Неговора Д.О.
студентка кафедры прикладной информатики и информационных технологий НИУ «БелГУ», бакалавр (Белгород, Россия)
Научный руководитель:
Коваленко А. Н.
ст. пр. кафедры прикладной информатики и информационных технологий НИУ «БелГУ», (Белгород, Россия)
Negovora D. O.
Student faculty applied informatics and information technologies National University of BelSU Belgorod, Russia
Scientific adviser:
Kovalenko A. N.
Senior Lecturer Department of Applied Informatics and Information Technology NRU "BelSU", Belgorod, Russia

РАЗРАБОТКА АЛГОРИТМА ДЕЙСТВИЙ ДЛЯ ЗАЩИТЫ БЕСПРОВОДНОЙ СЕТИ

DEVELOPING AN ACTION ALGORITHM FOR PROTECTING A WIRELESS NETWORK

Аннотация: в статье раскрывается понятие беспроводной сети, а также характеристика категорий основных атак. Описан алгоритм проведения диагностики эффективности защиты беспроводной сети, на основании которого составлены рекомендации по повышению уровня защищенности беспроводной сети (разработан алгоритм действий для защиты).

Abstract: the article reveals the concept of a wireless network, as well as a description of the categories of major attacks. An algorithm for diagnosing the effectiveness of wireless network protection is described, based on which recommendations are made to increase the level of security of the wireless network (an action algorithm for protection has been developed).

Ключевые слова:

Беспроводная сеть, информационная безопасность, атака сети, политика безопасности, компьютерные технологии.

Keywords: Wireless network, information security, network attack, security policy, computer technology.

Введение

Большинство современных устройств поддерживает беспроводной доступ в сеть, то есть возможность подключаться к интернету без сетевого кабеля. Главное преимущество беспроводных соединений - возможность работать с из любой точки помещения. Однако, если не принять мер к обеспечению безопасности беспроводного подключения, возможен ряд опасных ситуаций.

Так возникает необходимость защиты беспроводных сетей от вмешательства злоумышленников, а именно: уменьшение риска перехвата трафика данных, получения доступа к сети, а также захвата канала доступа в Интернет. Для достижения этой цели следует изучить понятие беспроводной сети, определить основные категории атак, затем провести сравнительный обзор средств обеспечения информационной безопасности и, наконец, разработать эффективный алгоритм действий для защиты беспроводной сети.

Понятие беспроводной сети и описание категорий основных атак

Беспроводная сеть – это передача информации на расстояние без использования электрических проводников или физического кабеля [4]. В настоящее время необходимо принимать во внимание беспроводные решения при проектировании любых сетей - от малого офиса до предприятия, поскольку это снижает расход денежных средств, трудозатраты и время.

Существует много случаев и причин, по которым беспроводные сети являются единственным или же самым удобным вариантом организации доступа к сети связи или интернету. Например, если необходимо организовать периодический доступ к сети в общественных местах, в зданиях без возможности проводного подключения, в случае мобильного доступа к сети, а также для организации дополнительных каналов связи.

Во время работы сетей такого типа часто возникают различные проблемы. Некоторые – по вине сотрудников компании, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится

ущерб. Данные события являются атаками, независимо от причин их возникновения.

Существуют четыре основных категорий атак: атака доступа (нарушение конфиденциальности информации злоумышленником), атака модификации (неправомерное нарушение целостности информации), атака на отказ в обслуживании (легальному пользователю запрещена работа с системой) и атака на отказ от обязательств, которая противодействует возможной идентификации информации [1].

Все перечисленные виды атак несут реальную угрозу передаваемой по сети информации, поэтому от пользователя требуется знание алгоритма действий для защиты от несанкционированного доступа.

