Содержание

Введение

Выбранная мною тема интересна своей актуальностью. В наше время, в век информации, СМИ и интернета, эта тема как нельзя кстати. Смотря фильмы, сериалы, передачи, мы задались вопросом, а все ли так, как показано на экране? Все ли настолько плохо или настолько хорошо?

Стоит ли бояться киберпреступлений нам - обычным людям? И если да, то как от них уберечься, защититься? Особую актуальность проблема киберпреступности приобрела в наше время. Социологические опросы в разных странах, и в первую очередь в высокоразвитых, показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей. Всё чаще поднимается проблема вопроса киберпреступности.

На сегодняшний день она достигла высокого уровня и продолжает развиваться. Это подтверждает статистика, в которой говорится, что ущерб российской экономике от преступной деятельности хакеров достиг 1,3 трлн рублей. Это результат их атак с 2020 года по июнь 2022 года на банки и интернет-банкинг граждан и предприятий. А что же до нас? Обычных людей, которые пользуются интернетом для общения с друзьями? Все тоже не так просто. Мы уязвимы, у нас есть слабые места, в которые способен залезть умелый хакер.

Так же стоит рассмотреть и такой вариант, что участники кибервойн будут использовать в качестве средства и места ее ведения обычные сети, что неизбежно затронет гражданское население.

Киберпреступность — это преступность в так называемом виртуальном пространстве. Виртуальное пространство, или киберпространство можно определить, как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленныев

математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям. Термин «киберпреступность» включает в себя любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети. Преступление, совершенное в киберпространстве, — это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

Кибербезопасность- это набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

***Актуальность:** 21 век - век информационных технологий. Почти у каждого из нас есть компьютер, телефон, плеер, телевизор. Более 70% процентов населения земли не могут представить свою жизнь без электронных технологий. Сегодня компьютеры используются во всех сферах жизнедеятельности человека – от повседневного быта до государственной безопасности. Быстрое увеличение персональных компьютеров и быстро развивающийся рынок новых электронных устройств изменили и способы проведения досуга, и методы ведения бизнеса.*

Мы храним огромные объемы информации в компьютерах и часто хотим эту информацию скрыть. Сегодня, как никогда ранее, актуальна проблема

защиты личных и конфиденциальных данных. По мере роста развития информационных технологий и развития систем безопасности, растет и количество киберпреступлений. Невозможно создать идеальную систему безопасности. В любой системе есть уязвимость.

Объект исследования: *объектом исследования является киберпреступность, ее виды и особенности, структура и способы борьбы с ней.*

Цели и задачи:

сформулировать понятие киберпреступности;

охарактеризовать основные виды преступления в сфере информационных технологий;

оценить ущерб, наносимый киберпреступностью.

Классификация киберпреступности .

Киберпреступность – это преступления, совершаемые в сфере информационных технологий, так называемом виртуальном пространстве.

- *Можно выделить основные виды киберпрестсупности:*
- *кража паролей,*
- *номеров кредитных карт,*
- *распространение вирусных программ; распространение оскорбляющей и абсурдной информации в сети Интернет.*
- *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);*
- *6.вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных); 7.вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения,*
- *8. удаления, нарушения, изменения либо пресечения компьютерных данных).*

Именно эти четыре вида преступлений являются собственно «компьютерными», остальные — это либо связанные с компьютером, либо совершаемые с помощью компьютера преступления.

Тем не менее, самым распространенным видом преступления, осуществляемым с помощью сети Интернет, является мошенничество. Так, вложение денежных средств на иностранные фондовые рынки через Интернет может привести к тому, что вас могут втянуть в различные мошеннические схемы.

Также еще один вид мошенничества может встретиться на интернет-аукционах, на которых сами продавцы делают ставки для поднятия цены товара.

Еще один вид киберпреступления – это распространение вредоносных компьютерных вирусов. Компьютерные вирусы – это вид программного обеспечения, способного создавать свои копии и внедряться в код другого программного обеспечения. Распространяются вирусы, встраивая свой код в другую программу, для выполнения дальнейших несанкционированных действий. Внедряясь в код других программ, вирусы могут производить различные действия, такие как уничтожение всех файлов и данных, и даже полностью уничтожить операционную систему пользователя. Примером вируса может послужить вирус известный, как LoveLetter , который в 2000 году за несколько часов успешно заразил десятки миллионов компьютеров.

Год за годом быстро растет количество кибератак на сайты инфраструктур и оборонных предприятий. В последние года ООН обеспокоенно увеличением количества кибератак и преступлений в сфере информационных технологий, что свидетельствует переход проблемы киберпреступности на международный уровень (Приложение 1).

