Голові разової спеціалізованої вченої ради
Національного університету «Львівська політехніка»
д.т.н., доценту Бешлею Миколі Івановичу

ВІДГУК
офіційного рецензента – к.т.н. доцента Коробейнікової Тетяни Іванівни
доцента кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»,
на дисертаційну роботу
Банаха Романа Ігоровича
«Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11»,
поданої на здобуття наукового ступеня доктора філософії
за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Актуальність даної роботи визначається високою роллю бездротових мереж стандарту IEEE 802.11 (Wi-Fi) у сучасному світі. Вони є невід'ємною частиною повсякдення як домашніх, так і корпоративних користувачів, надаючи свободу пересування під час роботи чи дозвілля. Однак, разом із перевагами, які надають мережі Wi-Fi, існують і значні виклики, пов'язані з інформаційною безпекою.

Відомо, що зловмисники можуть вторгнутись у бездротову мережу на відстанях до 2 км і більше, що ускладнює задачу визначення їх місцезнаходження. Крім того, незважаючи на зусилля постачальників Wi-Fi обладнання, які намагаються зробити свої пристрої безпечними "з коробки", відомо, що навіть найстійкіші протоколи захисту не можуть гарантувати повну безпеку через велику кількість відомих вразливостей в сучасних протоколах безпеки мереж стандарту IEEE 802.11.

Таким чином, у зв'язку з необхідністю забезпечення безпеки як корпоративних, так і персональних мереж Wi-Fi, а також недостатньою науково-методичною базою методів деанонімізації зловмисників для вирішення цієї проблеми, виникає науково-практична задача вдосконалення систем виявлення вторгнень та систем-приманок у мережах стандарту IEEE 802.11 шляхом дослідження характеристик взаємодії зі зловмисником. Це робить дану роботу актуальною та важливою у контексті сучасних викликів у галузі кібербезпеки.

Зв'язок теми дисертації з науковими програмами, планами і темами.

Наведені у дисертації дослідження виконувались автором відповідно науковому напряму «Розробка та дослідження методів та створення сучасних засобів захисту інформації в безпровідних мережах» кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка».

Тема дисертаційного дослідження відповідає пріоритетним напрямкам науково-дослідних робіт відповідно до координаційних планів Міністерства освіти і науки України та виконувалася в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації

0124U000407), а також межах міжнародного гранту наданого CRDF Global «Вдосконалення комплексу динамічної автентифікації кінцевих точок засобами машинного навчання та захисту корпоративних мереж від кібератак» (номер грантової угоди G-202401-71626).

Наукова новизна результатів дисертаційного дослідження:

Здобувачем, Банахом Р.І.:

- Вперше розроблено концептуальну модель системи захисту інформації із застосуванням систем виявлення вторгнень і систем-приманок для мереж IEEE 802.11 Wireless Honeypot as a Service використовуючи хмарні обчислення, яка на відміну від існуючих підходів до розгортання інфраструктури із системами-приманками дає можливість покращити характеристики швидкості та гнучкості розгортання цілісної системи захисту інформації для бездротових мереж.
- Вперше розроблено методику відслідковування зловмисників за метаданими, зібраними з їх пристроїв, застосовуючи публічні бази даних геолокації Wi-Fi пристроїв. Розроблено алгоритм з покращеними характеристиками визначення геолокації конкретної точки доступу, який на відміну алгоритму запису інформації за допомогою часових рядів, дозволяє точніше визначити геолокацію Wi-Fi точок доступу, що дає можливість уникнути хибних відображень на карті, а відповідно ідентифікувати попередні місця перебування зловмисників із вищою точністю.
- Вперше розроблено діагностичну модель системи-приманки для бездротових мереж стандарту IEEE 802.11, яка на відміну від підходів зі "сліпої конфігурації" чи клонування існуючої бездротової інфраструктури дозволяє оцінити рівень захищеності системи-приманки на відповідність до профілю зловмисника, що дає змогу згенерувати конфігурацію системи-приманки для зловмисника з потрібним рівнем підготовки у автоматичному режимі, і відповідно покращити пристосовуваність систем-приманок у бездротових мережах стандарту IEEE 802.11.
- Вперше розроблено метод виявлення вторгнень із застосуванням машинного навчання, а саме алгоритму K-найближчих сусідів, в якому на відміну від існуючих застосовано оригінальний метод агрегації даних про потужність сигналу, що дає можливість уникнути надлишкового навантаження на комп'ютерні мережі. Розроблений метод дає змогу ідентифікувати атаку «злий двійник» на ранніх стадіях атаки на Wi-Fi точки доступу, як елемента мережевої інфраструктури.

Ступінь обґрунтованості наукових положень та висновків дисертації та їх достовірність.

Під час вирішенні поставлених у дисертації задач, створенні наукових положень, висновків та рекомендацій здобувач застосовував дані, що одержані з літературних джерел, з результатів аналізу сучасного стану та перспектив розвитку та вдосконалення технології виявлення вторгнень та покращення характеристик систем-приманок у бездротових мережах стандарту IEEE 802.11. Наведені в дисертації результати є достатньо обґрунтованими, що підтверджується даними розрахунків, експериментальних досліджень та практичними результатами та актами впровадження.

Наукове значення виконаного дослідження.

Отримані здобувачем наукові положення, висновки та практичні результати можуть бути використані під час розробки нових, а також, під час вдосконалення існуючих систем виявлення вторгнень та є значущими для галузі 12 «Інформаційні технології» та спеціальності 125 «Кібербезпека».

