Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ, МИР 12866 31.03.2004, 13:16 298

Права вирмейкера как человека и гражданина - часть 1.

1. Введение.

С тех пор, как студент Калифорнийского университета Фрэд Коэн[1] в 1985 году, выступая на 7-й конференции по безопасности информации, рассказал о своих опытах над тем, что один его друг[2] назвал «компьютерным вирусом», прошло уже двадцать лет. К настоящему времени проблема компьютерной безопасности всерьJз и надолго вошла в нашу жизнь и коснулась практически каждого пользователя персонального компьютера. По отношению к этой проблеме компьютерное сообщество разделилось на два полюса. Первый полюс составляют люди озабоченные неприкосновенностью своих данных и люди, обеспечивающие эту неприкосновенность юридическими, программными и техническими средствами. Второй полюс составляют так называемые хакеры, крекеры, создатели вирусов, кардеры и другие интересующиеся обратной стороной проблемы компьютерной безопасности. Они примкнули к той части компьютерного сообщества, которое составляет так называемый «компьютерный андеграунд» (от английского underground - подполье) – рипперы, демомейкеры и другие.

Не стоит думать, что существует чJткая граница между двумя этими полюсами. Есть хакеры, занимающиеся вполне легальной работой в отделах безопасности различных фирм, и есть производители коммерческого программного обеспечения выполняющего поиск дыр в защите систем (например, сканер уязвимостей http://www.ptsecurity.ru). Как правило, увлечение преодолением систем защиты компьютерной безопасности - возрастное. Некоторые представители андеграунда в последствии становятся системными администраторами, занимаются делами далJкими от компьютерной безопасности (например, бывший вирусописатель Reminder – программист 1С-Бухгалтериии [http://reminder.h1.ru/cgi-bin/main.php?mode=read&xref=1]) или работают в сфере никак не связанной с программированием. Бывает и так, что вчерашние разработчики вирусов находят работу в антивирусных компаниях (например, бывший вирусописатель Dinky[3] – разработчик российского антивируса DrWeb [http://www.drweb.ru/]).

Было бы заблуждением полагать, что любой представитель компьютерного андеграунда является нарушителем законов. Компьютерный андеграунд представляет собой слоистый пирог интересов в диапазоне от познавательных исследовательских до ярко выраженных криминальных. Запрет абсолютно всей деятельности компьютерного андеграунда противоречил бы положению статьи 29 часть 2 Всеобщей Декларации Прав Человека [1]:

При осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других…

Основной стержень компьютерного андеграунда составляют профессионалы, так называемые «хакеры». При этом хакер – это не столько уровень мастерства, сколько отношение к жизни. Не стоит думать, что хакеры появились только с возникновением компьютеров. Хакерами с полной уверенностью можно назвать средневековых алхимиков, биолога Жана Батиста Ламарка, лесковского Левшу, выдающегося математика Пьера Ферма и пытавшихся доказать его теорему, астрономов Галилео Галилея и Джордано Бруно, изобретателя Николу Тесла и многих других людей, чьи исследовательские взоры были обращены в непознанное и перед чьим мастерством можно только преклоняться.

Общество боится неизвестного и не любит хакеров за то, что они «желают странного». Поэтому люди во все века боролись с ними под понятными обществу и благовидными предлогами, как, например, борьба со «служением дьяволу», «колдовством», «ересью», «лженаучностью» и «противозаконностью». Конечно, стоит учитывать, что обладание «нетрадиционными» знаниями и умениями часто подталкивает их обладателей к корыстному использованию, для получения власти над окружающими. Поэтому «отравители» среди алхимиков в истории действительно встречались, но сжигали люди на кострах всех подряд.

Вокруг законности деятельности компьютерного андеграунда в области компьютерной безопасности уже несколько десятков лет не утихают споры на различных уровнях. ЧJткой позиции по этому вопросу до сих пор не занимает никто. При этом следует отметить, что с экономической точки зрения эта область является успешно развивающейся, в которой ежегодно вращаются миллиарды долларов США. Поэтому, кажется, вполне обоснованным желание Государства построить чJткую правовую основу для отношений физических и юридических лиц в сфере компьютерной информации. Однако в силу того, что история этих отношений насчитывает всего несколько лет (к примеру, некоторые области юридической науки насчитывают несколько тысячелетий), законодательство в этой сфере далеко от совершенства.

Попытки рассмотреть все аспекты отношений между Законом и андеграундом неоднократно предпринимались и раньше. Однако неудачи этих попыток заключались в предвзятости (необъективности) мнения авторов статей, отсутствии у них полноценных знаний в той или иной области и неумении выделить из интересов андеграунда отдельные категории деятельности (бесплодные попытки объединить несовместимые вещи). Не последнюю роль в этих неудачах играет отсутствие во многих случаях формальных общепризнанных понятий для важных терминов.

