МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Пензенский государственный технологический университет»

(ПензГТУ)

Колледж технологический

Индивидуальный проект

по дисциплине

Информатика

на тему:

Безопасность в интернете

Выполнил студент: Комиссарова Кира Игоревна

Группа 22ИП1Т

Руководитель проекта: Пудовкина Ольга Николаевна

Проект защищен с оценкой

Дата защиты

Пенза, 2023 год

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Сегодня информацию обрабатывают с помощью персональных компьютеров. Атаки на компьютерные системы получили большую распространенность. Число активных пользователей Интернета растет в геометрической прогрессии. Проблема безопасности при работе в сети все более актуальна.

Знания пользователей о компьютерной безопасности при использовании сети Интернет отстают от темпов развития сети и роста угроз безопасности.

Угрозы безопасности в сети Интернет – это вредоносное программное обеспечение; интернет-мошенничество; атаки на отказ в обслуживании[1] [14]; кражи денежных средств; кражи персональных данных; несанкционированный доступ к информационным ресурсам и системам; распространение недостоверной информации. Основные угрозы информационной безопасности пользователя Интернета, идущие от авторизованных пользователей и электронных методов воздействия – умышленные повреждения или похищения данных хакерами, повреждения данных в результате неосторожных действий, электронные методы воздействия (спам, фишинг).

Актуальность темы

Безопасность использования Интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

Объектом исследования является возможность безопасной работы в сети Интернет.

Предметом исследования являются рекомендации IT-компаний по безопасной деятельности в Интернете и способам защиты от интернет-угроз.

Цель работы

Показать возможность безопасной работы в сети Интернет при соблюдении рекомендаций IT-компаний.

[1] Попытка причинить вред, сделав недоступной целевую систему, например веб-сайт или приложение, для обычных конечных пользователей. Злоумышленники генерируют большое количество пакетов или запросов, перегружают работу целевой системы.

Гипотеза

При условии выполнения рекомендаций по соблюдению мер безопасности при работе за компьютером можно избежать возникновения последствий интернет-угроз.

В соответствии с целью исследования и выдвинутой гипотезой были поставлены следующие **задачи**:

- проанализировать классификацию интернет-угроз;
- выделить изучить скрытые и открытые угрозы интернета;
- способы защиты от интернет-угроз;
- проанализировать материалы компаний Microsoft, Google и российских компаний по обеспечению безопасности;
- подготовить рекомендации;
- выполнить презентацию по материалам исследования.

Основными методами исследования являются: теоретический анализ материалов сети Интернет и рекомендаций ведущих интернет-компаний; отбор информации; анализ; обобщение; описание.

Теоретическая часть. Глава 1. Вредоносное программное обеспечение

1.1. Вредоносные программы

Вредоносные программы могут вывести из строя компьютер, испортить или удалить файлы, украсть личную информацию пользователя (например, считать пароль с клавиатуры) или использовать гаджет пользователя для корыстных целей (например, рассылать спам).

Эти программы можно разделить на три группы: вирусы, сетевые черви и трояны.

Компьютерные вирусы быстро распространяются путем самокопирования, незаметно для пользователя. Эти программы заражают и удаляют файлы, занимают место в системе, вызывают сбои в работе компьютера. Чаще всего это исполняемые файлы (с расширением .exe, .com) или документы (.doc, .xls), в которых есть вредоносные макросы.

Сетевые черви – это программы, которые самостоятельно распространяются через Интернет и локальные сети. Размножаются стремительно, действуют в тайне от владельца зараженного компьютера. Например, рассылают зараженные сообщения по всей адресной книге почтовой программы или организуют ботнет[2] [15] для рассылки спама. Могут перегрузить сеть и вывести ее из строя за счет интенсивного процесса распространения.

Трояны – программы, которые маскируются под видом безвредных или полезных программ, чтобы пользователь запустил их на своем устройстве (например, загрузив файл с трояном с файлообменника). В отличие от вирусов и червей самостоятельно распространяться не умеют. Цель такого «Троянского коня» – дать злоумышленнику доступ к компьютеру пользователя, после чего тот сможет завладеть паролями и другой ценной информацией.

