УДК 351.746:007–047.44

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Тарас Петренко

На сьогоднішній день бездротові технології інтенсивно розвиваються та проникають у суспільне життя, поступово замінюючи дротові. Зручність використання, нижча вартість розгортки систем – це основні переваги бездротових систем. Технологія стандарту IEEE 802.11, звана також Wi-Fi є найпопулярнішою на сьогодні технологією бездротового зв'язку. Кількість її користувачів щоденно збільшується. Проте системи захисту інформації даних в цій технології, по-перше, поступаються системам захисту дротових мереж через існування особливостей загроз в бездротових мережах, по-друге недостатньо досліджені та перевірені. Таким чином, проблема визначення та аналізу загроз інформаційної безпеки в мережах стандарту IEEE 802.11 є актуальною на сьогоднішній день. Проводячи аналіз ми спирались на дослідження зарубіжних вчених та практикуючих компаній, що займаються вивченням загроз та розробкою систем їх запобігання. Дослідження даного питання дає можливість визначити та класифікувати можливі загрози та модернізувати існуючі або розробити нові ефективні методи та заходи інформаційної безпеки.

Ключові слова: *комп'ютерні мережі, стандарт IEEE 802.11, Wi-Fi, загрози інформаційної безпеки, захист інформації.*

Постановка проблеми. В даний час, в Україні, у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій [1]. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені мережами мобільного зв'язку, факсимільний зв'язок став доступний для широкого кола користувачів. Мережі стандарту 802.11 активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Аналіз стану захисту інформації бездротових мереж – це комплексне вивчення фактів, подій, процесів, явищ, пов'язаних з проблемами захисту інформації, у тому числі даних про стан роботи по виявленню можливих каналів витоку інформації, про причини і обставини, що сприяють витоку і порушень режиму секретності (конфіденційності) в ході повсякденної діяльності підприємства [2].

Аналіз останніх досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В.В. Баранника, В.М. Богуна, С.В. Віхорева, І.Д. Горбенко, Ю.І. Грицюк, С.В. Казмирчук, Г.Ф. Конаховича, О.Г. Корченка, М.Г. Луцького, А.І. Марущака, В.П. Мельнікова, В.В. Мохора, О.М. Новікова, О.В. Олійника, О.В. Сосніна, С.В. Толюпи, В.О. Хорошко, О.К. Юдіна та ін.

Дослідження різноманітних аспектів інформаційно-аналітичної діяльності здійснювали Т.В. Абрамова, С.С. Алдишев, В.П. Александрова, А.А. Атаян, С.Ф. Багаундінова, Т.В. Вдовіна, А.В. Горячов, Р.О. Гуревич, М.І. Жалдак, О.П. Значенко, В.Г. Кальченко, Н.В. Кисіль, В.І. Клочко, Н.В. Морзе, С.Ю. Нікіфорова, О.В. Пархоменко, С.А. Раков, М.В. Селіна, Ю.М. Ткач, В.А. Сластьонін та ін.

Виділення не вирішених раніше частин загальної проблеми. Проте, незважаючи на значний обсяг накопичених у даній сфері знань, недостатньо дослідженою залишилась проблема захисту інформації комп'ютерних мереж стандарту 802.11.

Мета статті. Головною метою цієї роботи є аналіз основних типів загроз інформаційної безпеки в мережах стандарту 802.11. Визначення основних причин можливості втрати інформації.

Виклад основного матеріалу. На сьогоднішній день існує безліч можливостей для підключення пристроїв до мереж Wi-Fi: кафетерії, готелі, ресторани і аеропорти, навіть в міському транспорті ви можете вийти в он–лайн без підключення до мобільного Інтернету. Але найчастіше ці відкриті мережі не є безпечними. Що б ви не використали – ноутбук, планшет або смартфон, – підключення має забезпечувати захист ваших даних настільки, наскільки це можливо. Ми виділяємо три основні види загроз інформаційної безпеки в комп'ютерних мережах:

Втрата конфіденційної інформації;

Перехоплення конфіденційної інформації;

Знищення або спотворення конфіденційної інформації.

