ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

А.А. Томарович[1], В.Г. Жиркевич[2], Т.В. Куратева[3]

[1] - студентка 1 курса, факультета Права, группы ХП-1, Белорусского государственного экономического университета.

[2] – студентка 1 курса, факультета Права, группы ХП-1, Белорусского государственного экономического университета.

[3] – научный руководитель, старший преподаватель кафедры информациооных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр., 26, тел. (8017) 249-19-81, e-mail: petrov@bseu.minsk.by

Аннотация. В данной работе рассмотрены: виды комьпютерных преступлений , способы их совершения.

Ключевые слова: перехват информации, непосредственный перехват, электронный перехват , «мистификация», «троянский конь», «брешь», «люк», «компьютерный абортаж»

Введение. В последнее время все большее внимание уделяется преступлениям в сфере компьютерной информации. Такое внимание не беспочвенно. Сегодня практически ничто не делается без участия компьютера. Все важнейшие функции современного общества, так или иначе «завязаны» на компьютерах, компьютерных сетях и компьютерной информацией.

1.Виды преступлений в сфере компьютерной информации.

Понятие компьютерной информации определено в статье 349 Уголовного кодекса РБ. Предметом компьютерной информации являются информационные ресурсы, которые рассматриваются как отдельные массивы документов в информационных системах. Эти ресурсы содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления. В Законе дается полная расшифровка их содержания.

Особенность компьютерной информации – в ее относительно простых пересылке, преобразовании и размножении; при изъятии информации в отличии от изъятия вещи. Она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно практически неограниченное количество пользователей. Еще в 1982 году в предпринятом Верховным Судом СССР обзоре судебной практики были отражены условия использования компьютерной информации в уголовном судопроизводстве. Чаще всего несанкционированный доступ 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. Прогресс породил абсолютно новую категорию преступников – хакеры. Люди, увлеченные компьютерной техникой до такой степени, что это выходит за рамки приличий. По непроверенным данным в мире существуют целые сообщества хакеров, где они обмениваются информацией, данными и тому подобным. В большинстве случаев преступления в сфере компьютерной информации совершаются ими. Для некоторых взлом и попытка разобраться в украденной информации развлечение, для других бизнес. Есть еще несколько довольно простых и эффективных способов незаконного подключения к удаленным компьютерам. По этому поводу пишутся целые трактаты, их можно найти в неограниченном количестве в Интернете – глобальной всемирной компьютерной сети. Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Это создает

возможности для нахождения "брешей". Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Бывает, что программисты намеренно делают "бреши" для последующего использования. Прием "брешь" можно развить. В найденной (созданной)"бреши" программа "разрывается" и туда дополнительно вставляют одну или несколько команд. Этот "люк" "открывается" по мере необходимости, а встроенные команды автоматически осуществляют свою задачу. Чаще всего этот прием используется проектантами систем и работниками организаций, занимающихся профилактикой и ремонтом систем. Реже - лицами, самостоятельно обнаружившими "бреши". Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простой путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей. Здесь способов – великое множество, начиная с простого мошенничества

2.Способы совершения компьютерных преступлений.

Способ совершения преступления слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступления. Обычно преступники, совершая эти действия, оставляют определенные следы, которые впоследствие позволяют восстановить картину происшедшего, получить представление о своеобразии преступного поведения правонарушителя, о его личностных данных.

В настоящее время можно выделить свыше 20 основных способов совершения компьютерных преступлений и около 40 их разновидностей. И их число постоянно растет. Выделим 5 основных групп способов совершения компьютерных преступлений. Классифицирующий признак – метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями.

2.1. Изъятие средств компьютерной техники. Сюда относятся традиционные способы совершения «некомпьютерных» преступлений, в которых преступник, попросту говоря, изымает чужое имущество. Чужое имущество – средства компьютерной техники. К этой группе преступлений можно отнести, например, незаконное изъятие физических носителей, на которых находится ценная информация. Такие способы совершения компьютерных преступлений достаточно полно изучены отечественной криминалистической наукой, поэтому можно не заострять внимание на этой группе.

2.2. Перехват информации. Способы основаны на действиях преступника, направленных на получение данных путем определенного перехвата. Виды перехватов:

2.2.1.Непосредственный перехват. Подключение непосредственно к оборудованию компьютера, системы или сети.

