СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc64674810)

[ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА СЕТИ INTERNET 5](#_Toc64674811)

[1.1 История сети Internet 5](#_Toc64674812)

[1.2 Гипертекстовая технология WWW, URL, HTML 6](#_Toc64674813)

[ГЛАВА 2 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ INTERNET 16](#_Toc64674814)

[2.1 Средства защиты информации 16](#_Toc64674815)

[2.2 Принципы защиты информации в системе Comodo Firewall 23](#_Toc64674817)

[ЗАКЛЮЧЕНИЕ 35](#_Toc64674818)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 38](#_Toc64674819)

# ВВЕДЕНИЕ

Интернет – это всеобщая компьютерная сеть, охватывающая весь мир.

На данный период времени Интернет особо актуален и включает в себя не менее 15 миллионов клиентов в 150 странах мира. Каждый год размер сети увеличивается не менее чем на 70-90 %. Интернет создает свою базу, которая обеспечивает связь разных информационных сетей и является собственностью различных организаций во всем мире.

Если до этого времени сеть использовалась в виде средства для отправки данных и сообщений электронной почты, то сейчас решаются проблемы распределенного доступа к сервису. Примерно два года назад создавались специальные оболочки, которые обеспечивали функционирование сетевого поиска и доступа к информационным средствам, электронным библиотекам.

Сейчас Интернет служит не только исследовательским и учебным группам, а превращается все более актуальной системой в деловом мире.

Организаций притягивает простота, не дорогая глобальная связь, удобство для реализации совместных работ, доступные программы, уникальная база данных сети Интернет. Они собираются использовать глобальную сеть как прибавку к своим собственным локальным сетям.

Исходя из выше сказанного, Интернет это огромное количество локальных и глобальных сетей и принадлежащие разным организациям и предприятиям, связанных между собой разнообразными линиями связи. Интернет представляют как модель сложенную из не больших сетей различных размеров, которые производят взаимообмен, пересылая данные, сообщения и многое другое.

Пользователи имеют доступ к коммерческим и некоммерческим информационным службам Соединенных Штатов Америки, Канады других европейских стран, совершенно бесплатно.

Помимо этого, Интернет предоставляет уникальные возможности не дорогой, надежной и конфиденциальной глобальной связи по всему миру. Это удобно для организаций имеющих свои филиалы по всему миру, транснациональных корпораций и структур управления. Как правило, применение инфраструктуры Интернет для международной связи обходится значительно экономнее, прямой компьютерной связи через спутниковый канал или через телефон.

Самая удобная и актуальная услуга сети Интернет это электронная почта. На данный момент электронную почту используют примерно двадцать миллионов клиентов. Причем сообщение, отправленное по электронной почте доходит за несколько минут, хотя обычная отправка может занять несколько дней или недель.

В наше время Интернет испытывает период подъема, в основном благодаря помощи со стороны правительств европейских государств и Соединенных Штатов Америки. Каждый год в Соединенных Штатах Америки выделяется около 1–2 миллионов долларов на формирование новой сетевой инфраструктуры. Разработки в области сетевых коммуникаций финансируются также правительствами Англии, Швеции, Финляндии, Германии.

**Объект исследования:** Internet.

**Предметом исследования является:** защита информации в Интернете.

**Цель исследования:** изучение средств защиты информации в глобальной сети Интернет.

**Задачи исследования, изучить:**

1. Историю сети Internet;
2. Средства защиты информации;
3. Принципы защиты информации в системе Comodo Firewall.

**ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА СЕТИ INTERNET**

* 1. **История сети Internet**

Министерство обороны США создало впервые экспериментальную сеть передачи данных в 1961 году. Данная сеть была названа ARPENET. Изначально планировалось использовать сеть ARPANET для исследования методов, которые позволили бы обеспечить качественную связь между компьютерами совершенно разных типов. В основном способы, используемые для передачи данных, через специальные устройства называемые модемами были созданы в ARPANET. В то же время были созданы и протоколы передачи данных, всего их было два - TCP/IP. Они состоят из множества коммуникационных протоколов и помогали компьютерам разнообразных видов общаться между собой.

Многочисленные компании и организации захотели вступить в ARPANET и ежедневно использовать ее для передачи данных, так как опыт с этой сетью был крайне удачен. Исходя из этого ARPANET преобразилась в рабочую сеть из экспериментальной. Обязанности за управление сетью было передано Defence Communication Agency (DCA). В наше время это агентство называют Defence Information Systems Agency (DISA), предназначено для обороны информационных систем. Сама сеть все так же продолжается развиваться и стремиться к совершенству, как и протоколы TCP/IP.

