Автор: Артур Скальский ИНТЕРНЕТ, МИР 21368 31.03.2004, 13:14 298

Права вирмейкера как человека и гражданина - часть 3.

5.4. Принцип несанкционированности действий

ПриведJм ещJ один пример попытки дать определение термину «компьютерный вирус» на странице Регионального Представительства Лаборатории Касперского в Санкт-Петербурге и области (http://www.comprice.ru/virus/main34.phtml). Здесь можно найти следующие определения: программы-вандалы; троянские программы; троянские программы-вандалы; компьютерный вирус и стандартные COM-EXE-TSR-вирусы.

- Формально компьютерным вирусом называется программа, заражающая другие программы путем включения в них своей, возможно модифицированной, копии, способной к дальнейшему размножению. Зараженная вирусом программа может рассматриваться как автоматически созданная троянская программа. При этом, скрытым модулем является тело вируса, а одним из несанкционированных действий – заражение других программ. Кроме заражения, вирус, как и любая другая троянская программа, может выполнять и другие несанкционированные действия – от вполне безобидных, до крайне разрушительных, вплоть до уничтожения данных на зараженном диске. В этом случае вирус может рассматриваться как логическая мина.

Согласиться полностью с этим определением также невозможно. Дело в том, что существуют вирусы, не изменяющие инфицируемую программу ни на один байт. Кроме того, вирусы могут инфицировать и другие объекты, например, звуковые файлы, графические файлы, картографические данные и т.д., то есть объекты, которые программами не являются. Вирусы получают возможность к существованию благодаря ошибкам в программах (вьюверах, плеерах, ...) для работы с этими файлами.

Примером вируса, не внедряющего в инфицируемую программу никаких копий, являются компаньон - вирусы. Кроме того, такие вирусы могут не изменять ни на байт инфицируемую программу. Например, COM-вирус производит поиск на диске EXE-файлов (BAT-файлов) и записывается рядом с ними с именем инфицируемого файла, но с расширением COM. РасчJт на то, что при вызове инфицированного файла через командную строку без расширения (только по имени), операционная система вызовет программу с расширением COM, которая выполнит свои действия, а уж затем сама вызовет на исполнение EXE-программу (BAT-файл).

Инфицированная программа может рассматриваться только как «больная вирусом» программа и никак иначе. В случае инфицирования eJ вырожденной формой вируса – перезаписывающимся вирусом (Overwrite – запись поверх чего-либо, англ.), программа уничтожается. Только в случае такого рода вирусов, их можно отнести к троянским программам

Хотелось бы подчеркнуть, что вирус, как и абсолютно любая другая программа, может выполнять на компьютере действия, как санкционированные, так и несанкционированные пользователем. Кто может санкционировать или не санкционировать все действия операционной системы MS Windows ? Каким образом можно санкционировать каждое действие из цепочки действий, выполняемых любой программой, если пользователь не имеет даже представления о том, какие действия выполняет программа, насколько обоснованны эти действия (оптимизация) и насколько они безопасны для информации, хранимой на компьютере? Кто возьмJтся хотя бы перечислить все действия, выполняемые операционной системой в каждый конкретный промежуток времени?

Пример. При работе с программой MS Word происходит ошибка. Операционная система MS Windows выгружает приложение MS Word из памяти и при этом не сохраняет созданный или отредактированный пользователем документ. Пользователь теряет информацию (информация уничтожается). Санкционировал ли пользователь действия MS Windows? Скорее всего нет. Но и действия операционной системы и результат этих действий в точности совпадает с тем описанием, которое приведено в рассматриваемой публикации для троянских программ. Можно ли считать в таком случае операционную систему Windows «логической миной»?

Существуют и другие попытки дать определение термину «компьютерный вирус». Например, очень много информации на эту тему можно получить из вирусной энциклопедии (http://www.viruslist.com/default.asp). Однако следует учитывать, что каждый рассматриваемый случай определения компьютерного вируса будет выражать только субъективное мнение авторов, с которым всегда можно поспорить.