2.2.2.Злектронный перехват. Это дистанционный перехват. Он не требует непосредственного подключения к оборудованию компьютера. Способ основан на установлении приемника, который принимает электромагнитные волны. Благодаря этому способу можно принимать сигналы с больших расстояний.

2.2.3.Аудиоперехват. Это самый опасный способ перехвата информациии. Он заключается в установке специального прослушивающего устройства (« жучок »). Этим способом пользуются, в основном, профессиональные преступники.

2.2.4. Видеоперехват. Способ имеет две разновидности. Первая – физическая, заключается в применении преступником различных бытовых видеооптических приборов.

Во втором случае преступник использует специальные электронные устройства, которые предполагают наличие различных каналов связи.

2.2.5. «Уборка мусора». Этот способ совершения компьютерных преступлений заключается в неправомерном использовании преступником отходов технологического процесса. Он осуществляется в двух формах: физической и электронной. В первом случае преступник осматривает содержимое мусорных корзин, емкостей для технологических отходов; собирает оставленные или выброшенные физические носители информации. Что касается электронного варианта, то он требует просмотра содержимого памяти компьютера для получения необходимой информации. Существуют специальные программы, которые могут частично или полностью восстанавливать данные на компьютере. Преступник, используя такую программу, может получить необходимую информацию.

2.3. В третью группу способов совершения компьютерных преступлений можно отнести действия преступника, направленные на получение несанкционированнго доступа к средствам компьютерной техники. К ним относятся следующие:

2.3.1.«За дураком». Правонарушителями в данном случае являются внутренние пользователи определенной системы. Подключиться можно с помощью телефонной проводки. Преступление совершается в тот момент, когда сотрудник, который отвечает за работу средства компьютерной техники, ненадолго покидает свое рабочее место, оставляя технику в активном режиме.

2.3.2.«Компьютерный абордаж». Используя данный способ, преступник производит подбор кода. Для этих целей используются специальные программы, которые с помощью высокого быстродействия компьютера перебирают все возможные варианты пароля .

2.3.3.«Неспешный выбор». Данный способ характеризуется поиском преступником слабых мест в защите компьютерной системы. Когда такое место найдено, преступник копирует нужную информацию на физический носитель.

2.3.4.«Брешь». В этом случае преступник ищет конкретно участки программы, имеющие ошибки.

2.3.5.«Люк». Когда преступник находит «брешь», он может ввести туда несколько команд. Эти команды срабатывают в определенное время или при определенных условиях, образуя тем самым «люк», который открывается по мере необходимости.

2.3.5.«Маскарад». С помощью данного способа преступник входит в компьютерную систему, выдавая себя за законного пользователя.

2.3.6.«Мистификация». Пользователь, который подключается к чьей-нибудь системе, обычно уверен, что он общается с нужным ему абонентом. Этим пользуется преступник, который правильно отвечает на вопросы обманутого пользователя. Пока пользователь находится в заблуждении, преступник может получать необходимую информацию.

2.3.7.«Аварийная ситуация». Этот способ совершения компьютерных преступлений характерен тем, что преступник для получения несанкционированного доступа использует программы, которые находятся на самом компьютере. Обычно это программы, которые отвечают за «здоровье» компьютера.

2.3.8.«Склад без стен». В этом случае преступник проникает в систему во время поломки компьютера. В это время нарушается система защиты.

2.4. К четвертой группе способов совершения компьютерных преступлений относят группу методов манипуляции данными и управляющими командами средств компьютерной техники.

2.4.1.«Подмена данных». Наиболее популярный способ совершения преступления. Действия преступника при этом направлены на изменеие или введение новых данных. Это осуществляется при вводе-выводе информации.

2.4.2.«Троянский конь». Это тоже весьма популярный способ совершения преступления. Он заключается во введении преступником в чужое программное обеспечение специальных программ. Эти программы начинают выполнять новые действия, которые не

были запланированы законным владельцем средства компьютерной техники. Под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». «Троянский конь» по сути чем-то напоминает «люк». Отличие в том, что «троянский конь» не требует непосредственного участия самого преступника, программа делает все сама. Далее рассмотрим некоторые виды этой программы:

2.4.2.1. «Троянская матрешка». Это вид «троянского коня». Предполагает собой самоуничтожение программы из чужого программного обеспечения после выполнения своей задачи.