Первый стандарт, который был использован для TCP/IP разработан в 1983 году. Он вошел в ряд стандартных параметров для лабораторных испытаний военного стандарта США. По этой причине все кто использовал эти сети должны были перейти к этим протоколам. С целью упрощения перехода организация DARPA рекомендовали руководству Berkley Software Design ввести протоколы в Berkley Software Design UNIX. Так объединились операционная система UNIX и протокол TCP/IP.

Через определенный срок протокол TCP/IP был внедрен как стандарт для всеобщего использования, и это понятие вошло во всеобщее употребление. В 1983 году из ARPANET отделилась MILNET и была составляющей Defence Data Network (DDN) - военная сеть министерства обороны Соединенных Штатов Америки. MILNET и ARPANET объединили в одно понятие INTERNET, для обозначения одной сети. Понятие ARPANET перестали использовать еще в 1991 году, но сама сеть INTERNET пользуется популярностью на данный момент и ее размеры все так же увеличиваются, так как в ней объединены сети всего мира.

* 1. **Гипертекстовая технология WWW, URL, HTML**

Самым удобным и усовершенствованным механизмом для работы в глобальной мировой сети ИНТЕРНЕТ является – WWW. В переводе с английского обозначает «Всемирная паутина». Данная концепция возникла не так давно, но стремительно совершенствуется.

Огромное количество исследований имеют связь с создателями WWW - CERN, European Particle Physics Laboratory. Однако нужно понимать, что WEB создана не физиками и не для физиков. За счет эффективных и привлекательных идей, которые послужили созданию основы проекта, сделали из WWW механизм всемирного назначения, который позволяет брать любые сведения обо всех сферах человечества. WWW может охватить приблизительно тридцать миллионов клиентов в восьмидесяти странах.

Если говорить об отличиях механизма WWW и иных инструментов пользования Интернетом, то основное из них это работа с любыми видами документов. К примеру, это могут быть иллюстрации, видео ролики текстовые файлы и другие.

Можно сказать, что WWW это стремление собрать всю информацию, и даже локальную в виде гипертекстовых документов. Что позволяет любому пользователю переходить от одного документа к другому, при помощи гиперссылок. Документы используемые в сети разработаны на специальном языке HTML, расшифровывается как HyperText Markup Language. Данный язык очень похож на язык, использующийся для создания текстовых документов, но только HTML намного проще. Помимо упрощенности языка, он позволяет использовать сведения из Интернета, а так же внедрять созданные пользователем документы. При работе с HTML можно использовать ряд определенных рекомендаций.

Использование гипертекста позволяет пользователю переходить к необходимой информации щелчком мыши по ссылке. Так же есть возможность в одном документе вставлять ссылки на другие или даже документы, которые находятся на ином сервере.

Гипермедиа можно считать как множество гипертекста. В гипермедиа есть возможность производить операции над аудиоинформацией, иллюстрациями, анимацией, а не только над текстом, что во многом упрощает работу пользователя.

Не нужно забывать, что есть такие серверы WWW для таких операционных систем как Unix, Macintosh, MS Windows и VMS.

Используя такие серверы можно решить две основные проблемы:

1. Показать пользователям необходимую информацию об данной организации, каталог услуг и многое другое;

2. предоставить доступ сотрудникам организации к секретной информации. Например, это может быть номера телефонов всех сотрудников, задания от руководства, определенная документация и многое другое.

Данная информация первоначально оформляется как файлы на языке HTML. Это довольно простой язык предназначенный для гипертекстовой разметки документов, который позволяет использовать ссылки на другие документы, редактировать текст или фрагменты теста, тем самым представляя простой текст как отформатированный гипремедийный документ. Для создания такого документа можно использовать специальные редакторы и преобразователи файлов, но так же не сложно создать такой документ вручную.

Для того чтобы посмотреть готовый HTML документ используют специальные программы-браузеры, например Internet Explorer, lynx и другие. Каждый из браузеров хорош в своем определенном направлении. Lynx можно использовать для работы на символьных терминалах для контроля и визуализации можно использовать Mosaic или Netscape и так далее.

