|  |
| --- |
| T  Министерство образования Новосибирской области Государственное бюджетное профессиональное образовательное учреждение  Новосибирской области  «Новосибирский колледж почтовой связи и сервиса» |
| **ДОПУЩЕН КЗАЩИТЕ**  ам. директора поУПР  /Т.В.Пушкарева  приказ№  от« » 2021г |
| **«Установка и настройка программных средств защиты автоматизированных системы**  **и информационных сетей на основе технологии Wi-max и Wi-Fi»**  **Пояснительная записка к дипломному проекту** |
| **Специальность 12.02.08 Средства связи с подвижными объектами** |
| Студент Абенов И.Э.  Подпись Фамилия, И., О.студента |
| Группа ТС-43 |
| Руководитель Шабронов А.А  Подпись Фамилия, И., О.руководителя |
| Нормоконтроль  Подпись Фамилия, И.О. нормоконтролера |
| Председатель  Цикловой комиссии  Подпись Фамилия, И.О. председателя |
| Новосибирск, 2021 г. |

**Содержание**

[**Введение.**](#_Toc63049048)..................................................................................................................3

**1.1.Особенность беспроводной связи в безопасности**………………………..3

1.2. Отличия Защиты................................................................................................4

1.3. Идентификация пользователя...........................................................................5

1.4. Типы протоколов подключения……………………………………………...6

1.5. Угрозы и способы их распространения……………………………………..11

# 2. Легитимность использования программного обеспечения…………………12

2.1 Угрозы информационной безопасности Wi-Fi……………………………...16

3.Межсетевое взаимодействие…………………………………………………..20

4. Законодательство об информационной безопасности……………………….21

4.1 Механизмы защиты в информации в сетях Wi-Max………………………..23

4.2 Механизмы защиты в информации в сетях Wi-Fi…………………………..26

**Введение.**

#### Популярность беспроводных локальных сетей уже прошла стадию взрывного роста и дошла до состояния «привычной всем» технологии. Домашние точки доступа и мини-роутеры Wi-Fi недороги и широкодоступны, хотспоты встречаются достаточно часто, ноутбук без Wi-Fi – анахронизм. Как и множество других инновационных технологий, использование беспроводных сетей влечет не только новые выгоды, но и новые риски. Бум Wi-Fi породил целое новое поколение хакеров, специализирующихся на изобретении всё новых и новых способов взлома «беспроводки» и атаки пользователей и корпоративной инфраструктуры. Ещё с 2004 года Gartner предупреждали, что безопасность WLAN будет одной из основных проблем – и прогноз оправдывается.

#### Особенность беспроводной связи в безопасности.

#### В чём заключаются особенности беспроводной связи с точки зрения безопасности?

##### **Среда с общим доступом, которую практически невозможно контролировать.**

Традиционные проводные сети используют кабель для передачи информации. Кабель считается «контролируемой» средой, защищенной зданиями и помещениями, в которых он находится. Внешний «чужой» трафик, который входит в защищенный сегмент сети, фильтруется межсетевым экраном и анализируется системами IDS/IPS. Для того чтобы получить доступ к такому сегменту проводной сети, злоумышленнику необходимо преодолеть либо систему физической безопасности здания, либо межсетевой экран.  
  
Беспроводные же сети используют радиоволны. Эфир – среда с общим доступом и практически полным отсутствием контроля. Обеспечить эквивалент физической безопасности проводных сетей здесь просто невозможно. Как только пользователь подключает к проводной сети точку доступа, её сигнал может проходить сквозь стены, межэтажные перекрытия, окна здания. Таким образом, подключенный сегмент сети становится доступным с другого этажа или даже из соседнего здания, парковки или другого конца улицы – радиосигнал может распространяться на сотни метров за пределы здания. Единственной физической границей беспроводной сети является уровень этого самого сигнала.

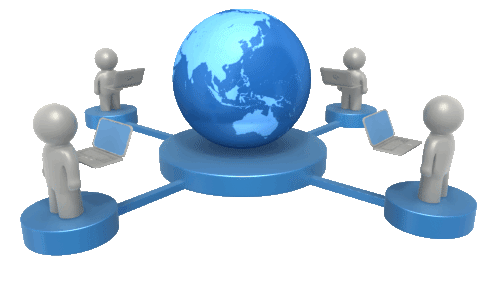
 Интересной особенностью беспроводных сетей является организация публичного и незащищенного доступа, приводящая к целому классу проблем безопасности, совершенно несвойственных проводным сетям.

1.2. Отличия защиты.

Специфика защиты беспроводных сетей, прежде всего, заключается в их отличии от сетей проводных. Беспроводные ЛВС, ввиду их широковещательной природы, требуют реализации дополнительных механизмов для:

* аутентификации абонентов (userauthentication) с целью предотвращения несанкционированного доступа к сетевым ресурсам;
* обеспечения конфиденциальности данных (dataprivacy) с целью обеспечения целостности и защиты при передаче по обще­доступному радиоканалу.

Безусловно, наряду с уникальными для беспроводных технологий проблемами безопасности существует ряд общих для проводных и беспроводных технологий проблем. Как правило, это атаки более высокого уровня, неселективные к используемой технологии доступа (фишинг и т. п.). Однако и здесь возможны варианты беспроводной специфики, например в случае DoS-атак. Интересной особенностью беспроводных сетей является организация публичного и незащищенного доступа, приводящая к целому классу проблем безопасности, совершенно несвойственных проводным сетям.



В целом можно сказать, что большое значение играет совершенно другая организация доступа к физической среде. В отличие от проводных подключений, в случае подключения беспроводного у нас присутствуют следующие моменты:

1. Может оказаться проблематичным достоверно определить местоположение клиента (точку подключения), особенно в случае разреженной беспроводной сети.
2. Трафик всегда передается по разделяемой среде (shared medium), то есть практически всегда имеется возможность для прослушивания и вмешательства в канал передачи данных (безусловно, успешность таких действий не гарантирована).
3. Местоположение сетевого устройства также неочевидно для подключающегося клиента, что облегчает злоумышленнику возможность выдать нелегитимное устройство за точку подключения к сети.
4. Клиентское устройство не зафиксировано в пространстве, более того, даже в случае неподвижного клиента мы не можем требовать подключения к одной и той же точке доступа в сеть, роуминг это нормальное поведение клиентского устройства (этот факт существенно затрудняет обнаружение попыток имперсонификации).
5. Кроме того, в случае Mesh-сетей мы имеем дополнительный класс инфраструктурных атак, где сетевые устройства не могут быть достоверно определены (т. е. мы не можем сказать, является upstream/downstreampeer легитимным или же нет);

Подытоживая: мы не можем быть уверены в клиенте, не можем быть уверены в точке подключения и в канале передачи, бонус затруднены выявление и локализация потенциального клиента-злоумышленника. Все, кроме первого, маловероятно в случае проводного подключения.

