Государственное общеобразовательное казенное учреждение

Амурской области «Общеобразовательная школа

при учреждениях исполнения наказания»

ИНДИВИДУАЛЬНЫЙПРОЕКТ

**Угрозы в сети Интернет**

Автор: Тымкив Владислав Юрьевич,

обучающийся 12 класса \_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись

Руководитель: Руцынская Наталья Викторовна,

учитель информатики

с. Среднебелая, 2023

|  |  |
| --- | --- |
| ОГЛАВЛЕНИЕ | 2 |
| ВВЕДЕНИЕ | 3-4 |
| 1 ОБЩАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ - УГРОЗ И ИХ ВИДЫ | 5-8 |
| 2 ЧТО ТАКОЕ БЕЗОПАСНОСТЬ И ЗАЩИТА В СЕТИ ИНТЕРНЕТ? | 9 |
| 3 ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО | 10 |
| 4 РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ ОБУЧАЩИХСЯ |  11-12 |
| ЗАКЛЮЧЕНИЕ | 13 |
| СПИСОК ЛИТЕРАТУРЫ | 14 |

ВВЕДЕНИЕ

Интернет  - это безграничный мир информации, который даёт широкие возможности для общения, обучения и отдыха, т. е. выполняет информационную, коммуникационную, образовательную, коммерческую, развлекательную и многие другие функции. Интернет является неотъемлемой частью жизни современного человека, на просторах сети Интернет пользователи обмениваются информацией, хранят персональные данные. Пользователем Всемирной паутины может быть любой человек, независимо от его социального статуса, профессии, интересов и т. д.

Нельзя отрицать того факта, что Всемирная паутина - это публичная открытая система, данные в которой ежедневно изменяются и пополняются и не могут быть полностью защищены. Огромная база данных интересует злоумышленников.

Информация может быть обнаружена, перехвачена и использована мошенниками.

Киберпреступники систематически разрабатывают вредоносное программное обеспечение и используют различные способы для кражи конфиденциальной информации. Жертвой вредоносной угрозы может стать как конкретный пользователь, так и организации, государство.

Международных органов, пресекающих эти преступные действия на глобальном уровне, не существует. В РФ существует специальный отдел «К», который занимается ловлей киберпреступников, осуществляет борьбу с компьютерными преступлениями и нелегальным оборотом РЭС (радиотехнических средств).

Именно в этом заключается **актуальность** **исследования**: важно знать о потенциальных угрозах в сети Интернет и уметь самостоятельно защищать свои данные.

**Объект** исследования: выявление угроз в сети Интернет.

**Предмет** исследования:защищённость пользователей сети.

**Проблема** исследования: слабая защищённость пользователе й сети Интернет.

**Цель** работы: на основе анализа изученной информации выделить угрозы в сети Интернет и разработать рекомендации для повышения уровня безопасности пользователей сети Интернет.

**Задачи** работы:

1. Проанализировать значение понятия «угроза» в сети Интернет и определить виды угроз.
2. Изучить способы защиты от угроз в сети Интернет.
3. С помощью анкетирования оценить уровень знаний одноклассников как пользователей сети Интернет.
4. Разработать рекомендации по соблюдению правил безопасности при работе в сети Интернет.

**Гипотеза** исследования:защищенность пользователя сети Интернет увеличится, если расширить кругозор Интернет - угроз и использовать разработанные рекомендации по соблюдению правил безопасности.

**Практическая значимость** проекта заключается в разработке буклета с рекомендациями по соблюдению правил безопасности в сети Интернет.

**Методы исследования**:

* теоретические - анализ, синтез, сравнение, обобщение, конкретизация, моделирование;
* эмпирические - изучение научной литературы;
* анкетирование.

1 ОБЩАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ – УГРОЗ И ИХ ВИДЫ

В современном мире Интернет является важной частью жизни человека, в среднем человек проводит около 5 часов во «Всемирной паутине». В сети можно найти огромное количество информации, но помимо пользы, в интернете существует немало опасностей. Каждому человеку необходимо осознавать, какие угрозы таятся в сети Интернет, как избегать этих угроз и как бороться с ними.