Архитектура WWW-технологии

Выше были описаны все необходимые элементы технологии WWW, теперь необходимо перейти к следующему пункту, т. е. к архитектуре связи программного обеспечения в WWW. В схеме «клиент-сервер» представлено распределение деятельности во Всемирной паутине (Рис. 1). Функцию интерфейса выполняет программа - клиент и она же может обеспечить доступ ко всем информационным ресурсам Интернета. Данная программа осуществляет такую же деятельность, как и telnet, то есть переходит за обычные рамки работы клиента только с сервером конкретного протокола. Считается, что Mosaic и Netscape, которые считаются WWW-клиентами, отвечают всего лишь за графический интерфейс в Интернете. Как было ранее установлено, нужно понимать, что элементы WWW-технологии (HTML и URL) особую роль при доступе к другим ресурсам играет браузер Mosaic и поэтому пользователи будут определены к WWW, а не к прочим информационным технологиям Internet. По сути, клиентом можно назвать интерпретатор HTML. Пользователь как обычный интерпретатор, осуществляет всевозможные функции, в зависимости от команд или разметки.



Рисунок 1 - Структура «клиент – сервер»

Функции, которые должен выполнять клиент помимо размещения текста, это обмен данными в зависимости от анализа полученного HTML, то есть это обмен текста с сервером, что можно увидеть наглядно при отображении интегрированных графических образов в текст. Во время анализа спецификации – URL (указатель ресурса) или по командам сервера пользователь запускает дополнительные программы для работы с документами в формате MPEG, GIF, JPEG, то есть форматов отличающихся от HTML. В принципе для пуска программы, независимо от типа файла, пользователем было создано программное обеспечение Luncher, но в наши дни огромное распространение получила система согласования запускаемых программ через MIME-типы. В иную долю взаимодействующих программ Всемирной паутины входит сервер протокола HTTP, базы данных в формате HTML, которые управляются сервером, и программное обеспечение, созданное в стандарте спецификации CGI. Вплоть до конечного периода, то есть до создания Netscape, применялись только два HTTP-сервера, такие как сервер NCSA и сервер CERN. На данный момент количество основных серверов увеличилось. Внедрили очень хороший сервер для операционной системы MS-Windows и Apachie-сервер для Unix-платформ. Есть так же и другие, однако если говорить о доступности использования, то два последних можно особенно выделить. Сервер, используемый для операционной системы Windows - это shareware, но без встроенного устройства, которое позволяет быстро и надёжно рассоединит детали механизма без участия человека, как в Netscape. Принимая во внимание общераспространенность персоналок в этой стране, подобное программное обеспечение позволяет узнать, что такое Всемирная паутина (WWW). Вторым сервером является ответ на угрозу извлечения прибыли всеми способами. Netscape уже не распространяет свой сервер Netsite свободно и говорят, что NCSA-сервер также будет распространяться на коммерческой основе. Именно поэтому изобретен Apachie, который, по слухам, будет freeware, реализующий новые дополнения к протоколу HTTP, связанные с защитой от несанкционированного доступа, предложеный группой по созданию этого протокола и работают практически во всех коммерческих серверах.

База данных HTML-документов—это доля файловой концепции, что включает в себе текстовые файлы в формате HTML, также сопряженные прочие средства. Основное внимание и интерес необходимо сосредоточить на документах, включающие в себя компоненты экранных конфигураций. Данные документы действительно гарантируют допуск к внешнему программному обеспечению.

Прикладное программное обеспечение, функционирующее с сервером, можно разбить в проекты-шлюзы. Шлюзами называют программы, обеспечивающие связь сервера с иными протоколами серверов, к примеру, ftp, либо с распределенными на сети серверами Oracle. Другие программы можно сказать проекты, к которым поступают сведения от сервера и исполняющие многие воздействия, например: реализацию графических гиперссылок, допуск к местным базам данных, получение текущей даты либо попросту вычисления.

Заканчивая рассмотрение архитектуры WWW хотелось бы выделить, то, что ее элементы существуют почти для всех видов компьютерных платформ и легкодоступны в сети. Каждый, у кого имеется допуск в Internet, способен сформировать собственный WWW- сервер, либо, просмотреть сведения с иных серверов.

Основные компоненты технологии World Wide Web

В 1989 году можно было утверждать, что гипертекст это новейшая технология, имевшая огромное количество реализаций в сравнении с другими механизмами. Огромные усилия были приложены для того чтобы создать формальные модели гипертекстовых концепций, нёсшие в себе описательный характер. У Т. Бернарс Ли была идея, он хотел, максимально удобным методом использовать гипертекстовую модель к информационным ресурсам, распределенным в сети. Он принял три основополагающие системы из четырех, такие как:

* универсальный способ адресации ресурсов в сети URL (Universal Resource Locator);
* язык гипертекстовой разметки документов HTML (HyperText Markup Lan-guage);
* протокол обмена гипертекстовой информацией HTTP (HyperText Transfer Protocol).