К несанкционированным действиям с данными относят: кражу, мошенничество, вымогательство и шпионаж за пользователем. Для кражи может применяться сканирование жесткого диска, регистрация нажатий клавиш

[2] Это сеть компьютеров, зараженная вредоносным программным обеспечением. Киберпреступники используют ботнет-сети, которые состоят и большого количества компьютеров для различных вредоносных действий без ведома пользователей.

(Keylogger)[3] [9] и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы; похищения данных, представляющих ценность или тайну; кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов, платежных систем). Аккаунты при этом применяются для рассылки спама, а через электронную почту можно заполучить пароли от других аккаунтов.

Вредоносные программы также выполняют другую незаконную деятельность: получение несанкционированного доступа к ресурсам самого компьютера или третьих ресурсов, доступных через него, в т.ч. прямое управление компьютером (backdoor[4]) [4], осуществляют организацию на компьютере открытых vpn-туннелей[5] [4] и общедоступных прокси-серверов. Зараженный компьютер (в составе ботнета) может быть использован для проведения DDoS-атак, сбора адресов электронной почты и распространение спама, в т.ч. в составе ботнета. К такой деятельности относится также накручивание электронных голосований, кликов по рекламным баннерам; генерирования монет платежной системы Bitcoin, и даже использование эффекта 25-го кадра для зомбирования человека.

1.2. Способы заразиться

Самые распространённые способы распространения вредоносного программного обеспечения – электронная почта, сообщения в мессенджерах и программы для обхода существующих правил: бесплатное повышение рейтинга в соцсетях, перехват СМС-сообщений с чужого телефона, программа слежки, дополнительные функции в сервисах, которых официально не существует (например, VIP-доступ, подарки, изменение цвета иконки в мессенджере) [16].

---

[3], Кейлогер (англ. keylogger, key – клавиша и logger – регистрирующее устройство) – программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши. Несанкционированное применение – установка кейлоггера происходит без ведома владельца конкретного персонального компьютера. Несанкционированно применяемые кейлоггеры – шпионские программные продукты или шпионские устройства. Несанкционированное применение связано с незаконной деятельностью. Несанкционированно устанавливаемые шпионские программные продукты имеют встроенные средства доставки и дистанционной установки сконфигурированного модуля на компьютер пользователя, то есть процесс инсталлирования происходит без непосредственного физического доступа к компьютеру пользователя и не требует наличия прав администратора системы.

[4] Вредоносная программа, намеренно оставленная лазейка в коде легальной программы, которая предоставляет доступ к устройству для несанкционированных действий. Бэкдор (от англ. back door – «черный ход»): скрытно впускает злоумышленника в систему, наделяя правами администратора.

[5]В компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей. VPN (англ. Virtual Private Network «виртуальная частная сеть») – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например, Интернет.

1.3. Защита от вирусов

Для защиты от вирусов необходимо, чтобы не было никаких вложений, присланных неизвестными отправителями. Подозрительные письма нужно удалять сразу.

Особую опасность могут представлять собой файлы с расширениями: .ade, .adp, .bas, .bat; .chm, .cmd, .com, .cpl; .crt, .eml, .exe, .hlp; .hta, .inf , .ins, .isp; .jse, .lnk, .mdb, .mde; .msc, .msi, .msp, .mst; .pcd, .pif, .reg, .scr; .sct, .shs, .url, .vbs; .vbe, .wsf, .wsh, .wsc.

Поэтому можно включить режим отображения расширений. Часто вредоносные файлы маскируются под обычные графические, аудио- и видеофайлы. Включить полный запрет на прием писем с исполняемыми вложениями (для установки программ). Если возникнет необходимость получить программу по почте, нужно попросить отправителя заархивировать ее.

Если случайно открыть письмо и исполняемым вложением, но еще не запустить его, то нужно отправить сообщение в «Корзину» и удалить не только из папки «Входящие», но и из «Удаленных».

Если получено извещение о том, что письмо не было доставлено, причина – возможная отправка вируса, срочно нужно проверить компьютер антивирусной программой.

