Муниципальное автономное общеобразовательное учреждение муниципального образования город Краснодар средняя общеобразовательная школа 74 имени Виктора Васильченко

Тема: «Киберпреступность и как её избежать»

Выполнил:
Гиза Даниил Александрович
обучающийся 9А класса
МАОУ СОШ «Школа №74
Учитель информатики
Войтехович Т.А

г. Краснодар
2022-2023 учебный год

Содержание

Введение

Сначала мы разберём что такое всё-таки киберпреступность и откуда она появилась. Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Родиной термина «киберпреступность» считается США, где в 1960 - х годах подобное словосочетание впервые появилось в СМИ в связи с выявлением первых преступлений.

Актуальность

Выбранная мной тема интересна своей актуальностью. В наше время, в век информации эта тема как нельзя кстати. Все ли настолько плохо. Стоит ли бояться киберпреступлений нам - обычным людям? И если да, то как от них уберечься, защититься? Еще Александр Суворов говорил «Предупрежден значит вооружен». Особую актуальность проблема киберпреступности приобрела в наше время. Социологические опросы знакомых, и в первую очередь показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей.

Цель

1. Исследовать киберпреступность как угрозы обществу.
2. Узнать какие существуют способы борьбы с киберпреступностью.
3. Рассказать о киберпреступности и какие совершали киберпреступления в мире
4. А также ущерб после киберпреступностью.

Задачи проекта

1. Изучить понятие киберпреступность поподробней и её виды
2. Узнать кто такие киберпреступники
3. Найти примеры киберпреступлений в мире
4. И подсказать как избежать кибератак

1. Основная часть

1.1. Понятие киберпреступности и ее виды.

Киберпреступность — преступления, совершаются в сфере информационных технологий. Преступления в сфере информационных технологий включают распространение вредоносных программ, взлом паролей. 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 вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, модификация цифровых данных, а также иные противоправные обществу опасные действия, совершенные с помощью компьютеров, компьютерных сетей и программ. Совет Европы о киберпреступности говорит, о четырех типах компьютерных преступлений определяя их как преступления против целостности и доступности компьютерных данных и систем:

Киберпреступник это лицо, которое осуществляет какую-либо незаконную деятельность с использованием компьютеров или других цифровых технологий, таких как Интернет. Преступник может использовать компьютерные знания, знания о человеческом поведении и различные инструменты и услуги для достижения своей цели.

1.2 Виды киберпреступности.

1. Незаконный доступ — (противоправный умышленный доступ к компьютерной системе либо ее части)
2. Вмешательство в данные — (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных)
3. Вмешательство в систему — (серьезное препятствие функционалу компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).
4. Незаконный перехват — (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

Именно эти четыре вида и считаются основными

1.3. Совершенные в мире киберпреступления

1. Кевин Митник признан одним из самых неуловимых киберпреступников в Соединенных Штатах Америки. В 80-е годы редко можно было встретить компанию, в систему которой не проникал Митник. На его счету взлом данных Novell, Motorola, Sun Microsystems, NASA и других корпораций. Громче всего имя хакера прозвучало в 1983 году, когда ему удалось получить доступ к компьютеру Пентагона. За содеянное мужчину многократно арестовывали, однако ему удавалось выходить «сухим из воды» до тех пор, пока за него не взялось ФБР. Тогда Кевин вынужден был «залечь на дно». Однако серьезное наказание не заставило себя долго ждать — в середине 90-х Митник получил серьезный срок за свои преступления. В этом ему помог хакер по имени Цутом Шимомура, который стал одной из жертв Кевина Митника. Обиженный Шимомура сделал все для того, чтобы помочь правоохранителям наказать оппонента по всей строгости закона.

2. Свои первые хакерские атаки Джулиан Ассанж, действующий под ником Mendax, совершил еще в 16 лет. В течение четырех лет он взломал системы огромного числа организаций и корпораций. Среди них NASA, Пентагон, Lockheed Martin, Стэндфордский университет. В 2006 году он разработал и запустил платформу под названием WikiLeaks. На сервисе публиковались секретные данные, которая была получена либо из анонимных источников, либо в результате утечки информации. Позже Ассандж был обвинен в шпионаже.

