# Компьютерная преступность как социологическая категория Компьютерная преступность является современным вариантом проявления социальной девиации (отклонения). Различаются, как правило, четыре вида компьютерных преступлений: компьютерное мошенничество; компьютерный терроризм (несанкционированный доступ к компьютерным системам и вирусописательство); копирование и продажа компьютерных программ в нарушение авторских прав, а также различные виды компьютерных злоупотреблений, которые не относятся к ранее перечисленным, например, случаи кражи данных, саботаж в вычислительных центрах и т.д. Уголовный Кодекс РФ с 1 января 1997 года впервые ввел в России ответственность за компьютерные преступления, однако, его практическому использованию мешает отсутствие в общественном сознании установки на осуждение компьютерной преступности, зачаточное состояние информационного права как правовой отрасли, а также явно недостаточное количество специалистов как по информационному праву, так и по правовой информатике. Компьютерофобия - социально-психологическое явление, выражающееся в отчуждении отдельных людей, а также определенных социальных групп от современной стремительно совершенствующейся компьютерной техники, от растущих и усложняющихся информационных потоков. Информомания как социально-психологическое явление выражается в приоритете общения с компьютером, а не с людьми, то есть в потере необходимой меры социализации личности. Используется иногда также термин "интеллектуальная наркомания". Очевидно, что компьютерная преступность и компьютеромания - два взаимосвязанных социальных явления. Все вместе эти явления представляют собой достаточно распространенные виды современной социальной девиации. Отметим объективные, наиболее значимые для социологии и социального управления причины упомянутых выше явлений. Это отсутствие компьютеров с дружественным интерфейсом (в случае компьютерофобии) и социально-экономическая обстановка в стране, а также отсутствие научно-обоснованной молодежной политики и политики занятости, сформированных с учетом реалий современной информационной среды (в случае компьютеромании и компьютерной преступности). Этот вывод подтверждает трансформация образа "хакера" в общественном мнении, отражающаяся в публикациях. До недавнего времени предполагалось, что "хакер" - это бледный, постоянно сидящий за экраном своего компьютера юноша или подросток, лишенный всяких жизненных интересов и ломающий голову над какой-либо очередной системой защиты или выдумывающий какой-либо вирус. Сегодня "хакерство" стало очевидным способом зарабатывания на жизнь. Расширенная сеть компьютерных рынков позволяет сбывать огромное количество пиратской программной продукции, следовательно, получать прибыль и организовывать бизнес. В основе такого бизнеса, в качестве основной рабочей силы и находятся "хакеры" - обычные молодые люди, получившие программистское образование. Существуют и субъективные причины компьютерной преступности. Так, например, попытка молодых людей реализовать себя в вирусописательстве часто связана с такими причинами, как желание самоутвердиться, "прогреметь", а также с отсутствием осознанных жизненных целей. К конкретным социальным группам, отождествляемым с киберпанками, по мнению специалистов, относятся "хакеры", "крэкеры" и "фрикиры". "Хакеры" - "сливки" компьютерного сообщества, люди, прекрасно разбирающиеся в работе компьютера. "Крэкеры" - реальные аналоги "ковбоев пульта" из фантастики в стиле киберпанк, вламывающиеся в компьютерные системы, как для незаконного обогащения, так ради удовольствия. "Фрикиры" - это те, кто занимается аналогичными вещами в телефонных сетях, изобретая способы оставить телефонные компании без причитающейся им платы за услуги. Особняком стоят "рейверы". К ним относятся люди, использующие синтетическую и выборочную музыку, компьютерное психоделическое искусство, а также искусственные наркотики. Этой же позиции, разводящей понятия "хакеры" и "крэкеры" придерживаются и С. Клименко и В. Уразметов, считающие, что: 1. Хакер (hacker) - это программист, способный писать программы без предварительной разработки детальных спецификаций и оперативно вносить исправления в работающие программы, не имеющие документации, в том числе и непосредственно в машинных кодах, что требует высочайшей квалификации. 2. Иногда под хакером ошибочно подразумевают взломщика, тогда как взломщик (cracker) - это пользователь вычислительной системы (обычно компьютерной сети), занимающийся поиском незаконных способов получить доступ к защищенным ресурсам, например, конфиденциальной информации. Аналогичного подхода придерживаются В.И. Першиков и В.М. Савинков, которые считают хакером программиста-фанатика, занимающегося доскональным изучением вычислительных систем с целью расширения их возможностей. Нам представляется, что понятие "хакер" может быть рассмотрено в широком и в узком смысле слова. В узком смысле слова "хакер" - это человек - представитель определенной социальной группы, нетрадиционно реализующей себя в условиях новой информационной реальности, т.е. носитель определенного стиля жизни. В широком смысле слова ("приговор общества") - это синоним компьютерного преступника и компьютеромана. По нашему мнению, криминализация содержания понятия "хакер" связана с отсутствием, как уже было отмечено, социального регулирования процессов самореализации молодежи в современной информационной среде. Компьютерная преступность

