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

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
д.т.н., професора, Одарченка Романа Сергійовича
В.о. декана факультету аеронавігації, електроніки та телекомунікацій
Національного авіаційного університету
на дисертаційну роботу
Банаха Романа Ігоровича
«Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11»
подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

1. **Актуальність теми дисертації, її зв'язок з науковими програмами, темами.**

Актуальність проблеми захисту інформації у мережах стандарту IEEE 802.11 обумовлена їх широким застосуванням у сучасному цифровому світі. На відміну від дротових комп'ютерних мереж, де порушення можна відстежити завдяки фізичній взаємодії зловмисника з обладнанням, у бездротових мережах така задача є значно складнішою. Це зумовлено тим, що точка підключення в бездротових мережах залежить від потужності приймача та передавача радіосигналу, що ускладнює визначення місця знаходження зловмисника і моніторинг його активності.

Проводячи атаку на бездротові мережі Wi-Fi зловмисники відчувають безкарність, оскільки ідентифікація особи порушника в контексті бездротових мереж є вкрай складним завданням. Сучасні системи виявлення вторгнень зазвичай зосереджені на сигнатурних підходах, які не завжди виявляються ефективними, а системи-приманки, в свою чергу, нерідко стають інструментом у руках зловмисників.

Поєднання цих двох підходів—виявлення вторгнень та використання систем-приманок, а також покращення їх характеристик—може суттєво покращити безпеку бездротових мереж Wi-Fi. Комплексне використання даних інструментів в рамках єдиної захисної стратегії забезпечить підвищений рівень безпеки і знизить ризики несанкціонованого доступу до інформації.

Зазначене свідчить, що тема дисертаційного дослідження є актуальною та практично значущою, що, зокрема підтверджується зв'язком з науковими програмами, планами, темами.

Тема дисертаційної роботи відповідає науковому напрямку кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка» «Розробка та дослідження методів та створення сучасних засобів захисту інформації в безпровідних мережах». Окремі частини роботи виконано

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 в 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).

2. **Ступінь обґрунтованості наукових положень, висновків і рекомендацій та аналіз змісту дисертаційної роботи.**

Аналіз змісту дисертації та анотації, рекомендацій та висновків свідчить, що наукова новизна дослідження має належний рівень обґрунтованості. Це підтверджено значною кількістю проаналізованих дисертантом літературних джерел з даної проблематики, науковими здобутками та прикладними напрацюваннями вчених і практиків у сфері кібербезпеки.

Обґрунтованість висунутих наукових положень підкріплюється логічним викладенням матеріалу, об'єктивним аналізом експериментальних результатів, розробкою практичних рекомендацій для удосконалення технології виявлення вторгнень та систем приманок для мереж стандарту IEEE 802.11. Основні наукові положення, висновки і практичні рекомендації, викладені в дисертації, є достатньою мірою обґрунтованими логічними і послідовними.

Структура дисертаційної роботи традиційна і включає вступ, чотири розділи, кожен з яких відрізняється певним науковим вкладом у вирішення проблем із вдосконалення технології виявлення вторгнень та систем-приманок у мережах стандарту IEEE 802.11.

У **першому розділі** розглянуто технологію Wi-Fi, включаючи її переваги, недоліки та сучасні підходи до впровадження систем виявлення вторгнень і приманок у комп'ютерних мережах цього типу. Проведено детальний аналіз наукових досліджень і публікацій, які стосуються актуальності використання систем виявлення вторгнень і приманок у бездротових мережах стандарту IEEE 802.11. Виконано порівняльну оцінку базових механізмів і продуктів як комерційного, так і з відкритим вихідним кодом. Відзначається, що навіть при розробці нових механізмів захисту та їх впровадженні на серверному обладнанні, необхідність зворотної сумісності з застарілими, вразливими клієнтськими пристроями залишається важливим викликом. Також досліджено можливості застосування алгоритмів машинного навчання для поліпшення виявлення вторгнень у Wi-Fi мережах. Розглянуто інтелектуальні підходи до конфігурації приманок, що допомагає уникати їх виявлення зловмисниками. У розділі представлено матеріал, який буде корисним для фахівців з безпеки мереж та може слугувати основою для подальших досліджень у цій сфері.