За класифікацією [3] загрози інформаційної безпеки можна розділити на:

прямі – загрози інформаційній безпеці, що виникають при передачі інформації;

непрямі – загрози, пов'язані з наявністю на об'єкті і поряд з об'єктом великої перешкод.

З точки зору безпеки, слід враховувати не тільки загрози, властиві провідним мережам, але також і середу передачі сигналу. У бездротових мережах отримати доступ до переданої інформації набагато простіше, ніж в провідних мережах, так само як і вплинути на канал передачі даних. Досить помістити відповідний пристрій в зоні дії мережі.

Існує два основних варіанти функціонування бездротової мережі:

Ad - hoc – передача безпосередньо між пристроями;

Hot - spot – передача здійснюється через точку доступу.

В Hot - spot мережах присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але і доступ до зовнішніх мереж. Hot - spot представляє найбільший інтерес з точки зору захисту інформації, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених в даній бездротовій мережі.

Традиційні провідні мережі використовують кабель для передачі інформації. Кабель вважається «контрольованим» середовищем, захищений будівлями та приміщеннями, в яких він знаходиться. Зовнішній «чужий» трафік, який входить в захищений сегмент мережі, фільтрується фаєрволом і аналізується системами IDS/IPS. Для того щоб отримати доступ до такого сегменту провідної мережі, зловмисникові необхідно подолати або систему фізичної безпеки будівлі, або міжмережевий екран.

Бездротові ж мережі використовують радіохвилі (ефір). Ефір – середа з загальним доступом і практично повною відсутністю контролю. Забезпечити еквівалент фізичної безпеки провідних мереж тут майже неможливо. Як тільки користувач підключає до провідної мережі точку доступу, її сигнал може проходити крізь стіни, міжповерхові перекриття, вікна будівлі. Таким чином, підключений сегмент мережі стає доступним з іншого поверху, з сусіднього будинку, або іншого кінця вулиці – радіосигнал може поширюватися на сотні метрів за межі будівлі. Єдиним фізичним обмеженням бездротової мережі є потужність сигналу. Тому, на відміну від дротових мереж, де точка підключення користувача до мережі визначена і відома, в бездротових мережах підключитися до мережі можна звідки завгодно, в межах дії сигналу.

Оскільки радіосигнали мають широкомовну природу, не обмежені стінами будівель і доступні всім приймачам, місце розташування яких складно або взагалі неможливо зафіксувати – зловмисникам особливо легко і зручно атакувати бездротові мережі. Отже, бездротові технології, що працюють без фізичних і логічних обмежень своїх дротових аналогів, які значно підвищують гнучкість робочого процесу і ефективність праці користувачів, що знижує витрати на розгортання мереж, також піддають мережеву інфраструктуру і користувачів значним ризикам.

На основі проведеного аналізу нами було виділено основні ризики інформаційної безпеки в бездротових мережах:

1. Чужинці (Rogue Devices, Rogues). Чужинцями називаються пристрої, що надають можливість неавторизованого доступу до корпоративної мережі, часто в обхід механізмів захисту, визначених корпоративною політикою безпеки. Найчастіше це ті самі самовільно встановлені точки доступу. Навіть якщо організація не використовує бездротовий зв'язок і вважає себе в результаті такої заборони захищеною від бездротових атак – впроваджений (навмисне чи ні) чужак з легкістю виправить це положення. Доступність і дешевизна пристроїв Wi-Fi призвели до того, що в Україні, наприклад, практично кожна мережа з числом користувачів більше 50 використовує його для передачі чи отримання даних.

Крім точок доступу в ролі чужинця можуть виступити домашній роутер з Wi-Fi, програмна точка доступу Soft AP, ноутбук з одночасно включеними провідним і бездротовим інтерфейсом, сканер, проектор і т.д.

2. Нефіксована природа зв'язку. Як вже було сказано вище – бездротові пристрою не «прив'язані» кабелем до розетки і можуть змінювати точки підключення до мережі прямо в процесі роботи. Прикладом є «Випадкові асоціації», коли ноутбук з Windows XP (досить довірливо відноситься до всіх бездротових мереж) або просто некоректно конфігурований бездротовий клієнт автоматично асоціюється і підключає користувача до найближчої бездротової мережі. Такий механізм дозволяє зловмисникам «перемикати на себе» користувача для подальшого сканування вразливостей, фішингу або атак Man-in-The-Middle. Крім того, якщо користувач одночасно підключений і до дротової

мережі – він стає зручною точкою входу – тобто класичним чужаком.