Интернет уже не тот, что был 5 – 10 лет назад. Сейчас в интернете больше сервисов, информации и возможностей. Киберпреступники тоже очень быстро развиваются, они становятся умнее, опытнее и профессиональнее. Но лишь сейчас начали уделять особое внимание этой угрозе. Если раньше вопрос о безопасности в Интернете сводился к защите личных данных, то теперь необходимо думать о защите от незаконного проникновения на секретные базы данных и целые компьютерные системы.

Вместе с хакерами начали появляться группы хактивистов – киберперступники (Приложение 2), которые готовы причинить значительный ущерб не только ради денежной выгоды, но и ради идеи.

Пентагон сейчас выделяет группу хактивистов Anonymous, как пример новой серьезной кибер угрозы, направленной против страны. Группа хактивистов Anonymous известна по нападения на сайты госструктур и корпораций. Мощными атаками подвергались не только компьютерные сети правительств разных стран, но и целые корпорации, которые занимаются производством оружия, атомных реакторов. Все это может привести к кибертерроризму или к кибервойнам.

Быстрому росту и развитию киберпреступности способствует сам вид данного преступления, который базируется на открытом доступе в сеть Интернет и безнаказанности преступников, а также слабой подготовкой правоохранительных органов по расследованию такого рода преступлений.

Мошенники, которые распространяют противоправную информацию, не могут использовать обычный Интернет, так как это подвергает их большому риску быть вычисленным и пойманным правоохранительными органами. Они используют так называемый Глубинный интернет.

Глубокая паутина – это множество веб-страниц, которые не индексируются обычными поисковыми системами. Значительной её частью является – Глубинный-веб, иначе именуемый как Deep Web.

Весь доступный простому пользователю, видимый Интернет составляет всего 1-2 % от всех возможных ресурсов. Считается, что этот вид Интернета является максимально анонимным, поэтому там много преступников, террористов, контрабандистов и хакеров. Самое страшное в оборотной его стороне, где Deep Web превращается в Dark Web, в котором не существует ограничений, законов и стран. Там мошенники и террористы занимаются продажей оружия, наркотическими веществами, поддельными паспортами, данными кредитных карт.

Несмотря на то, что немногие люди знают о нем, попасть туда достаточно просто, даже не имея какой-либо специальной подготовки.

Для подключения к сети Tor, которая является одним из самых крупных сегментов сети Deep Web, достаточно установить Tor-браузер.

Deep Web разрабатывался как секретная разработка военно-морскими силами США, но в последствие передан в открытое использование. Tor обеспечивает многослойное шифрование пакетов. Отправка пакетов осуществляется через выбранные случайным образом узлы. Каждый узел узнает только своих соседей в маршруте. Отследить происхождение пакета и раскрыть его содержимое на узле практически невозможно.

Одним из самых известных хакеров является хакер Андриан Ламо по прозвищу «Бездомный хакер». Это прозвище он получил из-за методов своей «работы». Он совершал свои взломы везде, где был Интернет. В список успешно проведенных им атак вошли Microsoft, Citigroup, New York Times, Yahoo, MacDonald's, Bank of America и Cingular. Однажды Андриан продемонстрировал свои способности в прямом эфире на телеканале NBC, под камерами он проник во внутреннюю сеть самой же телекомпании. На данный момент Андриан читает лекции по информационной безопасности.

Владимир Левин – самый известный хакер из России. В далеком 1994 году он взломал Citibank. Вместе со своими помощниками он украл более 10 миллионов долларов, но удалось обналичить всего 400 тысяч долларов. В 1995 в Лондоне в аэропорту полиции удалось арестовать Левина. Ему грозил срок пребывания в тюрьме до 60 лет по американским законам, но по решению суда был приговорен к трем годам лишения свободы.

Виды кибератак.

Trojan

Троянец (троянский вирус или троянская программа)- это тип вредоносных программ, маскирующихся под легитимное ПО. Он часто используется киберпреступниками для кражи личных данных, слежения за пользователями и получения несанкционированного доступа к системам.

Как и в истории с троянским конем из древнегреческой мифологии троянская вредоносная программа появляется в «образе» того, что вы хотите. Она часто маскируется под бесплатное ПО или вложение в электронном письме, а затем, как только вы даете ей разрешение на установку на вашем компьютере, она открывает шлюзы.

Как только у троянца появляется доступ к вашему компьютеру, он может делать что угодно, но большинство этих вредоносных программ стремятся получить полный контроль над вашим компьютером. Иными словами, все ваши действия на компьютере записываются и отправляются на сервер, указанный трояном. Это особенно опасно, если вы на своем компьютере выполняете финансовые транзакции, поскольку троянская программа отправляет информацию о вашей банковской карте или платежных реквизитах людям, которые могут использовать или продать ее.

Троянцы названы так потому, что им требуется ваше разрешение на запуск на вашем компьютере - либо когда вы запускаете программу самостоятельно, либо когда вы открываете документ или изображение, которое затем запускает программу. Исходя из этого, первая и лучшая защита от троянов - никогда не открывать вложение

2.2 Worm

Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях через сетевые ресурсы.