У **другому розділі** досліджено життєвий цикл систем захисту інформації в бездротових мережах стандарту IEEE 802.11, з акцентом на системах виявлення вторгнень і приманках. Виявлено, що важливою характеристикою таких систем є їх здатність протистояти атакам. Розроблено модель життєвого циклу систем захисту, яка дозволяє динамічно адаптуватися на основі аналізу історичних даних. Представлено моделі можливих загроз для корпоративних мереж. Особлива увага приділена виявленню ознак, які можуть видавати системи

захисту, що є важливим для забезпечення безпеки бездротових мереж. Створено концептуальну модель захисної системи, яка інтегрує системи виявлення вторгнень і приманки, а також визначено правила їх взаємодії. Окрім того, розглянуто можливість використання хмарних технологій для забезпечення масштабованості системи. Матеріал цього розділу містить ряд важливих висновків і рекомендацій, які можуть бути корисними фахівцям у сфері кібербезпеки. Запропонована концептуальна модель та рекомендації щодо її реалізації сприятимуть підвищенню рівня безпеки бездротових мереж стандарту IEEE 802.11.

У **третьому розділі** розглядається розробка та оптимізація моделі системи захисту інформації в бездротових мережах стандарту IEEE 802.11, з використанням систем виявлення вторгнень і приманок. Представлено розроблені та вдосконалені моделі захисту інформації для таких мереж. Запропоновано методику відслідковування зловмисників через аналіз пакетів Probe Request, що відкриває нові можливості для розуміння їх поведінки та визначення попереднього місця знаходження. Важливою частиною роботи є діагностична модель системи-приманки для бездротових мереж, яка охоплює протоколи безпеки WPA/WPA2. Автором вдосконалено методи виявлення вторгнень в мережах IEEE 802.11, використовуючи штучний інтелект. Зокрема, впровадження алгоритму машинного навчання KNN для ідентифікації підміни MAC-адрес і атак типу «злий двійник» на основі компактного апаратно-програмного комплексу для моніторингу та аналізу мережевих пакетів. Цей підхід забезпечує високу точність і швидкість виявлення вторгнень, що є важливим для ефективного захисту бездротових мереж.

У **четвертому розділі** виконано детальний аналіз та оптимізацію механізмів ідентифікації, виявлення вторгнень та ефективності систем-приманок у бездротових мережах стандарту IEEE 802.11. Розділ відзначається всебічним підходом до вирішення проблем кібербезпеки у бездротових мережах. Автором досліджено погану сумісність публічних баз даних про мережі Wi-Fi у застосуванні їх для виявлення місць перебування зловмисника. Як результат, одним із важливих результатів цього розділу є розробка методу покращення точності геолокації точок доступу за допомогою аналізу потужності сигналу. Внаслідок цього, точність виявлення точок доступу зросла з менш ніж 1% до 90%, що свідчить про значний прогрес у цьому напрямку. Розроблена діагностична модель дозволяє визначати коефіцієнти для різних механізмів захисту бездротових мереж, що дає можливість налаштовувати системи-приманки відповідно до профілю зловмисника. Також розглянуто метод виявлення атаки «злий двійник», де використовувався оригінальний підхід до агрегації даних та алгоритм машинного навчання KNN. Отримана модель машинного навчання досягла 100% точності у виявленні вторгнень, демонструючи високу ефективність цього методу.

3. Достовірність результатів і наукова новизна дослідження.

Достовірність висновків і рекомендацій, сформульованих у дисертаційній роботі, забезпечена використанням наукової методології та застосуванням сучасних методів проведення досліджень. Уважне ознайомлення зі змістом дисертації, анотації до неї та наукових публікацій дисертанта дає підставу

визначити основні наукові положення та висновки, що характеризуються науковою новизною і відображають особистий внесок автора, сукупність їх обґрунтованості та достовірності.

Наукова новизна одержаних результатів визначається особистим внеском автора у вирішення актуального науково-практичного завдання, що полягає в удосконаленні технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11.

Найсуттєвіші результати дослідження, що містять наукову новизну, полягають в тому, що:

- *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.
- *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.

1) 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.

2) 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.

3) 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.

4) 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 точки доступу, як елемента мережевої інфраструктури Wi-Fi.

4. Значення роботи для науки і практики та шляхи використання результатів дослідження.

Наукові результати, отримані автором, можуть бути використані при проектуванні захищеної мережевої інфраструктури, у якій застосовуються мережі стандарту IEEE 802.11.

