Муниципальное казенное общеобразовательное учреждение средняя общеобразовательная школа №2 с углубленным изучением отдельных предметов ПГТ Восточный Омутнинского района Кировской области.

Киберпреступность и методы борьбы с ней

Работу выполнил обучающийся 9В класса
Русинов.Д.Р
Руководитель проекта Попыванова О.А
Учитель информатики и ИКТ

Содержание

ВВЕДЕНИЕ

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства.

Но человечество, развивая информационные технологии, не предвидело, какие возможности для злоупотребления оно создает своими руками.

Сегодня, жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом, безопасность сотен тысяч людей может оказаться в зависимости от нескольких преступников и одной кнопки.

Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

Если говорить про 2020 год, то он был наполнен событиями, тесно связанными с киберпреступностью. Атаки вирусов-шифровальщиков, утечки хакерских инструментов американских спецслужб, проверка на прочность объектов энергетики. Не все оказались к ним готовы, скорее, наоборот [3].

Объект исследования: киберпреступность

Предмет исследования: виды киберпреступности и способы защиты

Цель работы: изучение материала по киберпреступности и создать памятку – правила «Как защитить себя от киберпреступлений»

Задачи:

1.Определить что такое Киберпреступность;

2.Изучить основные виды Киберпреступности;

3.Выяснить, что люди знают о Киберпреступности;

4.Создать памятку – правила «Как защитить себя от киберпреступлений».

Методы исследования: изучение и анализ литературы, опрос, анализ

результатов

ГЛАВА I. КИБЕРПРЕСТУПНОСТЬ, КЛАССИФИКАЦИЯ ИНТЕНЕТ - УГРОЗ

1.1. Понятие киберпреступности и ее виды

Киберпреступность — преступления, совершаемые в сфере информационных технологий. Преступления в сфере информационных технологий включают распространение вредоносных программ, взлом паролей [7].

Термин «киберпреступность» включает в себя любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети. Преступление, совершенное в киберпространстве — это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация цифровых данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ [5].

Конвенция Совета Европы о киберпреступности говорит, о четырех типах
компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- Незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
- Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
- Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Именно эти четыре вида преступлений являются собственно «компьютерными», остальные — это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера (computer-facilitated) преступления. К ним относятся:

- преступлении, связанные с нарушением авторских и смежных прав;
- действия, где компьютеры используются как орудия преступления (электронные хищения, мошенничества и т.п.);
- преступления, где компьютеры играют роль интеллектуальных средств

(например, размещение в сети Интернет детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.) .

1.2. Примеры и анализ наиболее крупных кибератак

Крупнейшие кибератаки

Сообщения о вирусах-шифровальщиках, атакующих компьютеры по всему миру, появляются на новостных лентах регулярно. И чем дальше, тем большие масштабы принимают кибератаки. Вот — лишь десять из них: самых резонансных и наиболее значимых для истории такого вида преступлений.

Червь Морриса, 1988 год

Сегодня дискета с исходным кодом червя Морриса — музейный экспонат. Взглянуть на неё можно в научном музее американского Бостона. Её бывшим владельцем был аспирант Роберт Таппан Моррис, который создал один из самых первых интернет-червей и привёл его в действие в технологическом институте штата Массачусетс 2 ноября 1988 года. В результате в США были парализованы 6 тыс. интернет-узлов, а общий ущерб

от этого составил 96,5 млн долларов.

Для борьбы с червём привлекли самых лучших специалистов по компьютерной безопасности. Однако и им не удалось вычислить создателя вируса. Моррис сам сдался полиции — по настоянию своего отца, также имевшего отношение к компьютерной индустрии.

Чернобыль, 1998 год

У этого компьютерного вируса есть и пара других названий. Также он известен как «Чих» или CIH. Вирус тайваньского происхождения. В июне 1998 года его разработал местный студент, запрограммировавший начало массовой атаки вируса на персональные компьютеры по всему миру на 26 апреля 1999 года — день очередной годовщины Чернобыльской аварии. Заложенная заранее «бомба» сработала чётко в срок, поразив полмиллиона компьютеров на планете. При этом вредоносной программе удалось совершить доселе невозможное — вывести из строя аппаратную часть компьютеров, поразив микросхему Flash BIOS.

