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

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
доктора філософії, доцента, Киричка Романа Васильовича
доцента кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка
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 дисертаційної роботи.**

Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання з удосконалення технології виявлення вторгнень і систем-приманок для бездротових мереж стандарту IEEE 802.11.

Бездротові мережі стандарту IEEE 802.11 (Wi-Fi) набули широкого розповсюдження і де-факто стали стандартом для користувачів як у домашніх умовах, так і в корпоративних середовищах. Їхня популярність викликає інтерес серед зловмисників, оскільки поширеність технології прямо впливає на бажання скомпрометувати її з метою отримання вигоди. Це твердження цілком справджується для мереж стандарту IEEE 802.11. У новому протоколі WPA3, який мав вирішити всі проблеми з безпекою, було знайдено ряд вразливостей менш ніж за рік з моменту дати його публікування. Вся серйозність проблеми полягає в тому, що цю технологію неможливо повністю захистити лише за допомогою програмних оновлень. Wi-Fi є складним для модернізації, оскільки це програмно-апаратне забезпечення, і щоб виправити всі проблеми з безпекою, виробникам доведеться відкликати мільярди пристроїв по всьому світу, що економічно не виправдано. Таким чином, Wi-Fi Alliance обмежується лише рекомендаціями щодо безпечної роботи в мережах стандарту IEEE 802.11, які здебільшого ігноруються користувачами.

Основною проблемою з виявлення вторгнень в бездротові мережі стандарту IEEE 802.11 є те, що мобільними є не лише користувачі, але і зловмисники. Виявити аномальний трафік допомагають системи виявлення

вторгнень, та виявити персону яка вчинила зловмисні дії є доволі складним завданням.

Хоч ринок і пропонує велику кількість систем виявлення вторгнень, та зловмисники постійно знаходять нові методи їх обходу. Не існує жодної системи, яка би могла запропонувати оцінку зловмисника і захисту відносно вказаного профілю. Такий підхід у поєднанні із системами-приманками дозволить значно підсилити безпеку бездротових мереж стандарту IEEE 802.11.

У даній роботі автор зосереджується на удосконаленні технології виявлення вторгнень у мережі стандарту IEEE 802.11 за допомогою аналізу потужності сигналу від обладнання Wi-Fi і застосування машинного навчання для виявлення вторгнень. Автор пропонує метод аналізу досвідченості зловмисника, який дозволяє покращити характеристики взаємодії системи-приманок із зловмисником, а також методику з відслідковування зловмисників за метаданими зібраними з їх пристроїв, що дозволяє дізнатись про місця попереднього та, імовірно, про місце перманентного перебування.

**2. Аналіз змісту дисертаційної роботи.**

Дисертація є завершеною дослідницькою роботою, що містить анотацію, вступ, 4 розділи, висновки, список використаних джерел та додатки. У вступі автором обґрунтовано актуальність теми, сформульовано мету та завдання дослідження, визначено наукову новизну та практичну цінність результатів дослідження, презентовано дані про апробацію та публікацію результатів дисертаційної роботи.

У **першому розділі** автор провів глибокий аналіз технологій забезпечення безпеки в Wi-Fi мережах, включаючи її переваги, недоліки та особливості сучасних підходів до впровадження систем виявлення вторгнень та систем-приманок у комп'ютерних мережах даного типу. Автор ретельно аналізує наукові дослідження та публікації, що стосуються актуальності використання систем виявлення вторгнень та систем-приманок у бездротових мережах стандарту IEEE 802.11. Проведено порівняльну оцінку базових механізмів і продуктів як комерційного характеру, так і продуктів з відкритим вихідним кодом. Автор переконливо демонструє, що навіть при розробці нових механізмів захисту та їх впровадженні на серверному обладнанні, необхідність зворотної сумісності з застарілими, вразливими клієнтськими пристроями залишається серйозним викликом. Водночас, розглядаються перспективи застосування інтелектуального підходу до конфігурації систем-приманок з метою уникнення їх виявлення зловмисниками та використання алгоритмів машинного навчання для покращення виявлення вторгнень у мережах Wi-Fi, що свідчить про всебічний і глибокий підхід до проблеми. Розділ демонструє високий рівень обізнаності

автора в області безпеки бездротових мереж та вносить вагомий внесок у розуміння сучасних викликів і можливих рішень.