В отличие от Net-Worm для активации Worm пользователю необходимо запустить его.Черви этого типа ищут в сети удаленные компьютеры и копируют себя в каталоги, открытые на чтение и запись (если таковые обнаружены). При этом черви данного типа перебирают доступные сетевые каталоги, используя функции операционной системы, и случайным образом

ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ.

Также к данному типу червей относятся черви, которые по тем или иным причинам не обладают ни одним из других поведений (например, «мобильные» черви).

Одной из крупнейших атак является вирус WannaCry:

Вредоносная программа сканирует диапазон IP-адресов локальной сети и случайно выбранные IP-адреса сети Интернет в поисках компьютеров с открытым TCP-портом 445, который отвечает за обслуживание протокола SMBv1. Обнаружив такой компьютер, программа предпринимает несколько попыток проэксплуатировать на нём уязвимость EternalBlue и, в случае успеха, устанавливает бэкдор DoublePulsar, через который загружается и запускается исполняемый код программы WannaCry. При каждой попытке эксплуатации вредоносная программа проверяет наличие на целевом компьютере DoublePulsar, и в случае обнаружения загружается непосредственно через этот BackDoor.

После заражения компьютера программный код червя шифрует почти все хранящиеся на компьютере файлы и предлагает заплатить денежный выкуп в криптовалюте за их расшифровку. В случае неуплаты выкупа в течение 7 дней с момента заражения возможность расшифровки файлов теряется навсегда.

2.3 BackDoor

Бэкдор, тайный вход (от англ. back door — «чёрный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

Основной целью бэкдора является скрытное и быстрое получение доступа к данным, в большинстве случаев — к зашифрованным и защищённым. Например, бэкдор может быть встроен в алгоритм шифрования для последующей прослушки защищённого канала злоумышленником.

Во-первых, бэкдор — это прежде всего метод, а не конкретная вредоносная программа.

Бэкдоры позволяют творить всё что угодно на инфицированных компьютерах: отправлять и принимать файлы, запускать их или удалять, выводить сообщения, стирать данные, перезагружать систему.

Многие компьютерные черви прошлого (Sobig, Mydoom и другие) устанавливали бэкдоры на заражённые ими компьютеры. Аналогично, многие сегодняшние троянцы обладают такими же функциями.

2.4 Botnet

Botnet -компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании (DoS- и DDoS-атаки). Боты не являются вирусами.

Они представляют собой набор программного обеспечения, который может состоять из вирусов, брандмауэров, программ для удаленного управления компьютером, а также инструментов для скрытия от операционной системы.

В последнее время появляется все больше одноранговых бот-сетей. В ботнете P2P нет централизованного сервера, боты подключены друг к другу и действуют одновременно как сервер и как клиента.

2.5 DDoS-Атаки

Распределенные сетевые атаки часто называются распределёнными атаками типа «отказ в обслуживании» (Distributed Denial of Service, DDoS). Этот тип атаки использует определенные ограничения пропускной способности, которые характерны для любых сетевых ресурсов, например, инфраструктуре, которая обеспечивает условия для работы сайта компании. DDoS-атака отправляет на атакуемый веб-ресурс большое количество запросов с целью превысить способность сайта обрабатывать их все, и вызвать отказ в обслуживании.

Основная цель DDoS-атаки — сделать веб-площадку недоступной для посетителей, заблокировав её работу. Но бывают случаи, когда подобные нападения производятся для того, чтобы отвлечь внимание от других вредных воздействий. DDoS-атака может, например, проводиться при взломе системы безопасности с целью завладеть базой данных организации.

Для отправки очень большого количества запросов на ресурс жертвы киберпреступник часто создает сеть из зараженных компьютеров. Поскольку преступник контролирует действия каждого зараженного компьютера, атака может быть слишком мощной для веб-ресурса жертвы.

Атакующий посылает серверу пакеты, которые не насыщают полосу пропускания (канал обычно довольно широкий), но тратят всё его процессорное время.

Процессор сервера, когда будет их обрабатывать, может не справиться со сложными вычислениями. Из-за этого произойдёт сбой, и пользователи не смогут получить доступ к необходимым ресурсам.

Таким образом, мы видим, что компьютерные преступления бывают разные, и для каждого необходима особая защита.

Фишинг

Фишинг – вид интернет-мошенничества, направленный на получения конфиденциальной информации пользователя – пароля и логина. Фишинг мошенники используют различные психологические приемы для того, чтобы пользователь ввел данные. Основная цель фишинг мошенников – это кража пароля и логина от какого-либо сайта, с дальнейшим использованием, это может быть и номер, и пин-код кредитной карточки, и аккаунт от социальных сетей, либо это может быть логин и пароль от банковского кабинета (Приложение 4). Тем самым фишинг мошенники могу вывести денежные средства с счета жертвы и перевести на свой банковский счет.

