УДК 004.056
DOI 10.17721/ISTS.2023.1.21-27

Наталія Лукова-Чуйко, orcid.org/0000-0003-3224-4061,
lukova@ukr.net
Тетяна Лаптєва, orcid.org/0000-0002-7291-1829,
tetiana1986@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ НЕЛЕГАЛЬНИХ ТОЧОК ДОСТУПУ ДО БЕЗДРОТОВОЇ МЕРЕЖІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Широке використання мобільних пристроїв привело до збільшення підключень до інтернету і розгортання нових бездротових локальних мереж. Згідно з останніми дослідженнями компанії Cisco, до кінця 2023 р. в усьому світі користувачами інтернету стануть 66 % населення Землі. До глобальної мережі будуть підключені більше 28 млрд пристроїв. В останні два десятиліття ми стали свідками народження і розвитку технології, яка істотно змінила нашу роботу і життя, – IEEE 802.11, також відому як Wi-Fi. Технологія Wi-Fi є улюбленим способом підключення до інтернету через простоту використання і гнучкість. Для підключення до бездротової мережі лише необхідно перебувати в радіусі її дії. Тобто споживачі і бізнес будуть усе більше покладатися на мобільні мережі. Однак слід зазначити, що кожна нова можливість цифровізації також дає нові можливості кіберзлочинцям і тому проблема безпеки бездротових мереж нині є однією з головних проблем IT-технологій. Неминуче поширення бездротових мереж і зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки. Основні загрози спрямовані на перехоплення, порушення конфіденційності і цілісності переданих даних, здійснення атак на доступність вузлів каналу передачі та їхню підміну. У статті проведено аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації. Удосконалено метод виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності. Проведено натурне моделювання виявлення несанкціонованого втручання в інформаційну бездротову мережу підприємства. Натурне моделювання підтвердило точність локалізації відкритої точки доступу до інформації у мережі Wi-Fi – до 2 м. Це дозволить своєчасно виявляти та локалізувати несанкціоновані точки доступу до інформації у бездротовій мережі підприємств та установ.

Ключові слова: *атака; радіосигнал; метод; загроза; витікання інформації.*

1. ВСТУП

Широке використання мобільних пристроїв привело до збільшення підключень до інтернету та розгортання нових і модернізації існуючих комп'ютерних мереж з акцентом на бездротові локальні мережі – WLAN (Wireless Local Area Network). Упровадження нових стандартів розширило зону покриття з меншими витратами, забезпечуючи водночас мобільність користувачів. Підключення до мережі Wi-Fi є улюбленим способом підключення до мережі інтернету. Для підключення до бездротової мережі лише необхідно перебувати в радіусі дії бездротової мережі.

З кожним днем кількість абонентів, які використовують пристрої з бездротовим виходом в інтернет, безперервно зростає. Згідно з останніми дослідженнями компанії Cisco, до кінця 2023 р. в усьому світі користувачами інтернету стануть 66 % населення Землі. До глобальної мережі будуть підключені більше 28 млрд пристроїв. Тобто споживачі й бізнес будуть все більше покладатися на мобільні мережі. Однак слід зазначити, що кожна нова можливість цифровізації також дає нові можливості кіберзлочинцям, і тому проблема безпеки бездротових мереж нині є однією з головних проблем IT-технологій. Серед усіх загроз безпеці бездротової мережі найсерйозніша – це шахрайські нелегальні точки доступу, які встановлюються зловмисником, без дозволу адміністратора бездро-

тової локальної мережі, з метою використовувати їх для конкурентної розвідки й атак. Загроза нелегальних точок доступу останнім часом стала важливою проблемою безпеки в бездротових локальних мережах.

Тому питання захисту інформаційних бездротових мереж, саме визначення сигналів несанкціонованих точок доступу, з метою виділення сигналів нелегальних точок доступу на фоні легальних радіосигналів бездротових мереж стає дуже гострим. А розроблення нових і вдосконалення існуючих методів виявлення нелегальних точок доступу у локальних бездротових мережах дуже актуальне.

2. МЕТА СТАТТІ

Метою роботи є аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації, а також удосконалення методу виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності.

3. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питанням захисту інформації, розроблення моделей виявлення каналів витікання інформації та засобів нелегального отримання інформації присвячено значну кількість публікацій. Так у роботі [1] розглянуто різні методи перехоплення інформації дешифрування й аналіз Wi-Fi-активності без будь-якого підключення до бездротової мережі. Хакери, намагаючись зламати захист на бездротових маршрутизаторах, можуть використовувати найрізноманітніші методи для отримання доступу до вашої конфіденційної інформації: від ресурсомістких атак грубої сили, що здійснюються за допомогою різних програм із підбору простих "словникових" паролів, до витончених схем соціальної інженерії, таких як фішинг Wi-Fi-паролів шляхом блокування з'єднання та створення підроблених точок доступу, проти яких безсилі навіть найнадійніші паролі. Як тільки облікові дані Wi-Fi будуть отримані, у зловмисників з'являються величезні можливості щодо прихованого захоплення й аналізу мережного трафіка скомпрометованої бездротової мережі. Але сам методологічний апарат не розкривається, методика наведена не в повному обсязі.

У роботах [2, 3] приділяється основна увага злому паролів бездротової мережі. Вразливі мережні пристрої та різноманітні помилки конфігурації роблять цей спосіб досить простим для зловмисника. Проникнувши в мережний периметр, порушник зможе розвинути атаку й отримати доступ до корпоративних ресурсів і критичних сфер інфраструктури. Дослідження безпеки Wi-Fi дозволить оцінити рівень захищеності бездротових мереж, знайти та усунути наявні проблеми. Проте методів виявлення каналів витікання інформації та локалізації можливих місць витікання інформації не наводиться.

У роботах [4–7] наведено можливі сценарії, які будуються на найбільш поширених векторах атак: безпосередньо на точки доступу; на канал взаємодії точки доступу з клієнтом (перехоплення та розшифрування трафіка); на процес аутентифікації (викрадення аутентифікаційних даних користувачів). Методологію припинення сценарію цих атак не наведено, методи виявлення вторгнень у бездротову мережу не розглянуто.

У роботах [8, 9] розглядається організація підроблених точок доступу, вихід із гостьової Wi-Fi-мережі в корпоративну або експлуатація вразливостей небезпечних протоколів автентифікації – лише частина можливих атак із арсеналу зловмисників, які експлуатують бездротові мережі. Тому завершеного характеру робота не отримала.

У роботі [10] доводиться, що зловмисник, метою якого є атака на корпоративну інфраструктуру, крім достатнього рівня кваліфікації може мати у своєму розпорядженні набір спеціалізованих інструментів. У його арсеналі можуть бути потужні Wi-Fi-адаптери для роботи в різних частотних діапазонах, антени, мікрокомп'ютери для створення підробленої точки доступу, обладнання для прихованого аналізу бездротових мереж і різноманітне програмне забезпечення, що дозволяє активно аналізувати безпеки Wi-Fi-мереж. Тобто більше уваги приділено апаратно-програмній частині атак, а не методу виявлення нелегального вторгнення.

У роботах доводиться, що атака на Wi-Fi точки доступу з глобальної та локальної мереж є недооцінена проблема. Вона базується на помилках налагоджування обладнання. Як правило, далі налаштування інтернету та Wi-Fi мало хто доходить. Мало хто дбає про те, щоб змінити пароль адміністратора, і вже зовсім одиниці вчасно оновлюють прошивку пристроїв. І всі це безліч пристроїв з обліковими даними admin: password прекрасні видно для сканерів у локальній або глобальній мережі ... (є винятки, наприклад, не видно пристрої із сірими адресами, за NAT тощо. Тобто їх не видно з глобальної мережі, але ніхто не скасовував їх видимість у локальних мережах). І вже є реалізації масової атаки на дефолтні облікові дані та відомі вразливості роутерів: Router Scan by Stas'M. Але це вторгнення у бездротову мережу цілком залежить від кваліфікації як користувача, так і зловмисника. Проблемі виявлення вторгнення у бездротову мережу не приділено уваги.

У цих роботах не повною мірою відображено питання методологічного визначення сигналів несанкціонованих точок доступу до інформації у бездротових мережах підприємств.

