ПРОЕКТ

на тему
«КИБЕРПРЕСТУПНОСТЬ»
предмет «Информатика»

Содержание

Введение

Актуальность: мы живем в 21 веке, в 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.

Что такое киберпреступность?

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.

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.

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).

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.

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).

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.

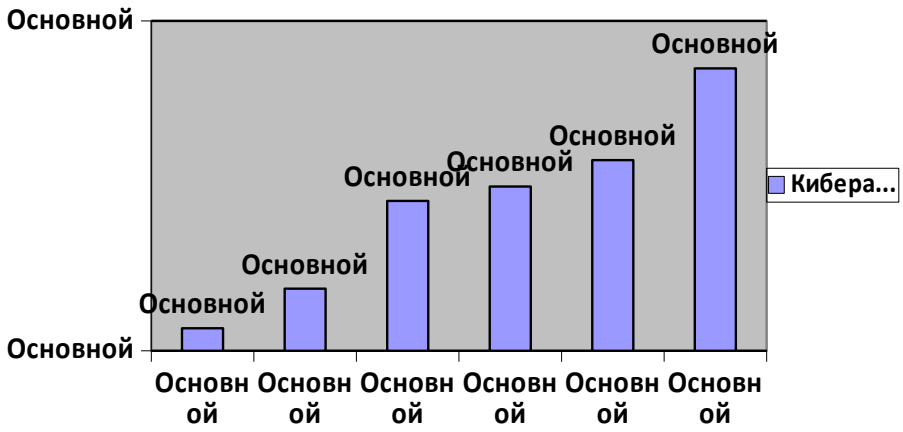
Список использованной литературы

1.Киберперступность: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%EF%F0%E5%F1%F2%F3%EF%ED%EE%F1%F2%FC/
2. Википедия. Преступления в сфере информационных технологий: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий
3.Википедия. Фишинг: https://ru.wikipedia.org/wiki/Фишинг
4. 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
6. Компьютерные вирусы : http://dic.academic.ru/dic.nsf/ruwiki/977057
7. Фишишнговая атака: http://it-web-log.ru/2012/02/fishingovaya-ataka/
8. Deep Web – глубинный интернет. Тёмная материя, обратная сторона Интернета: http://banda-rpt.com/publ/1/1/13-1-0-1718
9. Уголовный кодекс РФ: http://www.zakonrf.info/uk/gl28/
10. Управление <<К>>: https://ru.wikipedia.org/wiki/Управление_«К»
11. Убытки от киберпреступности: http://www.rg.ru/2013/10/16/spam.html
12. Norton Cybercrime Report: http://us.norton.com/cybercrimer
13. Телекоммуникационны технологии: http://book.itep.ru

Приложение

Приложение 1

Количество кибератак на сайты инфраструктур, 2009-2014 гг.

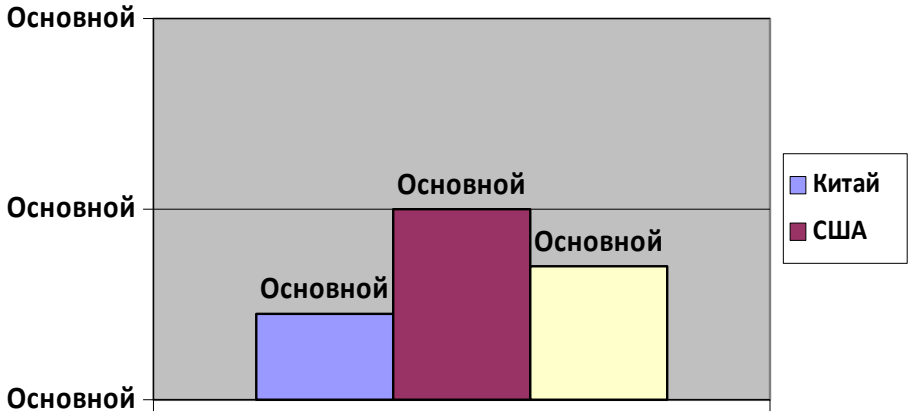


Приложение 2

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.