Мережі Ad - Hoc – безпосередні однорангові з'єднання між бездротовими пристроями без участі точок доступу – є зручним способом швидко перекинути файл колезі або роздрукувати потрібний документ на принтері з Wi-Fi. Проте, такий спосіб організації мережі не підтримує більшість необхідних методів забезпечення безпеки, надаючи зловмисникам легкий шлях до злому комп'ютерів користувачів мереж Ad - Hoc. Доступні технології VirtualWiFi і Wi-Fi Direct тільки погіршують ситуацію.

3. Уразливості мереж і пристроїв. Деякі мережеві пристрої, можуть бути більш уразливі, ніж інші – можуть бути неправильно сконфігуровані, використовувати слабкі ключі шифрування або методи аутентифікації. Не дивно, що в першу чергу зловмисники атакують саме їх. Звіти аналітиків стверджують, що понад 70 відсотків успішних зломів бездротових мереж відбулися саме в результаті неправильної конфігурації точок доступу або клієнтського ПЗ. За даними Лабораторії Касперського у 2014 році 87% компаній постраждали від внутрішніх загроз, 24% подібних інцидентів привели до втрати конфіденційної інформації [7]. Відповідно до результатів дослідження міжнародної організації Ponemon Institute втрати від інформаційних атак в 2014 році збільшились на 23% порівняно з 2013 роком і склали 3,8 мільйонів доларів [5]. Відповідно до щорічного звіту корпорації IBM кількість атак зменшилась на 36% у 2014 році (рис. 1), порівняно з 2013 роком. Дана статистика дозволяє зробити висновок, що не зважаючи на зниження загальної кількості подій, що загрожують інформаційній безпеці втрати від них зростають.