Melissa, 1999 год

Melissa был первым вредоносным кодом, отправленным по электронной почте. В марте 1999 года он парализовал работу серверов крупных компаний, расположенных по всему миру. Это произошло из-за того, что вирус генерировал всё новые и новые инфицированные письма, создавая мощнейшую нагрузку на серверы почты. При этом их работа либо очень сильно замедлялась, либо прекращалась полностью. Ущерб от вируса Melissa для пользователей и компаний оценивался в 80 млн долларов. Кроме того, он стал «родоначальником» нового типа вирусов.

Mafiaboy, 2000 год

Это была одна из самых первых DDoS-атак в мире, которую начал 16-летний канадский школьник. Под удар в феврале 2000-го попали несколько всемирно известных сайтов (от Amazon до Yahoo), в которых хакеру Mafiaboy удалось обнаружить уязвимость. В итоге работа ресурсов была нарушена почти на целую неделю. Ущерб от полномасштабной атаки

оказался весьма серьёзным, его оценивают в 1,2 млрд долларов.

Титановый дождь, 2003 год

Так назвали серию мощных кибератак, от которых в 2003 году пострадали сразу несколько компаний оборонной промышленности и ряд прочих госучреждений США. Целью хакеров было получение доступа к секретной информации. Отследить авторов атак (оказалось, что они — из провинции Гуандун в Китае) удалось специалисту по компьютерной безопасности Шону Карпентеру. Он проделал колоссальную работу, однако вместо лавров победителя в итоге получил неприятности. В ФБР посчитали некорректным методы Шона, ведь в ходе своего расследования он произвёл «незаконный взлом компьютеров за рубежом».

Cabir, 2004 год

До мобильных телефонов вирусы добрались в 2004 году. Тогда появилась программа, которая давала о себе знать надписью «Cabire», высвечивавшейся на экране мобильного устройства при каждом включении. При этом вирус, посредством технологии Bluetooth, пытался заразить и другие мобильные телефоны. И это очень сильно влияло на заряд устройств, его хватало в самом лучшем случае на пару часов.

Кибератака на Эстонию, 2007 год

То, что случилось в апреле 2007 года, можно без особых натяжек назвать первой кибервойной. Тогда в Эстонии разом ушли в офлайн правительственные и финансовые сайты за компанию с медицинскими ресурсами и действующими онлайн-сервисами. Удар оказался весьма ощутимым, ведь в Эстонии к тому моменту уже действовало электронное правительство, а банковские платежи практически полностью были в онлайне. Кибератака парализовала всё государство. Причём произошло это на фоне массовых протестов, проходивших в стране против переноса памятника советским воинам Второй Мировой.

Zeus, 2007 год

Троянская программа начала распространяться в социальных сетях в

2007 году. Первыми пострадали пользователи Facebook, получившие письма с прилагавшимися к ним фотографиями. Попытка открыть фото оборачивалась тем, что пользователь попадал на страницы сайтов, поражённых вирусом ZeuS. При этом вредоносная программа сразу же проникала в систему компьютера, находила личные данные владельца ПК и оперативно снимала средства со счетов человека в европейских банках. Вирусная атака затронула немецких, итальянских и испанских пользователей. Общий ущерб составил 42 мдрд долларов.

Gauss, 2012 год

Этот вирус — банковский троян, крадущий финансовую информацию с поражённых ПК — был создан американскими и израильскими хакерами, работавшими в тандеме. В 2012 году, когда Gauss ударил по банкам Ливии, Израиля и Палестины, его причисляли к кибероружию. Главной задачей кибератаки, как выяснилось позже, была проверка информации о возможной тайной поддержке ливанскими банками террористов.

WannaCry, 2017 год

300 тысяч компьютеров и 150 стран мира — такова статистика по пострадавшим от этого вируса-шифровальщика. В 2017 году в разных концах света он проник в персональные компьютеры с операционной системой Windows (воспользовавшись тем, что они не имели на тот момент ряда необходимых обновлений), перекрыл владельцам доступ к содержимому жёсткого диска, но пообещал вернуть его за плату в 300 долларов. Те, кто отказался платить выкуп, лишились всей захваченной информации. Ущерб от WannaCry оценивается в 1 мдрд долларов. Авторство его до сих пор неизвестно, считается, что к созданию вируса приложили руку разработчики из КНДР [9].

