Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.05.5

Высоцкая
Валерия Вячеславовна

Обеспечение безопасности Wi-Fi сетей

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 80 02 «Телекоммуникационные системы и компьютерные сети»

_____

Научный руководитель
Лыньков Леонид Михайлович
доктор технических наук,
профессор

_____

Минск 2018

КРАТКОЕ ВВЕДЕНИЕ

Большинство современных портативных устройств (ноутбуки, КПК, смартфоны) уже имеют встроенные средства для работы в беспроводных сетях.

Wi-Fi – это популярный термин, обозначающий высокочастотную беспроводную локальную сеть (WLAN). Wi-Fi предлагает своим пользователям свободу перемещения.

Так же современный мир ставит нас в условия быстро развивающихся технологий и криминогенной обстановки, которая во многом определяет желание большинства людей оградить себя от внешнего мира, построить вокруг себя надежную стену, чтобы устранить угрозы и риски на длительную перспективу, чувствовать себя в безопасности в общественных местах и транспорте. Так и организации пытаются ограничить доступ в помещения некоторых лиц, контролировать проходы в помещения, фиксировать факты нарушений и вести наблюдение за каждым посторонним человеком, посетителем или гостем. Вышеуказанные действия было бы невозможно совершить без различных комплексов технических средств. В этом случае и становиться актуальным широкое использование возможностей инновационных технологий в области видеонаблюдения. Процесс видеонаблюдения осуществляется с помощью систем видеонаблюдения.

Использование систем видеонаблюдения безгранично: фиксирование противозаконных действий в различных общественных и жилых местах, контроль над рабочим персоналом, обеспечение общей безопасности, применение в образовательных целях, высотное телевидение. Большое распространение получили системы видеонаблюдения основанные на сети беспроводного доступа Wi-Fi.

Технология Wi-Fi позволяет передавать информацию в сети при помощи радиосигнала. По сути, этот сигнал почти ничем не отличается от радиосигнала, принимаемого сотовым телефоном.

Wi-Fi может использоваться для распространения сигнала в квартире или конференц-зале, или на расстояние в несколько километров. Как правило, одна точка доступа может обеспечить радиус действия до 100-200 метров и намного более. Но такой принцип дает возможность подключиться любому человеку к сети при помощи своего ноутбука, карманного компьютера или смартфона, оснащенного Wi-Fi-адаптером.

Чтобы избежать подобного, есть разработанные методы защиты от несанкционированного доступа или различных угроз и атак.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научным исследованием университета

Тема магистерской работы утверждена приказом ректора учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» протокол № 1 от 04.09.2017.

Цель и задачи, проводимых исследования

Цель состоит в анализе способа защиты Wi-Fi сети для снижения атак и угроз на систему видеонаблюдения в мобильном объекте.

Для достижения цели необходимо было решить следующие задачи:

1. Провести обзор сети Wi-FI и ее режимов работы;
2. Исследовать виды угроз и их негативное воздействие на функционирование беспроводных сетей;
3. Выявить наилучшую технологию по защите сети беспроводного доступа.

Объектом исследования явилась система безопасности передачи данных видеоинформации мобильного объекта.

Предметов исследования технология защиты системы видеонаблюдения.

Практическая значимость полученных результатов

Полный анализ сети Wi-Fi мер защиты данных сетей, позволил выбрать наиболее лучший вариант защиты информационной безопасности, для системы видеонаблюдения в мобильном объекте на основе сети беспроводного доступа IEEE802.11.

Личный вклад соискателя

Содержание диссертации отражает личный вклад автора. Он заключается в обзоре сети беспроводного доступа, защите данных сетей, возможных угроз и атак на данные сети, технологии защиты, анализе и сравнении двух технологий защиты для системы видеонаблюдения в мобильном объекте на основе сети беспроводного доступа IEEE802.11. Определение целей и задача исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем, доктором технических наук, профессором Леонидом Михайловичем Лыньковым.

