всему первоначально имела место недооценка грузинских возможностей в сфере ПВО. При этом грузинская ПВО опиралась в основном на получение информации от радиолокаторов пассивной разведки «Кольчуга-М» минимально используя активные радары, а грузинские самоходные ЗРК" «Бук-М1» и «Оса-АК/АКМ» применяли тактику действия из засады. Это затрудняло борьбу с грузинскими средствами ПВО. Согласно последним неофициальным сведениям, грузинский «Бук-МІ» смог в первый день войны 8 августа сбить четыре российских самолета- штурмовика Су-25 и один бомбардировщик Ту-22М3. Кроме того, по неофициальным данным, Россия в ходе конфликта потеряла еще три самолета - один самолет-разведчик Су-24МР, один фронтовой бомбардировщик Су-24М и один штурмовик Су-25, а так же один ударный вертолет Ми-24. Оба Су-24, предположительно, были поражены грузинскими ЗРК «Оса-АК/АКМ» или ПТЗРК, а Су-25, по ряду сообщений, стал жертвой ошибочного «дружественного огня» ПЗРК российских войск. Еще минимум один российский Су-25 получил попадание ракеты грузинского ПЗРК, но смог благополучно вернуть на базу. В свою очередь, как сообщалось, ПВО российских войск сбила три грузинских штурмовика Су-25.

Опыт локальных войн и вооруженных конфликтов конца XX начала XXI вв. свидетельствует о том, что надежная противовоздушная оборона войск, важнейших государственных объектов приобрела значение стратегического фактора, оказывающего существенное влияние на их конечный результат.

Список использованных источников:

1. http://logoysk.by/
2. http://ru.wikipedia.org/

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВОЗНИКАЮЩИЕ ПРИ ИСПОЛЬЗОВАНИИ WI-FI СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шукайлов А. А., Минин Д. С.

Стандарт Wi-Fi разработан на основе IEEE 802.11 (англ. Institute of Electrical and Electronics Engineers), используется для широкополосных беспроводных сетей связи. В настоящее время сети Wi-Fi распространены повсеместно и зачастую имеют зоны покрытия целых районов города.

С точки зрения безопасности, следует учитывать не только угрозы, свойственные проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации намного проще, чем в проводных сетях, равно как и повлиять на канал передачи данных. Достаточно поместить соответствующее устройство в зоне действия сети.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

прямые - угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;

косвенные — угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

Прямые угрозы:

Радиоканал передачи данных, используемый в Wi-Fi потенциально подвержен вмешательству с целью нарушения конфиденциальности, целостности и доступности информации. В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои изъяны.

Первоначальный стандарт шифрования WEP был дискредитирован за счёт уязвимостей в алгоритме распределения ключей RC4. Это вызвало создание институтом IEEE рабочей группы 802.11i для разработки нового стандарта, обеспечивающего 128-битное AES шифрование и аутентификацию для защиты данных. Wi-Fi Alliance в 2003 представил свой вариант этого стандарта - WPA. WPA использует протокол целостности временных ключей TKIP. Также в нём используется метод контрольной суммы MIC для проверки целостности пакетов. В 2004 Wi-Fi Alliance выпустили стандарт WPA2, который представляет собой улучшенный WPA. Угроза блокирования информации в канале Wi-Fi практически оставлена без внимания при разработке технологии. Подобное вмешательство позволяет удалять, искажать или навязывать ложную информацию.

Чужаки

Чужаками называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, обычно в обход механизмов защиты, определенных политикой безопасности. В роли чужака может выступать всё, у чего есть проводной и беспроводной интерфейсы: точки доступа (включая программные), сканеры, проекторы, ноутбуки с обоими включёнными интерфейсами и т.д.

Нефиксированная природа связи

Беспроводные устройства могут менять точки подключения к сети прямо в процессе работы. Таким образом нарушитель переключает на себя пользователя для последующего сканирования уязвимостей, фишинга или атак "человек посередине". А если пользователь при этом подключен и к проводной сети, то он становится точкой входа - чужаком.

Ещё одна проблема - сети Ad-Hoc, с помощью которых удобно передавать файлы коллегам или печатать на принтере с Wi-Fi. Но такая организация сетей не поддерживает многие методы обеспечения безопасности, что делает их лёгкой добычей для нарушителя. Новые технологии Virtual WiFi и Wi-Fi Direct только ухудшили ситуацию.

Некорректно сконфигурированные точки доступа и беспроводные клиенты

Достаточно подключить неправильно настроенную точку доступа к сети для взлома последней. Настройки "по умолчанию" не включают шифрование и аутентификацию, или используют ключи, прописанные в

руководстве и поэтому всем известные. Маловероятно, что пользователи достаточно серьёзно озаботятся безопасной конфигурацией устройств. Именно такие привнесённые точки доступа и создают основные угрозы защищённым сетям.

Некорректно настроенные устройства пользователей - угроза опаснее, чем некорректно сконфигурированные точки доступа. Это устройства пользователей и они не конфигурируются специально в целях безопасности внутренней сети предприятия. К тому же они находятся за периметром контролируемой зоны, так и внутри него, позволяя злоумышленнику проводить всевозможные атаки, как то распространять вредоносное программное обеспечение или просто обеспечивая удобную точку входа.

