УДК 004.056
DOI: 10.31673/2409-7292.2022.040004

Лавровський І.М., Дунаєв Я.С., Коліда В.П.

ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ В ДОМАШНІЙ WI-FI МЕРЕЖІ ЗА ДОПОМОГОЮ УТИЛІТ WAIDPS І NZYME

У статті досліджено утиліти Waidps і Nzyme, що використовуються для моніторингу безпроводових мереж. Було описано деякі основні терміни мережі WLAN з можливими атаками на WLAN в цілому і описано, наскільки вони небезпечні. Досліджено, як працює кожна з утиліт: її можливості, недоліки та порядок застосування.

Ключові слова: WLAN, Wi-Fi, Waidps, Nzyme, аномалія трафіку, атака, захист.

Технологія безпроводової локальної мережі швидко стала дуже популярною у всьому світі. Завдяки випуску стандарту безпроводової локальної мережі IEEE 802.11, безпроводова технологія перетворилася на відкрите рішення для забезпечення мобільності та мережевих послуг без вимоги провідного з'єднання.

Актуальність забезпечення безпеки безпроводової мережі обумовлена тим, що в провідних мережах зловмисник повинен спочатку отримати фізичний доступ до кабельної системі або кінцевим пристроям, а в безпроводових мережах для отримання доступу достатньо звичайного приймача, встановленого в радіусі дії мережі. Незважаючи на відмінності в реалізації зв'язку, підхід до безпеки безпроводових мереж і їх дротових аналогів ідентичний. Але при реалізації методів захисту інформації в безпроводових мережах більше уваги приділяється вимогам до забезпечення конфіденційності і цілісності переданих даних, до перевірки автентичності безпроводових клієнтів і точок доступу.

Протокол безпроводової локальної мережі (WLAN), IEEE 802.11 і пов'язані з ним технології дозволяють забезпечити безпечний доступ до мережевої інфраструктури. До розвитку WLAN мережевий клієнт повинен був фізично підключений до мережі, використовуючи певний вид проводки. Завдяки швидкому збільшенню використання технології WLAN важливо забезпечити безпечний зв'язок через безпроводову мережу. З моменту свого створення безпека безпроводових мереж проходила через різні стадії розробки, від фільтрації MAC-адрес або WEP до WPA / WPA2.

Безпроводова технологія виявилася дуже практичною (не тільки) для домашніх користувачів: така можливість зручно підключатися до Інтернету на мобільному пристрої, не потребуючи проводів, все ще набирає популярність. Це призвело до спроби зробити конфігурацію WLAN простішим для звичайного користувача без будь-яких знань про комп'ютерні науки. Результатом цього стало стандартне Wifi Protected Setup (WPS).

Метою даної статті є дослідження технологій та засобів виявлення атак в безпроводових мережах на основі застосування утиліт Waidps і Nzyme.

Сутність WLAN

Безпроводова мережа – це мережа пристроїв, таких як комп'ютери, принтери, мобільні пристрої, які можуть спілкуватися та обмінюватися інформацією один з одним через безпроводове підключення до Інтернету, більш відоме як "wi-fi". Це можливо за допомогою пристроїв з точками доступу (для маршрутизаторів Wi-Fi), безпроводової карти (для ПК), PCMCIA (для ноутбуків без вбудованих компонентів wifi доступу). Мережі 802.11 складаються з чотирьох основних компонентів:

– Система розподілу - логічний компонент, який використовується для пересилання кадрів до місця призначення.

– Точки доступу (AP) - пристрої, що виконують функцію мостового з'єднання безпроводового зв'язку.

– Станції (STAs) - пристрій з безпроводовим мережним інтерфейсом, що зв'язується з іншими подібними пристроями через точки доступу.

– Безпроводовий носій - носій, який використовується для передачі кадрів від станції до станції. Два радіочастотні і один інфрачервоний фізичні рівні були стандартизовані.

Атаки на WLAN

Існує багато загроз і атак, які можуть пошкодити безпеку безпроводових локальних мереж. Ці атаки можна класифікувати в двох категоріях: 1) Логічні атаки; 2) Фізичні атаки.

