Затверджую
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
проф. Іван ДЕМИДОВ
_____
2 травня 2024 р.

Висновок
про наукову новизну, теоретичне та практичне значення результатів дисертації «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11»
здобувача наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 Інформаційні технології)
Банаха Романа Ігоровича

наукового семінару кафедри безпеки інформаційних технологій

1. **Актуальність теми дисертації**

Бездротові мережі стали невід'ємною частиною повсякдення як домашніх, так корпоративних користувачів надавши свободу пересування під час роботи чи дозвілля. Одними з них є мережі стандарту IEEE 802.11 (Wi-Fi), які з'явились на ринку відносно нещодавно, та зараз, мабуть, не знайдеться жодного мобільного пристрою, який би не був оснащений модулем Wi-Fi. У випадку передавання даних по радіоканалу, ще не винайдено нічого кращого за радіусом дії і швидкості передачі ніж Wi-Fi, та у випадку даної технології платити доводиться безпекою.

Безпека є надважливим аспектом організації обміну інформації будь-якого підприємства. Якщо доступ до дротових мереж можна отримати лише фізично підключившись до порта комутатора чи до мережевої розетки, то підключення до бездротової мережі є набагато простішим, необхідно бути лише у зоні її покриття. Бездротові мережі використовують радіохвилі, які розповсюджуються за законами фізики, і контролювати їх поведінку є не тривіальним завданням.

Поряд із перевагами, які надають мережі Wi-Fi, стоять і виклики, пов'язані із інформаційною безпекою. За наявності вузько-направленої антени високої потужності, зловмисник може вторгнутись у бездротову мережу на відстанях 2 км і більше, таким чином ускладнюється завдання визначення його місцезнаходження.

Завдяки зусиллям постачальників споживчого Wi-Fi обладнання, більшість пристроїв поставляються вже налаштованими за замовчуванням, що дозволяє відразу починати роботу. Та навіть, якщо користувач налаштує маршрутизатор, застосовуючи найстійкіші протоколи захисту, така мережа не може вважатись безпечною через велику кількість відомих вразливостей в сучасних протоколах безпеки мереж стандарту IEEE 802.11.

Одним із методів уникнення атак на виробничі середовища є системи-приманки, застосування яких для захисту мереж стандарту IEEE 802.11 є дуже недооціненим.

Якщо на початковому етапі Wi-Fi мережі були практично беззахисними від атак, то зараз ситуація помітно покращилась. На сучасному етапі розвитку технологій існує ціла низка рішень, які дозволяють зробити бездротову мережу відносно захищеною. Це можуть бути апаратні і/або програмні засоби, платні або безкоштовні рішення, та якщо взяти до уваги розповсюдженість технології Wi-Fi, то для створення безпечного середовища кожен користувач повинен володіти базовими знаннями з адміністрування комп'ютерних мереж та кібербезпеки. Окрім того, в арсеналі рядових користувачів немає інструментів за допомогою яких би вони могли ідентифікувати вторгнення, відводити атаки від власних мереж, а також виявляти особу зловмисника задля заяви про неправомірні дії у відповідні державні органи.

Отже, у зв'язку з необхідністю забезпечення безпеки як корпоративних, так і персональних мереж Wi-Fi, а також відсутністю простих механізмів для вирішення цієї проблеми, виникає науково-практичне завдання щодо удосконалення систем виявлення вторгнень та систем-приманок у мережах стандарту IEEE 802.11.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

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).