Цель данной работы: выделить из общей массы андеграунда разработчиков и исследователей компьютерных вирусов в отдельную группу и рассмотреть на eJ основе применение Законов Российской Федерации. В дальнейшем будем использовать для представителей этой группы термин «вирмэйкеры» (от английского virus maker – создатель вируса), используемый в компьютерном сленге. В различных источниках имеются аналоги термина «вирмейкер»: «программисты вирусов», «вирусописатели», «создатели вирусов», «разработчики вирусов», «технокрысы», …

Следует сразу сказать, что здесь не будет попыток оправдать разрушительные последствия применения вредоносного кода. Нанесение вреда в любой форме другим людям является преступлением и преследуется по закону. В Конституции Российской Федерации [2] сказано:

осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (статья 17 часть 3);

права потерпевших от преступлений и злоупотреблений властью охраняются законом. Государство обеспечивает потерпевшим доступ к правосудию и компенсацию причинJнного ущерба (статья 52).

Данная работа является исключительно частным мнением автора, занимающегося многие годы программированием в качестве работы и хобби и не обладающего глубокими юридическими познаниями. В работе возможны ошибки, а личные комментарии в представленной работе не являются официальной позицией автора или его попыткой оскорбить конкретные лица, фирмы или организации. Все упомянутые названия компаний и продуктов являются зарегистрированными торговыми марками. Статья предназначена для лиц интересующихся компьютерными вирусами и проблемой компьютерной безопасности по различным причинам, в том числе для юристов, вирусных аналитиков и вирмейкеров.

2. Обзор уголовного законодательства некоторых стран по преступлениям в сфере компьютерной информации

На странице http://www.crime-research.ru/library/Criminal_Code.html приведено законодательство в странах СНГ и Прибалтики по преступлениям в сфере компьютерной информации. К сожалению не нашлось ни одного из рассматриваемых государств, где так или иначе формулировки уголовных законов не вызывали бы нареканий. Замечания к текстам законов, в свете настоящей работы, вызваны следующим:

Использование термина «компьютерный вирус», общепринятого непротиворечивого определения для которого в мире до сих пор не существует.

Это замечание касается части 1 статьи 361 УК Украины, сформулированной следующим образом: «Незаконное вмешательство в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, которое привело к искажению или уничтожению компьютерной информации или носителей такой информации, а также распространение компьютерного вируса путем применения программных и технических средств, предназначенных для незаконного проникновения в эти машины, системы или компьютерные сети и способных повлечь за собой искажение или уничтожение компьютерной информации или носителей такой информации ...». При этом хочется отметить, что данная статья предусматривает наказание за действительно преступно совершенные деяния, которые принесли реальный вред.

Это замечание касается части 1 статьи 354 УК Республики Беларусь, имеющей в своей формулировке термин „вирусная программа“: «Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами ...». Аналогичная по формулировке статья 303 часть 1 включена в УК Республики Таджикистан, а именно: «Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами ...». Здесь стоит заметить, что не объясняется, кто должен давать санкцию для осуществления указанных действий и в чJм эта санкция должна выражаться.

Очень объемной и малопонятной является статья 174 УК Республики Узбекистан. ПриведJм часть формулировки этой статьи: «... Создание компьютерных вирусов или программ и их распространение без соответствующей санкции с целью изменения данных или программ, хранящихся в компьютерных системах, а равно несанкционированный доступ в информационную систему, повлекший искажение, изъятие, уничтожение информации или прекращение функционирования этой системы ...». Непонятно, на что требуется «соответствующая санкция», и кто уполномочен выдавать такие санкции.

Самой лаконичной и самой неправильной, на взгляд автора настоящей работы, является статья 273 УК Эстонской Республики, где несуществующее понятие вынесено даже в заглавие уголовного закона : «Статья 273. „Заведомое распространение компьютерных вирусов“. (1) Заведомое распространение компьютерных вирусов, -наказывается штрафом. (2) То же деяние, совершенное: 1) повторно, или 2) с причинением существенного вреда, или 3) с целью распространения вируса в государственной компьютерной системе, или 4) с целью распространения вируса в компьютерных сетях, предназначенных для всеобщего пользования, -наказывается штрафом, или арестом, или лишением свободы на срок от одного года до четырех лет».

Использование термина «вредоносная программа», без объяснения термина «вредоносность программ» и без указания критериев, по которым программы могут считаться вредоносными.

Это замечание касается статьи 273 УК Российской Федерации, статьи 272 УК Азербайджанской Республики, статьи 290 УК Кыргызской Республики и статьи 335 УК Туркменистана, имеющими идентичные формулировки. Здесь термин «вредоносная программа» вынесен даже в название уголовного закона: «Статья 273. „Создание, использование и распространение вредоносных программ для ЭВМ“. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами ...». Эта статья противоречит правам и свободам граждан, закреплJнные международными договорами РФ и Конституцией РФ. Пояснения к замечаниям по данной статье будут представлены в ходе дальнейших рассуждений.

Также неопределJнный термин «вредоносная программа» вынесен в названия уголовного закона Республики Беларусь (статья 354) и Республики Таджикистан (статья 303). Название статей идентично и выглядит следующим образом: «Статья 354. Разработка, использование либо распространение вредоносных программ».

