УДК 621.3

А.А. Калашян

Харьковский национальный экономический университет, Харьков

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ СТАНДАРТА 802.11

Определены основные тенденции в развитии средств связи. Приведена классификация интересов злоумышленников. Проведен анализ средств и протоколов защиты информации в системах беспроводной связи стандарта 802.11.

Ключевые слова: *Wi-Fi сети, методы защиты, шифрование аутентификация.*

Введение

Постановка проблемы. Являясь частью инфраструктуры экономики государства, телекоммуникационные сети играют чрезвычайно важную роль в жизни общества и определяют степень его развития. Увеличение числа пользователей, появление новых сетевых услуг, эволюция технологий передачи данных, разработка цифровых средств связи обусловили закономерный поэтапный переход к цифровым телекоммуникационным сетям и системам. Анализируя тенденции в развитии телекоммуникационных сетей, следует отметить появление и стремительное внедрение систем беспроводной связи, в частности систем стандарта 802.11. [1 – 4]. Несмотря на постоянный рост числа абонентов систем стандарта 802.11. вопросам обеспечения защиты информации до последнего времени должного внимания не было уделено. Так, разработанный в 90-х годах протокол защиты информации WEP, несмотря на «слабость» криптоалгоритмов, используемых в нем, продолжает повсеместно эксплуатироваться.

Анализ литературы [1 – 4] показал, что в последнее время разработаны и вводятся в эксплуатацию различные методы, алгоритмы, протоколы и средства защиты информации в сетях стандарта 802.11. Однако высокая стоимость оборудования, недостаточная подготовленность персонала и др. не позволяет повсеместно внедрять и эксплуатировать новейшие разработки.

Основной материал

Следует отметить, что возможные интересы злоумышленников, использующих ресурсы беспроводных сетей, с каждым годом возрастают (рис. 1).

истема защиты – это один из важнейших и сложных элементов беспроводных сетей. Способность хакеров отслеживать трафик, получать неавторизованный доступ к ресурсам и вызывать отказ в обслуживании беспроводной сетью ее пользователей – вот те проблемы, которые придется решать. Используя эффективные механизмы аутентификации и шифрования, можно существенно снизить опасность.

