Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ, МИР 4610 31.03.2004, 13:15 386

# Права вирмейкера как человека и гражданина - часть 2.

**3.7. Информация**

В законе «Об информации, информатизации и защите информации» [11] в статье 2 можно найти следующие определения: информация; информатизация; документированная информация (документ); информационные процессы; информационная система; информационные ресурсы; информация о гражданах (персональные данные); конфиденциальная информация; средства обеспечения автоматизированных информационных систем и их технологий; собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения; владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения; пользователь (потребитель) информации. ПриведJм некоторые из них:

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Таким образом, нельзя назвать информационной системой или информационным ресурсом WEB-страницы и электронные конференции. Однако опубликованные на них сведения являются информацией.

В законе «Об участии в международном информационном обмене» в статье 2 можно найти следующие определения:

конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетварения потребностей пользователей;

информационные услуги – действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами;

информационная сфера (среда) – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации;

информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Исходя из этих определений и того, что программа есть произведение литературного творчества, можно предположить, что публикуемые на WEB-страницах и в электронных конференциях программы являются информацией. Кроме того, компьютерные программы и данные, изменяемые в результате внедрения компьютерных вирусов, нельзя отнести к конфиденциальной информации из-за несоответствия определению

термина «документ».

В законе «О средствах массовой информации» [12] в статье 2 можно найти следующие определения: массовая информация; средство массовой информации; периодическое печатное издание; радио-, теле-, видео-, кинохроникальная программа; продукция средств массовой информации; распространение продукции средств массовой информации; специализированное средство массовой информации; редакция средства массовой информации; главный редактор; журналист; издатель; распространитель. ПриведJм некоторые из них:

под массовой информацией понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы;

под средством массовой информации понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации;

под периодическим печатным изданием понимается газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год;

под распространением продукции средства массовой информации понимается продажа (подписка, доставка, раздача) периодических печатных изданий, аудио- или видеозаписей программ, трансляция радио-, телепрограмм (вещание), демонстрация кинохроникальных программ.

Очень похоже на то, что представленная на WEB-страницах в Internet или опубликованная в электронных конференциях (неограниченный круг лиц) информация (программы для ЭВМ как произведение литературного творчества) относится также к массовой информации. И хотя формально WEB-страницы и электронные конференции нельзя отнести к средствам массовой информации, а опубликование в них нельзя назвать распространением, вступает в силу статья 3 этого Закона, а именно:

цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей – не допускается.

Следовательно, если в опубликовании вирусов нет преступления, то нет основания для запрета публикации вирусов и информации о них на WEB-страницах и в электронных конференциях. Такой запрет противоречил бы правам и свободам, закреплJнным во Всеобщей Декларации Прав Человека и в Конституции РФ, что является прямым нарушением статьи 3 Закона «О средствах массовой информации».

В работе Волчинской Е.К. «Информационные технологии и право» (http://crime-research.org/library/Inflaw.htm) можно найти пояснения к определению «информация»:

- Исчерпывающий перечень «видов объектов гражданских прав» в Гражданском Кодексе РФ не включает «информацию». Следовательно, информация как таковая не относится Гражданским Кодексом ни к вещам, ни к интеллектуальной собственности.

- Информация как таковая представляет собой категорию идеального, она неосязаема, непотребляема (не амортизируется) и не может быть объектом правоотношений безотносительно к еJ носителю, содержанию, идентифицирующим признакам. Информация, как таковая не обладает свойствами, позволяющими закрепить на нее исключительное право.

- В то же время неправомерно отождествлять информацию с носителем, хотя по истечении определенного времени ряд документов переходит в разряд архивных и охраняется соответствующим законодательством как «вещи».

В курсовой работе по курсу криминалистики (http://download.referat.su/15985.zip) даны следующие определения и пояснения:

- Информационные ресурсы отличаются от известных ранее сырьевых и энергетических ресурсов целым рядом особенностей, а именно:

§ они непотребляемы и подвержены не физическому, а моральному износу;

§ они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;

§ их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колосальной экономии средств;

§ процесс их создания и использования осуществляется особым способом – с помощью компьютерной техники.

- В отечественной криминалистической науке все еще не существует четкого определения понятия компьютерного преступления, дискутируются различные точки зрения по их классификации.