Логічні атаки

Логічна атака завжди пов'язана з програмним забезпеченням, системою та конфіденційними даними, що надходять у мережу. Головною метою цих атак є пошук і зловживання конфіденційними даними, що надходять у мережу. Деякі з найбільш поширених логічних атак визначені нижче [3]:

– Brute Force Attacks проти паролів точок доступу
– Напади на шифрування
– Підробка MAC-адресу
– Man in the Middle Attack
– Розвідувальні атаки
– Динамічна атака протоколу конфігурації хоста

Brute Force Attacks проти паролів точок доступу. Більшість безпроводових локальних мереж використовують попередньо розділений ключ або пароль, який використовуються усіма підключеними STA. Штурмовик словника намагається відновити цей ключ, поступово перевіряючи кожен з можливих паролів. Після успішного відновлення ключа зловмисник отримує доступ до мережі.

Напади на шифрування. Зловмисник може використовувати відому слабкість у способі шифрування даних у зв'язку між STA і AP, щоб відновити різні дані або мережевий пароль.

Підробка MAC-адресу. Підробка MAC-адресу є шкідливою технікою, яка використовується для отримання доступу до безпроводових мереж, захищених методом фільтрації MAC-адресів. Оскільки MAC-адреси передаються незашифрованими в заголовках 802.11, зловмисник може отримати MAC-адресу авторизованої станції, пасивно слухаючи комунікацію WLAN. Якщо одного разу MAC-адреса була отримана, зловмисник може легко використовувати її для отримання доступу до мережі.

Man in the Middle Attack. Атаки «людина в середині» - це атака, в якій зловмисник може читати, змінювати і вводити повідомлення між двома сторонами, тоді як жоден з них не знає, що повідомлення було атаковано. Використання таких методів, як IEEE802.1x для досягнення взаємної аутентифікації між AP та STA, а також прийняття інтелектуальної безпроводової системи виявлення вторгнень може допомогти у попередженні таких атак. Застосування WEP або WPA через безпроводову мережу також є спільним рішенням цієї проблеми [4].

Розвідувальні атаки. Атаки розвідки використовуються для збору інформації про цільову мережу або систему. Хоча така атака може виглядати в основному нешкідливою і часто пропускається з уваги, зазвичай інформація, отримана в результаті розвідки, використовується в наступних атаках Access або DoS.

Динамічна атака протоколу конфігурації хоста. Атака DHCP працює шляхом передачі DHCP-запитів з підробленими MAC-адресами. Якщо відправлено достатньо запитів, адресний простір, доступний серверам DHCP, може бути вичерпаний протягом певного часу. Згодом, законному користувачеві відмовляється від IP-адреси, запитаної через DHCP, що призводить до дисфункціональної мережі.

DHCP зазвичай є відмовою від обслуговування (DoS). Крім того, він може використовуватися разом з атакою зловмисного сервера, щоб перенаправляти трафік на зловмисний комп'ютер, готовий до перехоплення трафіку [5].

Фізичні атаки

Rogue Access Points. Точки доступу Rogue - це точки доступу WLAN, які не мають дозволу на підключення до цільової мережі. Rogue AP відкривають безпроводові отвори в мережі. Зловмисник може впровадити шахрайську AP, або працівник може невідомо для всіх створити дірку у безпеці, підключивши в мережу незахищену точку доступу [6]. Будь-який

АР може використовуватися будь-ким, хто може підключитися до АР, включаючи зловмисника, надаючи їм доступ до дротової мережі

Фізичне розміщення АР. Місце інсталяції точок доступу - це ще одна проблема безпеки, тому що розміщення АР неналежним чином піддасть його фізичним атакам. Якщо зловмисник може фізично отримати доступ до АР, то він може перемикати АР до своїх налаштувань за замовчуванням, які (в більшості випадків) небезпечні. Тому дуже важливо, щоб адміністратори мережної безпеки ретельно вибирали місця для розміщення точок доступу.

Jamming attacks. Jamming attacks виконується шляхом передачі сигналу на приймальну антену в тій же смузі частот або піддіапазоні, яку передає передавач зв'язку. Зловмисник з правильними інструментами та знаннями може легко заклинювати частоту 2,4 ГГц таким чином, щоб сигнал перейшов до рівня, коли безпроводова мережа більше не може функціонувати

Засоби виявлення атак в безпроводових мережах

Для виявлення атак і аномалій безпроводового ефіру можна використовувати високотехнологічні рішення (як правило дорогі), які дозволяють контролювати безпроводові мережі і виявляти спроби атак. Я розповім про дві безкоштовні утиліти, які дозволять вам контролювати безпроводовий ефір і оперативно реагувати на вторгнення зловмисників.