Кроме того, необходимо учитывать логическое деление беспроводных сетей.

Помимо корпоративных сетей с гостевым сегментом, для беспроводных сетей необходимо рассмотреть случаи организации публичного доступа (такого, например, как Wi-Fi в аэропортах, на конференциях и в торговых центрах), где нам необходимо обеспечить подключение самого широкого класса устройств, не имея возможности проконтролировать меры по безопасности на них; а также служебные сегменты сетей (Mesh-сети), которые в силу самой природы разделяемого доступа к среде передачи не могут быть надежно изолированы от окружающего мира. Необходимо также напомнить, что корпоративная сеть и ее гостевой сегмент не могут считаться полностью изолированными ни друг от друга, ни от внешнего мира в зависимости от используемых технологий подключения, некоторый объем информации о сети будет доступен стороннему наблюдателю.

Все вышеперечисленное делает задачу защиты беспроводных сетей весьма интересным и комплексным мероприятием.

Итак, на какие же потенциальные угрозы необходимо обратить внимание в беспроводных сетях? Вот их перечень:

* сбор информации о сети;
* сбор информации о клиентах;
* имперсонификация с целью получения доступа к сети;
* имперсонификация с целью получения контроля над клиентом;
* отказ в обслуживании (зачастую совмещенный с предыдущими пунктами).

1.3. **Идентификация пользователя.**

## Зачем нужна идентификация пользователя?

Злоумышленники, хакеры, а также террористы могут использовать гостевые WiFi-сети для сохранения своей анонимности при совершении преступлений. После терактов в Париже власти Франции предлагали даже ввести запрет на публичный Wi-Fi.

Изменения в российском законодательстве начались с антитеррористических поправок — реакции на взрывы в Волгограде в конце 2013 года. В соответствии с этими поправками Правительство РФ выпустило постановление №758 от 31 июля 2014 г., а также №801 от 12 августа 2014 г. об обязательной идентификации пользователей публичных WiFi-сетей. По закону, пользователей можно идентифицировать по паспортным данным, номеру мобильного телефона (SMS-идентификация), либо через логин на портале госуслуг. SMS-идентификация — самый простой способ для владельцев публичных точек доступа в интернет.

Данные пользователей, которые заходили в сеть через конкретную точку, понадобятся следователям в случае террористической угрозы: нельзя выйти на след подозреваемого, который заходил в интернет анонимно через публичную точку доступа. Идентификация позволяет исключить анонимность тех, кто использует публичные интернет-сети, — определить все MAC-адреса, подключенные к устройству, а значит, с большей вероятностью установить, кто совершил неправомерное действие. Это помогает следствию.

Злоумышленникам ничего не стоит создать публичную Wi-Fi-точку, назвав ее безобидным Wi-Fi Starbucks, и получить доступ к данным пользователей. Подключаясь к сети, пользователи не глядя подписываются под условиями использования. В Лондоне был проведен эксперимент, в котором для получения доступа к Wi-Fi люди соглашались с условиями, где были пункты «отдать своего первого ребенка или самое любимое домашнее животное».

**1.4. Типы протоколов подключения.**

Этот вид разделяется на следующие типы подключения (зашифрованные протоколы связи):

1. PPPoE. Это один из самых распространенных типов. С целью обеспечения доступа во всемирную паутину следует в мастере настроек кликнуть «Подключить к интернету». Далее клацнуть «Установить подключение вручную», указать одноименный тип подсоединения.
2. PPTP. Чтобы соединиться с глобальной сетью, требуется просто в мастере настройки клацнуть «Подключиться к рабочему месту». После этого выбрать графу «Подключение к виртуальной частной сети». Затем ввести адрес ВПН сервера.

## Комбинированное подключение.

Способ уже почти нигде в мире не используется, за исключением Российской Федерации. Этот тип относится к сложным и подразумевает двойной доступ «Dualaccess» с комбинированием соединений через локальную и частную сети.

При этом обеспечивается одновременный доступ к внешней глобальной и внутренним каналам поставщика интернета (интерактивное телевидение, пиринги и т.п.).

Также применяются и разные варианты с использованием локального и VPN подключений, например :

1. Доступ в глобальную сеть осуществляется с применением протокола PPPoE и адрес для работы в сети LAN присваивается в автоматическом режиме, а выход во «внешку» производится с динамической раздачей маршрутов.
2. Маршруты и адрес для подключения посредством PPPoE организуются с использованием статически заданных параметров.
3. Выход в интернет осуществляется с применением PPTP, при этом внутренний IP присваивается в автоматическом режиме, а посредством DHCP option раздаются маршруты, которые могут указываться самостоятельно либо выдаваться автоматически.
4. Этот вариант аналогичен предыдущему 3-му типу, но адреса статические, то есть задаются в ручном режиме.

Вышеуказанные комбинации могут использоваться в вариантах предоставления интернета через L2TP.

## Основные протоколы сети Интернет.

При упоминании любой сети чаще всего сейчас имеют в виду Интернет. Но, если глубже рассматривать эти явления, Интернет — не совсем отдельная сеть. Его можно назвать одним из способов передачи данных. У каждой сети свои варианты, которые контролируют работу этого элемента. Вид оборудования значения не имеет.

### IP, ICMP, TCP и UDP

IP и TCP — два совершенно разных решения. Но обычно их всё равно связывают друг с другом. На практике комбинации сразу нескольких элементов встречаются достаточно часто, поскольку это позволяет наиболее эффективно решать задачи, поставленные перед пользователем. Но каждый из элементов выполняет операции на своём, отдельном уровне. Протоколы обмена файлами в Интернете имеют обозначение согласно принятым стандартам.

TCPIP отвечает за создание интернет-пакетов, обратную сборку в месте получения. Он организует проверку целостности информации. Передача проходит повторно, если часть сведений всё-таки потеряна.

### Протоколы HTTP и HTTPS

HTML — так называемый язык гипертекста, который часто используют на различных страницах в Интернете. По сети эти страницы тоже передаются по определённому стандарту. Это протокол передачи гипертекста, который и обозначается как HTTP.

HTTPS — ещё один компонент, связанный с этим направлением. Он нужен для обеспечения шифрования при передаче данных, чтобы конфиденциальная информация получала дополнительную защиту. Адреса, поддерживающие протокол, имеют соответствующее обозначение.

## Какой протокол является базовым для сети Интернет.

TCP/IP — самый распространённый протокол, по которому в настоящее время передаётся информация. Хранение базовой передаваемой информации обеспечивается за счёт добавления к этой схеме трёх параметров:

* повторная отправка запросов, если возникла ошибка;
* идентификатор, по которому действия подтверждают механически;
* порядковый номер для определения приоритета, очереди пересылки сведений. Называться он может по-разному.