В статье 285 УК Грузии неопределJнный термин «вредоносная программа» присутствует и в названии уголовного закона и в его формулировке: «Статья 285. „Создание, использование или распространение вредоносных программ для ЭВМ“. 1. Создание вредоносных программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации либо нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами ...».

В УК Республики Казахстан уголовные законы, касающиеся компьютерных преступлений, отражены в статье 227 с названием «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ». Часть 3 этой статьи имеет аналогичную формулировку со статьJй 273 УК РФ.

Уголовное законодательство Российской Федерации в области компьютерных преступлений.

Глава 28 «Преступления в сфере компьютерной информации» УК РФ состоит из трJх статей.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -наказывается лишением свободы на срок до четырех лет.

В отношении лиц, совершивших преступные деяния, действуют следующие статьи Уголовного Кодекса РФ:

Граждане Российской Федерации и постоянно проживающие в Российской Федерации лица без гражданства, совершившие преступление вне пределов Российской Федерации, подлежат уголовной ответственности по настоящему Кодексу, если совершJнное ими деяние признано преступлением в государстве, на территории которого оно было совершено, и если эти лица не были осуждены в иностранном государстве (статья 12 часть 1).

Граждане Российской Федерации, совершившие преступление на территории иностранного государства, не подлежат выдаче этому государству (статья 13 часть 1)

Уголовный кодекс Федеративной Республики Германии

Для сравнения с рассмотренным выше уголовным законодательством в странах СНГ и Прибалтики, приведJм ответственность за совершение преступлений в сфере компьютерной информации, предусмотренной уголовным законодательством ФРГ.

2. Раздел. «Покушение (попытка)» [3]

Параграф 22. «Определение названия»

На преступление покушается тот, кто по его представлению о поступке непосредственно приступает к осуществлению состава преступления.

15 Раздел. «Нарушение персонального жизненного и тайного пространства» [3]

Параграф 202a. «Выведывание данных» (Шпионаж за сведениями)

1. Кто неуполномочено (неправомочно) данные, которые не предназначены для него и особенно которые защищены против неправомерного доступа, добывает для себя или кого-то другого, будет наказан лишением свободы до 3-х лет или денежным штрафом.

2. Данные, в смысле абзаца 1, только те, которые электронно, магнитно или по-другому не непосредственно воспринимаемые, сохраняемые или передаваемые (пересылаемые, посылаемые).

27 Раздел. «Повреждение имущества» [3]

Параграф 303. «Повреждение имущества»

1. Тот, кто неправомерно портит (повреждает) или разрушает (уничтожает) чужую вещь, будет наказан лишением свободы до 2-х лет или денежным штрафом.

2. Попытка (покушение) наказуема.

- Общая часть УК Германии [3], Параграф 11, I, N5: Для Закона неправомерное действие – только такое, которое удовлетворяет составу преступления уголовного закона.

- Общая часть Гражданского Кодекса Германии [4], Параграф 90: Вещи – для Закона вещами являются только телесные (материальные) предметы.

Параграф 303a. «Изменение данных»

1. Тот, кто неправомерно данные (Параграф 202a Абзац 2 УК Германии) удаляет, скрывает, приводит в негодность или изменяет, будет наказан лишением свободы до 2-х лет или денежным штрафом.

2. Попытка наказуема

Параграф 303b. «Компьютерное вредительство» (Саботаж)

1. Тот, кто нарушает обработку данных, имеющих большое значение для постороннего предприятия, посторонней фирмы или учреждения (ведомства, административного органа) тем, что он:

- совершает поступок согласно Параграфа 303a Абзац 1 или

- установку для обработки данных или носитель данных уничтожает (разрушает), повреждает, приводит в негодность, устраняет (ликвидирует) или изменяет

будет наказан лишением свободы до 5 лет или денежным штрафом.

2. Покушение (попытка) наказуемо.

Параграф 303c. «Жалоба (заявление) потерпевшего»

В случае параграфов 303-303b преследуется поступок только по подаче жалобы (заявления), кроме случая, когда по причине особенной общественной заинтересованности (государственного интереса) в уголовном преследовании орган уголовного преследования посчитает необходимым (требуемым) выступления ведомства в качестве подавателя жалобы.

Кроме того, правовые отношения в сфере компьютерной безопасности регулируются подписанной ФРГ в Будапеште 23.11.2001 года «Конвенцией о компьютерных преступлениях» [5].

3. Базовые понятия

Очевидна необходимость чJтко оговорить используемые в законах принципы и базовые понятия. Дело в том, что вполне похожие деяния (например, грабJж и кража – похищение имущества) имеют разные определения и различимы Законом. Кроме того, отношение деяния к разряду преступных происходит лишь при строгом

соответствии этого деяния к определению, данному в законе (принцип запрета аналогий в уголовном законодательстве). Рассмотрим общепризнанные определения базовым понятиям, представленные в своде законов Российской Федерации. При отсутствии таких определений – в опубликованных источниках, находящихся в свободном доступе.