**3.8. Автор и авторское право**

В законе «Об авторском праве и смежных правах» [13] в статье 4 даны определения следующих понятий: автор; аудиовизуальное произведение; база данных; воспроизведение произведения; воспроизведение фонограммы; запись; изготовитель аудиовизуального произведения; изготовитель фонограммы; исполнение; исполнитель; обнародование произведения; опубликование (выпуск в свет); передача в эфир; передача организации эфирного или кабельного вещания; показ произведения; последующая передача в эфир; программа для ЭВМ; произведение декоративно-прикладного искусства; публичный показ; режиссер-постановщик; репродуцирование (репрографическое воспроизведение); сдавать в прокат (внаем); сообщать; сообщать для всеобщего сведения по кабелю; фонограмма; экземпляр произведения; экземпляр фонограммы. ПриведJм некоторые из них:

автор – физическое лицо, творческим трудом которого создано произведение;

воспроизведение произведения – изготовление одного или более экземпляров произведения или его части в любой материальной форме, в том числе и в форме звуко- и видеозаписи, изготовление в трех измерениях одного или более экземпляров двухмерного произведения и в двух измерениях – одного или более экземпляров трехмерного произведения; запись произведения в память ЭВМ также является воспроизведением;

обнародование произведения – осуществленное с согласия автора действие, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, передачи в эфир или иным способом;

Здесь вводятся новые термины: «воспроизведение» и «обнародование». Вероятно, воспроизведением можно назвать любой процесс размножения компьютерного вируса, в том числе и его копирование лицом с использованием штатных средств. Обнародованием является первое опубликование компьютерного вируса (например, автором) и к распространению не имеет никакого отношения.

В соответствии с первой частью статьи 7 этого закона, «объектами авторского права являются литературные произведения (включая программы для ЭВМ)». Во второй части этой статьи поясняется, что «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». Статья 9 поясняет:

Авторское право на произведение науки, литературы и искусства возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трJх элементов:

- латинской буквы «С» в окружности ©;

- имени (наименования) обладателя исключительных авторских прав;

- года первого опубликования произведения.

Заметим, что и этим законом программы приравниваются к литературным произведениям. Следовательно, формулировка статьи 273 УК РФ противоречит основным правам и свободам людей, закреплJнным во

Всеобщей Декларации Прав Человека:

каждый человек имеет право… искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (статья 19;

каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами (статья 27 часть 1);

и в Конституции Российской Федерации:

каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (статья 29 часть 4);

гарантируется свобода массовой информации, цензура запрещается (статья 29 часть 5);

каждый имеет право на образование (статья 43 часть 1);

Российская Федерация устанавливает федеральные государственные образовательные стандарты, поддерживает различные формы образования и самообразования (статья 43 часть 5);

каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания (статья 44 часть 1);

Следует особенно подчеркнуть, что знак © не обязательно должен присутствовать в произведении для возникновения авторского права. Кроме того, в части 3 сказано:

При опубликовании произведения анонимно или под псевдонимом (за исключением случаев, когда псевдоним автора не оставляет сомнения в его личности) издатель, имя или наименование которого обозначено на произведении, при отсутствии доказательств иного считается представителем автора в соответствии с настоящим Законом и в этом качестве имеет право защищать права автора и обеспечивать их осуществление. Это положение действует до тех пор, пока автор такого произведения не раскроет свою личность и не заявит о своем авторстве.

Какими же правами обладают авторы вирусов по отношению к своим произведениям? Эти права делятся на личные неимущественные права (статья 15), а именно:

- право признаваться автором произведения;

- право использовать или разрешать использовать произведение;

- право обнародовать или разрешать обнародовать произведение в любой форме, включая право на отзыв;

- право на защиту произведения, включая его название;

и имущественные права (статья 16), а именно:

- автору в отношении его произведения принадлежат исключительные права на использование произведения в любой форме и любым способом;

- исключительные права автора на использование произведения означают право осуществлять или разрешать следующие действия:

· воспроизводить произведение;

· распространять экземпляры произведения любым способом: продавать, сдавать в прокат и так далее (право на распространение);

· публично показывать произведение (право на публичный показ).

Отсюда следует, что кроме противоречия статьи 273 УК РФ данному закону, возникает нарушение авторских прав антивирусными компаниями при искажении названий вирусов во время добавления их в вирусные базы.

ЕщJ одним интересным моментом является то, что финансовые доходы антивирусных компаний имеют прямую зависимость от использования ими компьютерных вирусов (имеется в виду продажа антивирусных

сканеров-фагов, в том числе, полифагов). В рассматриваемом Законе (статья 16, части 3 и 4) предусмотрены следующие взаимоотношения между авторами вирусов и антивирусными компаниями:

Если экземпляры правомерно опубликованного произведения введены в гражданский оборот посредством их продажи, то допускается их дальнейшее распространение без согласия автора и без выплаты авторского вознаграждения.