Один из видов фишинг-мошенничества — это массовая рассылка от имени какого-либо сервиса или компании. В таких письмах мошенники просят отправить свои личные данные. В таких письмах фишинг-мошенники бывают очень правдоподобны, и доверчивые пользователи отправляют свои данные, не подозревая, что они совершают огромную ошибку.

Второй вид фишинг-мошенничества — это подделка сайта. Обычно подделывается только страница ввода логина и пароля. В этом случае также используется массовая рассылка с просьбой перейти на сайт и ввести данные входа. После того, как пользователь ввел данные, обычно сайт выдает сообщение о неправильности введенных данных.

Слово фишинг пришло из английского языка (fishing) и переводится, как рыбалка. Действительно, этот вид мошенничества очень похож на рыбную ловлю, где в роли рыбака выступает мошенник, а в роли рыбы – обычный пользователь, а наживкой является – письмо (Приложение 5).

В России борьбой с киберпреступностью занимается Управление «К» МВД РФ. Управление «К» - одно из самых засекреченных подразделений МВД РФ, а также входит в Бюро СТМ МВД РФ.

Убытки от киберпреступности

Компания Juniper Research провела исследование и сделала выводы о том, что сохранение текущего уровня киберпреступности приведет к убыткам мировой экономики в 2.1 триллионов долларов. Общемировой ущерб от кибератак вырос в 4 раза. В России ущерб от киберпреступности составляет около двух миллиардов долларов в год.

Ущерб мировой экономики от киберпреступлений растет в геометрической прогрессии. Так, в 2011 году ущерб мировой экономики составил примерно 2.5 миллиардов долларов, а в 2012 году около 18 миллиардов. Экономика США, Китай, Германия страдает в наибольшей степени (Приложение 3).

В последнем году число пострадавших от киберпреступлений составляет около 550 миллионов пользователей сети Интернет, которым старше восемнадцати лет. Это больше чем все население, чем население Европейского союза.

Оборот киберпреступности (388 миллиардов долларов) больше, чем оборот на глобальном черном рынке марихуаны, кокаина и героина вместе взятых (288 миллиардов долларов) и приближается к значению оборота глобального рынка наркотиков (411 миллиард долларов) (Приложение 6).

***Классификация кибербезопасности**:*

Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также

конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.

Проблема кибербезопасности в нашей стране стоит особенно остро во многом из-за слабой нормативно-правовой базы. Фактически, сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.

Кибербезопасность ставит своей целью организацию безопасности киберсреды, системы, в которую могут входить акционеры, относящиеся ко многим общественным и частным организациям, использующим разнообразные компоненты и разные подходы к вопросу безопасности.

Защита от киберпреступности.

Антивирусные программы-специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом. Что нужно учитывать при выборе антивируса

Немецкая лаборатория AV-Test предлагает 3 основных параметра антивируса: защита от угроз, потребляемые ресурсы, ложные срабатывания. Защита от угроз – насколько хорошо антивирус справляется со своей основной задачей, потребляемые ресурсы – сколько он при этом «ест», ложные срабатывания – как часто антивирус принимает нормальные файлы за вирусные.

Начнем с того что на компьютере должны стоять антивирусные программы. Данные программы могут определить потенциальную опасность какого-либо вредоносного приложения, после этого удалит данный файл, и выдаст вам названия файла и тип вируса, который он содержит.

Также они фильтруют трафик в интернете, чтобы вы не попали на фишинговые, потенциально опасные и т.п. сайты.

На данный момент существует много различных антивирусов, большинство которых могут не помочь в случае нахождения вирусного файла. Исходя из этого я составил список 3 лучших антивирусных программ, по моему мнению:

1.Kaspersky Lab.- На данный момент считается одним из самых лучших антивирусных программ, которая защищает от 90% угроз и самая популярная программа в России.

Характеристики (AV-Test):

Комплексная защита от угроз: 6/6.

Экономия ресурсов компьютера: 5.5/6.

Удобство (отсутствие ложных срабатываний): 6/6.

Характеристики (AV-Comparatives, октябрь-декабрь 2021): Один из лучших продуктов в сфере антивирусов.

Оценка пользователей: 4.8/5.

2. ESET NOD32-Антивирусный пакет, выпускаемый словацкой фирмой ESET. Это лучшее решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, фишинг-атаки. В ESET NOD32 используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

Характеристики (AV-Test):

Комплексная защита от угроз: 6/6.

Экономия ресурсов компьютера: 5/6.

Удобство (отсутствие ложных срабатываний): 6/6.

Характеристики (AV-Comparatives, ноябрь-декабрь 2021): Лучший продукт в сфере антивирусов.

