УДК 004.056
П.С.Шолом, О.І. Міскевич, К.В. Мельник
Луцький національний технічний університет

АНАЛІЗ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ

Шолом П.С., Міскевич О.І., Мельник К.В. Аналіз загроз та оцінка ризиків безпеки інформації в безпровідних мережах.*Здійснено аналіз основних загроз безпеки інформації у безпровідних мережах та проведено їх класифікацію. Виявлено ризики, які необхідно усунути у корпоративних системах, в якихвикористовують безпровідні мережі.*
Ключові слова: *оцінка ризиків, загроза, безпровідні мережі*
Рис. 2, Літ. 6

Шолом П.С., Мискевич О.И., Мельник К.В. Анализ угроз и оценка рисков безопасности информации в беспроводных сетях.*Осуществлен анализ основных угроз безопасности информации в беспроводных сетях и проведена их классификация. Выявлены риски, которые необходимо устранить в корпоративных системах, в которых применяются беспроводные сети.*
Ключевые слова:*оценка рисков, угроза, беспроводные сети*
Рис. 2, Лит. 6

Sholom P., MiskevichO., Melnik K. Analysis of threatsand assessment of risk of information security in wireless networks. *Analysis of the major threats of information security in wireless networks and their classification are realized. Risks that need to be removed in enterprise systems that use wireless network are discovered.*
Keywords*: risk assessment, threat, wireless networks*
Fig.2, Ref. 6

Постановка проблеми.Діючі міжнародні стандарти [1-3]рекомендують методологію оцінки та управління інформаційними ризиками як інструмент дослідження загроз інформаційній безпеці в інформаційних системах. Ризик –це фактор, що відображає можливий збиток організації в результаті реалізації загрози інформаційній безпеці. Мета оцінки ризиків полягає у визначенні характеристик ризиків корпоративної інформаційної системи та її ресурсів [4], в результаті чого стає можливим вибір засобів, що забезпечують бажаний рівень інформаційної безпеки системи, зокрема безпровідної комп'ютерної мережі.

Безпровідні мережі поряд з очевидними перевагами мають і певні ризики безпеки. Повсюдне розгортання Wi-Fi мереж призвело до появи цілого покоління хакерів, які спеціалізуються на розробці нових способів злому корпоративних інфраструктур та здійсненні атак на користувачів. Для бізнес-сегменту очевидною є вигода від використання безпровідних мереж та мобільність, яка надається такою мережею. Однак, до тих пір, поки питання безпеки для IT-директорівзалишається не до кінця зрозумілим, думки організацій радикально різняться: від орієнтації на Wi-Fi-мережідля своїх ключових бізнес-процесів до повної заборони використання безпровідних пристроїв у мережах організації.

Аналіз останніх досліджень та публікацій.Проблема гарантуваннябезпеки інформації в безпровідних мережах є предметом досліджень багатьох вітчизняних та зарубіжних науковців. Чимало досліджень присвячено шляхам забезпечення захисту від несанкціонованого доступу до безпровідних мереж та аналізу і управлінню ризиками інформаційної безпеки у таких мережах. Цим питанням займались Щербаков В.Б., Єрмаков С.А., Гордейчик С.В., Дубровин В.В., Владимиров А.А. Праці названих вище авторів сприяли накопиченню і систематизації знань, узагальненню досвіду щодо особливостей проектування, розгортання і адміністрування безпровідних мереж в умовах необхідності забезпечення конфіденційності, цілісності та доступності оброблюваної інформації.

Метою роботи єаналіз основних загроз безпеки інформації у безпровідних мережах, проведення їх класифікації та виявлення ризиків, які необхідно усунути у корпоративних системах, де застосовуються безпровідні мережі.

Виклад основного матеріалу.Сучасний ринок вимагає мобільності та постійності зв'язку для ефективної конкуренції. Стільникові телефони та персональні цифрові секретарі (PDA – PersonalDigitalAssistant) стали обов'язковими для збільшення продуктивності та покращення конкурентоспроможності. Ноутбуки, нетбуки забезпечують користувачам мобільність роботи будь-де та будь-коли. Із їхньою появою постало питання щодо безпровідної передачі даних та з'єднання терміналів замість базових провідних мереж. Однією з найбільш відомих безпровідних технологій стала Wi-Fi (WirelessFidelity) безпровідна LAN (WLAN). Ця технологія базується на методі передачі інформації за допомогою радіохвиль для з'єднання терміналів в мережу із гарантованою пропускною здатністю – 11-54 Мб/с, що працює в діапазоні частот 2,4-5 ГГц.