**Угрозы со стороны не законных подключений к беспроводным сетям.**

# Безопасность сетей 802.11 — основные угрозы.

##### Риск первый — Чужаки (RogueDevices, Rogues).

Чужаками называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, зачастую в обход механизмов защиты, определенных корпоративной политикой безопасности. Чаще всего это те самые самовольно установленные точки доступа. Статистика по всему миру, например, указывает на чужаков, как на причину большинства взломов сетей организаций. Даже если организация не использует беспроводную связь и считает себя в результате такого запрета защищенной от беспроводных атак – внедренный (умышленно или нет) чужак с легкостью исправит это положение. Доступность и дешевизна устройств Wi-Fi привели к тому, что в США, например, практически каждая сеть с числом пользователей более 50 успела ознакомиться с данным феноменом.  
Помимо точек доступа в роли чужака могут выступить домашний роутер с Wi-Fi, программная точка доступа Soft AP, ноутбук с одновременно включенными проводным и беспроводным интерфейсом, сканер, проектор и т.д.

**Риск второй — нефиксированная природа связи**

Как уже было сказано выше – беспроводные устройства не «привязаны» кабелем к розетке и могут менять точки подключение к сети прямо в процессе работы. К примеру, могут происходить «Случайные ассоциации», когда ноутбук с Windows XP (достаточно доверительно относящейся ко всем беспроводным сетям) или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Такой механизм позволяет злоумышленникам «переключать на себя» ничего не ведающего пользователя для последующего сканирования уязвимостей, фишинга или атак Man-in-The-Middle. Кроме того, если пользователь одновременно подключен и к проводной сети – он только что стал удобной точкой входа – т.е. классическим чужаком.

##### **Риск третий — уязвимости сетей и устройств**

Некоторые сетевые устройства, могут быть более уязвимы, чем другие – могут быть неправильно сконфигурированы, использовать слабые ключи шифрования или методы аутентификации с известными уязвимостями. Неудивительно, что в первую очередь злоумышленники атакуют именно их. Отчеты аналитиков утверждают, что более 70 процентов успешных взломов беспроводных сетей произошли именно в результате неправильной конфигурации точек доступа или клиентского ПО.

##### **Риск четвертый — новые угрозы и атаки**

Беспроводные технологии породили новые способы реализации старых угроз, а также некоторые новые, доселе невозможные в проводных сетях. Во всех случаях, бороться с атакующим стало гораздо тяжелее, т.к. невозможно ни отследить его физическое местоположение, ни изолировать его от сети.

##### **Риск пятый — утечки информации из проводной сети**

Практически все беспроводные сети в какой-то момент соединяются с проводными. Соответственно, любая беспроводная точка доступа может быть использована как плацдарм для атаки. Но это еще не все: некоторые ошибки в конфигурации точек доступа в сочетании с ошибками конфигурации проводной сети могут открывать пути для утечек информации. Наиболее распространенный пример – точки доступа, работающие в режиме моста (Layer 2 Bridge), подключенные в плоскую сеть (или сеть с нарушениями сегментации VLAN) и передающие в эфир широковещательные пакеты из проводного сегмента, запросы ARP, DHCP, фреймы STP и т.д. Некоторые из этих данных могут быть полезными для организаций атак Man-in-The-Middle, различных Poisoning и DoS атак, да и просто разведки.  
Другой распространенный сценарий основывается на особенностях реализации протоколов 802.11. В случае, когда на одной точке доступа настроены сразу несколько ESSID, широковещательный трафик будет распространятся сразу во все ESSID. В результате, если на одной точке настроена защищенная сеть и публичный хот-спот, злоумышленник, подключенный к хот-споту, может, например, нарушить работу протоколов DHCP или ARP в защищенной сети. Это можно исправить, организовав грамотную привязку ESS к BSS, что поддерживается практически всеми производителями оборудования класса Enterprise (и мало кем из класса Consumer), но об этом нужно знать.

##### **Риск шестой — особенности функционирования беспроводных сетей**

Некоторые особенности функционирования беспроводных сетей порождают дополнительные проблемы, способные влиять в целом на их доступность, производительность, безопасность и стоимость эксплуатации. Для грамотного решения этих проблем требуется специальный инструментарий поддержки и эксплуатации, специальные механизмы администрирования и мониторинга, не реализованные в традиционном инструментарии управления беспроводными сетями.

Итого, беспроводные сети порождают новые классы рисков и угроз, от которых невозможно защититься традиционными проводными средствами. Даже если в организации формально запрещен Wi-Fi – это еще не значит, что кто-нибудь из пользователей не установит чужака и сведет этим все вложения в безопасность сети к нулю. Кроме того, ввиду особенностей беспроводной связи, важно контролировать не только безопасность инфраструктуры доступа, но и следить за пользователями, которые могут стать объектом атаки злоумышленника либо просто могут случайно или умышленно перейти с корпоративной сети на незащищенное соединение.  
  
Хорошей новостью, после столь депрессивного изложения, является то, что большинство перечисленных рисков могут быть минимизированы или вообще сведены к нулю.

**Угрозы и способы их распространения**

Доступ в Интернет открыт для всех пользователей. Любой компьютер или иное устройство, подключенное к Сети, может стать объектом атаки мошенников. Владелец не всегда имеет представление о том, что его файлы находятся под угрозой и нужно только уметь до них добраться. Они могут быть похищены, изменены или удалены. Физические способы защиты информации от несанкционированного доступа в данном случае малоэффективны.

Чаще всего несанкционированный доступ к чужой информации реализуется с помощью программного обеспечения, которое засылается на компьютер пользователя разными способами:

* в виде нагрузки к файлам, скачанным в Сети;
* с электронной почтой;
* с файлами, отправленными в социальных сетях, мессенджерах.

Принцип работы вредоносного ПО (или, как его обычно называют, компьютерных вирусов) заключается в том, что в оперативную память или на жесткий диск загружается небольшой самораспаковывающийся архив. Когда файл, содержащий вирус, загружен и запущен, вирус восстанавливает свой объем и встраивается в операционную систему. После этого его программа запускается и начинает действовать. Например, сканирует специальные разделы операционных систем и находит пароли, после чего отсылает их злоумышленнику. Примечательно, что большинство подобных вирусов действует вслепую, т. е. мошенник не всегда знает, кто оказался его жертвой.

## Средства защиты информации.

Для того чтобы предотвратить проникновение вредоносного ПО в систему компьютера используются различные программные и аппаратные средства.

Среди наиболее распространенных средств защиты информации – брандмауэры (или файрволы) и антивирусные программы.

Брандмауэр (межсетевой экран) – это программа, отсекающая попытки несанкционированного доступа злоумышленников из Сети. Кроме этого, он контролирует установленные программы и запрещает им несанкционированную передачу данных. Многие пользователи знают, что для запуска онлайн-игр или других веб-приложений надо сначала отключить брандмауэр, иначе связи с игровым сервером не будет.

Дополнительной функцией файрвола является контроль портов компьютера, поскольку через них также осуществляется прием и передача информации.

