**Франчук В. М.**

НПУ імені М.П. Драгоманова

## Захист даних в безпровідних комп’ютерних мережах

Безпровідні комп'ютерні мережі – це технології, за допомогою яких можна створювати обчислювальні мережі, які повністю відповідають стандартам звичайних провідникових мереж (наприклад, Ethernet), без використання кабельних проводів. Як носії сигналів в таких мережах виступають радіохвилі СВЧ-діапазону.

Засоби і системи безпровідного зв'язку використовуються, як правило, в мережах, що включають також і провідникові (кабельні) засоби, за допомогою яких можна зручно, швидко і економічно розв'язувати проблеми, що виникають в процесі створення і модернізації кабельних мереж. Безпровідні засоби зв'язку не слід вважати повною альтернативою кабельним мережам, а лише альтернативною технологією для реалізації окремих сегментів (або цілих рівнів) в проектованій, розширювальній або модернізованій локальній комп'ютерній мережі.

Безпровідні мережі використовуються там, де кабельна мережа не прокладена або неможливо її прокласти. Мережа, розгорнена відповідно до стандарту «RadioEthernet», є аналогом звичайної кабельної мережі Ethernet з колізійним механізмом доступу до середовища передавання даних. Різниця полягає лише в характері цього середовища. На базі «RadioEthernet» повністю забезпечуються всі потреби безпровідного передавання даних всередині приміщень.

При зовнішньому застосуванні «RadioEthernet» дуже зручно використовувати канал «остання миля» («остання миля» – канал, що сполучає кінцеве (клієнтське) обладнання з вузлом доступу провайдера) замість кабельних, тобто – для з'єднання між абонентом і найближчим вузлом основної мережі. При цьому реальна протяжність «останньої милі» може бути від кількох сотень метрів до 20-30 км і обмежена лише наявністю прямої видимості.

До недавнього часу створення офісних безпровідних мереж було зв'язано з необхідністю отримання дозволу місцевих органів влади. На початку 2002 року ситуація змінилася і тепер офісні безпровідні мережі можна створювати без дозволу на використання частот, досить лише налаштувати таку мережу.

Актуальною проблемою використання безпровідних мереж на сьогоднішній день є їх захист та способи захисту даних в них, оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір доступні для перехоплення. Компанії і індивідуальні користувачі повинні усвідомлювати потенційно існуючі проблеми і приймати відповідні заходи.

Існує кілька форм загрози безпеці в безпровідних мережах (рис. 1). Так, хакери (hackers – особи, які користуються своїми знаннями для досягнення «нестандартних» цілей) можуть викрасти дані, отримавши неавторизований доступ до мережі, і навіть порушити роботу мережі.


Рис. 1.

*Моніторинг трафіку.*

Досвідчений хакер або навіть випадковий снупер (snooper – відстежувач, перехоплювач) може відстежити пакети даних в незахищеній безпровідній мережі, використовуючи такі програмні засоби, як AirMagnet і AiroPeek, за допомогою яких можна повністю розшифрувати вміст пакетів даних із безпровідної мережі. Наприклад, снупери, знаходячись в кількох сотнях

метрів від будівлі, в якій функціонує безпровідна локальна мережа, можуть відстежити всі транзакції, що виконуються в безпровідній частині мережі. Звичайно, основна загроза полягає в тому, що в результаті атаки хтось може оволодіти важливими даними – дізнатися імена користувачів, паролі, номери кредитних карт і т.д.

*Неавторизований доступ.*

Також можна здійснити моніторинг виконуваних в мережі програм і без особливих зусиль, якщо не прийнято належних запобіжних заходів, отримати доступ до безпровідної мережі, знаходячись поза приміщенням, де вона функцонує. Наприклад, дехто, сидячи неподалік в припаркованому автомобілі, може під'єднатися до однієї з розташованих у будівлі базових станцій. Якщо не забезпечений належний захист, така особа отримує доступ до даних, що передаються в безпровідній мережі. Це рівносильне появі незнайомця у будинку.

На жаль, багато установ розгортають свої безпровідні мережі, використовуючи конфігурацію базових станцій, встановлену за замовчуванням і не забезпечують потрібного рівня захисту, що зумовлює безперешкодний доступ до комп'ютерів мережі. Це означає, що хто завгодно може отримати доступ до жорстких дисків або скористатися під'єднанням до глобальної мережі Internet.