Китайские хакерские чипы взломали оборудование 30 компаний США, 2018

В начале октября Bloomberg опубликовало статью, в которой утверждалось, что китайские хакеры пытались шпионить за американскими

компаниями с помощью микрочипов. По информации источников агентства, шпионские микросхемы внедрялись в материнские платы, предназначавшиеся для серверов, которыми пользовались такие компании, как Apple и Amazon. Источники утверждали, что это происходило на этапе сборки оборудования на фабриках в КНР, являющихся подрядчиками крупнейшего в мире производителя материнских плат Supermicro.

2020

Covid-19 радикально и трагически изменил жизнь во всем мире. Пандемия создала беспрецедентные условия в киберпространстве, заставляя компании перестраивать ИТ-инфраструктуру и открывая новые возможности для хакеров.

Взлом SolarWinds

В начале декабря, американская компания FireEye, специализирующаяся на разработке решений в области сетевой безопасности, сообщила, что пострадала от хакерской атаки.

Злоумышленники проникли во внутреннюю сеть и украли инструменты, которые использовались для пентеста (тестирования на проникновение) сетей клиентов компании.

Сам по себе, взлом FireEye, который быстро приписали российским хакерам, не был катастрофой. В тот день еще никто не подозревал насколько масштабной и беспрецедентной стала эта атака.

13 декабря, разнеслась волна новостей о том, что государственные учреждения США, такие как Министерство торговли, Казначейство, Министерство национальной безопасности, Министерство энергетики, а также крупные международные корпорации стали жертвами массированной шпионской кампании.

Еще в 2019 году злоумышленники взломали производителя ПО SolarWinds и внедрили вредоносный код в программу для мониторинга и управления сетевой инфраструктурой Orion. Данное ПО широко используется как государственными учреждениями, так и множеством

частных организаций по всему миру. Стоит отметить, что Orion используют практически все компании из списка Fortune 500, Госдеп США и администрация президента США.

Таким образом, любой заказчик, установивший патч для Orion, выпущенный в период с марта по июнь, также закладывал бэкдор в свою сеть.

Хакеры, ответственные за кибератаку получили доступ к исходному коду и системам корпорации Microsoft. Компания подтвердила, что загрузила программное обеспечение от своего поставщика SolarWinds

Твиттер

Взлом Твиттер-аккаунтов

В июле 2020 хакеры получили полный доступ к Twitter аккаунтам Джо Байдена, Барака Обамы, Илона Маска, Канье Уэста, Билла Гейтса и Майкла Блумберга, корпоративным аккаунтам Apple и Uber и др. Всего злоумышленники нацелились на 130 аккаунтов и взяли под контроль 45.

Последующее расследование показало, что злоумышленники позвонили в службу поддержки клиентов и техническую службу Twitter. Обманом заставили сотрудников перейти на фишинговый сайт и получили их учетные данные. Затем злоумышленники использовали доступ к учетным записям для сброса паролей на целевыех аккаунтах пользователей.

Garmin

В конце июля хакеры заразили сеть компании Garmin - производителя систем GPS-навигации и умных часов.

Атака поразила Garmin Connect, облачную платформу, которая синхронизировала данные о пользовательской активности, а также часть платформы Garmin.com. Были выведены из строя системы электронной почты компании и колл-центр. Помимо спортсменов, любителей фитнеса и других постоянных клиентов, с перебоями в работе устройств столкнулись и пилоты самолетов, использующие продукты Garmin для определения местоположения, навигации и хронометража. У приложений flyGarmin и

Garmin Pilot были перебои в работе, которые длились днями, что повлияло на некоторые аппаратные средства Garmin, используемые в самолетах (инструменты планирования полетов и авиационные базы данных). Приложение ActiveCaptain, обеспечивающее доступ к морским и сухопутным картам также пострадало из-за атаки.

Взлом больницы Дюссельдорфа

В сентябре была совершена атака на 30 серверов университетской больницы в Дюссельдорфе. В результате инцидента ИТ-системы больницы в т.ч. системы ухода за больными были частично заблокированы. Медицинские учреждения часто становятся жертвами атак программ-вымогателей из-за необходимости быстрого восстановления работы систем в интересах безопасности пациентов.

Тем не менее, инцидент в университетской больнице Дюссельдорфа был особенно значимым, поскольку он может представлять собой первый зафиксированный случай, когда человеческая смерть будет отнесена на счет кибератаки. В результате последствий инцидента больница была вынуждена перенаправить женщину, нуждающуюся в неотложной медицинской помощи, в другое учреждение. Транспортировка привела к часовой задержке в лечении. Женщина не выжила.