Угроза информационной безопасности - это совокупность факторов и их последствий, создающих реальную и потенциальную опасность состоянию защищенности национальных интересов государства, общества и личности в информационной сфере сети Интернет.

Интернет - угрозы принято разделять на:

* **контентные угрозы**, связанные с неподобающими и незаконными материалами;
* **коммуникационные угрозы,** связанные с контактами с интернет мошенниками;
* угрозы, связанные с **интернет - безопасностью**.

В проектной работе подробно рассмотрены угрозы, связанные с интернет – безопасностью так как избежать их значительно сложнее, чем контентные и коммуникационные угрозы.

Основные виды интернет - угроз:

**Вредоносные программы.**Цель вредоносных программ - причинить ущерб компьютеру, серверу или компьютерной сети.

Вредонсное ПО включают в себя ряд угроз, таких как:

**Вирус**  - это программа, которая может прикрепляться к файлам на компьютере, заражает их, а затем копирует себя для заражения других файлов. Популярным способом распространения вируса является электронная почта. Большинство компьютерных вирусов способны наносить повреждение, например, это может быть команда для удаления всех файлов в системе или вызвать другие подобные осложнения.

**Червь** отличается от вируса тем, что ему не требуется внедряться в существующую программу. Черви могут воспроизводиться и распространяться самостоятельно. В результате они быстро истощают ресурсы зараженного компьютера.

**Рекламное ПО** - вредоносный вирус, отображающий нежелательные рекламные сообщения в браузере и на рабочем столе, например, в виде баннеров, всплывающих окон или панелей инструментов. Такие программы обычно не вредны, но они очень затрудняют использование вашего компьютера.

**Шпионское ПО** - отслеживает активность пользователей - например, просмотренные страницы или запущенные программы. Разновидностью шпионского ПО является **кейлоггер** - программа, которая записывает нажатия клавиш на клавиатуре или делает снимки экрана;

Программы - вымогатели - разновидность вредоносных программ, способных блокировать доступ к вашему компьютеру. Чтобы снять блокировку, жертву обманом заставляют заплатить выкуп на указанный номер банковского счета.

Вредоносные программы часто выдают себя за законные и полезные программы, которые на деле оказываются троянскими программами.

 **Троянская программа** - программа, представляющая собой инструмент для атаки, замаскированный под некоторую легитимную программу. Успешное выполнение троянского коня зависит от успешности его маскировки под программу, которую пользователь согласится запустить. Троянские кони могут быть сравнительно безвредными или могут содержать код, способный повредить файлы на жестком диске пользователя.

**СПАМ** - это нежелательные сообщения, как правило, рекламного характера. Они рассылаются массово многим пользователям. Объявления побуждают пользователя перейти по ссылке, загрузить файл или выполнить определенное действие, например, купить или использовать услугу. Электронная почта и обмен мгновенными сообщениями чаще всего используются для рассылки СПАМА.

**Фишинг**, серьезная угроза в сети Интернет, - это методы, используемые киберпреступниками для введения пользователя в заблуждение с целью получения определенных преимуществ. Киберпреступники выдают себя за известные компании и учреждения, например, сбербанк, полицию, суд и другие. Они пытаются влиять на эмоции своих жертв, обычно вызывая у них страх или создавая ощущение нехватки времени. Чаще всего целью фишинговых кампаний является получение доступа к банковскому счету или личным данным.

**Взлом слишком простых паролей**

Хакеры могут легко и быстро взломать простые пароли и получить доступ к банковскому счету, электронной почте, интернет - магазину или другим веб - сайтам.

**DoS - атаки** и **DDoS - атаки** (атаки типа «отказ в обслуживании») используются для перегрузки сетевых серверов в попытке выключить веб - сайт или онлайн - сервис - на несколько минут, часов или даже дней. DoS - атаки осуществляются с одного компьютера, а DDoS - атаки осуществляются с целой сети заражённых компьютеров, называемой бот - сетью ботнетом.

