Государственное общеобразовательное казенное учреждение

Амурской области «Общеобразовательная школа

при учреждениях исполнения наказания»

ИНДИВИДУАЛЬНЫЙ ПРОЕКТ

Киберпреступность и методы борьбы с ней

Автор: Середа Кирилл Владимирович,

обучающийся 11« Б» класса \_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись

Руководитель: Руцынская Наталья Викторовна,

учитель информатики

с. Среднебелая, 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3 - 4

1 ПОНЯТИЕ КИБЕРПРЕСТУПНОСТИ 5

1.1 КТО ТАКИЕ КИБЕРПРЕСТУПНИКИ? 6

1.2 РАЗНОВИДНОСТИ КИБЕРПРЕСТУПЛЕНИЯ 7 - 8

1.3 ПРИМЕРЫ КИБЕРПРЕСТУПЛЕНИЙ 9 - 10

2 БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ 11 - 12

ЗАКЛЮЧЕНИЕ 13

СПИСОК ЛИТЕРАТУРЫ 14

ВВЕДЕНИЕ

Мы живем в XXI веке, который еще называют веком информационных технологий. Мир и жизнь каждого человека изменись с появлением информационных технологий, жизнь человека стала легче. Сегодня за человека много работы выполняют машины, нас повсюду окружает электроника.

Современное информационное общество подвержено ряду потенциальных угроз, одной из которых является киберпреступность.

Во все времена частная жизнь человека защищалась от проникновения посторонних. В информационном обществе защита личного пространства значительно усложнилась. Технологии и средства дают возможность превратить закрытую систему в прозрачную.

В массивных источниках формируются базы данных, содержащие персональную информацию, это обстоятельство представляет угрозу нарушения частой жизни.

Сегодня одной из престижных и востребованных специальностей является профессия «Специалист по компьютерной кибербезопасности», так как любая компания является потенциальной жертвой кибератак. Чем дороже компания, тем выше риск. А значит тем больше денег готовы тратить руководители компаний на специалиста по кибербезопасности.

Уважающая себя компания не жалеет денег и ресурсов на защиту данных. Согласно статистике за последний год бюджеты на кибербезопасность в российских организациях выросли на 20 %.

С каждым годом число кибератак увеличивается, а злоумышленники совершенствуют вредоносное ПО. Компаниям срочно нужны специалисты, которые смогут оперативно искать уязвимости и предотвращать утечки данных.

Хакеры могут легко получить доступ к конфиденциальным данным банков, важных предприятий или любого другого бизнеса. Чтобы защититься от преступников, компании активно ищут специалистов по компьютерной кибербезопасности.

Особую актуальность проблема киберпреступности приобрела в наше время.

Стоит ли бояться киберпреступлений обычным людям? И если да, то как от них уберечься и защититься?

**Цели** работы: исследовать киберпреступность, изучить профилактику киберпреступности и способы борьбы с ней.

**Задачи** работы:

* сформулировать понятие киберпреступности;
* изучить основные виды киберпреступности;
* узнать, кто такие киберпреступники;
* выявить способы профилактики киберпреступности и способы борьбы с ней;
* определить методы обеспечения защиты от киберпреступности для себя и своих близких.

**Объект** исследования: киберпреступность, ее виды и особенности.

**Методы** исследования:

* изучение научно-популярной литературы по данной проблеме;
* анализ и синтез полученной информации;
* анализ правовой базы и статистических данных;
* систематизация и обобщение, выводы по проблемному вопросу.

**Гипотеза**: киберпреступность может перерасти в более глобальную проблему и нанести огромный вред современному обществу.

1 ПОНЯТИЕ КИБЕРПРЕСТУПЛЕНИЯ

Что же такое киберпреступность? Киберпреступность: глобальная проблема человечества?

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство.

Киберпреступность - это преступность в виртуальном пространстве.

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.

