КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (18), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.18.99107
УДК 004.056

Корольков Роман Юрійович
кафедра захисту інформації,
Національний університет "Запорізька політехніка"
м. Запоріжжя, Україна,
ORCID ID: 0000-0001-5501-4600
romankor@zntu.edu.ua

Лаптєв Сергій Олександрович
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-7291-1829
salaptiev@gmail.com

НАТУРНЕ МОДЕЛЮВАННЯ АТАКИ «WAR DRIVING» НА БЕЗДРОТОВУ МЕРЕЖУ

Анотація. Неминуче поширення бездротових мереж та зростаючий трафік у них, може призвести до збільшення інцидентів інформаційної безпеки. Основні загрози спрямовані на перехоплення, порушення конфіденційності і цілісності переданих даних, здійснення атак на доступність вузлів каналу передачі та їх підміну. Бездротове середовище передачі даних внаслідок своїх особливостей створює потенційні умови для прослуховування мережного трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які перебувають в зоні її дії. Бездротові мережі, на відміну від дротових, надзвичайно вразливі до можливих атак і несанкціонованого доступу через використання радіодіапазону та широкомовну природу фізичного рівня. Для перехоплення даних достатньо перебувати в зоні дії мережі Wi-Fi. Тому зловмисник, перебуваючи на безпечній відстані, може використати бездротові пристрої для реалізації атак. У статті проведено аналіз кібератаки типу «War Driving» на бездротові мережи. Проведений у статті аналіз показав, що існують відкриті бездротові мережі. Бездротові мережі відкриті або тому, що адміністратори, які їх конфігурують, не інформовані про безпеку. Проведено натурне моделювання атаки типу «War Driving». Данні отриманні натурним моделюванням свідчать, що 10,1% мереж не використовують ніякого шифрування. Похибка виявлення точок доступу не використовуючих шифрування складає від 8% до 12%. Це е дуже гарним результатом та підтверджує адекватність проведеного натурного моделювання. Виходячи з аналізу результатів натурного моделювання, з метою захисту бездротової мережи від атаки типу «War Driving» розроблені рекомендації. Розроблені рекомендації дозволять захистити бездротові мережи від атак типу «War Driving».

Ключові слова: атака, загроза, бездротові мережи, натурне моделювання, точка доступу.

ВСТУП

Згідно з розрахунками експертів, обсяг світового ринку споживчого та корпоративного обладнання, призначеного для розгортання бездротових локальних мереж (WLAN), зріс на 10,9% багато в чому завдяки 16,4-відсотковому підйому споживчого сегменту. Що стосується бізнес-сектору, то він також показує позитивну динаміку, чому багато в чому сприяє перехід компаній на стандарт Wi-Fi 6. Зростання точок доступу у бездротовій локальній мережі за рік склало 23%. Виторг операторів зв'язку від послуг Wi-Fi минулого року на 12% більше, ніж у 2020 році. Розвиток бездротових мереж привів до негативних факторів. Аналіз показав, що основні загрози у бездротової мережи спрямовані на перехоплення, порушення конфіденційності і цілісності переданих даних. Серед усіх загроз безпеці бездротової мережі одна з

небезпечних загроз, атака типу «War Driving». Поки немає жодних спеціальних законів проти «War Driving», отримані дані можуть бути використані для експлуатації незахищених мереж, стаючи сірою зоною захисту особистої конфіденційності. «War Driving» являє собою фізичний пошук вразливих бездротових мереж з використанням транспортного засобу, що рухається, і меппінг (відображення) бездротових точок доступу. Є три основні причини, через які вардрайвери шукають незахищені Wi-Fi мережі. Перша причина – це крадіжка особистої та банківської інформації. Друга – можливість використовувати вашу мережу для злочинної діяльності, за яку відповідати будете ви, як власник мережі. І третя причина полягає в тому, щоб знайти дірки безпеки мережі[1,2]. Етичні хакери роблять це за допомогою «War Driving» з метою пошуку вразливостей підвищення загального рівня безпеки.

Виходячи з викладеного аналіз існуючих атак та вивчення методів проведення атак на бездротові інформаційні мережі є актуальним науковим завданням.

