Министерство общего и профессионального образования

Ростовской области

Муниципальное бюджетное общеобразовательное учреждение

Средняя общеобразовательная школа №9

Всероссийская исследовательская работа

«Online-угрозы и профилактика»

Подготовил: Евсюкова Софья Александровна

Обучающаяся 11 Б класса МБОУ СОШ№9

346880, г. Батайск, ул.Ленина, д.95/26

Домашний адрес с индексом и контактным телефоном:

346887, г.Батайск, ул.Ленина, д.123

т.89014464202

e-mail:sofievsukova25@gmail.com

Руководитель: Клеопина Светлана Вячеславовна

МБОУ СОШ№9

346880, г. Батайск, ул.Ленина, д.95/26

Батайск

2021 г.

**Введение:**

*С формированием мировой сети почти любой ежедневно использует ресурсами сети интернет. Установлено, то что всеобщая сеть, в первую очередь, считается неиссякаемым источником информации также полем с целью виртуального общения. Но далеко не все понимают, какой вред способен причинить индивидуальному компьютеру пользователя. Безопасность в сети интернет представляет собой принятие требуемых мер, которые обеспечивают защиту от компьютерных вирусов разной сложности, а еще от взлома ПК злоумышленниками с целью завладения индивидуальной либо корпоративной информацией.*

**Актуальность темы:** вопрос о безопасности встает на первое место. Безопасность использования интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

**Цель работы*:*** раскрыть источники угроз, которые несет всемирная сеть. Определить насколько осведомлены пользователи сети Интернет о безопасном использовании ресурсов, дать рекомендации по соблюдению правил безопасной работы в Интернете дома.

**Объектом** **исследования:** безопасность вИнтернете. Выявление способов защиты от интернет угроз при работе за компьютером дома.

**Предметом исследования:** является безопасная деятельность в интернете и способы защиты от интернет - угроз.

**Гипотеза:** пользователи сети Интернет, используя его, должны помнить об угрозах, которые он содержит.

**Задачи**:

* изучить скрытые и открытые угрозы интернета;
* выделить способы защиты от интернет угроз.

**Основные методы исследования**: теоретический анализ научной и методической литературы; отбор информации; анализ; обобщение; описание.

**Глава 1.**

**Какие сайты сливают ваши данные**

Зачастую, люди, когда проходят регистрацию на том или ином сайте, без разбора ставят галочку на пункте "Я прочитал и согласен с условиями политики конфиденциальности". Но ведь её никто не читал, а там может быть очень много интересных пунктов.

Из-за конструкции, состава и объёма, плюсом ко всему соглашение почти всегда пишут *маленьким шрифтом* и на юридическом языке - её мало кто читает, а если и находятся такие люди, то у них скорее всего последняя стадия паранойи. Такие уловки делают специально для того, чтобы пользователи оставались в неведении и не узнали истинную цель политики конфиденциальности.

Если почитать хотя бы одно соглашение, допустим от Вконтакте, то можно узнать - они продают ваши данные. Специально для более лёгкой проверки было создано расширение Privacy Monitor, оно автоматически проверяет соглашение и выносит вердикт, по которому пользователь должен уже сам судить - принимать/не принимать.

**Шпионское приложение MonitorMirror**

С помощью данного приложения хакер сможет без проблем полностью перехватить управление устройством, а именно: записывать звук с микрофона, записывать видео, просмотреть контакты, пин-коды, пароли и так далее.

Если на устройстве жертвы установлены root-права, то проникнуть можно даже в самую глубь системы и полностью вывести устройство из строя, перехватив абсолютно все данные.

Защита от MonitorMirror:

Установите достаточно надёжный пароль на ваше устройство, это не значит, что нужно ставить пароль "дата рождения мамы" - НЕТ. Воспользуйтесь специальными сервисами, которые помогут вам в создании хорошего пароля.