Киберпреступность - это следствие всеобъемлющей цифровизации современного общества, свободный доступ к сети Интернет и быстро развивающийся рынок новых коммуникационных устройств привлекает к виртуальному общению как молодежь, так и людей старшего поколения. Киберпреступность посягает на совершенно разные сферы жизни и общества - имущественные права граждан, объекты критической инфраструктуры, права личности, причиняют ущерб коммерческим организациям и государству в целом.

Социологические опросы показывают, что киберпреступность занимает четвертое место в мире по частоте совершения и является проблемой, которая тревожит людей сегодня.

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.

1.1 КТО ТАКИЕ КИБЕРПРЕСТУПНИКИ?

Киберпреступники - это злоумышленники, скрыть свою личность, которые взламывают информационные системы (компьютеры, серверы, сайты, программы и т.д.) для прекращения ее работы, вымогательства, кражи данных, с целью личной мести, материальной или другой выгоды, а также по идеологическим и политическим соображениям.

С каждым днем действия киберпреступников становятся все более агрессивными, они принимают меры к тщательному сокрытию следов, сохранению анонимности, продумывают свое поведение так, чтобы максимально осложнить сбор доказательств и избежать ответственности. Эти обстоятельства предопределяют правовую и фактическую сложность доказывания по таким делам.

Одна из главных проблем расследования киберпреступлений связана с невозможностью точного применения к ним стандартного алгоритма расследования. Киберпреступления совершаются в так называемом «виртуальном пространстве».

Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя - из личных или политических мотивов.

# Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации) определяется и предусмотрена Главой 28 Уголовного кодекса Российской Федерации (статья 272, 273, 274 ч.1 и 274 ч.2) сроком от семи до десяти лет лишения свободы.

1.2 РАЗНОВИДНОСТИ КИБЕРПРЕСТУПЛЕНИЯ

В ходе исследования я выделил несколько основных видов киберпреступлений. Среди них:

* Фишинг;
* Похищение цифровой личности;
* Спам;
* Инсайдинг;
* Хакерство;
* Телекоммуникационные преступления.

Фишинг - это интернет-мошенничество, когда всеми возможными правдами и неправдами у вас пытаются узнать различные персональные данные (пароли, логины, номера банковских карт и счетов).

Смысл заключается в том, чтобы побудить вас перейти по фишинговый ссылке на поддельную страницу, визуально похожую на настоящую, например, банка, где под различными предлогами пытаются выудить персональную информацию.

Похищение цифровой личности - неправомерное завладение профилем в социальной сети, с целью рассылки спама (использования личных данных), шантажа, выманивания денежных средств. С этим видом преступления сталкивались многие из нас.

Спам - нежелательные рекламные объявления и сообщения, предназначенные для распространения рекламных объявлений или вредоносных программ. Они доставляют пользователю неудобства и опасность так как авторы спама имеют множество средств для получения новых адресов электронной почты и способов нелегальной рассылки сообщений.

Инсайдинг. Инсайдер (освобожденный сотрудник компании) является потенциальным преступником. Он знает тонкости компьютерной системы компании, имеет неограниченный доступ к ним с целью незаконного вмешательства в работу автоматизированных ЭВМ и компьютерных сетей. С целью незаконного завладения информацией (собственностью компании).

Хакерство. Хакер - квалифицированный IT-специалист, который понимает самые глубины работы компьютерных систем.

Сначала хакерами называли программистов, которые исправляли ошибки в программном обеспечении быстрым и не профессиональным способом.

Однако, большинство людей считают, что хакер - компьютерный взломщик, проникающий в закрытые информационные сети, банки данных с целью получения доступа к секретной информации, а также заражения их вирусами.

Телекоммуникационные преступления - преступления, совершаемые через СМИ и средства связи.

Наиболее известным из них является атака с целью перегрузить оборудование жертвы и помешать его нормально использовать (DDOS-атака)

Председатель правительства Российской Федерации Дмитрий Анатольевич Медведев заявил, что угроза киберпреступности носит транснациональный характер, а потери от хакерских атак на банки оцениваются в глобальных масштабах.