Мережеві компоненти стають більш вразливими до дій зловмисників та ненавмисних помилок у політиці безпеки підприємства тому, що роль корпоративної мережі продовжує зростати, забезпечуючи з'єднання як внутрішнього, такі зовнішнього зв'язку у формі додатків Internet, Intranet та Extranet. Мережева безпека стала критичнішим елементом планування та виконання корпоративної мережі.

Традиційні провідні мережі використовують для передачі даних кабель, яке є «контрольованим» середовищем, щозахищене будівлями та приміщеннями, в яких він прокладений. Зовнішній трафік, що входить у захищений сегмент мережі, фільтрується брандмауером і аналізується системами IDS/IPS. Для того, щоб отримати доступ до такого сегменту провідної мережі, зловмисникові необхідно подолати або систему фізичної безпеки будівлі, або брандмауер [5].

Убезпровідних мережах використовується відкрите середовище з практично повною відсутністю контролю. Забезпечити еквівалент фізичної безпеки провідних мереж в цьому випадку просто неможливо. Безпровідний сегмент мережі стає доступним з іншого поверху або ззовні: єдиною фізичною границею безпровідної мережі є рівень самого сигналу. Тому, на відміну від провідних мереж, де місце підключення користувача відомо, під'єднатися до безпровідної мережі можливо із будь-якої точки з рівнем сигналу достатньої потужності. При цьому наявність приймача, що працює тільки на прослуховування, взагалі неможливо визначити.

Оскільки радіосигнали мають широкомовну природу, не обмежені стінами будівель і доступні всім приймачам, місце розташування яких складно або взагалі неможливо зафіксувати, зловмисникам особливо легко та зручно атакувати безпровідні мережі.

Безпровідні технології, що працюють без фізичних і логічних обмежень своїх провідних аналогів, піддають мережеву інфраструктуру та користувачів значним ризикам. До таких ризиків відносять: наявність «чужинця», нефіксована природа зв'язку, вразливість мереж і пристроїв, нові загрози та атаки, витік інформації з провідної мережі, особливості функціонування безпровідних мереж. Далі здійснено аналіз перелічених ризиків безпеки інформації для забезпечення безпечного функціонування безпровідних мереж.

Ризик 1 – «чужинці» (rogues). «Чужинцями» називаються пристрої, що надають можливість неавторизованого доступу до корпоративної мережі, часто в обхід механізмів захисту, що визначені корпоративною політикою безпеки. В основному – це самовільно встановлені точки доступу (ТД) [5]. Статистика вказує на чужинців як на причину більшості зломів безпровідних мереж організацій. Навіть якщо організація не використовує безпровідний зв'язок, вважати себе в результаті такої заборони захищеним від безпровідних атак чи можливого проникнення (навмисно або випадково) чужинців не можна (рис. 1).Крім точок доступу в ролі чужинця може виступити домашній маршрутизатор з підтримкою Wi-Fi, програмна точка доступу Soft AP, ноутбук з одночасно увімкненимпровідним і безпровідним інтерфейсами, сканер, проектор і т.п.

*Рис. 1.***Варіант можливого проникнення чужинця**

*Ризик 2 – нефіксована природа зв'язку.*Безпровідні пристрої можуть змінювати точки підключення до мережі прямо в процесі роботи. У цьому випадку можуть відбуватися «випадкові

асоціації», коли, наприклад, ноутбук з Windows XP (операційна система (ОС) досить довірливо ставиться до всіх безпровідних мереж) або просто некоректно сконфігурованийбезпровідний клієнт автоматично асоціюється і підключає користувача до найближчої безпровідної мережі. Такий механізм дозволяє зловмисникам «перемикати на себе» користувача, який нічого не підозрює, для подальшого сканування вразливостей, фішингу або атак типу Main-in-The-Middle [5, 6]. Крім того, якщо користувач одночасно підключений і до провідної мережі, то він стає зручною точкою входу.Багато користувачів ноутбуків, оснащених Wi-Fiта інтерфейсами для провідних мереж, у разі неякісної роботиостанньої можуть перемикатися на найближчі зони доступу. (або ж ОС робить це для них автоматично, наприклад, в разі відмови провідної мережі). У такій ситуації забезпечення мережевої безпеки ІТ-відділом буде безрезультатним.