Таким чином, нині у практиці і теорії побудови систем захисту інформації у бездротових мережах загострилося протиріччя між необхідністю швидкого й гарантованого визначення та точної локалізації несанкціонованих точок доступу, що працюють на фоні легальних радіосигналів у бездротових мережах, і можливостями існуючих методів, які використовуються для виявлення та блокування нелегальних точок доступу у бездротових мережах.

З урахуванням викладеного вище, розроблення й удосконалення моделей для виявлення та локалізації нелегального отримання інформації на об'єктах інформаційної діяльності є актуальними.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розглядаючи історію виникнення Wi-Fi, слід зазначити, що в основу технології покладено методику передачі даних радіоканалом на частоті 2,4 ГГц із використанням кодування сигналу робочими частотами і спеціальними додатками. Технологія Wi-Fi використовується для організації високошвидкісних бездротових локальних мереж, які працюють у міжнародному неліцензованому діапазоні частот (ISM) 2,4 ГГц і 5 ГГц. Основною перевагою Wi-Fi перед іншими технологіями є висока швидкість передачі інформації – до 1300 Мбіт/с. Тому ця технологія широко застосовується в різних бездротових телеметричних системах і на транспорті. Нині важко знайти іншу подібну за активністю використовувану ділянку радіочастотного спектра, частоти якого використовуються більше ніж діапазон Wi-Fi. Звісно, чим більш використовуваним є діапазон радіочастотного спектра, тим складніше його контролювати й аналізувати. Ця обставина є найвагомішим фактором для вибору зловмисниками середовища з метою маскування роботи своїх точок доступу, призначених для перехоплення інформації обмеженого доступу. Використовуючи для роботи несанкціонованих точок доступу сильно завантажені частотні діапазони бездротових мереж, зловмисник має намір максимально ускладнити їхнє виявлення. Логічно застосовувати для цього загальноприйняті й поширені в цих діапазонах стандарти зв'язку. Але найголовніше – важко відрізнити роботу двох пристроїв, що використовують один і той самий цифровий стандарт зв'язку, без виявлення їхніх унікальних ідентифікаторів (ID). У випадку з Wi-Fi таким ідентифікатором є MAC-адреса. MAC-адреса – це унікальний ідентифікатор мережного інтерфейсу (зазвичай мережної карти) для реалізації комунікації пристроїв у мережі на фізичному рівні. Це унікальний номер, який зберігається у постійній пам'яті, що доступна тільки для читання, і який призначений конкретній мережній карті її виробником. Також унікальним ідентифікатором може бути LLC (Logical link control) – підрівень керування логічним зв'язком – за стандартом IEEE 802 – верхній підрівень канального рівня моделі OSI, який керує передачею даних і забезпечує перевірку і правильність передачі інформації по з'єднанню. У цьому випадку нас цікавить використання технології Wi-Fi, а також вимоги, які необхідно пред'являти до сучасних засобів аналізу мереж Wi-Fi стосовно області пошуку і локалізації несанкціонованих точок доступу для запобігання витікання інформації радіоканалом Wi-Fi.

Актуальність викладеного підтверджується, крім теоретичного обґрунтування, ще і реальними спектрограмами. Реальні спектрограми, що доводять складність визначення несанкціонованих точок доступу існуючими методами, зображено на рис. 1 та 2.