Необходимо, чтобы были установлены самые последние версии браузера и антивирусной программы, регулярно проверять наличие обновлений операционной системы, не отключать программы-сторожа, которые входят в антивирусную программу. Обычно они запускаются при загрузке компьютера и отслеживают действия программ, блокируя нежелательные действия и запросы к системе.

Также необходимо проверять загруженные файлы антивирусной программой, регулярно сканировать систему полностью в целях профилактики заражения; менять пароли; регулярно выполнять резервное копирование важной информации [16].

1.4. Сохранение конфиденциальности личной информации

1.4.1. Беспроводная сеть

К беспроводным сетям подключаются компьютеры, мобильные устройства, планшеты и игровые системы. Такая сеть удобна, но уязвима. Её можно защитить, защитив беспроводной маршрутизатор. Изменить имя маршрутизатора с заданного по умолчанию на уникальное, которое трудно будет угадать; задать надежный пароль для маршрутизатора; выбрать для маршрутизатора параметры безопасности WPA2 или WPA; отключить гостевой вход [6].

1.4.2. Организации для защиты от мошенничества в Интернете

Управление «К» МВД РФ – https://мвд.рф/К

Управление «К» занимается нарушениями закона в сфере компьютерной информации. Сюда нужно обращаться, если взломали личный кабинет онлайн-банка и похитили деньги со счета или подделали банковскую карту. Также здесь помогут, если нарушены авторские права на цифровые произведения (например, фотографию используют в коммерческих целях без согласия).

Чтобы обратиться, нужно перейти в интернет-приемную по ссылке, выбрать в списке пункт «Управление «К» МВД России» и нажать «Продолжить» [10].

Роспотребнадзор – http://rospotrebnadzor.ru/

Защищает права потребителей. В Роспотребнадзор можно жаловаться на недобросовестные торговые онлайн-площадки. Если цена товара в итоге получилась выше, покупку не доставили и не возвращают предоплату, вещь оказалась некачественной и причинила вред здоровью. Роспотребнадзор принимает обращения в электронном виде. Предварительно необходимо ознакомиться с правилами обращения и авторизоваться через сайт госуслуг [12].

Роскомнадзор – https://rkn.gov.ru/

Сюда нужно обращаться, если пользователь узнал о нарушении в обработке личной информации. Принимает обращения в электронном виде.

Роскомнадзор ведет единый реестр запрещенных сайтов (http://eais.rkn.gov.ru/), реестр сайтов, на которых содержатся призывы к экстремистской деятельности и массовым беспорядкам (http://398-fz.rkn.gov.ru/);

реестр сайтов, на которых размещен нелегальный контент (http://nap.rkn.gov.ru/); реестр сайтов с высокой посещаемостью (http://97-fz.rkn.gov.ru/). Сюда можно обращаться, если сайт или блог вдруг стал недоступен без видимых техническим причин [11].

Глава 2. Методы безопасной работы в Интернете

2.1. Правила безопасной работы в Интернет

При работе в сети Интернет следует придерживаться следующих правил:

1. Не пересылать конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.

2. При входе в социальную сеть или почту с чужого компьютера, нужно «разлогиниться» (прекратить сеанс работы в качестве зарегистрированного пользователя).

3. Выключать Wi-Fi, если не пользоваться в текущий момент. Отключить функцию автоматического подключения к Wi-Fi в телефоне или планшете.

4. Не доверять непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Такие сети злоумышленники используют для воровства личных данных пользователей.

5. Не заходить в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Пользоваться мобильным интернетом.

6. Банки, сервисы и магазины никогда не рассылают писем с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные.

7. Отключить Сири (голосовой помощник поколения Apple) на айфоне. Мошенники выводят деньги через интернет-банк голосовыми командами.

8. Завести несколько адресов электронной почты: личная, рабочая и развлекательная (для подписок и сервисов).

9. Придумать сложный пароль, для каждого ящика разный.

10. Везде, где это возможно, включить двухфакторную аутентификацию [7].

11. Регулярно менять пароли, обновлять браузер и спам-фильтры.

12. Установить и обновлять антивирусные программы. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.