С *осторожностью* относитесь к программам, требующим доступ к "Специальным возможностям". Также стоит запретить установку приложений из сторонних источников. Установите хороший антивирус.

**Как сканы документов попадают в сеть, и что с их помощью могут провернуть мошенники**

Есть несколько вариантов того, как личные данные могли попасть в чужие руки.

Первый вариант. Вы загружали сканы или фото своих документов для регистрации на каком-то сайте или проходили идентификацию личности на каком-либо сервисе. Далее произошла утечка данных из-за взлома баз данных каким-нибудь хакером. После этого все сканы и фото документов попадают в руки к теневым продавцам, которые продают их на различных сайтах. Купить данные какого-нибудь неизвестного человека может практически каждый.

Второй вариант. Могло произойти и такое, что вы просто напросто загрузили фото документов на фейковый сайт и следовательно сами выдали мошенникам свои личные данные.

Третий вариант. Маловероятный, но всё же. Сливать данные документов могут недобросовестные работники госучреждений, которые имеют доступ либо к базе данных, либо к самим документам. Неизвестные их подкупают и получают все необходимые данные. Может произойти и так, что специальные люди устраиваются на работу в госучреждения и уже сами получают доступ к данным людей.

**Что злоумышленник может сделать, имея фото или сканы различных документов**

*Первое,* и наверное самое безобидное, это пройти идентификацию личности на сайте или получить VIP-доступ в каком либо сервисе, не выдавая свои личные данные. Зачастую идентификация проходит довольно просто, пользователь прикладывает фото документов и всё, он идентифицирован системой. Тоже самое делает злоумышленник, от Вашего лица он регистрируется в системе и производит какие-либо действия.

*Второе*. Он может зарегистрировать электронный кошелек для своих теневых транзакций. Чаще всего используют QIWI кошелек. С помощью ваших документов он пройдет идентификацию личности, которая в QIWI проходит так же, как я описала выше, и зарегистрирует кошелек на Ваше имя.

Никакого личного присутствия для подтверждения не требуется. Далее с помощью этого кошелька мошенник может производить какие угодно транзакции, не опасаясь, что его найдут. Все претензии сначала отправят владельцу паспортных данных, а пока поймут в чем дело, злоумышленник давно скроется и заметет следы.

*Третье.* Микрозаймы. Выдаётся только на именные банковские реквизиты, поэтому помимо паспортных данных ему понадобится доступ к банковскому счету жертвы, чтобы потом перевести деньги себе. Наиболее простой их получить - это применить социальную инженерию и скинуть файл с вредоносным ПО, которое жертва установит на свой компьютер (тут играют лишь умения злоумышленника). Либо начать общение с жертвой, втереться в доверие и скинуть ей файл с вредоносным ПО под каким-либо предлогом. С его помощью злоумышленник сможет следить за всем, что происходит на компьютере и рано или поздно узнает банковские реквизиты, логины и пароли от личных кабинетов, получив тем самым доступ к банковскому счету.

Поэтому перед тем как загрузить куда-либо свои данные, сканы документов или фото, внимательно ознакомьтесь с документацией и политикой конфиденциальности. Удостоверьтесь, что вы перешли на нужный сайт, они должны быть защищены и поддерживать шифрование.

**Кардинг — что это такое?**

Многие встречали в интернете кучу объявлений о продаже новых вещей или техники из США, Европы и так далее. Но вряд ли догадывались, что весомая их часть публикуется кардерами.

Здесь я расскажу, что это за тёмный бизнес, и как кардеры работают.

Кардинг – это кража денег с карты на свою карту, счет, аккаунт в платёжной системе, а также покупка товаров с использованием чужой кредитной карты. Чаще всего кардеры используют снятие наличных, покупку брендовой одежды или электроники. Но прежде всего, им нужен номер карты и данные для аутентификации. Кардеры покупают базу данных и проверяют актуальность информации в ней или же подбирают пароли с помощью брутфорса или других методов.