Встроенные брандмауэры есть на операционных системах Windows, начиная с XP и выше.

# Как регистрировать и использовать программы без проблем с законом

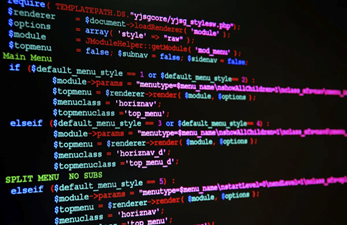
Программное обеспечение (ПО) - один из самых распространенных и перспективнейших нематериальных активов в настоящее время. Что же представляет с собой программное обеспечение с точки зрения права?

В первую очередь обратимся к статье 1261 Гражданского кодекса РФ. Данная статья посвящена правовой охране программы для ЭВМ как таковой. К числу программ для ЭВМ закон относит в том числе операционные системы и программные комплексы.

С точки зрения закона программа для ЭВМ - это совокупность данных и команд, при выполнении которых достигается определенный результат, а также порождаемые ею аудио и видео. Таким образом, в составе программы для ЭВМ можно выделить следующие охраняемые элементы:

1. исходный текст - текст такой программы, написанный на одном из языков программирования, и объектный код;

2. подготовительные материалы, полученные в процессе создания программы для ЭВМ;



3.аудиовизуальные отображения, порождаемые программой, в частности, интерфейс, дизайн компьютерных игр и т.п.

Закон охраняет программу для ЭВМ как литературное произведение. Что это значит на практике? Закон охраняет программу как исходный текст и объектный код, то есть форму программы, а не её алгоритм или идею.

## Приобретение прав на программное обеспечение

Правовая защита программное обеспечения начинается с оформления прав на него при приобретении или создании.

Права на программное обеспечение могут быть приобретены различными способами.

Самый простой - покупка уже созданного программного обеспечения у физического лица путем заключения договора об отчуждении исключительного права на программу для ЭВМ. Однако необходимо понимать, что такой способ крайне ограничен в сфере применения и по сути подходит только для ситуаций, когда автор программы уже создал её и желает продать.

Гораздо более распространены случаи, когда ПО создается по заказу фрилансерами или Вашими работниками.

 Такой способ требует особого внимания к оформлению документов с разработчиками. Почему? Согласно Гражданскому кодексу РФ первоначально права на программу ЭВМ возникают у её авторов-физических лиц. Поэтому если Вы не лично писали исходный код программы и создавали дизайн интерфейса, важно надлежащим образом оформить переход прав на ПО Вам.

При этом важно учитывать, что помимо самой программы для ЭВМ, созданной разработчиками-программистами, в состав программного обеспечения могут входить и иные объекты интеллектуальной собственности, о чем мы говорили в разделе 1. Важно оформить переход прав от всех таких разработчиков.

**Права авторов разработчиков.**

Говоря о правах авторов-разработчиков необходимо учитывать, что наряду с исключительными правами, которые могут быть переданы по договору, автор также обладает личными неимущественными правами, которые не могут быть переданы:

право авторства (то есть право признаваться автором ПО),

право на имя (то есть право разрешать использование ПО с указанием себя в качестве автора или анонимно),

право на неприкосновенность объекта (право разрешать или не разрешать внесение изменений в ПО)

Поэтому очень важно предусмотреть в договоре с автором необходимые Вам возможности: например, возможность использовать ПО анонимно, без указания фамилий разработчиков, возможность внесения в ПО изменений и т.д.

Закон предусматривает, как было сказано выше, специальный договор о создании объектов авторского права - договор авторского заказа. Более правильным является именно его заключение с разработчиками программ - физическими лицами. Но и в данном договоре важно предусмотреть все изложенные выше условия, а также обязательно регламентировать:

Срок создания ПО,

Цену договора или безвозмездность выполнения работ по созданию,- эти условия являются существенными, то есть обязательно должны быть указаны в договоре, иначе он считается незаключенным.

## Способы защиты программного обеспечения. Регистрация программы для ЭВМ

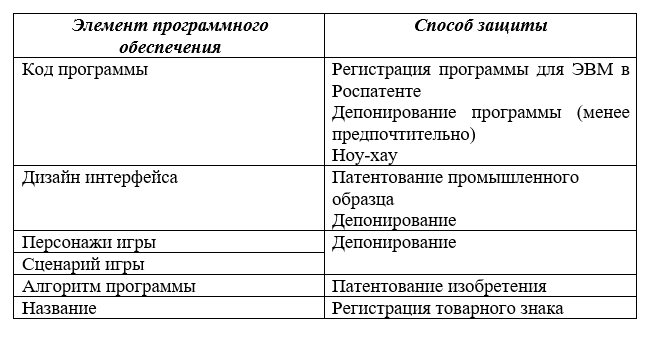
Как мы уже говорили выше, программа для ЭВМ является объектом авторского права, поэтому права на неё возникают с момента создания и не требует соблюдения каких-либо формальностей (пункт 4 статьи 1259 Гражданского кодекса РФ).

С одной стороны, это очень удобно - разработчики написали программу, Вы оформили с ними необходимые документы, о которых мы говорили в прошлом разделе - и Вы правообладатель программного обеспечения. Не нужно ждать регистрации, не нужно платить пошлины...

Но у такой простоты есть и отрицательные стороны. В случае, если кто-то будет использовать Ваше программное обеспечение и Вы решите обратиться в суд, Вам нужно будет доказать, что права на это ПО принадлежат Вам.

Именно формированию таких доказательств служат способы защиты прав на программное обеспечение, о которых мы хотели поговорить в данном разделе.

Для удобства сведем все эти способы в таблицу, а далее рассмотрим каждый способ в отдельности.

****

Первоочередным способом оформления прав на ПО является **регистрация программы для ЭВМ в Роспатенте** (а именно в его подведомственной организации Федеральном институте промышленной собственности - ФИПС). Такая регистрация защищает в первую очередь коды программы, так как именно они являются основным элементом программы ЭВМ.

**Угрозы информационной безопасности Wi-FI.**

# Очевидно, что в беспроводных сетях в качестве среды передачи данных используется радиоэфир. В то же время, вследствие его высокой доступности, остро встает вопрос обеспечения безопасности передаваемых через беспроводную сеть данных. Поэтому безопасность в беспроводных сетях обеспечивается на трех уровнях:

# · Физический;

# · Канальный;

# · Транспортный.

# На физическом уровне существуют два метода защиты - помехообразующие устройства и широковещание SSID. Помехообразующие устройства можно установить по периметру требуемого радиуса сети, чтобы беспроводная сеть функционировала только в заданной области, и ее сигнал невозможно было поймать вне этой зоны. Также существует возможность отключения широковещания SSID. SSID - это ServiceSetIdentifier, иными словами - имя сети, которое транслируется в сеть при помощи специальных пакетов раз в 100мс.

