ГБОУ Гимназия №1505

«Московская городская педагогическая гимназия-лаборатория»

**Диплом**

**Беспроводные сети и защита информации в них**

*автор*: ученица 10 класса «Б»

Точилкина Маргарита

*Руководитель:* Пяткина Г.А.

 Москва

 2016

**Оглавление**

Введение

Глава I. Проблема защиты информации в беспроводных сетях

§1.Причины использования беспроводных сетей и области их применения

§2.Виды беспроводных сетей

§3.Стандарты локальных беспроводных сетей

§4.Обеспечение безопасности во время подключения к сети

§5.Защита информации шифрованием

Глава II. Разработка программы потокового шифра

Заключение

Список литературы

***Введение***

*Беспроводные компьютерные сети* (Wireless Area Network) — это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей без использования кабельной проводки. В последнее время всё больше и больше устройств оснащается беспроводными модулями передачи данных, так как они позволяют свободно перемещаться в пределах радиоволн и не терять соединение с сетью интернет. С устройствами, использующими беспроводную передачу данных, появилась возможность свободно перемещаться:

1. По комнате или квартире (в случае персональной, реже локальной сети);
2. По офису и другим рабочим помещениям (в случае локальной сети);
3. По зданиям, в которых располагаются государственные учреждения (полиция, больницы и т.д.) (в случае муниципальной или городской сети);
4. По всему городу или стране (в случае глобальной сети).

У каждой такой сети есть свои стандарты, которые определяются в соответствии с радиусом действия и назначением.

Локальные беспроводные сети (Wireless Local Area Network, WLAN) являются наиболее часто повсеместно используемыми. Радиус действия беспроводных локальных в среднем составляет примерно 200-250 метров. Наиболее распространённым на сегодняшний день способом построения является Wi-Fi.

Проведение финансовых операций с использованием Интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам требуют обеспечения соответствующего уровня безопасности. Информация может быть изменена и передана адресату в измененном виде. Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. Такие средства, как, например, криптография, позволяют значительно усилить степень защиты, не ограничивая доступ пользователей к данным.

WLAN разрабатывалась на основе стандартов Ethernet (проводной сети). Именно поэтому беспроводные сети наследуют все уязвимости обыкновенных проводных сетей и добавляют к ним свои собственные. Распространение таких сетей идет одновременно с непрекращающейся информацией об их взломе. Хакеры охотятся за чужим трафиком, из которого можно извлечь различную конфиденциальную информацию (пароли, номера кредитных карт и т.д.). Это заставило разработчиков предпринять комплекс защитных мер: аутентификация, шифрования трафика, привязка к MAC-адресам ( MAC-адрес - уникальный идентификатор, присваиваемый каждой единице активного оборудования, или некоторым их интерфейсам в компьютерных сетях Ethernet). Также применяют шифрование всех передаваемых пакетов. Наиболее часто для таких целей используется WEP (Wired Equivalent Privacy) шифрование, которое основано на поточном алгоритме шифрования RC4.

**Актуальность темы:** в настоящее время невозможно представить нашу жизнь без сети Интернет. Она предоставляет нам возможность общения, помогает найти нужную информации и дает пространство для творчества. В связи с возросшей потребностью хранить и передавать информацию стало необходимо защищать её. Существует различное множество киберпреступлений. Злоумышленники пытаются заполучить личную информацию людей: логины, пароли, номера телефонов или даже банковские реквизиты. Поэтому ни в коем случае нельзя забывать о безопасности в сети.

К сожалению, многие люди пренебрежительно относятся к этой безопасности. По причине своей неосведомленности о правилах работы в интернете, любые незащищенные персональные могут легко угодить в руки злоумышленников. В своем реферате я хочу рассмотреть обозначенную **проблему**.

**Цель исследования** – изучение устройства беспроводных сетей, рассмотрение способов защиты информации в них, разработка программы алгоритма RC4 потокового шифра.

**Для выполнения этой цели были поставлены конкретные задачи**:

* Изучить информацию по данной теме реферата
* Объяснить причины использования беспроводных компьютерных сетей
* Изучить виды и стандарты локальных беспроводных сетей
* Рассказать о том, как следует обеспечить безопасность во время подключения к сети
* Рассмотреть способы защиты информации шифрованием
* Изучить алгоритм RC4 потокового шифра
* Разработать программу алгоритма RC4
* Написать отчет о проделанной работе

 При написании дипломной работы я буду пользоваться в основном тремя источниками. Главный источник - это книга  Баричева С.Г., Гончарова В.В. и Серова Р.Е. «Основы современной криптографии». Из нее я беру сведения о потоковых алгоритмах шифрования и в частности об алгоритме RC4. Остальные два источника – сайты, на одном из которых рассказывается о классификации беспроводных сетей и обеспечении безопасности, а на другом о защите информации в беспроводных сетях (с упоминанием WEP - шифрования, которое основано на поточном алгоритме шифрования RC4).

Сама дипломная работа будет состоять из введения и двух частей: практической и теоретической; заключения и списка литературы. В теоретической части я расскажу о причинах использования беспроводных сетей, их видах и стандартах и об обеспечении безопасности в сети (в особенности про защиту информации шифрованием), а в практической части будет разработана программа алгоритма RC4 потокового шифра.

**Список литературы**

1) Баричев С.Г., Гончаров В.В., Серов Р.Е. «Основы современной криптографии» - М.: Издательство НТИ «Горячая линия - Телеком», 2011. - 175 с.: ил., 2011

2) Гусева А.И., Киреев В.С. «Вычислительные системы, сети и телекоммуникации: учебник для студенческих учреждений высшего профессионального образования». - М.: Издательский центр "Академия", 2014.

3) Джим Гейер «Беспроводные сети. Первый шаг» : Пер. с англ. — М. : Издательский дом "Вильяме", 2005.

4) Статья "Безопасность в сетях Wi-Fi" интернет ресурса для IT-специалистов «ГетВайФай». [http://www.getwifi.ru/psecurity.html](http://www.getwifi.ru/psecurity.html%20) Ссылка действительна на 09.12.2015.

5) Статья "Защита информации в беспроводных сетях" интернет ресурса «XV Всероссийской научно-методической конференции "Телематика'2008"». <http://tm.ifmo.ru/tm2008/db/doc/get_thes.php?id=237> Ссылка действительна на 09.12.2015.

6) Статья "Классификация беспроводных сетей, обеспечение безопасности" интернет ресурса «Хабрахабр». [http://habrahabr.ru/sandbox/21711/](http://habrahabr.ru/sandbox/21711/%20) Ссылка действительна на 09.12.2015.

7) Статья "Механизм шифрования WEP" интернет ресурса «Сотспроф». <http://sotsprof.net/wi-fi/mechanizm-shifrovaniya-wep> Ссылка действительна на 09.12.2015.