Безопасность в сети интернет

Выполнил работу
студент группы СА1-11/12
Спиридонов Никита Андреевич
научный руководитель:
Хожайнова Марина Геннадьевна

Актуальность проекта

Я выбрал данную тему, потому что она связана с информационными технологиями, так же, как и моя профессия. А интересна она для меня тем, что я, как и большинство пользователей интернета, попадал в неприятную ситуацию, в которой злоумышленники присвоили мой аккаунт себе, для вымогания денег у моих знакомых и друзей.

Безопасность в сети интернет, в век компьютерных технологий, важна как никогда, но многие люди не знают, как обезопасить свое пребывание в интернете. Цель моего проекта - собрать и распространить информацию, связанную с защитой себя в интернете, показывая на примерах, какими разрушительными могут быть быть последствия.

Цель

Целью моего проекта - было разработать сайт, на котором содержалась бы информация, объясненная доступно для людей, которые хотят обезопасить свое пребывание в сети интернет

В результате работы, я хотел бы получить действительно качественный продукт, после которого люди смогли бы узнать действительно полезную информацию и конечно же сделать пребывание в интернете безопасным.

Задачи

При создании моего проекта мне потребовалось:

1. Прочитать и проанализировать материал по теме “Безопасность в сети интернет”
2. Написать свой текст, избегая копирования и повторений
3. Сделать свой сайт, и добавить информацию туда, которая будет находиться в свободном доступе, чтобы все заинтересованные люди смогли узнать что-то новое для себя.

Работа над проектом. Введение

Безопасность в сети интернет

Введение | Виды угроз | Борьба | Интересные факты | Правила/Заключение

Время, в котором мы живем часто называют «век компьютерных технологий» и это справедливо.
Невозможно представить сегодняшнюю жизнь без компьютеров и интернета. Они используются везде - в быту, практически в каждой семье имеется гаджет с доступом в интернет, на производстве, транспорте, различных технологических устройствах и т.д. так же используется всемирная сеть.

Однако массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе в сети интернет, разрушающих файловую структуру дисков и наносящих ущерб хранимой на устройстве информации, а также её пропаже.
Несмотря на разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них. Это и послужило стимулом для выбора темы моей работы.
В своем проекте я хочу рассказать о видах угроз в интернете, то как их избегать, и для наглядности, привести примеры из истории, чтобы доказать, что безопасность в Интернете очень важна.

Введение | Виды угроз | Борьба | Интересные факты | Правила/Заключение

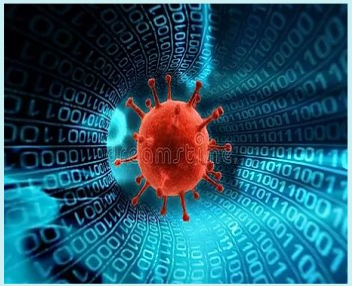
Ярославский Градостроительный Колледж
Никита Спиридонов
Группа СА1-12

2020

Работа над проектом. Виды угроз

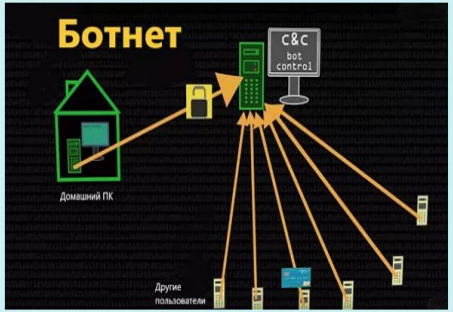
Начнем с того, что всего 2 причины по которым пользователи попадают в неприятные ситуации в интернете. Первая - это они сами, когда странствуют по интернету и без разбора переходят на разные сайты, а также скачивают и устанавливают непроверенные на угрозу файлы.
Вторая же - это, когда злоумышленники с помощью удаленного доступа, могут установить на чужой компьютер вирусные, троянские и вредоносные программы, из-за которых у пользователя могут пропасть важные личные данные, а так же пропасть полный доступ к устройству и оно будет без ведома владельца выполнять рассылку спама, участвует в DDoS-атаках на различные сайты, крадет пароли. Бывает и так, что провайдер вынужден принудительно отключить такое устройство от глобальной сети.