Мережі Ad-Hoc (однорангові з'єднання між безпровідними пристроями без участі ТД) дозволяють швидко відправити файл одержувачу або роздрукувати документ на віддаленому принтері з картою Wi-Fi. Такий спосіб організації мережі не підтримує більшість необхідних методів забезпечення безпеки, надаючи зловмисникам легкий шлях до злому комп'ютерів користувачів.

Ризик 3 – вразливості мереж і пристроїв. Деякі мережеві пристрої можуть бути більш вразливі по відношенню до інших. Вони можуть бути неправильно сконфігуровані, використовувати слабкі ключі шифрування або методи аутентифікації з відомими вадами. В першу чергу зловмисники атакують саме їх.

Одна некоректно сконфігурована ТД (в т.ч. чужинець) може послужити причиною злому корпоративної мережі. Налаштування за замовчуванням більшості ТД не включають аутентифікаціючи шифрування або ж використовують статичні ключі, що записані в інструкції і тому є загальновідомими. У поєднанні з невисокою ціною цих пристроїв даний фактор значно ускладнює завдання стеження за цілісністю конфігурації безпровідної інфраструктури та рівнем її захисту. Співробітники організації можуть самовільно приносити ТД і підключати їх до мережі. При цьому малоймовірно, що вони приділять достатньо уваги їх грамотній та безпечній конфігурації і узгодять свої дії з ІТ-відділом. Саме такі ТД і створюють найбільшу загрозу провідним табезпровідним мережам.

Некоректно сконфігурованібезпровідні клієнти являють більшу загрозу, ніж некоректно сконфігуровані ТД. Оскільки клієнти на підприємстві можуть дуже часто змінюватись, то під час підключення в мережуїхзазвичайспеціально не конфігурують з метою мінімізації безпровідних ризиків або задовольняються установками за замовчуванням (які не можуть вважатися безпечними). Саме в таких випадках система стає вразливою для хакерів, забезпечуючи зручну точку входу для сканування мережі та поширення в ній шкідливого програмного забезпечення (ПЗ).Зловмисникам доступні спеціальні засоби для злому мереж, що ґрунтуються на стандарті шифрування WEP. Вони використовують вразливості даного алгоритму, пасивно збираючи статистику трафіку в безпровідній мережі до тих пір, поки отриманих даних не виявиться достатньо для відновлення ключа шифрування. З використанням останнього покоління засобів злому WEP, що застосовують методи ін'єкції трафіку, термін злому коливається від 15 хвилин до 15 секунд [6].

Ризик 4 – нові загрози та атаки. Безпровідні технології породили нові способи реалізації старих загроз, а також деякі нові, до цього були неможливими в провідних мережах (рис. 2). У всіх випадках боротися зі зловмисником стало набагато важче, так як неможливо ні відстежити його фізичне місце розташування, ні ізолювати від мережі.