# Для повышения безопасности рекомендуется отключать широковещание SSID. Благодаря этому, вы сможете "скрыть" свою сеть, и подключение к ней будет возможно только после указания SSID. Однако данный метод защиты не является панацеей, так как злоумышленник сможет узнать SSID после анализа пакетов. На канальном уровне также существует метода защиты, такой как фильтрация MAC-адресов. При подключении к точке доступа, выполняется проверка MAC-адреса клиентского устройства, и если он совпадает с "белым списком", то разрешается подключение к сети. Аналогично, есть возможность работы по принципу "черного" списка. Становится ясно, что для защиты данных необходимо использовать механизмы шифрования на транспортном уровне.

# *Алгоритмы безопасности беспроводных сетей*

# Wired Equivalent Privacy (WEP) алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. Это одна из первых технологий, в настоящее время она является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. В основе WEP лежит поточный шифр RC4, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется CRC32.

# Формат кадра

# Кадр WEP включает в себя следующие поля:

# · Незашифрованная часть;

# · Вектор инициализации (англ. InitializationVector) (24 бита);

# · Пустое место (англ. Padding) (6 бит);

# · Идентификатор ключа (англ. Key*ID*) (2 бита);

# · Зашифрованная часть;

# · Данные;

# · Контрольная сумма (32 бита).

# Рисунок 1. Формат кадра WEP

# Ключи

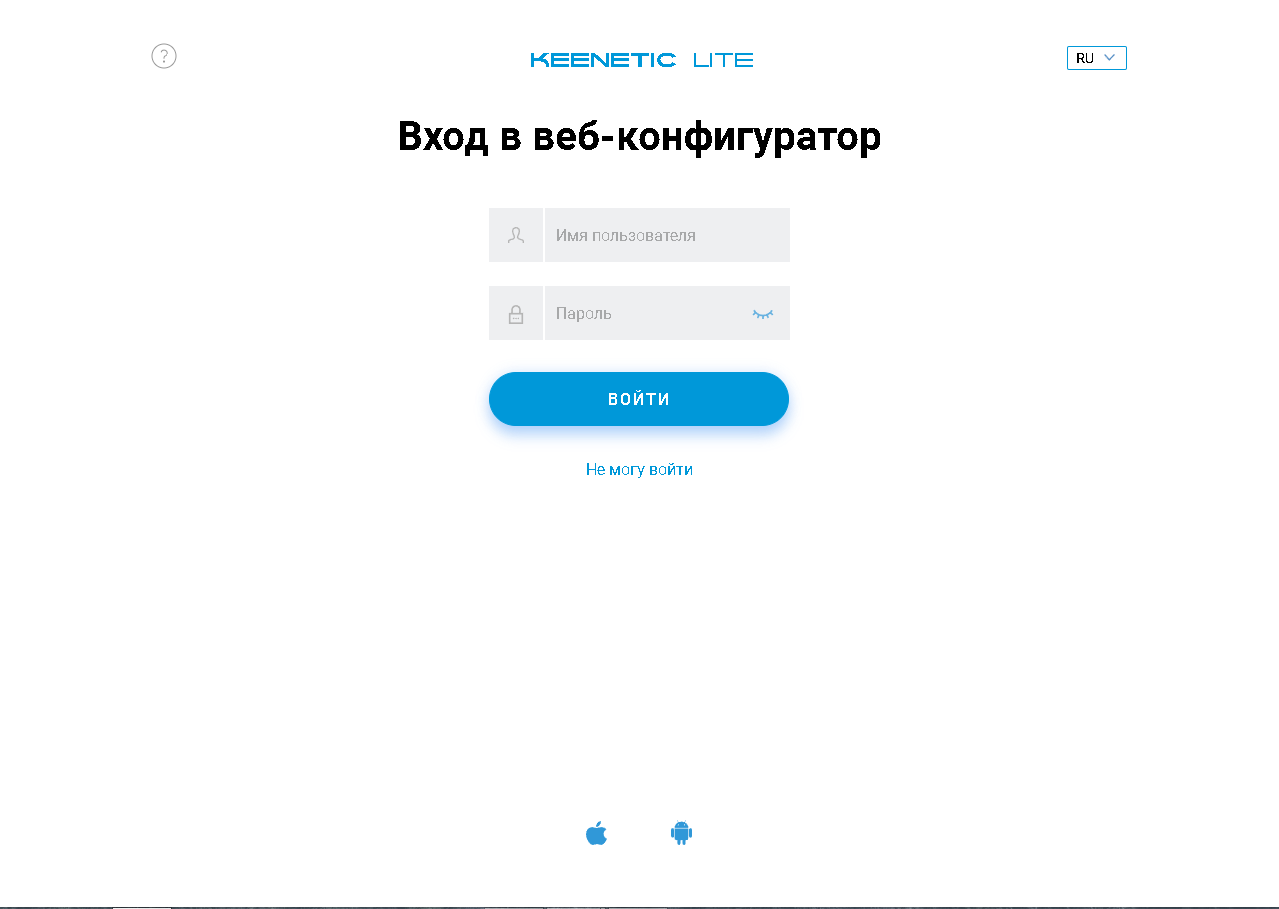
# Ключи имеют длину 40 и 104 бита для WEP-40 и WEP-104 соответственно. Используются два типа ключей:

# · ключи по умолчанию

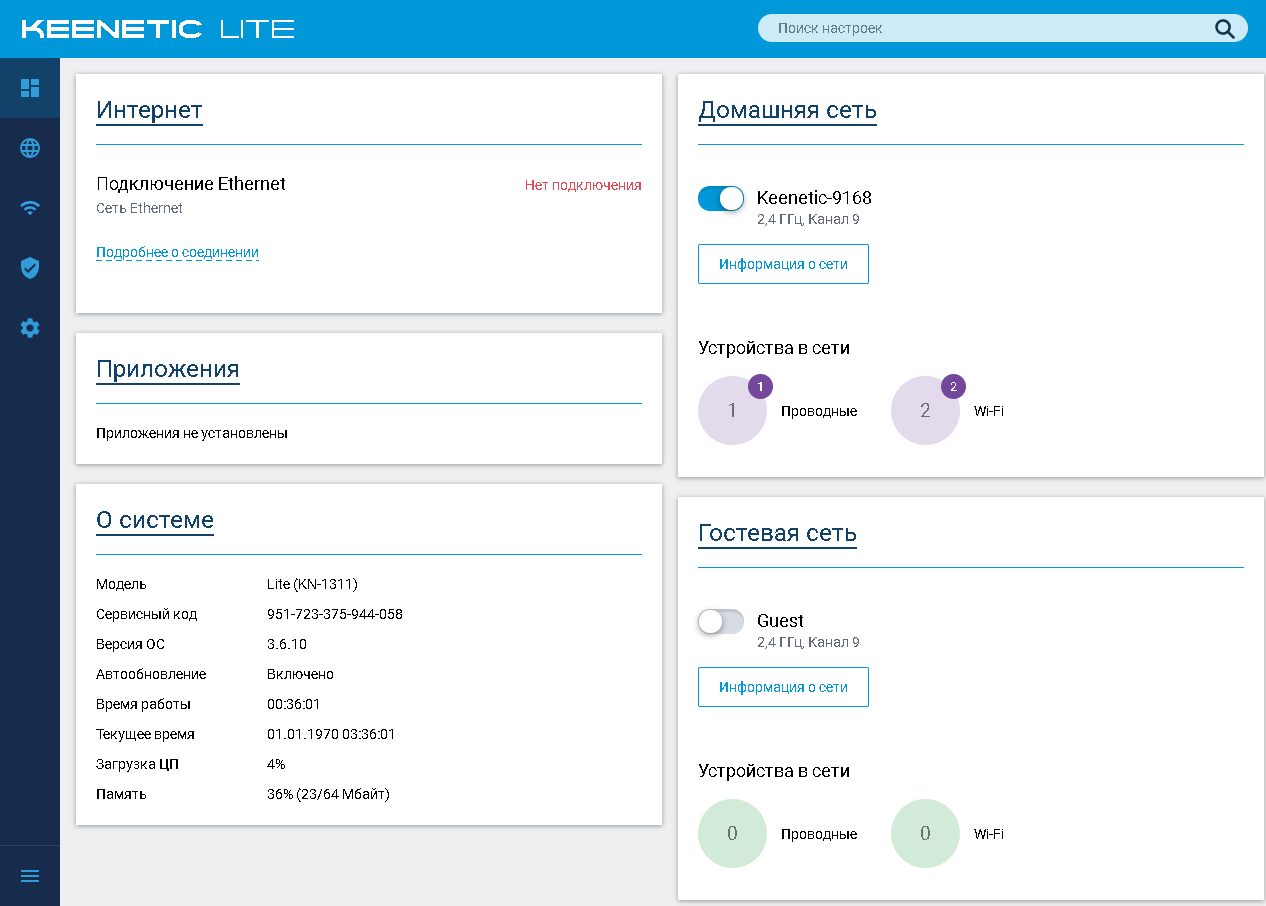
# · назначенные ключи.

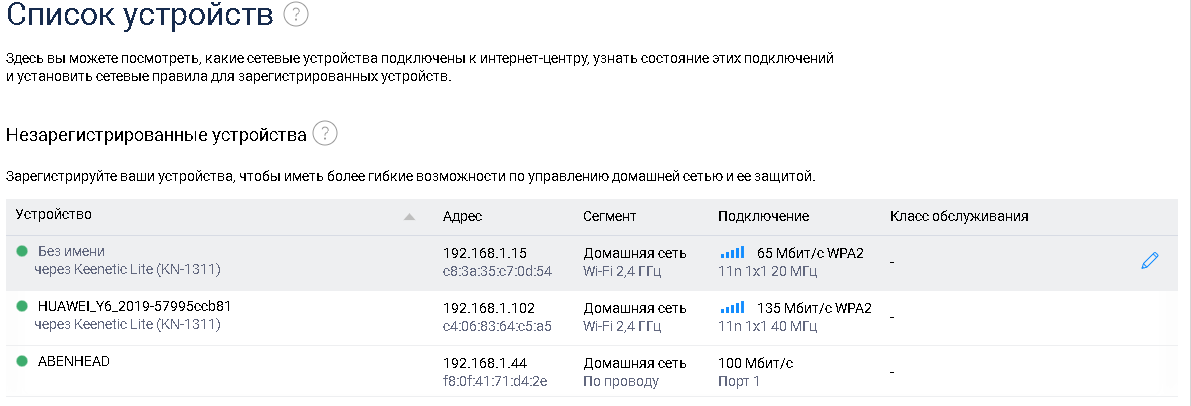
**Практическая часть.**

1. Мы заходим на выданный роутер KeeneticLiteи подключаемся на его веб- интерфейс.



1. Авторизуемся и выходим на веб-интерфейс:



1. Устройства которые зашли на роутер:

**Средства защиты информации в локальных вычислительных сетях при межсетевом взаимодействии**

### Законодательное регулирование межсетевого экранирования

Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.

Межсетевой экран - это программный или программно-аппаратный элемент компьютерной сети. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

Требования к межсетевым экранам определены приказом ФСТЭК России от 9 февраля 2016 г. №9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный №41564 для служебного пользования). Требования к межсетевым экранам выпущены на замену Руководящему документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД МЭ), утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

В целях разъяснения позиции ФСТЭК России в связи с утверждением Требований к межсетевым экранам было выпущено Информационное сообщение по вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации от 24 марта 2017 г. №240/24/1382.

Согласно информационного сообщения, с 1 декабря 2016 г. в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 сертификация разработанных и (или) производимых межсетевых экранов осуществляется на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. №9.

Согласно Требований 2016 года устанавливается 5 типов межсетевых экранов:

* Типа А - уровня сети;
* Типа Б – уровня логических границ сети;
* Типа В – уровня узла;
* Типа Г – уровня веб-сервера;
* Типа Д – уровня промышленной сети (АСУ ТП).

### Типы межсетевых экранов

«А» – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы. Межсетевые экраны типа «А» могут иметь только программно-техническое исполнение;

«Б» – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы. Межсетевые экраны типа «Б» могут иметь программное или программно-техническое исполнение;

«В» – межсетевой экран, применяемый на узле (хосте) информационной системы. Межсетевые экраны типа «В» могут иметь только программное исполнение и устанавливаются на мобильных или стационарных технических средствах конкретного узла информационной системы;

«Г» – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;

«Д» – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных.

# Законодательство об информационной безопасности: 5 ФЗ о том, как хранить и защищать информацию

## 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[149-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_61798/) — главный закон об информации в России. Он определяет ключевые термины, например, говорит, что информация — это любые данные, сведения и сообщения, представляемые в любой форме. Также там описано, что такое сайт, электронное сообщение и поисковая система. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

Основные функции которые защищают нас с юридической стороны.

1. Нельзя собирать и распространять информацию о жизни человека без его согласия.
2. Все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.
3. Есть информация, к которой нельзя ограничивать доступ, например сведения о состоянии окружающей среды.
4. Некоторую информацию распространять запрещено, например ту, которая пропагандирует насилие или нетерпимость.
5. Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.
6. У государства есть [реестр запрещенных сайтов](https://eais.rkn.gov.ru/). Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.