Интернет-пользователь может быть обманут или втянут в загрузку на компьютер вредоносного программного обеспечения. Основные типы таких программ представлены ниже:



- Вирус, иначе вредоносная программа — это любое программное обеспечение, используемое для получения несанкционированного доступа к информации или ресурсам компьютера с целью хищения, удаления, искажения или подмены данных. Вирусы делятся на группы по типу заражаемых объектов, методам заражения и жертвам. Заразить компьютер вирусом можно разными способами: от использования съемного носителя до посещения вредоносного сайта. Благодаря антивирусным компаниям в наше время вирусы встречаются довольно редко.

- Ботнет — компьютерная сеть, состоящая из запущенных ботов. Зачастую бот — специальная программа, устанавливаемая на компьютер пользователя без его согласия, которая позволяет злоумышленнику выполнять некие действия, такие как рассылка спама, переборка паролей.



Работа над проектом. Виды угроз

- Компьютерный вирус — это программы, которые создают копии самих себя с целью внедрения в коды других программ и системные области памяти, а также распространения самих себя по различным каналам связи. Чаще всего используются для захвата информации на компьютере. Компьютерные виды делятся на группы по поражаемым объектам, методам их заражения, поражаемым операционным системам и т. д.
- Лжеантивирус создает видимость работающего антивируса, что позволяет осуществить внедрение дополнительного заражения. Также может предлагать дополнительные услуги при введении пользовательских данных: кредитная карта, номер телефона и т. д.

- Сетевые черви в некотором роде являются вирусами, так как тоже способны копировать самих себя, но не могут нанести вред существующим файлам. Вместо этого они создают дополнительную нагрузку на компьютер за счет интенсивного распространения. Черви классифицируются по способу распространения и месту заражения.

- Вирус-вымогатель блокирует доступ к компьютеру или возможность считывания данных, а затем требует выкуп для восстановления исходного состояния. Вирусы этого типа могут шифровать данные, блокировать или препятствовать работе в системе или браузере.

- Программа-шпион — это программа, тайно отслеживающая активность пользователя и сообщающая о ней другим пользователям. Данный вид программ имеет широкий спектр возможностей: от сбора информации о посещаемых сайтах до удаленного управления компьютером или смартфоном.

- Кейлогер — программное обеспечение, регистрирующее нажатия клавиш на клавиатуре и мыши, а также дату и время этих действий.

Работа над проектом. Виды угроз

- **Вирус-вымогатель** блокирует доступ к компьютеру или возможность считывания данных, а затем требует выкуп для восстановления исходного состояния. Вирусы этого типа могут шифровать данные, блокировать или препятствовать работе в системе или браузере.

- **Программа-шпион** — это программа, тайно отслеживающая активность пользователя и сообщающая о ней другим пользователям. Данный вид программ имеет широкий спектр возможностей: от сбора информации о посещаемых сайтах до удаленного управления компьютером или смартфоном.

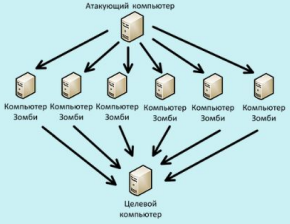
- **Кейлогер** — программное обеспечение, регистрирующее нажатия клавиш на клавиатуре и мыши, а также дату и время этих действий.

- **Троян** — вредоносная программа, проникающая на компьютер под видом легального программного обеспечения с целью выполнения действий, нужных злоумышленникам. Свое название вирус получил благодаря сходству по принципу действию с деревянным конем, погубившим Трою. Существует 5 основных типов троянов: удаленный доступ, уничтожение данных, загрузчик, деактиватор программ безопасности и сервер.

Помимо программ опасность представляют так же:

DdoS-атаки

DodS-атака (аббр. англ. Denial of Service «отказ в обслуживании») — это хакерская атака на систему, при которой реальные пользователи получают отказ в обслуживании. Проводятся с помощью создания большого количества запросов на сервер, что дает критическую нагрузку, при которой сервер может начать выдавать закрытую информацию или же просто перестает работать, что заставляет провайдера терять доход

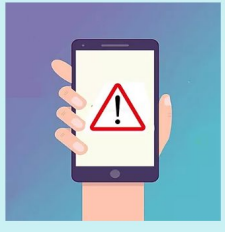


Фишинг

Фишинг — это вид интернет-мошенничества, в ходе которого злоумышленники получают доступ к конфиденциальной информации пользователя, такой как логин и пароль. Используется для массовой рассылки от имени популярных брендов, внутри частных сервисов или социальных сетей. В настоящее время цель фишеров — клиенты банков и электронных платежных систем.

