**Министерство просвещения РФ**

**муниципальное казённое общеобразовательное учреждение**

**«Вихоревская средняя общеобразовательная школа № 2»**

**Братского района Иркутской области**

**Конференция школьников**

**«Индивидуальная проектная деятельность»**

**Проект «Угроза в сети Интернет»**

 **Выполнил:**

 **Долинов Александр,**

 **ученик 8-в класса**

 **Руководитель:**

 **Кудрявцева М. Г.**

**Вихоревка, 2022 г**.

**Содержание**

Введение……………………………………………………………………………………….3

I. Угроза в сети Интернет……………………………………………………………….4

* 1. Вредоносные программы……………………………………………………………..4
	2. Вирусы, которые могут привести к различным нарушениям в работе компьютера………………………………………………………………………...………….6
1. Социальная инженерия………..……………………………………………………..8

#### Классификация вирусов по способу заражения файлов………………..………...10

1. Спам и фишинг…………………...………………………………………………….11

Заключение……...…………………………………………………………………………...12

Список используемой литературы……………………………………...………………….13

**Введение**

Интернет – это безграничный мир информации, который даёт широкие возможности для общения, обучения и отдыха и в то же время представляет собой огромную, ежедневно пополняющуюся базу данных, которая содержит интересную для злоумышленников информацию о пользователях.

Нельзя отрицать того факта, что Интернет все теснее проникает в нашу с вами жизнь.

Актуальность работы заключается в том, что интернет может быть использован для нанесения вреда нам, нашим близким и нашему имуществу, а его пользователи не знают, как защититься от угроз.

**Проблема:** слабая защищённость пользователей

**Цель работы** – создать инструкцию для повышения уровня безопасности людей, пользующихся интернетом.

**Задачи:**

1. Собрать материал для исследования.
2. Подвести итоги.

**Гипотеза:** защищённость пользователей интернета увеличится, если люди будут больше знать об его угрозах.

**Объект исследования:** процесс выявления опасностей в интернете.

**Предмет исследования:** защищённость пользователей интернета.

**Методы: п**оиск информации в сети Интернет.

1. **Угроза в сети Интернет**
	1. **Вредоносные программы**

**Цель вредоносных программ** – причинить ущерб компьютеру, серверу или компьютерной сети. Они могут испортить, украсть или стереть данные, хранящиеся на компьютере, замедлить или полностью остановить работу устройства. Вредоносные программы часто прячутся в письмах и сообщениях с заманчивыми предложениями от неизвестных лиц и компаний, в страницах новостных сайтов или других популярных ресурсах, которые содержат уязвимости. Пользователи заходят на эти сайты, и вредоносные программы незаметно проникают на компьютер.

Также вредоносные программы распространяются через электронную почту, съемные носители информации или скачанные из Интернета файлы.

Вредоносные программы могут скрываться и под видом звуковых или графических сообщений. Например, красивая экранная заставка, которой с удовольствием любуется пользователь, может оказаться троянской программой. Ссылки, которые появляются во всплывающих окнах и в рекламных объявлениях на различных сайтах, также могут содержать вирусы.

**Вирусы** - наиболее распространённый тип угроз способный заражать файлы на персональном компьютере, а также распространяться с одного устройства на другой. Когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях. По данным [Национального института стандартов и технологий (NIST)](https://csrc.nist.gov/publications/detail/nistir/4939/final) , первый компьютерный вирус под названием «Brain» был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты. Чем дольше вирус остается необнаруженным на компьютере, тем больше файлов он может заразить. Вирус - программа способная самопроизвольно присоединять к другим программам свои копии и внедрять их в файлы, системные области жестких дисков, компьютерные сети с целью нарушения работы компьютера.

**Червь -** это вредоносная программа, которая многократно копирует сама себя, но не наносит прямого вреда безопасности. Червь, однажды попавший на компьютер, будет искать способы распространения на другие компьютеры и носители. Существует много видов червей основные из них:

P2P - черви распространяющееся при помощи пиринговых (peer-to-peer) файлообменных сетей. Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера. Существуют более сложные.