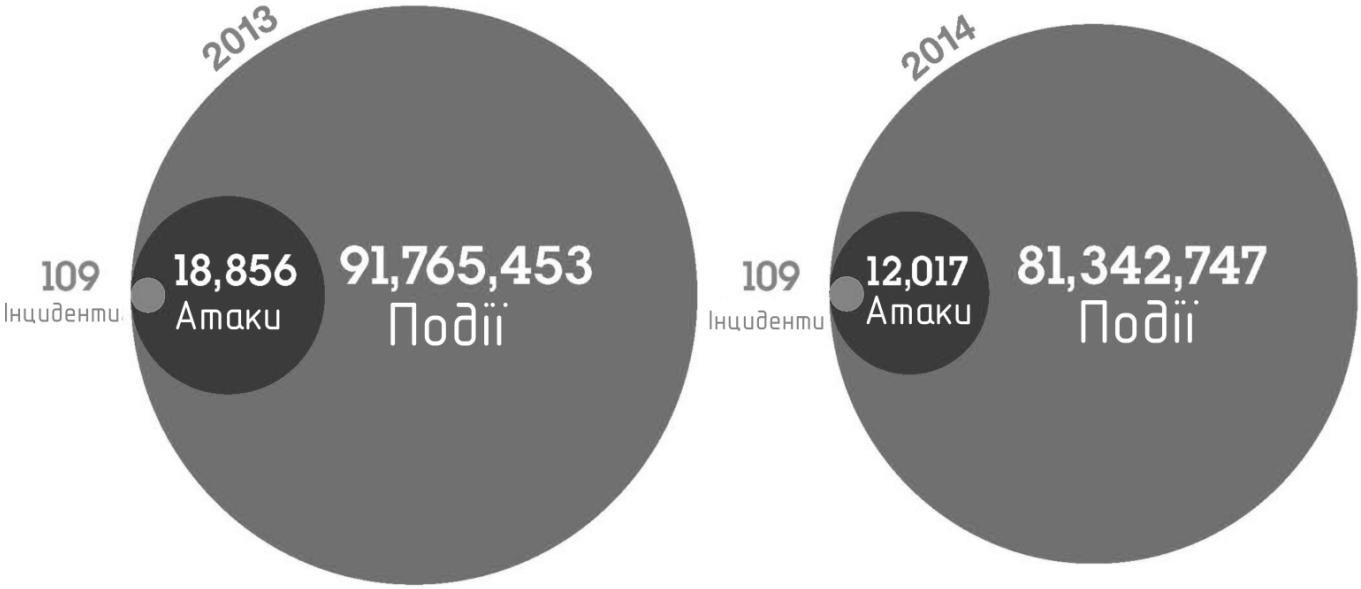

Рис. 1. – Середньорічна статистика подій, атак та інцидентів інформаційної безпеки*
**Джерело: за даними наукового звіту IBM 2015 Cyber Security Intelligence Index* [6]

Некоректно сконфігуровані точки доступу. Одна-єдина некоректно сконфігурована точка доступу (в т.ч. чужак) може послужити причиною злому корпоративної мережі. Налаштування за замовчуванням більшості точок доступу не включають автентифікацію або шифрування, або використовують статичні ключі, записані в керівництві і тому загальновідомі. У поєднанні з невисокою ціною точок доступу цей фактор значно ускладнює завдання стеження за цілісністю конфігурації безпровідної інфраструктури та рівнем її захисту. Співробітники організації можуть самовільно приносити точки доступу і підключати їх куди заманеться. При цьому малоймовірно, що вони приділять достатньо уваги їх грамотній і безпечній конфігурації і узгодженню своїх дій з відділом захисту інформації. Саме такі точки і створюють найбільшу загрозу дротових і бездротових мереж.

Некоректно сконфігуровані пристрої користувачів надають загрозу ще більшу, ніж некоректно сконфігуровані точки доступу. Ці пристрої буквально приходять і йдуть з підприємства, часто вони не конфігуруються спеціально з метою мінімізації бездротових ризиків і задовольняються конфігурацією за замовченням (яка, апріорі, не

може вважатися безпечною). Такі пристрої надають неоціненну допомогу зловмисникам в їх справі проникнення в дротову мережу, забезпечуючи зручну точку входу для сканування мережі та поширення в ній шкідливого ПЗ.

Зловмисникам давно доступні спеціальні засоби для злому мереж, що ґрунтуються на стандарті шифрування WEP. Ці інструменти широко висвітлені в Інтернет [4] і не вимагають особливих навичок для застосування. Вони використовують уразливості алгоритму WEP, пасивно збираючи статистику трафіку в бездротовій мережі до тих пір, поки зібраних даних не виявиться достатньо для відновлення ключа шифрування. З використанням останнього покоління засобів злому WEP, використовують спеціальні методи ін'єкції трафіку. Аналогічно, є уразливості різного ступеня небезпеки та складності, що дозволяють ламати TKIP і навіть WPA/WPA2-PSK. Єдиним «надійним» методом поки що залишається використання WPA/WPA2-Enterprise (802.1x) з серверними сертифікатами.

4. Нові загрози і атаки. Бездротові технології породили нові способи реалізації старих загроз, а також деякі нові, досі неможливі в провідних мережах. У всіх випадках, боротися з атакуючим стало важче, тому що неможливо відстежити його фізичне місце розташування та ізолювати його від мережі.

У 2014 році, несанкціонований доступ очолив список найрозповсюдженіших загроз інформаційної безпеки, обійшовши шкідливий код, який був на першому місці в 2013 році (рис. 2).

Більшість традиційних атак починаються з розвідки, в результаті якої зловмисником визначаються подальші шляхи розвитку атаки. Для бездротової розвідки використовуються як засоби сканування бездротових мереж (NetStumbler, Wellenreiter, вбудований клієнт JC), так і засоби збору та аналізу пакетів, тому багато керуючих пакетів WLAN незашифровані. При цьому дуже складно відрізнити станцію, що збирає інформацію, від звичайної станції, яка намагається отримати авторизований доступ до мережі або від спроби випадкової асоціації.