За допомогою сучасних операційних систем можна легко встановлювати під'єднання до безпровідних мереж, особливо до загальнодоступних. Коли комп'ютер (ноутбук) під'єднаний до безпровідної локальної мережі, його власник отримує доступ до будь-якого іншого комп'ютера (ноутбука), що під'єднаний до тієї самої безпровідної локальної мережі. Якщо на комп'ютері не встановлений персональний брандмауер, то хто завгодно може отримати доступ до вмісту жорсткого диска такого комп'ютера (ноутбука), а це велика загроза для безпеки даних.

Навіть якщо в безпровідній мережі задіяні механізми захисту, істотною загрозою є під'єднання до підставної точки доступу (rogue access point). Така

точка доступу (access point – точка доступу, точка безпровідного доступу – це концентратор, в якому підтримується стандарт 802.11a або 802.11b, чи обидва, і через який забезпечується під'єднання безпровідних клієнтів до локальної мережі або Інтернет.) є неавторизованою точкою доступу під'єднання до мережі. Будь-який службовець може придбати пристрій для організації безпровідної мережі (точку доступу) і встановити його в своєму кабінеті, не розуміючи (чи навмисно), які будуть наслідки для безпеки мережі. Хакер також може розмістити точку доступу в будівлі, навмисно під'єднавши незахищену точку доступу до корпоративної мережі (Рис. 2).

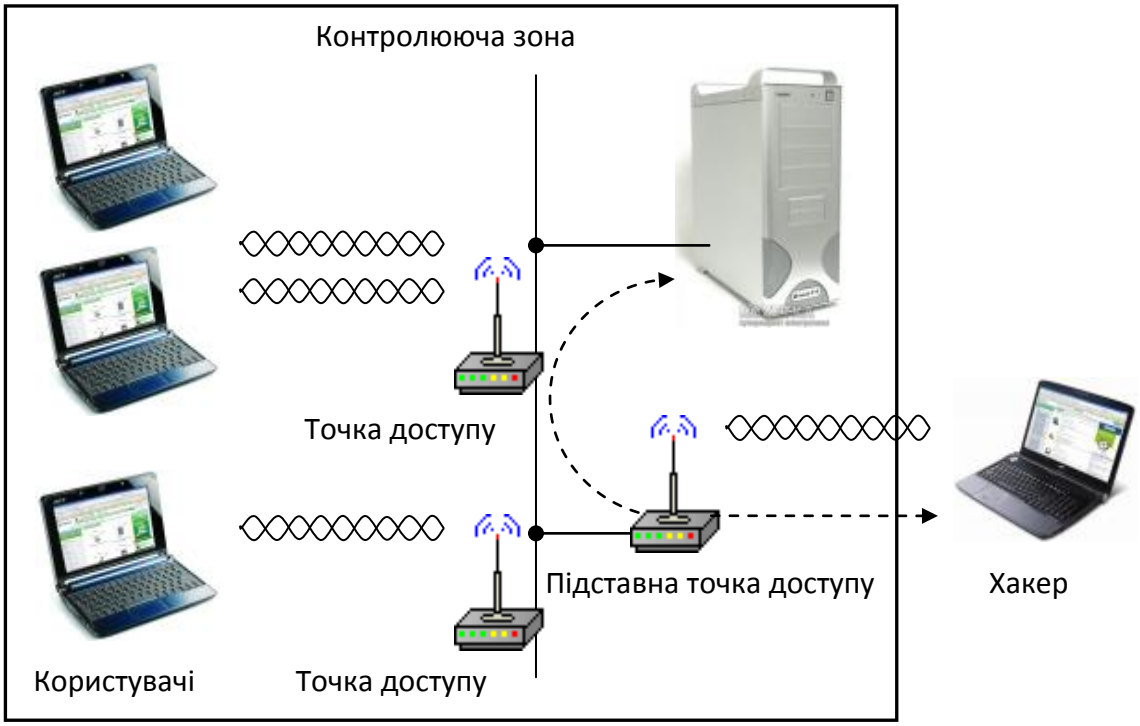


Рис. 2.