Другой вариант – организация фишинговой компании. Копируется страница банка с формой для входа в аккаунт или создаётся фальшивое приложение, с помощью спама распространяется ссылка на него. Пользователь, обеспокоенный тем, что его карту могут заблокировать; банк просит подтвердить операцию; поступил перевод неизвестно от кого – идёт на фальшивый сайт или запускает поддельное приложение. Кардер забирает введённые данные и переводит все деньги себе.

**Что такое вбив?**

Это процесс ввода данных карты в форму на сайте магазина или платёжной системы. Чтобы не рисковать, кардеры используют для вбива взломанные компьютеры рядовых пользователей. Затем их чистят от логов или избавляются от железа.

Другой вариант – работа с эмулятора Android-смартфона или виртуальной машины. После вбива достаточно удалить программное обеспечение, чтобы замести следы.

С карт можно заказать физические товары или вывести деньги. Есть казино, онлайн-игры и другие варианты виртуальной передачи денег.

Кассир в супермаркете тоже может быть кардером. Обычно они не могут похвастаться высокой зарплатой. Но если они занимаются кардингом, то получают в 5-10 раз больше денег. Когда вы проводите оплату картой, кассир или продавец может незаметно посмотреть и запомнить данные. Для некоторых сайтов при заказе товаров достаточно номера карты и CVV2, который написан на обороте. Но кардер может пойти дальше и поставить собственный «ридер» для считывания всех данных карты.

А что думает полиция?

Обычно полноценное расследование начинается, только если кардер украл значительную сумму средств – более 1000 долларов. Обычно после этого ФРБ направляет запрос полиции. И в запросе содержатся IP-адреса, имена, адреса отправки и другая информация о потенциальном преступнике.

Для этого кардеры используют дропов. Это люди, которые стоят на низшей ступени в цепочке и выполняют самую грязную работу: обналичивают деньги, предоставляют свои данные для получения посылок, отправляют посылки кардерам и т.д.

Кардеры дают дропам минимум информации и практически не контактируют с ними. Так что даже если дропа выследят, у него будет алиби на момент взлома банковского аккаунта или снятия денег с карты. Да и о кардере он ничего не сможет рассказать. В итоге преступление останется нераскрытым.

Практика показывает, что если кардер работает через VPN, прокси и другие сервисы, а также соблюдает правила безопасности в интернете, доказать его вину практически нереально. Поэтому даже если полиция нагрянет домой к кардеру, сотрудникам ещё придётся доказать факт совершения компьютерного преступления.. Ловят чаще всего на переписке в мессенджерах, наличии данных чужих карт и аккаунтов, сборок вредоносного программного обеспечения и т.п. Денежные переводы сами по себе достаточным доказательством не являются. Свидетельские показания тоже. Если кардер сможет притвориться дропом или посредником, то быстро переквалифицируется из обвиняемого в свидетеля.

Думайте, прежде чем переходить по ссылкам. Установите лимиты на оплату в интернете, не забывайте про антивирус на смартфоне Android и Windows-компьютере. Также лучше использовать одну карту для повседневных покупок, а вторую для хранения более крупных сумм денег, и по необходимости переводить деньги со второй на первую. В случае любых подозрений по поводу незаконного списания средств звоните в банк, чтобы заблокировать карту и начать расследование.

**Глава 2.**

*В данной главе я расскажу о маштабных примерах хакерства и как себя максимально обезопасить*

**Фальшивая раздача от Илона Маска**

Илон Маск - достаточно интересный персонаж, имя которого уже не первый год на слуху. Мошенники, конечно же, стараются выдавить из этого имени по максимуму выгоды, например, приплетая имя Илона к разного рода сомнительной деятельности.

Так, самая грандиозная афера с использованием имени Маска принесла злоумышленникам более 180 тысяч долларов в 2018 году всего за один день.

