УДК 004.9

К. Ю. Чернобай, С. В. Грибков
Національний університет харчових технологій,
кафедра інформаційних систем

АНАЛІЗ ТА ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ ЗАХИСТУ КОМЕРЦІЙНИХ БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖ WI-FI

Досліджено проблеми захисту конфіденційної та комерційної інформації з використанням бездротових локальних мереж, побудованих за технологією Wi-Fi. Розглянуто типи загроз та атак, спрямованих на бездротові локальні мережі, а також заходи щодо їх усунення та підвищення якості безпеки.

Ключові слова: бездротова локальна мережа, захист інформації, Wi-Fi технологія.

In this paper, the research of problems of protection of confidential and commercial information with the use of wireless local networks built on the technology of Wi-Fi was conducted. The types of threats and attacks aimed at wireless LANs, as well as methods for their elimination and improving the quality of security are considered.

Keywords: wireless LAN, data protection, Wi-Fi technology.

Вступ

Вже більше століття людство користується бездротовими засобами передавання інформації, що за останнє десятиріччя все більше розвивається та удосконалюється завдяки появі нових інформаційних технологій та пристроїв для удосконалення передавання інформації. Сьогодні особливого значення в бездротових технологіях набули бездротові локальні мережі (англ. Wireless Local Area Network – WLAN), адже вони дають змогу підключатися до локальної мережі без використання мережевих кабелів та використовувати мобільні пристрої, що дозволяє користувачу не прив’язуватися до конкретного місця, а бути в межах дії такої мережі. Великий поштовх розвитку цього напряму надало збільшення кількості збільшення користувачів мережі Інтернет. Починаючи з середини першого десятиліття XXI століття, кількість користувачів бездротового Internet-сервісу сягнула десятків мільйонів [1].

Найбільшої популярності набули бездротові локальні мережі, побудовані на базі технології Wi-Fi (Wireless Fidelity – перекладається як “бездротова якість” або “бездротова точність”) та відповідає стандарту бездротової мережі 802.11x, що входить до стандартів локальних мереж IEEE802.x, а також використовує фізичний та канальний рівні OSI (Open System Interconnection). Усі сучасні мобільні пристрої можуть працювати за цим стандартом.

Сьогодні не можливо уявити собі без точок доступу Wi-Fi офісні та торгові центри, готельні комплекси, місця проведення комерційних та громадських заходів. Як правило, наявність таких мереж у приміщеннях різного призначення забезпечують їх власникам більшу аудиторію з клієнтів та орендарів, адже все більше людей потребують постійного доступу до мережі Інтернет для особистого користування та ведення бізнесу.

Побудова та використання комерційних бездротових локальних систем на корпоративному рівні з кожним роком зростає, тому що стає стратегічним засобом для підвищення продуктивності (співробітники отримують постійний доступ до корпоративної інформації, швидше отримують

накази, розпорядження та новини), підвищується якість обслуговування клієнтів (є можливість миттєво реагувати на замовлення, пропозиції чи скарги по всій вертикалі управління) та забезпечує конкурентні переваги (підвищує швидкість обміну інформації, що впливає на швидкість та якість прийняття рішення).

Незважаючи на багато переваг бездротових локальних мереж, при їх впровадженні та використанні зростає загроза атак кіберзлочинців на їх користувачів та інфраструктуру загалом, а втрата особистої чи комерційної інформації може привести до фінансових збитків всієї компанії.