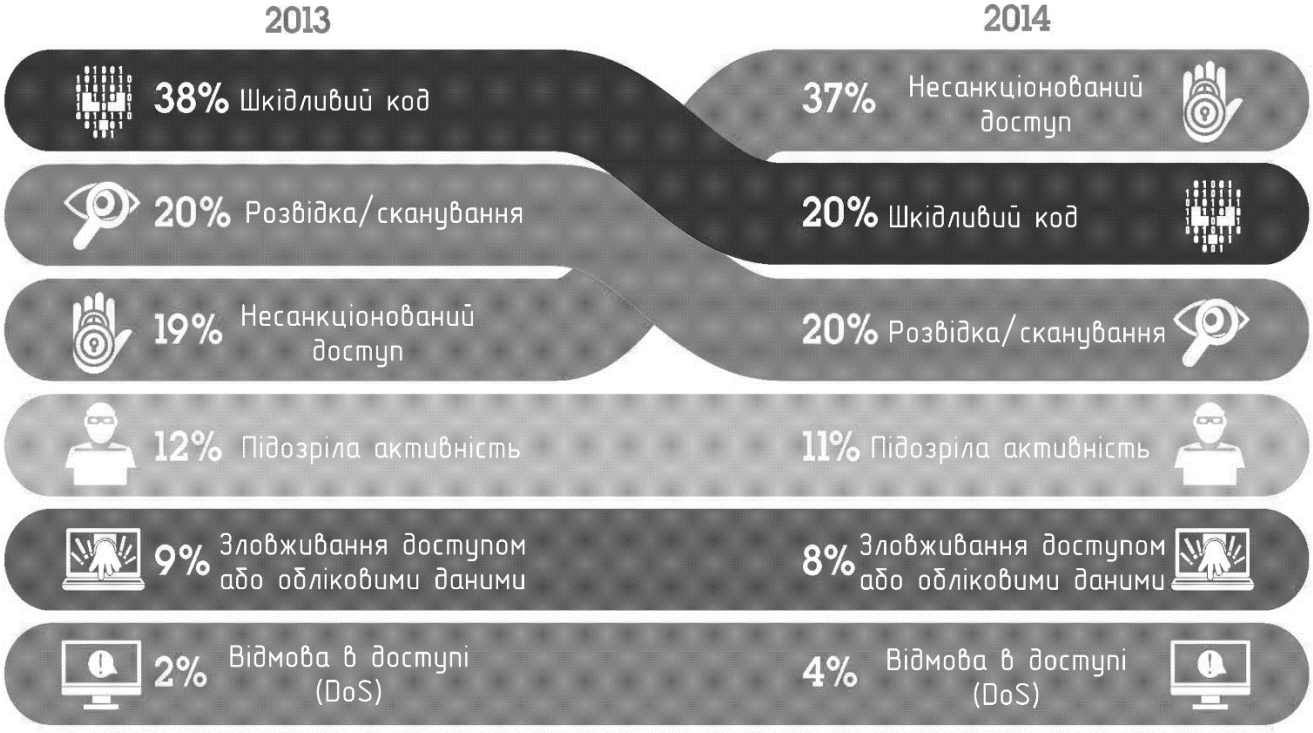

Рис. 2. Найросповсюдженіші категорії інформаційних загроз у 2013–2014 роках*

**Джерело: за даними наукового звіту IBM 2015 Cyber Security Intelligence Index* [6]

Багато хто намагається захистити свої мережі шляхом приховування назви мережі в сигналах (Beacon), що розсилаються точками доступу, і шляхом відключення відповіді на широкомовний запит ESSID (Broadcast ESSID). Ці методи, що відносяться до класу Security through Obscurity, є недостатніми, тому атакуючий все одно бачить бездротову мережу на певному радіоканалі, і все, що йому залишається – це чекати першого авторизованого підключення до такої мережі, тому в процесі такого підключення в ефірі передається

ESSID в незашифрованому вигляді. Після чого така міра безпеки просто втрачає сенс.