Словарь наиболее употребляемых компьютерных терминов приведJн в методических рекомендациях по теме «Расследование преступлений в сфере компьютерной информации» (http://deadman.interdon.net/tmp/27x.html). При этом следует учесть, что этот словарь составлен не профессиональными программистами и содержит большое количество неточностей. И хотя методы проведения следственных действий, описанные в этой работе, по характеру больше напоминают сюжет кинофильма «Гений», рекомендуется принять к сведению приведJнную в этой работе информацию. Ниже приведены некоторые примеры неточных определений, разъяснения к которым можно найти в настоящей работе:

КОД - набор выполняемых инструкций, составляющих программу, в отличие от данных, над которыми выполняются операции. Иначе говоря, кодом называется последовательность машинных инструкций, которые производит транслятор или ассемблер из текста программы.

КОМПЬЮТЕРНЫЕ ВИРУСЫ – небольшие программы, внедренные в программное обеспечение, обладающие возможностью к самотиражированию (распространению, заражению других программ). Обычно обладают враждебными функциями, которые влекут задержку работы, уничтожение данных и др.

3.1. Принципы законности

Для законотворчества (и для применения законов) действительны следующие правила:

- «требование определJнности» - закон должен быть изложен без допуска и двусмысленного его трактования;

- «презумпция невиновности» - при сомнении в пользу обвиняемого (IN DUBIO PRO REO – латынь);

- «запрет аналогии» - действие должно абсолютно точно подходить под определение, указанное в Уголовном Кодексе, только в этом случае оно являет собой состав преступления;

К правилу «презумпция невиновности», можно также добавить следующее: нет преступления без указания на то в законе (Nullum crime sine legis - латынь).

Эти правила отражены в Конституции РФ:

Обвиняемый не обязан доказывать свою невиновность (статья 49 часть 2).

Неустранимые сомнения в виновности лица толкуются в пользу обвиняемого (статья 49 часть 3).

Никто не обязан свидетельствовать против самого себя (статья 51 часть 1).

Закон, устанавливающий или отягчающий ответственность, обратной силы не имеет (статья 54 часть 1).

Никто не может нести ответственность за деяния, которое в момент его совершения не признавалось правонарушением. Если после совершения правонарушения ответственность за него устранена или смягчена, применяется новый закон (статья 54 часть 2).

Эти правила также отражены и в Уголовном Кодексе РФ [6]:

Применение уголовного закона по аналогии не допускается (статья 3 часть 2).

Лицо подлежит уголовной ответственности только за те общественно опасные действия (бездействие) и наступившие общественно опасные последствия, в отношении которых установлена его вина (статья 5 часть 1).

Объективное вменение, то есть уголовная ответственность за невинное причинение вреда, не допускается (статья 5 часть 2).

Основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного настоящим Кодексом (статья 8).

Преступность и наказуемость деяния определяются уголовным законом, действовавшим во время

совершения этого деяния (статья 9 часть 1).

Следует особо отметить, что поскольку преступления в компьютерной сфере попадают под юрисдикцию уголовного закона, то проведение любых аналогий между программами и атомными бомбами (и им подобные) являются некорректными и недопустимы для выдвижения обвинения.

3.2. Преступление

Понятие преступления даJтся в Уголовном Кодексе РФ в статье 14:

1. Преступлением признается виновно совершенное общественно опасное деяние, запрещенное настоящим Кодексом под угрозой наказания.

2. Не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного настоящим Кодексом, но в силу малозначительности не представляющее общественной опасности, то есть не причинившее вреда и не создавшее угрозы причинения вреда личности, обществу или государству.

В работе «Понятие преступления и его состав (http://refportal.ru/law/ref47145.html) можно найти следующие пояснения:

- Общественная опасность деяния – это материальный признак преступления. Общественная опасность означает, что деяние вредоносно для общества, т.е. общественная опасность состоит в том, что деяние причиняет или создает угрозу причинения существенного вреда общественным отношениям.

- Уголовная противоправность – это общественно опасное деяние, предусмотренное уголовным законом в качестве преступления.

- Обязательные признаки – это признаки присущие всем без исключения составам преступления. В каждом преступлении должны быть установлены:

§ конкретный объект;

§ мотив;

§ цель;

§ последствия преступления;

§ причинная связь между деянием и его последствиями, а также обстоятельства, характеризующие время, способ, обстановку, орудие и средства совершения преступления.

В Уголовном Кодексе в статье 24 объясняется, кто является виновным в преступлении, и какое деяние, совершенное по неосторожности, признается преступлением. В статье 26 представлены категории преступлений, совершенных по неосторожности. В статье 28 объясняется, какие деяния, имеющие состав преступления, преступлением не являются.

Ключевое слово «виновно» нужно трактовать так: если человек, совершивший деяние, должен был знать, знал или мог бы знать (в связи с доступностью информации) об общественной опасности своего деяния (об угрозе причинения существенного вреда), но всJ равно его совершил, то совершил он это виновно. Исключения: «несоответствие… психофизиологических качеств требованиям экстремальных условий или нервно-психическим перегрузкам», невозможность осознания общественной опасности своих действий по обстоятельствам дела, «либо не предвидело… и по обстоятельствам дела не должно было или не могло их предвидеть».