Уязвимости приложений

Приложения, используемые для доступа к интернет-ресурсам, могут содержать уязвимости безопасности, такие как ошибки безопасности памяти или ошибочные проверки подлинности. Самые серьезные из этих ошибок могут дать сетевым злоумышленникам полный контроль над компьютером. Большинство приложений и комплексов безопасности не способны обеспечить качественную защиту от этих видов атак.



Работа над проектом. Борьба

Борьба с интернет у грозами

Вирусные атаки

Чтобы избежать проникновения вируса на устройство:

- Следите за регулярным обновлением операционной системы. Если этого не происходит, вирусам легче найти уязвимые места и проникнуть в компьютер.
- Пользуйтесь антивирусными программами. Они устранят многие угрозы, подскажут, можно ли посещать неизвестный вам сайт, проверят файлы, скачиваемые из интернета.
- Старайтесь никому не сообщать пароли от личного кабинета, банковских карт, социальных сетей, от рабочей личной почты

Спам и Фишинг

Чтобы избежать спама и фишинговых атак:

- Старайтесь не оставлять адрес почты на сайтах общего доступа (соц.сети, форумы)
- Используйте несколько почтовых ящиков для разных целей.
- Никогда не отвечайте на спам. После вашего отказа на рассылку, письма могут пойти с новой силой.

Кибер Шпионаж

Чтобы избежать знакомства с программами-шпионами, старайтесь не устанавливать на компьютер условно-бесплатные программы и не нажимайте на рекламные ссылки, которые открываются во всплывающих окнах.

Мошенничество

Чтобы обезопасить себя от мошенничества с банковскими картами:

- Нельзя сообщать посторонним людям секретную информацию, размещенную на обороте вашей дебетовой или кредитной карты.
- Для совершения операции по оплате достаточно фамилии имени и отчества держателя карты, а также номера карты.
- Если у вас возникает хотя бы малейшее сомнение в добросовестности продавца или покупателя, требуйте личной встречи и не передавайте деньги заранее.

Браузерный эксплойд

Чтобы избежать изменения в работе браузера:

- Не забывайте регулярно его обновлять
- Проверяйте, работает ли на вашем компьютере Брандмауэр – специальная программа, которая сканирует данные из интернета и регулирует их передачу на устройство.
- Не скачивайте условно-бесплатные рекламное программное обеспечение

Введение | Виды угроз | Борьба | Интересные факты | Правила/Заключение

Работа над проектом. Интересные факты

1. По статистике ежегодно каждый третий компьютер подвергается вирусным атакам хотя бы один раз в течении года.

2. По статистике ежегодно каждый третий компьютер подвергается вирусным атакам хотя бы один раз в течении года.

3. По исследованиям специалистом было выяснено, что антивирусы устаревают за 1-2 дня. За счет этого 15% вирусов спокойно проникают в компьютер невзирая на антивирусную защиту. Ведь ежедневно хакеры придумывают все более изощренные способы заразить технику.

4. Каждый год компьютерные вирусы наносят мировой экономике финансовый ущерб в размере $1,5 триллиона.

5. Самым безопасным вирусом считается вирус имеющий название «Blaster» также известный как Lovsan, Lovesan или MSBlast. Эпидемия червя наблюдалась в августе 2003 года. История началась с того, что коллектив Xfocus нашёл уязвимость в операционных системах Windows, связанную с переполнением буфера. За счет этой уязвимости появились вирусные программы, самой известной из которых стал именно червь Blaster. Червь попадая в компьютер начинал генерировать случайные IP-адреса и после этого искал уязвимости в системе жертвы, а найдя заражал электронику и так цикл многократно повторялся.

За счет такого распространения пострадало 300 тысяч компьютеров, 30 из которых в России. Для пользователей вирус был безопасен, разве что из-за вируса приходилось все время перезагружать компьютер. Целью Blaster была атака серверов Microsoft. Однако компания смогла сократить ущерб от червя к минимуму, благодаря временному закрытию серверов. Идея вируса заключалась в том, что червь содержал в коде скрытое послание, адресованное Биллу Гейтсу: «Billy Gates why do you make this possible? Stop making money and fix your software!!» («Билли Гейтс, зачем вы делаете это возможным? Хватит делать деньги, исправьте ваше программное обеспечение!»).
Создателем вируса оказался американский школьник Джеффи Ли Парсон, которого посадили на полтора года в тюрьму и поручили 225 часов общественных работ.