Аналіз досліджень та публікацій

Останнім часом чимало публікацій присвячено проблемам захисту інформаційних систем та мереж, серед яких доцільно виділити ті, в яких розглядають захист бездротових мереж, тому що з їх поширенням все гострішими стають проблеми їх безпеки, адже допущена під час настроювання мережі та введення елементів захисту навіть найменша помилка може призвести до таких небажаних наслідків, як створення умов для проникнення вірусів, несанкціонований доступ та модифікація корпоративних даних кіберзлочинцями, які постійно вдосконалюють способи та підходи для пошуку вразливостей та здійснення пошкоджень. У роботі [2] розглянуто сучасний стан засобів захисту інформації в бездротових мережах на основі груп протоколів IEEE 802.11, а також розроблення комплексу заходів для підвищення безпеки на основі практичних послідовних рекомендацій. Автори роботи [3] розглянули основні ризики використання бездротових мереж. У праці [4] висвітлено основні аспекти інформаційної безпеки в комп'ютерних мережах та інформаційно-обчислювальних системах. У публікації [5] висвітлено основні особливості захисту інформаційних ресурсів у корпоративних мережах та системах, а також запропоновано підхід до їх оцінювання. Незважаючи на чималу кількість публікацій за цим напрямом, актуальним завданням є дослідження проблем захисту комерційних бездротових локальних мереж Wi-Fi та підходів до їх усунення, адже втрата комерційної інформації чи порушення роботи інфраструктури підприємства призводить до колосальних збитків.

Формулювання цілі статті

Необхідно дослідити проблеми бездротових локальних мереж, побудованих за технологією Wi-Fi, та підходи до їх вирішення, а також розглянути типи загроз та атак, спрямованих на бездротові локальні мережі, і заходи щодо їх усунення та підвищення якості безпеки.

Особливості мереж Wi-Fi та складнощі захисту

Бездротові мережі Wi-Fi відрізняються від кабельних мереж на фізичному (Phy) і частково на канальному (MAC) рівнях моделі взаємодії OSI. Фізичним рівнем Wi-Fi є радіоканал, що характеризує параметри фізичного середовища передавання даних. У стандарті IEEE 802.11x використано два методи передавання сигналу інформації, що відрізняються за способом модуляції, але використовують однакову технологію розширення спектра, а саме: прямої послідовності (DSSS – Direct Sequence Spread Spectrum); частотних стрибків (FHSS – Frequency Hopping Spread Spectrum). Канальний рівень здійснює управління доступом до середовища передавання та забезпечує пересилання кадрів між будь-якими двома пристроями бездротової мережі. На канальному рівні в Wi-Fi мережі у підрівні MAC використано напівдуплексний режим передавання даних. Як методи доступу до середовища передавання даних використано методи множинного доступу з контролем несучої інформації і попередженням колізій або зіткнень (CSMA / CA – Carrier Sense Multiple Access / Collision Avoidance).

Бездротова мережа Wi-Fi може працювати в двох режимах: режим клієнт/сервер, що характеризується наявністю як мінімум однієї точки доступу AP (Access Point) та певною кількістю

кінцевих станцій; режим точка-точка, де зв'язок між станціями встановлено напряму без реалізації спеціальних точок доступу.

Технологія бездротової передачі даних має такі переваги:

- можливість розгортання мережі без використання фізичного кабелю зв'язку, що зменшує вартість організації та подальшого розширення мережі, а також важливо в місцях, де відсутня можливість прокладання кабелю;
- надання доступу до локальної мережі та мережі Інтернет через використання різних мобільних пристроїв, зокрема комп'ютерів та ноутбуків;
- широке поширення на ринку Wi-Fi-пристроїв, а також їх гарантована сумісність завдяки обов'язковій сертифікації обладнання Wi-Fi Alliance;
- низький рівень випромінювання Wi-Fi-пристроями в момент передавання даних (у 10 разів менше, ніж у мобільного телефону).

Бездротові мережі на базі протоколів IEEE 802.11 мають такі складнощі захисту порівняно з кабельними комп'ютерними мережами [1]: для підключення до бездротової мережі не потрібен фізичний доступ до кабелю мережі, а достатньо перебувати у робочій зоні покриття маршрутизатора з використанням обладнання того типу, на якому побудовано мережу; передача даних по бездротовому каналу може бути перехоплена і оброблена навіть без пристрою доступу, спеціальними апаратними або програмними засобами.

Стандартні заходи захисту інформації у мережі Wi-Fi

До стандартних заходів захисту належать програмні й апаратні засоби, призначені для вирішення таких завдань: запобігання несанкціонованому підключенню до бездротової мережі сторонніх користувачів; запобігання доступу до заборонених ресурсів вже підключених користувачів; збирання та аналіз інформації у випадку несанкціонованого доступу для запобігання наступному подібному інциденту.