Обзор средств и методов обеспечения информационной безопасности беспроводных сетей

При построении системы обеспечения безопасности важно определить модель угроз, т. е., решить, чему собственно защита будет противостоять. На сегодняшний день компании, использующие сети беспроводного локального соединения (далее – WlAN), внедряют четыре отдельных решения для безопасности WLAN и управления доступом и конфиденциальностью:

- Открытый доступ - функции безопасности должны быть включены на беспроводных устройствах в процессе их установки, поскольку все продукты для беспроводных локальных сетей, поставляются для работы в режиме открытого доступа с выключенными функциями безопасности;

- Базовая безопасность - заключается в использовании идентификаторов сети, с помощью различных комбинаций идентификаторов можно настроить элементарные средства управления доступом и конфиденциальностью;

- Повышенная безопасность – рассматривается приобретение средства безопасности повышенного уровня с блоками двусторонней аутентификации;

- Безопасность удаленного доступа – с помощью удаленного виртуального доступа, администраторы могут настроить виртуальную частную сеть (VPN) и позволить мобильным пользователям обмениваться

данными с корпоративной сетью из общественных хот-спотов, например, аэропортов, отелей и конференц-залов.

В итоге, можно прийти к выводу, что для обеспечения информационной безопасности любой сети, не только беспроводной, важно качественное управление доступом и конфиденциальностью. Для этого на сегодняшний день активно внедряют четыре отдельных решения: открытый доступ, базовая безопасность, повышенная безопасность, безопасность удаленного доступа.

Разработка алгоритма действия для защиты беспроводной сети

Для того чтобы определить преимущество того или иного метода защиты беспроводной сети целесообразно провести оценку её защищенности. Ниже (на рисунке 1) представлена схема [5] пошаговых действий для проведения оценки.