13. Не «кликать» по ссылкам, пришедшим в сообщениях от незнакомых людей. Это способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного знакомого, поэтому лучше уточнить, что он прислал и нужно ли это открывать.

14. Не запускать неизвестные файлы, особенно с расширением .exe.

15. Внимательно проверять адреса ссылок, логотипы, текст и отправителя сообщений.

16. Никогда не отвечать на спам.

17. Если в мессенджер пришла просьба от знакомого с просьбой срочно выслать денег, ничего не отправлять. Сначала перезвонить ему, аккаунт может быть взломан злоумышленниками.

18. Минимум личной информации: не публиковать в сети домашний адрес, не писать, в какое время вас не бывает дома, не описывать свой постоянный маршрут, не хвалиться крупными покупками, не афишировать уровень достатка.

19. Регулярно выполнять резервное копирование данных. Следовать правилу «3-2-1»: создать одну основную копию и две резервные. Сохранить две копии на разных физических носителях, а одну – в облачном хранилище (например, Google Диск, Яндекс.Диск). Не забывать бэкапить (делать резервные копии) все устройства: смартфоны, планшеты, компьютеры/ноутбуки.

20. Чтобы никогда не терять деньги на незаметных платежах, не покупать дополнительных услуг по ошибке и точно заплатить за нужные, всегда читать правила перед тем, как поставить галочку напротив чекбокса[6] [13] «согласен» и перейти к оплате.

21. Если в секретном вопросе указали девичью фамилию матери, которая сейчас есть в открытом доступе на ее страницах в соцсетях, обязательно поменять

[6] Флажок, флаговая кнопка, чекбокс (от англ. check box), галочка – элемент графического пользовательского интерфейса, позволяющий пользователю управлять параметром с двумя состояниями – ☑ включено и ☐ отключено. Во включённом состоянии внутри чекбокса отображается отметка (галочка (✓), или реже крестик(×)). По традиции флажок имеет квадратную форму. Рядом с флажком отображается его обозначение, обычно – подпись, реже – значок.

секретный вопрос.

22. Не скачивать сомнительные приложения и не делать это по неизвестным ссылкам. Пользоваться только официальными магазинами App Store, Google Play и Windows Market.

23. Совет для пользователей Google Chrome, Firefox и Opera: при частом входе в сеть с ноутбука в сеть с ноутбука в общественных местах, установить специальное расширение для браузера для безопасного выхода в интернет – HTTPS Everywhere от Electronic Frontier Foundation (EFF). По умолчанию этот плагин обеспечивает безопасное соединение для Yahoo, eBay, Amazon и некоторых других веб-ресурсов.

24. Ничего не покупать в социальных сетях, особенно с предоплатой. Лучше переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).

25. Покупая в интернет-магазинах, сохранять здоровый скептицизм. Цена не может быть слишком низкой, тем более, если это оригинальная продукция бренда.

26. Изучить историю магазина в сети, проверить наличие контактов, выяснить, можно ли туда приехать и познакомиться вживую. Читая отзывы, обратить внимание, чтобы они были разными. Заказные отзывы пишут люди, которым приходится делать это много раз в день, поэтому такие тексты будто написаны по шаблону.

27. Посмотреть, как на отзывы реагируют продавцы. Обратить особое внимание на негативные: если их отрабатывают, это хороший знак (причем ситуация должна быть конкретная, содержать номер заказа).

28. Платить безопасно. Классический случай –переадресуют на защищенную страницу (адрес начинается с «https://»). Если нет, лучше не рисковать. По правилам эквайринга[7] на сайте продавца должна быть информация о том, кто принимает платеж. Нужно прочитать её и сверить с тем, что написано на следующей странице [18].

[7] Технология безналичного приема платежей с использованием банковских карт и систем бесконтактной оплаты. Для обработки и передачи платежной информации клиента используется специальный терминал. Оплата возможна дебетовыми и кредитными картами, с помощью мобильных телефонов через приложения Apple Pay и Samsung Pay и связанных с ними носимых устройств – часов или браслетов. При любом способе оплаты деньги сначала поступают в банк-эквайер, а затем переводятся на счет торговой компании.