3. Одна из самых известных атак Ламо пришлась на 2002 год, когда он попал во внутреннюю сеть The New York Times, назвавшись обозревателем. Также известно, что хакер взламывал сети корпораций Yahoo и Microsoft. В 2004 году Андриан Ламо признался в содеянном и получил наказание в виде шести месяцев домашнего ареста. Общемировую известность киберпреступник получил после ареста военнослужащего армии США Брэдли Мэннинга, который сотрудничал с Wikileaks. Мэннинг рассказал Ламо, что передал в Wikileaks некоторые секретные материалы. После этого Андриан поделился этой информацией с властями Штатов. Последние годы перед своей смертью киберпреступник работал частным аналитиком по безопасности. 37-летний Ламо скончался в 2018 году.

4. Вернёмся в далёкий 1983 год и вспомним о первой кибератаке в истории СССР. Выпускник МГУ Мурат Уртембаев, которого руководство завода «АвтоВАЗ» обделило почётной грамотой, решил отомстить работодателю и внёс изменения в код программы, управляющей подачей деталей на конвейер. В результате автозавод встал на три дня, что

привело к многомиллионным потерям. Уртембаев не выдержал угрызений совести и пришёл к начальству с повинной. За такие преступления в Советском Союзе не было предусмотрено наказания, поэтому Мурата осудили на полтора года условно по статье «за хулиганство» и оштрафовали на стоимость двух «Жигулей». Этот человек вошёл в историю, как первый русский хакер. По крайней мере, первый, которого удалось поймать.

5. Одним из самых неуловимых хакеров по сей день считается россиянин Евгений «lucky12345» Богачёв. Он создал группировку киберпреступников, куда входили граждане России, Украины и Великобритании. В общей сложности злоумышленникам удалось украсть у американских граждан и компаний более 100 миллионов долларов (реальная сумма наверняка гораздо больше). Свои преступления Евгений и его приспешники проворачивали с помощью вируса Zeus, заражающего тысячи компьютеров. Богачёва также обвиняют во вмешательстве в американские выборы 2016 года. Несмотря на то, что за любую информацию о местонахождении хакера ФБР объявила награду в 3 миллиона долларов, Богачёв по сей день продолжает успешно скрываться от правосудия.

2. Практическая часть

2.1 Ущерб после кибератак.

Когда бизнес подвергается кибератаке, наносится вполне очевидный и непосредственный ущерб. Чувствительная, конфиденциальная информация компрометируется. В среднем прямые убытки вследствие подобной утечки данных для предприятия со штатом свыше 1000 сотрудников составляют 551 000 руб. Хотя одной этой цифры достаточно, чтобы как минимум занервничать, есть ещё дополнительные расходы; вы можете и не задумываться о них, но они способны подорвать репутацию вашего бизнеса на довольно продолжительный период. Данные аспекты помогут обрисовать чёткую картину того, почему предприятиям нужен надёжный и эффективный план ИТ-безопасности. Атака зачастую останавливает непрерывность бизнеса, что приводит к длительным периодам простоя сотрудников, пока компания пытается оправиться от удара. По подсчётам, пострадавшие предприятия испытывали 23 часа простоя в среднем, вследствие чего средние потери составляли 1,4 млн. руб. Компании, пострадавшие от кибератак, также несут репутационный ущерб, что может привести к потерям, связанным с нежеланием клиентов пользоваться их продуктами или услугами. По подсчётам, издержки от ущерба бренду компании в 7,5 раза больше прямых затрат, связанных с восстановлением после взлома. Клиентам нужна уверенность в том, что предприятия защищены, и многие не желают доверять компании, которая, по их мнению, не справляется с обеспечением безопасности. Многие убеждены в том, что угроза кибератак снижается, но это совсем далеко от истины. Исследования показали, что количество инцидентов с безопасностью совокупно увеличивается на 66% в год. По подсчётам, к 2020 году 30% из мирового списка 2000 компаний подвергнется непосредственной угрозе со стороны независимой группы кибератвистов или злоумышленников. Исследования показали, что средние общие финансовые потери от инцидентов с безопасностью на предприятиях достигают 3,4 млн. руб. Эти цифры ясно дают понять, что кибер атака любого вида может оказать разрушительное действие на бизнес, и наличие плана по обеспечению ИТ-безопасности становится важным больше, чем когда-либо.