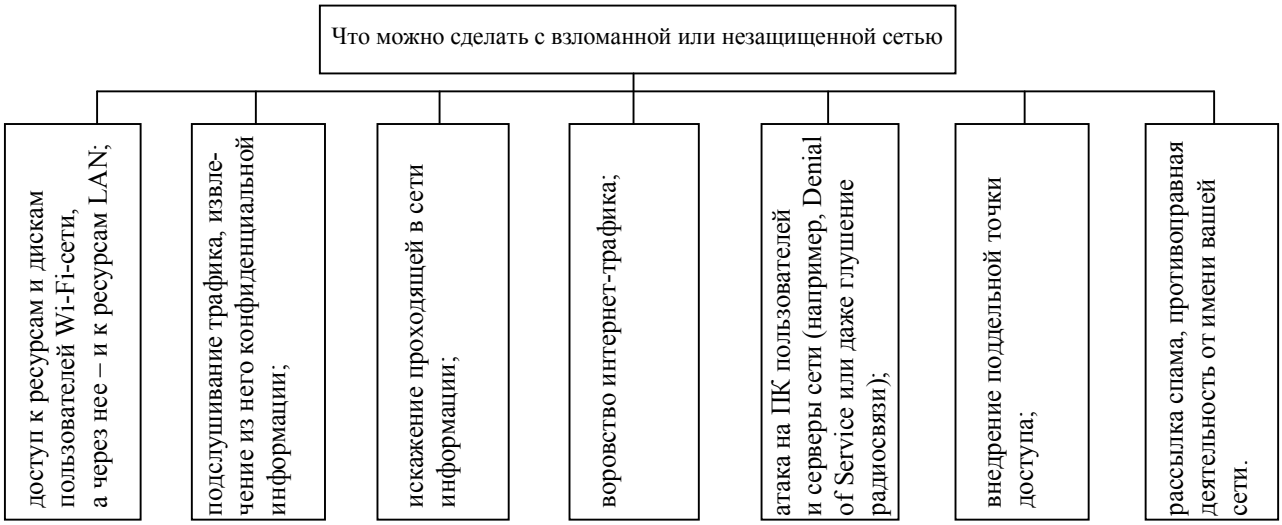

Рис. 1. Интересы злоумышленников

СОдним из первых средств защиты беспроводных сетей был протокол WEP (Wired Equivalent Protocol). Основная функция этого протокола шифрование данных при передаче по радио и предотвращение неавторизованного доступа в беспроводную сеть. Проблемы алгоритма WEP носят комплексный характер и кроются в целой серии слабых мест: механизме обмена ключами (а точнее, практически полном его отсутствии); малых разрядностях ключа и вектора инициализации (Initialization Vector -- IV); механизме проверки целостности передаваемых данных; способе аутентификации и алгоритме шифрования RC4 [1, 2, 4].

Следующим протоколом защиты информации стал протокол Temporal Key Integrity Protocol (TKIP) предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP -- RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей: динамические ключи, измененный метод генерации ключей, более надежный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерация пакетов.

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет так называемый Message Integrity Code (MIC), обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных) [1, 2, 4].

Стандарт 802.11i помимо временного решения TKIP, содержит протокол улучшенного стандарта шифрования (advanced encryption standard, AES), который обеспечивает более надежное шифрование. Протокол AES использует алгоритм шифрования Rine Dale, который обеспечивает существенно более надежное шифрование, чем заменяемый им алгоритм RC4. Многие криптографы считают, что AES вообще невозможно взломать. Кроме того, стандарт 802.11i будет включать AES как опциональный, используемый поверх TKIP.

Проблема, связанная с AES, состоит в том, что для его реализации требуется большая вычислительная мощность, чем та, которой обладают большинство точек доступа, предлагаемых сегодня на рынке. Поэтому компаниям для применения AES придется модернизировать аппаратное обеспечение своих беспроводных локальных сетей, чтобы оно поддерживало производительность, необходимую для применения алгоритма AES [1, 2, 4].

Выводы

Основы безопасности необходимо закладывать еще на стадии проектирования беспроводной сети.

• Защищайте свою сеть при помощи VPN или access control list.

• Точка доступа не должна быть напрямую подсоединена к локальной сети, даже если WEP включен.

• Точка доступа никогда не должна находиться позади брандмауэра.

• Доступ клиентам беспроводной сети надо давать по secure shell, IPSec или виртуальные частные сети. Они обеспечивают приемлемый уровень безопасности.

Список литературы

1. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А.А. Владимиров, К.В. Гавриленко, А.А. Михайловский. – М.: НТ Пресс, 2005. – 463 с.

2. Величко В.В. Передача данных в сетях мобильной связи третьего поколения / В.В. Величко. – М.: Радио и связь, Горячая линия-Телеком, 2005. – 332 с.

3. Галкин В.А. Телекоммуникации и сети: Учеб. пособие для вузов / В.А. Галкин, Ю.А. Григорьев. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2003. – 608 с.

4. Педжман Рошан. Основы построения беспроводных локальных сетей стандарта 802.11 / Педжман Рошан, Джонатан Лиэри. – М: Вильямс, 2004. – 302 с.

Принято 12.03.2009

Рецензент: канд. физ.-мат. наук, снс А.А. Можаев, Национальный технический университет «ХПИ», Харьков.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ СТАНДАРТУ 802.11

А.А. Калашян

Визначені основні тенденції в розвитку засобів зв'язку. Приведена класифікація інтересів зловмисників. Проведений аналіз засобів і протоколів захисту інформації в системах бездротового зв'язку стандарту 802.11.

***Ключові слова**: Wi-Fi мережі, методи захисту, шифрування аутентифікація.*

ANALYSIS of METHODS of DEFENCE of INFORMATION In WIRELESS COMMUNICATION of STANDARD NETWORKS 802.11

A.A. Kalashyan

Basic tendencies are certain in development of communication means. Classification of interests of malefactors is resulted. The analysis of facilities and protocols of defence of information is conducted in wireless communication of standard networks 802.11.

***Keywords**: Wi-Fi of network, methods of defence, coding is authentification.*