У підставній точці доступу, як правило, не активізується система шифрування і вона буде «відкритими дверима» для будь-кого, хто захоче отримати доступ до корпоративної мережі, знаходячись поза будівлею. Тому установи повинні постійно перевіряти наявність підставних точок доступу. Ця проблема актуальна незалежно від того, встановлена безпровідна мережа чи ні. Хтось може під'єднати підставну точку доступу і до повністю провідної мережі.

*Атака типу «людина всередині»*

Завдяки використанню механізмів шифрування і аутентифікації підвищується безпека безпровідної мережі, проте досвідчені хакери відшукують слабкі місця, знаючи, як працюють протоколи мережі. Певну небезпеку представляють атаки типу «людина всередині» (man-in-the-middle attacks): хакер розміщує фіктивний пристрій між легальними користувачами і безпровідною мережею. Наприклад, при здійсненні стандартної атаки типу «людина всередині» використовується протокол перетворення адрес (address resolution protocol (ARP)), який використовується у всіх мережах Ethernet. Хакер, маючи необхідне програмне забезпечення, може, скориставшись ARP, отримати контроль над безпровідною мережею (Рис. 3).

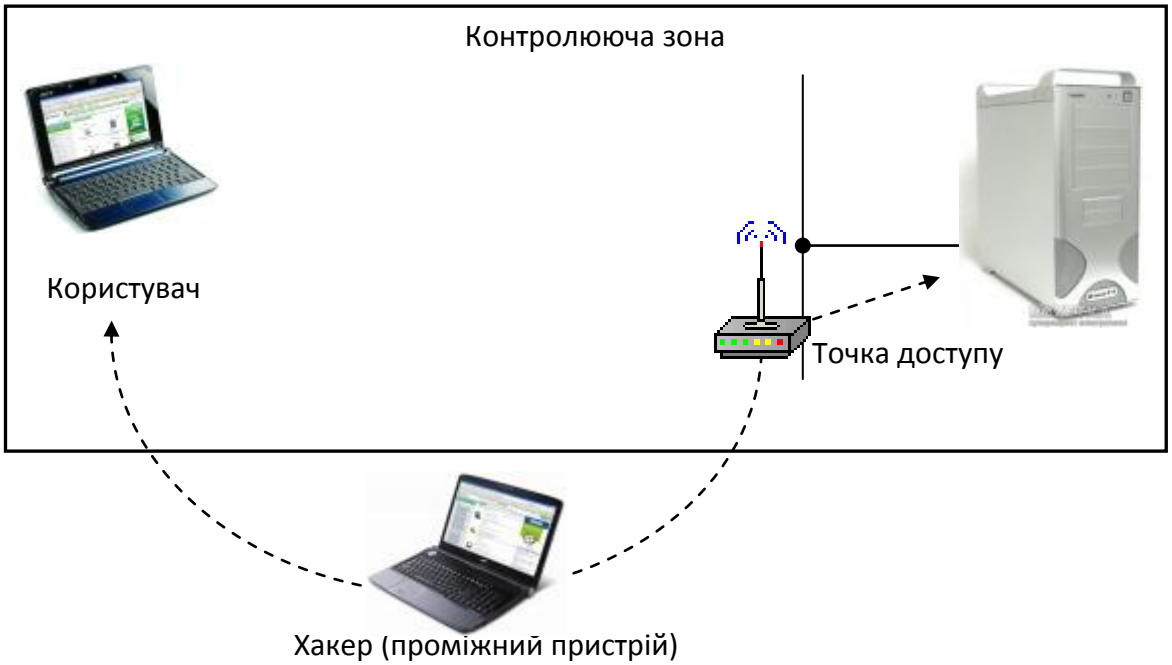


**Рис. 3.**

За допомогою ARP відправляються запити (як в провідниковій, так і в безпровідниковій мережі) через мережеву плату з метою виявлення іншої фізичної адреси, куди має прийти даний запит. Фізична адреса мережевої плати – це MAC (Media Access Control)-адреса, яка встановлюється на платі її виробником і відрізняється від адреси будь-якої іншої мережевої плати, тобто вона унікальна.