Среди основных видов киберпреступности выделяют:

* распространение вредоносных программ и вирусов;
* взлом паролей,
* кражу номеров кредитных карт и других банковских реквизитов;
* распространение противоправной информации (клеветы, порнографических материалов) через интернет;
* преступления, связанные с нарушением авторского права и смежных прав.

1.3 ПРИМЕРЫ КИБЕРПРЕСТУПЛЕНИЙ

Редакция журнала «Информационная безопасность/Information Security» публикует результаты отчета компании Symantec – NORTON REPORT 2013 (ранее известныи как Norton Cybercrime Report) - это одно из крупнейших в мире исследований киберпреступности в потребительском сегменте. Цель исследования - понять, какое влияние киберпреступность, а также развитие и внедрение новых технологий оказывают на пользователя и его безопасность. Исследование было проведено международной компанией Edelman Berland.

Чаще всего страдают от киберпреступлений:

* пользователи публичных/незащищенных сетеи Wi-Fi - 68 %;
* развивающиеся рынки - 68 %;
* молодые люди - 66 % (в России 85 %);
* родители детей (в возрасте от 8 до 17 лет) - 65 %;
* мужчины - 64 % (в России 88 % , женщин - 58 %);
* представители старшего поколения - 64 %;
* владельцы мобильных устройств - 63 %;
* пользователи социальных сетей - 63 %.

Страны, где больше всего жертв киберпреступлений среди пользователей:

* Россия – 85 %;
* Китай - 77 %;
* Южная Африка – 73 %;
* Мексика, ОАЭ – 71 %;
* Новая Зеландия – 69 %;
* Канада – 68 %;
* Индия – 65 %;
* Колумбия – 64 %;
* Турция, США – 63 %;
* Саудовская Аравия – 62 %;
* Сингапур – 61 %;
* Австралия, Бразилия и Польша – 60 %;
* Объединенное Королевство – 58 %,
* Италия и Швеция – 56 %;
* Германия – 53 %;
* Дания и Нидерланды – 50 %;
* Франция – 45 %;
* Япония – 19%.

Масштабы киберпреступности в потребительском секторе:

* 378 млн. жертв в год, что почти в 2,8 раза выше ежегодного показателя рождаемости;
* Более 1 млн. жертв в день, достаточно для того, чтобы 10 раз заполнить стадион Уэмбли (Англия);
* 12 жертв в секунду;
* 50 % интернет-пользователей старше 18 лет за последний год становились жертвами киберпреступлений или неприятных ситуации в сети Интернет;
* 41% интернет-пользователей старше 18 лет становились жертвами вредоносных программ, хакерского взлома, мошенничества или кражи.

Информационно-коммуникационные технологии используются для содействия в совершении «*груминга*» в отношении детей.

«*Груминг*» детей – это процесс установления взаимопонимания и доверия через развитие эмоциональных отношений с жертвой.

Как отмечается в публикации Whittle at al. (2013), «*процесс «груминга*» варьирует в значительных пределах с точки зрения стиля, продолжительности и интенсивности, что зачастую зависит от личных качеств и поведения преступника».

2 БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ

В настоящее время борьба с киберпреступностью – довольно распространенное явление, ведь кибератаки занимают четвертое место в мире по частоте совершения.

Конечно, спецслужбы не в состоянии полностью контролировать киберпреступность и в связи с этим, число киберпреступлений растет день за днем.

В 2022 году число кибератак в Россиивыросло в три раза, тем самым увеличилось за год на 21 % и достигло 911 тысяч.

Выросло число кибератак на ИТ-компании через шпионское ПО. За год количество зафиксированных атак на государственный сектор составило 403 атаки. По данным МИД РФ: Число кибератак на Россию выросло на 80 %.