Спустя некоторое время NCSA решила добавить четвертый компонент:

• универсальный интерфейс шлюзов CGI (Common Gateway Interface).

Идея по созданию HTML была удачным проектом, которая позволила решить многие проблемы связанные с построением гипертекстовой системы не без помощи средств управления отображением. В создании языка гипертекстовой разметки значительное воздействие проявили 2 фактора:

1. исследование в сфере интерфейсов гипертекстовых систем;
2. стремление гарантировать обычный метод разработки гипертекстовой базы данных, распределенной на сети.

В 1989 г. стремительно дискуссировали вопрос интерфейса гипертекстовых систем, а именно методов представления гипертекстовой информации и навигации в гипертекстовой сети. Смысл гипертекстовой технологии сопоставляли со смыслом книгопечатания. Утверждалось, то, что бланк документа и компьютерные ресурсы отображения/воспроизведения всерьез различаются друг от друга, и по этой причине модель представления данных также обязана различаться. Более результативными моделями организации гипертекста были приняты контекстные гипертекстовые ссылки, но помимо этого так же было принято разделение на ссылки, группированные с абсолютно всеми важными целыми файлами или его частями.

Наиболее легким методом формирования каждого важного документа считается его набор в текстовом редакторе. Навык формирования хорошо размеченных с целью дальнейшего отражения документов в CERN\_е, было - сложно отыскать физика, который не использовал бы систему TeX либо LaTeX. Помимо этого на данный период времени был создан стандарт языка разметки—Standard Generalised Markup Language (SGML).

Нужно понимать, что в соответствии с собственным предложением Бернерс Ли подразумевал объединить в общую концепцию существующие информативные ресурсы CERN, также основными демо версиями обязаны были стать системы для NeXT и VAX/VMS.

Как правило, гипертекстовые системы обладают специализированными программными средствами создания гипертекстовых взаимосвязей. Сами гипертекстовые ссылки сохраняются в специальных форматах либо создают специальные файлы. Такого рода аспект неплох для локальной системы, но только не для распределенной на множестве разных компьютерных платформ. В HTML гипертекстовые ссылки интегрированы в тело документа и сохраняются как его часть. Зачастую в системах используют основные форматы хранения сведений с целью увеличения оперативности допуска. В WWW документы - это простые ASCII - файлы, которые возможно подготовить в каждом текстовом редакторе. Исходя из этого, вопрос по формированию гипертекстовой базы данных разрешен весьма просто.

За основу по созданию гипертекстовой разметки, подобрали SGML (Standard Generalised Markup Language). Придерживаясь академическим нормам, Бернерс Ли расписал HTML в определения SGML. Безусловно, в HTML выполнены все без исключения разметки, например выделение шрифтов, параграфов, стилей и тому подобное, так как разработка для NeXT предполагала графический интерфейс. Значимым элементом языка является представление интегрированных и группированных гипертекстовых ссылок, встроенной графики и предоставление права сбора информации по ключевым (основным) словам.

После создания первой версии языка HTML 1.0. прошло уже более семи лет. За этот период времени произошли достаточно значительное изменение языка. Практически в два раза увеличилось количество новых компонентов разметки, оформление схоже с оформлением качественных печатных изданий, усовершенствовались типы стилей. По сути можно отметить, что HTML формируется в сторону создания интерфейсов локальных и распределенных систем.

Следующей основополагающей системой WWW оказалась многофункциональная модель адресации информативных ресурсов. Universal Resource Identification (URI) рекомендует достаточно слаженную концепцию, которая предусматривает навык адресации и идентификации e-mail, Gopher, WAIS, telnet, ftp и тому подобное. Но без исключения все, что изложено в системе URL, для сбора баз данных в WWW необходимо только для Universal Resource Locator (URL). При отсутствии данной спецификации сила HTML стала бы ненужной.

URL гарантирует доступ к распределенным ресурсам сети, которые так же применяются в гипертекстовых ссылках. В URL позволено адресовать другие гипертекстовые файлы формата HTML, впрочем, как и ресурсы. Некоторые из них: telnet, ftp, Gopher, e-mail, WAIS. Доступ к данным ресурсам происходит по-разному, в зависимости от интерфейсных программ. Некоторые программы, такие как Netscape, могут сами поддерживать связь по протоколам, отличающимся от протокола HTTP, базового для WWW, или прочие, к примеру, Chimera, призывает для этой цели внешние программы. И все же базовой формой представления отображаемой информации считается HTML, а ссылки на прочие ресурсы имеют форму URL. Необходимо отметить, что приложения обработки электронной почты в формате MIME кроме того обладают возможностью отображать документы, представленные в формате HTML. Для этой цели в MIME зарезервирован тип “text/html”.