Размер и порядок исчисления авторского вознаграждения за каждый вид использования произведения устанавливаются в авторском договоре, …

Под словом «правомерно» следует понимать опубликование произведения без нарушения авторских прав, то есть опубликование самим автором или с его согласия. Поскольку безвозмездное использование вирусов антивирусными компаниями допускается только в случае покупки вирусов, антивирусные компании обязаны заключать с вирмейкерами договора и выплачивать им авторское вознаграждение. Допускается использование вируса без согласия автора в соответствии со статьJй 26, но и при этом должны быть выплачены авторские вознаграждения.

В соответствии со статьJй 18, допускается без согласия автора и без выплаты авторского вознаграждения воспроизведение программ для ЭВМ в личных целях, за исключением случаев, предусмотренных статьей 25 рассматриваемого Закона. Также использование вируса без согласия автора и без выплаты авторского вознаграждения, но с обязательным указанием имени автора, допускается в случае

- цитирования в научных, исследовательских, полемических, критических и информационных целях;

- иллюстрации в изданиях, в радио- и телепередачах, звуко- и видеозаписях учебного характера;

- воспроизведения в газетах, передача в эфир или сообщение по кабелю для всеобщего сведения, в случаях, когда такие воспроизведения не были специально запрещены автором;

- …

В статье 25 рассматриваются случаи свободного воспроизведения программ для ЭВМ и баз данных, а также декомпилирование программ для ЭВМ. Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора или иного обладателя исключительных прав на использование произведения и без выплаты дополнительного вознаграждения:

- внести в программу для ЭВМ или базу данных изменения с целью адаптации;

- сделать бэкап (Back Up – англ.), то есть сделать архивную копию;

- декомпилировать программу или объектный код с целью адаптации к ней собственных программ пользователя.

В любом случае применение положений этой статьи «не должно наносить неоправданного ущерба нормальному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного обладателя исключительных прав на программу для ЭВМ или базу данных». Таким образом обозначена ещJ одна проблема, касающаяся взаимоотношений между вирмейкерами и разработчиками антивирусных программ. Более подробное рассмотрение этих взаимоотношений выходит за рамки данной работы.

Относительно же применения этого закона к распространению компьютерных вирусов (использование для несанкционированной модификации программ) можно сказать, что очевидно нарушение посредством компьютерных вирусов авторских прав в части статьи 25, требующей правомерного владения инфицируемыми экземплярами программ для ЭВМ. Однако ответственность за нарушение авторских прав компьютерными вирусами должна возлагаться на тех, по чьей вине произошло это нарушение. Точно так же недопустимо наказание авторов специальных программных средств (например, дизассемблеров и отладчиков), которыми создавалась архивная копия или производились адаптация и декомпилирование на незаконных основаниях конкретным лицом (без правомерного владения экземпляром программы для ЭВМ).

**3.9. Собственник, владелец, пользователь информации**

В законе «Об участии в международном информационном обмене» [10] в статье 2 можно найти следующие определения:

собственник документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена – субъект, реализующий полномочия владения, пользования, распоряжения указанными объектами в объеме, устанавливаемом законом;

владелец документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена – субъект, реализующий полномочия владения, пользования и распоряжения указанными объектами в объеме, устанавливаемом собственником;

пользователь (потребитель) информации, средств международного информационного обмена (далее - пользователь) – субъект, обращающийся к собственнику или владельцу за получением необходимых ему информационных продуктов или возможности использования средств международного информационного обмена и пользующийся ими;

Интересным замечанием к данному законодательству является то, что часто при устройстве программиста на работу, подписывается договор, содержащий следующую формулировку: «любой код, произведJнный за время работы, является собственностью компании». В некоторых случаях это условие может распространяться и на нерабочее время. Означает ли это, что компьютерный вирус, созданный программистом, работающим по контракту, является собственностью работодателя? Какие последствия для работодателя может иметь создание программистом компьютерного вируса в рабочее время?

**3.10. Архив**

В Основах законодательства Российской Федерации «Об Архивном фонде Российской Федерации и архивах» [14] в статье 1 даны следующие определения: Архивный фонд Российской Федерации; архивный документ; архивный фонд; архив; тайный архив; архивное дело. ПриведJм некоторые из них:

под архивным документом понимается документ, сохраняемый или подлежащий сохранению в силу его значимости для общества, а равно имеющий ценность для собственника;

под архивом понимается совокупность архивных документов, а также архивное учреждение или структурное подразделение учреждения, организации или предприятия, осуществляющее прием и хранение архивных документов в интересах пользователей;

под тайным архивом понимается архив, о котором не заявлено публично.