Практичне значення одержаних результатів.

Практичне значення одержаних результатів полягає полягає у їх застосуванні для підсилення наявних систем виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11 у корпоративному, академічному і приватному середовищах. Зокрема, наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри безпека інформаційних технологій Національного університету «Львівська політехніка», зокрема для студентів спеціальності 125 «Кібербезпека» в курсі лекцій з дисципліни «Інформаційно-комунікаційні системи». Основні результати дисертаційної роботи використано і впроваджено з метою покращення захищеності комп'ютерної мережі та систем в компанії ТзОВ «Інститут інформаційних технологій «Інтелліас», що підтверджено актами впровадження.

Повнота оприлюднення результатів дисертаційної роботи.

Результати дисертації доповідалися здобувачем та обговорювались на 16-и міжнародних і державних науково-технічних конференціях. Загальна кількість публікацій за темою дисертації становить **27**, з них **11** статей, **9** з яких входять до переліку видань ВАК, **2** проіндексовано міжнародною наукометричною базою даних SCOPUS, **1** проіндексована міжнародними наукометричними базами даних Copernicus та Google Scholar, **1** розділ монографії. **14** тез доповіді, **3** з яких проіндексовано міжнародною наукометричною базою даних SCOPUS.

Короткий аналіз структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 192 сторінках та складається із анотації, змісту, переліку скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків.

Дисертація написана українською мовою на високому мовно-стилістичному рівні, стиль викладення матеріалу є послідовним та логічним. За своєю структурою, мовою та стилем викладення вона відповідає вимогам МОН України.

У вступі здобувачем обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок.

У першому розділі проведено аналіз сучасного стану питання в галузі виявлення вторгнень та систем-приманок у бездротових мережах стандарту IEEE 802.11 також особливу увагу приділено перспективам розвитку цього наукового напрямку.

У другому розділі досліджено передумови для побудови системи захисту інформації в бездротових мережах та запропоновано відповідну концепцію для

стандарту IEEE 802.11 11 із застосуванням систем виявлення вторгнень і систем-приманок

У третьому розділі запропоновано розроблення та оптимізація моделі системи захисту інформації бездротових мереж стандарту IEEE 802.11 із застосуванням систем виявлення вторгнень і систем-приманок, зокрема: методика відслідковування зловмисників; модель системи-приманки бездротової мережі стандарту IEEE 802.11; вдосконалення методів виявлення вторгнень в мережах IEEE 802.11 за допомогою систем штучного інтелекту;

У четвертому розділі обґрунтовано доцільність застосування та, власне, застосовано авторські механізми ідентифікації виявлення вторгнень, особи зловмисника та ефективності систем-приманок у бездротових мережах стандарту IEEE 802.11, зокрема: методика з відслідковування зловмисника; діагностична модель системи-приманки для бездротових мереж стандарту IEEE 802.11; також показано виявлення атак «злий двійник» на мережі стандарту IEEE 802.11 (Wi-Fi) за допомогою моделі класифікації KNN.

У загальних висновках дисертаційної роботи сформульовано основні результати дисертаційної роботи, які узгоджуються з метою та завданнями дослідження.

Список використаних джерел складається з 103 елементів.

Зауваження та дискусійні положення щодо змісту дисертації.

1) Наукове дослідження недостатньо враховує ті системи виявлення вторгнень, які працюють із несигнатурними методами і чи можуть бути застосовними запропоновані автором методи та засоби для таких систем виявлення вторгнень.
2) В тексті дисертації описано мінімальний набір апаратних елементів та відповідного системного програмного забезпечення, на яких реалізовано модель системи захисту інформації з використанням систем-приманок; проте з тексту дисертації незрозуміло, чи впливає збагачення елементної бази та системного програмного забезпечення на якісні показники роботи запропонованої автором моделі системи захисту інформації.
3) В тексті дисертації сказано, що покращення методики визначення геолокації точок доступу вдалось досягти точності у віднайдені унікальних екземплярів з точністю 90—100% на противагу 0.5—1% у публічних базах даних; проте не приділено уваги в тексті дисертації можливій комерціалізації продукту.
4) Метод відслідковування зловмисника скорше за все матиме зниження продуктивності, якщо метадані їх пристроях будуть приховані. В роботі не описано чи враховується це під час визначення досвідченості зловмисника.
5) У тексті представленої роботи іноді зустрічається стилістичні і орфографічні неточності.

Слід зауважити, що зазначені зауваження ніяким чином не зменшують загальної позитивної оцінки дисертаційної роботи.

Висновок.

Незважаючи на виявлені неточності та зазначені зауваження дисертаційна робота Банаха Романа Ігоровича на тему «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» є завершеною науково-дослідною роботою, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»), яка за своїм

змістом, структурою, обсягом науковою новизною та практичним значенням відповідає паспорту спеціальності 125 «Кібербезпека» та вимогам «Порядку присудження ступеня доктора філософії та скасування рішень разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 зі змінами згідно з Постановою КМ № 341 від 21.03.2022, а її автор Банах Роман Ігорович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Офіційний рецензент,
кандидат технічних наук, доцент,
доцент кафедри безпеки
інформаційних технологій
Національного університету
"Львівська політехніка" Тетяна КОРОБЕЙНІКОВА

Підпис к.т.н., доцента Коробейнікової Т.І. засвідчую
Вчений секретар
Національного університету
«Львівська політехніка»
к.т.н., доцент Роман БРИЛИНСЬКИЙ