Переважно використовують такі стандартні заходи з підвищення рівня захисту бездротової мережі [2]:

- заміна ключів доступу на більш комплексні; зміна протоколів шифрування на сучасніші і стійкіші до злому методом перебору;
- відключення технології WPS; відключення транслювання імені SSID; включення фільтрації MAC-адрес;
- установка програмного забезпечення для протоколювання доступу користувачів до ресурсів усередині мережі.

Окремими засобами є заходи, спрямовані на протидію соціальним методам злому, таким, як доступ легальними технічними заходами з нелегальними цілями або підміною особи доступу через віддаленість терміналу.

Сучасні апаратні засоби для бездротових мереж, що відповідають стандарту IEEE 802.11, забезпечують чотири рівні безпеки: фізичний, ідентифікатор набору служб (SSID – Service Set Identifier), ідентифікатор управління доступом до середовища (MAC ID – Media Access Control ID) і шифрування.

Необхідно зазначити, що своєчасне оновлення та використання основних пристроїв при побудові WLAN забезпечить підвищення ефективності захисту, адже в них використовуються нові стандарти безпеки WPA та WPA2 (Wi-Fi Protected Access). Технологія WPA прийшла на заміну технології WEP (Wired Equivalent Privacy. Вона поєднує такі технології: стандарти 802.1X; фреймворк аутентифікації EAP (Extensible Authentication Protocol, Розширюваний Протокол Аутентифікації), що використовується для вибору методу аутентифікації, передачі ключів і обробки цих ключів модулями EAP; протокол динамічних ключів TKIP (Temporal Key Integrity Protocol); перевірка цілісності повідомлень MIC (Message Integrity Check), що використовується для запобігання перехопленню пакетів даних, зміст яких може бути змінено, а модифікований пакет

знову переданий по мережі. Стандарти 802.11i та WPA надійно реалізують високий рівень захисту у бездротових мережах у разі правильного їх створення.

Використання стандартів безпеки WPA та WPA2 усуває більшість проблем, але важливо не забувати про сучасніші технологій Intrusion Prevention System (IPS), що запобігають вторгненню в мережі доступу Wi-Fi.

Рекомендації для забезпечення безпеки у мережі Wi-Fi

Для підвищення надійного захисту у мережі Wi-Fi необхідно дотримуватися таких вимог [2, 6]:

- при створенні на фізичному рівні необхідно обмежити доступ до мережі;
- оптимального налаштування параметрів конфігурації механізмів аутентифікації та шифрування для забезпечення ефективності роботи, надійності та безпеки мережі;
- використання програмних засобів захисту пристроїв користувача та контролю усієї мережі;
- постійний моніторинг мережі для запобігання створенню в корпоративній мережі несанкціонованих точок доступу чи підключення;
- використання VPN (Virtual Private Network) для усіх пристроїв корпоративних клієнтів, що забезпечить захист при використанні різних точок доступу, що не належать корпоративної інфраструктурі, а також широкі можливості з вибору алгоритмів аутентифікації, шифрування та перевірки цілісності потоку даних[12];
- формування політики безпеки та складання відповідної документації;
- проведення інструктажів та семінарів для ознайомлення корпоративних робітників з основами правил безпеки під час роботи з офісною технікою та засобами зв'язку, зокрема і мережі Інтернет.

Протягом багатьох років одним з надійних засобів захисту комп'ютерних мереж залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори). Вони бувають апаратні та програмні, що дає змогу забезпечити високий рівень захисту. Мережевий екран є одним з декількох механізмів, що використовуються для управління і спостереження за доступом до мережі з метою її захисту [7], зокрема до бездротових мереж. Крім цього, використання комплексних засобів захисту, що містять засоби антивірусної безпеки та мережевих екранів, гарантує дуже надійний рівень захисту.