У **другому розділі** розглядається розвиток систем захисту інформації в бездротових мережах стандарту IEEE 802.11 з акцентом на системах виявлення вторгнень та системах-приманках. Аналіз виявив, що однією з ключових характеристик таких систем є їхня стійкість до атак. Автор вдало розробив життєвий цикл систем захисту, який забезпечує можливість динамічної адаптації систем на основі історичних даних. Також було представлено й проаналізовано моделі можливих зловмисників для корпоративних мереж. Особливу увагу було приділено дослідженню ознак, що можуть демаскувати системи захисту, що є досить актуальним аспектом для підвищення безпеки бездротових мереж. Завдяки цьому, було створено концептуальну модель системи захисту, яка включає інтеграцію систем виявлення вторгнень і систем-приманок, а також визначено правила взаємодії між її компонентами. Водночас, автором також було розглянуто можливість застосування хмарних обчислень для вирішення питань масштабованості даної системи. Таким чином, розділ демонструє високий рівень дослідницької роботи та містить низку важливих висновків і рекомендацій, які можуть бути корисними для фахівців у галузі кібербезпеки. Розроблена концептуальна модель і пропозиції щодо її впровадження можуть значно підвищити рівень безпеки бездротових мереж стандарту IEEE 802.11.

У **третьому розділ** проведено розробку та оптимізацію моделі системи захисту інформації бездротових мереж стандарту IEEE 802.11 із застосуванням систем виявлення вторгнень і систем-приманок. Автором успішно розроблено та вдосконалено моделі систем захисту інформації у бездротових мережах стандарту IEEE 802.11. Запропонована методика відслідковування зловмисників через аналіз пакетів Probe Request, яка відкриває нові можливості для розуміння поведінки зловмисників та їх попереднього місця перебування. Особливої уваги заслуговує представлена діагностична модель системи-приманки для бездротових мереж, яка охоплює протоколи бездротової безпеки WPA/WPA2. Цей підхід є не лише актуальним, але й надзвичайно ефективним у контексті сучасних загроз інформаційній безпеці. Автор вдосконалив методи виявлення вторгнень в мережах IEEE 802.11 за допомогою використання алгоритму машинного навчання KNN для ідентифікації підміни MAC-адреси та атак типу «злий двійник» на основі компактного апаратно-програмного комплексу для моніторингу та аналізу мережевих пакетів. У цілому, третій розділ демонструє високий рівень наукової роботи та містить значний внесок у розвиток технологій захисту бездротових мереж. Результати цього розділу є цінними як для наукової спільноти, так і для практиків у сфері інформаційної безпеки.

У **четвертому розділі** автор проводить всебічний аналіз і покращення механізмів ідентифікації, виявлення вторгнень та ефективності систем-приманок у бездротових мережах стандарту IEEE 802.11. Цей розділ вирізняється своєю глибиною та комплексним підходом до вирішення актуальних проблем у сфері кібербезпеки бездротових мереж. Автор ретельно дослідив недоліки у використанні публічних баз даних як інструмента для відслідковування зловмисників. Це дослідження підкреслює обмеження традиційних методів ідентифікації та відзначає необхідність їх подальшого вдосконалення. Одним із ключових досягнень цього розділу є визначення підходу до покращення точності геолокації точок доступу шляхом використання метрики потужності сигналу. Результати, де точність виявлення точок доступу зросла з менш ніж 1% до 90%, свідчать про значний прогрес і можливості подальшого покращення цього методу. Завдяки розробленій діагностичній моделі, автору вдалося надати коефіцієнти для різних механізмів захисту бездротових мереж. Це дозволяє налаштувати системи-приманки відповідно до профілю зловмисника, що є значним кроком вперед у підвищенні ефективності захисних заходів. Окремо слід відзначити дослідження, присвячене виявленню атаки «злий двійник», де використовувався оригінальний метод агрегації даних і алгоритм машинного навчання KNN. Натренована модель машинного навчання досягла 100% точності у виявленні фактів вторгнень, що свідчить про її високу ефективність і надійність. У цілому, четвертий розділ демонструє глибокі знання автора та його здатність розробляти інноваційні рішення для покращення безпеки бездротових мереж. Представлені результати досліджень цього розділу можуть стати основою для подальших досліджень у цій галузі.