2.4.2.2.«Салями». Данный способ основан на быстродействии средств компьютерной техники. Дело в том, что при совершении коммерческих сделок конечные суммы округляются. Остаточные суммы настолько малы, что вообще не учитываются.

2.4.2.3.«Логическая бомба». Этот способ преступник использует, когда уверен, что наступят определенные обстоятельства. Способ представляет собой тайное внесение в чужое программное обеспечение специальных команд. Разновидностью этого способа является «временная бомба».

2.5. Компьютерные вирусы. Это программы, которые самопроизвольно присоединяются к другим программам и при запуске последних выполняют нежелательные действия (порча файлов и каталогов, искажение и уничтожение информации и т.д.). В настоящее время в мире существует очень много видов компьютерных вирусов (более 4000). Но всех их можно разбить на несколько групп:

2.5.1..Загрузочные вирусы. Заражение происходит при загрузке компьютера с носителя информации, содержащего вирус. При этом вирус автоматически внедряется во внутреннюю структуру носителя.

2.5.2.Файловые вирусы. Они поражают исполняемые файлы: EXE, COM, SYS, BAT. Эти вирусы заражают компьютер, если была запущена программа, которая уже содержит вирус. В этом случае происходит дальнейшее заражение других программ. Сначала появление вируса практически невозможно зафиксировать, так как он заразил не все нужные программы. Далее происходят нарушения в работе компьютера. Большинство вирусов не носят разрушительного характера. Для изучения вирусов создана специальная наука – компьютерная вирусология. С точки зрения этой науки вирусы можно разделить на резидентные и нерезидентные, «вульгарные» и «раздробленные».

2.5.3 .Резидентные и нерезидентные. Во-первых, резидентной называется программа, которая по окончании работы оставляет свой код в оперативной памяти компьютера. Оперативная память – это память, предназначенная для исполняемых в данный момент программ и оперативно необходимых для этого данных. Резидентная программа работает параллельно другим программам. И если вирус попадает в оперативную память компьютера, то он фактически заражает все программы, с которыми функционирует параллельно. Резидентный вирус, оставляя свой код в оперативной памяти, возобновляется при каждом включении компьютера. Менее опасными являются нерезидентные вирусы. Они оставляют в оперативной памяти небольшие программы, которые не имеют алгоритма распространения вируса. Такой вирус погибает при выключении компьютера.

2.5.4.«Вульгарные» и «раздробленные» вирусы. Такое деление произведено по алгоритму строения и обнаружения того или иного вируса. «Вульгарные» вирусы написаны одним блоком и легко обнаруживаются специалистами с помощью специальных антивирусных программ. Что касается «раздробленного» вируса, то нужно сказать, что такая программа разделена на части. Эти части никак не связаны друг с другом, но они «собираются» при определенных условиях во вполне здоровый вирус. При выполнении своей задачи такой вирус распадается или самоуничтожается.

Далее рассмотрим наиболее популярные вирусные модификации:

2.5.5.Вирусы-«черви». Эти вирусы не изменяют программные файлы. Они

проникают в память компьютера из компьютерной сети, и вычисляют адреса других компьютеров.

2.5.6.«Ппаразитические». Сюда входят вирусы, которые обязательно изменяют программные файлы.

2.5.7.«Студенческие». Такие вирусы содержат много ошибок, и легко обнаруживаются специальными программами.

2.5.8.Вирусы-невидимки. Это достаточно совершенные вирусы. Их трудно обнаружить антивирусной программой и невозможно увидеть при обычном просмотре файлов.

2.5.9.Вирусы-призраки. Это тоже трудно обнаруживаемые вирусы. Дело в том, что они, заражая программы, постоянно меняют свой код (содержание). Так что во всех следующих зараженных программах нельзя заметить какого-то совпадения. Поэтому эти вирусы трудно обнаружить с помощью антивирусных программ, основанных на этом принципе.