5.5. Принцип полезности и троянские программы

Так что же такое «компьютерный вирус»? Автор настоящей работы не берJт на себя смелость дать хоть какое-нибудь определение этого термина. Известно лишь, что возможным прародителем современных компьютерных вирусов явилась однобайтовая команда языка Ассемблер MOVSB[20]. Команда эта выполняет единственную функцию – пересылает байт информации из одного участка компьютерной памяти в другой. При определJнных значениях в регистрах процессора эта команда может перенести саму себя в такое место памяти, которое снова будет выполнено процессором. Дальнейшие развитие этого эффекта привело к появлению самораспространяющихся программных механизмов (СМ). СМ стали самостоятельно подготавливать такие ситуации, при которых они гарантированно были бы скопированы и копия СМ гарантированно была бы исполнена. Под самокопированием следует понимать стремление уменьшить влияние пользователя на процесс создание дубликата СМ. Так появились самые старые представители компьютерных вирусов – черви. Самый знаменитый из них был создан и запущен в компьютерную сеть 2-го ноября 1988 года аспирантом Корнеллского университета по имени Роберт Таппан Моррис [17]. В дальнейшем СМ стали осваивать другие объекты для самораспространения (загрузочные сектора, программы, драйвера, документы с макрокомандами и др.) и заботиться о том, чтобы как можно дольше оставаться в инфицированной ими системе. Для этого они стараются не конфликтовать с программным обеспечением и устройствами компьютера; скрывают своJ присутствие, например, за счJт манипуляции функциями операционной системы; шифруют собственное тело и включают в свой код приJмы, мешающие их исследованию с помощью штатных отладочных средств. Классификации компьютерных вирусов основываются на различных свойствах вирусов. Существуют разделения вирусов в зависимости от среды обитания (файловые вирусы, почтовые черви, архивные черви, загрузочные вирусы, резидентные вирусы, макровирусы и др.). Существуют разделения вирусов в зависимости от второстепенных признаков (шифрованные, полиморфные, невидимки и др.). При осваивании вирусами новых сред обитания, появились и новые классы вирусов (Win32-вирусы, Linux-вирусы, Script-черви и др.), в том числе и «многоплатформенные» вирусы. Всех их объединяет только одно – стремление к самокопированию. Все остальные функции (полиморфизм, невидимость, визуальные эффекты, звуковые эффекты, наличие троянских компонент в коде, текстовые сообщения в коде, реакции на события таймера и др.) являются второстепенными и не характеризуют вирусы в качестве СМ. Второстепенными функциями могут вполне обладать абсолютно любые программы. Например, никто не мешает создать графический редактор, который бы при исполнении становился невидимым, в 17:00 проигрывал бы мелодию, а его работающая копия в оперативной памяти менялась бы от запуска к запуску (была бы полиморфной). Кроме того, вирусы, несущие в себе деструктивные функции, составляют всего несколько процентов от общего количества СМ.

Таким образом, компьютерный вирус является обычной безвредной программой, служащей хорошим стимулом для своего автора к изучению тонкостей работы операционной системы и устройств компьютера, а также возможностью померяться интеллектом с разработчиками антивирусных программ (своего рода шахматная партия). Хорошо сделанные вирусы содержат в себе результаты изучения их авторами программного обеспечения и устройств компьютера, реализованные идеи и алгоритмы, концепции освоения новых объектов для обитания, способы оптимизации кода и многое другое, представляющее собой красоту программистской мысли и ценность как литературное произведение для посвященных людей. Поэтому такие вирусы часто становятся предметом коллекционирования (вид электронного нумизмата или филателизма) и обмена. Это всJ ещJ раз подчJркивает, что запрет на создание и распространение компьютерных вирусов не имеет под собой основания. Боязнь перед компьютерными вирусами, вероятно, вызвана только невежеством простых пользователей и отсутствием разъяснительной работы со стороны вирмейкеров (вероятно из-за страха быть осужденными по статье 273 УК РФ). Кроме того, не последнюю роль играет спекуляция термином «компьютерный вирус» средствами массовой информации и антивирусными компаниями. ВсJ это приводит к ещJ большему невежеству пользователей и угрозе компьютерной безопасности (человек всегда останется самым слабым звеном в любой системе защиты, а неграмотный человек все усилия по защите сведJт к нулевому результату), а также необоснованному наказанию программистов, реализующих свои права на творчество, образование, создание архивов (коллекций) и др.

