всю послідовність оцінювання для конкретного IoT-пристрою: формування профілю, уточнення параметрів, отримання RiskLevel і підготовку рекомендацій. Це допомогло б краще зрозуміти доведення ефективності моделі в складі інформаційної технології.

Наведені зауваження стосуються окремих формулювань, оформлення та подальшого розвитку дослідження. Однак вони не ставлять під сумнів основні наукові та практичні результати й не змінюють позитивної оцінки дисертації.

Висновок про дисертаційну роботу

Дисертація 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 формування контекстно-ризикового профілю IoT-пристрою та врахування його параметрів при оцінюванні ризиків інформаційної безпеки в процесі аудиту. На основі моделі й методу створено інформаційну технологію їх узгодженого застосування.

За змістом, науковою новизною, обґрунтованістю положень та практичним значенням робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії за спеціальністю 122 – Комп’ютерні науки галузі

знань 12 – Інформаційні технології. Основні результати висвітлено у публікаціях та апробовано на наукових заходах.

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

Офіційний рецензент:
професор кафедри інформаційних
технологій та програмної інженерії
Національного університету
«Чернігівська політехніка»,
доктор технічних наук, професор  Марія ДОРОШ