УДК 621.396.67

К.В. Заїчко,
Я.В. Савенко

АСПЕКТИ БЕЗПЕКИ ПРИСТРОЇВ БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖ

Розглянуто аспекти безпеки пристроїв бездротових локальних мереж на основі запропонованої функціональної моделі з урахуванням можливих схем атак і диверсій. Наведено характеристику можливих схем атак і диверсій. Запропоновано шляхи забезпечення безпеки застосування пристроїв бездротових локальних мереж.

Ключові слова: *бездротові локальні мережі, точка доступу, пристрій користувача, безпека.*

Рассмотрены состояние и проблемы использования устройств беспроводных локальных сетей на основе предложенной функциональной модели с учетом возможных схем атак и диверсий. Представлена характеристика возможных схем атак и диверсий. Предложены пути обеспечения безопасности использования устройств беспроводных локальных сетей.

Ключевые слова: *беспроводные локальные сети, точка доступа, устройство пользователя, безопасность.*

Paper describes the problems and use of wireless local area networks device, based on the proposed functional model, taking into account the possible schemes of attacks and sabotage. Characteristics of the possible schemes of attacks and sabotage is considered. Ways of the safety ensuring of wireless local area networks device are presented.

Keywords: *wireless local area networks, access point, user unit, safety.*

На сьогодні широкого застосування в різних сферах діяльності людини – як спеціальних, так і побутових – отримали пристрої, у яких реалізовано бездротові технології обміну даними. Однією з них є технологія бездротових локальних мереж (*wireless local area network, WLAN*) [1].

Водночас слід відзначити наявність певних проблем функціонування пристроїв бездротових локальних мереж, які знижують ефективність їх застосування в певних сферах діяльності людини. До таких проблем, по-перше, можна віднести несанкціоноване втручання в роботу цих пристроїв та локальних бездротових мереж, із якими вони з'єднані. По-друге, відсутність надійних технологій захисту (протидії) від несанкціонованих дій порушника.

У зв'язку з цим, видається актуальним розгляд питання аналізу та оцінки ефективності функціонування пристроїв бездротових локальних мереж в умовах диверсій при певному захисті. Назвемо ризиком застосування пристроїв бездротових локальних мереж – функціонування пристроїв та бездротових локальних мереж, з якими вони зв'язані в умовах диверсій при певному захисті. Таким чином, аналіз ризику – це системний аналіз функціонування пристроїв, функціонування бездротових локальних мереж, диверсій та захисту від них.

Функціональна модель бездротових локальних мереж

Проаналізуємо функціонування пристроїв бездротових локальних мереж на прикладі поширеного класу пристроїв типу WiFi. Ядром бездротової локальної мережі, із якою з'єднуються WiFi-пристрої, є так звана точка доступу, що підключається до мережевої інфраструктури (каналам інтернет-провайдера) і забезпечує передачу радіосигналу до пристрою (споживача). Представимо схему функціонування пристроїв споживача із вмонтованими WiFi-пристроями бездротових локальних мереж (рис.1).

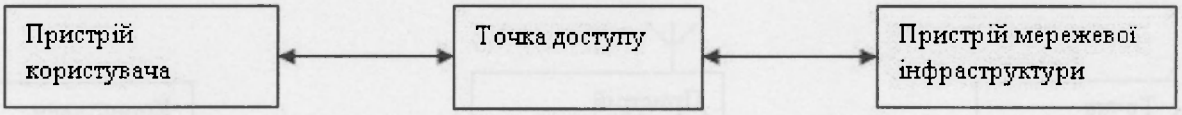

Рис. 1. Функціональна схема бездротової локальної мережі із застосуванням WiFi-пристроїв із точкою доступу

Схема складається із таких елементів: пристрою споживача, WiFi-пристрою, вбудованого в пристрій споживача, точки доступу, пристрою мережевої інфраструктури (що відноситься до провайдера). У свою чергу, точка доступу складається із приймача, передавача, інтерфейса для підключення до дротової мережі та програмного забезпечення для обробки даних. Навколо точки доступу формується зона WiFi, яку називають хот-спотом. Ця територія обмежена радіусом 50–100 метрів (відповідно до стандарту). однак на відкритій місцевості вона може сягати 300–400 м. Слід пам'ятати, що збільшення стандартного радіусу зони може призводити до підвищення ризиків застосування пристроїв бездротових локальних мереж.

Характеристика атак та диверсій

Функціонування пристроїв бездротових локальних мереж дає великі переваги стосовно вільного переміщення в межах визначеної зони. Водночас є наявність ризиків щодо організації та проведення диверсій та атак [2].