Імперсонації авторизованого користувача – серйозна загроза будь-якої мережі, не тільки бездротової. Однак в бездротовій мережі визначити справжність користувача складніше. Звичайно, існують SSID і можна намагатися фільтрувати по MAC-адресам. Але і те й інше передається в ефірі у відкритому вигляді, і те й інше нескладно підробити, а підробивши – як мінімум «зайняти» частину пропускної здатності мережі. Існує помилкове переконання, що імперсонації користувача можлива тільки у разі MAC-аутентифікації або використання статичних ключів, що схеми на основі 802.1x, є абсолютно безпечними. На жаль, це вже давно не так. Більшість механізмів (LEAP) зламуються не складніше WEP. Інші схеми, наприклад, EAP–FAST або PEAP-MSCHAPv2 є більш надійними, але не гарантують стійкості до комплексної атаки, що використовує декілька факторів одночасно.

Завданням атаки «Відмова в обслуговуванні» є або порушення показників якості функціонування мережевих послуг, або повна ліквідація можливості доступу до них для авторизованих користувачів. Для цього, наприклад, мережа може бути завалена «сміттєвими» пакетами (з неправильною контрольною сумою і т.д.), відправленими з легітимної адреси. У разі бездротової мережі відстежити джерело такої атаки без спеціального інструментарію просто неможливо, тому він може перебувати де завгодно. Крім того, є можливість організувати DoS на фізичному рівні, просто запустивши досить потужний генератор перешкод в потрібному частотному діапазоні.

Інструментарій для організації атак на бездротові мережі широко доступний і постійно поповнюється новими засобами, починаючи від всіма відомого AirCrack і закінчуючи хмарними сервісами по розшифровці хешів. Плюс, як тільки отриманий доступ – в хід йде традиційний інструментарій більш високих рівнів.

5. Виток інформації з провідної мережі. Практично всі бездротові мережі в якийсь момент з'єднуються з дротовими. Відповідно, будь бездротова точка доступу може бути використана як плацдарм для атаки. Деякі помилки в конфігурації точок доступу в поєднанні з помилками конфігурації провідної мережі можуть відкривати шляхи для витоків інформації. Найбільш поширений приклад – точки доступу, що працюють в режимі моста (Layer 2 Bridge), підключені в плоску мережу (або мережі з порушеннями сегментації VLAN) та передавальні в ефір широкомовні пакети з дротового сегмента, запити ARP, DHCP, фрейми STP і т.д. Деякі з цих даних можуть бути корисними для організацій атак Man-in-The-Middle, різних Poisoning і DoS атак, та й просто розвідки.

Інший поширений сценарій ґрунтується на особливостях реалізації протоколів 802.11. У випадку, коли на одній точці доступу налаштовані відразу кілька ESSID, широкомовний трафік буде поширюватися відразу в усі ESSID. У результаті, якщо на одній точці налаштована захищена мережа і публічний хот-спот, зловмисник, підключений до хот-споту, може, наприклад, порушити роботу протоколів DHCP або ARP в захищеній мережі. Це можна виправити, організувавши прив'язку ESS до BSS, що підтримується практично всіма виробниками обладнання класу Enterprise (і мало ким із класу Consumer).

6. Особливості функціонування бездротових мереж. Деякі особливості функціонування бездротових мереж породжують додаткові проблеми, здатні впливати в цілому на їх доступність, продуктивність, безпеку і вартість експлуатації. Для грамотного вирішення цих проблем потрібен спеціальний інструментарій підтримки та експлуатації, спеціальні механізми адміністрування та моніторингу, не реалізовані в традиційному інструментарії управління бездротовими мережами.

Оскільки бездротові мережі не обмежуються межами приміщень, як провідні, підключитися до них можна в будь-якому місці і в будь-який час. Через це, багато організацій обмежують доступність бездротових мереж у своїх офісах виключно робочими годинами (аж до фізичного відключення точок доступу). У світлі сказаного, природно припустити, що всяка бездротова активність в мережі в неробочий час повинна вважатися підозрілою і підлягати розслідуванню.

Точки доступу, що дозволяють підключення на низьких швидкостях, дозволяють підключення на більшій дальності. Таким чином, вони представляють додаткову можливість безпечного віддаленого злому. Якщо в офісній мережі, де всі працюють на швидкостях 24/36/54 Мбіт/с раптом з'являється з'єднання на 1 або 2 Мбіт/с – це може бути сигналом, що хтось намагається пробитися в мережу з вулиці.