Далее в списке это протокол обмена данными WWW, который получил название HyperText Transfer Protocol. HyperText Transfer Protocol производит обмен гипертекстовых файлов и учет специфики данного обмена. В процессе такого взаимодействия, пользователь может получать новые адреса ресурса сети, так же передавать и принимать настройки и тому подобное. Сам процесс по контролю в HTTP выполняется в виде ASCII-команд. Поэтому сам разработчик базы данных при реализации внешних расчетных программ либо во время доступа к внешним базам данных, может столкнуться с элементами протокола.

Заключительной основной частью Всемирной паутины является результат работы группы NCSA - спецификация Common Gateway Interface (CGI). Она была создана с целью увеличения способностей технологии WWW за счет подсоединения различного внешнего программного обеспечения. Такого рода подход логично продолжал принцип публичности, удобства разработки и увеличения способностей Всемирной паутины. В случае если команда CERN рекомендовала удобный и быстрый метод разработки баз данных, то NCSA усовершенствовала этот метод до создания программных средств. Нужно понимать, что в доступной для всех библиотеке CERN были модули, которые позволяли разработчикам присоединять свои программы к серверу HTTP, однако это требовало пользование данной библиотекой. Представленный и расписанный в CGI метод соединения не требовал других библиотек и удивлял своим удобством и доступностью. Сервер взаимодействовал с приложениями через обычные потоки ввода/вывода, что облегчает разработку до максимума. Во время осуществления CGI особое значение занимали способы доступа, расписанные в HTTP. Хотя они используют только GET и POST, формирование HTML демонстрирует, что организация WWW ожидает усовершенствования и CGI по мере сложившихся проблем, в которых будет применяться WWW-технология.

**ГЛАВА 2 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ INTERNET**

**2.1 Средства защиты информации**

На данный момент вряд ли кому- либо нужно доказывать, что при подключении к Интернету подвергается риску защищенность локальной сети и секретность содержащейся в ней данных. В 2020 г. команда экстренной готовности Соединенных Штатов Америки (US-CERT) привнесла в Национальную базу 17 447 новых уязвимостей – 4-ый подряд рекордный коэффициент за целый год (предыдущий рекорд был зафиксирован в 2019 году – 17 306).

Согласно сведениям, полученным в Национальном институте стандартов Соединенных Штатов Америки, в прошлом году было отмечено 4168 высоко опасных, 10710 средне опасных и 2569 мало опасных уязвимостей. Если сравнивать с 2019 годом таких уязвимостей было больше чем в нынешнем году.

Специалисты CERT - это категория исследователей, аналитиков, инженеров-программистов безопасности и экспертов по цифровой разведке, трудящихся вместе для разбора уязвимостей безопасности в программных продуктах, содействия долгосрочным изменениям в сетевых системах и разработки передовой информации и обучения для улучшения практики кибербезопасности.

Самый распространённый метод защиты от «хакеров», это использование межсетевых экранов - брэндмауэров (firewalls).

При выборе файрвола для операционной системы Windows необходимо опираться на такие факторы как: легкость настройки и простота использования, обучающий режим для новичков. Не меньшую роль играют так же наличие соответствующего языка и необходимые функции.

В 2020 году лучшими средствами защиты информации в Интернете считаются:

* **Comodo Firewall**

Ссылка: [comodo.com](https://www.comodo.com/);

Требования к ПК: Windows XP SP2, 400 Мбайт;

Цена:39$, есть бесплатная версия без дополнительных настроек;

Язык: русский.

Данная программа приобрела обширную популярность еще во времена Windows XP, когда Comodo Firewall был не наиболее популярный, бесплатный firewall в Российской Федерации.

Используется он также в настоящее время. Создатели говорят о про активной охране с HIPS, межсетевой экранировке, защите от переполнения буфера и также неразрешенном допуске, охране реестра, системных файлах и прочее (Рис. 2).



Рисунок 2- Окно программы Comodo Firewall

* **Avast! Internet Security**

Ссылка: [avast.com/f-firewall](https://www.avast.com/f-firewall);

Требования к ПК: Windows XP SP3, 1,5 Гбайт на диске;

Цена:  30 дней бесплатно или 1450 р. в год;

Язык: русский.