Висновок

У результаті проведеного дослідження є можливість стверджувати, що використання сучасного обладнання та апаратно-програмних засобів можуть забезпечити відповідний рівень захисту комерційних бездротових локальних мереж Wi-Fi. Але необхідно зазначити, що розглянуті в роботі заходи дають змогу захистити від так званого "силового" методу проникнення до інфраструктури з мережею Wi-Fi, отже, тільки комбінуванням різних методів і підходів можна забезпечити захист від несанкціонованого доступу. Необхідно зазначити також, що найбільше втрат інформації та порушень безпеки відбуваються внаслідок необізнаності та недотримання елементарних правил безпеки корпоративними співробітниками. Однією з таких помилок може бути використання в комерційних цілях публічних точок доступу до мережі Інтернет, неперевіреної техніки, що належить третім особам, чи підозрілого програмного забезпечення. На думку авторів, цікавим напрямом подальшого розвитку є впровадження та використання біометричних систем безпеки через мобільні пристрої та додатки.

1. Беспроводные сети Wi-Fi [Електронний ресурс] / А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов, А. В. Бобков, Д. Н. Чирков, В. А. Платонов. – Режим доступу до ресурсу : http://www.intuit.ru/department/ network/wifi/. 2. Визавитин О. И. Практика защиты информации в Wi-Fi сетях на основе современных программно-аппаратных средств // Молодой ученый. – 2016. – № 5. – С. 182–184. 3. Бандурян А. Анализ угроз для беспроводных сетей [Електронний ресурс] / Арсен Бандурян // Компьютерное обозрение, № 12 (723), 2010 г. – Режим доступу до ресурсу :

http://ko.com.ua/analiz_ugroz_dlya_besprovodnyh_setej_49014. 4. Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере. – М.: Форум, 2009. – 368 с. 5. Кононова В. О., Грибков С. В., Харкянен О. В. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, С. В. Грибков, О. В. Харкянен // Вісник Нац. ун-ту "Львівська політехніка". – 2014. – № 806. – С. 99–105. 6. Как защитить беспроводную сеть wi fi [Електронний ресурс] // Защита информации. – 2003. – Режим доступу до ресурсу: http://infoprotect.net/protect_network/kak_zasccitityy_setyy_wi_fi. 7. Защита сетевого периметра: наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений [Текст] / С. Норткатт [и др.]; науч. ред. Н. И. Алишов. – К. ; М. ; СПб. : DiaSoft, 2004. – 664 с. 12. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М. : ДМК, 2000. – 445с.

УДК 621.398

П. В. Мокренко, Б. І. Задерецький
Національний університет "Львівська політехніка",
кафедра комп'ютеризованих систем автоматики

КОДОІМПУЛЬСНІ СИСТЕМИ ТЕЛЕВИМІРЮВАННЯ (будова, принцип роботи, особливості)

Розглянуто побудову та принцип роботи багатоканальних кодоімпульсних систем телевимірювання та ні відмінності від аналогових систем. Показано переваги кодоімпульсних систем телевимірювання та їхні особливості.

Ключові слова: квантування, кодування, частотний сигнал, первинний перетворювач, швидкодія.

It is in-process considered construction and principle ofwork of the multichannel digital systems of telemetering and their difference from the analog systems. Shown advantages of the digital systems of telemetering and their feature.

Keywords: quantum, code, frequency signal, primary transformer, speed.

Вступ

Вимоги забезпечення високої точності, швидкодії і достовірності передачі інформації та уведення її у цифрові обчислювальні (ЦОМ) та керуючі (ЦКМ) машини, з одного боку, та необхідність обробки великих масивів інформації для вирішення інших завдань науки і техніки, зокрема пов'язаних з освоєнням космосу, морів і океанів, з іншого – наклало великий відбиток на розвиток теорії і практики систем телемеханіки [1–5].

У системах телемеханіки поширено цифрові методи вимірювання та обробки інформації, внаслідок чого аналогові системи стали витіснятися цифровими багатоканальними, які економічно вигідніші в експлуатації.

Досягнення мікроелектроніки зробили можливою побудову систем телемеханіки четвертого покоління, які приходять на зміну системам третього покоління, дають змогу вирішувати складні завдання, що пов'язані з обробкою інформації з метою маштабування величин, лінеаризації шкал, виконання різних функціональних перетворень і т. п.