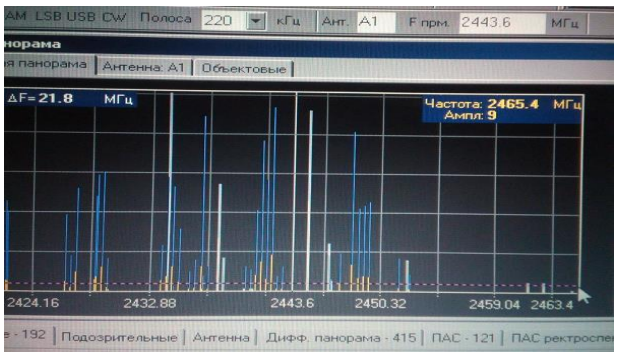

Рис. 1. Спектр сигналів діапазону Wi-Fi, отриманий АПК зі сканувальним приймачем

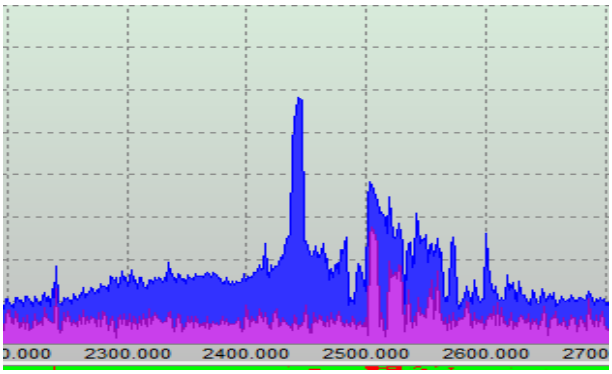

Рис. 2. Спектр сигналів діапазону Wi-Fi, отриманий АПК зі сканувальним приймачем іншого АПК

На рис. 1–3 показано графіки спектрів сигналів, отриманих різними АПК. На рис. 1 та 3 бачимо, що виявити та розпізнати сигнал, який не належить до легальних сингалів, неможливо. Якщо аналоговий сигнал можна виявити за акустичним відгуком, установивши сканувальний приймач на частоту сигналу, то цифровий сигнал так виявити неможливо, тому що він закодований. Замість акустичного сигналу ми будемо чути імпульси цифрового сигналу, без визначення його походження.

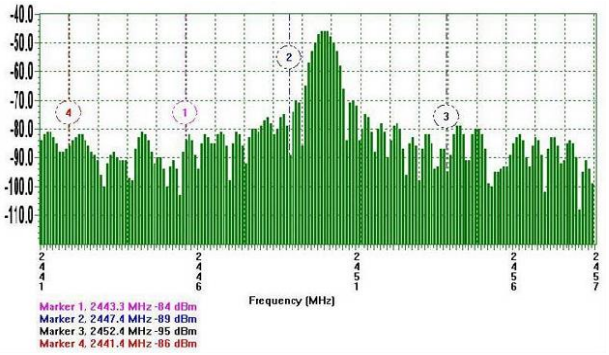

Рис. 3. Спектр сигналів діапазону Wi-Fi, отриманий АПК за допомогою спектр-аналізатора

Отже, сканування цифрового радіодіапазону не дозволить остаточно виявити, а тим більше розпізнати сигнал несанкціонованої точки доступу.

Якщо брати до уваги, що ринок зараз наповнюється високоякісними мініатюрними диктофонами з убудованими Wi-Fi-передавачами, які поєднують у собі диктофон і передавач Wi-Fi, тоді зрозуміло, що цей діапазон буде ще більше завантажуватися.

Беручи до уваги, що у комплекті з Micro Wi-Fi диктофоном поставляється мінімаршрутизатор, який можна конфігурувати так, щоб він автоматично виявляв мережу диктофона, підключався до неї і завантажував аудіозапис, тоді оператору досить наблизитися з ноутбуком із підключеним маршрутизатором на відстань дії мережі Wi-Fi (до 50 м у приміщеннях), щоб завантажити всю накопичену інформацію. Завантаження добового аудіоспостереження, у разі якісного Wi-Fi-з'єднання, з диктофона такого типу займає всього декілька хвилин. Виявити такі пристрої дуже складно. Але таких передавачів частот Wi-Fi, які зовсім не можна виявити, не існує.

Отже, виявити пристрій найімовірніше саме у момент передачі накопиченої інформації по мережі Wi-Fi.

Після тестування такого диктофона, у реальних умовах можна підтвердити основні ТТХ та відмітити його особливості:

1) диктофон може бути виявлено в мережі як точку доступу по SSID. Тут SSID (Service Set Identifier) – унікальний ідентифікатор бездротової мережі, що відрізняє одну мережу Wi-Fi від іншої. У налаштуваннях усіх пристроїв, які повинні працювати в одній бездротовій мережі, має бути зазначений однаковий SSID. Причому SSID можна привласнити будь-яке ім'я;

2) передавання півгодинного запису розмови здійснюється за 30 с.

Це дуже важливе спостереження щодо необхідності повного перегляду концепції моніторингу мереж Wi-Fi. Постійний і безперервний у часі аналіз мереж Wi-Fi тепер стає актуальним, як і постійний радіомоніторинг на об'єктах із наявністю інформації обмеженого доступу.