Кроме знаменитого антивируса, Avast изготавливает также файрвол, который идет в комплект с программами Avast Premium Security (Рис. 3). Этот firewall идет в пакете с антивирусом, модулем охраны беспроводных сетей и также к комплекте других функций, коммерческую версию можно приобрести за 1450 р. в год на один единственный компьютер.



Рисунок 3 – Окно программы Avast! Internet Security

* **AVG Internet Security**

Ссылка**:** [avg.com](https://www.avg.com/);

Требования к ПК: Windows XP SP3

Цена: 30 дней бесплатно или 1990 р. за год;

Язык: русский.

Файрвол идет в комплекте AVG Internet Security. Помимо самого файрвола туда входит еще различные программы, а так же антивирус (Рис. 4). Только платная версия.



Рисунок 4 - Окно программы AVG Internet Security

* **ZoneAlarm Free Firewall**

Ссылка: [zonealarm.com](https://www.zonealarm.com/);

Требования к ПК: Windows XP

Цена: бесплатно или 40$ в год;

Язык: English

Фирма ZoneAlarm не так известна, как другие компании выше, однако так же занимается разработкой антивирусов. ZoneAlarm Firewall идет как бесплатная и как платная версия. При покупке платной версии будут доступны различные дополнительные настройки, а так же есть возможность включать или отключать пункты, отсутствует реклама и можно добавлять различные правила фильтрации трафика(Рис. 5).



Рисунок 5 - Окно программы ZoneAlarm Free Firewall

* **GlassWire**

Ссылка: glasswire.com;

Требования к ПК: Microsoft Windows 7, 8, 10 (x86,x64), Intel Core 2 Duo or Faster Processor, 4 Гбайт RAM.

Цена: пробный период семь дней или 39$;

Язык: русский.

Firewall для фирмы GlassWire это главное творение, в отличие от компаний описанных выше. Поэтому у GlassWire больше полезных качеств работы (Рис. 6). GlassWire’s Firewall разработала как настольную, так и мобильную версию. Загрузка программы удобная и вполне примитивная.



Рисунок 6 - Окно программы GlassWire

* **TinyWall**

Ссылка: tinywall.pados.hu;

Требования к ПК: Microsoft Windows 7, 8, 10 (x86,x64), Intel Core 2 Duo or Faster Processor, 4 Гбайт RAM. Минимальные еще ниже;

Цена: бесплатная программа;

Язык: русский.

Firewall TinyWall разработалКароя Падоша (Károly Pados) и является бесплатным. Программа выполняется из трея, то есть из части пользовательского интерфейса, можно увидеть значки функций и программ, которых нет на рабочем столе (Рис. 7). Однако при проведении 1-го теста, TinyWall не позволяет пробиться «вредоносу».



Рисунок 7 - Окно программы TinyWall

## 2.2 Принципы защиты информации в системе Comodo Firewall

Как говорилось выше Comodo Firewall это бесплатная программа-фаервол, предназначенная для защиты ПК от любых сетевых угроз, интернет-атак, установки вредоносного ПО, передачи данных пользователя через интернет, переполнения буфера, а также контролирует запускаемые программы.

Для начала необходимо установить Comodo Firewall  данную программу:

1. Для этого необходимо перейти на сайт разработчика и скачать файл установки как показано на рисунке 8.



Рисунок 8 – Сайт разработчика

1. Для того что бы начать процесс установки, необходимо запустить ранее скаченный файл (Рис. 9)



Рисунок 9 – Распаковка файла

1. После откроется окно, где нужно выбрать язык установки. Здесь выбираем русский язык (Рис. 10).



Рисунок 10 – Мастер установки

1. Далее вводим адрес электронной почты, по желанию. Теперь убираем галочки с пунктов «Я хочу использовать облачный анализ поведения приложений, передавая неопознанные программы в COMODO», и «Анонимно оправлять в COMODO данные об использовании приложения для внесения изменений, улучшающих работу программы», так как в данном случае в них нет необходимости (Рис. 11) и нажимаем «Настроить установку».



Рисунок 11 – Окно мастера установки

1. После нажатия на кнопку «Настроить установку» откроется окно, которое позволить выбрать необходимые компоненты для установки программы как показано на рисунке 12. Здесь каждый компонент имеет свою функцию, и необходимо выбрать варианты установки.



Рисунок 12 – Настройка установки

1. Теперь необходимо перейти на вкладку Варианты конфигурации. Здесь оставляем все как есть, это позволит не возиться с лишними настройками (Рис. 13). Таким образом программа Comodo Firewall будет сама принимать решения, такие как разрешать соединения приложений либо запрещать известным вредоносным или подозрительным файлам загрузку.