2.6.1.«Асинхронная атака». Для понимания этого способа совершения компьютерных преступлений нужно дать понятие операционной системе. Операционная система – комплекс программных средств, обеспечивающих управление информационными процессами при функционировании компьютерной системы. Главная задача операционной системы – обеспечение максимальной производительности компьютера. Функции: управление, коммуникация, планирование и т.д.

2.6.2.Моделирование. Данный способ совершения компьютерных преступлений представляет собой моделирование поведения устройства или системы с помощью программного обеспечения.

2.6.3.Копирование. Этот способ совершения преступления представляет собой незаконное копирование информации преступником программных средств компьютерной техники.
2.6.4.Преодоление программных средств защиты. Это скорей вспомогательный способ совершения преступления. Он представляет собой умышленное преодоление системы защиты. Существует несколько раздновидностей этого способа:

2.6.5.Создание копии ключевой дискеты. Для запускания некоторых систем необходима ключевая дискета. На этой дискете записаны необходимые системные файлы.

2.6.6.Модификация кода системы защиты. Код системы защиты выполняет в компьютере следующие функции:

2.6.7.Проверка ключевой дискеты;

2..6.8.Проверка санкционированности запуска защищенного информационного ресурса.

Модифицируя этот код, преступник просто обходит эти функции.

2.6.9.Использование механизма установки (снятия) программных средств защиты информации. Некоторые программные средства защиты устанавливаются на физический носитель и закрепляются на нем вместе с другими данными.

2.6.9.Снятие системы защиты из памяти ЭВМ.

Система защиты периодически загружает защищаемое программное средство в оперативную память для передачи управления этой программой коду защиты. Когда код еще не взял управление на себя, в оперативной памяти находится совершенно незащищенная программа. Опасность компьютерного вируса состоит в том, что он может привести к полной дезорганизации системы компьютерной информации, может бездействовать достаточно длительное время, затем неожиданно активизироваться и привести к катастрофе. Вирус может оказаться причиной катастрофы в таких областях использования компьютерной информации.. Под использованием (распространением) вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в компьютер, систему, сеть компьютеров. Можно предположить, что под распространением следует понимать и их копирование. Законодатель, наконец, осознал серьезность создавшиейся ситуации, предусмотрев квалифицирующие признаки: такое преступление может иметь и тяжкие последствия – гибель людей, причинение тяжкого вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности. Выявляется вирус не

сразу: первое время компьютер "вынашивает инфекцию", поскольку для маскировки вирус нередко используется в комбинации с "логической бомбой" или "временной бомбой". Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы. Специалисты предостерегают от копирования ворованных программ.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является "средством" достижения цели. В тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, соответственно ее хищение, уничтожение или повреждение подлежит квалификации по статьям Уголовного кодекса. Но дело в том, что информационная структура (например программы и информация) не может быть преступлением против собственности, поскольку машинная информация не отвечает ни одному из основных принципов предмета преступления против собственности, в частности, она не обладает физическим признаком (другими словами ее просто нет в реальном мире, она эфемерна). Что же касается компьютера как орудия преступления, то его следует рассматривать в ряду таких средств, как оружие или транспортное средство. В этом смысле использование компьютера имеет уже прикладное значение при совершении преступления, то есть хищения денежных средств, сокрытие налогов. Кроме того, компьютер может использоваться в целях хранения какой-либо информации, он может служить типографским станком, аппаратурой для неправомерного доступа в базы данных, копирования информации и так далее. Такие действия не рассматриваются в качесвте самостоятельных преступлений, а подлежат квалификации по иным статьям в соответствии с объектом посягательства. Вся проблема стоит в том, что компьютер по сути своей универсален, и позволяет выполнять практически любую работу очень широкого круга назначения. Здесь также можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

Другой вид преступлений с использованием компьютеров получил название "воздушный змей". В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами.

ЗАКЛЮЧЕНИЕ. Как известно-наиболее опасные преступления-это те, которые носят экономический характер. Например, это неправомерное обогощение путем злоупотребления с автоматизированными информационными системами ,экономический шпионаж, кража программ и так называемого «компьютерного времени», традиционные экономические преступлния, совершаемые с помощью компьютера.

ЛИТЕРАТУРА.

1. Уголовный кодекс Республики Беларусь.
2. Крылов В.В. «Инфор-ые комп-ые пркступ-ия».