Аналіз проблем захисту комерційних бездротових локальних мереж Wi-Fi та підходів їх усунення

Катерина Чорнобай[1], Сергій Грибков[2]

1. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: kat.chornobai@gmail.com

2. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: sergio_nuft@ukr.net

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.

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

Вступ

Вже більше століття людство користується бездротовими засобами передачі інформації, що за останнє десятиріччя все більше набирає розвитку та удосконалюється за рахунок появи нових інформаційних технологій та пристроїв для удосконалення передачі інформації. Сьогодні особливу нішу в бездротових технологій набули бездротові локальні мережі (англ. Wireless Local Area Network; Wireless LAN; WLAN), адже вони дозволяють підключатися до локальної мережі без використання мережив кабелів та використовувати мобільні пристрої, що дозволяє користувачу не прив'язуватися до конкретного місця, а достатньо бути в межах дії такої мережі. Великий поштовх розвитку даного напрямку забезпечило збільшення користувачів мережі Інтернет. Починаючи з середини першого десятиліття XXI століття рахунок користувачів бездротового Internet-сервісу пішов на десятки мільйонів [1].

Найбільшу популярність 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 даним стандартом.

На сьогоднішній день 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 в приміщеннях різного призначення забезпечують їх власникам більшу аудиторію з клієнтів та орендаторів, адже все більше людей потребують простійного доступу в мережу 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 впроваджені та використанні зростає загроза атак кіберзлочинців на їх користувачів та інфраструктуру в цілому, а втрата особистої чи комерційної інформації може привести до фінансових збитків всієї компанії.

Враховуючи все вище сказане, актуальною задачею є дослідження проблем захисту комерційних бездротових локальних мереж Wi-Fi та підходів їх усунення, адже втрата комерційної інформації чи порушення роботи інфраструктури підприємства призводить у наш час до колосальних збитків.

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 передачі даних. У стандарті IEEE 802.11x використовуються два методи передачі сигналу інформації, що відрізняються за способом модуляції, але використовують однакову технологію розширення спектру, а саме: прямої послідовності (DSSS – Direct Sequence Spread Spectrum); частотних стрибків (FHSS – Frequency Hopping Spread Spectrum). Канальний рівень здійснює управління доступом до середовища передачі та забезпечує пересилання кадрів між будь-якими двома пристроями бездротової мережі. На канальному рівні в Wi-Fi мережі у підрівні MAC використовується напівдуплексний режим передачі даних. В якості методів доступу до середовища передачі даних використовуються 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 характерна як мінімум однією точкою доступу AP (Access Point) та певною кількістю кінцевих станцій; режим точка-точка, де зв'язок між станціями встановлюється на пряму без реалізації спеціальних точок доступу.

Особливість бездротових мереж на базі протоколів IEEE 802.11 призводить до наступних складнощів захисту, в порівнянні з кабельними комп'ютерними мережами[1]: для підключення до бездротової мережі, не потрібно фізичний доступ до кабелю мережі, а

достатньо перебувати у робочій зоні покриття маршрутизатору з використанням облад-нання того типу, на якому побудована мережа; 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 відносяться програмні і апаратні засоби, призначені для вирішення наступних завдань: запобігання несанкціонованого підключення до бездротової мережі сторонніх користувачів; запобігання доступу до заборонених ресурсів вже підключених користувачів; збір та аналіз інформації у випадку несанкціонованого доступу, для запобігання наступного подібного інциденту.

Як правило, в більшості випадків виконуються наступні стандартні заходи по підвищенню рівня захисту бездротової мережі [2]: заміна ключів доступу на більш комплексні; зміна протоколів шифрування на більш сучасні і стійкі до злому методом перебору; 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 рівня безпеки: фізичний, ідентифікатор набору служб (SSID – Service Set Identifier), ідентифікатор управління доступом до середовища (MAC ID – Media Access Control ID) і шифрування.

Необхідно відмітити, 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 в собі наступні 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 перехоплення 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 при правильному їх створенні.

Рекомендації для забезпечення безпеки у мережі Wi-Fi

Для підвищення надійного захисту у мережі Wi-Fi необхідно дотримуватися наступного [2-3]: 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 уникнення створення 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; проведення інструктажів та семінарів для ознайомлення корпоративних робітників з основами правил безпеки при роботі з офісною технікою та використання засобів зв'язку, зокрема і мережі Інтернет.

Висновок

В 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 дозволяють захистити від так званого «силового» методу проникнення у інфраструктуру з мережею Wi-Fi, таким чином тільки комбінування різних методів і підходів можуть забезпечити захист від несанкціонованого доступу. Необхідно відзначити також, що найбільший відсоток втрат інформації та порушень безпеки відбувається за рахунок 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 напрямком подальшого розвитку є впровадження та використання біометричних систем безпеки через мобільні пристрої та додатки.

Література

[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] Візавітін О. І. Практика захисту інформації в Wi-Fi мережах на основі сучасних програмно-апаратних засобів // Молодий вчений. – 2016. – №5. – С. 182 – 184.

[3] Как защитить беспроводную сеть wi fi [Електронний ресурс] // Защита информации. – 3003. – Режим доступу до ресурсу: http://infoprotect.net/protect_network/kak_zasccitityy_setyy_wi_fi.