Ни в одном из уголовных кодексов союзных республик не удастся найти главу под названием “Компьютерные преступления”. Таким образом компьютерных преступлений, как преступлений специфических в юридическом смысле не существует.

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название “компьютерная преступность”. Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

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

**1. Несанкционированный доступ к информации,**хранящейся в компьютере. 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.

Хакеры “электронные корсары”, “компьютерные пираты” - так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая на удачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если

**- 5 -**

теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

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.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению “брешей”.

Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

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 простейший путь его осуществления :

- получить коды и другие идентифицирующие шифры законных пользователей.

Это может делаться :

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

- обнаружением такого документа в организациях, где не налажен

достаточный контроль за их хранением;

- подслушиванием через телефонные линии.

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 намеревался. 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 коды.

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.

ADVERTISEMENT

**- 6 -**

Несанкционированный доступ может осуществляться 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.

“Временная бомба” - разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени.

Способ “троянский конь” состоит в тайном введении в чужую программу таких команд, позволяют осуществлять новые, не планирывавшиеся 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 последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность “троянского коня”. Ее особенность состоит в том, что в безобидно выглядящей кусок программы вставляются не команды, собственно, выполняющие “грязную” работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом 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), создающие “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 компьютерах оказалась “временная бомба”, которая “взрывается” в самый неожиданный момент, разрушая всю библиотеку данных. Не следует думать, что “логические бомбы” - это экзотика, несвойственная нашему обществу.

**- 7 -**

**3. Разработка и распространение компьютерных вирусов.**

“Троянские кони” типа “сотри все данные этой программы, перейди в следующую и сделай тоже 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. Пользователь 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 “Business world”, дискеты-вирусоносители получены десятью тысячами организаций, использующих в своей работе компьютеры. Для поиска и выявления злоумышленников созданы специальные отряды английских детективов.

По оценке специалистов в “обращении” находится более 100 типов вирусов.

Но все их 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, прикладную программу или в сетевой драйвер.

**- 8 -**

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.

По-видимому, в будущем будут появляться принципиально новые виды вирусов. Например, можно себе представить (пока подобных сообщений не было) своего рода “троянского коня” вирусного типа в электронных цепях. В самом деле, пока речь идет только о заражении компьютеров. А почему бы - не микросхем? Ведь они становятся все более мощными и превращаются в подобие ЭВМ. И их необходимо программировать. Конечно, ничто не может непосредственно “заразить” микросхему. Но ведь можно заразить компьютер, используемый как программатор для тысячи микросхем.

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.

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.

**- 9 -**

Естественно, что против вирусов были приняты чрезвычайные меры, приведшие к созданию текстовых программ-антивирусов. Защитные программы подразделяются на три вида : **фильтрующие**(препятствующие проникновению

вируса),

**противоинфекционные** (постоянно контролирующие

процессы в системе) и

**противовирусные**(настроенные на выявление

отдельных вирусов).

Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

Заметим, что пожелание ограничить использование непроверенного программного обеспечния скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные прогаммы на “стерильных” носителях стоят немалых денег в 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**

последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.

Особенностью компьютерной неосторожности является то, что безошибочных 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 не достижима.

**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.

**- 10 -**

Идея преступления состоит в подделке выходной информации компьютеров с целью иммитации работоспособности больших систем, составной частью которых является компьютер. При достотачно 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.

**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 изятием 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.

Собственность на информацию, как и прежде, не закреплена в законодательном порядке. На мой взгляд, последствия этого не замедлят сказаться.

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.

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, а

**- 11 -**

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.

Можно представить себе создание специализированного компьютера-шпиона, который будучи подключен к разведуемой сети, генерирует всевозможные запросы, фиксирует и анализирует полученные ответы. Поставить преграду перед таким хакером практически невозможно. Не трудно предположить, что организованная преступность давно приняла на вооружение вычислительную технику.