ТЕХНИЧЕСКИЕ НАУКИ

Ефимова Наталья Игоревна
студентка
Абдиева Александра Хайирбековна
студентка
Гуримская Ирина Анатольевна
старший преподаватель

Технический институт (филиал) ФГАОУ ВПО «Северо-Восточный федеральный университет им. М.К. Аммосова»
г. Нерюнгри, Республика Саха (Якутия)

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация*: в статье рассмотрены вопросы защиты беспроводной сети, угрозы информационной безопасности со стороны злоумышленников. Авторами выведены средства защиты: целостность, доступность и конфиденциальность.*

Ключевые слова*: атаки, угрозы, злоумышленники, безопасность, беспроводные сети, целостность, доступность, конфиденциальность.*

Если рассматривать атаки на беспроводные сети, нужно понимать, что процедура развертывания сети включает в себя множество мероприятий, которые уже включают свои меры по обеспечению безопасности. Трудность ряда таких мер делает незащищенными беспроводные сети, если при настройке сети были допущены ошибки или просто-напросто что-то было упущено. Потеря данных в беспроводных сетях является негативным действием, потому, многие предприятия реализуют продуманную политику безопасности. Популярность данного вида с каждым годом растет. Популярность чего-либо в сфере компьютерных технологий всегда вызывает нездоровый интерес различных «криминальных элементов от IT».

После всего вышесказанного, стоит задуматься о безопасности, ведь и стандартные средства могут оказаться бессильными. Одной из главных целей нашей работы является получение знаний по беспроводным сетям, способам их защиты, уязвимости их к взлому. Если научиться настраивать беспроводные сети, то можно легко понять их стороны уязвимости. Все специалисты, которые работают в сфере IT-технологий, знают способы и средства защиты беспроводных сетей, но, если постоянно наращивать эти средства, то могут появиться места, которые будут подвержены сетевым атакам. Собственно, так и произошло. На смену проводным сетям пришли беспроводные.

В чем состоит отличие проводной сети от беспроводной? Проводная сеть, если ее правильно использовать, может быть атакована только извне (Интернет). Беспроводная же представляет собой большую опасность, так как помимо вторжений из Интернета ей угрожает попытка «прослушивания» со стороны конкурентов или же недоброжелателей. Из этого следует вывод, что если не уделять внимание политике безопасности, это неизбежно отразится на ее функционировании [1].

Попытки взлома корпоративной сети могут исходить из нескольких обстоятельств:

1) целенаправленный взлом с целью похищения важной конфиденциальной информации. Именно поэтому стоит заботиться о безопасности беспроводного сегмента сети;

2) популярными также являются попытки воспользоваться чужим Интернет-соединением. В данном случае также происходит воровство Интернет-трафика, скорости соединения [1].

Причины взлома беспроводных сетей:

1) целенаправленный взлом с целью получения необходимых засекреченных данных;

2) целенаправленное изменение файлов;

3) незаконное использование чужого Интернет-трафика.

В современном обществе легко заметить тенденции роста замены проводных сетей на беспроводные. Это прослеживается на всех уровнях жизни.

Выделим несколько типов беспроводных технологий:

– для связи различного оборудования в пределах рабочего места;

– беспроводные локальные сети WLAN;

– беспроводная сеть WMAN [2], радиус воздействия которой, функционирует в черте города.

Для того, чтобы взломать беспроводную сеть понадобится:

1) ноутбук/нетбук/компьютер с беспроводным адаптером. При попытке такого взлома возникает проблема, связанная с совместимостью между чипом беспроводного адаптера и операционной системой;

2) программы для взлома и правильно настроенная ОС. «Перешагнуть» систему безопасности на базе WEP-шифрования очень легко, потому, на смену WEP-протоколу пришел более устойчивый протокол – WPA.

Также, для увеличения точек действия беспроводной сети появляются распределенные беспроводные сети (WDS) на базе нескольких точек доступа. Они не поддерживают WPA-протокол и единственной допустимой мерой безопасности в данном случае является применение WEP-шифрования.

Даже с такой хорошей безопасностью, WDS-сети легко взламываются, если они находятся на базе хотя бы одной точки доступа. Кроме того, КПК, обладающие беспроводным модулем, тоже не поддерживают протокол WPA, поэтому для добавления клиента на базе КПК в беспроводную сеть, нужно использовать в ней протокол WEP.

Из всего вышесказанного следует, что WEP протокол еще очень долгое время будет актуален. Рассмотренные примеры взлома беспроводных сетей весьма наглядно демонстрируют их уязвимость.

Если рассматривать такие меры предосторожности, как фильтрация по MAC-адресам и режимы скрытых идентификаторов сети, то их вообще нельзя воспринимать, как эффективное средство защиты. Однако, даже такие средства

нельзя не учитывать для защиты ценной информации, но, естественно, только в комплексе с другими мерами [3; 4].

Список литературы

1. Патий Е. Проблемы безопасности в беспроводных сетях / Е.Патий // Искусство управления информационной безопасностью [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/ chitalnyi-zai/ bezopasnost-besprovodnyh-setei/problemy-bezopasnosti-v-besprovodnyh-setyah/

2. Куц В. Современные беспроводные сети – история, применение, перспективы / В. Куц // Федеральный медиа-ресурс, посвященный рынку современных информационных технологий [Электронный ресурс]. – Режим доступа: http://www.comprice.ru/articles/detail.php?ID=225105

3. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Компьютерный информационный портал [Электронный ресурс]. – Режим доступа: http://www.oszone.net/3652_1/

4. Практика взлома беспроводных сетей / С. Пахомов, М. Афанасьев // Компьютер Пресс [Электронный ресурс]. – Режим доступа:http://www.compress.ru/Article.aspx?id=17372