При отнесении деяния к противоправным деяниям нужно ориентироваться лишь на перечень деяний, приведJнных в законах. Деяния в зависимости от степени опасности относятся к преступлениям (перечислены в уголовных законах) или к проступкам (перечислены в административных законах). ВсJ, что не нашло отражения в уголовном законе, преступлением не является.

3.3. ЭВМ, сеть ЭВМ, программа для ЭВМ

В законе «О правовой охране программ для электронных вычислительных машин и баз данных» [7] в статье 1 даны следующие определения: программа для ЭВМ; база данных; адаптация программы для ЭВМ или базы

данных; модификация (переработка) программы для ЭВМ или базы данных; декомпилирование программы для ЭВМ; воспроизведение программы для ЭВМ или базы данных; распространение программы для ЭВМ или базы данных; выпуск в свет (опубликование) программы для ЭВМ или базы данных; использование программы для ЭВМ или базы данных; правообладатель. В соответствии с этим законом:

программа для ЭВМ – это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определJнного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе еJ разработки, и порождаемые ею аудиовизуальные отображения.

Недостатком такой формулировки является ее неприменимость для всех компьютерных платформ (архитектур) и в первую очередь не применимость к IBM-совместимым компьютерам с операционными системами типа MS DOS или MS Windows, речь о которых идJт в настоящей работе. Дело в том, что ни для процессора, ни для операционной системы не существует различия между командами и данными. Команды могут интерпретироваться как данные (например, при копировании исполняемого файла все его команды превращаются в копируемые данные), а данные могут интерпретироваться как команды (именно на этом, к примеру, основаны уязвимости по переполнению буфера, используемые в программных и сетевых атаках). Отсутствие такого различия между данными и командами является одной из основных причин возможности существования компьютерных вирусов. В данном случае корректнее было бы считать программой любое адресное пространство (блок памяти, файл на диске, запись в загрузочном секторе и т.д.), содержащее информацию, так как содержимое любой информации может интерпретироваться как команды.

Для рассматриваемых систем верным является следующее: любому файлу, например содержащему текстовые (файлы с расширениями TXT, LST, DOC, MSG и т.д.) или графические (файлы с расширениями BMP, PCX, GIF, JPG, TIF и т.д.) данные, можно присвоить расширение исполняемого файла (COM, EXE, BAT и т.д.). Такой файл будет воспринят операционной системой как программа, а его содержимое будет воспринято центральным процессором как команды. При этом возможно даже будет получен определJнный результат, например, зависание операционной системы или выдача на консоль случайных символов.

Следует сделать ещJ одно замечание по поводу «цели получения определJнного результата». Существуют программы, определить назначение которых невозможно. Например, программист может сгенерировать случайную программу с целью проверить, насколько успешно эмулятор процессора (эмуляторы процессоров применяются, например, в антивирусных программах) обнаруживает недопустимые инструкции (illegal instructions – англ.). Или другой пример, написание программы для несуществующего процессора (ассемблер Кнута).

В статье 2 в части 2 этого Закона сказано:

Программы для ЭВМ и базы данных относятся настоящим Законом к объектам авторского права. Программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных – как сборникам.

Отсюда следует, что вполне возможно рассуждать в дальнейшем о программах для ЭВМ как о произведениях литературного творчества. Заметим, что в соответствии с определением программы для ЭВМ, компьютерные вирусы являются одной из разновидностью компьютерных программ.

Получается очень интересный юридический казус. Если компьютерный вирус не является программой, то статья 273 УК РФ не может быть применена в силу принципа «запрета аналогии». Если же вирус является программой, то эта статья вступает в противоречие с международными договорами РФ и с еJ Конституцией, образуя запрет на:

- создание литературного произведения;

- использование информации в целях недопустимого ограничения права человека на образование и самообразование (при условии, что вирус создаJтся и используется именно в этих целях);

- распространение информации любыми законными способами.

Некоторые пояснения к определениям можно найти в сети Internet. Например, в работе «Преступления в сфере компьютерной информации» http://vano-zhuk.narod.ru/pravo_ecom.html есть следующие пояснения:

- В соответствии с этой статьJй применительно к статьям о компьютерных преступлениях под компьютерной

информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, то есть совокупность символов, зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). Следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

- ЭВМ (компьютер) – устройство или система (несколько объединенных устройств), предназначенное для ввода, обработки и вывода информации.

- Сеть ЭВМ – совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера, включенного в сеть независимо от его места нахождения.

Хочется заметить, что в теории программирования не говорят о компьютерах, как об устройствах. Существует, например, такое понятие, как машина Тьюринга, являющаяся по существу теоретическим компьютером (теоретическая ЭВМ).