На нашу думку, велику загрозу мають також Wi-Fi-відеокамери. Як приклад, розглянемо доступну модель Defender MULTICAM WF-10HD. Достатньо розглянути її ТТХ, щоб зрозуміти, що в руках досвідченого зловмисника цей пристрій цілком може стати суттєвою проблемою для фахівців із захисту інформації. Прикладом може бути налагодження з можливістю доступу до камери з будь-якої точки світу через спеціалізований ресурс. У цьому випадку головним є можливість підключення камери до мережі інтернет, що нині виконати не важко. Модифіковані зразки такого типу відеокамер можуть працювати аналогічно прикладу з диктофоном, тобто використовувати передачу по Wi-Fi на короткі відстані.

Проблеми виявлення таких пристроїв виникають з урахуванням можливостей сучасних аналізаторів Wi-Fi, які зазвичай використовуються пошуковими бригадами під час пошукових заходів і в моніторингу контрольованих об'єктів. Більшість аналізаторів із широкими можливостями мають досить великі габарити і прив'язані до комп'ютера. Якщо останній і існує, то у кращому випадку, він розміщений на посту контролю, який може бути значно віддалений від контрольованого приміщення, де зазвичай немає можливості встановити окремий аналізатор.

На підставі викладеного, а також аналізу нових загроз, сформуємо методику пошуку за допомогою автоматизованого програмного комплексу (АПК) мереж Wi-Fi на наявність нелегальних сигналів.

Основою методики виявлення, розпізнавання та локалізації пристроїв і каналів витікання інформації, що працюють у діапазоні Wi-Fi, є аналіз спектральної щільності сигналів. Він базується на

тому, що в активному режимі трансляції інформації спектральна щільність збільшується значно помітніше ніж спектр. Це пов'язано з тим що, залежність спектральної щільності сигналу від звичайного спектра сигналу – квадратична. Тобто зростає значно швидше ніж звичайний спектр.

Оскільки у мережах Wi-Fi завжди використовують маршрутизатори й комутатори, то ці мережі дуже добре захищені та програмно керовані, і проводити перевірку можливо двома способами. Перший, практично відкритий, спосіб – коли всі точки доступу Wi-Fi будуть виключені, тоді "чужі" точки доступу працюватимуть. "Чужі" сигнали дуже просто буде виявити та локалізувати за допомогою запропонованого АПК. Але, якщо потрібно проводити пошукові роботи приховано, тоді цей метод використати неможливо. Потрібно буде застосовувати програмний засіб АПК, що дозволяє аналізувати покриття приміщення, визначати MAC-адреси всіх точок доступу Wi-Fi. Потім цей програмний засіб визначає LLC. На карту приміщення наносить розташування всіх точок доступу та робить карту покриття сигналом Wi-Fi.

Далі аналізує базу MAC-адрес та LLC, виконуючи порівняльний аналіз, виявляє та розпізнає сигнал цифрових засобів негласного отримання інформації.

З огляду на те, що на першому етапі перевірки в базу АПК завантажується, у чіткому масштабі, схематичний план приміщення, визначення "чужого" випромінювання та місце його розташування чітко визначатиметься на схематичному плані приміщення. Алгоритм роботи запропонованого АПК наведено на рис. 4. Слід зазначити, що вказаний алгоритм і наведена методика є частиною цілої методики виявлення, розпізнавання та локалізації цифрових засобів нелегального отримання інформації. Тобто, процес сканування за запропонованою методикою проходить обов'язково, тому що цифровий діапазон складається з багатьох піддіапазонів, деякі вже були розглянуті, а інші розглядатимемо пізніше.

Методика пошуку цифрових засобів нелегального отримання інформації у діапазоні частот мережі Wi-Fi накладає умови, які повинні відповідати таким вимогам:

1. Неперервний (цілодобовий), за допомогою АПК, контроль мережі Wi-Fi усіх стандартів (IEEE 802.11 a / b / g / n) [9], з прив'язкою всіх вимірювань до часу (якщо є така можливість, то контроль приміщень потрібно здійснювати постійно, мати в наявності АПК і спеціаліста із захисту інформації).