Такие виды атак могут использоваться опытными хакерами и теми, кто готов заплатить за DoS - атаки или арендовать ботнеты (специальную сеть компьютеров, зараженных вирусом). DoS - атаки и DDoS - атаки не особо опасны для вашей безопасности в сети Интернете как для отдельного пользователя. Они направлены скорее на тех, кто занимается бизнесом в сети Интернет или имеет свой веб - сайт. Почему? Потому что эти атаки могут привести к незапланированному простою в работе сайта и, следовательно, к предотвращению доступа клиентов, что может привести к огромны финансовым потерям.

**Уязвимости приложений** – ошибки, допущенные программистами на этапе разработки программного обеспечения. Они позволяют злоумышленникам получить незаконный доступ к функциям программы или хранящимся в ней данным.

Обнаружение вредоносной программы становится чрезвычайно трудным, если она установлена вместе с **руткитом** - вредоносным кодом, скрывающим опасные процессы в системе. Хакеры также могут получить полный контроль над компьютером, что разрешено эксплойтом - программой, которая позволяет брать на себя права администратора, например, для кражи или удаления файлов.

Киберпреступники обычно используют уязвимости в операционной системе компьютера для установки вредоносного ПО. Вы также можете неосознанно привести к заражению, например, загрузив зараженный файл из сети Интернет или посетив зараженный веб - сайт.

Таким образом, можно сделать вывод, что в сети Интернет содержится большое количество различных угроз, каждая из которых может принести огромный ущерб вашей личной информации.

2 ЧТО ТАКОЕ БЕЗОПАСНОСТЬ И ЗАЩИТА В СЕТИ ИНТЕРНЕТ?

**Интернет безопасность** - это процесс сохранения безопасности пользователя в сети Интернет. Необходимо убедиться, что потенциальные уязвимости в сети Интернет не ставят под угрозу вашу личную информацию или сохранность устройства, которое вы используете.

Согласно распространённому определению, **защита в сети Интернет** - это соблюдение правил и выполнение действий с целью удостовериться, что личные данные пользователя в сети Интернет не попали в руки киберпреступников.

Защиту в сети Интернет легко спутать с безопасностью в сети, но лучший способ отличить их – это понять следующее: Защита в сети Интернет - это то, что обеспечивает вашу безопасность в сети.

Защита в сети Интернет - это примерно такая же сложная система, как и предотвращение кражи кредитных карт, но при этом настолько же простая, как использование антивирусных программ для защиты технических устройств от вредоносных программ и вирусов.

Таким образом, в современном мире, хакерские атаки происходят примерно каждые 39 секунд, к безопасности и защите в сети Интернет следует относиться серьёзно. Иначе всем вашим личным данным может угрожать опасность.

3 ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Как защититься от онлайн - угроз?

Мы уже знаем, каковы наиболее распространенные опасности в сети Интернет, также следует знать, как их предотвратить.

Прежде всего:

* защитите свой компьютер с помощью антивирусной программы - обязательно с защитой сети Интернет в реальном времени. Используйте антивирус, который также включает в себя родительский контроль, фильтр защиты от спама для электронной почты и брандмауэр;
* не забывайте регулярно обновлять операционную систему, антивирус, браузер и другие приложения;
* будьте бдительны - при использовании сети, не переходите по ссылкам от неизвестных отправителей и всплывающей рекламе, не загружайте вложения из отправленных ими сообщений;
* создавайте сложные для расшифровки пароли, состоящие из множества букв, цифр и специальных символов;
* скачивать файлы из надежных источников - легально работающих сайтов, с хорошими отзывами от многих пользователей;
* обращайте особое внимание на домены, которые представляют собой странную комбинацию букв и отличаются от привычных com, org, edu, ru и других.

На всех устройствах следите за возможным появлением ранних признаков заражения вредоносным ПО, чтобы не дать ему закрепиться в недрах системы.

Во время работы в сети Интернет не нажимайте на рекламные блоки во всплывающих окнах. Не открывайте вложения в электронных письмах, которые пришли от незнакомого отправителя, не загружайте программы с непроверенных веб - сайтов или через пиринговые сети.

4 РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ ОБУЧАЩИХСЯ

Чтобы проверить, насколько мои одноклассники готовы защититься от сетевых опасностей было проведено тестирование, в котором приняли участие 10 человек.

