УДК 004.49

Современные киберпреступления и основы кибербезопасности

А. В. Гром, К. Н. Ефименко
Донецкий национальный технический университет
grom.anastasiya@inbox.ru, KN_Efimenko@mail.ru

Гром А. В., Ефименко К. Н. Современные киберпреступления и основы кибербезопасности. *Рассмотрены основные виды компьютерных преступлений, вредоносных программ и способы мошенничества в сети Internet, а также даны рекомендации по общим принципам защиты от киберпреступлений.*

Ключевые слова: *компьютерные преступления, вредоносные программы, Internet-мошенничество, безопасность.*

Введение

Ежедневно по всему миру все большее количество компьютеров подвергается вирусной атаке. Так 27 июня 2017г. от атаки компьютерного вируса-шифровальщика Petya.A пострадали десятки компаний в РФ и на Украине. 24 октября 2017г. атаке криптовируса-вымогателя Bad Rabbit (англ. «плохой кролик») подверглись компьютеры в РФ, на Украине, в Турции и Германии. И наконец, 3 ноября этого года вирус WCry – сокращение от английского Wanna Cry (англ. «Хочется плакать») проник в сети МВД, МЧС, РЖД, Сбербанка, «Мегафона» России. За 24 часа заражению подверглись 45 тысяч систем в 74 странах. Именно такие вредоносные программы и их массовое распространение заставляет все чаще задумываться о кибербезопасности.

Актуальность изучения вопроса компьютерных преступлений

Стремительный рост научно-технического прогресса является одним из аспектов, влияющих на значительную трансформацию преступности. Компьютерные технологии используются практически во всех сферах жизнедеятельности человека, начиная от контроля над пассажирской транспортной системой и заканчивая решением вопросов национальной безопасности. Распространение компьютерных сетей привело к всеобщему использованию электронной почты, как наиболее удобному средству связи и обмена информацией. Все большую популярность набирает размещение социальной информации, предназначенной для использования большого количества пользователей, в глобальной сети на специализированных сайтах органов управления, ведомств и министерств.

Данные изменения в распространении информации можно отметить как положительные, упрощающие и модернизирующие жизнь современного общества, аспекты. Но вместе с тем не стоит забывать о том, к каким негативным последствиям это может привести. Разработка большого количества разнопланового программного обеспечения, рост производства и совершенствование вычислительных машин, повсеместное использование компьютерной информации разного рода значимости на просторах Интернета, приводят к совершенствованию «традиционных» видов преступных действий (хищение денежных средств и информации разного назначения, подделка документов и ценных бумаг и т.д.) и способствуют созданию новых разновидностей преступлений (компьютерное мошенничество, несанкционированное использование информации и др.).

Целью данной работы является изучение вопросов компьютерных преступлений, выявление общих и особых характеристик разного рода преступлений, совершающихся с использованием компьютерной техники и выбор наиболее действенных способов защиты от вторжения компьютерных преступников.

Характеристики компьютерных преступлений и вредоносных программ

Изучением проблемы компьютерных преступлений в криминалистической науке занимались многие исследователи, например, Н. П. Яблоков, И. Ф. Герасимов, Г. Г. Зуйков, И. Ф. Пантелеев и др. Обзор научной литературы, судебной и следственной практики позволяет сделать вывод, что на данный момент разработаны только частные методики расследования некоторых видов преступлений данной категории, а конкретно методика раскрытия преступлений в сфере компьютерной информации еще не получила достаточного освещения в юридической литературе. Большинство уголовных дел по компьютерным преступлениям остаются нераскрытыми. К сожалению, при высоком техническом оснащении и тщательной подготовке

преступления, поймать киберпреступника очень сложно. Тем не менее, возможно.

Компьютерные преступления – это предусмотренные уголовным законодательством общественно опасные действия, в которых объектом или средством преступного посягательства является машинная информация. Другими словами, в качестве предмета или орудия такого преступления выступает машинная информация, компьютер, компьютерная система или сеть.