3. Особистий внесок здобувача в отриманні наукових результатів

Аналіз структури та змісту дисертаційної роботи та наукових праць, що опубліковані автором, дозволяє стверджувати, що усі наукові та практичні результати отримані ним особисто та повною мірою опубліковані й апробовані. Банахом Р.І. було проаналізовано сучасний стан захищеності комп'ютерних мереж Wi-Fi, на основі чого було розроблено діагностичну модель для систем-приманок в мережах стандарту IEEE 802.11. Також здобувачем було описано основні характеристики технології Wi-Fi, методи її захисту та нормативно-правове забезпечення, яке стосується даної технології. Окрім того, було досліджено перспективи розвитку систем-приманок для їх застосування у бездротових мережах. В групі наукових праць автором було застосовано практики тестування на проникнення для визначення ефективності систем виявлення вторгнень та систем-приманок у бездротових мережах стандарту IEEE 802.11. Автором було запропоновано оригінальну методику для збору інформації про зловмисників, які здійснили атаки на бездротові мережі стандарту IEEE 802.11, а також здійснено аналіз відкритих баз даних, які надають інформацію про точки доступу Wi-Fi, як інструменту для виявлення потенційних місць перебування зловмисника, описано їх недоліки та запропоновано шляхи їх вирішення. У своїх наукових працях здобувач детально описав концепцію побудови апаратно-програмного комплексу із застосуванням систем виявлення вторгнень, систем-приманок, застосовуючи хмарні обчислення та одноплатні комп'ютери, які можуть бути застосовані для покращення кібербезпеки у бездротових мережах стандарту IEEE 802.11. Автором було запропоновано застосування хмарних обчислень, як платформи до розв'язання проблеми з визначення рівня захищеності бездротових мереж стандарту IEEE 802.11, а також запропоновано принципово новий підхід до вибору ключів WPA/WPA2 для подальшого їх застосування на системах-приманках. Здобувачем Банахом Р.І. було розроблено метод виявлення атак з підміни MAC адрес та «злий двійник» із застосуванням штучного інтелекту, на основі аналізу потужності сигналу від точок доступу Wi-Fi.

4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій

Аналіз змісту розділів, використаного інструментарію та способів його застосування дозволяє зробити висновок про належну обґрунтованість наукових результатів. Наукові положення, висновки та рекомендації, сформульовані у дисертації, повністю обґрунтовано теоретичним аналізом, результатами практичного використання та інформацією з науково-технічної літератури, підтверджено характеристиками впроваджених результатів.

Список опублікованих праць за темою дисертації:

Статті у наукових виданнях, які включені до міжнародної наукометричної бази даних SCOPUS:

1. Banakh R., Piskozub A., Opirskyy I. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices // Advances in Intelligent Systems and Computing (AISC). 2019. 754: Advances in computer science for engineering and education : 1st International conference on computer science, engineering and education applications, ICCSEEA2018, Kiev, Ukraine, 18 20 January 2018. P. 468–477.
2. Banakh R., Piskozub A., Opirskyy I. Devising a method for detecting "evil twin" attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model // Східно-Європейський журнал передових технологій. 2023. № 3/9 (123). P. 20–32. (квартиль Q3 у НМДБ Scopus)

Статті у наукових фахових виданнях України:

1. Дудикевич, В. Б. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку. / Дудикевич, В. Б., Микитин, Г. В., Ребець, А. І., Банах, Р. І. // Сучасна спеціальна техніка, (2014/4), 75-82 сс.
2. Дудикевич В. Б. Інформаційна модель безпеки технологій зв'язку. / Дудикевич В. Б., Хорошко В. О., Микитин Г.В., Банах Р.І., Ребець А.І. // Інформатика та математичні методи в моделюванні 2014 Том 4. – №2. – 137–148 сс.
3. Банах Р. І. Створення концепції захищеної хмарної обчислювальної інфраструктури з використанням систем приманок / Банах Р. І., Піскозуб А. З., Стефінко Я. Я. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". 2015. № 821. С. 74–78.
4. Стефінко Я. Я. Тестування на проникнення з Metasploit і shell скриптами / Стефінко Я. Я., Піскозуб А. З., Банах Р. І. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". 2015. № 821. С. 90–93.
5. Банах Р. І. Автоматизація розгортання Wi-Fi точки доступу, як зовнішнього елементу системи приманки / Банах Р. І., Піскозуб А. З., Стефінко Я. Я. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". 2016. № 852. С. 130–136.

6. Банах Р. І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Банах Р. І., Піскозуб А. З. // Системи обробки інформації. 2017. Вип. 2 (148). С. 77–83.
7. Банах Р. І., Піскозуб А. З. Оцінка надійності елементів системи-приманки у мережі стандарту IEEE 802.11 як розгалуженої системи зі складним підпорядкуванням / Банах Р. І., Піскозуб А. З. // Вісник Національного університету "Львівська політехніка". Серія "Автоматика, вимірювання та керування". 2017. № 880. С. 94–98.
8. Банах Р. І. Визначення параметрів ключа методу автентифікації WPA/WPA2 для системи-приманки мережі стандарту IEEE 802.11 / Банах Р. І. // Радіоелектроніка, інформатика, управління. 2018. №1. С. 110–118.
9. Банах Р. І. Застосування хмарних обчислень для визначення рівня захищеності бездротових мереж стандарту IEEE 802.11 / Банах Р. І., Піскозуб А. З. // Сучасна спеціальна техніка. 2021. № 4 (67). С. 5–15.