Основные положения, выносимые на защиту

1. Обзор сети беспроводного доступа и анализ способов защиты сети;

2. Обзор объекта защиты, т.е. системы видеонаблюдения в мобильном объекте на основе сети беспроводного доступа IEEE802.11, обзор оборудования данной системы и выбора технологии защиты.

Апробация результатов диссертации

Основные положения диссертации обсуждались на 54-ой научной конференции аспирантов, магистрантов и студентов (Минск, 2018).

Опубликование результатов

Материалы результатов исследований, представленных в диссертации, опубликованы в 1 тезисе по материалам доклада на конференции [1-А].

Структура и объем работы

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованной литературы.

Общий объем магистерской диссертации составляет 69 страницы, включая 14 иллюстраций, 6 таблиц, список использованной литературы из 32 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1 осуществлен обзор сети беспроводного доступа. Важно отметить, что сеть беспроводного доступа – сеть, основанная на беспроводном (без использования кабельной проводки) принципе, полностью соответствующая стандартам для обычных проводных сетей.

Существует два основных направления применения беспроводных компьютерных сетей:

– работа в замкнутом объеме;

– соединение удаленных локальных сетей (или удаленных сегментов локальной сети).

Определяет два режима работы сети:

1 Режим Ad-hoc («точка-точка») – это простая сеть, в которой связь между станциями (клиентами) устанавливается напрямую, без использования специальной точки доступа.

2 Режим Infrastructure («клиент-сервер») – беспроводная сеть состоящая, как минимум, из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций.

В настоящее время существует множество стандартов семейства IEEE 802.11, основные из них: 802.11, 802.11a, 802.11b, 802.11g, 802.11n.

Помимо основных стандартов 802.11a, b, g, n, существуют и используются дополнительные стандарты для реализации различных сервисных функций: 802.11d, 802.11e, 802.11f, 802.11h, 802.11i, 802.11k, 802.11m, 802.11p, 802.11r, 802.11s, 802.11t, 802.11u, 802.11v, 802.11y, 802.11w, 802.11ac.

Стандарт IEEE 802.11 работает на двух нижних уровнях модели OSI: физическом и канальном. Другими словами, использовать оборудование Wi-Fi так же просто, как и Ethernet: протокол TCP/IP накладывается поверх протокола, описывающего передачу информации по каналу связи.

Глава номер 2 посвящена анализу безопасности Wi-Fi. Из этой главы можно сделать вывод, что если беспроводная сеть останется незащищенной, она будет уязвима для доступа из других компьютеров.

Есть следующие виды персональной защиты:

1 Открытая и общая сетевая аутентификация. Спецификация 802.11 поддерживает два метода сетевой аутентификации: открытую систему и с использованием общего ключа.

2 WEP-шифрование. WEP-шифрование специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой.

3 WPA-персональная. Режим персональной защиты WPA используется в домашних условиях или сетях малого бизнеса. Для персональной защиты WPA необходимо вручную сконфигурировать предварительно опубликованный общий ключ (PSK) в точке доступа или клиентах.

4 WPA2-персональная. Для персональной защиты WPA2 необходимо вручную сконфигурировать предварительно опубликованный общий ключ (PSK) в точке доступа или клиентах. Для защиты WPA2-персональная доступны алгоритмы шифрования данных TKIP и AES-CCMP.

5 WPA-Enterprise (WPA-предприятие). Корпоративный режим аутентификации предназначен для использования в масштабах предприятий или сетях государственных учреждений. WPA-предприятие проверяет пользователей сети, используя сервер RADIUS или другой сервер аутентификации.

В сетях Wi-Fi используются следующие виды шифрования данных:

1 AES – CCMP. TKIP. Протокол TKIP (Temporal Key Integrity Protocol) использует функцию смешения содержимого ключа для каждого пакета, проверку целостности сообщений и механизм манипуляций с ключом. Протокол TKIP доступен для сетевой аутентификации WPA/WPA2-персональная/предприятие.

2 CKIP. Cisco Key Integrity Protocol (CKIP) – это собственный протокол защиты Cisco для шифрования в среде 802.11. Протокол CKIP использует следующие особенности для усовершенствования защиты 802.11 в режиме «infrastructure»:

– Key Permutation (KP) – манипуляции с ключом;

– Message Sequence Number – номер последовательности сообщения.