Отдельным вопросом следует рассмотреть лишь троянские компоненты кода. Эти компоненты не относятся к СМ по определению (не обладают свойством делать свои дубликаты). Автор настоящей работы не берJтся судить, но возможно родоначальником современных троянских компонент были обычные ошибки в

операционной системе MS DOS и сервисные программы, выполняющие штатные действия по форматированию дисков (первые троянские программы на персональных компьютерах имитировали ошибки операционной системы и работу программы FORMAT.COM), санкционированному блокированию устройств компьютера (закрытие дисководов для невозможности несанкционированного копирования информации) и др., а также пресловутые «логические бомбы», встраиваемые нечистоплотными программистами в свои программы. Развиваясь, такие компоненты стали сами содержать все необходимые функции для уничтожения информации, блокированию устройств компьютера, воровству информации и др., а также стали появляться не просто компоненты, а целые программы, предназначенные исключительно для совершения преступлений. Однако в большинстве своJм эти компоненты и программы не представляют собой ничего необычного. Для выполнения своих разрушительных функций они используют штатные средства операционной среды, других программ и языков программирования, которые (штатные средства) известны каждому программисту. В данном случае было бы неправильно карать программистов только за использование всех этих средств (эти средства используются также для разработки вполне полезных программ), но следует карать за использование этих средств для нанесения вреда.

В одной и той же программе могут находиться разные подпрограммы, выполняющие разные функции: «полезные», «бесполезные» и «вредные». Функции, выполняемые конкретной подпрограммой, могут быть отнесены в любую из этих категорий в зависимости от ситуации. Так, например, «полезные» действия, могут оказаться «вредными». Однако практически у каждой программы можно выделить главную (основную) функцию (речь не идJт о конкретной подпрограмме). Например, главная функция операционной системы – обеспечить выполнение компьютером заложенных в пользовательские программы операций, главная функция вируса – саморазмножение, главная функция троянской программы – нанесение вреда, главная функция текстового редактора – редактирование текстовых файлов, главная функция музыкальной программы – воспроизведение музыкальных композиций. Автору кажется наиболее правильным выделять основную функцию каждой рассматриваемой программы для того, чтобы можно было правильно отнести eJ к тому или иному классу программ. Технология и критерии выделения главной функции программы являются отдельным большим вопросом, выходящим за рамки настоящей работы. Однако не следует путать понятие «главная функция» с понятием «использование программы». Так, например, существуют программы двойного назначения (twinware – англ.), главная функция которых может быть применена как на пользу, так и во вред компьютерному сообществу. Ярким примером таких программ являются сканеры открытых портов или сканеры сетевых уязвимостей.

5.6. Компьютерная программа

По отношению же к компьютерным вирусам, как к программам для ЭВМ вполне применимы следующие законы:

- Авторское право распространяется на любые программы для ЭВМ и базы данных, как выпущенные, так и не выпущенные в свет, представленные в объективной форме, независимо от их материального носителя, назначения и достоинства[21].

- Автору программы для ЭВМ или базы данных или иному правообладателю принадлежит исключительное право осуществлять и (или) разрешать осуществление следующих действий[22]:

§ выпуск в свет программы для ЭВМ или базы данных;

§ воспроизведение программы для ЭВМ или базы данных (полное или частичное) в любой форме, любыми способами;

§ распространение программы для ЭВМ или базы данных;

§ модификацию программы для ЭВМ или базы данных, в том числе перевод программы для ЭВМ или базы данных с одного языка на другой;

§ иное использование программы для ЭВМ или базы данных.

- Объектами авторского права являются: литературные произведения (включая программы для ЭВМ)[23].

- Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в том числе на операционные системы, которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код[24].

- Автору в отношении его произведения принадлежат исключительные права на использование произведения в любой форме и любым способом[25].

По отношению к опубликованию вируса в электронной конференции или на WEB-странице вполне применимо следующее законодательство:

- Воспрепятствование осуществляемому на законном основании распространению продукции массовой информации со стороны граждан, объединений граждан, должностных лиц, предприятий, учреждений, организаций, государственных органов не допускается[26].

- Контролируют осуществление международного информационного обмена федеральные органы исполнительной власти и органы исполнительной власти субъектов Российской Федерации в пределах своей компетенции, определяемой законодательством Российской Федерации[27].

- Производители документов обязаны доставлять обязательный бесплатный экземпляр получателям документов бесплатно[28].