Монографії

1. Banakh R. Wi-Fi Honeypot as a service. Conception of business model / Banakh R. // "ENGINEER OF XXI CENTURY": VI INTER UNIVERSITY CONFERENCE OF STUDENTS, PHD STUDENTS AND YOUNG SCIENTISTS. Bielsko-Biała, Poland December 02, 2016. – 928p. – 59–64 pp.

Матеріали конференцій

1. Банах Р. І. Аналіз подій у безпровідних комп'ютерних мережах для автоматизації тестування на проникнення / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем" – Львів, 2015. – 73–74 сс.
2. Банах Р. І. Створення концепції захищеної хмарної обчислювальної мережі із застосуванням систем приманок / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем" – Львів, 2015 – 75–76 сс.
3. Банах Р. Одноплатна робоча станція як компонент системи приманки у безпровідних комп'ютерних мережах. / Банах Р., Стефінко Я. // Захист інформації в інформаційно-комунікаційних системах. Тези доповідей І Міжвузівської науково-практичної конф. студентів і курсантів – Львів, 2015 – С. 6–7.

4. Піскозуб А.З. Тестування на проникнення з допомогою open-source OS Linux і shell скриптів / Піскозуб А.З., Стефінко Я.Я., Банах Р.І. // Матеріали п'ятої науково-практичної конференції FOSS Lviv 2015 (23-26 квітня 2015р.), м Львів – 133–136 сс.
5. Банах Р.І., Тестування на проникнення як механізм аналізу ефективності системи приманки для мережі Wi-Fi. / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Тези доповіді ІІ-ої Міжнародної науково-технічної конференції 24-25 листопада 2016 р. «Інформаційна безпека в сучасному суспільстві» 119с., 79—80 сс.
6. Стефінко Я. "Тестування на проникнення у навчальних лабораторіях з застосуванням контейнеризації" / Стефінко Я., Піскозуб А., Банах Р. // Тези доповідей: Матеріали 8-ї науково-практичної конференції "Інноваційні комп'ютерні технології у вищій школі" . Львів – В-во наук.тов. ім.Т.Г.Шевченка - 2016.- С. 144-151.
7. Banakh R. External elements of honeypot for wireless network / Banakh R., Piskozub A., Stefinko Y. // "Modern Problems of Radio Engineering, Telecommunications, and Computer Science": Proceedings of the XIIIth International Conference TCSET'2016. Lviv-Slavsko, Ukraine February 23 – 26, 2016. Lviv Publishing House of Lviv Polytechnic 2016. 480-482p.
8. Manual and Automated Penetration Testing. Benefits and Drawbacks. Modern Tendency» / Yaroslav Stefinko, Andrian Piskozub, Roman Banakh // Modern Problems of Radio Engineering, Telecomunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET'2016 – Lviv-Slavsko, Ukraine, 2016. – 961p. 488-491p.
9. Банах Р. Перспективи розвитку систем приманок для безпровідних мереж / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Інформація, комунікація, суспільство 2016: матеріали 5-ої Міжнародної наукової конференції ІКС-2016, 19–21 травня 2016 року, Україна, Львів, Славське / Національний університет "Львівська політехніка", Кафедра соціальних комунікацій та інформаційної діяльності. – Львів: Видавництво Львівської політехніки, 2016. – С. 30–31.
10. Банах Р.І. Збір та обробка метаданих зловмисника для виявлення імовірних місць його перебування з пристроїв стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // 4-th International Conference on Computational Intelligence (ComInt 2017), Taras Shevchenko National University of Kyiv, May 16-18, 2017. – 197–198 сс.
11. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // Матеріали Міжнародної

науково-практичної конференції "Проблеми і перспективи розвитку IT-індустрії": тези доповідей, 20 – 21 квітня 2017 р. – Х.: ХНЕУ імені Семена Кузнеця, 2017. – 92 с. – 27–28 сс.

