|  |
| --- |
| Министерство образования Новосибирской области Государственное бюджетное профессиональное образовательное учреждение  Новосибирской области  «Новосибирский колледж почтовой связи и сервиса» |
| **ДОПУЩЕН КЗАЩИТЕ**  зам. 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  цикловойкомиссии  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

**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.

#### 1.1.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.

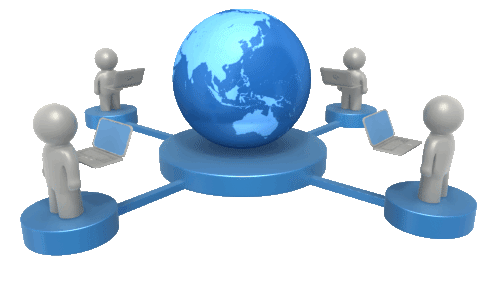
 Интересной особенностью беспроводных сетей является организация публичного и незащищенного доступа, приводящая к целому классу проблем безопасности, совершенно несвойственных проводным сетям.

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 (sharedmedium), 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? Вотихперечень:

* 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 предлагалидаже 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-FiStarbucks, 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

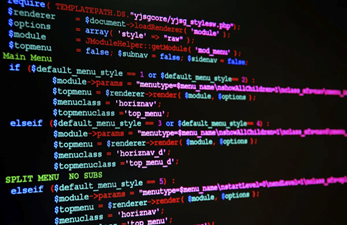
Программное обеспечение (ПО) - один из самых распространенных и перспективнейших нематериальных активов в настоящее время. Что же представляет с собой программное обеспечение с точки зрения права?

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

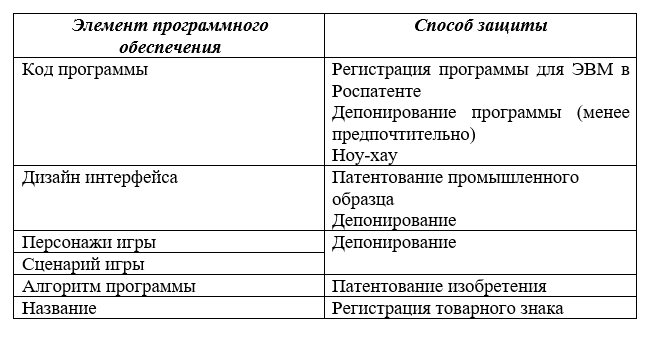
Как мы уже говорили выше, программа для ЭВМ является объектом авторского права, поэтому права на неё возникают с момента создания и не требует соблюдения каких-либо формальностей (пункт 4 статьи 1259 Гражданского кодекса РФ).

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.

# *Алгоритмыбезопасностибеспроводныхсетей*

# WiredEquivalentPrivacy (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.**