3 WEP. WEP-шифрование (Wired Equivalent Privacy) использует специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой. Только компьютеры, использующие этот же ключ, могут получить доступ к сети и расшифровать переданные другими компьютерами данные. Корпоративная WEP-защита отличается от персональной WEP-защиты тем, что для нее может быть выбрана открытая сетевая аутентификация, а затем можно выбрать 802.1X и указать нужный тип аутентификации клиентов. Выбор типов аутентификации недоступен для персональной защиты WEP.

Глава 3 содержит данные об объекте защиты, т.е. системы видеонаблюдения в мобильном объекте на основе сети беспроводного доступа IEEE802.11.

В главе 4 посвящена моделированию Wi-Fi сети по маршруту следования мобильного объекта от станции метро «Октябрьская» до пересечения улицы Городской вал и проспекта Независимости. В ходе моделирования был создан отчет, согласно которому на 75,3% площади уровень сигнала является надежным и находится в пределах от -45 дБм до -65 дБм. На остальном 24,7% площади уровня сигнала составляет от -65 дБм до -70 дБм. Так же скорость передачи по маршруту следования в основном составляет 130-150 Мбит/с, что позволит системе видеонаблюдения использовать высокоскоростной доступ в интернет из любой точки следования по маршруту.

Так же данная глава посвещена сравнение WPA и WPA2, т.к. точка доступа использует WPA/WPA2, WPA-PSK/WPA2-PSK (AES/TKIP). Важно отметить что на сегодняшний день ситуация такова, что все устройства,

работающие в сетях Wi-Fi, обязаны поддерживать WPA2, так что выбор WPA обусловлен может быть только нестандартными ситуациями. К примеру, операционные системы старше Windows XP SP3 не поддерживают работу с WPA2 без применения патчей, так что машины и устройства, управляемые такими системами, требуют внимания администратора сети. С другой стороны, некоторые версии Windows старше XP не поддерживают работу с WPA2 на уровне объектов групповой политики, поэтому требуют в этом случае более тонкой настройки сетевых подключений.

Техническое отличие WPA от WPA2 состоит в технологии шифрования, в частности, в используемых протоколах. В WPA используется протокол TKIP, в WPA2 – протокол AES. На практике это означает, что более современный WPA2 обеспечивает более высокую степень защиты сети.

ЗАКЛЮЧЕНИЕ

Сеть беспроводного доступа – сеть, основанная на беспроводном (без использования кабельной проводки) принципе, полностью соответствующая стандартам для обычных проводных сетей.

Если беспроводная сеть останется незащищенной, она будет уязвима для доступа из других компьютеров. Можно очень просто защитить домашнюю сеть и сеть малого бизнеса от почти любых форм несанкционированного доступа, используя для этого методы защиты, описываемые далее в этом разделе.

Есть следующие виды персональной защиты:

– открытая и общая сетевая аутентификация.

– WEP-шифрование.

– WPA-персональная.

– WPA2-персональная.

Так же проанализировав WPA и WPA2 были сделаны следующие выводы:

– WPA2 представляет собой улучшенный WPA;

– WPA2 использует протокол AES, WPA – протокол TKIP;

– WPA2 поддерживается всеми современными беспроводными устройствами;

– WPA2 может не поддерживаться устаревшими операционными системами;

– степень защиты WPA2 выше, чем WPA.

Таким образом, для системы видеонаблюдения в мобильном объекте на основе сети беспроводного доступа с учетом проведенного анализа технологий защиты и технических характеристик оборудования данной системы, самый лучший вариант WPA2-PSK (AES).

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А Высоцкая, В. В. Безопасность сети беспроводного доступа / В. В. Высоцкая // Телекоммуникационные системы и сети: материалы 54-й научной конференции аспирантов, магистрантов и студентов (Минск, 23 –27 апреля 2018 г.). – Минск: БГУИР, 2018.