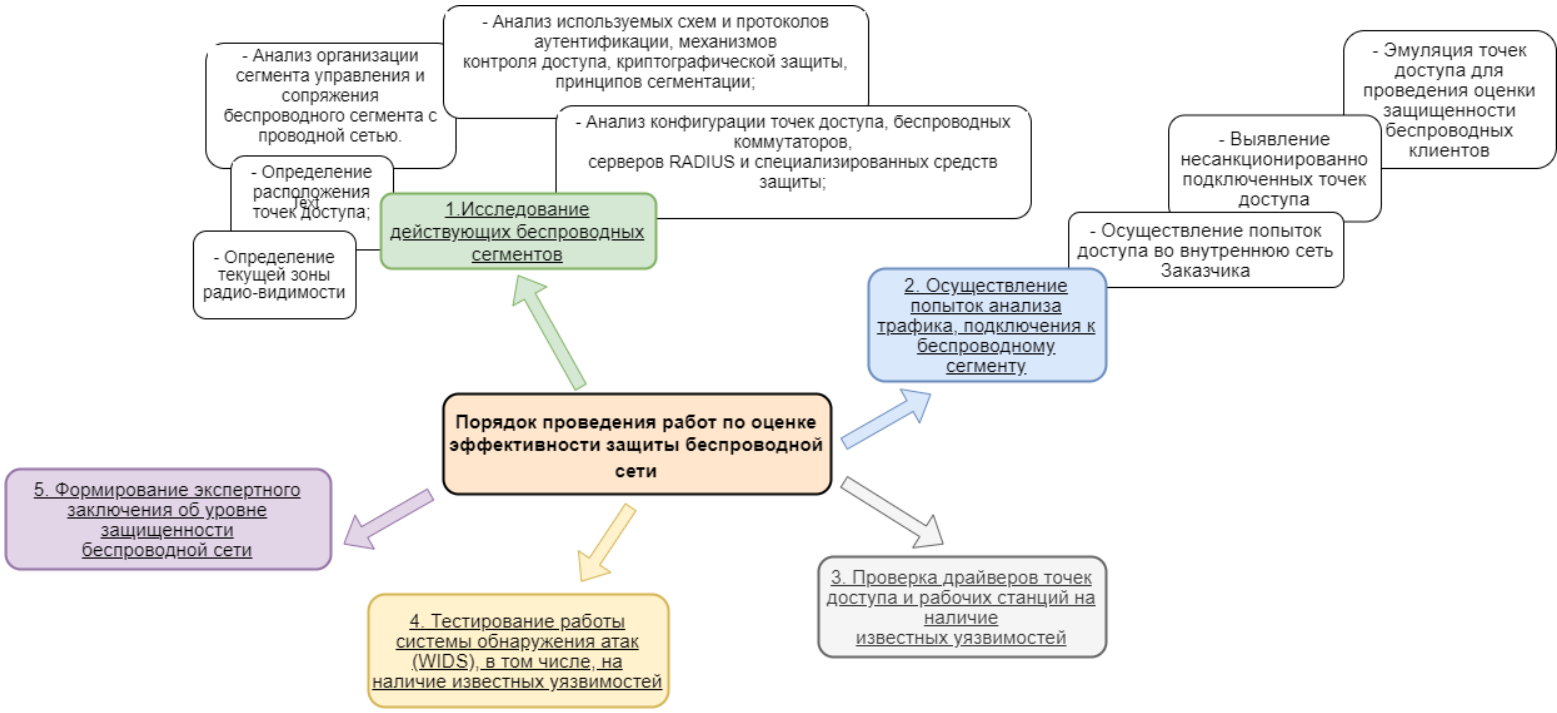

Рисунок 1. Порядок проведения диагностики эффективности защиты беспроводной сети.

Результатом работы будет являться отчет, содержащий:

1. Описание организации беспроводной сети;

2. Оценку существующих уязвимых мест и проблемных областей, включая результаты попыток несанкционированного доступа;
3. Рекомендации по повышению уровня защищенности беспроводной сети.

Логическим продолжением являются работы по проектированию и внедрению систем защиты на основании простого алгоритма:

1. Сменить логин и пароль для администрирования точки доступа;
2. По возможности, настраивать точку доступа через проводное соединение и отключить возможность доступа к настройкам точки доступа через беспроводное соединение;
3. Скрыть сеть от глаз - задать уникальный SSID сети и отключить трансляцию её SSID;
4. Установите фильтрацию по MAC-адресам, если число подключаемых к сети пользователей ограничено;
5. Вместо обычной аутентификации использовать метод WPA или WPA2;
6. Обязательно использовать шифрование потока данных. Минимум - WEP, но лучше WPA-PSK, WPA TKIP или WPA EAS, WPA 2;
7. Использовать длинные пароли. Минимум - 128 бит, но лучше 256 бит.

Заключение

В настоящее время беспроводные соединения получили широкое распространение, в основном, благодаря их способности работать с интернетом в любой точке дома или офиса. Однако если не принять мер к обеспечению информационной безопасности беспроводной сети, то злоумышленник может перехватить передаваемые данные, получить доступ к сети и файлам на компьютере, а также выходить в интернет, используя подключение.

И если обеспечение физической безопасности имеет давнюю традицию и устоявшиеся подходы, то информационная безопасность постоянно требует новых решений, поскольку компьютерные и телекоммуникационные

технологии, в том числе и беспроводные сети, постоянно обновляются, на компьютерные системы возлагается все большая ответственность.

Перечисленных в работе мер достаточно, чтобы защитить домашнюю или малую офисную сеть, состоящую из одной точки доступа и нескольких клиентских машин, от хакерских атак.

Библиографический список

1. Актуальные проблемы безопасности информационных технологий: материалы II Международной научно-практической конференции (9-12 сентября 2008, г. Красноярск) / под общей ред. О.Н. Жданова, В.В. Золотарева, Сиб. гос. аэрокосмич. ун-т. - Красноярск, 2010. - 100 с.
2. Воронков Б.Н. Криптографические методы защиты информации / Б. Н. Воронков. - изд. Воронежский государственный университет, 2011.
3. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось. - М.: Горячая линия - Телеком, 2010. - 544 с.
4. Информатика и компьютерные технологии. Основные термины. Толковый словарь. Фридланд А.Я. и др. 3-е изд., испр. и доп. - М.: АСТ, Астрель, 2009. - 272 с.
5. Милославская Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью / Н. Г. Милославская. - М. 2012. - 166 с.