В прикладних програмах, за допомогою яких передаються дані, використовується IP (Internet Protocol)-адреса одержувача, а в мережевій платі, за допомогою якої передаються дані, використовується протокол ARP для виявлення відповідної фізичної адреси. Щоб отримати потрібну адресу одержувача, за допомогою мережевої плати розсилаються ARP-пакети, в яких оголошується IP-адреса мережевої плати одержувача. Всі комп'ютери мережі «чують» цей запит, і комп'ютер (мережева плата) з відповідною IP-адресою повертає пакет відповіді за протоколом ARP, що містить MAC і IP-адреси одержувача. Потім ця MAC-адреса додається в фрейм запиту в якості адреси одержувача і зберігається разом з IP-адресою в спеціальній таблиці на деякий проміжок часу (до тих пір, поки станція не отримає іншу MAC-адресу від комп'ютера, де є ця IP-адреса).

Проблема, яка виникає при використанні протоколу ARP, полягає в тому, що є небезпека для системи захисту даних за допомогою спуфинга (spoofing (спуфінг) – імітація з'єднання, отримання доступу обманним шляхом). Можна імітувати з'єднання між комп'ютерами, посилаючи на один з комп'ютерів через підставний мережевий пристрій фіктивний ARP запит, що містить IP-адресу дійсного мережевого пристрою і MAC-адресу підставного. Це приведе до того, що на всіх комп'ютерах мережі автоматично відновляться ARP-таблиці, які будуть містити помилкові дані. В результаті за допомогою комп'ютерів передаватимуться пакети до підставного пристрою, а не до дійсної точки доступу або маршрутизатора. Це і є класична атака типу «людина всередині», в результаті якої можна отримати доступ до управління сеансами зв'язку користувача, отримати паролі, важливі дані і навіть можна отримати доступ до корпоративних серверів, неначе вхід на сервери був здійснений з реального комп'ютера мережі.

Для запобігання такого роду атак з використанням спуфінга ARP розробники (наприклад, компанія OptimumPath) пропонують захищені ARP (secure ARP, SARP). Цей вдосконалений ARP забезпечує спеціальний

захищений канал зв’язку («тунель») між кожним клієнтом і безпровідною точкою доступу або маршрутизатором, за допомогою якого ігноруються всі ARP-відповіді, не пов'язані з клієнтом, що знаходиться на другому кінці цього каналу зв’язку. Отже, тільки реальні ARP-відповіді будуть служити підставою для оновлення ARP-таблиць. Комп’ютери, на яких використовується протокол SARP, захищені від спуфінгу. Проте для використання протоколу SARP на всіх точках доступу або маршрутизаторах потрібно встановити спеціальне програмне забезпечення, а це не завжди можливо реалізувати. Але можна встановити SARP на клієнтських пристроях (комп’ютерах, ноутбуках), забезпечивши захист мережі від атак типу «людина всередині».

*Атака типу «Відмова в обслуговуванні»*

Атака типу «відмова в обслуговуванні» (denial of service, DoS) – це атака, в результаті якої безпровідна мережа стає недоступною або її робота блокується. Можливість такої атаки потрібно враховувати при створенні і використанні безпровідних мереж. Серйозність DoS-атаки залежить від того, до яких наслідків може привести вихід з ладу безпровідної мережі. Наприклад, можна заблокувати безпровідну локальну мережу, розгорнуту в будинку, результатом цього буде лише неспокій власника. А відмова в обслуговуванні безпровідної мережі на підприємстві приведе до істотних фінансових втрат. Одним з різновидів DoS-атак є метод «грубої сили» (brute-force attack). Масове розсилання пакетів в мережі, при якому використовуються всі ресурси мережі, в результаті чого мережа переповнюється і блокується – це і є варіант DoS-атаки, виконаний за методом «грубої сили». У глобальній мережі Internet можна знайти програмні засоби, за допомогою яких можна викликати інтенсивне передавання пакетів в безпровідній мережі. Можна провести DoS-атаку за методом «грубої сили» шляхом відправляння пакетів серверу з інших комп'ютерів мережі. Це викликає істотні непродуктивні витрати ресурсів мережі і не дозволяє використовувати її пропускні характеристики користувачами цієї мережі.