29. Завести отдельную (можно виртуальную) карту для платежей в интернете.

30. Если для оплаты в интернете пользоваться своей обычной картой, не хранить на ней крупные суммы денег.

31. Подключить в банке СМС-информирование обо всех операциях по картам и счетам. Так можно быстро заметить, если карта будет скомпрометирована, и заблокировать ее.

32. Страницы ввода конфиденциальной информации любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета.

33. Обращаться о работе интернет-магазина: Роспотребнадзор, Общество защиты прав потребителей, на Горячую линию Рунета – www.hotline.rocit.ru.

34. Нужно быть осторожными при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.

35. Случайных многомиллионных наследств и неизвестных богатых родственников, которые просто так хотят поделиться, не бывает.

36. Не делать репостов жалостливых объявлений про милого котика, который срочно ищет дом (а в посте – телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Это мошенники, решившие заработать на сердобольных и доверчивых гражданах.

37. Логотип известного благотворительного фонда еще не означает, что деньги пойдут туда – реквизиты счета могут быть подделаны. Помогать нужно только для лично знакомых или, например, с проектом dobro.mail.ru.

38. Не покупать авиабилеты на незнакомых сайтах, особенно если они стоят гораздо дешевле, чем на всех остальных. Зайти на настоящийбилет.рф и удостовериться в подлинности ресурса. Также посетить сайт авиакомпании, которой нужно улететь, и сравнить цену билета на нужное направление [3].

39. Обращать внимание на адрес страницы, если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), ввести его вручную самостоятельно.

40. Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайти в ближайший офис мобильного оператора или позвонить ему с другого телефона и выяснить, в чем проблема. Возможно, кто-то получил дубликат симки и ее нужно срочно заблокировать.

По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт. Злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают [2].

При потере телефона, к которому привязана банковская карта, нужно срочно блокировать и симку, и карту.

41. Не пользоваться торрентами[8] [17], можно загрузить зараженный вирусом файл.

42. Мошенники создают сайты, на которых «можно» бесплатно посмотреть или скачать фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так со счета могут списать значительную сумму за СМС, а сам телефон попадет в базу спамеров.

43. Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего пользователь должен самостоятельно отключить услугу. Если он этого не делает, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.

2.2. Рекомендации безопасной работы от ведущих IT-компаний

Безопасность с Microsoft Windows

Компания предлагает продукты для улучшения безопасности и рекомендации по возникшей проблеме или вопросу. При этом советы даются в формате рассказа о ситуации с конкретным человеком и рассматриваются пути решения. Но ответы на некоторые вопросы выполнены машинным переводом, это не очень удобно.

Рекомендации Microsoft по защите от мошеннических сообщений и атак в сети:

Фишинг

[8] Специальный протокол, предназначенный для обмена файлами между пользователями. Пользователи скачивают файлы не с какого-то сервера, а друг у друга прямо с персональных компьютеров

Атаки, когда злоумышленник связывается с вами, выдавая себя за человека, которого вы знаете, или за организацию, которой вы доверяете, и пытается получить от вас личные сведения или убедить вас открыть вредоносный веб-сайт или файл.

Чаще всего попытки фишинга осуществляются по электронной почте, но также могут использоваться SMS-сообщения, прямые сообщения в социальных сетях или даже телефонные звонки.

Во всех случаях у попыток фишинга есть общие черты:

Доверенный отправитель

Сообщение или звонок поступают от человека или от организации, которым вы доверяете. Это может быть ваш банк, государственные службы, такие как Netflix или Spotify, tech company, такие как Microsoft, Amazon или Apple, или другая служба, распознаемая вами. Мошенники могут попытаться выдать себя за руководителя или члена семьи.

Срочный запрос

Как правило, подобные сообщения требуют от вас срочных действий. Что-то отменяется, или вам придется заплатить какой-либо штраф, или вы не сможете получить какую-то особенную скидку, поэтому вам требуется действовать НЕМЕДЛЕННО.