Рисунок 13 – Настройка конфигурации

1. После нажимаем на вкладку расположение файлов и выбираем путь для установки, как показано на рисунке 14:



Рисунок 14 – Расположение файла

1. Далее нажимаем на кнопку «Назад» для того чтобы вернуться к первоначальному окну мастера настройки где нажимали на вкладку «Настроить установку» и нажимаем на «Вперед». Откроется следующее окно где можно либо убрать галочки, либо оставить, если пользователю необходим браузер Яндекс. Теперь нажимаем на кнопку «Согласен. Установить» как показано на рисунке 15.



Рисунок 15 – Подтверждение установки

1. Теперь откроется окно процесса установки программы (Рис. 16).



Рисунок 16 – Процесс установки

1. Для завершения процесса установки необходимо перезагрузить компьютер (Рис. 17).



Рисунок 17 – Перезагрузка ПК

1. После установки и перезагрузки ПК появиться окно с пунктами, от выбора которых будет зависеть уровень безопасности компьютера и внутренних настроек (Рис. 18)



Рисунок 18 – Внутренние настройки

1. Далее открываем программу, всплывет главное окно программы, как показано на рисунке 19.



Рисунок 19 – Главное окно программы

1. Здесь отображается кнопки, каждая из которой выполняет свою функцию. Если нажать на кнопку «Сканирование», программа просканирует ПК и выдаст отчет с подозрительными файлами как показано на рисунке 20, 21.



Рисунок 20 – Сканирование ПК



Рисунок 21 – Рейтинговое сканирование

1. Следующая вкладка «Обновление». Эта кнопка позволяет обновить приложение, если появились новые версии программы (Рис. 22).



Рисунок 22 – Вкладка «Обновление»

1. Далее вкладка «Виртуальный рабочий стол», которая позволяет запустить изолированную среду. Здесь можно заходить в опасные сайты. Между рабочими столами можно переключать по необходимости.
2. Следующие кнопки «Карантин» и «Онлайн - поддержка» (Рис. 23). При переходе на вкладку «Карантин» можно увидеть все удаленные приложением файлы, то есть файлы с повешенной угрозой. «Онлайн - поддержка» это обычная техническая поддержка для пользователя.



Рисунок 22 – Вкладки «Карантин» и «Онлайн - поддержка»

1. После перехода на вкладку «Карантин» нажимаем на кнопку в левом верхнем углу, здесь можно увидеть подробную информацию о активных соединениях (Рис. 23). То есть увидеть число входящих и исходящих соединений, блокировки и прочее
2. Нажав на соответствующий файл, можно рассмотреть более подробную информацию как показано на рисунке 24.

****

Рисунок 23 – Активные соединения

****

Рисунок 24 – Окно входящих и исходящих соединений

1. Установка и настройка программы Comodo Firewall  завершена.

# ЗАКЛЮЧЕНИЕ

В целом безопасность любой информации представляет собой использование огромного набора методов нацеленные на защиту от любых угроз безопасности. Создание и использование таких методов, не зависимо от того профилактические они или отражающие реальные атаки и угрозы, должны быть основаны на основных способах защиты информации или данных в сети.

Методы, используемые для защиты информации должны без конца совершенствоваться в зависимости от тенденций изменения средств защиты и новых угроз безопасности. Исходя из этого, можно сказать, что система информационной безопасности должна непрерывно развиваться.

Развитие в научно- техническом направлении в последние годы обретает огромные успехи в области информатизации общества на основе современных средств вычислительной техники, связи, и конечно способов автоматизации обработки данных. Разрабатываемые на сегодняшний день информационно-вычислительные системы и сети оказываются глобальными, а использование этих способов и средств принимает всеобщее направление. В этот процесс входит сбор, передача, накопление, хранение, поиск, переработка и выдача информации для использования.

В данный период времени, современное общество считает что информация это самая ценная вещь в жизни, которая требует безопасности от несанкционированного проникновения лиц не имеющих к ней доступа.

В 1960 и в 1970 годах решение таких проблем как угроза безопасности информации, решалась довольно просто, при помощи организационных мер. Выделим основные из них:

* Охрана;
* Сигнализация;
* Программные средства для защиты информации;
* Режимные мероприятия и другие.

Использование этих мер достигалось на основе централизации данных на вычислительных центрах, что обеспечивало защиту информации относительно простыми методами и средствами.

В наше время нет ни одной фирмы или предприятия , которые не использовали бы современные средства обработки или передачи данных. В электронно-вычислительных машинах на носителях набираются определенное количество информации, которые в основном являются конфиденциальными или представляют особую ценность для организации.