Оскільки бездротові мережі використовують радіохвилі, якість роботи мережі залежить від багатьох факторів. Найбільш яскравим прикладом є ін-

терференція радіосигналів, здатна значно погіршити показники пропускної спроможності і кількості підтримуваних користувачів, аж до повної неможливості використання мережі. Джерелом інтерференції може бути будь-який пристрій, який випромінює сигнал достатньої потужності в тому ж частотному діапазоні, що і точка доступу: від сусідніх точок доступу у умовах густонаселеного офісного центру, до електромоторів на виробництві, гарнітур Bluetooth і навіть мікрохвильовок. З іншого боку, зловмисники можуть використовувати інтерференцію для організації DoS атаки на мережу.

Чужинці, що працюють на тому ж каналі, що і легітимні точки доступу, відкривають не тільки доступ в мережу, але й порушують працездатність «правильної» бездротової мережі. Крім того, для реалізації атак на кінцевих користувачів і для проникнення в мережу за допомогою атаки Man-In-The-Middle зловмисники часто заглушають точки доступу легітимною мережі, залишаючи тільки одну – свою точку доступу з тим же самим ім'ям мережі.

Крім інтерференції, існують інші аспекти, що впливають на якість зв'язку в бездротових мережах. Оскільки ефір є середовищем із загальним доступом, кожен невірно конфігурований клієнт, або збій антени точки доступу можуть створювати проблеми, як на фізичному, так і на канальному рівні, приводячи до погіршення якості обслуговування інших клієнтів мережі.

Висновки. Бездротові мережі породжують нові класи ризиків і загроз, від яких неможливо захиститися традиційними засобами. Навіть якщо в організації формально заборонений Wi-Fi – це ще не означає, що хто-небудь з користувачів не встановить чужинця і анулює роботу відділу інформаційної безпеки. Крім того, зважаючи на особливості бездротового зв'язку, важливо контролювати не тільки безпеку інфраструктури доступу, але і стежити за користувачами, які можуть стати об'єктом атаки зловмисника або просто можуть випадково або умисно перейти з корпоративної мережі на незахищене з'єднання.

Більшість перерахованих ризиків можуть бути мінімізовані або взагалі зведені до нуля. Для організації безпечної роботи бездротової мережі (включаючи інфраструктуру і користувачів) використовується підхід, що в цілому збігається з підходом «багаторівневої безпеки», що використовується для традиційних провідних мереж (з поправкою на специфіку WLAN).

ЛІТЕРАТУРА

[1]. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1126–97–%D0%BF

[2]. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2010. – №3.

[3]. Корченко О. Г. Системи захисту інформації [Текст] : Монографія / О. Г. Корченко. — К. : НАУ, 2004. – 264 с.

[4]. Практическая атака на беспроводную сеть с WEP шифрованием [Електронний ресурс] // Хабрахабр. – 2010. – Режим доступу до ресурсу: http://habrahabr.ru/post/92681/

[5]. 2015 Cost of Data Breach Study [Електронний ресурс] // Ponemon Institute. – 2015. – Режим доступу до ресурсу: http://www–03.ibm.com/security/infographics/data–breach/#scene2.

[6]. IBM 2015 Cyber Security Intelligence Index [Електронний ресурс] // IBM corporation. – 2015. – Режим доступу до ресурсу: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

[7]. It security risks survey 2014: a business approach to managing data security threats [Електронний ресурс] // KasperskyLab. – 2014. – Режим доступу до ресурсу: http://media.kaspersky.com/en/it_security_risks_survey_2014_global_report.pdf.

REFERENCES

[1]. The concept of technical protection of information in the area of Ukraine, 2011, http://zakon5.rada.gov.ua/laws/show/1126–97–%D0%BF

[2]. Korchenko A.G., Ivanchenko E.V., Kazmirchuk S.V., Analysis and definition of the risk to its interpretation in the field of information security, Zahist ìnformacìï, 2010, №3.

[3]. Korchenko O.G. , Information protection systems, Monograph, K: NAU , 2004, 264 p.