# Законодательство РФ предусматривает уголовную ответственность за совершение киберпреступлений (Глава 28 УК РФ (статья 272 - 274) лишением свободы сроком от одного до десяти лет и штрафом в размере от 100 тысяч до 500 тысяч рублей.

# В последние годы, преступления на просторах сети Интернет становятся все более изощренными, исполнители которых хорошо скрываются и поймать их является задачей сложной.

В РФ существует специальный отдел «К», который занимается ловлей киберпреступников, осуществляет борьбу с компьютерными преступлениями и нелегальным оборотом РЭС (радиотехнических средств).

Также хотелось бы сказать об основных правилах компьютерной безопасности:

* не посещайте сайты, если вы не уверены в их благонадежности и отсутствии на них вирусов;
* старайтесь использовать сложные пароли и не храните их на компьютере;
* регулярно делайте резервное копирование данных;
* обновляйте систему и устаревший браузер;
* не устанавливайте программы из непроверенных источников;
* установите качественное антивирусное программное обеспечение, которое регулярно обновляется и др.
* Не открывать писем от незнакомых пользователей.

Ущерб мировой экономики от киберпреступлений растет в геометрической прогрессии.  Экономика США, Китая и Германии страдает в наибольшей степени.

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).

Основная цель киберпреступников – интернет-банки. Количество атак на них, по данным правоохранительных органов, – растет стремительно, прирост от 80 до 200 процентов ежегодно.

Интернет-преступления удобны: можно украсть миллион, не вставая с кресла. Границы не важны – опять же сидя на своем диване вы в состоянии совершить преступление одновременно в ста странах. Современные законы не успевают за действиями хакеров, в итоге те часто уходят от возмездия.

ЗАКЛЮЧЕНИЕ

Киберпреступность является следствием глобализации информационных процессов и появления глобальных информационных сетей. Особенно киберпреступность проявляется в странах, которые перешли на новую - инновационную ступень развития. В настоящее время человек использует информационные технологии в самых различных сферах своей деятельности, и вместе с этим растет и их использование в целях совершения преступлений.

Компьютерная атака способна полностью парализовать информационную инфраструктуру государства и вызвать социальную, финансовую или экологическую катастрофу.

Например, 15 февраля 2015 года «Лаборатория Касперского», Европол и Интерпол раскрыли киберпреступную операцию, которая продолжалось два года и затронуло около 100 финансовых организаций по всему миру в ходе которой хакеры похитили 1 млрд долларов.

В декабре 2016 года Центробанк РФ сообщил, что за год киберпреступники похитили 2 млрд рублей со счетов российских банков. Одной из крупнейших стала кража 200 млн рублей у столичного Металлинвестбанка.

Таким образом, можно считать, что поставленные цели достигнуты. Мы узнали много нового, интересного и полезного. Полученные знания пригодятся в жизни.

О безопасности надо думать сегодня, завтра уже может быть поздно.

СПИСОК ЛИТЕРАТУРЫ

1. Киберпреступность - что это такое (<https://ru-act.com/ugolovnyj-kodeks/chto-takoe-kiberprestupnost.html>)

Образовательный портал <https://obrazovanie-gid.ru/pereskazy1/opasnosti-informacionnogo-obschestva-kratko.html>

2. Киберпреступность как вид преступления в сфере компьютерной информации (<https://active-region.ru/drugoe/kiberprestupnost-kak-vid-prestuplenija-v-sfere-kompjuternoj-informacii-sposoby-borby-i-zashhity.html>)

3. Первый элитный блог «Нет Ничего Невозможного» (<http://berichnow.ru/stati/21-vek-vek-informatsionnyih-tehnologiy-chto-v-nem-osobennogo>)

4. Студенческий научный форум - 2020

(<https://scienceforum.ru/2020/article/2018020683>)

5. КонсультантПлюс Уголовный Кодекс Российской Федерации (<https://www.consultant.ru/document/cons_doc_LAW_10699/>)

6. Харб (<https://habr.com/ru/companies/digitalrightscenter/articles/688502/>)