Безусловно, о причинно-следственной связи можно спорить, да и количество смертей, причиной которых косвенно могла стать кибератака, в реальности, должно быть гораздо больше.

Утечки персональных данных

Во второй раз за два года компания Marriott обнаружила, что персональные данные примерно 5,2 млн. гостей отеля утекли в сеть. Информация включала в себя имена, адреса, номера телефонов и даты рождения. По некоторой информации отдельные строки слитой базы содержали паспортные данные и номера водительских прав.

Наряду с этим инцидентом можно упомянуть и об утечке персональных данных пользователей Telegram. На базу, содержащую данные

нескольких миллионов пользователей обратил внимание портал "Код Дурова".

Вспомним возможную утечку персональных данных людей, зарегистрированных на электронное голосование по поправкам в Конституцию (представители правительства Москвы утечку отрицают) и утечке персональных данных москвичей, переболевших коронавирусом. Данные содержали Ф.И.О., даты рождения, адреса проживания, телефоны и номера паспортов.

Во втором случае Представители департамента информационных технологий Москвы (ДИТ) заявили, что утечка произошла из-за действий сотрудников, которые допустили передачу данных третьим лицам. Был ли факт передачи информации случайным (отправка файла по незащищенным каналам связи) или сознательным не уточняется [2].

Zoom

Журналист подключился к закрытой видеоконференции министров обороны Евросоюза.

В связи с быстрым увеличением количества людей, работающих на дому, Zoom превратился из малоизвестного сервиса в одну из наиболее широко используемых платформ для видео и аудиоконференций.

Как и следовало ожидать при таком резком взрывном росте, компания Zoom столкнулась с несколькими инцидентами, связанными с безопасностью, в частности, с утечкой примерно 500 000 учетных записей пользователей, которые можно было купить на теневых форумах. Как сообщается, учетные записи были получены с помощью логинов и паролей, которые были скомпрометированы при предыдущих взломах. Таким образом, хакеры могли получить доступ к важной личной или корпоративной информации.

Так, голландский журналист получил доступ к закрытой видеоконференции министров обороны Евросоюза. Он смог подключиться к

звонку после того, как заметил код встречи и пароль на одной из фотографий, опубликованой в Twitter министра оборона Нидерландов.

Криминалисты по всему миру заявляют: преступники уходят в интернет, а банки обчищают не в ходе налётов, а с помощью внедрённых в систему зловредных вирусов. И это сигнал для каждого пользователя: быть аккуратнее со своей личной информацией в сети, надёжнее защищать данные о своих финансовых счетах, не пренебрегать регулярной сменой паролей [1].

Вывод:

Мы живем во время революции кибер-угроз? Кажется, что так. Вредоносные программы становятся все более и более изощренными, а техники атак постоянно совершенствуются. Сейчас цель уже не выбирается случайно: атаки все чаще становятся направленными и скоординированными, использующими различные направления заражения.

Кибернетические атаки могут стать идеальными инструментами следующих войн – они стремительны, эффективны в своей разрушительности и, как правило, анонимны.

ГЛАВА II. КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРПРИСТУПНОСТИ

2.1 Опрос жителей поселка Восточный

Я решил узнать, насколько осведомлены жители моего села в вопросе киберпреступлений.

Мною был проведен небольшой опрос.

Предложены следующие вопросы:

1. Знаете ли вы что такое киберпреступление?
2. Взламывали ли ваши страницы в соц. сетях?
3. Стоит ли сообщать не знакомым людям пароль или номер банковских карт?
4. Совершали ли вы оплату интернет - покупок с помощью банковских карт?
5. Знаете ли вы как защититься от киберпреступлений?

В анкетирование приняли участие 21 человек пгт Восточный.

На первый вопрос были получены следующие результаты: Да-13 человек, Нет- 8.

Можно сделать вывод, что больше половины опрашиваемых знают, что такое киберпреступление.

Рис.1 «Знаете ли Вы что такое киберпреступление?»

На второй вопрос утвердительно ответили 16 человек.

Таким образом, мы можем увидеть, что из 21 случайно опрошенного человека от взлома страниц пострадали наибольшее количество человек.

Рис.2 «Взламывали ли Ваши страницы в соц.сетях?»