2. Пошукові модулі АПК мають бути розміщені безпосередньо в контрольованих приміщеннях (без необхідності установки у приміщенні додаткових ПК) та з'єднані в єдину мережу.

3. Оператор має здійснювати роботи з локалізації мобільно, без необхідності підключення до стаціонарних ПК, накопичений архів даних у цьому разі повинен зберігатися тривалий час.

4. АПК має вести список легальних MAC-адрес для швидкого виявлення й ідентифікації нових передавачів Wi-Fi, та виявляти всі MAC-адреси всіх приладів.

5. Для остаточного виявлення та локалізації цифрових засобів негласного отримання інформації оператору потрібно мати легкий, мобільний та економічний приймальний пеленгаційний модуль. Цей модуль потрібен для розв'язання оперативних завдань.

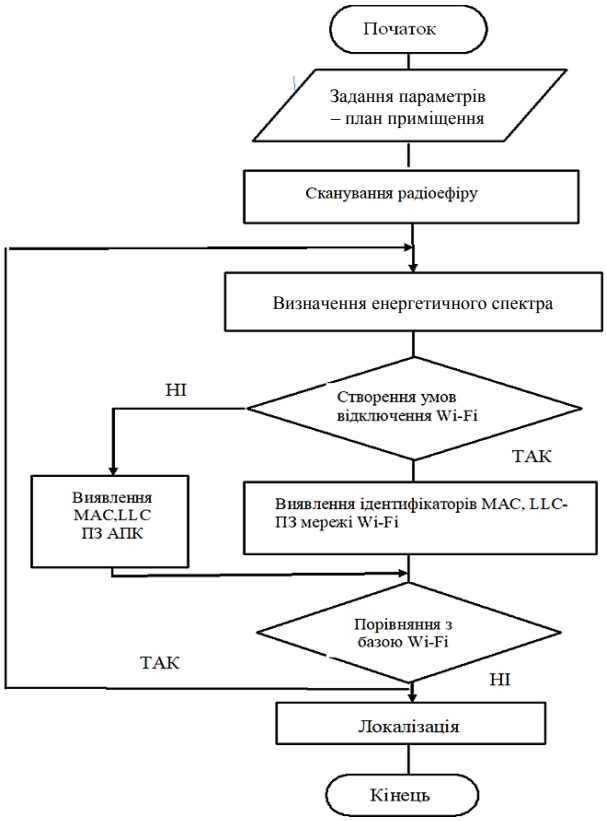

Рис. 4. Алгоритм роботи пошуку цифрових засобів нелегального отримання інформації у діапазоні частот мережі Wi-Fi

Для постійної роботи з протидії незаконним методам отримання інформації необхідна наявність мережного програмного забезпечення, підтримка зонального розміщення необхідної кількості пошукових модулів, які будуть виконувати задачі з пошуку цифрових засобів негласного отримання інформації на постійній основі.

З метою підтвердження алгоритму пошуку цифрових засобів негласного отримання інфор-

мації в діапазоні частот Wi-Fi проведено натурне моделювання пошуку цифрових засобів негласного отримання інформації. Використавши мережне програмне забезпечення, яке імітувало ПЗ АПК, установили імітатори пошукових модулів, це точки доступу Wi-Fi, які були переведені в режим сканування, у лабораторному приміщенні на рис. 5.

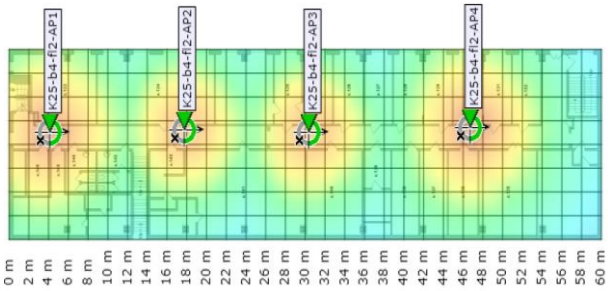

Рис. 5. Приміщення з розташованими пошуковими модулями

Провели сканування приміщення, з метою уточнення розташування пошукових модулів, отримали схему приміщення з рівнем покриття сигналами пошукових модулів (рис. 6).