Зарубежный и российский опыт свидетельствует о том, что субъекты компьютерных преступлений различаются как по уровню их профессиональной подготовки, так и по социальному положению. «Компьютерных» преступников можно разделить на несколько групп.

Первая группа – нарушители правил пользования ЭВМ. Они совершают преступления из-за недостаточно хорошего знания техники, желания ознакомиться с интересующей их информацией, похитить какую-либо программу или бесплатно пользоваться услугами ЭВМ.

Ко второй группе относят лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности, так называемых «хакеров» или «одержимых программистов». Они воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам, что служит побуждающим фактором для совершения противоправных действий. Характерной особенностью этой группы является отсутствие у преступников четко выраженных намерений получить материальную выгоду. Практически все действия совершаются ими с целью проявления, подтверждения и доказательства своих способностей.

Третьих иногда называют «информационными путешественниками». Они специализируются на проникновении в чужие компьютеры и сети.

Четвертые – создатели троянских программ и компьютерных вирусов. Впрочем, их уже нельзя назвать хакерами, так как: неформальный «кодекс» хакеров запрещает использование своих знаний во вред пользователям. Эту группу составляют профессиональные «компьютерные» преступники, которые совершают противоправные деяния с ярко выраженными корыстными целями. Эти преступники характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на сокрытие преступлений. Они обычно являются членами хорошо организованных и технически оснащенных первоклассным оборудованием преступных групп и сообществ. Чаще всего, это высококвалифицированные специалисты, имеющие высшее техническое, юридическое или экономическое (финансовое) образование. Их целью является получение стратегически важных данных о противнике в экономической, технической и других областях. На долю этих преступников приходится максимальное число совершенных особо опасных посягательств (до 79 % хищений денежных средств в крупных и особо крупных размерах и различного рода должностных преступлений, совершенных с использованием средств компьютерной техники) [1].

Выделяют пять наиболее распространенных мотивов совершения компьютерных преступлений:

1. Корыстные соображения;
2. Политические цели (шпионаж; преступления, направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений);
3. Исследовательский интерес (студенты и профессиональные программисты);
4. Хулиганские побуждения и озорство (хакеры);
5. Месть.

Условно компьютерные преступления можно разделить на две категории [2]:

1. Преступления, связанные с вмешательством в работу компьютера;
2. Преступления, использующие компьютер как необходимое техническое средство.

Каждая из них связана с несанкционированным доступом к сетям, серверам, машинным ресурсам. Однако, первая категория включает те преступления, в рамках которых вмешательство в работу компьютеров, направлено на повреждение или уничтожение информации, нарушение нормального их функционирования. Наиболее яркий пример – вирусы. В преступлениях второй категории, компьютер выступает не объектом посягательства, но его средством, а целью является получение и использование информации, в том числе, и для совершения иных преступных деяний. Например, хищений денежных средств с банковских счетов. Необходимо отметить, что во многих случаях одно нарушение может иметь признаки преступлений, относящихся к обеим категориям [3].

Компьютерные преступления можно разделить на несколько видов [4].

1. Несанкционированный доступ к информации, хранящейся в компьютере,

осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

2. Создание и распространение вредоносных программ – любого программного обеспечения (ПО), предназначенного для получения несанкционированного доступа к вычислительным ресурсам или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации. Вредоносные программы делятся на обычные вирусы, сетевые черви и троянские программы.

К *обычным вредоносным объектам* относят программы, которые распространяют свои дубликаты на локальном компьютере. Главной целью является запуск определённого программного алгоритма при выполнении пользователем некоторых действий или при последовательности действий. Эти вирусы не используют напрямую ресурсы локальной или глобальной сети для размножения, а выполняют заражение исполняемых файлов, перемещаясь на локальные компьютеры других пользователей. Обычные компьютерные вирусы распространяются посредством переноса информации самим пользователем, будь то съёмный носитель, электронная почта или открытые ресурсы локальной сети.