12. Банах Р.І. Вимірювання потужності сигналу від клієнтських пристроїв в мережах IEEE 802.11 для тренування моделей машинного навчання задля виявлення атак / Банах Р.І., Піскозуб А.З. // Матеріали IX Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем» – Львів : Видавництво Львівської політехніки, 2023. – 185 с. – 53–54 сс.
13. Банах Р.І. Проблематика використання відкритих джерел даних у розслідувані кіберзлочинів у мережах стандарту IEEE 802.11 / Банах Р.І. // Матеріали II Міжнародної наукової конференції «Теорія модернізації в контексті сучасної світової науки», м.Ужгород, 1 березня, 2024р. / Міжнародний центр наукових досліджень. — Вінниця: ТОВ «УКРЛОГОС Груп, 2024.—244с. – 145–147 сс.

5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру

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.

6. Перелік наукових праць, які відображають основні результати дисертації

Загальна кількість публікацій за темою дисертації становить 27, з них одинадцять статей, дев'ять з яких входять до переліку наукових фахових видань України, дві проіндексовано міжнародною наукометричною базою даних SCOPUS, одна проіндексована міжнародними наукометричними базами даних Copernicus та Google Scholar. Одна монографія. Чотирнадцять тез доповідей, три з яких проіндексовано міжнародною наукометричною базою даних SCOPUS.

7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні наукові результати і положення дисертації представлені, доповідались та обговорені на 16-и міжнародних і державних науково-технічних конференціях: I Міжвузівська науково-практична конференція студентів і курсантів «Захист інформації в інформаційно-комунікаційних системах» (м. Львів, 2015 р.), IV Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем" (м. Львів, 2015 р.), V науково-практична конференція FOSS Lviv 2015 (м. Львів, 23-26 квітня 2015 р.), XIII Міжнародна конференція TCSET'2016 «Modern Problems of Radio Engineering, Telecommunications, and Computer Science» (м. Львів, м. Славсько, 23 – 26 лютого, 2016 р.), XIII науково-практична конференція «Інноваційні комп'ютерні технології у вищій школі» (Львів, 2016 р.), V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2016 р), V Міжнародна наукова конференція «ICS-2016» (Львів, 2016 р.), II Міжнародна науково-технічна конференція «Інформаційна безпека в сучасному суспільстві» (Львів, 2016 р.), VI міжуніверситетська конференція студентів, аспірантів та молодих вчених «ENGINEER OF XXI CENTURY» (Польща, Б'єльсько-б'яла 2016), VIII Міжнародна конференція молодих вчених «Комп'ютерні науки та інженерія» (CSE 2016) (Львів, 2016 р.), 4-а Міжнародна конференція з обчислювального інтелекту «ComInt 2017» (Київ, 2017 р.), Міжнародна науково-практична конференція "Проблеми і перспективи розвитку IT-індустрії" (Харків, 20–21 квітня 2017 р), Міжнародна науково-практична конференція «обчислювальний інтелект (результати, проблеми, перспективи)»

(Київ-Черкаси, 16-18 травня 2017р.), V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем 2017» (Львів, 01–02 червня 2017 р.), IX Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2023 р.), II Міжнародній науковій конференції «Теорія модернізації в контексті сучасної світової науки» (Ужгород, 1 березня 2024 р).

8. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати

Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри «Безпека інформаційних технологій» Національного університету «Львівська політехніка» при вивченні дисциплін:

- «Інформаційно-комунікаційні системи» для студентів 125 «Кібербезпека», спеціалізації «Кібербезпека комп'ютерних систем та мереж», тема №1 «Застосування віртуалізації та контейнеризації в інформаційно-комунікаційних системах» – огляд технологій, переваги та недоліки, масштабованість, застосування технологій віртуалізації та контейнеризації для високонавантажених систем обчислення; тема №5 «Безпека інформації у хмарних обчисленнях» – використання хмарних обчислень та організація безпеки в середовищі хмарного провайдера Amazon Web Services.

9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані

Практична цінність роботи полягає у можливості їх безпосереднього застосування для підсилення наявних систем виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11 як у корпоративному, так і приватному середовищах.

1. Проведено огляд існуючих рішень та реалізацій систем виявлення вторгнень і систем-приманок для комп'ютерних мереж стандарту IEEE 802.11, а також проаналізовано стан сучасних досліджень у цій галузі. За результатами аналізу встановлено, що сучасні системи виявлення вторгнень переважно базуються на сигнатурних методах, а системи-приманки частіше використовуються як інструменти зловмисників. Також визначено, що виявлення зловмисника, який здійснює атаку на бездротову мережу, може становити проблему через його можливе операційне виходження за межі контрольованої зони. Обґрунтовано актуальність науково-практичного завдання дослідження, включаючи розробку методології оцінки захисту систем-приманок та використання штучного інтелекту для поліпшення ефективності систем виявлення вторгнень.