З точки зору забезпечення безпеки відстеження безпроводових пристроїв дозволяє негайно інформувати про те, в яку точку необхідно направити співробітників відділу безпеки. Існує маса загроз безпеки мережі, які не виявляються традиційними системами IDS / IPS, оскільки їх можна виявити тільки на радіочастотному рівні. У число таких загроз входять безпроводові мости, що функціонують відповідно до пропрієтарних протоколів, і пристроїв, що функціонують відповідно до більш ранніх стандартів, наприклад, 802.11FH, які можуть стати точкою вторгнення в мережу [7].

До цих загроз також відносяться WiFi-пристрої зловмисників, які працюють на нестандартних робочих частотах або використовують нестандартну модуляцію. І крім того, завжди існують атаки типу «відмова в обслуговуванні», які можуть виходити від пристроїв придушення безпроводової мережі. Для виявлення атак і аномалій безпроводового ефіру можна використовувати високотехнологічні рішення (як правило дорогі), які дозволяють контролювати безпроводові мережі і виявляти спроби атак. До таких рішень можна віднести Cisco CleanAir. Ми ж будемо використовувати два безкоштовних рішення - Waidps і Nzyme (рис. 1, 2) [8].

Важливе зауваження: для роботи утиліт необхідно щоб ваш Wi-Fi адаптер міг працювати в режимі монітора.

Waidps. Для виявлення аномалій безпроводового ефіру в "домашніх" умовах можна використовувати утиліту Waidps. Це багатоцільовий інструмент, створений для аудиту (тестування на проникнення) мереж, виявлення безпроводового вторгнення (атаки WEP / WPA / WPS) а також запобігання вторгнення (зупинка зв'язку станції з точкою доступу). Крім цього, програма буде збирати всю WiFi інформацію в окрузі і зберігати в базах даних.

Waidps здатна виявляти масові деаутентіфікаціі, які можуть сигналізувати про можливу атаку на WPA (для перехоплення хендшейка), виявляти атаки з використанням ARP запитів, за допомогою Rogue AP і Evil_Twin, можливих атак перебором WPS-Піна та багато іншого.

Утиліта сама піднімає необхідні їй інтерфейси і почитає моніторити ефір. Цікавою особливістю є, що утиліту можна використовувати не тільки для виявлення атаки, але й для проведення аудиту АР який нас цікавить.

Для роботи утиліти необхідно додатково встановити пакет Aircrack-ng і Wireshark. Утиліта моніторить безпроводовий ефір і сигналізує про аномалії - поширені атаки на безпроводову мережу, а також про появу підроблених точок доступу - RogueAP. За допомогою декількох точок Waidps можна налаштувати моніторинг периметра, вивіривши рівень сигналу до кожної станції (фізичним розташування) - для того щоб виявляти

приблизне місце дислокації порушника. Оптимальний варіант - запустити утиліту на кілька годин щоб зняти «чисту» картину ефіру для порівняння.