Іншим методом припинення роботи більшості безпровідних мереж, особливо тих, в яких використовується метод виявлення мережі, є використання сильного радіосигналу, що «глушить» всі інші. Проте спроба проведення атаки на мережу з використанням сильного радіосигналу може виявитися вельми ризикованою, оскільки для проведення такої атаки потрібний потужний передавач, який повинен розташовуватися в безпосередній близькості від приміщення, в якому розгорнута безпровідна мережа. Власник мережі може виявити цей передавач, використовуючи засоби виявлення, що входять до складу мережевих аналізаторів. Після того, як джерело навмисних перешкод буде знайдено, його власникові доведеться припинити атаку. Іноді «відмова в обслуговуванні» безпровідної мережі виникає внаслідок ненавмисних дій. Так, мережі стандарту IEEE 802.11b (англ. Institute of Electrical and Electronics Engineers – Інститут інженерів з електроніки та електротехніки, 802.11b – стандарт бездротових локальних мереж, заснований на безпровідному передаванні даних в діапазоні 2,4 Ггц) функціонують в переповненому спектрі частот, а такі пристрої, як радіотелефони, мікрохвильові печі і пристрої Bluetooth, можуть викликати істотне зниження продуктивності мережі цього стандарту.

Найбільш дієвим захистом від DoS-атак є розробка і дотримання таких правил безпеки:

- встановлення та оновлення брандмауерів;
- постійне оновлення антивірусних програмних засобів;
- встановлення останніх «латок» (оновлень), за допомогою яких ліквідовують недоліки в системі безпеки операційної системи;
- використання довгих паролів;
- від’єднання мережевих пристроїв, які не використовуються.

Також забезпечити захист безпровідної мережі від атак типу «відмова в обслуговуванні» можна за допомогою зменшення проникнення радіосигналів ззовні в будівлю.

Наведемо деякі рекомендації, слідуючи яким, можна зменшити потік радіосигналів у приміщення:

- якщо внутрішні стіни будівлі мають металеві стійки і косяки, їх потрібно заземлити;
- потрібно встановити теплоізольовані, покриті мідною або металевою плівкою, вікна;
- замість жалюзі і занавісок можна скло металізувати;
- для внутрішніх і зовнішніх стін потрібно використовувати фарби з домішками металів;
- провести тестування, щоб визначити ступінь проникнення сигналу назовні. Також можна відрегулювати потужність передавача так, щоб повністю усунути витік сигналу або понизити його рівень до тих значень, при яких можна буде легко виявити хакера;
- використання направлених антен, за допомогою яких сигнал посилається всередину приміщень.

Універсального способу протидії DoS-атакам всіх типів не існує. Тому, якщо в результаті атаки безпровідна мережа все ж таки вийшла з ладу, слід забезпечити перехід до пакетного опрацювання даних за допомогою провідникової мережі.

*Способи захисту даних в безпровідних мережах*

1. Фізичний захист безпровідних точок доступу.

Деякі точки доступу мають спеціальну кнопку «Reset», за допомогою якої можна повернути налаштування пристроїв за замовчуванням. В такому випадку пристрій не буде забезпечувати навіть мінімального захисту безпровідної мережі. Це зробить таку точку доступу уразливою. Тому слід забезпечити адекватну фізичну захищеність апаратного забезпечення точок доступу. Наприклад, не слід розташовувати точки доступу в загальнодоступному місці. Навпаки, її потрібно встановити в такому місці, щоб вона по можливості була непомітною. Деякі точки доступу не мають

кнопки «Reset», але їх можна перезапустити за допомогою кабеля, який під’єднується до спеціального інтерфейсу (наприклад RS-232 – це стандарт інтерфейсу обміну даними між пристроєм передавання даних (точка доступу, модем) і комп'ютером шляхом послідовного передавання даних), використовуючи консоль. Щоб запобігти цьому, потрібно забезпечити фізичну недоступність цього спеціального інтерфейсу. Також не слід залишати точки доступу в місцях, де можна замінити реальну захищену точку доступу на незахищену, до якої може отримати доступ будь-який користувач. Тому слід приховувати, наскільки це можливо, точки доступу, щоб зловмисник не міг їх знайти. Якщо навчальний заклад (підприємство) велике, то потрібно скласти схему розміщення цих точок доступу, щоб їх можна було відшукати при потребі.

