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

ВІДГУК
офіційного рецензента – д.т.н, професора Мельника Віктора Анатолійовича
професора 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»)

1. Актуальність теми дисертації.

Робота здобувача Банаха Р.І. є актуальною, особливо з огляду на поширеність бездротових технологій у сучасному світі та прогнозовану подальшу зростаючу популярність цих технологій. За останні роки бездротові мережі стали невід'ємною складовою повсякденного життя для багатьох людей, як у домашньому, так і у корпоративному середовищах. Вони забезпечують високу мобільність та зручність у доступі до Інтернету та інших мережних ресурсів. Завдяки широкому розповсюдженню смартфонів, планшетів, ноутбуків та інших мобільних пристроїв, попит на бездротові технології стабільно зростає.

З урахуванням цього тренду, проблема забезпечення безпеки бездротових мереж стає все більш актуальною. Зростаюча кількість пристроїв, які використовують бездротові зв'язки, призводить до збільшення ризику вторгнень та інших кіберзагроз у цих мережах. Таким чином, розвиток технологій виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11 стає важливим завданням для забезпечення безпеки та конфіденційності інформації в бездротових середовищах.

У даній роботі пропонується низка нових та вдосконалених підходів до виявлення вторгнень у бездротових мережах за допомогою систем-приманок, що є необхідністю зважаючи на розповсюдженість пристроїв Wi-Fi. Її результати та методи можуть стати основою для подальших досліджень та розробок у сфері кібербезпеки і безпеки мереж стандарту IEEE 802.11. Методи, засоби та підходи розроблені у даній роботі дозволять підвищити ефективність захисту бездротових мереж та зменшити ризик вторгнень, що є вкрай важливим у сучасному цифровому світі.

2. 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 ґранту наданого CRDF Global «Вдосконалення комплексу динамічної автентифікації кінцевих точок засобами машинного навчання та захисту корпоративних мереж від кібератак» (номер ґрантової угоди G-202401-71626).

3. 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.

4. 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.

5. 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».

6. 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.

7. 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 **28**, з них **12** 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. **14** тез доповіді, **3** з яких проіндексовано міжнародною наукометричною базою даних SCOPUS.

8. 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.

9. Зауваження та дискусійні положення щодо змісту дисертації.

1) У вступі варто перерахувати українських та закордонних науковців та компаній, які внесли внесок у розвиток даної тематики.
2) В кінці першого розділу, на основі поданого вище вмісту розділу, варто чіткіше сформулювати задачу, яка має бути розв'язана в дисертаційному дослідженні, та обґрунтувати використання приманок для її розв'язання.
3) В розділі 2.4. пропонується нова під-концепція SECaaS, із запропонованою назвою «Wireless Honeypot as a Servic», однак про це не сказано в науковій новизні
4) На початку розділу 2.4.1. «Елементи моделі Wireless Honeypot as a Service» варто сформулювати вимоги до моделі, на основі яких можна було б ідентифікувати та обґрунтувати вибір елементів моделі. Інфраструктуру моделі WHaaS варто також побати схематично чи графічно.
5) В розділі 2.4.3. «Вибір платформи зовнішніх елементів системи-приманки та системи виявлення вторгнень для мереж стандарту IEEE 802.11» доцільно виходити з потреб систем виявлення вторгнень, а не лише з існуючих технічних рішень, яких є достатньо багато крім описаних в підрозділі.
6) В розділі 3.3.3. «Розроблення методу ідентифікації атак з підміни MAC адреси та «злий двійник»» не сказано про інші, існуючі методи, як не сказано й чим запропонований метод є кращим від них. Про це також не сказано у висновках до розділу
7) Низка підходів і технічних рішень в розділі 4, потребують обґрунтування. Зокрема:
   - Вибір сервісу WiGLE для пошуку геолокації пристроїв Wi-Fi
   - Використання програмного пакету Scapy для перехоплення пакетів
   - Використання одноплатного комп'ютера Raspberry Pi 4 Model B із GPS модулем та мережевою картою Alfa AWUS036NHA

- Розроблення (на потреби досліду) власного алгоритму для пошуку точок доступу, за допомогою якого в подальшому було здійснено збір інформації
- Карти OpenStreetMap
- ОС Linux на базі дистрибутиву Debian

8) В розділі 4.3. «Аналіз результатів з удосконалення методики розподіленого підбору ключа доступу до механізму захисту WPA2 у мережах IEEE 802.11» потрібно довести достовірність результатів, адже невідомо, чи залежить методика від використаного в ході експериментів обладнання і програмного забезпечення.

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,
Доктор технічних наук, професор,
професор кафедри безпеки
інформаційних технологій
Національного університету
"Львівська політехніка

Віктор МЕЛЬНИК

Підпис д.т.н., професора Мельника В.А.
засвідчую
Вчений секретар
Національного університету
«Львівська політехніка»
к.т.н., доцент

Роман БРИЛИНСЬКИЙ