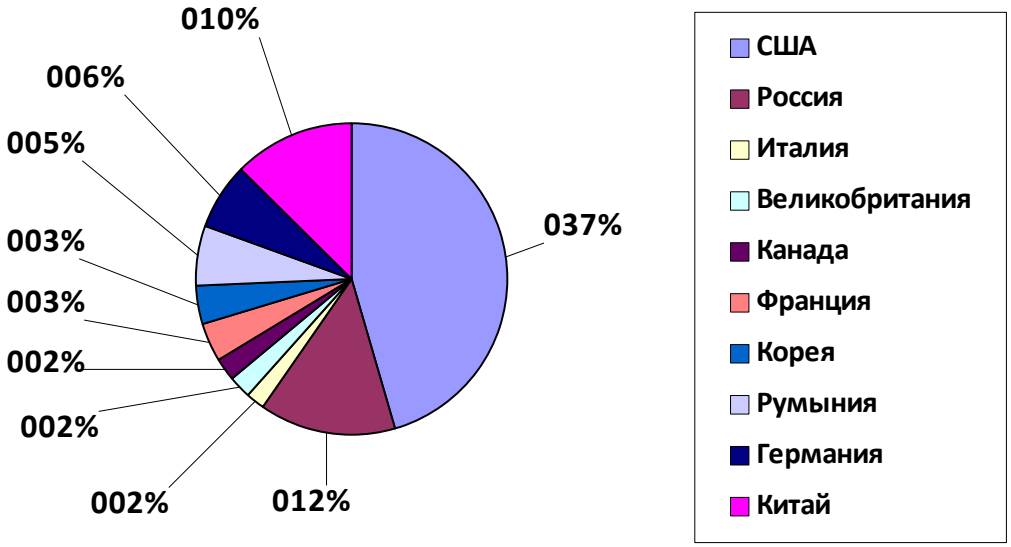
Приложение 3

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



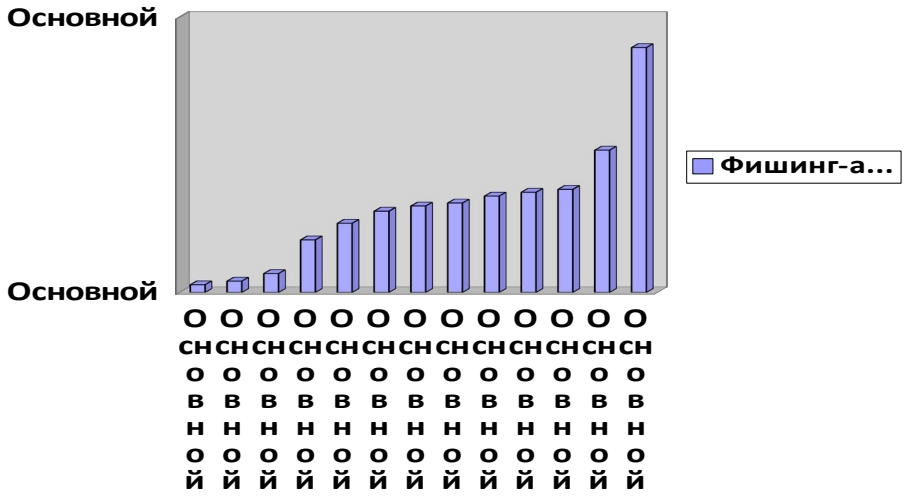
Приложение 4

10 стран по количеству фишинг-атак.



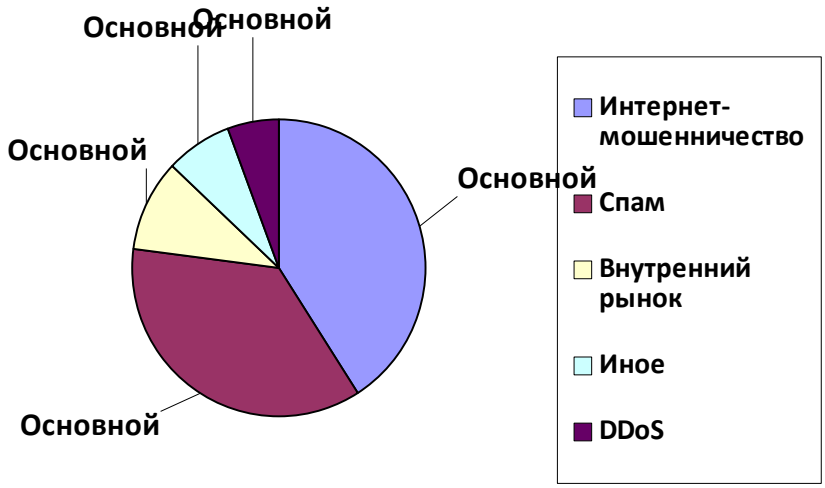
Приложение 5

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



Приложение 6

Ущерб от киберпреступлений в России (млн. $)


Основной
Основной
Основной
Основной
Основной
Интернет-мошенничество
Спам
Внутренний рынок
Иное
DDoS