Сетевые черви являются вредоносными объектами, распространяющие свои копии по глобальной или локальной сети, при этом используются так называемые «дыры» в программах и установленных на компьютерах пользователей ОС. Как правило, червь может проникать сквозь почтовое сообщение, при этом будет иметь вид зараженного файла, или через ICQ сообщение. Существуют «пакетные» или «бесфайловые» черви, распространяющиеся посредством сетевых пакетов, при этом используются обычные сетевые протоколы, которые сразу попадают в память компьютера, где активируются самостоятельно.

К *троянским программам* относят все вредоносные программные элементы, использующие информацию либо ресурсы компьютера для своего хозяина. Как правило, происходит шифрование или стирание данных пользователя, пересылка конфиденциальной информации пользователя, воровство паролей доступа к сетевым ресурсам, использование ресурсов компьютера для рассылки спама или атак серверов. Обычно троянские программы не способны нарушить работу зараженного компьютера, они ведут себя достаточно тихо, без особых проявлений.

3. Компьютерный шпионаж или компьютерное пиратство.

Компьютерный шпионаж или кибершпионаж – это методы получения секретной конфиденциальной информации без предварительного разрешения владельцев данной информации (личной, служебной или засекреченной): частных лиц, конкурентов, правительства либо врагов. Такой вид слежения за компьютерами предполагает использование неких методов доступа к секретной, конфиденциальной информации либо контроля компьютерных систем, целых сетей для получения стратегических преимуществ применимых к психологической, политической и физической деятельности, в частности диверсий. В последнее время кибершпионаж все чаще применяется для анализа общественной активности на сайтах соцсетей.

Под *компьютерным пиратством* обычно понимается несанкционированное правообладателем копирование, использование и распространение программного обеспечения. Компьютерное пиратство может принимать различные формы, однако можно выделить несколько наиболее распространенных его разновидностей:

– интернет-пиратство – это распространение нелегальных копий программных продуктов с использованием Интернет. Данная разновидность пиратства выделена специально для того, чтобы подчеркнуть ту большую роль, которую играет сегодня Интернет для незаконного копирования и распространения поддельного и иного незаконно распространяемого программного обеспечения. В понятие Интернет-пиратства входит, в частности, использование глобальной сети для рекламы и публикации предложений о продаже, приобретении или распространении пиратских копий программных продуктов. Сюда же относится публикация в сети Интернет серийных номеров коммерческого ПО.

– нелегальное тиражирование – это широкомасштабное изготовление подделок (ПО и упаковки) и распространение их в каналах продаж под видом легальных продуктов. Для изготовления подделок могут использоваться современные технологии, при этом зачастую достигаются такое качество и такая точность копирования упаковки, логотипов и элементов защиты, что становится нелегко отличить подделку от оригинального продукта. Распространители поддельного ПО, как правило, привлекают покупателей низкими

ценами, не упоминая о рисках для пользователей, связанных с использованием их товаров. Распространители поддельного ПО также обычно скрывают тот факт, что продают нелицензионный продукт, покупатель которого фактически не приобретает законного права им пользоваться.

4. Компьютерный саботаж или терроризм. Компьютерный саботаж – это умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя.

Кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. Одним из способов кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Это проявляется в угрозе насилия, поддержании состояния постоянного страха с целью достижения определенных политических или иных целей, принуждении к определенным действиям, привлечении внимания к личности кибертеррориста или террористической организации, которую он представляет. Кибертерроризм угрожает не только высокоразвитым в технологическом плане странам, но учитывая динамику развития сети Интернет, и всему миру в целом [5].

