УДК 621.324.067

ДОСЛІДЖЕННЯ НАПРЯМІВ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Д. т. н. С. А. Михайлов, С. В. Шрейнер

Міжнародний гуманітарний університет
Україна, м. Одеса
SMikhailov@i.ua, Denial24@xaker.ru

Існуючі безпроводові інформаційно-телекомунікаційні системи підприємств і організацій потребують додаткових заходів із захисту інформації. Для забезпечення якісного захисту комп'ютерних систем від мережних атак та дій внутрішніх зловмисників розроблено комплекс організаційних і технічних заходів.

Ключові слова: захист інформації, загрози та вразливості, багаторівневий захист, аутентифікація.

З появою безпроводового зв'язку на перший план вийшли питання забезпечення безпеки та конфіденційності зв'язку. Основні загрози безпеці при використанні безпроводових мереж пов'язані з перехопленням інформації спецслужб, комерційних підприємств і приватних осіб, зняттям коштів з кредитних карток громадян, крадіжкою оплаченого часу з'єднання, втручанням в роботу інформаційно-телекомунікаційних систем, несанкціонованим доступом до конфіденційної інформації та ін.

Все зазначене визначає перспективність наукового напрямку, пов'язаного із забезпеченням безпеки безпроводових мереж зв'язку.

Серед методів забезпечення доступності інформації в безпроводових мережах дослідниками виділяється комбінування різних методів контролю, дублювання, резервування. Цілісність і конфіденційність інформації в безпроводових мережах забезпечується методами побудови віртуальних каналів, заснованих на застосуванні криптографічних інструментів.

Загальний недолік даних методів – це зниження продуктивності мережі, яке пов'язане з вимогою додаткової обробки інформації, що передається. Зазначений недолік є особливо критичним для передачі цифрової відеоінформації. Крім того, вдосконалення методів криптоаналізу все більше знижує надійність існуючих криптоалгоритмів [1] .

З вищесказаного випливає висновок про необхідність розробки нових способів захисту інформації при передачі в розподілених безпроводових мережах в умовах впливу навмисних атак. У зв'язку з цим тема роботи є актуальною і практично важливою.

Метою роботи є удосконалення систем забезпечення інформаційної безпеки в безпроводових системах радіодоступу в інформаційно-телекомунікаційні мережі. З цією метою створено і запропоновано моделі багаторівневого захисту і формалізовано процедури організації багаторівневого захисту інформації в системах радіодоступу.

Один з підходів до забезпечення безпеки безпроводових мереж, так само як і проводових, полягає в побудові глибокоешелонованої безпеки мережі. Добре відомо, що захист будь-якої мережевої інфраструктури одними лише методами створення охоронюваного периметра неефективний, оскільки найчастіше найбільш небезпечні атаки викликаються факторами всередині мережі, наприклад:

– протиправними діями власних співробітників;

– впровадженням шкідливих програм (вірусів, троянів, тощо);

– застосуванням однорангових комунікацій в каналі зв'язку;

– діями гостей компанії, які отримали доступ до мережі.

Система безпеки мережі повинна враховувати всі ці фактори, щоб максимально наблизитися до схожості в рівнях безпеки проводових і безпроводових сегментів мережі [2].

При побудові системи безпеки безпроводової мережі потрібно використовувати основні механізми захисту, до яких відносяться:

– контроль доступу;
– аутентифікація користувачів;
– шифрування трафіку;
– система запобігання вторгненням в безпроводову мережу;
– система виявлення чужих пристроїв і можливості їх активного придушення;
– моніторинг спотворення сигналів і DoS-атак;
– моніторинг вразливостей в безпроводовій мережі та можливості аудиту вразливостей;
– функції підвищення рівня безпеки інфраструктури безпроводової мережі, наприклад, аутентіфікація пристроїв (X.509 і т. п.), захист даних управління (Management Frame Protection).

Було запропоновано шість основних напрямів вдосконалення інформаційної безпеки безпроводової мережі при побудові глибокоешелонованої оборони [3].

Напрямок 1: аутентифікація та авторизація всіх користувачів мережі.

Напрямок 2: конфігурування WLAN для поділу трафіку (наприклад, гості/співробітники, високий рівень доступу/низький рівень доступу тощо) і введення первинного або грубого сегментування.

Напрямок 3: використання міжмережевих екранів на рівні портів для формування більш тонкого рівня безпеки.

Напрямок 4: використовування шифрування на всіх сегментах мережі для забезпечення конфіденційності.

Напрямок 5: виявлення небезпек порушення цілісності мережі і вживання заходів вирішення цієї проблеми.

Напрямок 6: включення забезпечення безпеки кінцевих пристроїв в загальну політику інформаційної безпеки.

Таким чином, були сформульовані пропозиції щодо розвитку і вдосконалення систем безпеки безпроводових інформаційно-телекомунікаційних мереж на основі моделі багаторівневого захисту, що визначає набір рівнів або профілів захисту інформаційної системи. Коректна організація захисту на кожному з виділених рівнів дозволяє вберегти систему від реалізації загроз інформаційній безпеці. У багаторівневий захист входять фізичний захист, захист мережі, захист вузлів, захист користувальницьких додатків і захист даних в мережі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Владимиров А. А. Боевые приемы взлома и защиты беспроводных сетей.— Москва: НТ Пресс, 2005.
2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях.— СПб: ДМК Пресс, 2002.
3. Глубокоэшелонированная защита [Электронный ресурс] – Режим доступа: http://dic.academ.ru/dic.nsf/5.

———————

S. A. Mikhailov, S. V. Shreyner

Research on ways to improve the security of wireless information and telecommunication networks.

The existing wireless information and telecommunication systems of enterprises and organizations have problems with information security and there is a need for additional measures to protect information. To ensure the quality of protection of computer systems from network attacks, a set of organizational and technical measures is developed.

Keywords: *information security, threats and vulnerabilities, multilevel protection, authentication.*

———————