6. Пояснения к российскому законодательству в сфере компьютерных преступлений

Из формулировки статьи 273 УК РФ не становится ясным, каков принцип определения цели написания программы («специально разработанные»), и какова совокупность критериев для отнесения программ к разряду вредоносных. Очевидна большая разница между понятиями «умение создавать вирусы» и «желание создавать вирусы для совершения преступного деяния». Если человек не высказывает никакой цели, сообщает о цели научиться писать вирусы (но не высказывает при этом желания совершать с помощью вирусов преступления) или говорит о желании разобраться в написании вирусов, то его цель не может содержать состава преступления. Позволю себе аналогию: желание научиться стрелять из пистолета не является преступлением, а желание научиться стрелять из пистолета для совершения убийства – содержит состав преступления.

Как известно из статьи 15 части 1 Конституции РФ:

Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.

Следовательно, нельзя применять эту статью к людям создающим компьютерные вирусы и использующим их в образовательных, научных и иных законных целях (если не будет доказано обратное) даже в том случае, если вирус можно будет назвать «вредоносной» программой. На то, что должны быть такие исключения в части использования указывает хотя бы то, что создание антивирусных программ без использования компьютерных вирусов не представляется возможным. Что касается опубликования компьютерного вируса сетевыми способами, то влияние статьи 273 УК РФ на это деяние не распространяется и само это деяние является правом человека, обеспеченным международными договорами и Конституцией РФ. Даже в случае «распространения» компьютерных вирусов должны быть исключения, иначе передача пользователями вирусов в антивирусные компании становится преступлением. Кроме того, становится невозможным противостоять эпидемиям компьютерных вирусов в мировом масштабе без обмена вирусами между антивирусными компаниями (фактически – распространение). К сожалению, особые условия (исключения) нигде в законах не оговорены. Если такие особые условия будут предусмотрены в будущем, то было бы неправильным сделать их исключениями только для антивирусных компаний. Закон не должен ограничивать доступ к информации по компьютерным вирусам, так как такое ограничение нанесло бы вред безопасности самих пользователей (основная причина мировых эпидемий вирусов – неграмотность пользователей).

Кроме того, разработка антивирусных программ, как и любых других программ (например, операционных систем), не является исключительным правом конкретных фирм (таких как САЛД или ЛК). Поскольку антивирусная программа не является вредоносной (с точки зрения законодательства), то любой человек имеет право создавать, использовать и распространять антивирусные программы, отличные от предлагаемых на рынке конкретными фирмами (например, DrWeb или KAV). Однако, как было сказано выше, разработка антивирусных программ без использования компьютерных вирусов не представляется возможной.

Неофициальные разъяснения к статьям 272, 273 и 274 можно найти в работе «Преступления в сфере компьютерной информации» (http://download.referat.su/15856.zip):

- Важным является наличие связи между несанкционированным доступом и наступлением предусмотренных статьей 272 «Неправомерный доступ к компьютерной информации» УК РФ последствий, поэтому простое

временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями и программными ошибками и неправомерного доступа не влечет уголовной ответственности.

- Под созданием вредоносных программ в смысле статьи 273 «Создание, использование и распространение вредоносных программ для ЭВМ» УК РФ понимаются программы специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу.

- Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым.

- Применение статьи 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» УК РФ невозможно для Internet, ее действие распространяется только на локальные сети организаций.

- Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты.

- Компьютерная программа отличается от вещей и материальных активов главным образом тем, что поддается свободному копированию, не теряя ни грамма своих свойств при этом.

- Каждый пользователь имеет право использовать только тот программный продукт, который он получил на основании договора либо приобрел путем покупки, взял в аренду или в прокат и т.д.

- Овладение компьютером, не имеющим источников питания, а также машинным носителем информации как вещью, не рассматривается как доступ к компьютерной информации и в соответствующих случаях может повлечь ответственность по статьям о преступлениях против собственности. Точно так же не образует объективной стороны данного преступления уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитным излучением, ударами и иными подобными способами.

- Также стоит упомянуть о том, что правила обращения с компьютерной информацией могут устанавливаться собственником либо владельцем информации, …

7. Некоторые примеры применения уголовного законодательства РФ в компьютерной сфере

В статье «ФСБ поймала хакера, который качал секретные данные» (http://www.securitylab.ru/44098.html) есть упоминание: «Из наиболее известных случаев можно вспомнить событие почти годичной давности, когда в подмосковных Мытищах был задержан двадцатилетний хакер, взломавший сайт местного узла связи. Молодой человек более месяца осуществлял незаконный доступ в международную компьютерную сеть Интернет. В результате этого в систему был занесен компьютерный вирус».