# Механизмы защиты информации в сетях WiMAX

Стандарт 802.16 разрабатывался с учетом накопленного опыта построения беспроводных сетей, поэтому оказался избавленным от большинства уязвимостей, присущих сетям 802.11. Реализована аутентификация с использованием цифровой подписи и сертификатов Х.509, причем процедура аутентификации периодически повторяется в процессе работы пользователя. Используются различные ключи для аутентификации, шифрования трафика и шифрования сеансовых ключей. Оборудование WiMAX предназначено в первую очередь для операторов связи, и безопасность заложена в него еще на этапе разработки стандарта 802.16, которым определено, что весь трафик должен быть зашифрован с использованием алгоритма AES, а для аутентификации используется протокол на основе TLS с шифрованием открытым ключом. В системах Fixed Broadband Wireless Access, к которым относится и WiMAX-сертифицированные системы, беспроводное устройство является граничным в сети, поэтому к нему предъявляются требования по маршрутизации и ограничению входящего и исходящего трафика, а также шифрации передаваемого в эфир трафика. Однако аутентификация абонентов оборудованием данного класса не производится. Кроме того, устройство имеет аппаратно прошитый сертификат, который крайне сложно подделать.

Вообще уязвимость беспроводных сетей заложена в самой их природе, в относительной простоте перехвата трафика, в нестойкости канала связи к всевозможным воздействиям. На это накладывается несовершенство платформенной реализации этой технологии и возможность атаки на операционную систему хоста на сетевом уровне модели ISO. Как бы ни развивались механизмы безопасности, встроенные в сетевые технологии, они не станут достаточными для обеспечения безопасности информационных систем корпоративного и государственного уровня.

В отличие от технологии беспроводных локальных сетей 802.11, WiMAX уже сразу в стандартах предполагает реализацию достаточно серьезных функций безопасности.

Среди основных и наиболее значительных необходимо отметить следующие:

* — аутентификация пользовательского оборудования путем обмена сертификатами с базовой станцией для исключения возможности функционирования неавторизированного терминала;
* — аутентификация пользователя с использованием протокола ЕАР (Extensible Authentification Protocol — расширяемый протокол аутентификации);
* — кодирование передаваемых данных с использованием стандарта AES (Advanced Encryption Standard). Данные каждой из предоставляемых услуг шифруются с собственными ключами, что позво- ляяет избегать перехвата и расшифровки трафика терминалами, авторизированными для работы в том же домене WiMAX;
* — на канальном уровне в подуровне MAC предусмотрено использование механизма типа «запрос — ответ» (grant — request) для авторизации права передачи данных. Кроме улучшения безопасности данная функция упрощает управление и поддержку трафика реального времени, а также голосовых приложений.

Как известно, обеспечение качества обслуживания (QoS, Qualityof Service) является сравнительно старой задачей или даже проблемой сетей, построенных на протоколе IP. Было предложено большое количество методов, алгоритмов и даже архитектур, но проблема и по сей день, фактически, решается путем предоставления для трафика избыточных сетевых ресурсов. Реализация беспроводного интерфейса на доступе к сети делает проблему еще более сложной: неустойчивые характеристики беспроводных каналов существенно повышают значения задержки передачи пакета и вероятности возникновения ошибки. Стандарт 802.16 изначально разрабатывался с учетом описанной проблемы, поэтому уже сейчас можно утверждать, что поддержка качества обслуживания в технологии WiMAX является одной из приоритетных задач. Концептуальным является отказ от вероятностного алгоритма конкуренции за право передачи на канальном уровне в подуровне MAC (Media Access Control — контроль доступа к среде передачи), реализованного в беспроводных локальных сетях, и переход на детерминированный (polling-based) алгоритм «опроса на передачу». Более того, начиная со стандарта 802.11а, на подуровне MAC реализована процедура разделения канала на временные слоты TDMA, что позволяет существенно улучшить характеристики предоставляемой услуги с точки зрения значения параметра задержки. Среди остальных механизмов QoS необходимо отметить ARQ (Automatic Repeat Request автоматический запрос на повторную передачу) и обеспечение QoS для отдельного соединения (рег- connection QoS).

 При работе последнего из механизмов, каждое соединение ассоциируется с функцией планировщика данных, а эта функция, в свою очередь, ассоциируется с набором значений параметров QoS, определяющих ее функционирование. В стандарте 802.16-2004 определеныследующиетипыуслуг:

* — UGS (UnsolicitedGrantService — услуга постоянной скорости передачи) разработана для поддержки трафика с постоянной скоростью передачи, например, эмуляция Е1;
* — rtPS (Real-timePollingService — услуга реального времени с опросом на передачу) разработана для поддержки трафика с переменной скоростью передачи реального времени, например, трафик MPEG1;
* — nrtPS (Non-real-timePollingService — услуга нереального времени с опросом на передачу) разработана для поддержки трафика с переменной скоростью передачи, не предъявляющего жесткие требования к значениям параметров QoS, например, трафик FTP;
* — BE (BestEffort — услуга наилучшей попытки) разработана для поддержки обычного трафика Интернета.

## Механизмы защиты информации в сетях Wi-Fi

Большинство существующего на данный момент Wi-Fi оборудования имеет поддержку технологии WPA (Wi-FiProtectedAccess), которая пришла на смену технологии WEP.

Технология WPA состоит из нескольких компонентов:

* — протокол 802.1х — универсальный протокол для аутентификации, авторизации и учета (ААА);
* — протокол ЕАР — расширяемый протокол аутентификации (ExtensibleAuthenticationProtocol);
* — протокол TKIP — протокол временной целостности ключей, другой вариант перевода — протокол целостности ключей во времени (TemporalKeyIntegrityProtocol);
* — MIC — криптографическая проверка целостности пакетов (MessageIntegrityCode);
* — протокол RADIUS.

За шифрование данных в WPA отвечает протокол TKIP, который в отличие от WEP, использует динамические ключи (то есть ключи часто меняются). Он применяет более длинный вектор инициализации и использует криптографическую контрольную сумму (MIC) для подтверждения целостности пакетов (последняя является функцией от адреса источника и назначения, а также поля данных).

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS- сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме.

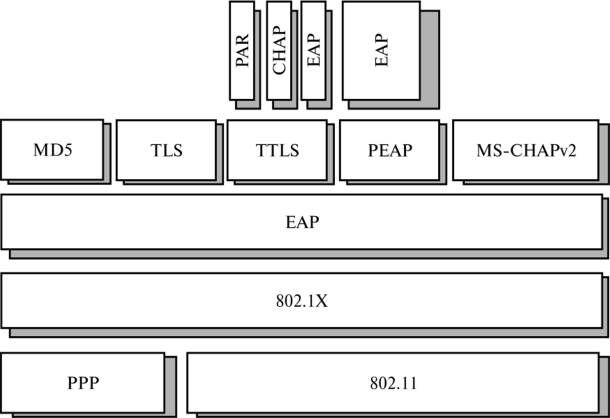
Если в сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа — так называемый режим WPA-PSK (pre-sharedkey, общий ключ). В этом режиме в настройках всех точек доступа заранее прописывается общий ключ. Он же прописывается и на клиентских беспроводных устройствах. Такой метод защиты не очень удобен с точки зрения управления. PSK-ключ требуется прописывать на всех беспроводных устройствах, пользователи беспроводных устройств его могут видеть. Если потребуется заблокировать доступ какому-то клиенту в сеть, придется заново прописывать новый PSK на всех устройствах сети и так далее. Другими словами, режим WPA-PSK подходит для домашней сети и, возможно, небольшого офиса, но не более того.