Постановка проблеми. Існують відкриті бездротові мережі. Бездротові мережі відкриті або тому, що адміністратори, які їх конфігурують, не інформовані про безпеку, або тому, що ці точки доступу навмисно залишають відкритими. Тому існує проблема втрати данних користувачів у бездротових мережах. Для вирішення цієї проблеми пропонується провести аналіз кібератак на бездротові мережи, провести натурне моделювання небезпечної атаки типу «Вардрайвінг» та розробити рекомендації . що до захисту бездротової мережі від такого типу атак.

Аналіз останніх досліджень і публікацій. Для застосування вирішення завдань аналізу атак на бездротові мережі використовується багато різних методів моделювання.

Так у роботах [2,5-9] наводиться приклад атаки на бездротову мережу за допомогою набора спеціалізованих інструментів. Для цього в арсеналі можуть бути потужні Wi-Fi адаптери, спрямовані антени, мікрокомп'ютери для створення шахрайської точки доступу, обладнання для потайного аналізу бездротових мереж, що дозволяє проводити активний аналіз безпеки бездротової мережі. Описується алгоритм здійснення атаки. На початковому етапі отримуються дані про механізми безпеки, що використовуються алгоритми шифрування та механізми аутентифікації. Вся отримана інформація надалі бути використана безпосередньо для атак на інформаційну мережу. Говориться, що більшість компаній, в інфраструктурі яких використовуються бездротові мережі, не вживають достатніх заходів щодо їх захисту. Тобто більш детально розглядаються атаки із середини мережи. Повний перелік атак не розглядається.

У роботах [3,10,11] наводиться приклади небезпеки бездротової мережи. Особливість передачі інформації, передача повітрям означає, що «підслухати» вас може будь-хто. Рік у рік фахівці з мережевої безпеки продовжують озвучувати просто жахливу статистику своїх спостережень - величезна кількість компаній по всьому світу продовжують недбало ставитися до безпеки своїх корпоративних Wi-Fi мереж. В останні роки також почастішали випадки з використанням безпілотних апаратів. Результати їх досліджень вражають. Так, наприклад, з 81 743 бездротових мереж, просканованих кілька років тому в Лондоні, 29,5 % взагалі не мають жодного захисту або використовують алгоритм WEP (Wired Equivalent Privacy), який уже понад 15 років вважається вкрай вразливим. Більше того, ще 52% відсканованих мереж використовували Wi-Fi protected Access (WPA), який також не рекомендується використовувати спеціалістами у сфері інформаційної безпеки. У цих роботах головний акцент присвячено саме відсутності захисту бездротових мереж, атаки на ці мережи детально не розглядаються.

У роботі [4,12-15] описуються короткі відомості про бездротові мережі, зокрема - Wi-Fi, оскільки ця мережа зустрічається навіть у віддалених куточках світу і означає

для багатьох бездротовий доступ в інтернет за допомогою смартфона або ноутбука. Проаналізовано методи шифрування WEP, WPA, WPA та розглянуто знайдені вразливості у них. Зокрема, розглянуті практичні дії в операційній системі Kali Linux для проведення тестування безпеки своєї мережі, а також будуть надані рекомендації для забезпечення безпеки своєї мережі Wi-Fi.

Разом із тим, в цих роботах не в повній мірі відображені питання реалізації атак на бездротову мережу. Тому проведення натурного моделювання атак на бездротові мережі та розробка рекомендацій щодо захисту бездротових мереж є актуальним науковим завданням.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Оскільки використання бездротових мереж стрімко зростає, а безпека бездротових мереж - актуальна проблема в усьому світі, особливо в останні роки, важливо провести дослідження безпеки Wi-Fi мереж.

Для збору і аналізу інформації щодо протоколів захисту і методів шифрування, що використовуються в Wi-Fi мережах міста, використано техніку «War Driving» [12]. «War Driving» представляє собою спосіб пошуку/виявлення бездротових мереж під час руху по вулицях міста, що дозволяє пасивно збирати дані, які стосуються точок доступу Wi-Fi.