Далі у лабораторному приміщенні було встановлено нештатний пристрій Wi-Fi. Проведено повторне сканування та отримано схему приміщення, з визначенням "чужого" сигналу. На рис. 6 показано реальну роботу вдосконаленої методики та програмного засобу виявлення, розпізнання та локалізації імітатора цифрових засобів негласного отримання інформації.

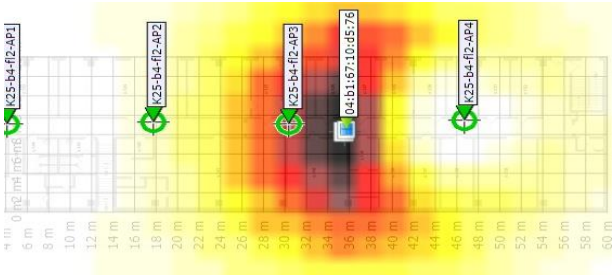

Рис. 6. Схема виявлення імітатора цифрових засобів негласного отримання інформації з використанням запропонованої методики

На рис. 6 темним кольором позначено місце локалізації імітатора цифрових засобів негласного отримання інформації. Отже, одержано результати, які цілком підтверджують запропоновану нами методику пошуку цифрових засобів негласного отримання інформації у цифровому діапазоні Wi-Fi.

Саме таким чином, згідно із запропонованою методикою та за допомогою нових розроблених ПЗ АПК, які можуть виконувати ці завдання, можна виявити й локалізувати цифрові засоби негласного отримання інформації, що працюють під прикриттям легального частотного діапазону Wi-Fi.

5. ВИСНОВКИ

Проведено аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації. Удосконалено метод виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності. Виконано натурне моделювання виявлення несанкціонованого втручання в інформаційну бездротову мережу підприємства. Натурне моделювання цілком підтвердило запропонований нами вдосконалений метод виявлення та локалізації несанкціонованих точок доступу до інформації у бездротовій мережі підприємства. Натурне моделювання підтвердило точність локалізації несанкціонованої точки доступу до інформації у мережі Wi-Fi – до 2 м. Це дозволить своєчасно виявити та локалізувати несанкціоновані точки доступу до інформації у бездротовій мережі підприємств та установ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Барсуков, О. М., Кав'юк, В. В., & Потапенко, В. В. (2018). Виділення аудіосигналу на фоні шуму з використанням методу сингулярного спектрального аналізу. *Системи озброєння і військова техніка,* 1(53). 61–66.

[2] Лаптєв, О. А. (2018). Модель інформаційної безпеки на основі марковських випадкових процесів. *Зв'язок.* К., ДУТ, 6(136). 45–49.

[3] Барабаш, О. В., Лаптєв, О. А., & Зозуля, С. А. (2019). Векторні аналізатори сигналів для удосконалення методики пошуку засобів негласного отримання інформації. *Телекомунікаційні та інформаційні технології.* К., ДУТ, 1. 55–61.

[4] Лаптєв, О. А. (2019). Методика виявлення та локалізації засобів негласного отримання інформації, працюючих у цифровому діапазоні. *Сучасний захист інформації.* К., ДУТ, 2(38). 25–31.

[5] Половінкін, І. М., Лаптєв, О. А., Чумаченко, С. Н., & Гуйда, О. Г. (2019). Визначення основних характеристик випадкових сигналів моделі пошуку засобів негласного отримання інформації. *Вчені записки Таврійського нац. ун-ту ім. В. І. Вернадського*, т. 30 (69), № 6. 101–105.

[6] Павлов, І. М., & Хорошко, В. О. (2013). Функторність і граничність відображень об'єктів множин у системах захисту інформації. *Інформаційна безпека,* 1. 107–116.

[7] Хорошко, В. А. (1999). Вибір критеріїв для оптимізації системи технічного захисту інформації. *Захист інформації: зб. наук. пр.* К., КМУГА, 1999, 7–9.

[8] Хорошко, В. О. Хохлачова, Ю. Є., & Тимченко, М. П. (2017). Оцінка захищеності систем зв'язку. *Системи обробки інформації.* Х., ХНУПС, 2., 134–137.

[9] Лужецький, В. А., & Дудатьєв А. В. (2017). Концептуальна модель системи інформаційного впливу. *Безпека інформації,* т. 23, № 1, С. 45–49.