В технологии WPA2 используется протокол ССМР (CounterModewithCipherBlockChainingMessageAuthenticationCodeProtocol), взамен TKIP, в нем применяется усовершенствованный стандарт шифрования AES (AdvancedEncryptionStandard). А для управления и распределения ключей по-прежнему применяется протокол 802.1х.

Как уже было сказано выше, протокол 802.1х может выполнять несколько функций. В данном случае нас интересуют функции аутентификации пользователя и распределение ключей шифрования. Необходимо отметить, что аутентификация происходит «на уровне порта» — то есть пока пользователь не будет аутентифицирован, ему разрешено посылать/принимать пакеты, касающиеся только процесса его аутентификации (учетных данных) и не более того. Только после успешной аутентификации порт устройства будет открыт и пользователь получит доступ к ресурсам сети.

Функции аутентификации возлагаются на протокол EAR Кадр этого протокола приведен на рис. 5.13. Протокол ЕАР является лишь каркасом для методов аутентификации. Данный протокол очень просто реализовать на аутентификаторе (точке доступа), так как ей не требуется знать никаких специфичных особенностей различных методов аутентификации. Аутентификатор служит лишь передаточным звеном между клиентом и сервером аутентификации. Методов же аутентификации, которых существует довольно много:

* — ЕАР-SIM, ЕАР-АКА — используются в сетях GSM мобильной связи;
* — LEAP — методот Cisco systems;
* — EAP-MD5 — простейший метод, аналогичный CHAP (не стойкий);
* — EAP-MSCHAP V2 — метод аутентификации на основе логи- на/пароля пользователя в MS-сетях;
* — EAP-TLS — аутентификация на основе цифровых сертификатов;
* — EAP-SecurelD — метод на основе однократных паролей.



**Структура ЕАР-кадра**

Кроме вышеперечисленных, следует отметить следующие два метода, EAP-TTLS и ЕАР-РЕАР. В отличие от предыдущих, эти два метода перед непосредственной аутентификацией пользователя сначала образуют TLS-туннель между клиентом и сервером аутентификации. А уже внутри этого туннеля осуществляется сама аутентификация, с использованием как стандартного ЕАР (MD5, TLS), или старых методов (PAP, CHAP, MS-CHAP, MS-CHAP v2), последние работают только с EAP-TTLS (РЕАР используется только совместно с ЕАР методами). Предварительное туннелирование повышает безопасность аутентификации, защищая от атак типа «man- in-middle», «sessionhihacking» или атаки по словарю.

Протокол РРР появился на рис. 5.13 потому, что изначально ЕАР планировался к использованию поверх РРР туннелей. Но так как использование этого протокола только для аутентификации по локальной сети — излишняя избыточность, ЕАР-сообщения упаковываются в «ЕАР over LAN» (EAPOL) пакеты, которые и используются для обмена информацией между клиентом и аутентификатором (точкой доступа).

Схема аутентификации состоит из трех компонентов:

* — Supplicant-софт, запущенный на клиентской машине, пытающейся подключиться к сети;
* — Authenticator — узел доступа, аутентификатор (беспроводная точка доступа или проводной коммутатор с поддержкой протокола 802Лх);
* — AuthenticationServer — сервер аутентификации (обычно это RADIUS-сервер).

Теперь рассмотрим сам процесс аутентификации. Он состоит из следующих стадий:

* 1. Клиент может послать запрос на аутентификацию (EAP-startmessage) в сторону точки доступа
* 2. Точка доступа (аутентификатор) в ответ посылает клиенту запрос на идентификацию клиента (EAP-request/identitymessage). Аутентификатор может послать EAP-request самостоятельно, если увидит, что какой-либо из его портов перешел в активное состояние.
* 3. Клиент в ответ высылает ЕАР-responsepacket с нужными данными, который точка доступа (аутентификатор) перенаправляет в сторону Radius-сервера (сервера аутентификации).
* 4. Сервер аутентификации посылает аутентификатору (точке доступа) challenge-пакет (запрос информации о подлинности клиента). Аутентификатор пересылает его клиенту.

# Пути решения проблем защиты информации в сетях

Для поиска решений проблем информационной безопасности при работе в сети Интернет был создан независимый консорциум ISTF (InternetSecurityTaskForce) — общественная организация, состоящая из представителей и экспертов компаний-по-ставщиков средств информационной безопасности, электронных бизнесов и провайдеров Internet-инфраструктуры. Цель консорциума — разработка технических, организационных и операционных руководств по безопасности работы в Internet.

Консорциум ISTF выделил 12 областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание создатели электронного бизнеса, чтобы обеспечить его работоспособность. Этот список, в частности, включает:

* • аутентификацию (механизм объективного подтверждения идентифицирующей информации);
* • право на частную, персональную информацию (обеспечение конфиденциальности информации);
* • определение событий безопасности (SecurityEvents);
* • защиту корпоративного периметра;
* • определение атак;
* • контроль за потенциально опасным содержимым;
* • контроль доступа;
* • администрирование;
* • реакцию на события (IncidentResponse).
* Рекомендации ISTF предназначены для существующих или
* вновь образуемых компаний электронной коммерции и электронного бизнеса.
* Их реализация означает, что защита информации в системе электронного бизнеса должна быть комплексной.

Для комплексной защиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо:

* • проанализировать угрозы безопасности для системы электронного бизнеса;
* • разработать политику информационной безопасности;
* • защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
* • гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Internet, а также общения с пользователями этих сетей;
* • защитить отдельные наиболее коммерчески значимые ИС независимо от используемых ими каналов передачи данных;
* • предоставить персоналу защищенный удаленный доступ к информационным ресурсам корпоративной сети;
* • обеспечить надежное централизованное управление средствами сетевой защиты.

Согласно рекомендациям ISTF, первым и важнейшим этапом разработки системы информационной безопасности электронного бизнеса являются механизмы управления доступом к сетям общего пользования и доступом из них, а также механизмы безопасных коммуникаций, реализуемые МЭ и продуктами защищенных виртуальных сетей VPN.

Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI — инфраструктура открытых ключей), можно получить целостную, централизованно управляемую систему информационной безопасности.

Следующий этап включает интегрируемые в общую структуру средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (SingleSignOn).

Антивирусная защита, средства аудита и обнаружения атак, по существу, завершают создание интегрированной целостной системы безопасности, если речь не идет о работе с конфиденциальными данными. В этом случае требуются средства криптографической защиты данных и электронно-цифровой подписи.