Итоговый индивидуальный проект

Направление: Физико-математическое

Тема: « Интернет без опасности»

Выполнил: _____

Руководитель проекта: _____

_____ год

Содержание

Введение

В настоящее время почти каждый человек использует ресурсы сети Интернет. Интернет помогает сделать нашу жизнь интереснее. Но, к сожалению, с развитием технологий появляется всё больше людей, которые хотят нанести вред личным данным простого пользователя или просто человеку и крупным предприятиям, и организациям. Значит, вопрос о безопасности встаёт на первое место. Поэтому данная работа актуальна.

Цель работы: обобщить и систематизировать информацию по безопасному пользованию ресурсов сети Интернет в виде листовки.

Для достижение цели надо решить следующие задачи:

1. изучить научную литературу;
2. обобщить и систематизировать полученную информацию;
3. провести анкетирование учащихся;
4. оформить листовку средствами MS Word.

Продукт проекта: листовка с советами по безопасному использованию ресерсов Интернета.

Глава 1 Компьютерные преступления

Компьютерные преступления - это преступления, совершенные с использованием компьютерной информации. При этом компьютерная информация является предметом и средством совершения преступления.

Компьютерные преступления очень сложно предотвратить, потому что методы защиты постоянно отстают от методов нападения. Такие преступления совершаются в глобальном масштабе, преступники действуют на большом удалении, выследить их очень сложно, из-за того что они прикрываются чужими именами, и след их, если таковой остается, крайне запутан. Компьютерная преступность повсеместно принимает организованный характер.

Также в Интернете очень распространены случаи, когда подростков просят распространять наркотические вещества или завлекают в секты и экстремистские организации. Регистрируясь на каком-нибудь сайте, вы можете указать конфиденциальную информацию, которой могут воспользоваться мошенники. Кроме этого, в интернете люди могут подвергнуться травле.

Преступники в области информационных технологий – это не только высококвалифицированные специалисты в области компьютерной техники и программирования, но обычные пользователи ПК, которые в силу недостаточного знания техники или желания бесплатно воспользоваться какой-либо программой, совершают незаконные действия, сами того не подозревая. По статистике из каждой тысячи киберпреступлений, только семь совершаются профессионалами, которые характеризуются многократностью применения противоправных действий с целью достижения корыстных целей, а также непременным сокрытием состава преступления.

Основные разновидности киберпреступлений:

- *Взлом* – это получение несанкционированного доступа к данным, через компьютерные системы.
- *Фишинг* — это попытка завладеть конфиденциальной информацией, такой как имена пользователей, пароли и данные кредитной карты, которая выглядит как источник, заслуживающий доверия.
- *Компьютерные вирусы* — это компьютерные программы, которые могут размножаться и нанести вред компьютерным системам по сети без ведома пользователей системы.

• *Киберпреследование* – это использование коммуникационных технологий, главным образом Интернета, с целью преследования лиц.

• *«Кража личности»* — это одна из самых серьезных фальсификаций, когда происходит хищение денег и получение других благ через использование фальшивого удостоверения.

• *Кибервымогательство* – это угроза или вред веб-сайту, серверу или компьютерной системе с помощью отказа в обслуживании или других атак на уязвимую систему с целью шантажа, называется кибервымогательством.

• *Кибервойны* – это действие государства по проникновению в компьютеры или сети другого государства, с целью нанесения ущерба или разрушения.

Опасности в интернете можно разделить на несколько групп:

Контентные - разного рода материалы (текстовые, видео и аудио) содержащие вредоносную информацию, способную нанести психологический и физический вред нашему здоровью.

Коммуникационные — это потенциальные опасности, которые таит в себе интернет-общение. Сеть создает иллюзию доверительных отношений. Одной из опасностей, связанной с коммуникационными рисками, является киберпреследование.

Интернет-мошенничество — это одна из важных и острых проблем всего Интернета. Постоянно появляются все новые и новые схемы по выкачиванию денег с наивных пользователей. Безнаказанность мошенников, анонимность и простодушность самих людей, вечно тяготеющих к легкой выгоде и простым решениям, создают благодатную почву для процветания мошенничества в Сети.

Можно выделить ряд наиболее типичных схем одурачивания наивных пользователей:

• **потребительское мошенничество** – приобретение сомнительных, контрафактных, фальсифицированных товаров или же вовсе потеря денежных средств без получения желаемой покупки.

• **фишинг** – разновидность сетевого мошенничества, целью которого является получение недоброжелателем платежных данных вашей банковской карты.

Существует несколько разновидностей фишинга. Массовые рассылки направлены на очень широкую аудиторию, и чаще всего слеплены довольно поспешно, что сразу вызывает подозрения у опытных пользователей. Письма, в которых идет речь об огромных

выигрышах и победе в какой-либо рекламной акции обычно сходу удаляется или бросается в папку «*Спам*». Тем не менее, массовая рассылка берет числом и назойливостью, поэтому всегда находятся жертвы необдуманного азарта.

Обычно мошенники рассылают множество писем с заманчивыми предложениями, сообщениями о мнимом выигрыше или купонами от известных магазинов, с сообщениями о скидках и акциях. Часто в таких письмах прикрепляются поддельные ссылки на сайты. Цель таких писем – обманным путём заполучить личные данные, платежные реквизиты и т.д.