Під час емпіричного дослідження проведено збір даних на головній вулиці міста. Його довжина становить 11 км, він пролягає вздовж чотирьох міських районів де розташовані адміністративні, офісні будівлі великих компаній, кафе і ресторани, громадські місця, майданчики для відпочинку і багато ін.

Для пошуку і аналізу Wi-Fi точок доступу використано:

- пристрій для визначення координат GPS GlobalSat BU-353s4;
- дводіапазонній Wi-Fi адаптер Alfa AWUS036ACH;
- ноутбук, ОС Linux і утиліту airodump-ng з пакету програм aircrack-ng.

На рис.1 представлено обладнання, яке використано для аналізу захищеності Wi - Fi мереж.

Рис. 1. Обладнання для аналізу захищеності Wi-Fi мереж

Ноутбук, GPS-приймач і мережеві адаптер були розташовані в автомобілі, який рухався по міському району зі швидкістю 10-20 км/год. ОС Linux запускалася в режимі

реального часу на ноутбуці. Бездротовий інтерфейс мережного адаптера був переведений в режим моніторингу, щоб він міг прослуховувати бездротові пакети за допомогою інструменту airmon-ng. GPS-приймач використовувався для визначення географічного розташування точок доступу. Отримані при проході маршруту дані вносилися в таблицю за допомогою програми airodump-ng. Автоматично були визначені наступні параметри точок доступу:

- ідентифікатор SSID;
- тип шифрування, що використовується точками доступу;
- виробник точок доступу;
- спосіб авторизації;
- канал, на якому працює пристрій (пошук здійснюється в двох частотних діапазонах: 2,4 ГГц і 5ГГц).
- координати точки доступу;
- час і дата.

Для більш наочного розташування точок доступу була використана програма Google Earth, на карті якої позначені всі виявлені Wi-Fi мережі, рис. 2. Захоплені пакети були перетворені в базу даних за допомогою інструменту Giskismet Kali Linux та в Giskismet в файл Keyhole Markup Language (KML), щоб її можна було переглядати в Google Earth.