Остается непонятным, в результате чего был занесен компьютерный вирус? В результате того, что человек больше месяца имел доступ в сеть? В результате того, что он имел доступ в сеть? В результате того, что доступ был незаконным? В результате того, что доступ был в сеть Интернет? В результате того, что сеть Интернет является международной? Ни одно из этих обстоятельств не является действительной причиной для заражения сайта того узла связи компьютерным вирусом. Действительные преступления молодого человека: взлом сайта, неправомерный доступ к сети и информации. Ни одно из этих деяний к вирусам не имеет никакого отношения. К заражению вирусом данного узла связи может иметь отношение лишь безответственность системного администратора, оставившего сайт беззащитным перед лицом компьютерной угрозы (осуществлJн взлом сайта и осуществлено заражение вирусом).

В статье «В России впервые осужден создатель вируса для кассового аппарата» (http://securitylab.ru/36142.html) приведена ещJ более безумная история: «Следствием установлено, что программа, созданная Эрзяйкиным, позволила изменять и обнулять данные по выручке, которые хранились в фискальной памяти контрольно-кассовых машин, изменять дату, количество покупок… Они (сотрудники МВД – прим. автора) купили у Эрзяйкина процессор за 300 долларов и после того, как он продемонстрировал программу в работе, его задержали».

Описанные функции программы скорее относят еJ к троянской программе, чем к вирусу, так как ничего не сказано о возможности этой программы к самораспространению. Более того, непонятно, зачем было покупать сотрудникам МВД целый процессор. Неужели вирус представляет собой самокопирующийся процессор?

Возникает подозрение, что компьютерные вирусы здесь абсолютно ни при чJм.

В статье «Создатель компьютерных вирусов осужден в Магадане (http://www.securitylab.ru/44100.html) приведено два уголовных дела. В одном житель Магадана осуждJн за незаконное копирование и распространение справочной юридической программы «Консультант-Плюс». Во втором другой житель Магадана хранил в зашифрованном виде файлы, содержащие информацию о пароле и имени пользователя (вероятно это были логин и пароль пользователя программы «Консультант-Плюс» - прим. автора). Какое отношение к незаконному копированию и распространению программы «Консультант-Плюс» имеют компьютерные вирусы? Каким образом наличие у конкретного человека имени пользователя и пароля к программе «Консультант-Плюс» свидетельствует о том, что он является создателем вируса? Может быть с помощью программных средств (один из видов троянских программ – перехватчик клавиатуры) были получены имя зарегистрированного пользователя и пароль? Но какое это имеет отношение к СМ? Наиболее вероятным кажется использование одним из жителей Магадана троянской программы для незаконного получения личных данных зарегистрированного пользователя.

В новостях (http://www.webplanet.ru/news/lenta/2002/8/26/1459.html) приведен следующий пример:

- Суд Советского района Томска вынес обвинительный приговор двум местным жителям за распространение в интернете компьютерных вирусов типа «троянский конь», сообщает Интерфакс.

Здесь явно видно, что перепутаны понятия «вирус» и «троянская программа».

Вывод из приведJнных примеров может быть сделан только один: неграмотность и некомпетентность людей порождает негативное отношение ко всему, что им непонятно. И самое ужасное в том, что на почве этой неграмотности возникают нездоровые спекуляции со стороны действительно компетентных лиц, которыми являются представители антивирусных компаний.

В статье «ФСБ впервые возбудило уголовное дело по обвинению в распространении компьютерного вируса» (http://www.fsb.ru/smi/ufsb/2000/000428-2.html) действительно правдоподобная история: «По информации спецслужб, А. Ялькин, работая в отделе информационных систем одного из ООО Кирова, создал вредоносную программу, которая приводила к сбоям работы ЭВМ и локальной компьютерной сети. По данным следствия, А. Ялькин установил программу на сервере фирмы и каждый, кто входил на сервер, получал компьютерный вирус».

Это действительно похоже на правду. И преступные деяния подпадают не только под формулировку статьи 273 УК РФ, но и под формулировку статьи 274 УК РФ. Однако, по неподтверждJнным данным, Ялькин был полностью оправдан на суде из-за отсутствия состава преступления.

В новостях (http://www.kompas.ru/news.asp?ID=821) также можно найти следующее: «Однако, в отличие от товара обыкновенных „пиратов“, CD-ROM, которые распространяли задержанные, содержали программы взлома систем защиты компьютерных сетей и различные вирусы».