У **висновках** дисертаційної роботи викладено основні результати і рекомендації, які випливають з проведених досліджень, представлено та охарактеризовано показники ефективності параметрів захищеності на основі використання запропонованої методології дослідження, що включає методи, методики та експеримент.

**3. Наукова новизна одержаних результатів.**

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

*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, 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 від 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.
- *розроблено* діагностичну модель системи-приманки для бездротових мереж стандарту IEEE 802.11, яка на відміну від підходів зі «сліпою конфігурацією» чи клонуванням існуючої бездротової інфраструктури дозволяє оцінити рівень захищеності системи-приманки у 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.
- *розроблено* метод виявлення вторгнень із застосуванням машинного навчання, а саме алгоритму K-найближчих сусідів, в якому застосовано оригінальний метод агрегації даних щодо потужності сигналу, що зокрема 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. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних дисциплін, де можуть бути застосовані отримані результати.**

Наукові результати, отримані автором, можуть бути використані при проектуванні захищеної бездротової мережевої інфраструктури для комерційних та некомерційних структур, а також для збору розвідувальних даних у військових операціях.

Отримані здобувачем наукові положення, висновки та практичні результати можуть бути використані під час розробки нових, а також вдосконалення вже існуючих навчальних дисциплін для галузі 12 «Інформаційні технології» та спеціальності 125 «Кібербезпека та захист інформації» пов'язаних з забезпеченням належного функціонування інформаційно-комунікаційних систем, зокрема із забезпеченням їх безпеки та проведення тестування їх захищеності.

**5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна** базується на кваліфікованому підході до постановки завдань дослідження, логічно правильному обґрунтуванні прийнятих допущень

під час вибору математичних моделей і коректному використанні математичного апарату. Достовірність результатів проведеного дослідження забезпечена методологічною обґрунтованістю, застосуванням комплексу різноманітних методів, які взаємно доповнюють один одного і відповідають предмету, меті та завданням дослідження, а також об'єктивним аналізом експериментальних результатів, що характеризуються науковою новизною. Крім того, достовірність підтверджується результатами фізичного та комп'ютерного моделювання і розробкою практичних рекомендацій для підвищення ефективності застосування систем виявлення вторгнень і систем-приманок для мереж стандарту IEEE 802.11.

6. **Практичне значення одержаних результатів** полягає у тому, що:

- Обґрунтовано актуальність науково-практичного завдання дослідження, включаючи розробку методології оцінки захисту систем-приманок та використання штучного інтелекту для поліпшення ефективності систем виявлення вторгнень.

- Розроблено та проаналізовано моделі порушника у бездротових мережах стандарту IEEE 802.11. Даний аналіз дозволяє краще зрозуміти можливі ризики і розробляти ефективні методи їх протидії. Досліджено можливі демаскуючі ознаки систем-приманок, зокрема можливість їх виявлення на різних рівнях моделі OSI: канальному, мережевому та прикладному, що дозволяє уникнути виявлення систем-приманок зловмисниками і позитивно впливає як на функціонування безпосередньо самих систем-приманок, так і на безпеку бездротової мережі Wi-Fi в цілому.

- Розроблено концептуально нову модель системи захисту інформації з використанням систем-приманок, що відповідає сучасним викликам і вимогам безпеки. У цьому контексті описано мінімальний набір елементів, за допомогою яких можна реалізувати таку систему. Регламентовано правила комунікації між їх елементами. Для елементів зовнішнього сегменту системи захисту інформації та системи бездротової мережі запропоновано обчислювальні платформи. Для розв'язання проблем масштабованості розробленої системи також запропоновано використання хмарних обчислень.