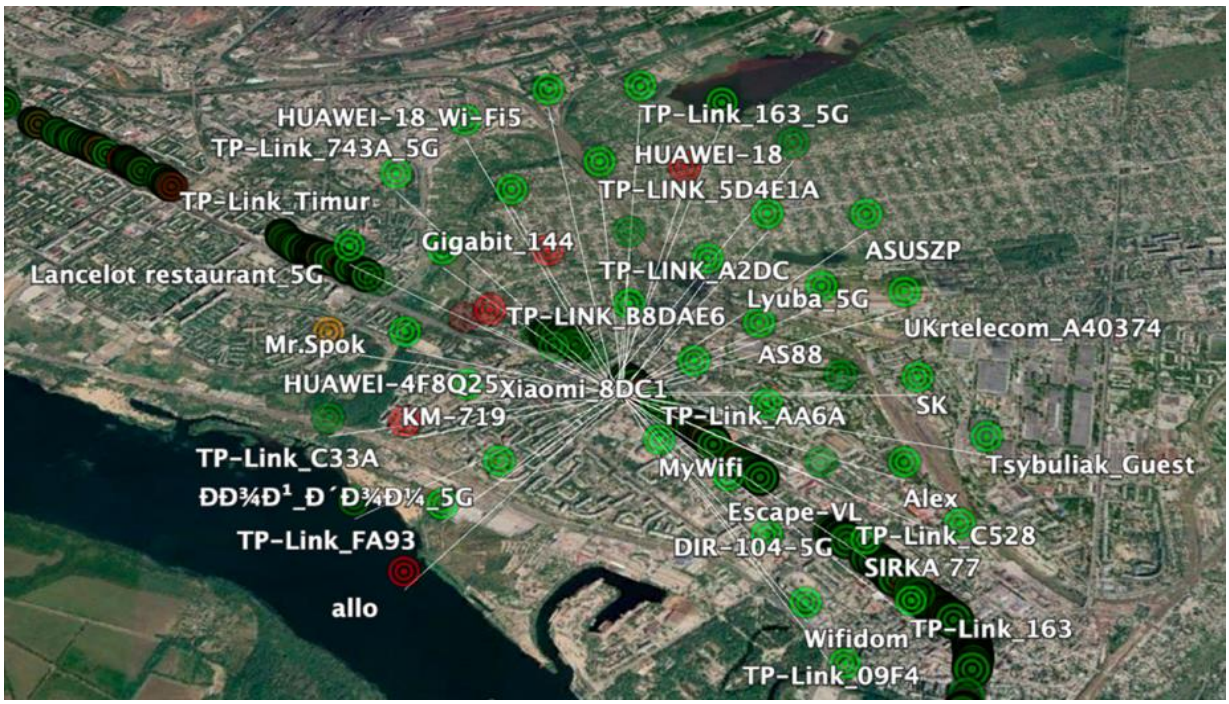

Рис. 2. Розташування точок доступу Wi-Fi на мапі Google Earth

Під час сканування зібрано дані по 2132 точкам доступу бездротових мереж Wi-Fi і зроблено статистичний звіт, який не є репрезентативним, але ілюструє розподіл різних типів шифрування, які застосовуються адміністраторами мереж і налаштовані у відповідних точках доступу мереж Wi-Fi.

На рис. 3, показано кількість відкритих мереж і мереж з обмеженням доступу.

ISSN 2663 - 4023

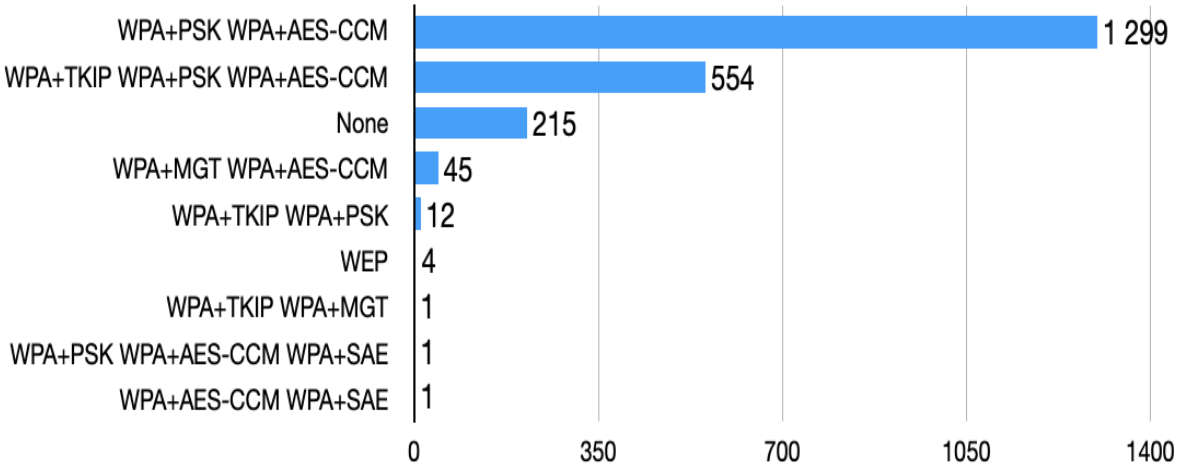

Рис. 3. Розподіл Wi-Fi мереж за методами шифрування

Статистичні дані показують, що 10,1% мереж не використовують ніякого шифрування. Ці мережі відкриті або тому, що адміністратори, які їх конфігурують, не інформовані про безпеку, або тому, що ці точки доступу навмисно залишають відкритими, наприклад в громадських місцях, щоб клієнти або відвідувачі могли підключитися до Інтернету. З іншого боку, більшість точок доступу використовують шифрування. Як випливає з рисунка 3, більшість мереж в даний час (61%) захищені WPA2, а це означає, що вразливість в WPA2 може привести до великої кількості потенційних цілей, ніж при використанні протоколу WPA3. Поодинокі використання WPA3 свідчить про те, що новий стандарт безпеки WPA3, який спрямовано на усунення вразливостей старих стандартів безпеки та забезпечення високого рівня безпеки, в даний час знаходиться в стадії поступового/початкового впровадження.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведений аналіз показав, що існують відкриті бездротові мережі. Бездротові мережі відкриті або тому, що адміністратори, які їх конфігурують, не інформовані про безпеку, або тому, що ці точки доступу навмисно залишають відкритими, наприклад в громадських місцях, щоб клієнти або відвідувачі могли підключитися до Інтернету. Данні отриманні натурним моделюванням свідчать, що 10,1% мереж не використовують ніякого шифрування. Існуючи статистичні данні, наведені відомими зарубіжними фірмами свідчать про 9 - 11% не використовують ніякого шифрування. Тобто похибка складає від 8% до 12%. Це е дуже гарним результатом та підтверджує адекватність проведеного натурного моделювання. Виходячи з аналізу результатів натурного моделювання, з метою захисту бездротової мережи від атаки типу «War Driving» потрібно зробити наступне:

• Увімкнути шифрування: виберіть найвищий протокол мережі безпеки, вибираючи WEP, WPA і WPA2, і ніколи не залишайте свою мережу відкритою або без протоколу безпеки.

• Оновити пароль: змініть пароль, налаштований за замовчуванням на маршрутизаторі, і використовуйте багатофакторну автентифікацію, якщо вона доступна.

• Додати гостьову мережу: налагодить гостьову Wi-Fi мережу для гостей та інших розумних пристроїв, які підключаються до Інтернету, щоб обмежити доступ цих менш захищених пристроїв.

• Використовуйте брандмауер: брандмауери блокують несанкціоновані з'єднання та спроби доступу до вашої системи.

• Оновити ваші пристрої: завжди встановлюйте оновлення, щоб використовувати найсвіжіші патчі та підтримувати максимально високий рівень безпеки вашого апаратного та програмного забезпечення.

Таким чином проведене натурне моделювання дозволило зробити рекомендації що до захисту бездротової мережі.

Напрямки подальших досліджень: аналіз та удасканаленя методу захисту бездротових мереж від нових типів атак (котрі постійно зявляються та модернізуються) на особисті данні коростувачих у загально доступних бездротових мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Закон України "Про інформацію". https://zakon.rada.gov.ua/laws/show/2657-12#Text..

2 Корольков, Р.Ю. (2021). Сценарій атаки з використанням несанкціонованої точки доступу у мережах IEEE 802.11. *Кібербезпека: освіта, наука, техніка, 3*(11), 144-154.

3 Собчук, В.В., Савченко, В.А., Лаптєв, О.А. (2019). Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, *66*, 124 – 132.

4 Лаптєв, О.А. (2019). Експериментально-статистичний метод обчислення кореляційної взаємозалежності параметрів розпізнавання засобів негласного отримання інформації. *Сучасний захист інформації: науково-технічний журнал, 3*(39), 23 – 29.

5 Корольков, Р.Ю., Куцак, С.В. (2019). Особливості реалізація атаки деавтентифікації в мережах стандарту 802.11. *Захист інформації, 21*(3), 175-181.

6 Korolkov, R.Yu., Kutsak, S.V. (2021). Analysis of attacks in IEEE 802.11 networks at different levels of OSI model. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 2*, 163-169.

7 Korolkov, R.Yu., Kutsak, S.V. (2021). Received-signal-strength-based approach for detection and 2D indoor localization of evil twin rogue access point in 802.11. *International Journal of Safety and Security Engineering, 11*(1), 13-20.

8 Korolkov, R.Yu., Kutsak, S.V., Voskoboinyk, V. (2021). Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection. *Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 50*, 59-71.

9 Schepers, D., Vanhoef, M., Ranganathan, A. (2021). A framework to test and fuzz wi-fi devices. У *WiSec '21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM. https://doi.org/10.1145/3448300.3468261.

10 Noman, H.A., Abdullah, S.M., Mohammed, H.I. (2015). An automated approach to detect deauthentication and disassociation DOS attacks on wireless 802.11 networks. *International Journal of Computer Science Issues (IJCSI), 12*(4), 107-112.

11 Хорошко, В.О. Хохлачова, Ю.Є. (2012). Оцінка захищеності інформаційних систем. *Сучасний захист інформації, 4*, 50 – 57.