Очень похоже на правду. Однако удручает неграмотность журналиста. Сами по себе CD-ROM не могут содержать никаких программ, тем более вирусов, так как являются устройствами для чтения дисков. (подобным устройством для чтения дискет является дисковод). Вероятно журналист имел ввиду CD-диски (компакт-диски).

Вот ещJ интересное дело (http://www.decopro.ru/?m=6&&nid=187&&t=2): «Российская контрразведка обвинила сотрудника ФБР США в несанкционированном проникновении в российские компьютерные сети, сообщает NTVRU.com. В отношении агента ФБР США Майкла Шулера было возбуждено уголовное дело по статье 272 часть 2 Уголовного кодекса РФ (несанкционированный доступ к компьютерной информации). Дело было возбуждено по инициативе следователя УФСБ РФ по Челябинской области Игоря Ткача».

Жаль, что неизвестны подробности дела. К какой именно компьютерной информации несанкционированно получил доступ агент ФБР США? Зачем ему это понадобилось? Каким образом он был уличJн в преступлении и как УФСБ РФ по Челябинской области выяснило персональные данные агента ФБР США. Чем закончилось следствие?

Не стоит безоговорочно верить таким, даже правдоподобным, сообщениям. Вот пример опровержения (http://www.strana.kaliningrad.ru/N111/oproverjenie.html) такой новости: «В прошлом номере нашей газеты под заголовком „Тихо! Враг подслушивает!“ была опубликована заметка, в которой сообщалось, что против двух сотрудников областной администрации были возбуждены уголовные дела по статье 273 Уголовного кодекса

РФ „разглашение государственной тайны“. К сожалению, эта информация неверна. На самом деле уголовные дела по этой статье были возбуждены в Калининградской области в 2000 – 2001 годах против руководителей неких предприятий, не имеющих отношения к обладминистрации. Как нам стало известно, один из них был даже осужден, но попал под амнистию».

Очень много информации подобного рода можно найти на сайте работника прокуратуры Алексея Сорокина (http://www.zaural.ru/procur/my_page.htm). Стоит заметить однако, что компетентные лица в области компьютерной безопасности не могут воспринимать серьJзно приведJнные там материалы.

8. Правила безопасности при опубликовании вирусов

Проанализировав приведJнную в данной работе информацию, можно сказать, что при осуществлении деяний, вероятность отнесения которых к общественно опасным очень высока, следует придерживаться следующих правил, выполнение которых позволяет избежать уголовной ответственности при создании, использовании и распространении компьютерных вирусов:

- предпринимать все возможные меры предосторожности;

- переложить ответственность за возможные последствия на плечи того, кто может умышленно совершить действительно общественно опасное деяние на основании использования предоставленной информации.

Суть этих правил при публикации исходного или исполняемого кода вируса заключается в следующем:

- Необходимо оценить, насколько высока вероятность возможного вреда от прямого использования публикуемого вируса без дополнительной модификации или уточнения. Это может следовать, например, из того, что вирус был распространJн до появления рассматриваемой публикации. В этом случае пользователи ЭВМ уже должны были предпринять все необходимые меры безопасности, а антивирусные компании уже должны были включить этот вирус в свои базы.

- В случае публикации собственного вируса необходимо заранее собственноручно разослать его антивирусным компаниям и желательно дождаться выхода обновлений антивирусных программ. В случае игнорирования антивирусными компаниями посланного им вируса можно обвинить их в преступном бездействии.

- Если возможно, то перед публикацией следует привести публикуемый вирус в нерабочее состояние, чтобы любое его использование без дополнительной модификации было невозможно. Однако требовать этого в обязательном порядке нельзя, как нельзя требовать наличие трусиков у Галины[29] на картинах Сальвадора Дали[30].

- Публикация должна быть сопровождена соответствующими текстами, в которых получателям информации должно быть сообщено, что это – вирус. Также в сопровождении должны быть указаны условия использования публикуемого вируса (для исследовательских целей, для самообразования пользователей, для разработки антивирусной программы и т.д., то есть для того, что не может считаться общественно опасным деянием) и напоминание о том, что недопустимо использование вируса в противозаконных целях.