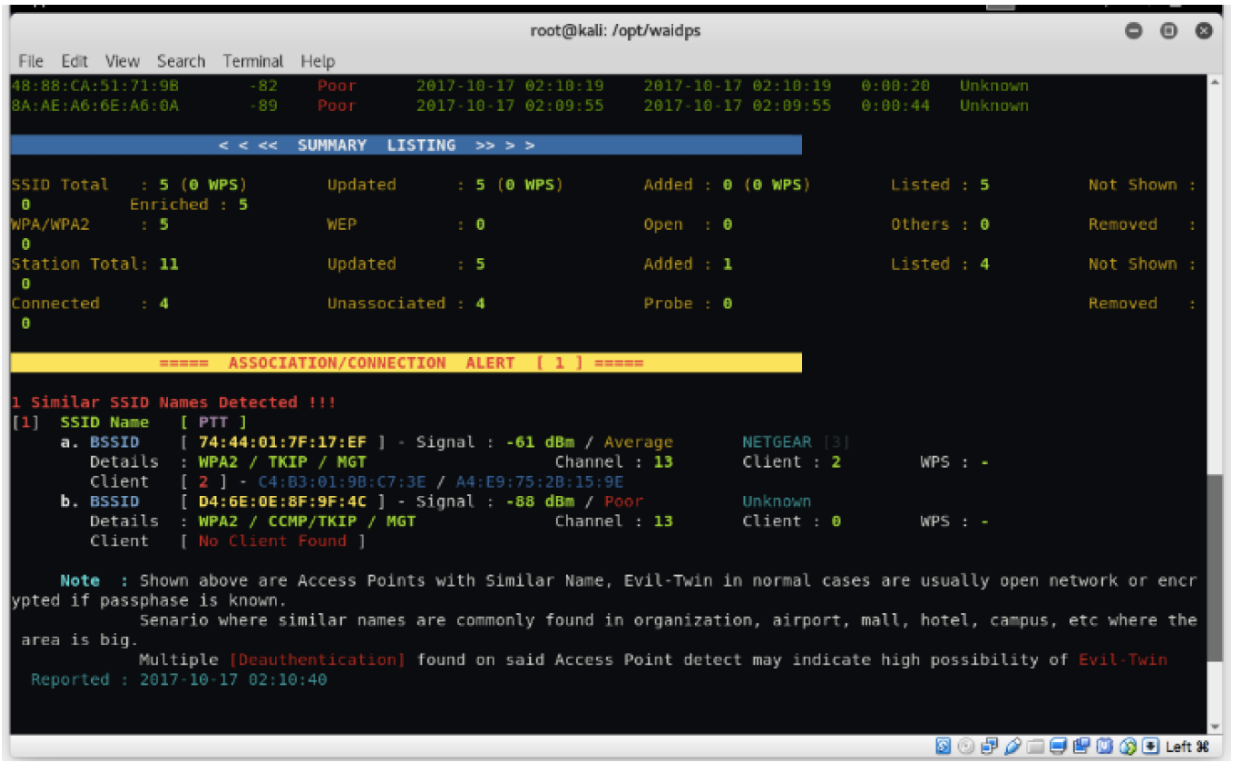

Рис. 1. Робота Waidps

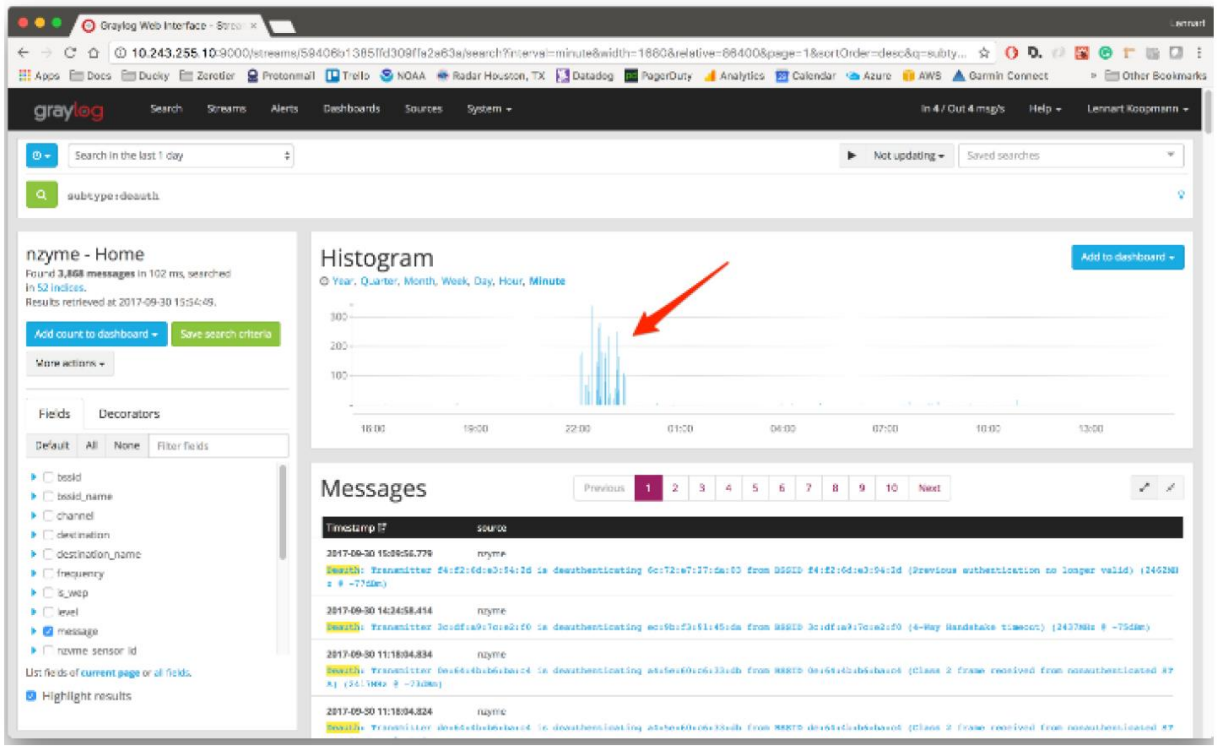

Рис. 2. Інтерфейс Nzyme

Nzyme. Nzyme збирає фрейми 802.11 безпосередньо з ефіру і відправляє їх у систему управління журналом Graylog (з відкритим вихідним кодом), що дозволяє використовувати її в якості IDS WiFi, моніторингу та реагування на інциденти. Для цього потрібно тільки JVM і

WiFi-адаптер, що підтримує режим моніторингу. Відмінною особливістю даного інструменту є початкова «заточенність» на запуск на слабкому обладнанні, наприклад на Raspberry Pi. Також є можливість запуску Nzyme «з коробки» на MacBook.

Для початку необхідно конфігурувати систему для роботи, встановивши deb пакет або скориставшись jar файлом. Також необхідно налаштувати конфіг файл для з'єднання з Graylog (рис. 3):

```
nzyme_id = nzyme
channels = en0:1,2,3,4,5,6,8,9,10,11
channel_hop_command = sudo
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
{interface} channel {channel}
channel_hop_interval = 1
graylog_addresses = %graylog IP%:12000
beacon_frame_sampling_rate = 0
```

Рис. 3. Конфіг для налаштування

Для відображення використовується Graylog (можна використовувати у вигляді віртуальної машини), що дозволяє виводити інформацію в інтерфейсі (рис. 4).