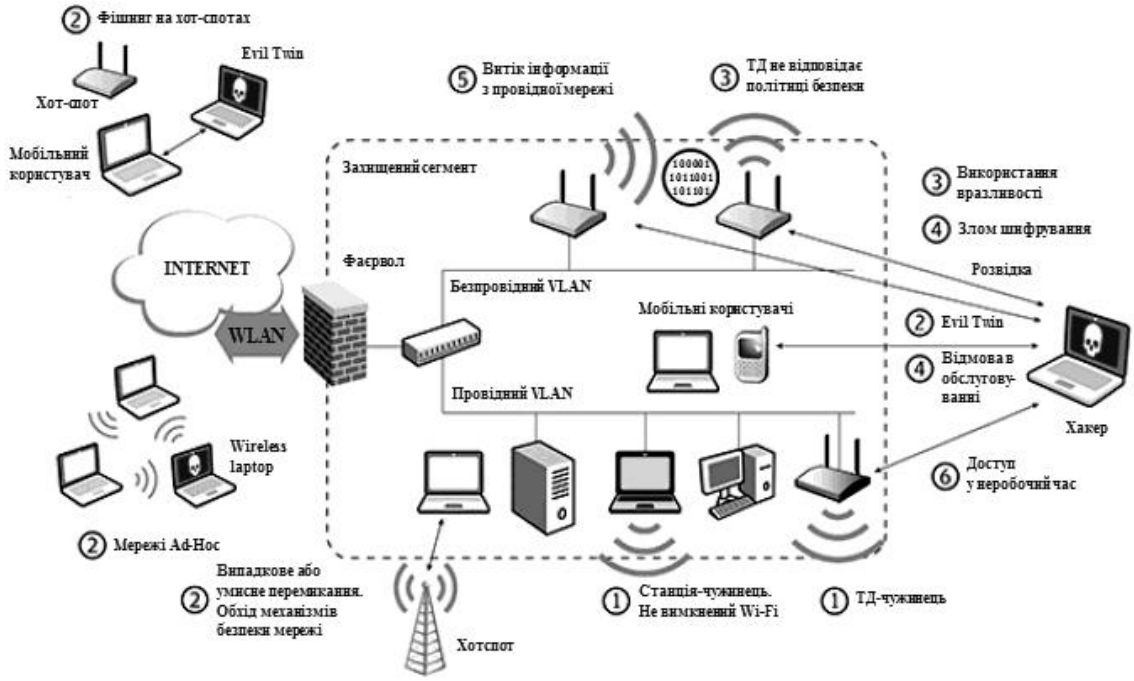

*Рис. 2.***Ненадійність традиційних методів захисту від нових класів атак**

Більшість традиційних атак розпочинаються з розвідки, в результаті якої зловмисником визначаються подальші шляхи їх розвитку. Для безпровідної розвідки використовуються як засоби сканування безпровідних мереж (NetStrumbler, Wellenreiter, вбудований клієнт JC) так і засоби збору та аналізу пакетів, оскільки багато керуючих пакетів WLAN є незашифрованими. При цьому дуже складно відрізнити станцію, що збирає інформацію, від звичайної, яка намагається отримати авторизований доступ до мережі або від спроби випадкової асоціації.

Імперсоналізація(IdentityTheft)авторизованого користувача – це серйозна загроза будь-якої комп'ютерної мережі. Однак у випадку безпровідної мережі визначити справжність користувача складніше. Звичайно, існують SSID і можна спробувати здійснити фільтрацію по MAC-адресам, однак і те й інше передається в ефірі у відкритому вигляді,тому йпідробити ці способи нескладно, а підробивши – можна відібрати як мінімум частину пропускної спроможності мережі та вставляти неправильні фрейми з метою порушення авторизованих комунікацій. Розколовши таким чином (хоч і не повністю) алгоритми шифрування, можна здійснювати атаки на структуру мережі(наприклад, ARP Poisoning, як у випадку з нещодавно виявленою уразливістю TKIP). Аналіз показує, що імперсоналізація користувача можлива не лише у випадку MAC-аутентифікації або застосування статичних ключів, але й схем на основі 802.1x. Деякі механізми не є абсолютно безпечними, тому що їх злом не є складнішим за злом стандарту шифрування WEP. Вже зараз доступний інструментарій для проведення злому механізму LEAP. Інші схеми, наприклад, EAP-TLS або PEAP більш надійні, але і вони не гарантують стійкості до комплексної атаки, що використовує декілька факторів одночасно [5].

Завданням атаки «Відмова в обслуговуванні» (DenialofService, DoS) є або порушення показників якості функціонування мережевих послуг, або повна ліквідація можливості доступу до них для авторизованих користувачів. Для цього в мережу посилаються «помилкові» пакети (з неправильною контрольною сумою і т.д.), які відправлені з легітимної адреси. У випадкубезпровідної мережі відстежити джерело такої атаки без спеціального інструментарію неможливо. Крім того, є можливість організувати DoS на фізичному рівні, запустивши досить потужний генератор перешкод в потрібному частотному діапазоні.

Основними видами інструментів зловмисників є:

– засоби розвідки – сканування мереж та визначення їх параметрів, збору та аналізу трафіку (Kismet, NetStrumbler, AirMagnet, Ethereal, Wireshark зі спеціальним модулем, THC-RUT);

– інструменти злому шифрування (AirCrack, WEPWedgie, WEPCrack, WEPAttack, AirSnort);

– інструменти злому механізмів аутентифікації для їх обходу або отримання параметрів облікового запису доступу користувача (ASLEAP, THC-LEAPCracker);

– інструменти організації відмов в обслуговуванні (WLANNjack, hunter_killer);

– сканери вразливостей (Nessus, xSpider);

– інструменти маніпулювання безпровідними з'єднаннями (HotSpotter, SoftAP, AirSnarf,);
– традиційний інструментарій (SMAC, IRPAS, Ettercap, Cain&Label, DSNIFF, IKECrack).