6. Самый быстрый вирус в мире — Slammer, переводится как тюрьма. За считанные минуты компьютерный червь смог заразить более 75 тысяч компьютеров.

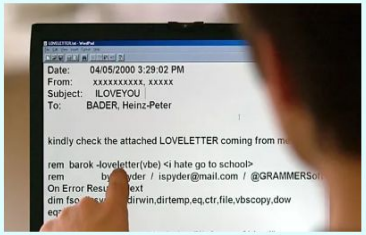
7. Первая масштабная вирусная атака в сети произошла в 1988 году. Она получила название «червь Морриса». Вирус заразил более 6 тысяч компьютерных систем в США (включая исследовательский центр NASA), парализовав их работу. Так «червь Морриса» принесла финансовый ущерб в размере $96 миллионов.

8. Компьютерные вирусы кроме уничтожения, дали жизнь новой отрасли экономики — ежегодно антивирусные компании зарабатывают до 2 миллиардов долларов на производстве антивирусных программных обеспечениях.

9. Компьютерные вирусы кроме уничтожения, дали жизнь новой отрасли экономики — ежегодно антивирусные компании зарабатывают до 2 миллиардов долларов на производстве антивирусных программных обеспечениях.

10. На интернет-аукционе в Нью-Йорке в мае был продан подержанный ноутбук Samsung NC10, зараженный шестью самыми известными компьютерными вирусами в мире. В совокупности они принесли финансовый ущерб мировой экономике на $95 млрд. Цена лота, который получил название Persistence of Chaos («Постоянство хаоса»), превысила $1,3 млн, или 83,7 млн рублей. Этот арт-объект выполнил китайский художник Го О Дун, работающий в области современного искусства, известной как пост-интернет. Вирусы господину Го предоставила израильская компания кибербезопасности Deep Instinct. Целью работы было придать физический смысл абстрактным угрозам, создав своего рода «каталог исторических угроз». В США запрещено распространение вредоносного ПО. Поэтому организаторы аукциона позиционировали лот как произведение искусства или объект для научных исследований. Более того, перед вручением Persistence of Chaos победителю торгов у компьютера обещали «отрубить» все порты для выхода в интернет. Вирусы, которыми заражен ноутбук представленный ниже:

Работа над проектом. Интересные факты



I love You

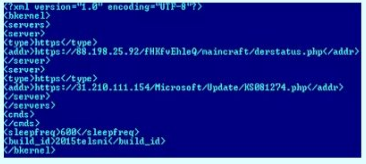
Первым экспонатом кунсткамеры китайского художника стал вирус с романтическим названием ILOVEYOU, также известный как LoveLetter. Вирус был разослан по электронной почте с Филиппин в ночь на 5 мая 2000 года. К письму с заголовком ILoveYou прилагался файл LoveLetter («Любовное послание»). При открытии вирус рассылал копию самого себя всем контактам в адресной книге Microsoft Outlook. Также он перезаписывал личные файлы, включая документы, изображения и аудио. Только в США число атакованных пользователей превысило 2,5 млн. Среди пострадавших оказались парламенты Англии и скандинавских стран, конгресс США, а также Пентагон. За невиданный размах ILOVEYOU даже внесли в Книгу рекордов Гиннесса. На сайте аукциона утверждается, что суммарный ущерб

WannaCry

Прогремевший на весь мир вирус-шифровальщик WannaCry ожидаемо вошел в коллекцию Го О Дуна. Массовая эпидемия началась 12 мая 2017 года. Вирус атаковал компьютеры под управлением Windows, шифровал все файлы пользователя и требовал выкуп в биткоинах за расшифровку. Жертвы вымогателей пополняли биткоин-кошельки в надежде вернуть свои файлы, но чаще всего впустую. Менее чем за неделю были заражены до 300 тыс. компьютеров по меньшей мере в 150 странах, сообщала информационная служба McClatchy со ссылкой на американских экспертов.