- Чтобы гарантировать попадание публикуемого вируса только в руки вменяемых, грамотных лиц, способных прочитать сопроводительную информацию и адекватно на неJ реагировать, следует упаковать публикуемый вирус архиватором и использовать при этом пароль (текст пароля должен содержать такое количество символов, которое бы исключало возможность случайного набора). Сообщить этот пароль необходимо отдельно (например, в отдельном документе или в сопроводительной информации). Дополнительно такой приJм обезопасит людей, использующих почтовую программу или браузер, которые могут в силу различных причин исполнить автоматически любой обнаруженный код (на странице в Internet или в прилагаемом к Email приложении).

- Публикацию вирусов следует осуществлять в специализированных местах (специализированных конференциях или журналах), сводящих к минимуму вероятность попадание вируса в руки человека, не имеющего никакого представления о том, что ему в руки попало.

Все эти действия докажут, что были предприняты все меры предосторожности для того, чтобы публикация даже вредоносной программы перестала в силу «малозначительности» представлять общественную опасность, а действия автора публикации перестали быть преступлением. Ответственность за последствия от противозаконного применения опубликованного вируса будут определяться Федеральным Законом РФ «Об

информации, информатизации и защите информации». Например, в статье 22 часть 3 сказано:

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Таким образом, в случае исполнения всех условий, нельзя будет утверждать, что публикация имела своей целью введение вредоносной программы в оборот (в случае, если считать вирусы вредоносными программами), то есть имела целью нанесение вреда и осуществления общественно опасных деяний. Следовательно, такое опубликование не будет отвечать определению «использование программы». Кроме того, деяние, называемое «опубликованием» не подпадает под действие статьи 273 «Создание, использование и распространение вредоносных программ для ЭВМ» Уголовного Кодекса РФ даже в том случае, если будет доказано, что конкретный вирус является вредоносной программой.

Обязательное условие опубликования вирусов в виде архивов с паролем и описанием (включая «условия использования» как порядок использования) не просто является смягчающим обстоятельством, а целиком снимает ответственность с автора публикации за возможное использование содержимого архива в преступных целях. Это положение содержится в статье 20 Закона «Об Архивном фонде Российской Федерации и архивах»:

пользователи архивных документов несут ответственность за их использование и сохранность в установленном порядке.

9. Список использованных источников

1. Всеобщая Декларация Прав Человека. (http://www.unhchr.ch/udhr/lang/rus.htm)

2. Конституция Российской Федерации. (http://constitution.garant.ru/DOC_10003000_sub_para_N_1000.htm)

3. Strafgesetzbuch (StGB), 36 Auflage, München: Beck - Texte im Deutscher Taschenbuch Verlag, 2001.

4. Bürgerliches Gesetzbuch (BGB), 47, überarbeitete Auflage, München: Beck - Texte im Deutscher Taschenbuch Verlag, 2000.

5. Council of Europe, Convention on cybercrime (http://icpo-vad.tripod.com/mzhru.html)

6. Уголовный Кодекс Российской Федерации. (http://www.d-sign.ru/uk/)

7. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 года N 3523-I (http://wbase.duma.gov.ru/ntc/vdoc.asp?kl=8770)

8. Е. Касперский, «Компьютерные вирусы». (http://viruslist.com/viruslistbooks.html)

9. Федеральный закон Российской Федерации «Об обязательном экземпляре документов» от 23 ноября 1994 года (подписан Президентом 29 декабря 1994 года) N 77-ФЗ (http://gdm.ru/normativ/77-fz_291194.htm)

10. Федеральный закон Российской Федерации «Об участии в международном информационном обмене» от 5 июня 1996 года (подписан Президентом 4 июля 1996 года) N 85-ФЗ (http://www.fips.ru/npdoc/law/INFO.HTM)

11. Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» от 25 января 1995 года (подписанный Президентом 20 февраля 1995 года) N 24-ФЗ (http://www.gmd.ru/normativ/24-fz_250195.htm)

12. Закон Российской Федерации «О средствах массовой информации» от 27 декабря 1991 года N 2124-I (http://wbase.duma.gov.ru/ntc/vdoc.asp?kl=8693)

13. Закон Российской Федерации «Об авторском праве и смежных правах» от 9 июля 1993 года N 5351-I (http://wbase.duma.gov.ru/ntc/vdoc.asp?kl=8892)

14. Основы законодательства Российской Федерации “Об Архивном фонде Российской Федерации и архивах” от 7 июля 1993 года (http://ascomplect.ru/indexphp?cat=5&topcat=5&doc=49)

15. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 года N 5485-I (http://wbase.duma.gov.ru/ntc/vdoc.asp?kl=8900)

16. Физико-биологические основы информационных процессов в живом веществе /Е.И. Нефедов, А.А. Протопопов, А.А. Хадарцев, А.А. Яшин; Под редакцией А.А. Яшина. – Тула: Изд-во ТулГУ, 1998. – 333 с.