Цей список може бути і ширшим.

*Ризик 5 – витік інформації з провідної мережі.*Практично всі безпровідні мережі є частиною провідної комп'ютерної системи. Відповідно, будь-яка безпровідна ТД може бути використана як джерело атаки. Деякі помилки в їх конфігурації у поєднанні з помилками конфігурації провідної мережі можуть відкривати шляхи для просочувань інформації. Найбільш поширений приклад – ТД, що працюють у режимі мосту (Layer 2 Bridge) і підключені в плоску мережу (чи мережу з порушеннями сегментації VLAN) та передають в ефір широкомовні пакети з провідного сегменту, запити ARP, DHCP, фрейми STP і т.п. Деякі з цих даних можуть бути корисними для організації атак Main-in-The-Middle, Poisoning і DoS.

Інший поширений сценарій ґрунтується на особливостях реалізації протоколів 802.11. У випадку, коли на одній ТД налаштовані відразу кілька ESSID, широкомовний трафік буде поширюватись відразу на них усіх.В результаті, якщо на одній точці налаштовані захищена мережа і публічна зона доступу, зловмисник, підключений до останньої, має можливість порушити роботу протоколів DHCP або ARP в захищеній мережі. Для захисту необхідно увімкнути режим Multi-BSSID (Virtual AP).

*Ризик 6 – особливості функціонування безпровідних мереж.*Деякі особливості функціонування безпровідних мереж породжують додаткові проблеми, здатні впливати на їх доступність, продуктивність, безпеку і вартість експлуатації. Для вирішення цих проблем потрібний спеціальний інструментарій підтримки та експлуатації, спеціальні механізми адміністрування і моніторингу, що не реалізовані в традиційному інструментарії управління безпровідними мережами.

До безпровідних мереж можна підключитися в будь-якому місці в зоні їх покриття та в будь-який час. Через це багато організацій обмежують доступність безпровідних мереж в своїх офісах виключно робочими годинами [5, 6].

ТД, що дозволяють підключення на низьких швидкостях, мають велику зону покриття. Таким чином, вони надають додаткову можливість віддаленого злому. Якщо в офісній мережі, де всі працюють на швидкостях 24/36/54 Мб/с, раптом з'являється з'єднання на 1 або 2 Мб/с, то це може бути сигналом, що хтось намагається пробитися в мережу з вулиці.

Якість роботи безпровідної мережі залежить від багатьох факторів. Найбільш яскравим прикладом є перешкоди, що значно знижують пропускну здатність мережі, та кількість підтримуваних клієнтів. Джерелом перешкод може бути будь-який пристрій, що випромінює сигнал достатньої потужності в тому ж частотному діапазоні, що і ТД. З іншого боку, зловмисники можуть використовувати перешкоди для організації DoS-атаки на мережу.

Крім перешкод, існують інші аспекти, що впливають на якість зв'язку в безпровідних мережах – невірно сконфігурований клієнт або збій антени ТД можуть створювати проблеми як на фізичному, так і на канальному рівні, що може призвести до погіршення якості обслуговування інших клієнтів мережі.

Висновки.Таким чином, поширеність безпровідних технологій ставить під загрозу не тільки мережі, в яких вони застосовуються, але і ті, де вони не використовуються. Традиційні засоби захисту безсилі проти принципово нових класів безпровідних загроз.Ситуація ускладнюється тим, що при захисті своїх користувачів (які можуть знаходитися і далеко від офісу) не можна порушувати функціонування сусідніх мереж. Для гарантування безпеки інформації від розглянутих загроз як убезпровідних, так і в провідних мережах необхідно використовувати комплекс сучасних методів захисту.

1. ISO/IEC 27001:2005«Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».
2. ISO/IEC 27002:2005«Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».
3. ISO/IEC 27005:2007«Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности».
4. Петренко С.А., Петренко А.А. Аудит безопасности INTRANET – М.: ДМК Пресс, 2002. – 386 с.
5. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Владимиров А.А.,. Гавриленко К.В., Михайловский А.А.; пер. с англ. АА. Слинкина. – М.: НТ Пресс, 2005. – 463 с.
6. Столлингс В. Основы защиты сетей. Приложения и стандарты / Вильямс Столлингс. – М.: Вильямс, 2002. – 432 с.