2. Розроблено та проаналізовано моделі порушника у бездротових мережах стандарту IEEE 802.11 для підприємства. Даний аналіз дозволяє краще

зрозуміти можливі ризики та розробляти ефективні методи протидії. Досліджено можливі демаскуючі ознаки систем-приманок, зокрема їх можливість виявлення на різних рівнях моделі OSI: канальному, мережевому та прикладному, що дозволяє уникнути виявлення систем-приманок зловмисниками та позитивно впливає як на функціонування систем-приманок, так і на безпеку бездротової мережі Wi-Fi та інших пов'язаних мережевих ресурсів.

3. 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.

4. 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 потужності сигналу, введення поняття унікальності знайдених екземплярів та стандартизації обладнання контрибюторів. В результаті вдалось досягти точності у віднайденні унікальних екземплярів з точністю 90—100% на противагу 0.5—1% у публічних базах даних.

5. Розроблено та застосовано діагностичну модель, визначено коефіцієнти для усіх наявних механізмів захисту бездротових мереж стандарту IEEE 802.11 (Wi-Fi). 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 віртуалізації – повна і контейнеризація. Визначено, що контейнеризація є продуктивнішою на 11% за повну віртуалізацію і дозволяє швидко масштабувати ресурси.

6. Розроблено та застосовано модель машинного навчання на основі алгоритму KNN для виявлення атаки "злий двійник" в мережі стандарту IEEE 802.11 (Wi-Fi). 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". Виявлення цього типу атак є надзвичайно важливим для захисту мереж стандарту IEEE 802.11 (Wi-Fi), оскільки атака "злий двійник" є одним із інструментів у широкому спектрі векторів атак, включаючи атаки на WPA3.

Наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри безпеки 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.

10. Оцінка структури дисертації, її мови та стилю викладення

Дисертація в цілому має логічну структуру, яка визначається метою та етапами вирішення поставлених завдань. Мова та стиль викладення матеріалу дисертації не викликають суттєвих зауважень.

У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

11. З урахуванням зазначеного, на науковому семінарі кафедри безпеки інформаційних технологій ухвалили:

11.1. Дисертація Банаха Романа Ігоровича «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» є завершеною науковою працею, у якій розв'язано конкретне наукове завдання з *удосконалення технології виявлення вторгнень і систем-приманок у мережах IEEE 802.11*, що має важливе значення для кібербезпеки бездротових комп'ютерних мереж.

11.2. Основні наукові положення, методичні розробки, висновки та практичні рекомендації, викладені у дисертаційній роботі, логічні, послідовні, аргументовані, достовірні, достатньо обґрунтовані. Дисертація характеризується єдністю змісту.

11.3. У 27 наукових публікаціях повністю відображені основні результати дисертації, з них дев'ять статей у наукових фахових виданнях України та дві статті у наукових періодичних виданнях, що індексуються в наукометричній базі даних Scopus.

11.4. Дисертація відповідає вимогам наказу МОН України №40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. №44, зі змінами).

11.5. Дисертація є результатом самостійних досліджень, не містить елементів фільсифікації, компіляції, плагіату та запозичень, що констатує

відсутність порушення академічної доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

11.6. З урахуванням наукової зрілості та професійних якостей Банаха Романа Ігоровича дисертація «Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» рекомендується для подання до розгляду та захисту у спеціалізованій вченій раді.

За затвердження висновку проголосували:

за	- двадцять один
проти	- немає
утримались	- немає

Головуючий на науковому семінарі кафедри безпеки інформаційних технологій, д.т.н., с.т.с., завідувач кафедри безпеки інформаційних технологій _____ Ігор ЖУРАВЕЛЬ

Рецензенти:

к.т.н., доцент кафедри безпеки інформаційних технологій _____ Тетяна КОРОБЕЙНІКОВА

д.т.н., професор, професор кафедри безпеки інформаційних технологій _____ Віктор МЕЛЬНИК

Відповідальний
у ННІ за атестацію PhD
д.т.н., професор, професор кафедри захисту інформації _____ Любомир ПАРХУЦЬ

«25» квітня 2024 р