Вирус блокировал работу множества организаций и предприятий: больниц, аэропортов, банков, заводов. В частности, вирус поразил серверы национальной системы здравоохранения Великобритании, чем причинил ущерб на €92 млн (около $120 млн), по данным британского министерства здравоохранения и социальной защиты. В ряде британских госпиталей было отложено выполнение назначенных медицинских процедур, обследований и срочных операций. На прием к врачам оказались отменены 19 тыс. записей.

WannaCry до сих пор продолжает периодически заражать компьютеры, хотя уже и в меньших масштабах, отметили в Techcrunch. Согласно данным на сайте аукциона, общий ущерб от действия вируса приблизился к $4 млрд.



BlackEnergy 2

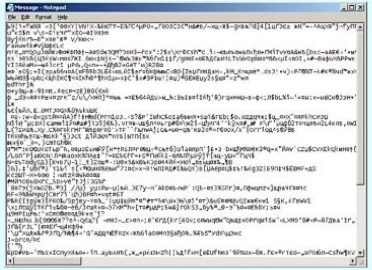
Вирус BlackEnergy 2 создали на базе довольно простого троянца BlackEnergy, который применялся злоумышленниками с 2007 года для проведения DDoS-атак. Однако новая версия была значительно модернизирована и теперь представляет собой набор инструментов для самых разных деструктивных задач. Например, программа может уничтожить жесткий диск, перезаписав всю информацию на нем случайным массивом данных.

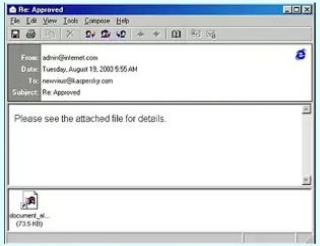
MyDoom

MyDoom («Моя погибель») стал одной из самых разрушительных программ за всю историю вирусописания. Эпидемия началась 26 января 2004 года, когда почтовый червь стал с молниеносной скоростью распространяться по интернету. Антивирусная компания MessageLabs к 4 февраля 2004 года зарегистрировала свыше 21 млн инфицированных писем.

MyDoom удалял некоторые файлы с жесткого диска и организовывал DoS-атаки на разные сайты.

По данным компании mi2g, ущерб от деятельности MyDoom на вторую половину 2 февраля 2004 года оценивался в $39 млрд. Сюда вошли задержки онлайн-платежей, потери пропускной способности сетей, восстановление работоспособности инфицированных систем и т.д.





SoBig

Червь SoBig распространялся через электронную почту как вирусный спам. Днем рождения вируса считается 9 января 2003 года. Чтобы заразиться, пользователь самостоятельно запускал зараженный файл. Вредоносное ПО значительно замедляло работу компьютера и пересылало себя дальше по почте. SoBig затронул сотни тысяч компьютеров и нанес ущерб мировой экономике более чем на $37 млрд.

DarkTequila

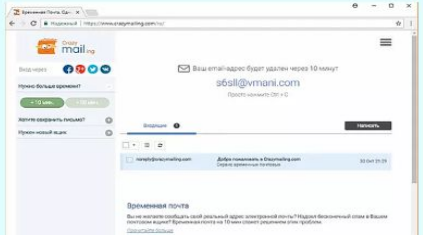
DarkTequila — это сложная и трудноуловимая вредоносная программа, нацеленная главным образом на пользователей в Мексике. Вирус создавался с целью воровать финансовую информацию пользователей, а также логины и пароли для входа на популярные веб-сайты. Вредоносная программа распространяется через письма от мошенников и USB-устройства. По данным «Лаборатории Касперского», вирус активен с 2013 года. DarkTequila нанес убытки на миллионы долларов множеству пользователей.

Работа над проектом. Правила и Заключение

1. Используйте надёжный пароль, состоящий из буква верхнего и нижнего Регистра и содержащий цифры и другие символы. Не используйте пароль, свеянный с темы данными, которые могут быть о Вас известны, например, Ваши имя или дату рождения.