Ощущение срочности заставит вас серьезно отнестись к сообщению и выполнить запрошенные отправителем действия, не обдумав их как следует, не обратившись к надежному советнику и не определив, является ли сообщение поддельным.

Ссылка или вложение

Сообщение может включать объект, который вы должны открыть: как правило, это ссылка на веб-сайт или вложенный файл. Скорее всего, веб-сайт будет поддельным вариантом надежного веб-сайта, предназначенным для того, чтобы ввести имя пользователя и пароль или другие личные сведения, чтобы они могли украсть эти сведения, чтобы использовать их сами. Любой вложенный файл почти наверняка является вредоносным.

Как защититься от фишинга?

1. Внимательно изучайте все сообщения, требующие от вас каких-либо срочных действий. Обращайте особое внимание на адрес электронной почты отправителя. Если в сообщении говорится, что это ваш банк, но адрес отправитель не является доменным именем вашего банка, это должно быть громкое предупреждение.

2. Никогда не переходите по ссылкам и не открывайте вложения, получения которых вы не ожидали, даже если они внешне выглядят как отправленные человеком или организацией, которым вы доверяете. При получении ссылки от банка или другой доверенной организации откройте в веб-браузере новую вкладку и перейдите непосредственно на веб-сайт этой организации: используйте ссылку в избранном или результаты веб-поиска либо самостоятельно введите имя домена организации. Ссылка из фишинговых сообщений позволит вам зайти на сайт, который выглядит как настоящий, но с его помощью можно ввести свои персональные данные. Если вы получили вложение, которого не ожидали, не открывайте его. Вместо этого вы можете связаться со звонив отправителю другим способом, например с помощью текстового сообщения или телефонного звонка, и проверить, является ли вложение истинным, прежде чем открывать его.

Вредоносные программы

Компьютер может заразиться вредоносными программами разными способами, но чаще всего это открытие вложения с вредоносным файлом или скачивание и открытие файла с небезопасного веб-сайта.

Вы также можете заражение вредоносными программами, открыв файл или установив приложение, которое кажется полезным, но на самом деле вредоносным. Такие атаки называются «троянами». Одна из версий, которую используют злоумышленники, – это замаскировать вредоносную программу как обновление браузера. Если вы заметите необычное уведомление о том, что браузер нужно обновить, закройте сообщение о подозрительном обновлении и перейдите в меню параметров браузера. Перейдите на страницу Справка > О программе. Во всех основных браузерах на этой странице можно проверить обновления для браузера.

Один из типов вредоносных программ, который часто называют программой-вымогателями. Это определенный тип вредоносных программ, которые шифруют ваши файлы, а затем требуют оплаты от злоумышленников, чтобы разблокировать их для доступа к ним. Все чаще программы-вымогающие программы пытаются украсть ваши данные, чтобы злоумышленники также могли угрозу освободить ваши файлы, если вы не оплатите их.

Как защититься от вредоносных программ?

1. Не открывайте вложения и ссылки, которые вы не ожидали. Очень осторожно относитесь к выбору устанавливаемых приложений. Устанавливайте только надежные приложения известных поставщиков. Будьте особенно внимательны при скачивании файлов и приложений с сайтов то потоков или общего доступа к файлам.

2. Поддерживайте систему в обновленном состоянии. Убедитесь, что операционная система и приложения обновлены, на них должны быть установлены последние исправления. На ПК с Windows может помочь обновление.

3. Защищайте свои системы. На компьютере должна быть действующая современная антивирусная программа. В состав Windows 10 входит антивирусная программа «Защитник Windows», она включена по умолчанию. Кроме того, существует ряд сторонних антивирусных программ.

2.2.1. Безопасность с Google

Компания Google использует передовые средства защиты и удобные инструменты конфиденциальности, которые позволяют вам управлять своими данными. Чтобы обеспечить безопасность ваших данных, во всех сервисах Google используется встроенная защита, которая автоматически обнаруживает и предотвращает угрозы

Шифрование передаваемых данных

Когда вы отправляете письмо, открываете доступ к видео или посещаете сайт, происходит обмен информацией между вашим устройством, сервисами Google и центрами обработки данных. В целях безопасности они шифруют эту информацию,

используя многоуровневую систему защиты, в том числе передовые технологии HTTPS и TLS.