Взлом шифрования

О защищённости WEP и речи уже нет. Интернет полон специального и удобного в использовании ПО для взлома этого стандарта, которое собирает статистику трафика до тех пор, пока её не станет достаточно для восстановления ключа шифрования. Стандарты WPA и WPA2 также имеют ряд уязвимостей разной степени опасности, позволяющих их взлом. Пока что нет информации об успешных атаках на WPA2-Enterprise (802.1x).

Имперсонация и Identity Theft

Имперсонация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и их несложно подделать, а подделав – как минимум снизить пропускную способность сети, вставляя неправильные кадры, а разобравшись в алгоритмах шифрования – устраивать атаки на структуру сети (например, ARP-spoofing).

Отказы в обслуживании (DoS-атака)

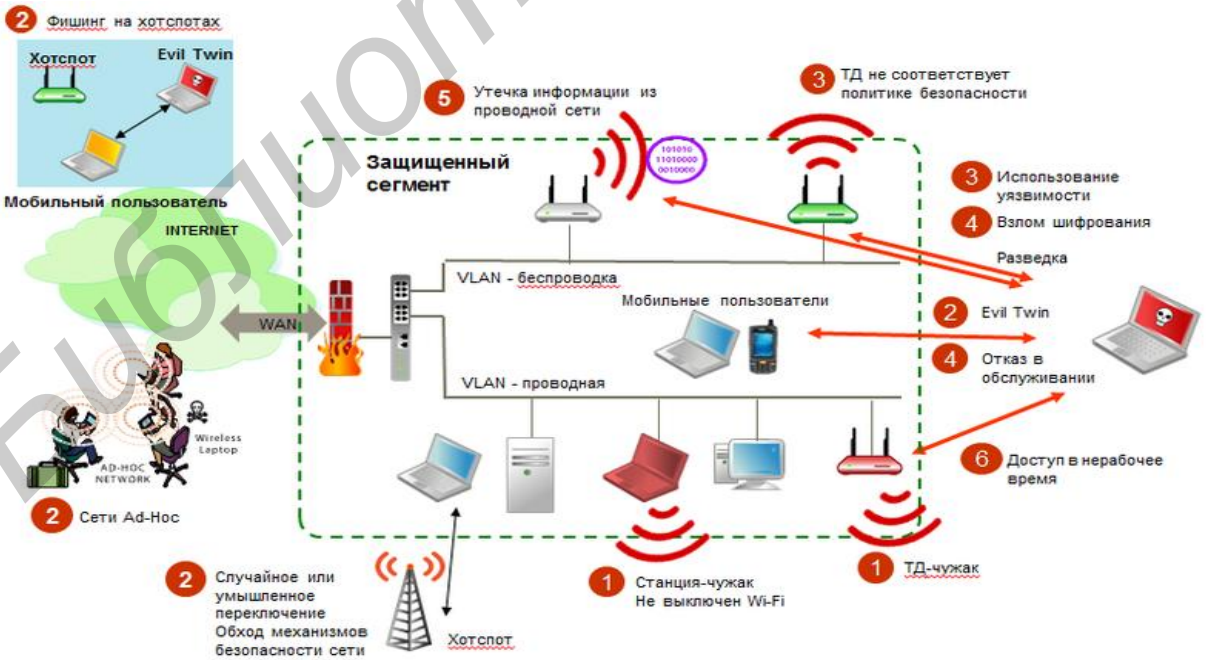
DoS атаки направлены на нарушение качества функционирования сети или на абсолютное прекращение доступа пользователей. В случае Wi-Fi сети отследить источник, заваливающий сеть "мусорными" пакетами, крайне сложно - его местоположение ограничивается лишь зоной покрытия. К тому же есть аппаратный вариант этой атаки - установка достаточно сильного источника помех в нужном частотном диапазоне.

Косвенные угрозы:

Сигналы WiFi-устройств имеют достаточно сложную структуру и широкий спектр, поэтому эти сигналы, а тем более, окружающие устройства Wi-Fi невозможно идентифицировать обычными средствами радиомониторинга. Исходя из того, что практически каждый объект окружает множество "чужих" Wi-Fi сетей, отличить легальных клиентов своей сети и соседних сетей от нарушителей крайне сложно, что позволяет успешно маскировать несанкционированную передачу информации среди легальных Wi-Fi-каналов.

В крупных городах Wi-Fi сети общего пользования имеют достаточно обширную зону покрытия, чтобы отпала необходимость использовать мобильный пункт приёма информации рядом с объектом - несанкционированное устройство может подключиться к доступной Wi-Fi сети и использовать её для передачи информации через Интернет в любое требуемое место.

Пропускная способность Wi-Fi сетей позволяет передавать звук и видео в реальном времени. Это упрощает злоумышленнику использовать акустические и оптические каналы утечки информации - достаточно легально купить Wi-Fi-видеокамеру и установить её в качестве устройства негласного получения информации.



Список использованных источников:

1. https://ru.wikipedia.org/wiki3ащита_в_сетях_W-Fi;