Отримані автором наукові результати, висновки та пропозиції становлять науковий інтерес та мають практичну цінність, що підтверджено їх впровадженням у навчальний процес на кафедрі «Безпека інформаційних технологій» Національного університету «Львівська політехніка» під час викладання дисциплін освітнього рівня бакалавр спеціальності 125 «Кібербезпека».

5. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових результатів в опублікованих працях.

Оформлення дисертації відповідає усім вимогам. Зміст, структура та послідовність викладення результатів відповідають як темі роботи, так і чинним вимогам МОН України. Дисертаційна робота написана державною мовою, матеріали викладені професійно та логічно, термінологія є загальновизнаною, стиль викладення результатів досліджень, висновків і рекомендацій забезпечує їх нормальне сприйняття і використання.

Тема роботи розкрита у 27 наукових працях, в тому числі 11 саттях, з яких 9 входять до переліку видань ВАК та 2 проіндексовано міжнародною наукометричною базою даних SCOPUS, в яких відображені результати проведених досліджень. Ґрунтовність, логічність та достовірність отриманих наукових положень, висновків та рекомендацій підтверджується також оприлюдненням та апробацією результатів дослідження на 7 міжнародних науково-технічних конференціях за темою дисертаційного дослідження.

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

6. Зауваження та дискусійні положення щодо змісту роботи.

- У розділі 2.4.3 автором представлено готові платформи для реалізації комплексної системи з виявлення вторгнень. Використання таких готових рішень

дозволяє швидко побудувати функціональний прототип, демонструючи можливість реалізації основних концепцій системи. Однак, варто зазначити, що залежність від цих платформ може обмежити розвиток проєкту на стадії доведення концепції (proof of concept), оскільки такі рішення можуть мати обмежену гнучкість і адаптивність або, навпаки, надлишкову функціональність, що може викликати проблеми інтеграції та масштабування у реальних умовах. Додатково, готові платформи можуть не повністю відповідати специфічним вимогам безпеки та функціональним потребам певних організацій, що ускладнює їх адаптацію до унікальних сценаріїв використання.

- У розділі 3.2.1 автором представлено платформу WiGLE як інструмент для пошуку Wi-Fi точок доступу, якими потенційно міг користуватися зловмисник. Платформа WiGLE надає можливість отримання доступу до бази даних Wi-Fi мереж, що може бути корисним для аналізу попередніх місць перебування зловмисників на основі зібраних даних про точки доступу. Однак, в роботі не було наведено детального огляду інших подібних платформ, які також можуть бути корисними для аналогічних завдань, та не розглянуто критеріїв, на підставі яких перевага була надана саме WiGLE. Відсутність аналізу альтернатив може обмежувати об'єктивність вибору та можливість використання інших, потенційно більш ефективних, інструментів для виконання аналогічних задач.
- У розділі 4.4 автор використав алгоритм K-Nearest Neighbors (KNN) для тренування моделі машинного навчання, застосовуючи його як алгоритм навчання з учителем. Модель продемонструвала високу ефективність у виконанні поставленого завдання, що підтверджує її придатність для застосування у даній сфері. Проте, для забезпечення більш обґрунтованого вибору методики машинного навчання, було б доцільно провести порівняльний аналіз алгоритму KNN з іншими існуючими алгоритмами машинного навчання, такими як Decision Trees, Random Forests, Support Vector Machines (SVM) або Neural Networks. Це дозволило б оцінити переваги та обмеження KNN у контексті вирішення задачі та визначити, чи є цей алгоритм оптимальним вибором серед інших можливих варіантів.

Загальні висновки щодо дисертаційної роботи

Дисертаційна робота Банаха Романа Ігоровича «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» є завершеною, самостійною працею, відповідає паспорту заявленої спеціальності і такою, що містить достатню наукову новизну та практичну цінність отриманих результатів, які дозволяють підвищити безпеку бездротових мереж стандарту IEEE 802.11.

Дисертаційна робота відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року та Вимогам до оформлення дисертації (наказ Міністерства освіти і науки України від 12.01.2017 №40).

Вважаю, що автор дисертаційної роботи Банах Роман Ігорович заслуговує на присудження ступеня доктор філософії за спеціальністю 125 «Кібербезпека та захист інформації».

Офіційний опонент
В.о. декана факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету Роман ОДАРЧЕНКО

Проректор з навчальної роботи
А. [illegible]

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