Предупреждения системы безопасности

Если Google выявляют потенциальную угрозу, то сообщают вам об этом и рассказывают, как можно усилить защиту. Это происходит, например, когда кто-то пытается войти в ваш аккаунт с неизвестного устройства или вы намереваетесь открыть вредоносный сайт, файл или приложение. Когда они замечают что-то подозрительное в вашем аккаунте, то отправляют вам уведомление. Оно приходит по электронной почте или показывается на телефоне, чтобы вы могли защитить свои данные одним нажатием.

Автоматическое обнаружение и блокировка угроз

Функция "Безопасный просмотр" защищает четыре миллиарда устройств, в том числе и ваше. Чтобы сделать интернет безопаснее для всех, они бесплатно предоставили эту технологию другим компаниям, и теперь она используется в таких браузерах, как Safari, Mozilla Firefox и других.

Глава 3. Практическая часть

1. Анкетирование

Изучая проблему нежелательного контента, я решила сделать провести практический эксперимент: насколько возможно подвергнуться риску при осуществлении поисковой деятельности в сети. Рассматривая теоретические аспекты проблемы исследования, я встретилась со следующими рисками:

- окна всплывающей рекламы,
- ссылки с предложением перейти на другой сайт,
- предложения зарегистрироваться и ввести персональные данные,
- предложения сыграть в игру,
- информационные всплывающие сообщения о личной жизни артистов.

Среди моих знакомых есть пользователи, чьи аккаунты в социальных сетях были взломаны и использовались мошенниками для сбора денег и распространения нежелательной информации через сервис личных сообщений.

Можно сделать вывод, что при отсутствии знаний о киберугрозах пользователь (особенно в детском возрасте) может легко стать жертвой нежелательного контента или мошенников.

Я провела анкетирование среди учащихся своего потока. Приняли участие 40 человек.

Выводы:

1. Среди участников опроса большинство (65%) ответили, что проводят в Интернете большую часть своего свободного времени, примерно около 9 часов.

2. Все, кто проходил опрос, знают о киберугрозах.

3. Среди самых популярных ответов на вопрос «О каких киберугрозах ты знаешь?» равное количество ответов (по 36%) получили «Троллинг» и «Киберзапугивание».

4. С целью избежания киберугроз большинство респондентов (37%) предложили не размещать персональные данные в сети интернет.

2. Правила пользования Интернетом

Всегда спрашивай родителей, взрослых о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

Нежелательно размещать персональную информацию в интернете. Персональная информация — это ваше имя, фамилия, возраст, номер мобильного телефона, адрес электронной почты, домашний адрес и адрес школы, в которой Вы учитесь.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на

него специальную программу — антивирус!

Пользуйтесь браузерами Яндекс, Opera, Google Chrome и Safari!

Контролируйте работу за компьютером. Неограниченное использование компьютера может привести к физическим (глазным, гиподинамия, остеохондроз) и психологическим заболеваниям (Интернет-зависимость). Через каждые 20 минут работы выполни зарядку для глаз.

Заключение

Цифровые технологии кардинально меняют модели взаимодействия между людьми и организациями, и внутри них. Формируется виртуальный мир, в котором нематериальные активы управляют материальными онлайн. Это – электронная торговля, интернет-банкинг. Глобальное информационное пространство сегодня включает свыше 311 млн доменных имен.

Зависимость киберпространства от информационных технологий, повсеместное активное использование площадок и сервисов определяют не только новые возможности, но и порождают новые угрозы безопасности.

Ряд факторов способствует возникновению угроз кибербезопасности – рост объема информации, развитие технологий сбора сведений о гражданах с

использованием различных каналов, возможность недобросовестных субъектов получить информацию о людях и объектах, важных с точки зрения безопасности. Нужен баланс безопасности и личной свободы в киберпространстве.