Оценка пользователей: 4.5/5.

3. 360 Total Security

Описание: крайне распространенный китайский антивирус. При работе использует сразу несколько движков и вирусных баз, что обеспечивает ему большое «попадание» во вредоносный код. Есть как обычная защита от вредоносных файлов, так и защита от различных интернет-угроз. Дополнительно Total Security предлагает утилиты для очистки кэша, для удаления приватных данных с компьютера, для обновления WIndows и прочие.

Характеристики (AV-Test):

Комплексная защита от угроз: 5.5/6.

Экономия ресурсов компьютера: 5.5/6.

Удобство (отсутствие ложных срабатываний): 6/6.

Характеристики (AV-Comparatives, лето-осень 2021): не участвует.

С какими проблемами сталкиваются пользователи: с тех пор, как из 360 Total Security убрали движки Avira и BitDefender, антивирус стал работать существенно хуже.

Оценка пользователей: 3.34/5.

Далее же могу сказать о элементарных правилах безопасности в интернете и компьютерной сфере:

1.Тщательно контролируйте своё поведение в социальных сетях. Мошенники-виртуозы очень искусны в использовании личной информации, с помощью которой они с лёгкостью могут взломать коды безопасности, и получить доступ к другим учётным записям. За последние несколько лет этот способ кибератаки стал одним из самых распространённых.

2.Не используйте дебетовые карты онлайн. Несанкционированные платежи дебетовой карты изымаются непосредственно с вашего банковского

счёта, и даже если вы немедленно сообщите о нарушении, на восстановление прежнего баланса потребуется не одна неделя. В случае с кредитной картой в аналогичной ситуации при оспаривании подозрительных оплат клиент имеет доступ к своим счетам.

3. Не станьте жертвой Clickjacking. Этот вид атаки таит в себе гиперссылки под тем, что, на первый взгляд, выглядит как безобидный контент. Однако при нажатии ссылки открывается канал для вредоносных программ, которые могут вторгнуться в компьютер или передать вашу личную информацию.

4. Не будьте опрометчивы в использовании любого Wi-Fi соединения. Горячие точки Wi-Fi чаще всего небезопасны, так как не кодируют информацию, передаваемую в интернете. Более того, инструменты, которыми пользуются хакеры, позволяют им «заглянуть» через ваше плечо и выудить имена пользователей, пароли или другую информацию, предоставляющую доступ к финансовым счетам. Сотовая сеть в этом плане более безопасна.

5. В сообщениях электронной почты и на веб-сайте, внимательно смотрите на URL-адреса, даже если они содержат имена авторитетных финансовых учреждений, с которыми вы имеете дело. Самый распространённый подвох – это комбинация имени законного веб-сайта и подделки. Эти адреса очень часто ведут на сайты-подражатели, которые под внешне законным видом скрывают принадлежность к хакерской деятельности. Иногда URL-адрес может оказаться подлинным, но, когда вы нажимаете на ссылку, он переносит вас на другой сайт.

Уголовно-правовые меры по борьбе с киберпреступностью

В УК РФ есть ряд законов, относящиеся к сфере информационных технологий. Все они описаны в главе 28, в статьях 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных компьютерных программ), 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) уголовного кодекса Российской Федерации. Но сфера киберпреступлений настолько обширна, что всего три статьи не могут охватить её всю. Поэтому, здесь есть небольшая особенность и заключается она в том, что в отношении одного гражданина может быть заведено множество уголовных дел.

Главные проблемы преступлений в сфере информационных технологий – это слабая подготовка правоохранительных органов по борьбе с киберпреступностью и расследованию преступлений в сфере информационных технологий, а также высоким уровнем скрытности преступлений в этой сфере. Поэтому, только 15% от общего числа киберпреступлений доходят до правоохранительных органов и становятся известными общественности.

Заключение

Сегодня преступления в сфере информационных технологий стали опасными для общественности. Несмотря на то, что компьютерные преступления появились сравнительно недавно, они быстро развиваются. Слабая подготовка правоохранительных органов по расследованию такого рода преступлений и высокий уровень скрытности преступников, способствует развитию киберпреступлениям и привлекает все больше и больше людей.

Киберпреступность сильно отличается от традиционных видов преступлений. Следовательно, порождает ряд проблем по развитию защитных мер от несанкционированного доступа к компьютерной информации, с дальнейшим её использованием и распространением вирусных программ, которые нарушают работу систем. Преступления в сфере информационных технологий привлекательны большому числу преступников своей невероятной выгодностью и безнаказанностью преступных деяний.

К вопросу о киберпреступности нужно отнестись очень серьезно. Технологии в современном мире не стоят на месте и быстро развиваются, что дает новые возможности для совершения нового рода киберпреступлений. Правительственным органам нужно довольно серьезно заняться решением проблемы киберпреступности, иначе это может привести к необратимым последствиям.