5. Компьютерное мошенничество представляет собой умышленное раскрытие информации, замена или искажение данных, хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием с использованием компьютерных систем. Наиболее распространены следующие виды компьютерного мошенничества [6]:

– аукционные мошенничества/интернет-мошенничества – например, несуществующая победа на аукционе в интернете, либо на каком-то портале находят товар и рекомендуют его купить, покупатель переводит деньги, но товар не получает;

– мошенничество с банковскими карточками – без ведома человека и без его согласия по его карточке снимаются деньги с его счета;

– мошенничество с кредитными карточками и манипуляции с расчетным счетом – без ведома человека и без его согласия с его расчетного счета производятся денежные операции (сделаны перечисления, оплата кредитной карточкой и т.п.);

– манипуляции с виртуальными счетами/телефонами – по мобильному телефону, не принадлежащему мошеннику, заказаны платные услуги или перечислены на некий виртуальный счет деньги (например, Rate SOL, заказы «Теста смерти», теста IQ, мелодий игр и т.д.).

В связи с тем, что компьютеры и всемирная сеть становятся основными источниками хорошего дохода многих людей, все большее распространение получают различные виды интернет-мошенничества, к которым относятся [6]:

– *фиктивные интернет-магазины*, предлагающие купить товар по низким ценам. Особенно привлекательно это тогда, когда дается возможность купить эксклюзивный товар по заниженной стоимости. Первый способ обмана – требование полной оплаты покупки или ее предоплата до получения. После перечисления денег на счет мошенников, они просто исчезают и не выходят на связь. Второй вариант – это когда оплачивается товар, а взамен покупатель получает или подделку, или какую-нибудь ерунду, которую не заказывал. И снова все попытки связаться с продавцом терпят неудачи.

– *фишинг* – это получение данных чужой платежной карты. Обычно высылаются письма от имени банков или хостингов, на которых заводят электронные кошельки, содержащие информацию о том, что необходимо срочно погасить кредит. Или предлагается по указанной ссылке зайти на сайт банка (выглядеть такая страница будет точно так же, как и реальный сайт, только с небольшими видоизменениями) для ознакомления с изменениями в какой-либо области его деятельности (например, меняется система оплаты и обналичивания средств), где пользователя просят ввести персональные данные с платежной карты. В результате вся информация поступит мошеннику. Так что никогда не следует переходить по подозрительным ссылкам, присланным по электронной почте с неизвестных адресов, и тем более не указывать никаких персональных данных.

– *попрошайки* – виды мошенничества в интернете, которые направлены на человеческую психологию. Точнее говоря, они попросту «давят» на некоторые точки, которые вынуждают людей по собственной воле отдавать свои деньги. Это коварные виды мошенничества и никто не станет писать письма с банальной просьбой «подайте на пропитание». На сайтах или в социальных сетях размещаются объявления с просьбами помочь больному ребенку или сироте. В объявлении, как правило,

указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, вы просто пополняете счет какому-то мошеннику.

– *брачная афера* или мошенничества на сайтах знакомств. Они направлены на наивность людей и их отзывчивость. Это довольно популярный способ обмана. Особенно, молоденьких девушек и состоятельных мужчин. Такие виды мошенничества в интернете заняли второе место по «прибыли» и «безнаказанности». Большой популярностью пользуются брачные аферы среди иностранных граждан. В крайнем случае, соотечественников, живущих далеко от злоумышленника. Обычно все начинается с простого знакомства. Это может быть объявление в интернете от лица нетребовательной милой девушки, которая ищет серьезные отношения или же прямое письмо в социальной сети (этот вариант наименее вероятен – мошенника будет довольно легко выследить). Виды мошенничества на сайтах знакомств могут длиться долгий период времени. Обычно такая афера требует 2-3 месяца. После этого периода, наполненного романтикой и любовью, мошенник просит помочь решить финансовые проблемы. Например, дать денег на устройство родителей в пансионат, перевести сумму для перелета к жениху/невесте и так далее. После того как денежные средства попадают на счет, жертва больше не имеет возможности выйти на связь со злоумышленником.

Заключение

В заключение хотелось бы отметить несколько надежных способов, как обезопасить себя и свой персональный компьютер, поскольку каждый из нас в независимости от уровня владения ПК и длительности работы на компьютере, хотя бы раз в жизни становился жертвой компьютерных преступников.