17. Д. Маркоф, К. Хефнер. Хакеры. Повести. Полиграфкнига, Киев, 1996. -360 с.

[1] Фрэд Коэн учился в USC (University of Southern California), затем преподавал в Лехайском университете

[2] Преподаватель по компьютерной безопасности, профессор Len Adleman (http://www.usc.edu/dept/molecular-science/fm-adleman.htm)

[3] См. например, описание к вирусу Micro-66 в файле AIDSVIR.TXT из архива ftp://ftp.dials.ru/dsav/russian/aidstest.zip

[4] DDoS-атака – от английского «Distributed Denial of Service Attack»

[5] Электронный журнал MooN BuG #9, декабрь 1998 (http://vx.netlux.org/vx.php?id=zm03)

[6] Microsoft предлагает $250 тыс. за сведения об авторе вируса MyDoom.B (http://www.cpv.ru/news/References/30011213.html)

[7] SCO предлагает 250 000$ за голову автора вируса Mydoom (http://introweb.ru/inews/news1223.php)

[8] Адрес страницы, имя файла и дата последней модификации могут быть изменены без того, чтобы можно было зафиксировать эти изменения. Модификация этих данных не требует глубоких знаний или специальных инструментов.

[9] WEB-сайтом (site – англ.) называется набор логически связанных между собой WEB-страниц

[10] Хост (host - англ) – компьютер (сервер), на котором располагаются WEB-сайты

[11] Например, в соответствии с релятивистской теорией, базой данных называется любая группа файлов (обычно расположенных в отдельном каталоге на диске), содержащих однотипную информацию. Такие файлы называются таблицами (table – англ.). Таблицы состоят из записей (record – англ.), которые в свою очередь состоят из полей записи (field – англ.).

[12] ACG - Amazing Code Generator (http://www.viruslist.com/viruslist.html?id=52)

[13] VCG – Virus Code Generator (http://www.viruslist.com/viruslist.html?id=2495)>

[14] RMNS.MW (http://www.viruslist.com/viruslist.html?id=1974)

[15] Win95.Babylonia (http://www.viruslist.com/viruslist.html?id=4030)

[16] Вспомните: „Это картина о художниках, чью выставку в Манеже буквально разгромил Хрущев, о тех, чьи работы давили бульдозерами при Брежневе“ (http://rodalin.ru/people/redel/inerview-01.shtml)

[17] И.С. Барков (http://pathology.dn.ua/Humor/Barkov/Barkov.shtml)

[18] Черный супрематический квадрат (http://www.agniart.ru/rus/item-16693~Art-prints-on-canvas~Malevich-Kazimir~Black-Superematist-Square-Art-print-on-canvas)

[19] К.С. Малевич (http://www.allabout.ru/a11131.html)

[20] Питер Абель. Ассемблер и программирование для IBM PC (http://www.moshkow.pp.ru/CTOTOR/IBMPC/abel.txt)

[21] Закон «О правовой охране программ для электронных вычислительных машин и баз данных», статья 3.

[22] Закон «О правовой охране программ для электронных вычислительных машин и баз данных», статья 10.

[23] Закон «Об авторском праве и смежных правах», статья 7 часть 1.

[24] Закон «Об авторском праве и смежных правах», статья 7 часть 2.

[25] Закон «Об авторском праве и смежных правах», статья 16 часть 1.

[26] Закон «О средствах массовой информации», статья 25.

[27] Федеральный Закон «Об участии в международном информационном обмене», статья 16.

[28] Федеральный Закон «Об обязательном экземпляре документов», статья 6 часть 1.

[29] Небольшая выставка знаменитого художника (http://www.peterlink.ru/misc/dali/chose.html)

[30] Мир Сальвадора Дали (http://daliworld.narod.ru/)

Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ, МИР 21368 31.03.2004, 13:14 298
URL: https://babr24.com/?ADE=12255 Bytes: 37472 / 37379 Версия для печати Скачать PDF

Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com