3.4 Вредоносность программ

Законом не оговорены критерии, по которым программы могут быть отнесены к разряду вредоносных, и в законах отсутствует перечень программ, называемых вредоносными. Дать определение термину «вредоносный» в отношении программ не представляется возможным. Дело в том, что вполне «полезные программы» могут нанести вред в результате программных ошибок, как, например, уничтожение информации ранними версиями антивирусной программой DrWeb на дисках инфицированных вирусом OneHalf или уничтожение информации на дисках с файловой системой FAT32 антивирусной программой AidsTest при поиске загрузочных вирусов. «Нейтральные» программы могут в результате неправильного применения нанести не меньший вред, чем троянская программа. Например, при запуске программы FORMAT.COM с определJнными параметрами в командной строке вся информация на диске будет утеряна. И наоборот, отнесенные антивирусными компаниями программы к разряду «вредоносных» могут выполнять не вредные, а полезные действия. Например, описанная в книге Е.В. Касперского «Компьютерные вирусы» [8] в главе «Что такое компьютерный вирус» в разделе «Попытка дать “нормальное” определение», программа KOH, выполняющая действия по защите информации от несанкционированного доступа отнесена к категории компьютерных вирусов.

Сложность заключается ещJ в том, что даже при наличии причинJнного значительного ущерба в результате использования программы, отнести эту программу к разряду вредоносных программ не всегда возможно. Например, в результате интернет-cJрфинга или использования таких программ, как компьютерные игры, на служебном компьютере в рабочее время, может быть нанесJн огромный материальный ущерб (потеря рабочего времени). Более того, массовое обращение пользователей к on-line играм (например, «Пингвин» на странице http://deadman.interdon.net/tmp/penguin.swf или «Закупка в магазине Real» на странице http://www.real.de/set/set.php?cont=gewinnen) может по своим результатам быть схожей с DDoS-атакой[4] на сервера, эти игры распространяющие. Однако обвинять в этом разработчиков браузеров или игр было бы несправедливо.

Как было сказано выше, теоретически возможно, что при переименовании файла данных (например, графический файл с расширением JPG) в файл с расширением COM и его запуска как программы, будут выполнены деструктивные функции (уничтожена информация). Следует ли считать такой файл вредоносной программой, а компьютерного художника привлекать к уголовной ответственности по статье 273 УК РФ?

Кроме того, существуют различные платформы, программы для которых могут быть несовместимы частично или полностью. В результате несовместимости написанная для одной платформы очень полезная программа может выполнить вредоносные (деструктивные) действия при исполнении eJ на другой платформе. Стоит ли называть такие программы «вредоносными»? И наоборот, возможно вредоносная программа для одной платформы будет абсолютно безобидной программой для другой платформы.

Некоторые пользователи называют в качестве критериев вредоносности то, что вирус зря занимает ресурсы (с точки зрения пользователей), и отсутствует контроль над ним (вирус невозможно удалить по желанию пользователя без специальных средств). Однако пользователи не могут назвать пользу от каждого конкретного файла, что лежат на жJстком диске в каталоге ..:Windows или от каждой конкретной программы, которая находится в списке процессов (список видимых процессов можно посмотреть при нажатии комбинации клавиш Ctrl+Alt+Del). Стоит ли считать на этом основании, что эти файлы зря занимают ресурсы (место на диске, блок памяти, время работы ЦПУ и т.д.)? Большинство программ для операционной среды MS

Windows невозможно удалить из системы без специальных средств, называемых деинсталляторами (uninstall – англ.). Имеют ли пользователи контроль над операционной средой MS Windows? Могут ли они удалять по своему желанию компоненты операционной системы MS Windows (например, удалить иконки «рабочий стол», «мусорная корзина», «сетевое окружение», «Internet Explorer»)?

Из приведJнных выше рассуждений становится очевидным, что определение «вредоносность» в проблематике данных вопросов слишком субъективно для того, чтобы его можно было выносить в формулировку уголовного закона.

Компьютерный вирус перестаJт быть самостоятельной программой после внедрения его в файл. Он становится частью той программы, в которую внедрился. При этом сама инфицированная программа не получает возможности самокопирования, а стало быть, вирусом не является. Поскольку в формулировке статьи 273 УК РФ говорится о «вредоносных программах», то такими программами, очевидно, нужно считать все инфицированные программы, если внедрившийся в них вирус несJт в себе деструктивные функции. Наказывать всех авторов (например, при инфицировании вирусом FMRA[5] исходного кода программ) и владельцев инфицированных программ было бы чрезмерно и скорее всего невыполнимо.

Часто «вредоносностью» компьютерного вируса называют выполнение инфицированными программами недокументированных функций. Однако довольно большое количество программ имеет недокументированные функции, и только на этом основании называть их вредоносными нельзя. ВсJ дело в том, что за нанесение ущерба от выполнения программами таких функций ответственность несJт разработчик программы, так как все выполняемые программой функции являются сервисом, получаемым от конкретного производителя. При этом к ответственности можно призвать и за невыполнение контракта – EULA. Вирус (и производимые им действия) не является сервисом, предоставляемым разработчиком программы.

