Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. Здесь я не буду касаться "околокомпьютерных"преступлений, связанных с нарушением авторских прав программистов, незаконным бизнесом на вычислительной техике и т. п, а также физического уничтожения компьютеров взрывами, огнем или кирпичом. Перечислю неко

торые основные виды преступлений, связанных с вмешательством в работу компьютеров.

1) Несанкционированный доступ к информации,хранящейся в компьютере.

Несанкционированный доступ осуществляется, как правило, с использо

ванием 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.

Хакеры.Гудини информационных сетей.Для некоторых взлом и копание в информации развлечение , для других бизнес. Они могут ночами биться в закрытые двери (шлюзы) сетей или компьютеров конкретных людей перебирая простые слова в качестве пароля. И это не так глупо как кажется (по крайней мере было до недавнего времени).Есть еще несколько довольно простых и эффективных способов незаконного подключения к удаленным компьютерам но я пишу не учебник для хакеров,поэтому приводить их не буду а продолжу классификацию.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может неспеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз как покупатель рассматривает товары на витрине или читатель выбирает книгу,просматривая полки библиотек. Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. На пример, практика качественного программирования предполагает, что когда программа Х требует использования Программы У, должна выдаваться только информация, необходимая для вызова У. Составление программ группировки данных - дело довольно скучное и утомительное, поэтому иногда прибегают к упрощению, указывая, где можно найти нужные данные в рамках более общего списка. Это создает возможности для нахождения "брешей". Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Например, не все комбинации букв используются для команд, указанных в руководстве по эксплуатации компьютера. Некоторые такие сочетания могут приводить к неожиданным результатам. Все эти небрежности,ошибки, слабости логики приводят к появлению "брешей". 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".

Таким образом некий Роберт Моррис сумел парализовать работу 6000компьютеров в США,используя найденные им "бреши" в ОС UNIX.О нем я еще упомяну.

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.

Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то

системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеривался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности кода.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ,своеобразный аналог приспособлений, помещаемых в транспорте под надписью "Разбить стекло в случае аварии". Такая программа -- мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к непринадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает,что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

2) Ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники,например, отчисляют на свой счет определенную сумму с каждой операции.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен тысяч, а иногда и миллионов команд. Поэтому "троянский конь" из нескольких десятков команд вряд ли может быть обнаружен,если, конечно, нет подозрений относительно этого. Но и в послед -- нем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Интересен случай использования "троянского коня" одним американским программистом. Он вставил в программу компьютера фирмы, где работал, команды, не отчисляющие деньги, а не выводящие на печать для отчета определенные поступления. Эти суммы, особым образом маркированные, "существовали" только в системе. Вульгарным образом украв бланки, он заполнял их с указанием своей секретной маркировки и получал эти деньги, а соответствующие операции по-прежнему не выводились на печать и не могли подвергнуться ревизии.

Есть еще одна разновидность "троянского коня".Ее особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно выполняющие "грязную" работу. а команды, формирующие эти команды и после выполнения уничтожающие их. В это случае программисту, пытающемуся найти "троянского коня", необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т. д.(сколь угодно большое число раз), которые создают "троянского коня".

В США получила распространение форма компьютерного вандализма,при которой "троянский конь" разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу юмпьютерах оказалась "временная бомба", которая "взрывается" в самый неожиданный момент, разрушая всю библиотеку данных.

К сожалению, очень многие заказчики прекрасно знают, что после конфликтов с предприятием-изготовителем их программное обеспечение,которое до сих пор прекрасно работало, вдруг начинало вести себя самым непредсказуемым образом и наконец полностью отказывало. Нетрудно догадаться, что и копии на магнитных лентах или дисках, предусмотрительно сделанные, положения нисколько не спасали.

Оставался один путь -- идти с повинной к разработчику.

3) Разработка и распространение компьютерных вирусов.

"Троянские кони" типа сотри все данные этой программы, перейди в

следующую и сделай то же самое" обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер "вынашивает инфекцию", поскольку для маскировки вирус нередко используется в комбинации с "логической бомбой" или "временной бомбой". Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека. Начиная действовать (перехватывать управление), вирус дает команду компьютеру,чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователъ ничего не заметит, так как его компьютер находится в состоянии"здорового носителя вируса". Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер "заболевает".

Экспертами собрано досье писем от шантажистов, требующих перечисления крупных сумм денег в одно из отделений американской фирмы "ПК Сиборг"; в случае отказа преступники грозятся вывести компьютеры из строя. По данным журнала"Бизнес уорлд", дискеты-вирусоносители получеы десятью тысячами организаций, использующих в своей работе компьютеры.

Для поиска и выявления злоумышленников созданы специальные отряды английских детективов .

Все вирусы можно разделить на две разновидности, обнаружение которых различно по сложности: "вульгарный вирус" и "раздробленный вирус". Программа "вульгарного вируса" написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить ее в самом начале эпидемии (размножения). Эта операция требует, однако, крайне тщательного анализа всей совокупности операционной системы ЭВМ.

Программа "раздробленного вируса" разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции которые указывают компьютеру как собрать их воедино, чтобы воссоздать и, следовательно,размножить вирус. Таким образом, он почти все время находится в "распределенном" состоянии, лишь на короткое время своей работы собираясь в единое целое. Как правило, создатели вируса указывают ему число репродукций, после достижения которого он становится агрессивным.

Вирусы могут быть внедрены в операционную систему, в прикладную программу или в сетевой драйвер.

Варианты вирусов зависят от целей, преследуемых их создателем.

Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея (т. н. "итальянский попрыгунчик"). Признаки могут быть эволютивными, и "болезнь" будет обостряться по мере своего течения. Так по непонятным причинам программы начинают переполнять магнитные диски,в результате чего существенно увеличивается объем программных файлов.

Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения,

Каковы способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве "средства передвижения". То есть с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда "здоровая" дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. 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.

Иногда, однако, и официально поставляемые программы могут быть источником заражения. Например, фирма "Альдус" выпустила несколько тысяч зараженных дискет с графическими программами.

Часто с началом компьютерной эпидемии связывают имя уже упоминаемого Роберта Морисса студента Корнеллского университета (США), в результате действий которого зараженными оказались важнейшие компьютерные сети восточного и западного побережий США . Эпидемия охватила более б тысяч компьютеров и 70 компьютерных систем. Пострадавшими оказались, в частности, компьютерные центры НАСА, Диверморской лаборатории ядерных исследований, Гарвардского, Питсбургского, Мэрилендского, Висконсинского, Калифорнийского, Стзнфордского университетов. Пикантность ситуации в том, что отец Р. Морисса -- высокопоставленный сотрудник отдела безопасности компьютеров Агентства национальной безопасности .

А изобретателем вируса является, однако, совсем другой человек В августе 1984 года студент Калифорнийского университета Фред Коуэн,выступая на одной из конференций, рассказал про свои опыты с тем, что один его друг назвал "компьютерным вирусом". Когда началось практическое применение вирусов, неизвестно, ибо банки, страховые компании,предприятия, обнаружив, что их компьютеры заражены вирусом, не допускали, чтобы сведения об этом просочились наружу.

В печати часто проводится параллель между компьютерным вирусом и вирусом "AIDS". Только упорядоченная жизнь с одним или несколькими партнерами способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражению. Замучу, что пожелание ограничить использование непроверенного программного обеспечения скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные программы на "стерильных" носителях стоят немалых денег в конвертируемой валюте. Поэтому избежать их неконтролируемого копирования почти невозможно.

Справедливости ради следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности,они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету,

4) Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транс

порта и т. п.

Особенностью компьютерной неосторожности является то, что безошибочньх программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

5) Подделка компьютерной информации.

По-видимому этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т. п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

Здесь можно вспомнить, например, случай с исчезновением 352 вагонов на нью-йоркской железной дороге в 1971 году. Преступник воспользовался информацией вычислительного центра, управляющего работой железной дороги, и изменил адреса назначения вагонов. Нанесенный ущерб составил более миллиона долларов .

Очень близкое по способу совершения преступление было раскрыто в армейском компьютерном центре в Таегу (Южная Корея). Здесь путем подделки компьютерной информации большое количество продовольствия и обмундирования направлялось с военных складов на "черный рынок". Общая сумма хищения достигла 10 млн. долларов .

Служащий одного нью-йоркского банка, изменяя входные данные, похитил за 3 года 1,5 миллиона долларов. В Пеисильвании (США) клерк и несколько рабочих крупного мебельного магазина, введя с терминала фальшивые данные, украли товаров на 200 тыс. долларов .

6) Хищение компьютерной информации.

Если "обычные" хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение,поскольку хищение сопряжено с изьятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является "средством" достижения цели. Здесь 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.

Классическим примером служит дело собственника компьютерной службы, бухгалтера по профессии, служившего одновременно бухгалтером пароходной компании в Калифорнии (США), специализировавшейся на перевозке овощей и фруктов. Он обнаружил пробелы и деятельности ревизионной службы компании и решил использовать этот факт. На компьютере своей службы он смоделировал всю бухгалтерскую систему компании. Прогнав модель вперед и обратно, он установил, сколько фальшивых счетов ему необходимо и какие операции следует проводить.

Он организовал 17 подставных компаний и, чтобы создать видимость реальности ситуации, обеспечил каждую из них своим счетом и начал денежные операции. Модель бухгалтерского баланса подсказала ему, что при имеющихся пробелах в ревизионной службе, 5%-ное искажение не будет заметно, Его действия оказались настолько успешными, что в первый год он похитил 250 тыс. долларов без какого-либо нарушения финансовой деятельности компании. К тому времени, когда увеличенные выплаты вызвали подозрение -- даже не у самой компании, а у ее банка, -- сумма хищения составила миллион долларов .

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. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк так чтобы общая сумма покрывала требование о первом переводе . Этот цикл повторяется большое число раз ("воздушный змей" поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Дело этого типа имело место в Лондоне. Группа мошенников объединилась с несколькими специалистами по компьютерам. Они обзавелись микрокомпьютером, сделали моделирующую программу и начали действовать по указанию из "штаб-квартиры", куда звонили по телефону и получали указания в соответствии с рекомендациями модели. Все шло блестяще и "змей" уже забрался чрезвычайно высоко, но тут произошел сбой в компьютере. Дублирующего компьютера не предусмотрели, и "змей" рухнул.

Скотлэнд Ярд за несколько дней арестовал всех мошенников. След естественным образом привел к "штаб-квартире", где специалисты по компьютерам, забыв об отдыхе, пытались наладить работу компьютера .

Тем же самым способом служащий банка в Лос-Анджелесе со своими сообщниками, которые давали поручения о переводе, похитил 21,3 млн.долларов. Здесь технология запуска "змея" была более четкой.По указаниям моделирующей программы открывалось большое количество новых счетов, размер переводимых сумм менялся и т. д.

А вот другой пример. В Великобритании один из пользователей компьютерного центра написал особую программу и записал ее на диск,зная, что ею заинтересуются и постараются посмотреть, что она из себя представляет. Программа начала работу, а затем смоделировала системную поломку. Затем программа записала коды всех пользователей, осуществляющих несанкционированный доступ в нее. Автор модели после того, как собрал необходимые ему сведения, использовал их в своих интересах.