REFERENCES

[1] Barsukov, O. M., Kavyuk, V. V., & Potapenko V. V. (2018). Isolation of an audio signal against a background of noise using the method of singular spectral analysis. *Weapon systems and military equipment*, 1 (53). 61–66 [in Ukrainian].

[2] Laptev O. A. (2018). Model of information security based on Markov random processes. *Zvyazok: Scientific and practical magazine*., K.: DUT, 6(136). 45–49 [in Ukrainian].

[3] Barabash, O.V., Laptev, O. A., & Zozulya, S. A. (2019). Vector signal analyzers for improving the method of finding means of tacitly obtaining information. *Telecommunications and information technologies: a scientific journal*, K., DUT, 1. 55–61 [in Ukrainian].

[4] Laptev, O. A. (2019). The method of detection and localization of means of secretly obtaining information working in the digital range. *Modern information protection: scientific and technical journal*, K., DUT, 2(38). 25–31 [in Ukrainian].

[5] Polovinkin, I. M., Laptev, O. A., Chumachenko, S. N., & Guida, O. G. (2019). Determination of the main characteristics of random signals of the model of the search for means of obtaining information secretly. *Scientific Notes of V. I. Vernadskyi Tavra National University: jour*., vol. 30(69), no. 6., 101–105 [in Ukrainian].

[6] Pavlov, I. M., & Khoroshko, V. O. (2013). Functority and finiteness of mappings of set objects in information protection systems. *Informational security*, 1. 107–116 [in Ukrainian].

[7] Khoroshko, V. A. (1999). Selection of criteria for optimization of systems of technical protection of information. *Protection of information: a collection of scientific works*, K., KMUGA, pp. 7–9 [in Ukrainian].

[8] Khoroshko, V. O., Khokhlacheva, Yu. E., & Tymchenko, M. P. (2017). Evaluation security of communication systems. *Information Processing Systems*. Kharkiv, KhNUPS, no. 2, 134–137 [in Ukrainian].

[9] Luzhetsky, V. A., & Dudatiev, A. V. (2017). Conceptual model of the system of information influence. *Information security*, vol. 23, no. 1., 45–49 [in Ukrainian].

Стаття надійшла до редколегії 12.02.2023

Improvement of the method of detection and location of illegal access points to the wireless network of information activity objects

Extensive use of mobile devices has led to increased Internet connections and the deployment of new wireless LANs. According to the latest Cisco research, by 2023, 66% of the world's population will be Internet users worldwide. More than 28 billion devices will be connected to the global network. In the last two decades, we have witnessed the birth and development of a technology that has significantly changed our work and life - IEEE 802.11, also known as Wi-Fi. Wi-Fi is a favorite way to connect to the Internet because of its ease of use and flexibility. To connect to a wireless network, you only need to be within range. That is, consumers and businesses will increasingly rely on mobile networks. However, it should be noted that each new opportunity of digitalization also gives new opportunities to cybercriminals and therefore, the problem of security of wireless networks today is one of the main problems of IT technologies. The inevitable proliferation of wireless networks and the growing traffic in these networks can lead to many information security incidents. The main threats are aimed at interception, breach of confidentiality and integrity of transmitted data, attacks on the availability of transmission channel nodes and their substitution.

The article analyzes the existing methods of detecting unauthorized access points to information. The method of detection and localization of unauthorized access points to information circulating in the wireless network at the objects of information activities has been improved. Natural modeling of detection of unauthorized interference in the information wireless network of the enterprise was carried out. Full-scale simulation confirmed the accuracy of localization of an unauthorized point of access to information in the Wi-Fi network – up to 2 m. This will allow timely detection and localization of unauthorized access points to information in the wireless network of enterprises and institutions.

Keywords: *attack; radio signal; method; threat; flow of information*

Наталія Лукова-Чуйко,
д-р техн. наук, проф.
Завідувачка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Nataliya Lukova-Chuiko,
Dr. Sci. (Engin.), Prof.
Head of the Department of Cyber Security and Information Protection of the Faculty of Information Technologies Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Тетяна Лаптєва,
Аспірантка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Tetyana Lapteva,
PhD Student Department of Cyber Security and Information Protection of the Faculty of Information Technologies of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.