Хотелось бы отметить, что отношение к документированным функциям бывает также неоднозначным. Например, на сайте разработчиков антивирусной компании KAV (http://avp.ru/news.html?id=146070069) сообщается, что «теперь Антивирус Касперского способен распознавать защищенные архивы, осуществлять поиск паролей в тексте электронного письма и проверять такие файлы на наличие вирусов». Возможно эта функция будет очень полезной при нейтрализации вирусных эпидемий, однако подбор паролей к архиву (то есть к частной информации с ограниченным доступом) является по меньшей мере делом неэтичным. Самым неприятным моментом является то, что использоваться эта функция будет на почтовых порталах Internet, то есть, доступ к закрытой конфиденциальной информаци будет осуществляться бесконтрольно, в принудительном порядке, без согласия пользователей. Это очень походит на желание некоторых организаций взять под свой контроль каждый вздох сограждан и может напомнить методы КГБ.

При соблюдении некоторых условий (см. раздел 8), создание, опубликование и использование компьютерных вирусов вообще не представляет общественной опасности, а наоборот позволяет людям осуществить свои права на творчество и образование и реализовать свободу на использование информации. Кроме того, опубликование, использование и распространение компьютерных вирусов позволяет улучшить системы защиты информации, оперативно реагировать на новые угрозы безопасности и вести здоровую конкуренцию в области коммерческого применения средств защиты информации (отсутствие монополии на производство программных систем защиты информации, например, антивирусных программ). Также, изучение компьютерных вирусов позволяет использовать некоторые идеи из них для разработки собственных средств защиты информации (пример с программой KOH из книги Е. Касперского), полиморфные драйвера (используется в программно-аппаратном комплексе Sheriff [http://www.antivirus.ru/Okno5_Sheriff.html], продаваемый фирмой ДиалогНаука [http://www.dials.ru]), программы-архиваторы (пример – ASPack [http://www.aspack.com/]) и др.

Создание и опубликование компьютерных вирусов может также иметь целью проверку надJжности выбранной системы защиты информации. Многолетний опыт публикаций вирусов в электронных конференциях, электронных журналах, печатных изданиях и на WEB-страницах показывает, что эта цель доминирует.

Однако самым главным достоинством опубликования вирусов и распространения информации о них является повышение грамотности пользователей персональных компьютеров. Не секрет, что нашумевшие в последнее время эпидемии компьютерных червей, таких как LoveScan, Sobig или MyDoom, стали возможны только благодаря отсутствию у пользователей персональных компьютеров элементарных знаний в области безопасности.

Кроме того, тотальный перевод создания, использования и распространения компьютерных вирусов в раздел преступлений не может решить проблемы компьютерной безопасности. Дело в том, что люди,

осуществляющие противоправные деяния с помощью компьютерных вирусов, не афишируют свои действия и свои авторские права, так как опасаются справедливого возмездия от пострадавших сторон. Именно поэтому с таким трудом органам правопорядка удаJтся найти компьютерных преступников (и эти случаи единичны) и доказать в судебном порядке их вину. Подавляющее большинство компьютерных преступлений остаJтся нераскрытыми даже в том случае, когда за «голову» создателя вируса, нанесшего колоссальный ущерб, пострадавшие стороны предлагают значительные суммы вознаграждения[6], [7].

3.5. Распространение, опубликование и использование программ для ЭВМ

В законе «О правовой охране программ для электронных вычислительных машин и баз данных» в статье 1 даны следующие определения:

распространение программы для ЭВМ или базы данных – это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей;

выпуск в свет (опубликование) программы для ЭВМ или базы данных – это предоставление экземпляров программы для ЭВМ или базы данных с согласия автора неопределенному кругу лиц (в том числе путем записи в память ЭВМ и выпуска печатного текста), при условии, что количество таких экземпляров должно удовлетворять потребности этого круга лиц, принимая во внимание характер указанных произведений;

использование программы для ЭВМ или базы данных – это выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается использованием программы для ЭВМ или базы данных передача средствами массовой информации сообщений о выпущенной в свет программе для ЭВМ или базе данных.

Здесь следует учитывать, что строго говоря, «распространение» и «опубликование» – два разных понятия. Распространение – это предоставление доступа к программе на материальном носителе (CD, дискете, жестком диске и так далее). Под сетевым способом распространения подразумевается предоставление доступа к работающей программе через специальный протокол. Примерами сетевого распространения могут служить online-проверка пользовательских файлов антивирусной программой DrWeb (http://www.dials.ru/www_av/) через WEB-сервис (в данном случае речь идJт о распространении программы DrWeb), online-перевод текстов с одного языка на другой непосредственно на сервере фирмы PROMT (http://www.translate.ru/) через WEB-сервис (в данном случае речь идJт о распространении программы PROMT), конвертирование текстовых файлов в PDF-формат на сервере фирмы Adobe (https://createpdf.adobe.com/index.pl/1672561531.57312?BP=IE&v=AHP) через WEB-сервис (в данном случае речь идJт о распространении программы Adobe Distiller) и так далее. Поэтому под сетевым распространением вирусов нужно понимать инфицирование пользовательских файлов через WEB-сервис непосредственно на сервере лица, распространяющего вирус. Также под сетевым распространением можно понимать инфицирование файлов на компьютере пользователя при просмотре WEB-сайта лица, распространяющего вирус. Опубликование – это помещение программы (в том числе и исходных кодов) на WEB-странице, в журнале или посылка в конференцию (электронные конференции не являются материальной формой представления информации) в качестве информации.