Вопросы теста «Безопасность в сети Интернет»:

1. Что из предложенного НЕ является опасностью в сети?

|  |  |
| --- | --- |
| а) Травля в сети; | б) Фишинговые сайты; |
| *в) Общение с друзьями;* | г) Общение с незнакомцами. |

2. Если твой друг часто делится фотографиями в сети, какая настройка безопасности ему совершенно необходима?

|  |
| --- |
| а) Кто может писать мне личные сообщения: ВСЕ. |
| *б) Кто может смотреть фотографии со мной: ТОЛЬКО ДРУЗЬЯ.* |
| в) Кто может смотреть фотографии со мной: ВСЕ. |
| г) Кто может писать сообщения на моей странице: ТОЛЬКО ДРУЗЬЯ. |

3. Что нужно делать, если ты подвергся травле в сети?

|  |
| --- |
| а) Написать другу - он поддержит. |
| б) Закрыть страницу - тогда тролли не смогут ничего писать. |
| в) Поговорить со взрослым - он сможет держать ситуацию на контроле. |
| *г) Все вышеперечисленные варианты вместе!* |

4. Что такое фишинг в сети?

|  |
| --- |
| а) Онлайн - игра про ловлю рыбы. |
| *б) Вид мошенничества: создание поддельных сайтов - сообщений с целью получить личную информацию.* |
| в) Рекламные сообщения на тему рыбалки. |
| г) Навязчивая реклама в сети. |

5. Какой вред наносят сетевые тролли?

|  |
| --- |
| а) Никакого - это же просто шуточки. |
| б) Воруют деньги с банковских карт. |
| *в) Обидными сообщениями портят настроение, собираются в стаи и не дают жертве покоя.* |
| г) Ломают троллейбусы. |

В результате проведения данного теста было выявлено, что из 10 опрошенных:

1. 80 % ответили верно, что общение с друзьями не является опасностью в сети Интернет?

2. 50 % ответили верно, что смотреть фотографии со мной могут смотреть только друзья.

3 40 % опрошенных знают, как правильно себя вести, если ты подвергся травле в сети .

4. 90 % опрошенных знают, что такое фишинг.

5. Какой вред наносят сетевые тролли? Ответили верно 80 %.

ЗАКЛЮЧЕНИЕ

В ходе исследования выяснилось, что все люди пользуются сетью Интернет, но не все знают, какие интернет - угрозы их ожидают**.** Лишь 90 % опрошенных знают как правильно себя вести в сети Интернет, чтобы не подвергаться интернет - атакам. Что не нужно заходить на незнакомые нам сайты, скачивать и устанавливать неизвестные программы, размещать информацию о себе и своих близких.

Пользователям сети Интернет, требуется сформировать эффективную политику безопасности информационных технологий, быть в курсе происходящего, т. е. следить за новостями в сфере защиты информации, а так же не забывать о том, что виртуальный мир, как и реальный - требует внимания к мелочам, даже к тем, который порой кажутся совсем незначительными.

Пользуясь интернетом всегда нужно быть бдительным и внимательным. Мировая паутина всегда имеет таких пауков, которые могут навредить пользователям.

Цель и задачи исследования выполнены. Гипотеза исследования:защищенность пользователя сети Интернет увеличится, если расширить кругозор Интернет - угроз и использовать разработанные рекомендации по соблюдению правил безопасности подтвердилась.

В результате изучения и анализа материала по теме проведённого исследования мной были получены новые и ценные знания, которые пригодятся не только мне, но и моим родственникам и друзьям.

Сейчас я смогу просто и понятно объяснить моим знакомым, как действовать в том или ином случае и как их предостеречь, чтобы не стать жертвой мошенников.

СПИСОК ЛИТЕРАТУРЫ

1. Башлы П. Н. Информационная безопасность / П. Н. Башлы. -Ростов н/Д: Феникс, 2016.

2. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / Петр Николаевич Девянин. - М.: Издательский центр «Академия», 2015.

3. Мельников В. П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. - М.: Издательский центр «Академия», 2015.

4. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.

5. Юрьева Т. Ю. Словарь информационных продуктов и услуг / Т. Ю. Юрьева. - Кемерово.: - РОСТИКС, 2016.