12 Мусієнко, А.П., Барабаш, О.В., Лукова-Чуйко, Н.В., Собчук, В.В. (2018). Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам. *Сучасні інформаційні системи. Харків: НТУ «ХПІ», 2*(1), 56 – 64.

13 Лукова-Чуйко, Н. (2015). Моделювання оптимальних систем захисту інформації. У *Науково-технічна конференція «Інформаційна безпека держави»* (с. 119–120). КНУ імені Тараса Шевченка.

14 Sundararajan, A., Chavan, A., Saleem, D., Sarwat, A. (2018). A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. *Energies, 11*(9), 2360

15 Zou, Y., Zhu, J., Wang, X., Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE, 104*(9), 1727-1765.

16 Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Qbea'H, M., Alrabaee, S. (2020). Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux. In *2020 12th Annual Undergraduate Research Conference on Applied Computing* (URC) (p. 1-4)

17 Хорошко, В., Хохлачова, Ю. (2016). Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. У *Частина 1: Безпека інформації* (Т. 22). https://doi.org/10.18372/2225-5036.22.11104

18 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security*,*13*(1), 15-21.

19 Лаптев, О.А., Собчук, В.В., Саланди, И.П., Сачук, Ю.В. (2019). Математична модель структури інформаційної сеті на основі нестационарної ієрархічної та стаціонарної гиперсети. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, *64*, 124 – 132.

20 Laptev, A., Sobchuk, V., Barabash, O., Musienko, A. (2019). Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise. *Sciences of Europe*, *1*(42), 41 – 44.

21 Yevseiev, S., Laptiev, O., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky, R. (2021). Analysis of information security threat assessment of the objects of information activity. *International independent scientific journal*, *1*(34), 33 – 39.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Roman Yuriyovych Korolkov
Department of Information Protection, Zaporizhia Polytechnic National University
Zaporizhzhia, Ukraine
ORCID ID: 0000-0001-5501-4600
romankor@zntu.edu.ua

Serhii Laptiev
PhD-student
Taras Shevchenko National University of Kyiv
Faculty of information tehnology
Department of Cyber Security and Information Protection
ORCID ID: 0000-0002-7291-1829
salaptiev@gmail.com

REAL SIMULATION OF A "WAR DRIVING" ATTACK ON A WIRELESS NETWORK

Abstract. The inevitable spread of wireless networks and the growing traffic in them can lead to an increase in information security incidents. The main threats are aimed at interception, violation of the confidentiality and integrity of transmitted data, attacks on the availability of nodes of the transmission channel and their substitution. Due to its characteristics, the wireless data transmission environment creates potential conditions for eavesdropping on network traffic and uncontrolled connection to the wireless network by attackers who are in its range. Wireless networks, unlike wired networks, are extremely vulnerable to possible attacks and unauthorized access due to the use of radio spectrum and the broadcast nature of the physical layer. To intercept data, it is enough to be in the range of the Wi-Fi network. Therefore, an attacker, being at a safe distance, can use wireless devices to carry out attacks. The article analyzes a cyberattack of the "War Driving" type on wireless networks. The analysis carried out in the article showed that there are open wireless networks. Wireless networks are open or because the administrators who configure them are not security aware. A full-scale simulation of a "War Driving" attack was carried out. Real-time simulation data show that 10.1% of networks do not use any encryption. The detection error of access points not using encryption is from 8% to 12%. This is a very good result and confirms the adequacy of the conducted full-scale modeling. Based on the analysis of the results of live simulation, recommendations have been developed to protect the wireless network from a "War Driving" attack. The developed recommendations will protect wireless networks from "War Driving" attacks.