2.2 Как избежать кибератак.

В XXI веке почти у каждого в кармане есть устройство с выходом в интернет. Более того, количество личной информации, которую мы храним на смартфонах, планшетах и

ноутбуках колоссально. Значительная ее часть является лакомым кусочком для различных мошенников. «TechInsider» рассказывает, как существенно снизить свои шансы стать мишенью для атаки киберпреступников. Перед подключением к Wi-Fi сети в каком-либо заведении, не выбирайте ее наугад, обратитесь к сотрудникам и уточните имя (SSID). Мошенники могут разместить фальшивую сеть, которая похожа или вовсе имеет идентичное название. Лучше отключить поиск Wi-Fi сетей в фоновом режиме, а также все возможные сервисы обмена известными сетями с другими устройствами. Существуют способы узнать, какие точки доступа ищет ваш телефон и «подсунуть» ему требуемые.

Идеальным вариантов будет установить VPN-клиент и подключиться либо к собственному серверу, либо к надежному платному. В этом случае вообще все соединения с вашего устройства будут идти по зашифрованному туннелю и перехватить их будет невозможно. Бесплатными VPN-сервисами пользоваться менее безопасно, так как чаще всего они зарабатывают на анализе трафика для рекламодателей. Современные программы невероятно сложны и постоянно совершенствуются. В приложениях постоянно обнаруживаются потенциальные уязвимости и ошибки, а задача разработчиков — оперативно их исправлять. В свою очередь, хакеры непрерывно ищут узкие места в программном обеспечении и создают механизмы атаки на них. С каждым новым обновлением наши любимые мессенджеры, социальные сети и банковские клиенты становятся не только функциональнее, но и безопаснее. Регулярное обновление ПО — залог сохранности ваших персональных данных и финансов. Даже риск ухудшения работоспособности или неприятного изменения дизайна не стоит «угнанного» аккаунта в соцсети либо потери всех средств на счете. Аналогично работают и создатели операционных систем. Например, чтобы проверить актуальность подсистемы безопасности ОС Android, нужно зайти в настройки и найти пункт «О телефоне» или аналогичный. В нем должен быть подпункт «версии ПО», где присутствует строка вида «патч безопасности». Если он старше трех месяцев — стоит проверить обновления системы или обратиться к производителю. В крайнем случае, подобное устаревание операционной системы является серьезным поводом заменить гаджет, особенно когда он является основным телефоном и на нем установлены банковские приложения.

Любопытство — не порок, но способно навредить. Новое письмо или сообщение в мессенджере, сопровождающееся интригующим текстом? Заманчивый диалог с привлекательным человеком, заканчивающийся предложением перейти в «более приятное

место в сети»? А как насчет посмотреть девятый сезон «Игры престолов» онлайн, бесплатно, без регистрации и СМС? Лучше не делать этого, правда. Такие ссылки могут вести на сайт с вредоносным кодом, который атакует уязвимости в браузере. Или загрузит на устройство файл, который тоже захочется посмотреть, а в итоге получить «трояна».

Простой пароль, да еще и одинаковый для нескольких аккаунтов — просто мечта для любого киберпреступника. К сожалению, статистика показывает, что из года в год ситуация не улучшается и люди, прекрасно понимая все риски, продолжают использовать «QWERTY» или «ЙЦУКЕН». В большинстве случаев, мошенникам даже не приходится прибегать к сложным алгоритмам подбора: достаточно перебрать словарь типовых паролей. Придумывая учетные данные для своего аккаунта, стоит придерживаться следующих критериев: • Длина — не менее 10 символов, лучше больше 12 • Состав — прописные и строчные буквы, цифры, специальные символы • Срок — лучше менять пароль не реже чем раз в кварт

Как следует из предыдущего пункта, внимательность способна спасти от множества проблем. Не стоит бездумно доверять красиво и профессионально выглядящим сайтам свои персональные данные. Даже если формально ресурс не является мошенническим, он может на абсолютно законных основаниях передавать информацию о вас третьим лицам. Изучите пользовательское соглашение, договор оферты на предоставляемые услуги, а также все данные о юридическом лице, которое владеет веб-страницей. Если этих документов на сайте нет либо в них содержится информация о том, что ваши данные будут использованы в коммерческих целях, лучше уйти с этого ресурса. Предоставив такому сервису сведения о себе, вы, в лучшем случае, подпишетесь на рекламную рассылку или получите навязчивые звонки на телефон, а в худшем — даже можете потерять деньги.