- Досліджено критичні недоліки публічних баз даних з геолокації точок доступу Wi-Fi як інструменту пошуку зловмисника за слідами, залишеними до, під час та після проведення атаки на Wi-Fi інфраструктуру. Такими недоліками визначено відсутність стандартизації обладнання, яке проводить збір та обробку даних; відсутність валідації даних, які приходять від контриб'юторів; відсутність агрегації даних на основі унікальних екземплярів. Натомість запропоновано методику, яка дозволяє безперервно покращувати точність геолокації знайдених точок доступу за рахунок метрики потужність сигналу, введення поняття

унікальності знайдених екземплярів та стандартизації обладнання контриб'юторів. Як результат, вдалось досягти високої ефективності у віднайдені унікальних екземплярів з точністю 90-100% на противагу 0.5-1% з використанням публічних базах даних.

- Розроблено та застосовано діагностичну модель, визначено коефіцієнти для усіх наявних механізмів захисту бездротових мереж стандарту IEEE 802.11. Даний підхід дозволяє підібрати налаштування системи-приманки згідно із визначеним профілем зловмисника, що може значно покращити продуктивність у їх застосуванні. Зважаючи на актуальність протоколу захисту WPA2 було розроблено деталізовану діагностичну модель відносно складності подолання його ключа. Для обчислення складності перебору було використано дві різні технології – повна віртуалізація та контейнеризація. Визначено, що контейнеризація є продуктивнішою на 11% за повну віртуалізацію і дозволяє швидко масштабувати ресурси.
- Розроблено та застосовано модель машинного навчання на основі алгоритму KNN для виявлення атаки «злий двійник» в мережі стандарту IEEE 802.11. Розроблено програмно-апаратний комплекс, що забезпечує моніторинг службових пакетів в етері мережі стандарту IEEE 802.11 з високою ефективністю та мінімальним енергоспоживанням. Завдяки безперервному моніторингу етеру та використанню алгоритмів машинного навчання на зібраних даних моделі вдалося відрізнити легітимні точки доступу від імітованих нелегітимних у 100% випадків. Це свідчить про високу ефективність даного підходу у виявленні атаки «злий двійник».

**7. Повнота оприлюднення результатів дисертаційної роботи.**

Основні наукові результати дисертаційної роботи Банаха Р. І. достатньо повно відображені у 27 працях, з них 11 статей, 9 з яких входять до переліку видань ВАК та 2 проіндексовано міжнародною наукометричною базою даних SCOPUS, 1 проіндексована міжнародними наукометричними базами даних Copernicus та Google Scholar, 1 розділ монографії. 14 тез доповідей, 3 з яких проіндексовано міжнародною наукометричною базою даних SCOPUS. Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. З праць, опублікованих у співавторстві, у дисертації використано лише ті результати, які отримано здобувачем самостійно.

**8. Оцінка структури дисертації, її мови та стилю викладення.**

Дисертація за структурою, мовою та стилем викладення оформлена відповідно до вимог МОН України, що висуваються до подібного роду наукових робіт. Дисертація написана грамотною українською мовою з використанням

сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним. Зміст наукових праць доповнює основні положення дисертації.

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

Ознайомлення з текстом анотації дає змогу констатувати, що її зміст повною мірою відображає основні положення і висновки дисертації.

**9. Зауваження та дискусійні положення щодо змісту роботи.**

Загалом позитивно оцінюючи дисертаційне дослідження, також доречно висловити певні зауваження та вказати на окремі положення роботи, що викликають дискусію:

1) У розділі 1.1 дослідження надано детальний опис переходу між протоколами захисту WEP і WPA, а також між протоколами WPA2 та WPA3. Однак, перехід між протоколами WPA та WPA2 не розглянуто настільки детально, хоча між ними існує значна кількість відмінностей. Зважаючи на важливість цього аспекту, доцільно було б включити більш розгорнутий аналіз переходу між WPA і WPA2, з метою детального висвітлення змін та покращень, які були впроваджені з метою підвищення безпеки бездротових мереж. Такий аналіз дозволив би краще зрозуміти еволюцію протоколів безпеки і важливість кожного з них у контексті захисту інформації.

2) В рамках даного дисертаційного дослідження автор здійснює досить поверхневий опис лише певної частини можливих атак на мережі стандарту IEEE 802.11, дещо деталізуючи деякі з них в окремих підрозділах. Доречно було б акумулювати та деталізовано описати саме ті типи атак, на виявленні яких акцентується увага, а решту винести за рамки дослідження. Це дозволило б більш ґрунтовно підійти до питання побудови моделі порушника.