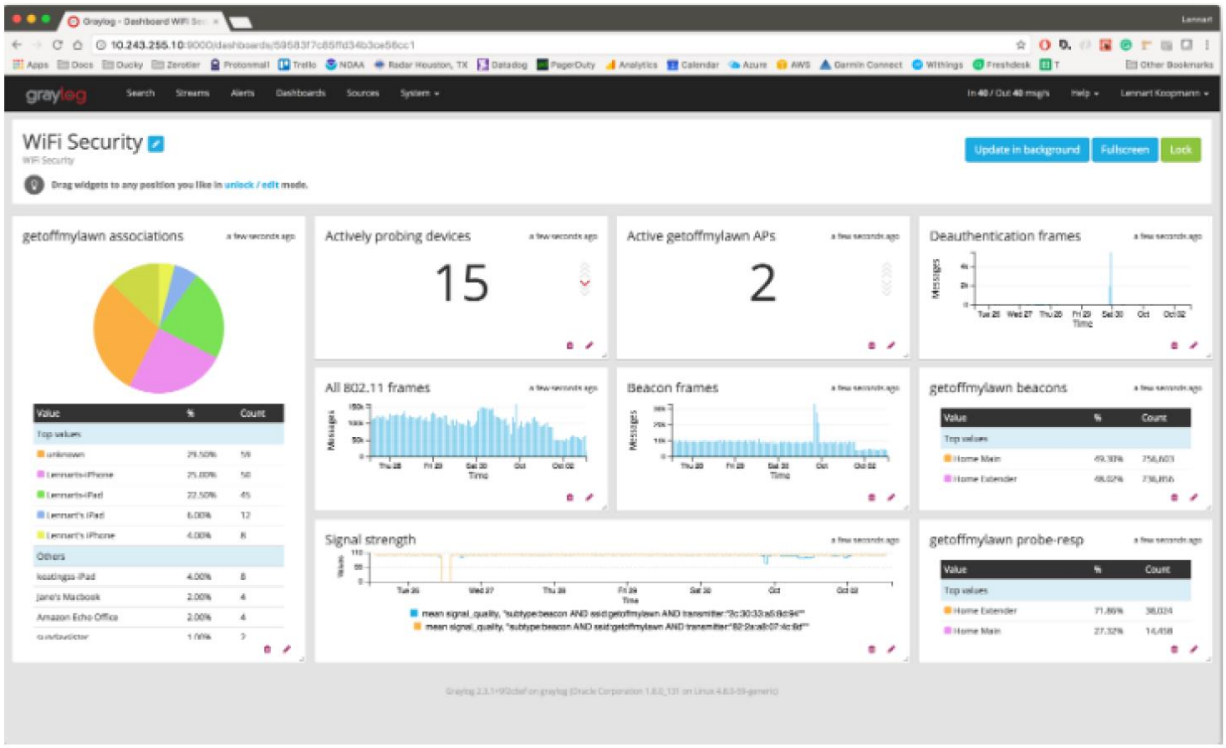

Рис. 4. Інтерфейс Graylog

Ці утиліти ні в якій мірі не замінять «професійних» рішень по захисту безпроводового ефіру, але тим не менш зможуть дати інформацію про його «чистоту».

Сучасне обладнання дозволяє проводити постійне активне прослуховування по всіх каналах, здійснювати перевірку нових точок за різними критеріями, дозволяє швидко виявляти точки зловмисників. Після виявлення генеруються відповідні повідомлення. Технологія Management Frame Protection (MFP) нейтралізує атаки типу Evil Twin, так як при її використанні в кожен безпроводовий фрейм вставляється спеціальний підпис, і клієнт з підтримкою цієї фічі просто не стане аунтефікуватися на точці доступу зловмисника [10].

Крім того, можна включити активний режим стримування (Active Rogue Containment) і тоді при виявленні точки зловмисника на неї будуть масово відправлятися пакети de-authentication, що не дозволить до неї нікому підключитися.

Для виявлення нових точок підключених безпосередньо в локальну мережу підприємства, необхідно використовувати технологію Switchport Tracing, в результаті роботи якої можна знайти і заблокувати порт на комутаторі і точка зловмисника втрачає доступ в локальну мережу.

Також, крім вбудованого базового IDS існують так же і адаптивні wIPS. wIPS вміють виявляти в тому числі і використання інструментів (Karma, Aircrack), сплески трафіку в неробочий час, DHCP сервери атакуючих, підбір ключів WEP і т.д. [11].

Висновки

Технологія WLAN швидко розвивається, з все більшою кількістю нових характеристик та конфігурацій для підтримки більшої пропускної здатності, легшої установки і задоволенням технологічних та економічних вимог. Крім того, Wi-Fi тепер також допомагає користувачам отримувати доступ з майже всіх громадських приміщень, таких як бібліотеки, парки, аеропорти, тощо.

Що стосується WLAN, важливо зосередитися на його безпеці, оскільки WLAN може бути легкою здобиччю для хакерів / кіберзлочинців, для викрадання цінної інформації. Таким чином, поряд із швидким розвитком функцій WLAN, захист від небезпечних загроз також важливий. Це підвищує продуктивність праці та створює довіру у користувачів. Створення мережі з ідеальним рішенням безпеки дуже важко. Залежно від того яка саме мережа: домашня, шкільна, публічна або корпоративна, існують різні заходи безпеки, які підходять для кожного відповідного сценарію.

Практичне значення результатів дослідження полягає в тому, що отримані в статті результати можуть бути використані на етапі проектування захищеної безпроводової мережі.

Перелік посилань

1. Андрєєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки; за ред. В.О. Хорошка. – [2-е вид.]. – К.: Вид. ДУІКТ, 2009. – 292 с.

2. Glore, N. & Mishra, A., Chapter 11 «Privacy and Security in WiMAX Networks» in «WiMAX Standards and Security» (Edited by M. Ilyas & S. Ahson) – Boca Raton, Florida: CRC Press, 2008. ISBN 978-1-4200-4523-9

3. M. Gast, 802.11 Wireless networks: The definitive guide. O'Reilly & Associates, Inc., Sebastopol, 2002.

4. "What is 802.11 wireless?." http://technet.microsoft.com/en-us/library/ cc785885(v=ws.10).aspx.

5. "DHCP starvation attack." http://www.networkdictionary.com/networking/DHCPStarvationAttack.php.

6. S. DeFino, B. Kaufman, N. Valenteen, and L. Greenblatt, Official Certified Ethical Hacker Review Guide. Cengage Learning, 2009.

Надійшла: 06.11.2022 Рецензент: д.т.н., професор Кожухівський А.Д.