На третий вопрос ответ «да» – 0 человек, ответ «нет» - 21 человек. Жители моего поселка понимают, что нельзя сообщать пароли или номера банковских карт незнакомым людям.

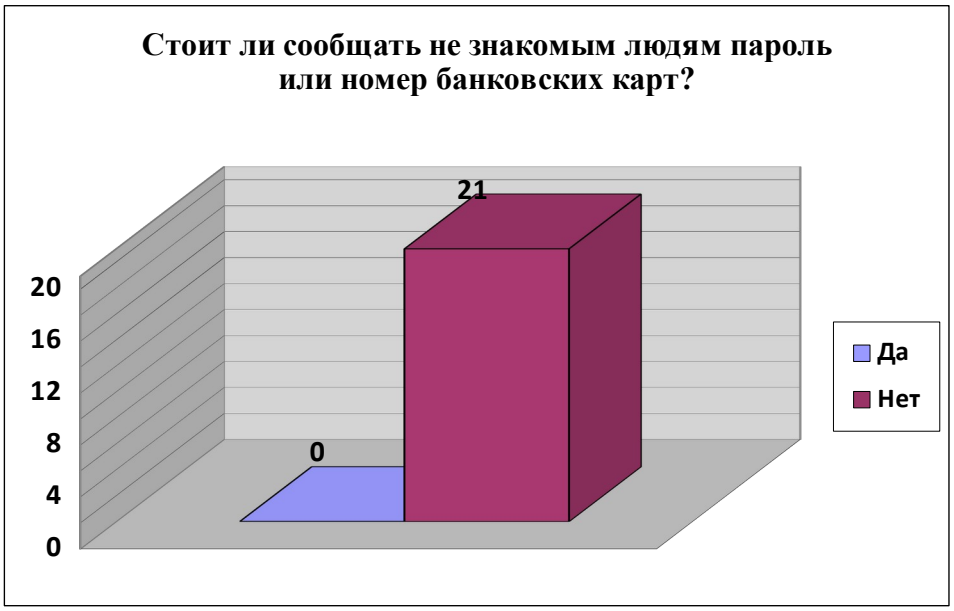

Рис.3 «Стоит ли сообщать не знакомым людям пароль или номер банковских карт?»

На четвертый вопрос «да» - ответили 15 человек, «нет» - 6 человек.

Здесь можно обратить внимание, что большинство опрашиваемых, совершают покупки в Интернете, при этом не задумываются, что вводят

данные, которые не должен знать никто, при этом облегчая жизнь мошенникам, помогая им легко взломать свои банковские счета.

Рис.4 «Совершали ли вы оплату интернет - покупок с помощью банковских карт?»

На последний вопрос ответ «да» я получил от 5 человек, все остальные ответили отрицательно.

Рис.5 «Знаете ли вы как защититься от киберпреступлений?

Проанализировав результаты опроса, можно сделать вывод, что люди знакомы с киберпреступлениями, понимают, что нельзя никому сообщать пароль и номер счета банковских карт, но при этом набольшее количество опрошенных не знают, как защититься от киберпреступлений.

Проведя этот опрос, я еще раз удостоверился, что моя работа актуальна и памятка, которую я хочу создать и распространить в поселке, может помочь многим жителям избежать кибер – угроз.

2.2. Как защитить себя от киберпреступлений

Говоря о Киберпреступности, необходимо понимать, что технический

прогресс играет на руку преступникам. Всего один человек с ноутбуком способен нанести колоссальный ущерб, как большой компании, так и конкретному человеку и с большой долей вероятности остаться безнаказанным. Специалисты по кибербезопасности всегда должны работать на опережение, но хакеры время от времени выигрывают эту битву. Поэтому крайне важно, чтобы пользователи интернета сами повышали собственный уровень безопасности, тем самым повышая его в целом [6].

Для того чтобы обезопасить своих односельчан от Киберпреступлений, я создал памятку, которая содержит в себе следующие правила:

1.Использование антивирусных программ.

2.Использование сложных уникальных паролей для каждой службы.

3.Регулярное обновление программного обеспечения. Используя его уязвимости, преступники легко могут получить доступ к компьютеру.

4.Ограничение личной информации в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона и т.д.

5.Регулярно проводите беседы с детьми о правилах поведения в интернете, особенно в соц. сетях. Ваши дети должны знать о недопустимости любого негативного воздействия на них и необходимости сообщить родителям о подобных инцидентах.