Опубликование будет являться использованием лишь в том случае, если целью опубликования является введение в оборот опубликованной программы (например, цель публикации для текстового редактора – редактирование текстов получателями; цель публикации троянской программы – воровство паролей, цель публикации компьютерного вируса – инфицирование файлов).

Довольно интересный пример распространения антивирусной компанией вируса приведJн на новостном сайте VIRUSLIST, посвященном компьютерной безопасности (http://www.viruslist.com/index.html?tnews=1001&id=144716956):

01.03.2004. Компания F-Secure разослала клиентам вирус и принесла извинения.

Финский производитель антивирусного программного обеспечения F-Secure принес извинения за массовую рассылку почтового червя Netsky.B (Moodown.b) нескольким тысячам своих клиентов в Великобритании, сообщает сайт Vnunet.com.

«В силу человеческого фактора вы могли получить электронное письмо, зараженное вирусом Netsky.B. Червь был получен нами через внешний почтовый сервер и оказался в списке рассылки для британских клиентов.

Червь вышел не из нашей сети: в список рассылки его направил неизвестный. Если вы уже обновили антивирусные базы, действие Netsky.B в вашей машине уже прекращено», - говорится в тексте официального письменного извинения F-Secure.

3.6. Документ

В законе «Об обязательном экземпляре документов» [9] в статье 1 даны определения следующих понятий: обязательный экземпляр документов; документ; система обязательного экземпляра; обязательный бесплатный экземпляр; обязательный платный экземпляр; обязательный бесплатный федеральный экземпляр; обязательный экземпляр субъекта Российской Федерации; обязательный бесплатный местный экземпляр; производитель документов; получатель документов; национальный библиотечно-информационный фонд Российской Федерации. ПриведJм одно из таких определений:

документ – материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования.

Поскольку компьютерная информация не является материальным объектом, то, вероятно, eJ нельзя рассматривать в качестве документа (следовательно, нельзя использовать в суде в качестве доказательства вины). К сожалению, в законах не дано определение термина «зафиксированность информации». Вероятно, здесь следует понимать, что зафиксированной является такая информация, которая становится частью материального носителя и не может быть модифицирована или удалена с него без того, чтобы материальный носитель не потерял хотя бы часть своих свойств. Примером такой фиксации информации, возможно, следует считать проявленные фото- и киноплJнки, фотографии, отображJнные специальной краской на бумаге тексты и изображения, перфокарты и перфоленты, распечатки исходных текстов программ, прожигание не перезаписываемых CD-дисков и т.д. Если это верно, то нельзя назвать фиксацией временное хранение информации в оперативной памяти компьютера, на перезаписываемых материальных носителях, которыми являются микросхемы с флэш-памятью, гибкие магнитные диски (дискеты), жJсткие магнитные диски (винчестеры), перезаписываемые CD-диски и т.д.

В законе «Об участии в международном информационном обмене» [10] в статье 2 можно найти следующие определения: документированная информация; конфиденциальная информация; массовая информация; информационные ресурсы; информационные продукты (продукция); информационные услуги; собственник документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена; владелец документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена; пользователь (потребитель) информации, средств международного информационного обмена; информационные процессы; международный информационный обмен; средства международного информационного обмена; информационная сфера (среда); информационная безопасность. ПриведJм одно из них:

документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

Другими словами, если опустить замечания к предыдущему определению, то любая WEB-страница (страница имеет адрес, имя файла и дату последней модификации[8]) могла бы являться документом при условии принятия закона об электронной подписи и содержании WEB-страницой такой подписи. В настоящее время невозможно утверждать даже то, что страница принадлежит владельцу сайта[9] (эту страницу мог создать или модифицировать владелец хоста[10], или эта страница была создана или модифицирована злоумышленниками). Сообщение в электронной конференции также могло бы являться документом, тем более что оно имеет реквизиты (номер сообщения, дату, путь прохождения, данные об авторе), если бы было защищено электронной подписью автора, подлинность которой можно было бы подтвердить.

Таким образом, в качестве документа возможно использовать лишь ту компьютерную информацию, которая стала частью материального носителя и при этом имеет такие идентификационные признаки, подлинность которых можно было бы подтвердить (например, доказать авторство информации). Любая другая информация документом не является. Исключение могут составлять лог-файлы, отчJты и прочая информация из сертифицированных систем.

ПРОДОЛЖЕНИЕ

Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ, МИР 12866 31.03.2004, 13:16 298
URL: https://babr24.com/?ADE=12257 Bytes: 49233 / 49032 Версия для печати Скачать PDF