P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно — при этом червь предлагает для скачивания свою копию.

это вредоносная программа, которая многократно копирует сама себя, но не наносит прямого вреда безопасности. Червь, однажды попавший на компьютер, будет искать способы распространения на другие компьютеры и носители. Существует много видов червей основные из них:

Почтовые черви - черви, распространяющиеся в формате сообщений электронной почты. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте). В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Сетевые черви (интернет черви) использующие для распространения протоколы Интернет. Преимущественно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов TCP/IP.

**Сетевые черви (интернет черви)** использующие для распространения протоколы Интернет. Преимущественно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов TCP/IP

## **Троянская программа**

Трояны - вредоносные программы, для активации которых, требуется запуск их пользователем или другой вредоносной программой.

Получили они своё название от одноименного печально извест­ного мифологического коня - вредоносный компонент проникает в систему под видом какой-либо полезной программы или утилиты. Как правило, троянскую программу предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности она делает то, что нужно злоумышленникам. И основная задача троянских программ состоит именно в различной деструктивной деятельности: от блокирования различных программ или установки рекламных баннеров до шифрования файлов и перехвата паролей к платёжным системам. Современные троянские программы эволюционировали до таких сложных форм, как, на­пример, бэкдор (перехватывает на компьютере административные функции операционной системы) и загрузчик (устанавливает на компьютер жертвы вредоносный код).

Эти весьма опасные приложения могут выполнять следующие несанкционированные пользователем действия:

* удаление данных
* блокирование данных;
* изменение данных;
* копирование данных;
* замедление работы компьютеров и компьютерных сетей.

Руткит - Работа руткитов заключается в том, чтобы прикрывать хакеров. Лучшая или худшая сторона руткитов состоит в том, что они также могут скрываться от антивирусного программного обеспечения, из-за чего пользователь не знает, что в системе присутствует руткит.Это помогает хакеру, и он может распространять вредоносное ПО в системе. Поэтому важно иметь хороший антивирус со сканером руткитов , который сможет обнаружить вторжение.

Spyware - шпионское ПО, как следует из названия, предлагает шпионить за сетью и компьютерной системой. Они могут быть непреднамеренно загружены с разных веб-сайтов, сообщений электронной почты или мгновенных сообщений.

В некоторых случаях они также могут пробираться через другое прямое соединение для обмена файлами. Иногда нажав «Принять лицензионное соглашение», вы можете подвергнуть компьютер риску.

Кража информации

# **Невидимка -** файловый вирус, остающийся "невидимым" для антивирусных программ. При проверке системы вирус-невидимка пытается перехватить запросы и выдать сфальсифицированный ответ, сигнализирующий, что все в порядке. Вирусы-невидимки являются разновидностью резидентных вирусов (постоянно находяться в оперативной памяти). Stealth-вирусы фальсифицируют информацию прочитанную из диска так, что программа, которой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах.

* 1. **Вирусы, которые могут привести к различным нарушениям в работе компьютера**

**Очень опасные.**

Вирусы, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

#### **По среде обитания**

Под “средой обитания” понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса.

##### **Файловые вирусы**

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они:

* различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);
* создают файлы-двойники (компаньон-вирусы);
* создают свои копии в различных каталогах;
* используют особенности организации файловой системы (link-вирусы).

Все, что подключено к Интернету – нуждается в антивирусной защите: 82% обнаруженных вирусов находятся в файлах с расширением PHP, HTML и EXE. Это говорит о том, что выбор хакеров – это Интернет, а не атаки с использованием уязвимостей программного обеспечения. Угрозы имеют полиморфный характер, это означает, что вредоносные программы могут быть эффективно перекодированы удаленно, что делает их трудно обнаруживаемыми. Поэтому высокая вероятность заражения связана, в том числе, и с посещениями сайтов.

##### **Загрузочные вирусы**

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией.

##### **Макро-вирусы**

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий. Эти макро-языки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

##### **Скрипт-вирусы**

Скрипт-вирусы, также как и макро-вирусы, являются подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы, либо являются частями многокомпонентных вирусов.