Со временем, махинации, связанные с известными именами, настолько расплодились по инету, что многие личности были вынуждены даже оставлять специальные метки на своих официальных страницах по типу "криптовалюты не раздаю", но, как показывает практика, многие не особо осведомленные личности, по прежнему продолжают верить в то, что такие раздачи честные и за ними и вправду стоят громкие имена, при том никак не проверяет информацию.

В некоторых же ситуациях дела обстоят иным образом. Личные страницы громких имён просто взламываются хакерами и, таким образом, с верифицированной страницы производится розыгрыш. И до момента, пока страница будет восстановлена, многие пользователи успевают потерять значительную часть своих средств. Чаще всего, злоумышленники пишут небольшой пост со страницы знаменитости, куда помещают ссылку на "конкурс", которая представляет из себя фишинговый сайт. Ни о чём не подозревающие пользователи переходят по ней, вводят свои конфиденциальные данные, а также, добровольно прощаются со своими деньгами, ведь иногда условия "конкурса" подразумевают перевод n-суммы. Многие люди в погоне за лёгкими деньгами забывали об элементарных правилах безопасности и собственноручно вручали преступникам свои деньги.

**Google раскрыли новую хакерскую атаку**

Недавно Google опубликовали отчёт, подробно описывающий очередную хакерскую операцию, которая была обнаружена компанией в начале 2020 года.

Атаки хакерской группы были направлены на пользователей Google, которые используют компьютеры на операционный системе Windows, а также устройства Android. В общей сложности, хакеры использовали 4 уязвимости нулевого дня. Суть атаки заключалась в том, что хакеры внедряли на легитимные сайты свой фишинг-код, который перенаправлял посетителей на источники злоумышленников. В общих чертах, эксплойты, которые использовались злоумышленниками, представляли из себя разнородные комбинации из найденных уязвимостей в Google, а также других проблем.

Использование найденных уязвимостей позволяло хакерам проникнуть в устройства жертв, развернув эксплойт в операционной системе, таким образом, получив практически полный контроль к устройствам своих жертв.

**Использование Интернета является безопасным, если выполняются три основные правила:**

***1. Защитите свой компьютер***

Используйте антивирусную программу.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

***2. Защитите себя в Интернете***

С осторожностью разглашайте личную информацию.

Думайте о том, с кем разговариваете.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

***3. Соблюдайте правила***

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

И в Интернете, и в реальной жизни агрессия, кража, обман – запрещены

**1. «Сильный» пароль на самом деле может предотвратить большинство атак**

Директор по информационной безопасности Yahoo Алекс Стамос большую часть своей карьеры посвятил обнаружению угроз и определению, как хакеры могут использовать уязвимости в ПО. Вот что он говорит:

«Я наблюдаю много пренебрежения вопросами безопасности с тех пор, как Сноуден опубликовал секретные документы. Общее мнение примерно такое – мы ничего не сможем сделать, чтобы быть в безопасности. Это может быть правдой в отношении обычного человека и аппарата разведки уровня государства, но это не должно мешать людям предпринять необходимые шаги для защиты себя от более реалистичных угроз.

Пользователи могут предпринять следующее, что им действительно поможет:

1. Инсталлировать менеджер паролей и использовать его для того, чтобы создавать уникальный пароль для каждого сервиса, который они используют
2. Активировать двухфакторную идентификацию (как правило через смс) в емэйл или социальных сетях

Также я бы хотел, чтобы СМИ перестали формировать мнение о том, что если в сфере хай-енд хакеров возможны действительно невероятные вещи, то это должно значить, что невозможно обезопасить себя от абсолютного большинства наиболее вероятных атак.»

**2. Новое устройство – не означает «безопасное»**

Когда вы открываете коробку с только что купленным смартфоном или компьютером, вы ожидаете, что он полностью «чист» и безопасен, но это не так. Элеонора Саитта, технический директор Института современных СМИ, что это самый опасный миф – что новое устройство безопасно, и только впоследствии, от его использования в разных условиях, оно может подхватить вирус или вредоносное ПО.