В первую очередь, чтобы не столкнуться с мошенничеством на этапе покупки компьютера необходимо обращаться только в специализированные магазины. Так же обратите особое внимание на гарантийный талон, поскольку вещь дорогостоящая и в случае брака или выхода машины из строя вам гарантированно должны будут его заменить или вернуть деньги, если срок гарантийного талона еще не вышел.

На следующем этапе, при установке программного обеспечения стоит тщательно подходить к выбору данного продукта. На сегодняшний день у каждой компании-разработчиков программного обеспечения существуют нормы упаковки. Перед совершением покупки изучите какой материал использует компания разработчика, что должно быть в упаковке и многие другие характеристики, отличающие лицензированное программное обеспечение от подделки.

Для того чтобы обезопасить себя от вредоносных программ необходимо тщательно подойти к выбору антивирусной программы. Наиболее популярны такие антивирусы, ориентированые с учетом новейших вирусов, как Касперский (KAV), Dr. Web, Avast, 360 Total Security. Но иногда и этого бывает недостаточно. Будьте бдительны и не посещайте сомнительные сайты, не пользуйтесь непроверенными съемными носителями, при скачивании файлов внимательно читайте информацию, которая вам предоставляется.

Так же будьте внимательны при посещении разного рода сайтов на просторах Интернета. Старайтесь не вводить личные паспортные данные, номера телефонов и банковских карт. Не разрешайте подозрительным сайтам использовать ваши данные с других более популярных сайтов. Пользуйтесь более распространёнными ресурсами, на них риск угрозы менее велик.

Будьте осторожны при общении в социальных сетях, не доверяйтесь мало знакомым людям, старайтесь не использовать в разговорах и переписках информацию, не рассчитанную для большого круга лиц. Такого рода вопросы лучше решать при личном контакте с собеседником. Так же будьте осторожны и не верьте всему что написано, до тех пор, пока не убедитесь лично в правдивости информации предоставленной вам.

Старайтесь не совершать покупки в интернет-магазинах, а если уж и возникла такая необходимость, то используйте наиболее популярные сервисы или проверенные интернет-магазины, услугами которых пользовались ваши знакомы.

Соблюдение этих простых правил позволит обезопасить себя и свой компьютер, что в итоге значительно снизит расход денежных средств. Старайтесь быть в курсе часто встречающихся компьютерных преступлений, дабы знать от чего стоит защищать свое IT-устройство.

Литература

1. Электронная библиотека Vizlib [Электронный ресурс] / Интернет-ресурс. – Режим доступа : http://www.pravo.vuzlib.su/book_z2055 _page_17.html.

2. Крылов, В.В. Информационные компьютерные преступления : учебное пособие / В.В. Крылов. – Москва: Юрид. Лит., 2005. – 240 с.

3. Портал «Компьютерные преступления [Электронный ресурс] / Интернет-ресурс. –

Режим доступа : https://sites.google.com/site/komputernyeprestuplenia.

4. Студопедия [Электронный ресурс] / Интернет-ресурс. – Режим доступа : https://studopedia.org/4-77485.htm.

5. Электронная библиотека Kursak.net [Электронный ресурс] / Интернет-ресурс. – Режим доступа : http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/

6. Форум [Электронный ресурс] / Интернет-ресурс. – Режим доступа: http://figvam.org

Гром А. В., Ефименко К. Н. Современные киберпреступления и основы кибербезопасности. *Рассмотрены основные виды компьютерных преступлений, вредоносных программ и способы мошенничества в сети Internet, а также даны рекомендации по общим принципам защиты от киберпреступлений.*

Ключевые слова: *компьютерные преступления, вредоносные программы, Internet-мошенничество, безопасность.*

Grom A. V., Efimenko K. N. Modern cybercrime and the basics of cybersecurity*The main types of computer crimes, malicious programs and methods of fraud in the Internet are considered, as well as recommendations on the general principles of protection from cybercrime.*

Keywords: *computer crimes, malicious programs, Internet-fraud, security.*

Статья поступила в редакцию 4 мая 2018 г.
Рекомендована к публикации профессором Павлышом В. Н.