**По способу заражения:**

1. **Резидентные.**

Такие вирусы, получив управление, так или иначе остается в памяти и производят поиск жертв непрерывно, до завершения работы среды, в которой он выполняется. С переходом на Windows проблема остаться в памяти перестала быть актуальной: практически все вирусы, исполняемые в среде Windows, равно как и в среде приложений Microsoft Office, являются Срезидентными вирусами. Соответственно, атрибут резидентный применим только к файловым DOS вирусам. Существование нерезидентных Windows вирусов возможно, но на практике они являются редким исключением.

1. **Нерезидентные**

Получив управление, такой вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту). К такому типу вирусов можно отнести скрипт-вирусы.

## **По степени воздействия:**

1. **Безвредные**

Вирусы, никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).

1. **Неопасные**

Вирусы, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

**II.** **Социальная инженерия**

Сюда относятся все ситуации, когда мошенники получают данные напрямую от жертвы. Чаще всего жертва сама позволяет злоумышленникам похитить деньги, сообщая нужные данные, пароли и коды из СМС.

Эти способы пока что являются для мошенников наиболее эффективными и менее затратными — не нужно разрабатывать специальное ПО и покупать прочие инструменты. Достаточно знать фамилию, имя и телефон жертвы. В некоторых случая даже нет необходимости иметь какие-либо банковские данные. Последним новшеством в действиях мошенников стала подмена официальных номеров банков.

Возможно, вы задались вопросом откуда берутся эти данные?

С начала года Банком России было зафиксировано 18 утечек баз данных из банков, государственных учреждений и небанковских организаций кредитной сферы. Большая часть утечек не получила широкой огласки, поэтому мы про них даже не слышали. За этот же период было найдено почти 13 тысяч объявлений о продаже баз данных граждан РФ на различных нелегальных интернет-ресурсах.

Напрашивается вывод, что большинство личных данных воруется не с помощью утечек баз данных, а иными способами. Как мы уже выяснили, в подавляющем большинстве случаев мошенники получают данные от самих же владельцев. Но есть и другие способы завладеть этими данными.

Как защититься: никому не говорить по телефону свои данные, особенно номера карт и пароли из СМС. Настоящие сотрудники банка никогда не будут вас просить сообщить пароль из СМС или ввести его куда-то.

## C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9075D912.tmpСайты объявлений. Зная фамилию, имя и телефон жертвы, несложно найти её объявления на торговых площадках. Мошенники парсят торговые площадки, а потом сверяют данные с имеющейся базой. В результате базы сопоставляются и объединяются, массив украденных данных растёт, всё больше данных о вас оказывается у мошенников в руках.

Если обнаруживаются совпадения, то в дело вступает социальная инженерия. Позвонив якобы по объявлению или написав сообщение, злоумышленники пытаются выяснить номера карт: например, под предлогом «перевести залог». Но такие разговоры не всегда заканчиваются кражей — иногда цель просто узнать данные.

Чтобы в следующий раз уже другой мошенник перезвонил вам от имени вашего банка, назвал вам номер карты, втёрся тем самым в доверие и попытался совершить перевод.

Самая распространенная мошенническая схема со стороны продавца выглядит так: вы находите привлекательное по цене или другим признакам объявление. Вас просят отправить аванс или предоплату до того-как вы встретитесь с продавцом, чтобы подтвердить свои намерения или “отложить” востребованный товар. Для получения предоплаты продавец предлагает перевод на карту, оплату на счет мобильного телефона или денежный перевод частному лицу. После получения предоплаты мошенник перестанет отвечать на ваши звонки, а доказать факт мошенничества не получится, так как вы добровольно перевели деньги частному лицу.

Правило по определению мошенника 1 слишком низкая цена 2 предоплата или дополнительные услуги 3 просят сообщить личные данные 4 продавец вас торопит не даёт проверить товар. Для торговли на них используйте отдельные карты (виртуальные или бесплатные карты мгновенной выдачи), не храните на этих картах деньги. Оплату за продаваемые вещи принимайте наличкой, почтовым переводом, на электронный кошелек или любым другим способом, которые позволит не сообщать данные своих действующих карт.