2. Заходите в интернет с компьютера, на котором установлен Файерволл или антивирус с файерволлом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3. Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах, Вы будете указывать его. Это необходимо, если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите никому свой пароль к почте, иначе злоумышленник сможет через Вашу почту получить доступ ко всем сервисам и сайтам, на которых указан ваш



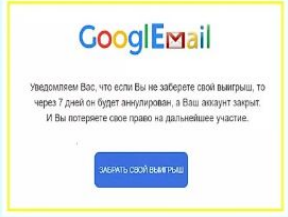
4. Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес свой электронный почты, то скорее всего на Ваш адрес будут высылать рекламу или спам, в таких случаях пользуйтесь одноразовыми почтовыми ящиками.

Сайт для создания одноразового почтового адреса
https://www.crazymailing.com/

5. Скачивайте программы не с подозрительных сайтов или с файлообменников, а с официальных сайтов разработчиков. Так Вы уменьшите риск скачать вирус вместо программы.

6. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были, в лучшем случае Вы поможете автору сайта получить деньги, а в худшем – получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.

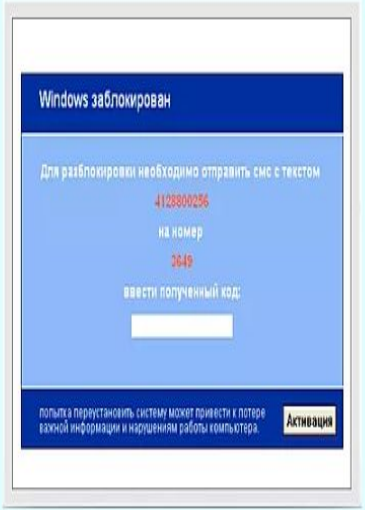
7. Если Вы работаете за компьютером, к которому имеют доступ другие люди (на работе, интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.

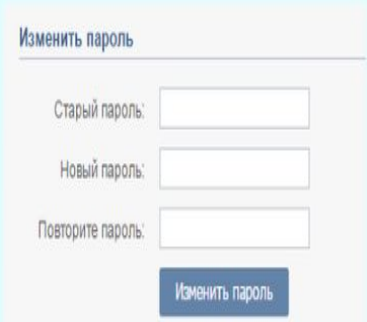


8. Не открывайте письма от неизвестных вам пользователей или письма/ баннеры с оповещением о выигрыше в лотерее, в которой вы просто не участвовали.

Работа над проектом. Правила и Заключение

9. Не нажимайте на всплывающие окна, в которых написано, что Ваша учетная запись социальной сети заблокирована, это проделки злоумышленников. Если Вас вдруг заблокируют, вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит вам электронное письмо





10. Периодически меняйте пароли на самых важных сайтах, так вы уменьшите риск взлома Вашего пароля.

ЗАКЛЮЧЕНИЕ

Территория безопасности сети зависит только от осторожности и бдительности пользователя. Главное – помнить, что какое бы выгодное предложение ни поступало в интернете от незнакомых, а иногда даже и знакомых людей, компьютеры которых могут быть уже заражёнными, всегда нужно проявлять бдительность и осторожность.

Работа над проектом и его достоинства

Во время работы над проектом я узнал для себя полезную информацию по защите себя в сети интернет, которая, надеюсь сможет помочь обезопасить себя и другим пользователям интернета

Из достоинств моего проекта я бы отметил доступность информации и приятный, не напрягающий, легкий дизайн сайта, выполненный в светлых тонах.

Источники

- Габдулина Гульшат Халиковнаю. Безопасность в сети интернет – подробная статья [Электронный ресурс]//FinFocus –16.11.2018. – Режим доступа: https://nsportal.ru/nachalnaya-shkola/materialy-dlya-roditelei/2018/11/16/bezopasnost-v-seti-internet,
- Семенько Татьяна Владимировна. Безопасность в сети интернет [Электронный ресурс]//CyberLenika – 2019. – Режим доступа: https://cyberleninka.ru/article/n/bezopasnost-v-seti-internet, свободный (дата
- Киприот Виктор. Безопасность в сети интернет. Информационная безопасность в интернете [Электронный ресурс]//FB – 2018. Режим доступа: https://fb.ru/article/159338/bezopasnost-v-seti-internet-informatsionnaya-bezopasnost-v-internete, свободный
- Иван Носатов. Источник заразы: шесть самых зловещих вирусов в истории интернета [Электронный ресурс]//IZ.ru - 09.06.2019.- Режим доступа: https://iz.ru/885015/ivan-nosatov/istochnik-zarazy-shest-samykh-zloveshchikh-virusov-v-istorii-interneta