Список использованной литературы

1.https://www.kaspersky.ru/resource-center - Информация об угрозах Касперского

2.Об антивирусных программах сайты https://www.av-test.org

https://ru.wikipedia.org/wiki/ESET_NOD32

3.О киберперступности и кибербезопасности

https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

https://translated.turbopages.org/proxy_u/en-ru.ru.b9ade3ac-622dffe7-1d75bae9-74722d776562/https/en.wikipedia.org/wiki/Cybercrime

4.Киберперступность:http://www.securitylab.ru/news/tags/

5. Википедия. Преступления в сфере информационных технологий: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных технологий.

6.Википедия. Фишинг: https://ru.wikipedia.org/wiki/Фишинг

7. Татьяна Тропина «Киберпреступность и кибертерроризм»: http://www.phreaking.ru/showpage.php?pageid=542335. И. М. РАССОЛОВ «Киберпреступность»: понятие, основные черты, формы проявления>>: http://www.center-bereg.ru/h1529.html

8. Компьютерные вирусы : http://dic.academic.ru/dic.nsf/ruwiki/977057

9. Фишишинговая атака: http://it-web-log.ru/2012/02/fishingovaya-ataka/

10. Deep Web – глубинный интернет. Тёмная материя, обратная сторона Интернета: http://banda-rpt.com/publ/1/1/13-1-0-1718

11. Уголовный кодекс РФ: http://www.zakonrf.info/uk/gl28/

12. Управление <<К>>: https://ru.wikipedia.org/wiki/Управление_«К»

13. Убытки от киберпреступности: http://www.rg.ru/2013/10/16/spam.html

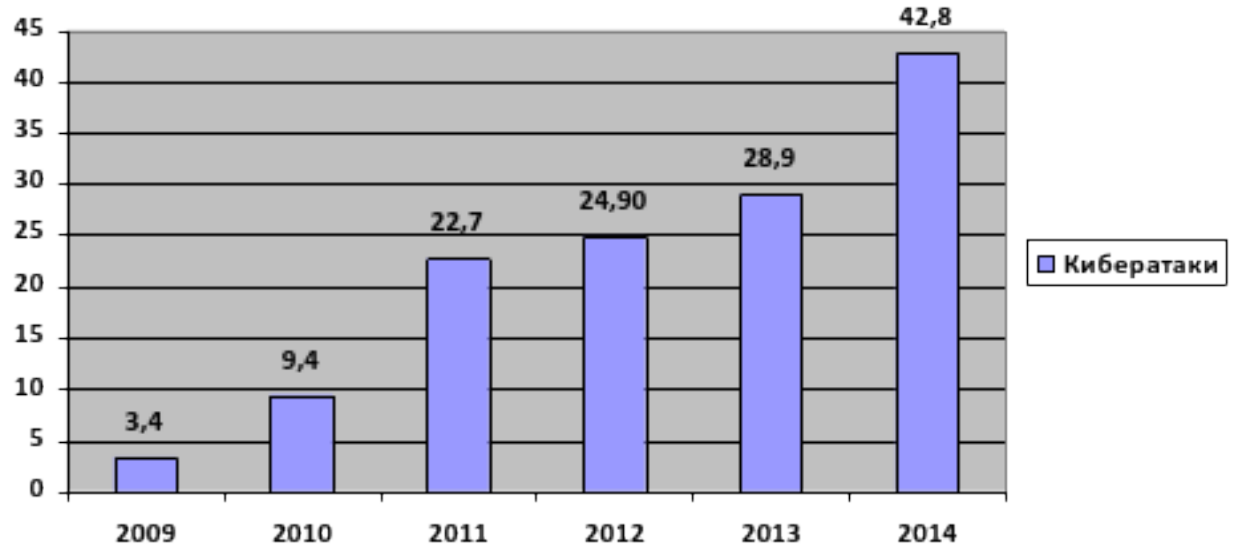
14. Norton Cybercrime Report: http://us.norton.com/cybercrimer

15. Телекоммуникационные технологии: http://book.itep.ru

Приложения

Приложение 1

Количество кибератак на сайты инфраструктур, 2009-2014 гг.