#### **III. Классификация вирусов по способу заражения файлов**

##### **Перезаписывающие**

Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

##### **Паразитические**

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

##### **Вирусы-компаньоны**

К ним относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла.

##### **Вирусы-ссылки**

Вирусы-ссылки или link-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла “заставляют” ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

##### **Файловые черви**

Файловые черви не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям “специальные” имена, чтобы подтолкнуть пользователя на запуск своей копии — например, INSTALL.EXE или WINSTART.BAT.

**IV. Спам и фишинг**

Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками, цель которых:

1. выудить деньги у некоторого количества получателей, ответивших на сообщение;
2. провести фишинговую атаку, чтобы обманным путем получить пароли, номера кредитных карт, банковские учетные данные и т.д.;
3. распространить вредоносный код на компьютерах получателей.

**Как защитить себя от спама и фишинга?**

1. Заведите себе несколько адресов электронной почты.
2. Лучше всего иметь по крайней мере два адреса электронной почты. Этот адрес должен использоваться только для личной корреспонденции. Поскольку спамеры создают списки возможных адресов электронной почты (используя комбинации очевидных имен, слов и номеров), необходимо придумать такой адрес, который спамерам будет трудно угадать. Личный адрес не должен состоять просто из вашего имени и фамилии, а чтобы защитить его, следуйте указанным ниже рекомендациям.
3. Никогда не публикуйте личный адрес электронной почты на общедоступных интернет-ресурсах.
4. Если требуется опубликовать личный адрес в электронном виде, попробуйте замаскировать его, чтобы спамеры не смогли «распознать» его. Например, «Саша.Долинов@yahoo.com» — это простой адрес, который без труда найдут спамеры. Вместо этого попробуйте представить его в таком виде: Саша-точка-Долинов-собака-yahoo.com».
5. Если нужно опубликовать личный адрес на веб-сайте, безопасней сделать это в виде графического файла, а не в виде ссылки.
6. Если личный адрес обнаружен спамерами, его следует поменять. Несмотря на возникающее вследствие этого неудобство, изменение адреса электронной почты поможет избежать получения спама.
7. «Публичный» электронный адрес. Используйте этот электронный адрес для регистрации на общедоступных форумах и в чатах, а также для подписки на почтовую рассылку и другие интернет-услуги.

Уменьшить объем спама, доставляемого на этот адрес, также помогут указанные ниже советы:

* + 1. Относитесь к общедоступному адресу как к временному. Шансы, что спамеры перехватят адрес, используемый в открытом доступе, очень велики — особенно если он используется часто.
		2. Попробуйте завести несколько «публичных» адресов. В этом случае будет больше шансов отследить, какие службы отправляют адреса спамерам.
		3. Никогда не отвечайте на спам.
		4. Большинство спамеров фиксируют получение ответов. Обычно чем больше вы отвечаете на спам, тем больше его приходит.
		5. Своевременно обновляйте браузер. Убедитесь, что на компьютере используется самая последняя версия веб-браузера и загружены все последние исправления, связанные с интернет-безопасностью.
		6. Используйте спам-фильтры. Заводите учетную запись для электронной почты только у тех провайдеров, которые используют спам-фильтры. [Выберите антивирус](https://www.kaspersky.ru/kav-vs-kis), который имеет также расширенные функции защиты от спама.

**Заключение**

Цель работы была выполнена, мои одноклассники узнали, как защитить свою информацию. Гипотеза была доказана.

Эта тема будет актуальна всегда, так как постоянно будут появляться новые способы обмана людей, но на данный момент при изучении данной темы никаких вопросов у меня не появилось.

Интернет может быть очень опасным, но в тоже время, нельзя не упомянуть о том, что Интернет сегодня является необходимостью. И здесь, как и в реальной жизни, всё зависит от самого человека. Если у него есть чувство меры *в «*отношениях с Интернетом*»* и не возникает нездоровая Интернет-зависимость, то такое достижение человечества, как Интернет вполне достойно всяческого уважения.