Безопасность информации в сети становиться все более актуальной на сегодняшний день, проблему защиты информации можно обосновать тремя основными пунктами уязвимости:

* угроза несанкционированного доступа к информации для людей которым она не предназначена;
* искажение или удаление конфиденциальных, ценных данных;
* случайное или умышленное изменение информации.

Процесс защиты информации на данный момент, как было расписано выше, является основным условием для полноценной работы любой информационной системы. В бизнесе и государственных структурах это наиболее актуально, так как данные могут быть особенно ценными и необходимо усилить защиту от «хакеров». Безопасность данных можно подразделить на три основных и взаимодополняющих направления:

* защита от несанкционированного доступа к данным при помощи специальных технических средств, например использование файрвола;
* усовершенствование технологий и организационно-технических мероприятий технологии обработки информации с целью ее защиты от внешних и внутренних угроз безопасности;

Необходимо отметить, что есть определенные моменты, из-за которых сложно решить данную проблему, то есть проблему защиты информации в INTERNETE. Выделим основные из них:

* массовое применение;
* сложность функционирования;
* увеличение количества угроз.

В ходе выполнения работы были рассмотрены все методы и способы защиты информации в сети. Что касается регулярного роста количества угроз, можно отметит основные из них:

* утечка секретных данных;
* компрометация информации;
* отказ от информации;
* несанкционированный взаимообмен информацией пользователей друг с другом;
* несанкционированное применение информационных ресурсов;
* нарушение информационного обслуживания;
* ошибочное применение информационных ресурсов;
* незаконное применение преимуществ клиентов и админов.

Исходя из проделанной работы могу сказать, что поставленные цели и задачи были успешно выполнены.

#

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Браун С. «Всемирная паутина» для доступа в Интернет: перевод c английского - М.: Мир: Малип: СК Пресс, 2019. - 167c.
2. Гайкович В., Першин А. Безопасность электронных систем. - М.: "Единая Европа", 2018. - 264 c.
3. Гилстер П. Новый навигатор Интернет: Перевод с английского - Киев: Диалектика, 2020. - 495 c.
4. Игер Б. Работа в Интернете / Под редакцией А. Тихонова; Перевод с английского - М.: БИНОМ, 2017. - 313 c.
5. Кент П. Интернет / Перевод с английского, В.Л. Григорьева. - М.: Компьютер, ЮНИТИ, 2018. - 267 c.
6. Колесников О.Э. Internet для делового человека. - M.: МЦФ. Издат. фирма “Яуза”, 2018. - 281 c.
7. Крол Эд. Все об Интеренет: Руководство и каталог / Перевод с английского. С.М. Тимачева. - Киев: BNV, 2019. 591 c.
8. Левин В.К. Защита информации в информационно-вычислительных cистемах и сетях // Программирование. - 2018. - N5. - C. 5-16.
9. Нольден М. Ваш первый выход в Интернет: Для начинающих пльзователей Интернета и широкого круга пользователей PC / Гл. ред. Е.В. Кондукова; Перевод с немецкого. К.А. Шиндер. - Спб.: ИКС, 2019. - 238 с.
10. Продукты года // LAN - русское издание. - апрель 2020. - том 1. - номер 1. - C. 6-25.
11. Об информации, информатизации и защите информации: Федеральный Закон // Российская газета. - 2018. - 22 февраля. - C. 4.
12. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Интернет, E-mail, FTP, WWW, и HTML. - Диалог - МИФИ, 2017.- 283 c.
13. Хоникат Д. Интернет Windows 16: Руководство пользователя / Перевод с английского. В. Неклюдова. - М.: БИНОМ, 2019. - 334 с.
14. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 2018. - 275 c.
15. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2018. - 310 c.
16. Хоникарт, Джерри. Интернет без проблем. - М.: Радио и связь, 2019. - 240с.
17. Шаньгин Владимир Защита компьютерной информации. Эффективные методы и средства. М.: ДМК-Пресс. 2018. - 239 с.
18. Кирк, Черил. Интернет. Книга ответов. - М.: Юнити, 2020. - 220 с.
19. Корнеев, И. К., Степанов, Е. А. Защита информации в Интернете. - М. Проспект. 2020. - 265 с.
20. Куприянова, Г. И. Информационные ресурсы Интернета. - М.: ЭДЭЛЬ, 2019. - 209 с.
21. Браун, С. Мозаика и Всемирная паутина для доступа в Интернет: Пер. c англ. - М.: Мир: Малип: СК Пресс, 2017. - 234 с.