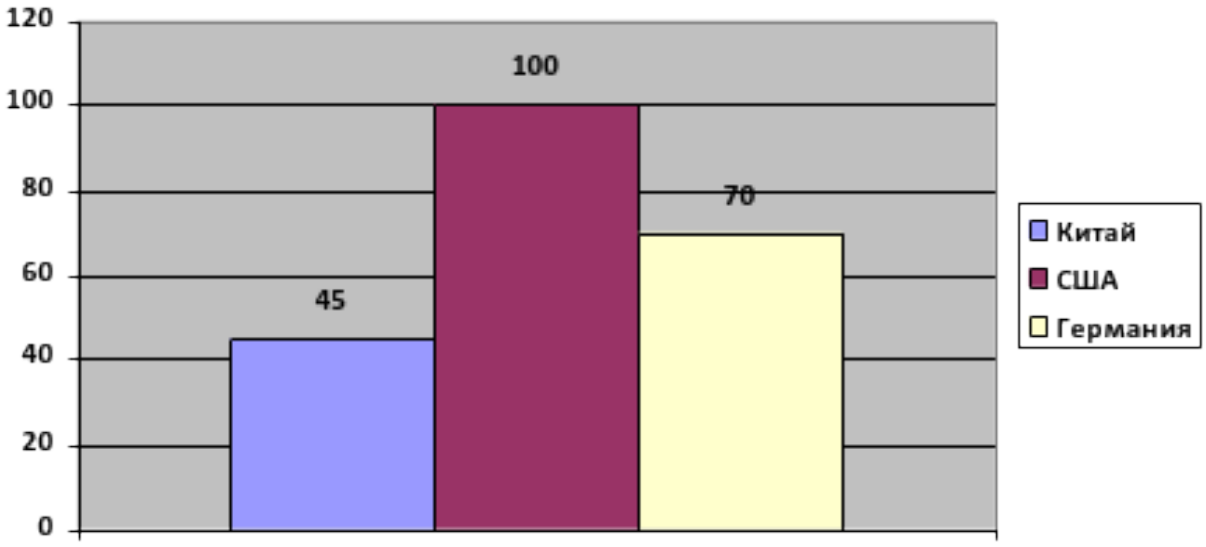


Приложение 2

Хактивизм , по мнению специалистов - это синтез социальной активности и хакерства (соединения двух слов «Hack» и «Activism»). В 2011 году известные группы хакеров заявили о своей поддержки народных протестов в различных странах, именную себя «хактивистами». Общепринятого определения понятию «хактивизм» не существует и по сей день. Хактивисты с одной стороны – это активисты различный политических движений, осваивающие методы киберборьбы, а с другой стороны – это уже состоявшиеся хакеры, которые присоединяются к социальным движениям.

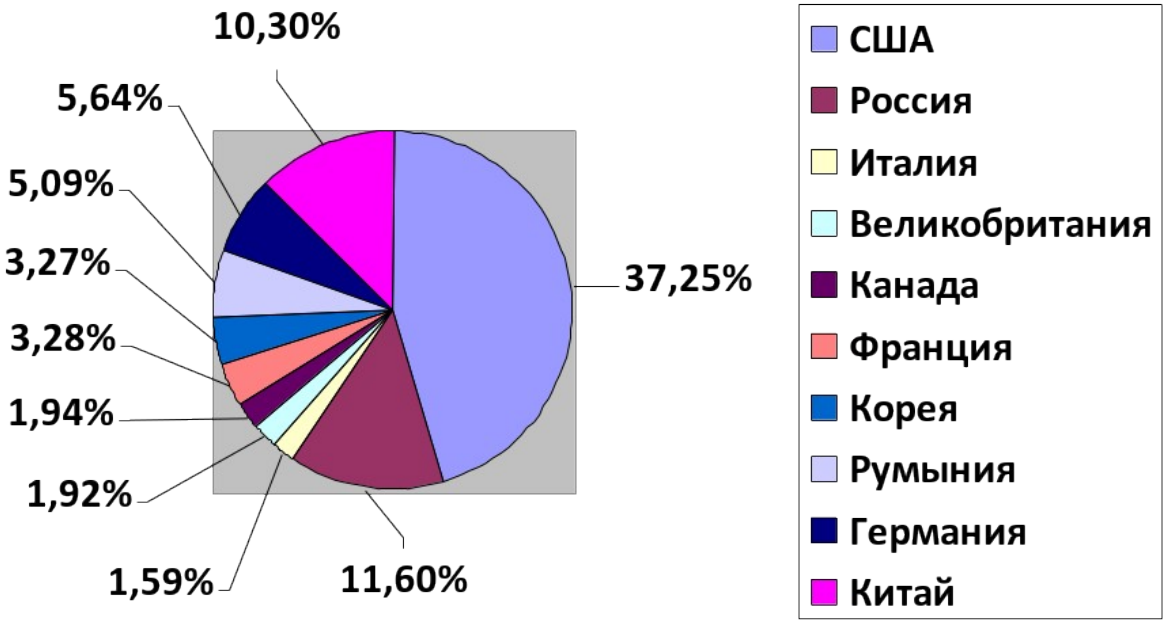
Приложение 3

США, Китай, Германия – страны чья экономика страдает в наибольшей степени (млрд. $).