Ще одним дієвим способом зменшення ризику для безпеки точок доступу, якщо це можливо, є відключення точок доступу, які тимчасово не потрібні користувачам. Можна вимикати електроживлення кожної точки доступу, або якщо є можливість використовувати обладнання, управління електроживленням якого здійснюється через мережу, такі точки доступу можна вмикати і вимикати дистанційно.

2. Використання систем шифрування та аутентифікації.

Також слід звернути увагу на захист даних в безпровідних мережах. Для цього слід використовувати, як мінімум, шифрування цих даних. В процесі шифрування біти даних змінюються за допомогою секретного ключа. Оскільки ключ секретний, зловмиснику (хакеру) буде важко дешифрувати отримані дані. Тому за рахунок використання ефективних механізмів шифрування можна підвищити захищеність даних.

В сучасних точках доступу використовуються наступні методи шифрування даних:

- WEP (англ. Wired Equivalent Privacy) – стандарт захисту бездровідної мережі, заснований на методі потокового кодування з використанням алгоритму RC4 (з використанням загального секретного ключа).

Існують варіанти шифрування з довжиною ключа 64, 128 і 256 бітів. Використання стандарту WEP для захисту мереж не можна вважати надійним способом гарантування безпеки. Проблема полягає в реалізації вибору вектора ініціалізації, що використовується як псевдовипадкова послідовність для шифрування даних.

- WPA (англ. Wi-Fi Protected Access) – один з стандартів безпеки, який використовується для захисту бездротових мереж. Створений для заміни застарілого протоколу WEP. Заснований на TKIP (Temporary Key Integrity Protocol – протокол тимчасової цілісності ключів), за допомогою якого ефективно вирішується проблема, що лежить в основі вразливості стандарту WEP – повторного використання ключів шифрування.
- AES (Advanced Encryption Standard) – стандарт симетричного блочного шифрування (довжина блоку – 128 бітів), підтримуються 128-розрядні ключі, але можуть підтримуватися і довші, 192- і 256-розрядні.

Для протидії з неавторизованим доступом до безпровідної мережі використовується метод аутентифікації, який здійснюється між клієнтськими пристроями і точками доступу. Аутентифікація (Authentication – аутентифікація, перевірка (підтвердження) істинності. Процес перевірки, що користувач, який намагається за допомогою комп'ютера одержати доступ до деякої категорії даних, комп'ютерної системи, обчислювальної мережі або електронної пошти, є тим, за кого себе видає) – це підтвердження ідентичності користувача або пристрою. У безпровідній мережі повинні застосовуватися методи, використання яких дозволяє у точці доступу упевнитися в ідентичності клієнта. Крім того, точки доступу повинні проходити процедуру аутентифікації на комутаторах, що виключає появу в мережі підставних точок доступу.

Недоцільно використовувати на точках доступу паролі, задані за замовчуванням. Паролі за замовчуванням добре відомі, тому хтось зможе з легкістю змінити параметри точки доступу на свою користь. Замість них

потрібно задавати паролі, які важко підібрати. Непогано використовувати в паролях символи верхнього і нижнього регістрів, а також спеціальні символи. Також не слід забувати періодично змінювати паролі.

Отже, системи захисту безпровідних мереж – це один з найважливіших і складніших елементів налаштування безпровідних мереж. Здатність зловмисників відстежувати за допомогою спеціальних програмних засобів і пристроїв трафік, отримувати неавторизований доступ до ресурсів і викликати «відмову в обслуговуванні» безпровідної мережі для користувачів – це проблеми, які необхідно вирішувати при використанні безпровідних мереж. Використовуючи ефективні механізми аутентифікації і шифрування, можна істотно понизити небезпеку. Проте слід мати на увазі, що необхідний рівень безпеки залежить від вимог, які ставляться до мережі. Рівень захисту, прийнятний для домашньої мережі, абсолютно не відповідає вимогам, що пред'являється до системи безпеки мережі підприємства (навчального закладу).

**Список використаних джерел**

1. Антонов В.М. Современные компьютерные сети. – МК-Пресс, 2005. – 478 с.

2. Джим Гейер Беспроводные сети. Первый шаг. – САНКТ-ПЕТЕРБУРГ, «Вильямс», 2005. – 176 с.

3. Вікіпедія [Електронний ресурс] – режим доступу: http://uk.wikipedia.org.