По данным Выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей Росстата доля населения в возрасте 15-74 лет, использовавшего мобильный телефон или смартфон за последние 3 месяца 2020 года, составляет 97,3%, число пользователей сети Интернет в возрасте 15-74 лет, являющегося активными пользователями сети Интернет составляет 84,15%, в том числе использует сеть Интернет для заказов товаров и/или услуг 46,2%, и только 2,4% – имеет опасения насчет защиты и безопасности персональных данных при работе в сети Интернет [5].

Поэтому имеет большое значение обеспечение безопасности при пользовании ресурсами Интернета с персональных компьютеров или мобильных устройств. Россия занимает первое место по количеству жертв киберпреступлений среди частных лиц.

При выполнении работы были изучены угрозы Интернета. Вредоносные программы, несанкционированные действия с данными, рассмотрены возможности сохранения личной информации.

Для организации защиты от мошенничества в Интернете предложены государственные порталы, куда можно обращаться по поводу большинства преступлений в сети Интернет.

Изучены, проанализированы и предложены правила безопасной работы в сети Интернет по материалам Microsoft Windows, Google, РОЦИТ (Регионального общественного центра интернет-технологий). Подробно рассмотрен электронный метод воздействия – фишинг и способы защиты от него.

Все предложенные рекомендации являются доступными любому пользователю при работе в сети.

По результатам работы выполнены презентации для публикации в сети Интернет и ознакомления студентов колледжа.

Цели и задачи работы выполнены.

Список использованных источников

1. Backdoor // TGLOBAL.COM –группа компаний, глобальный поставщик ИТ-услуг, продуктов и сервисов: сайт. // URL: https://vk.cc/c2djFr (дата обращения: 21.05.2021).

2. https://tcinet.ru/whois/.

3. https://настоящийбилет.рф.

4. VPN // ВикипедиЯ: сайт. // URL: https://ru.wikipedia.org/wiki/VPN (дата обращения: 21.05.2021).

5. Выборочное федеральное статистическое наблюдение по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей. // Росстат: сайт. URL:

https://gks.ru/free_doc/new_site/business/it/ikt20/index.html (дата обращения 13.04.2021).

6. Горячая линия Лаборатории Касперского // Сайт компании Kaspersky. URL: https://newvirus.kaspersky.ru/

7. Двухфакторная аутентификация, и как её включить. // Сайт компании Epic Games. URL: https://vk.cc/c1BvMR (дата обращения: 13.04.2021).

8. Дети онлайн // Линия помощи «Дети онлайн» – бесплатная всероссийская служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи. URL: http://detionline.com/helpline/about.

9. Кейлогер // ВикипедиЯ: сайт. // URL: https://vk.cc/4eJAeN (дата обращения: 21.05.2021).

10. МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ. // Сайт. URL: https://мвд.рф (дата обращения: 19.05.2021).

11. Роскомнадзор // Сайт ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ. URL: https://rkn.gov.ru/ (дата обращения: 19.04.2021).

12. Роспотребнадзор // Сайт Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека. URL: – http://rospotrebnadzor.ru/(дата обращения: 19.05.2021).

13. Флажок (интерфейс). // ВикипедиЯ: сайт. // URL: https://ru.wikipedia.org/wiki/ Флажок_(интерфейс) (дата обращения: 13.03.2021).

14. Что такое DDOS-атаки? // AWS: публичное облако компании Amazon. 2006 год. URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/#:~:text (дата обращения: 21.05.2021).

15. Что такое ботнет? // ESET: сайт компании ESET Internet Security. // URL: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/zashchita-ot-botnetov/ (дата обращения 21.05.2021).

16. Что такое вредоносное ПО и как от него защититься. // РОЦИТ: сайт Регионального общественного центра интернет технологий – общественной

организации Рунета. 28.11.2017. URL: https://rocit.ru/knowledge/soft/how-to-protect-from-malware (дата обращения: 13.02.2021).

17. Что такое торренты и как ими пользоваться. // EXLER.ru: сайт Алекса Экслера. URL: https://vk.cc/c1BvMR (дата обращения: 13.04.2021).

18. Что такое эквайринг. // Райффайзен БАНК. Сайт компании. // URL: https://www.raiffeisen.ru/wiki/chto-takoe-ekvajring/ (дата обращения: 20.03.2021).