Если облака для вас   
не просто теория

Широкий спектр услуг   
по выделенным северам   
и мультиклауд-решениям

Конфигурация VPS и бесплатный тест уже через 2 минуты

Организация вашей IT-инфраструктуры на основе мультиклауд-решения

«Вот почему Superfish так много значил (это adware, которое предустанавливалось на лэптопах Lenovo). В нем был встроен бэкдор, и но сделано было это очень плохо, и в итоге оказалось, что воспользоваться им может каждый.»

Многие устройства приходят к пользователям с уже инсталлированными бэкдорами. Как правило это делается по требованию государства, для помощи правоохранительным органам.

«Если какой-то обходной путь встраивается в систему, то вы встравиаете проблему своими собственными руками. Да, вы каким-то образом можете контролировать доступ, но в конце концов – этой уязвимостью может воспользоваться каждый»

**3. Самое лучшее ПО содержит уязвимости**

Многие люди думают, что хорошее ПО и надежные сети гарантируют защиту. Париса Табриц, руководитель отдела безопасности в Google Chrome, считает следующее:

«Иметь абсолютно надежный софт означает иметь ноль багов в миллионах строк кода, что невозможно, в то время, как хакеру нужно найти лишь один, который можно использовать. В ПО всегда будут ошибки. Какие-то из них будут иметь влияние на безопасность, и необходимо определить, на какие из них необходимо потратить ресурсы, чтобы обезопаситься, и многое зависит от того, как какие существуют модели угроз»

Специалист по компьютерной безопасности корпорации RAND Лиллиан Эблон считает, что не существует абсолютно безопасной системы:

«С наличием соответствующих ресурсов, всегда найдется способ взлома. Целью информационной безопасности должно стать сделать взлом максимально дорогим для атакующего – в смысле как денег, так и других ресурсов, времени»

**4. Каждый вебсайт и приложение должны использовать https**

Мы все слышали про какие-то проблемы с https – он замедляет работу, он только для сайтов, которые должны быть супер-безопасными, он плохо работает. Все совсем не так. Питер Экерсли, специалист, который изучал вопросы https для Electronic Frontier Foundation, говорит следующее:

«Часто думают так – раз мы не принимаем платежи по пластиковым картам, нам не нужен https на сайте или в приложении. Каждому сайту нужен https – поскольку без него для хакеров очень легко перехватить информацию о том, что именно вы читаете на сайте, какие данные обрабатывает ваше приложение, а может быть и модифицировать эти данные в процессе.»

**5. Облако, как и любая система, не может быть полностью безопасным**

Сегодня все в облаках. Там ваша почта, фотки, мгновенные сообщения, и так далее. И это на самом деле безопаснее, чем вы можете подумать, но там возникают проблемы другого рода. Ли Ханивэлл, специалист по информационной безопасности крупной облачной компании, объясняет:

«Облачные сервисы могут связать данные и поведение своих клиентов – например, мы можем увидеть, что с одного ip-адреса залогинились на несколько аккаунтов, причем из совсем другой страны, чем когда-либо с них логинились»

Другими словами – многие из атак становятся очевидными для систем защиты облачных сервисов, которую обычный пользователь никогда не создаст самостоятельно.

«Сначала я сама обслуживала свой емэйл-сервер, но потом переключилась на хостящийся сервис, потому что знаю, что Gmail или Outlook.com делают это гораздо лучше меня. Но для многих людей возможность наблюдения за их действиями со стороны Агентства национальной безопасности является проблемой, и они обслуживают свои емэйл-сервера самостоятельно»

**6. Обновления ПО критически важны для безопасности**

Мало что раздражает так, как появляющееся сообщение, что надо что-то обновить в ПО. Но часто это единственное, что стоит между вами и «плохим парнем».