Keywords: attack, threat, wireless networks, simulation, access point.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Zakon Ukrainy "Pro informatsiiu". https://zakon.rada.gov.ua/laws/show/2657-12#Text..
2 Korolkov, R.Iu. (2021). Stsenarii ataky z vykorystanniam nesanktsionovanoi tochky dostupu u merezhakh IEEE 802.11. Kiberbezpeka: osvita, nauka, tekhnika, 3(11), 144-154.
3 Sobchuk, V.V., Savchenko, V.A., Laptiev, O.A. (2019). Metod pidvyshchennia zavadostiikosti systemy vyiavlennia, rozpiznavannia i lokalizatsii tsyfrovykh syhnaliv v informatsiinykh systemakh. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, 66, 124 – 132.
4 Laptiev, O.A. (2019). Eksperymentalno-statystychnyi metod obchyslennia koreliatsiinoi vzaiemozalezhnosti parametriv rozpiznavannia zasobiv nehlasnoho otrymannia informatsii. Suchasnyi zakhyst informatsii: naukovo-tekhnichnyi zhurnal, 3(39), 23 – 29.
5 Korolkov, R.Iu., Kutsak, S.V. (2019). Osoblyvosti realizatsiia ataky deavtentyfikatsii v merezhakh standartu 802.11. Zakhyst informatsii, 21(3), 175-181.
6 Korolkov, R.Yu., Kutsak, S.V. (2021). Analysis of attacks in IEEE 802.11 networks at different levels of OSI model. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 2, 163-169.
7 Korolkov, R.Yu., Kutsak, S.V. (2021). Received-signal-strength-based approach for detection and 2D indoor localization of evil twin rogue access point in 802.11. International Journal of Safety and Security Engineering, 11(1), 13-20.
8 Korolkov, R.Yu., Kutsak, S.V., Voskoboinyk, V. (2021). Analysis of deauthentication attack in IEEE

802.11 networks and a proposal for its detection. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 50, 59-71.

9 Schepers, D., Vanhoef, M., Ranganathan, A. (2021). A framework to test and fuzz wi-fi devices. U WiSec '21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM. https://doi.org/10.1145/3448300.3468261.

10 Noman, H.A., Abdullah, S.M., Mohammed, H.I. (2015). An automated approach to detect deauthentication and disassociation DOS attacks on wireless 802.11 networks. International Journal of Computer Science Issues (IJCSI), 12(4), 107-112.

11 Khoroshko, V.O. Khokhlachova, Yu.Ie. (2012). Otsinka zakhyshchenosti informatsiinykh system. Suchasnyi zakhyst informatsii, 4, 50 – 57.

12 Musiienko, A.P., Barabash, O.V., Lukova-Chuiko, N.V., Sobchuk, V.V. (2018). Zabezpechennia funktsionalnoi stiikosti informatsiinykh merezh na osnovi rozrobky metodu protydii DDoS-atakam. Suchasni informatsiini systemy. Kharkiv: NTU «KhPI», 2(1), 56 – 64.

13 Lukova-Chuiko, N. (2015). Modeliuvannia optymalnykh system zakhystu informatsii. U Naukovo-tekhnichna konferentsiia «Informatsiina bezpeka derzhavy» (s. 119–120). KNU imeni Tarasa Shevchenka.

14 Sundararajan, A., Chavan, A., Saleem, D., Sarwat, A. (2018). A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. Energies, 11(9), 2360

15 Zou, Y., Zhu, J., Wang, X., Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE, 104(9), 1727-1765.

16 Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Qbea'H, M., Alrabaee, S. (2020). Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux. In 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC) (p. 1-4)

17 Khoroshko, V., Khokhlachova, Yu. (2016). Informatsiina viina. ZMI yak instrument informatsiinoho vplyvu na suspilstvo. U Chastyna 1: Bezpeka informatsii (T. 22). https://doi.org/10.18372/2225-5036.22.11104

18 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security,13(1), 15-21.

19 Laptev, O.A., Sobchuk, V.V., Salandy, Y.P., Sachuk, Yu.V. (2019). Matematychna model struktury informatsiinoi seti na osnovi nestatsyonarnoi ierarkhichnoi ta statsionarnoi hypersety. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, 64, 124 – 132.

20 Laptev, A., Sobchuk, V., Barabash, O., Musienko, A. (2019). Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise. Sciences of Europe, 1(42), 41 – 44.

21 Yevseiev, S., Laptiev, O., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky, R. (2021). Analysis of information security threat assessment of the objects of information activity. International independent scientific journal, 1(34), 33 – 39.