[4]. Practical attack on a Wireless Network with WEP Encryption, Habrahabr, 2010, http://habrahabr.ru /post/ 92681/

[5]. 2015 Cost of Data Breach Study, Ponemon Institute, 2015, http://www–03.ibm.com/security /infographics / data–breach/#scene2

[6]. IBM 2015 Cyber Security Intelligence Index, IBM corporation, 2015, http://public.dhe.ibm.com /common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

[7]. It security risks survey 2014: a business approach to managing data security threats, KasperskyLab, 2014, http://media.kaspersky.com/en/it_security_risks_survey_2014_global_report.pdf.

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СТАНДАРТА IEEE 802.11

На сегодняшний день беспроводные технологии интенсивно развиваются и внедряются в общественную жизнь, постепенно заменяя проводные. Они удобны в использовании, имеют низкую стоимость развертки – это основные преимущества беспроводных систем. Технология стандарта IEEE 802.11, называемая также Wi-Fi является самой популярной на сегодня технологией беспроводной связи. Количество пользователей ежедневно увеличивается. Однако системы защиты информации данных в этой технологии, во-первых, уступают системам защиты проводных сетей из-за существования особенностей угроз в беспроводных сетях, во–вторых недостаточно исследованы и проверены. Таким образом, проблема определения и анализа угроз информационной безопасности в сетях стандарта IEEE 802.11 является актуальной на сегодняшний день. Проводя анализ мы опирались на исследования зарубежных ученых и практикующих компаний, занимающихся изучением угроз и разработкой систем их предотвращения. Исследование данного вопроса дает возможность определить и классифицировать возможные угрозы и, в дальнейшем, модернизировать существующие или разработать новые методы и меры информационной безопасности.

Ключевые слова: компьютерные сети, стандарт IEEE 802.11, Wi-Fi, угрозы информационной безопасности, защита информации.

ANALYSIS INFORMATION SECURITY THREATS NETWORK STANDARD IEEE 802.11

Nowadays wireless technologies are constantly evolving and penetrate the social life, gradually replacing the wire. Easy to use, lower cost of installation – are the main advantages of wireless systems. The technology of standard IEEE 802.11, also known as Wi-Fi is today's most popular wireless technology. The number of users increases daily. However, information security data in this technology, first, inferior protection systems wired networks because of the existence of threats features wireless networks, and secondly insufficiently researched and tested. So the problem identification and analysis of threats to information security network standard IEEE 802.11 is relevant today. By analyzing threats we relied on foreign research scientists and practitioners companies in this area involved in the study of development threats and prevent them. Researches of the issue makes it possible to identify and classify potential threats and, subsequently, upgrade existing or develop new effective methods and measures against threats to information security.

Keywords: computer network, IEEE 802.11, Wi-Fi, threats to information security, information security.

Мехед Дмитро Борисович, кандидат педагогічних наук, доцент кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.
Мехед Дмитрий Борисович, кандидат педагогических наук, доцент кафедры математического моделирования и информационной безопасности Черниговского национального технологического университета.
Mekhed Dmitry, PhD, associate professor of mathematical simulation and information security department, Chernihiv National University of Technology.
E–mail: tkach_ym@ukr.net

Ткач Юлія Миколаївна, кандидат педагогічних наук, доцент, завідувач кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.
Ткач Юлия Николаевна, кандидат педагогических наук доцент, заведующая кафедрой математического моделирования и информационной безопасности Черниговского национального технологического университета.
Tkach Yulia, PhD, associate professor, head of the department of mathematical simulation and information security, Chernihiv National University of Technology.
E–mail: tkach_ym@ukr.net

Базилевич Володимир Маркович, старший викладач кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.
Базилевич Владимир Маркович, старший преподаватель кафедры математического моделирования и информационной безопасности Черниговского национального технологического университета.
Bazylevych Volodymyr, senior lecturer of mathematical simulation and information security department, Chernihiv National University of Technology.
E–mail: tkach_ym@ukr.net

Петренко Тарас Анатолійович, старший викладач кафедри математичного моделювання та інформаційної безпеки Чернігівського національного технологічного університету.
Петренко Тарас Анатолиевич, старший преподаватель кафедры математического моделирования и информационной безопасности Черниговского национального технологического университета.
Petrenko Taras, senior lecturer of mathematical simulation and information security department, Chernihiv National University of Technology.
E–mail: tkach_ym@ukr.net