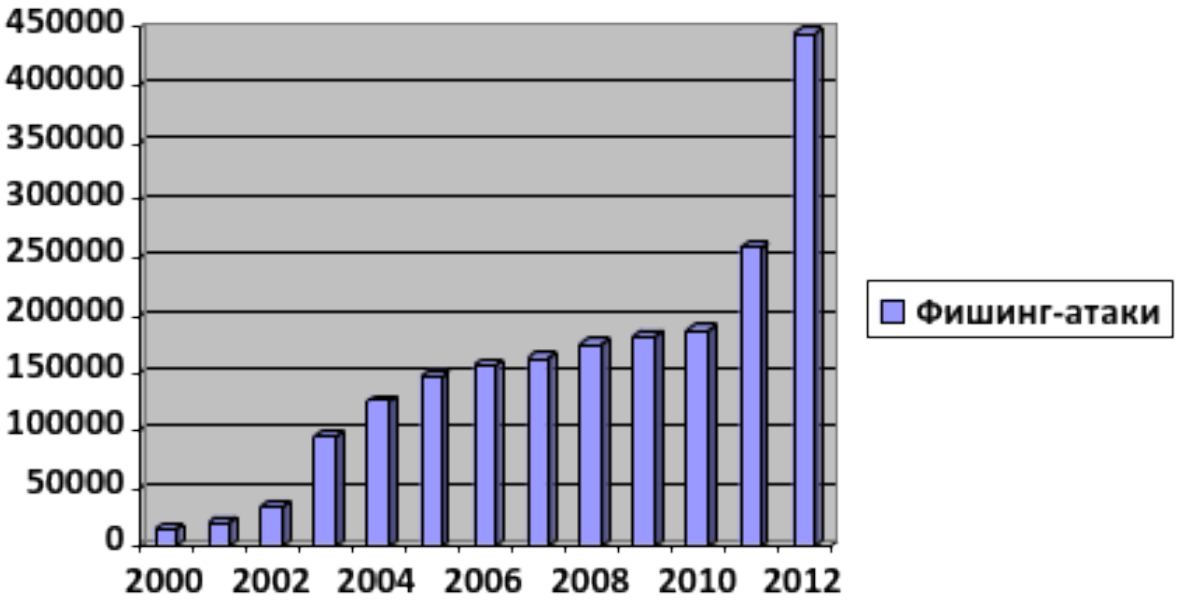
Приложение 4

10 стран по количеству фишинг-атак.



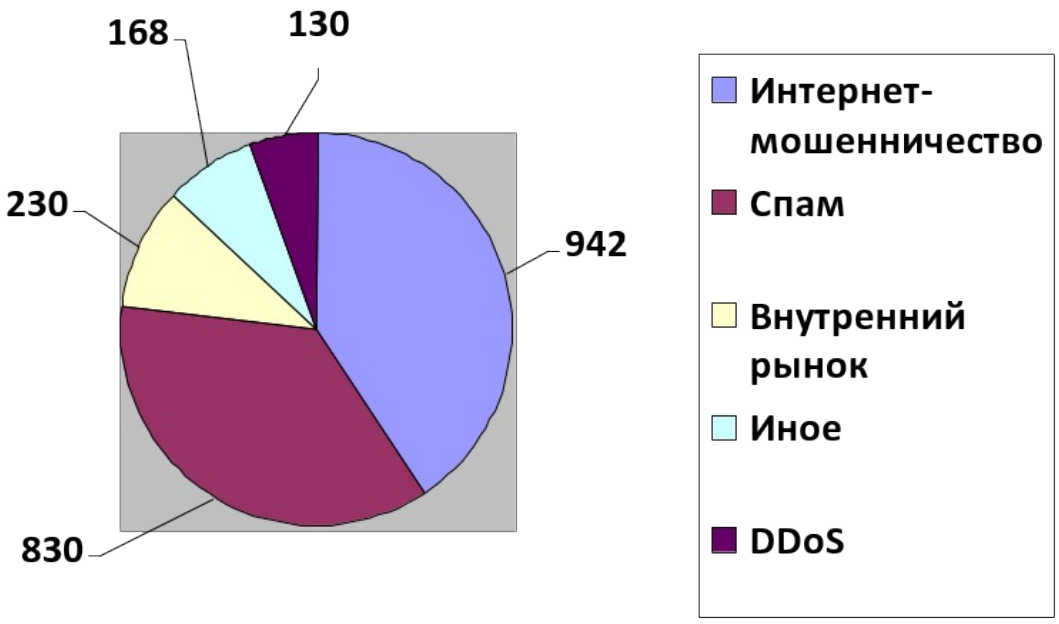
Приложение 5

Развитие фишинга в России и США, 2000-2012 гг.



Приложение 6

Ущерб от киберпреступлений в России (млн. $)


168
130
230
942
830
Интернет-мошенничество
Спам
Внутренний рынок
Иное
DDoS