2.3 Способы борьбы с киберпреступностью

Илья Сачков, президент компании Group-IB занимающейся расследованием компьютерных преступлений, утверждает – если вы знаете правила технической самозащиты, вы будете в безопасности. Компания уже десять лет разрабатывает специальные памятки, в которых рассказывает, что делать, чтобы не воспользовались вашей информацией. Но распространение в обществе этих знаний идет чрезвычайно медленно.

Памятка

1. К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

2. Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

3. Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код

4. Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

6. Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

7. Не переходите необдуманно по ссылкам, содержащимся в спамрассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

8. Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

9. Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

10. Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

11. 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 стал одним из самых распространенных.

12. Остерегайтесь сообщений подобного рода: «Внимание! Ваш аккаунт был взломан. Вы должны позвонить, чтобы подтвердить свой аккаунт. Отправьте нам сообщение, и мы перезвоним Вам».

13. 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.

14. 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.

15. 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.

16. Никогда не кликайте на сообщения, присланные на электронную почту и предлагающие обновить персональные данные. В большинстве случаев такие запросы инициируются после того, как вы входите в свой аккаунт не через электронный адрес.

17. Не используйте одинаковый пароль для разных учётных записей. Выбирайте для паролей необычные символы, цифры и пробелы. В качестве дополнительной меры предосторожности, заполните вопросы безопасности вымышленными, простыми для запоминания ответами, а не фактами, которые могли бы раскрыть ваши личные данные.

18. Установите на компьютер антивирусное и антишпионское программное обеспечение. Убедитесь, что эти программы работают и обновляются автоматически. Данный свод правил я оформил наглядно в виде рекламного буклета, для того, чтобы распространить среди населения станицы. В дальнейшем в мои планы входит распространение данного буклета среди жителей других населенных пунктов с разрешения и с помощью администрации города.

Заключение.

Хотел бы подвести итоги что мы узнали за сегодня, что же такое киберприступность, какие виды есть киберприступности, а также как её избежать и защищаться, и что для этого надо сделать, также мы узнали одни из самых крупных киберприступников разных поколей и стран и сколько они причинили вреда всему миру

Киберпреступность сегодня составляет значительно более серьезную опасность, чем 5 лет назад, в связи с использованием преступниками новейших информационных технологий, а также через растущую уязвимость современного индустриального общества.

Невзирая на усилия государств, которые направлены на борьбу с киберпреступниками, их количество в мире не уменьшается, а, напротив, постоянно растет.

Ни одно государство сегодня не способно противостоять этому злу самостоятельно.

Необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

Список литературы:

http://elcomrevue.ru/kibeoprestupnost-chto-eto/

https://infourok.ru/issledovatelskaya-rabota-po-teme-kiberprestupnost3249489

https://www.miloserdie.ru/article/11-pravil-setevoj-gigieny-kak-zashhititsya-otkiberprestupnosti/

https://www.osp.ru/news/2014/1015/13026164/

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

Приложение №1 Увеличение ущерба после кибератак

Приложение №2 Таблица Памятка

№ п/п	Способ защиты
1	В банке выпустить доп. карту
2	Проверка банковских счетов
3	Тайна ПИН кода
4	Виртуальные карты
5	Лимиты
6	Почта с вирусами
7	Спам рассылки
8	Безопасность личных данных
9	Почта с разными адресатами
10	Насторожённость от немедленных действий
11	Поведение с соц. сетях
12	Взлом аакаунта
13	Clickjacking
14	Wi-Fi соединения
15	URL-адреса
16	Сообщение об обновлении персональных данных
17	Одинаковый пароль
18	Антивирусная защита компьютера