Для защиты от фишеров следует учитывать следующие моменты:

1. Помнить, что пароль – только ваш, ни одна организация не станет требовать его от вас. Он необходим только для доступа к определённому сервису и только вы должны знать его.
2. Внимательно проверять каждое полученное почтовое сообщение с неизвестного адреса на предмет наличия всевозможных просьб перейти по ссылке.
3. Всегда проверять с помощью адресной строки, на том ли сайте вы вводите свои идентификационные данные. Обычно подделывается и домен, поэтому он бывает похожим на свой оригинал. Различие может заключаться лишь в одной букве (например, mail.ru легко превращается в meil.ru).
4. Использовать последние версии интернет-браузеров и лицензионные антивирусные программы.
5. При входе на банковские сайты следить за тем, чтобы было установлено защищённое соединение https.

- **интернет-попрошайничество** – размещение фиктивных объявлений с просьбой о благотворительной помощи.
- **Социальные сети, Знакомства, блоги, чаты, секты.**
- **Мошенничество через внедрение вредоносных программ на ваш компьютер.**
- **Распространение наркотиков.**

Сейчас незаконный оборот наркотиков посредством сети Интернет совершается очень продуманными схемами преступной деятельности. Уровень профессионализма участников растет с каждым днем. Современные технологии позволяют полностью исключить встречу участников сделки, а тем более с организатором, обеспечив тем самым бесконтактный способ распространения наркотиков. Как правило, при таких схемах

удается поймать и привлечь к уголовной ответственности лишь рядовых участников преступных групп – курьеров и закладчиков, а выявить организаторов на сегодняшний день практически невозможно, что обусловлено использованием участниками современных телекоммуникационных технологий и соблюдением мер конспирации, использования зашифрованных сетевых ресурсов, псевдонимов и кодовых слов.

- **Экстремизм, нацизм, фашизм.**

Информационный экстремизм – деятельность, направленная на социально-психическое деструктивное воздействие граждан через использование информационных технологий для достижения противоправных целей. Признаком информационного экстремизма является нанесение морального, физического и материального ущерба в результате нарушения законных интересов, прав и свобод граждан**.** По статистике больше всего уголовных дел заведено в отношении пользователей социальных сетей

Глава 2 Ход работы

Сначала в разных источниках была рассмотрена информация о различных видах преступлений и способах защиты от них.

После этого было проведено анкетирование [Приложение 1]среди одноклассников для того, чтобы еще раз убедиться в актуальности проблемы безопасности в Интернете. Результаты анкетирования показали, что 83% участников сталкивались с разного рада неприятностями в сети Интернет. Но только 26% из них регулярно поддерживают свою киберграмотность.

После анализа полученной информации была проведена систематизация материала. Затем отобран наиболее существенный, нашей точки зрения материал. Таким образом, получился перечень правил для безопасного использования ресурсов Интернет.

Советы по защите информации

Пользуйтесь двухфакторной аунтификацией. Этот инструмент не идеален, но значительно повысит защиту. Злоумышленнику понадобится не только ваш интернет-аккаунт, но и доступ к телефону. Продвинутые преступники могут взломать и мобильное устройство, но угроза от большей части хакеров будет устранена.

Используйте несколько аккаунтов/почт. Не нужно привязывать все ваши сервисы к одной электронной почте. Потому что, если преступник получит доступ к этой почте, вы можете потерять все аккаунты, привязанные к ней.

Используйте сложные пароли, регулярно их меняйте. Способность злоумышленников подбирать и генерировать новые пароли постоянно растёт. Соответственно, необходимо менять и усложнять свои пароли, защищающие доступ к вашей информации.

Регулярно копируйте свою информацию. При заражении вашего устройства или сети, ваша информация также находится под угрозой. Поэтому необходимо всегда иметь резервную копию данных, к которой можно будет прибегнуть в случае возникновения критической ситуации.

Не доверяйте никому. Иногда злоумышленником может оказаться даже ваш близкий друг, которому зачем-то понадобились ваши данные. А зачастую преступники могут просто использовать аккаунты ваших знакомых, чтобы переслать вам заражённые файлы и получить доступ к вашим деньгам или информации.

Не делайте в сети то, что не сделали бы прилюдно. Всё, что попадает в интернет, остается там навсегда. Грамотный специалист сможет получить любую информацию о вас когда-либо опубликованную в сеть, например.

Поддерживайте свою киберграмотность. Если вы будете регулярно следить за новостями мира кибербезопасности и пользоваться рекомендациями экспертов в этой сфере – вы будете подготовлены к киберугрозам и защищены от них лучше, чем подавляющее большинство людей. Злоумышленники хотят получить доступ к вашим деньгам или информации. Но мало кто из них будет стараться обходить защиту, которая потребует для них дополнительных усилий.

Из данных правил были выделены основные тезисы для листовки. Для подготовки буклета было решено использовать текстовый процессор MS Word.

Таким образом, продуктом проекта является листовка, содержащая основные советы по безопасности в Интернете.

Вывод

В результате работы над проектом была изучена и систематизирована информация о видах угроз в Интернете и способах безопасного поведения в Сети. Была подготовлена листовка с советами по безопасности в Интернете. Таким образом, поставленная цель достигнута.

Данную листовку можно использовать в качестве раздаточного материала среди школьников.

Список использованной литературы

1. Интернет-безопасность: что это и как сохранить безопасность в сети?/ Текст: электронный. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security?ysclid=lfy8lxpllv788623051 (дата обращения 21.12.2022).

2. Угрозы в сети Интернет [Электронный ресурс] – Режим доступа:: https://safe-surf.ru/users-of/article/212/?ysclid=lfy8o2ixfm127401182 (дата обращения: 26.11.2022).

3. Босова Л.Л. Информатика. Базовый уровень 9 класс : учебник / Л.Л. Босова, А.Ю. Босова - .: БИНОМ. Лаборатория знаний, 2019

Приложение 1

Результаты анкетирования

В проведенном анкетировании приняли участие 24 человека 9 класса. Каждый из них пользуется интернетом.