3) У розділі 2.4.2 на рис. 2.3 – 2.4 автор вдало представив концепцію користувацького застосунку у графічному форматі. Проте, варто зазначити, що більш інформативним було б представлення виконане за допомогою гіпертекстової мови розмітки та каскадних таблиць стилів. Такий підхід не тільки дозволив би забезпечити наочність та структурованість інформації, але й сприяв би підвищенню зручності користувача під час взаємодії з застосунком. Використання сучасних веб-технологій могло б значно покращити візуалізацію та функціональність розробленої концепції.

4) В основу представленої в розділі 3.1. здобувачем методики відслідковування зловмисників покладено механізм повторного підключення до мережі, що дозволяє отримувати дані про те, до яких мереж зловмисник підключався раніше. Водночас, припускаючи, що пристрій атаки з високою імовірністю буде не єдиним пристроєм зловмисника і потрапивши у зону

покриття своєї цілі, інші пристрої (смартфон, розумний годинник та інші IoT пристрої) зловмисника будуть надсилати пошукові пакети в етер. Однак, автором попередньо не визначено механізму ідентифікації самого зловмисника (пристрою атаки). І хоча здобувач пропонує вдосконалений метод виявлення атак пов'язаних з підміною MAC адрес попередньо ідентифікуючи активний пристрій атаки (розділ 3.3.), в решті випадків такий пристрій залишається поза увагою, зокрема при реалізації атаки на ключі шифрування.

5) В рамках вдосконаленого методу виявлення вторгнень в мережі IEEE 802.11 автором, без попереднього проведення дослідження можливостей застосування різних моделей машинного навчання, було прийнято рішення застосовувати алгоритм класифікації k-найближчих сусідів (KNN). Відсутність такого порівняння обмежує обґрунтованість вибору KNN як оптимального методу. Доречно було б дослідити ефективність інших алгоритмів, таких як метод опорних векторів (Support Vector Machine, SVM), ізоляційний ліс (Isolation Forest, IF), метод k-середніх (Average KNN, AKNN), кластерний метод (Cluster-based Local Outlier Factor, CLOF) та ін.

6) У розділі 3.1.1, на рисунку 3.4, представлено візуалізацію графу територіального розташування точок доступу, зібраних з клієнтських пристроїв зловмисника. Хоч пояснення щодо рисунку є присутнім, проте, функціональна цінність цієї візуалізації не є повністю розкритою. Візуалізація виглядає дещо абстрактною, і додаткові коментарі або приклади застосування могли б допомогти підкреслити її практичне значення та корисність.

7) У розділі 4.1 автором запропонована методика відстеження зловмисників, яка передбачає попереднє збирання інформації про точки доступу на певній територіальній одиниці. Однак, виникають питання щодо правової бази для застосування цієї методики в рамках українського законодавства. Незважаючи на те, що зібрана інформація може бути відкритою, можливі правові колізії, які потребують детального розгляду. Доцільно було б надати додаткове обґрунтування щодо законодавчої правомірності використання цієї методики та описати можливі ризики або обмеження, які можуть виникнути при її застосуванні у практичних умовах.

8) Визначення чіткіших критеріїв дало б змогу краще оцінити ефективність зокрема в числовому еквіваленті розроблених методів.

**Загальні висновки щодо дисертаційної роботи.**

Дисертаційна робота Банаха Романа Ігоровича «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» є завершеним, самостійним та цілісним науковим дослідженням, що містить достатню наукову новизну та практичну цінність отриманих результатів, які дозволяють підвищити ефективність систем виявлення вторгнень та систем-

приманок, які застосовуються у мережах стандарту IEEE 802.11. Зміст дисертаційної роботи «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» відповідає обраній темі та забезпечує досягнення поставленої мети, відповідає вимогам порядку присудження ступеня доктора філософії, а її автор, Банах Роман Ігорович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації».

**Офіційний опонент**
доцент кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка
доктор філософії, доцент Роман КИРИЧОК

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Кириченко Р.
(ПІБ)
ЗАСВІДЧУЮ
Провід. фах. В.К.
(посада)