О’Доннелл из компании Сisco говорит следующее:

«Частота обновления ПО редко зависит от введения новых фич в ПО, но больше зависит от того, как компании обнаруживают какие-то новые угрозы, которыми может воспользоваться хакер, чтобы получить доступ к вашей системе»

**7. Хакеры – это не всегда преступники**

Многие хакеры занимаются своим ремеслом, чтобы сделать системы более надежными. Когда уязвимость установлена, ее можно устранить.

О’Доннелл из Cisco говорит:

«Если кто-то хочет взломать вас, он может купить все существующие системы защиты, которые могут быть у вас, и тестировать свою атаку в похожей среде, но для борьбы с угрозами нужно знать не только инструменты, которые могут использоваться, но нужны также люди, которые знают как эти инструменты можно использовать».

Эблон из RAND считает, что обычный хакер, как мы его себе представляем – редко является серьезной угрозой. Настоящая проблема может исходить от людей, которых вы и не подозреваете, и их мотивация может быть гораздо более сложной, чем обычное воровство.

«Во многих случаях собственный работник или инсайдер – настолько же большая угроза, которая может поставить бизнес на колени».

**8. Кибертерроризм – очень редкая штука**

Как правило, самая страшная вещь, которая может с вами случиться, это что кто-то вломится в вашу систему, потому что у вас слабенький пароль. Но почему-то люди как правило думают, что кибератаки это прямо-таки «смертельная» угроза. Но системы восстанавливаются из бэкапов, угрозы изолируются, и никто не умирает. Эблон говорит:

«Нам не следует забывать про безопасность «интернета вещей», но кибертерроризм (пока) фактически не существует. То, что сейчас называют кибертерроризмом, это фактически «хактивизм» - хакерские активистские действия – типа взлома страничек и распространения на них пропагадны Исламского государства»

**9. Darknet и Deepweb – это разные понятия**

Эблон отмечает, что в СМИ постоянно путают, что это значит.

«Deepweb относится к той части интернета, которая непроиндексирована поисковыми системами, и соответственно, не может быть найдена через, например, Google. Darknet – это сети, не являющиеся частью обычного интернета, где пользователям нужно специальное ПО для доступа к ним. Например, Silk Road и многие противозаконные торговые площадки хостятся на сетях из Darknet таких как I2P или Tor»

Таким образом, заведите себе хранилище паролей, используйте двухфакторную идентификацию, старайтесь пользоваться сайтами с https и не перестаньте опасаться взлома вашего компьютера со стороны правительственных органов, если вы только не преступник международного масштаба :)

**Заключение:**

Сеть Интернет может быть весьма опасным, однако в свою очередь, невозможно никак не отметить о том, что Сеть Интернет на сегодняшний день является необходимостью. И здесь, как и в реальной жизни, всё зависит от самого человека. Если у него существует границы в «отношениях с Интернетом» и не зарождается нездоровая Интернет-зависимость, то подобное достижение человечества, как Сеть Интернет абсолютно достойно всяческого уважения.

Так же достигнуты все задачи, которые мы ставили перед собой:

* изучили скрытые и открытые угрозы интернета;
* проанализировали классификацию интернет - угроз
* выделили способы защиты от интернет угроз;

**Список литературы**:

1. Левский Н.А. Чего опасаться в Интернете. Самые опасные сайты. Вредоносные программы. // Журнал ComputerBild – 2013, - Режим доступа - http://www.windxp.com.ru/acpeg.htm , свободный.
2. Добреля Т.В. Чего опасаться в Интернете http://tim-plus.ru/opasnost-v-internete-i-kak-ee-izbezhat.html
3. http://www.microsoft.com/rus/athome/security/children/backtoschool.mspx - сайт корпорации Microsoft, посвященный проблемам безопасности в сети Интернет.
4. http://www.compdoc.ru/secur/internet/securpolicy/glava5\_2.shtml - сайт посвящен Политике безопасности сети.
5. Юрьева, Т. Ю. Словарь информационных продуктов и услуг / Т.Ю. Юрьева. - Кемерово.: - РОСТИКС,2006.- 50 с.
6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008