Найпростішим способом проведення диверсії є глушення, при якому в радіусі зони створюється завада, яка не дозволяє здійснювати радіообмін на певних каналах. Глушення дає можливість виконувати імітацію відмови в обслуговуванні. Підготовлені атаки переривають з'єднання користувача з точкою доступу з метою під'єднання до точки доступу зловмисника. Найбільш поширеною проблемою є прослуховування. Сигнали радіообміну між точкою доступу та периферійними пристроями можуть бути перехоплені та розшифровані. Перехоплення інформації виявити неможливо, а запобігти йому – ще важче. Прослуховування використовується для збирання інформації та підготовки подальших атак. Зловмисник намагається визначити можливості обладнання та програмного забезпечення. Деякі мережеві протоколи обміну інформацією дають можливість отримати без додаткових заходів дані щодо користувачів, паролів тощо. Серед способів прослуховування є підключення до точки доступу бездротової локальної мережі. Зловмисник може надсилати відповіді на які не проводилися запити. При цьому є можливість отримати дані щодо всього трафіку.

Повний параліч може викликати атака типу DoS, при якій виникає сильна інтерференція, що запобігає встановленню зв'язку. Диверсія типу глушення може бути здійснена на точку доступу. При цьому зловмисник здійснює підміну. Здійснюючи атаку типу вторгнення та модифікації даних, зловмисник додає інформацію до потоку наявних даних із метою їх пересилання, а також постановки команд за своїми сценаріями. При постановці відповідних команд зловмисник має можливість від'єднувати користувача від точки доступу.

Атаки та диверсії, внаслідок дії яких знижується рівень безпеки застосування пристроїв бездротових локальних мереж, можуть здійснюватися в різні способи.

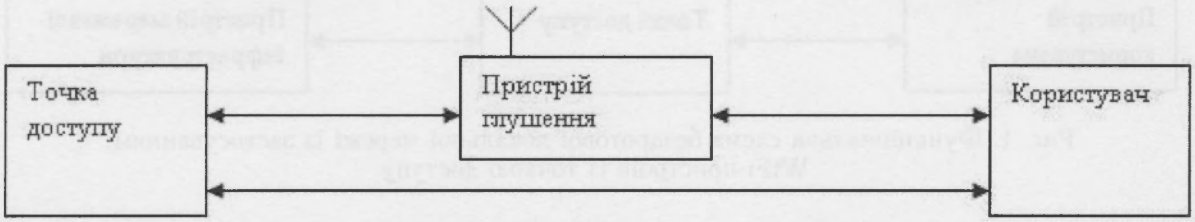

Рис. 2. Схема диверсії у вигляді глушення

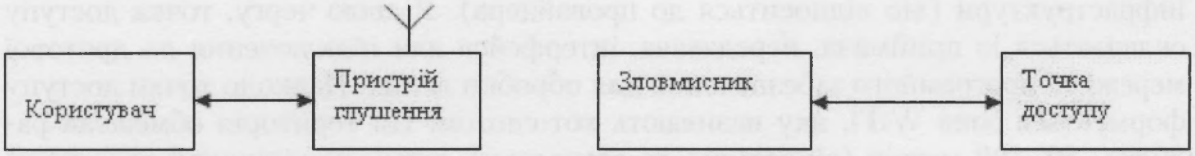

Рис. 3. Схема атаки з під'єднанням до точки доступу зловмисника

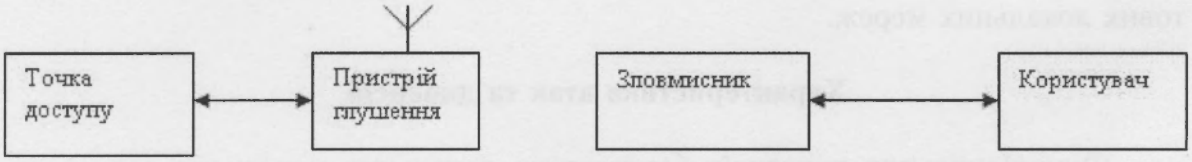

Рис. 4. Схема диверсії з підслуховуванням

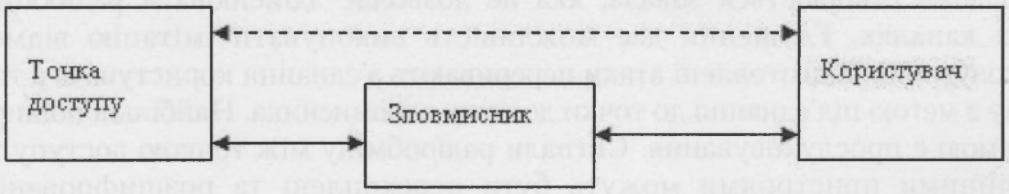

Рис. 5. Схема атаки типу вторгнення та модифікації даних

Висновки

Аналіз стану та проблем застосування пристроїв бездротових локальних мереж на основі запропонованої функціональної моделі з урахуванням можливих схем атак і диверсій дозволив визначити шляхи забезпечення безпеки застосу-

вання пристроїв бездротових локальних мереж, до яких слід віднести такі: зменшення зони радіопокриття до мінімально припустимої; використання протоколів високого рівня захисту; використання сучасних комплексів радіомоніторингу, що дозволить виявляти атаки й визначати місцерозташування зловмисника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IEEE 802.16e-2005 p. " 225 t. – 132 a.
2. *Кохановіч Г.Ф.* Специальный радиомониторинг. / Г.Ф. Кохановіч. – МК-Пресс, 2007.

Отримано 5.12.2011