6.Отслеживайте информацию о нарушении безопасности ваших данных на сайтах, на которых вы зарегистрированы, особенно если через эти сайты ведется коммерческая деятельность.

7.Никогда не открывайте письма на электронной почте, если не уверены в отправителе.

8.Не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут.

9.Не подключайтесь к сомнительному WiFi.

10.Не подключайте чужие USB-носители.

11.Не предоставляйте возможность физического доступа к вашим

устройствам. Относитесь к вашим устройствам, как к кошельку с кучей денег, потому что так оно и есть на самом деле – информация стоит дорого.

12.Проверяйте информацию, прежде чем в нее поверить.

13.Проверяйте аккаунт пользователя, прежде чем добавлять его в друзья.

Если вы стали жертвой киберпреступников, вы должны сообщить об этом в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого.

Если каждый будет придерживаться этих советов, то значительно снизится уровень киберприступности.

ЗАКЛЮЧЕНИЕ

Изучив теоретическую и практическую сторону данного вопроса, можно сказать, что с приходом Интернета мы принесли и новую беду 21 века. Люди сами того не сознавая вредят себе, совершая оплату покупок, различных услуг, но при этом даже не задумываются о безопасности.

Я считаю, что актуальность моей работы подтвердилась, и многие люди воспользуются, той информацией, которая представлена в моей работе.

Цель достигнута, все задачи выполнены, создана памятка – правила по данной теме.

Я надеюсь, что, проведя опрос и рассказав о киберпреступлениях, я многим людям помогу избежать кибератак, немного себя обезопасить от мошенников.

СПИСОК ЛИТЕРАТУРЫ

1.Вехов В. Б. Компьютерные преступления: Учебное пособие / Под ред. В. П. Тихомирова, А. В. Хорошилова. - М.: Финансы и статистика, 2006.

2.Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. канд. юрид. наук. - Н. Новгород, 2012.

3.Макклуре С, Скембрэй Дж., Куртц Дж. Секреты хакеров, проблемы и решения сетевой защиты. М.: ЛОРИ, 2016. 435 с.

4.Мельников Защита информации в компьютерных системах / Мельников, Викторович Виталий. - М.: Финансы и статистика; Электроинформ, 2017. - 368 с.

5.Мещеряков Р.В., ШелупановА.А., Белов Е.Б., Лось В.П. Основы информационной безопасности.- М.: Горячая линия-Телеком, 2014. - 350 с.

6.Первин Ю.А. Информатика дома и в школе. Книга для ученика. – СПб.: БХВ – Петербург, 2003. – 352 с.

7.Толков. Слов.: Более 1000 базовых понятий и терминов. – 3-е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. – М.: ООО «Издательство Астрель», 2003. – 272 с.

8.Шаньгин, В.Ф. Защита компьютерной информации / В.Ф. Шаньгин. - М.: ДМК Пресс, 2017. - 544 с

9.Шафрин Ю.А. 1500 основных понятий, терминов и практических советов для пользователей персональным компьютером. – М.: Дрофа, 2001. – 272 с.

ПАМЯТКА

«КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРПРЕСТУПЛЕНИЙ»

1.Использование антивирусных программ.

2.Использование сложных уникальных паролей для каждой службы.

3.Регулярное обновление программного обеспечения. Используя его уязвимости, преступники легко могут получить доступ к компьютеру.

4.Ограничение личной информации в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона и т.д.

5.Регулярно проводите беседы с детьми о правилах поведения в интернете, особенно в соц. сетях. Ваши дети должны знать о недопустимости любого негативного воздействия на них и необходимости сообщить родителям о подобных инцидентах.

6.Отслеживайте информацию о нарушении безопасности ваших данных на сайтах, на которых вы зарегистрированы, особенно если через эти сайты ведется коммерческая деятельность.

7.Никогда не открывайте письма на электронной почте, если не уверены в отправителе.

8.Не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут.

9.Не подключайтесь к сомнительному WiFi.

10.Не подключайте чужие USB-носители.

11.Не предоставляйте возможность физического доступа к вашим устройствам. Относитесь к вашим устройствам, как к кошельку с кучей денег, потому что так оно и есть на самом деле – информация стоит дорого.

12.Проверяйте информацию, прежде чем в нее поверить.

13.Проверяйте аккаунт пользователя, прежде чем добавлять его в друзья.