В данном случае под архивом следует понимать не столько программно сжатый файл с информацией (программы-архиваторы: ARJ, ZIP, RAR, …), сколько вообще хранение в интересах пользователей любых файлов, зафиксированных на материальном носителе, имеющих ценность для собственников архивов. В соответствии со статьJй 7 этого Закона, любой человек имеет право хранить любые документы (в том числе и опубликованные вирусы) на своих носителях:

юридическим и физическим лицам Российской Федерации гарантируется право на создание архивов.

Следовательно, такое деяние, как коллекционирование вирусов (создание и хранение архивов) преступлением не является и не может выступать в качестве улики или предмета обвинения его собственника. Кроме того, в соответствии со статьJй 9 этого Закона, никто не имеет права изъять архив у собственника без соответствующего решения суда:

право собственника независимо от формы собственности охраняется законодательством Российской Федерации. Ни один архивный документ не может быть без согласия собственника или уполномоченного им органа или лица изъят иначе, как на основании судебного решения.

**3.11. Средство защиты информации**

В Законе Российской Федерации «О государственной тайне» [15] в статье 2 приведены следующие определения: государственная тайна; носители сведений; система защиты государственной тайны; допуск к государственной тайне; доступ к сведениям, составляющим государственную тайну; гриф секретности; средства защиты информации. ПриведJм одно из них:

государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях;

средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Из этого следует, что государственная тайна должна охраняться образом, исключающим любое непреднамеренное eJ разглашение. Кроме того, создание и использование компьютерного вируса как программы для ЭВМ с целью контроля эффективности защиты информации (например, для тестирования антивирусных программ) является уже не созданием и использованием вредоносной программы, а созданием и использованием средства защиты информации. В мировой юридической практике существуют примеры оправдания деяний, направленных на тестирование систем защиты. Так в новостях (http://www.securitylab.ru/43199.html) можно найти следующую статью: «Суд оправдал хакера, взломавшего сайт „Моссада“».

Израильский подросток, обвиненный в попытке взлома сайта "Моссада", был признан невиновным Магистратским судом Иерусалима. Как сообщает Ha`aterz, судья Абрахам Тенненбойм пришел к выводу о том, что Ави Мизрахи не пытался взломать сайт, но лишь проверял уровень его защиты, а проверка защищенности любого сайта - деяние, достойное похвалы.

**3.12. Эксперты, привлекаемые следствием и судом**

В методических рекомендациях по теме «Расследование преступлений в сфере компьютерной информации» (http://deadman.interdon.net/tmp/27x.html) можно найти обоснование (раздел 1.1) для привлечения экспертов в ходе следственных действий по компьютерным преступлениям:

Важно учитывать, что следователь, в силу специфики своей деятельности, не может обладать достаточно глубокими знаниями и навыками специалиста в области компьютерной техники, которые требуются при исследовании механизма совершения преступления, и может совершить неисправимые ошибки в ходе обследования технической аппаратуры, снятия необходимой информации или изъятия вещественных доказательств. Поэтому, все эти действия необходимо выполнять в присутствии и с помощью специалиста. Участие соответствующего специалиста необходимо также и при производстве допросов, на которых выясняются технические аспекты совершенного преступления.

К экспертам предъявляются следующие требования:

При осмотре места происшествия следователь обязательно должен использовать помощь незаинтересованных специалистов в области установки и функционирования средств электронно-вычислительной техники, программирования, а также специалиста-криминалиста (раздел 2.1).

Прежде чем приступить к осмотру места происшествия, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации (раздел 2.1).

В качестве понятых при производстве следственных действий рекомендуется привлекать лиц, обладающих специальными познаниями в области компьютерной техники и информации (раздел 2.3).

В разделе 4 этих рекомендаций перечислены объекты и цели экспертных исследований. Кроме того, сказано, кто может быть привлечJн следствием в качестве экспертов. Поскольку этот вопрос очень важен и при этом мало освещен в других источниках информации, приведJм расширенную цитату:

В системе Министерства внутренних дел в настоящее время нет специальных экспертных подразделений, которые производят компьютерно - технические экспертизы носителей машинной информации, программного обеспечения, баз данных и аппаратного обеспечения ЭВМ. В связи с этим они могут быть назначены специалистам соответствующей квалификации из вне экспертных учреждений. В частности, такие специалисты могут быть в информационных центрах, учебных и научно-исследовательских заведениях МВД России. Кроме того, для производства этого вида экспертиз можно привлекать специалистов учебных и научно-исследовательских заведений, не относящихся к системе МВД России, фирм и организаций, занимающихся разработкой программного и аппаратного обеспечения для компьютеров, их эксплуатацией и ремонтом. Данный вид экспертиз может быть поручен специалистам в области эксплуатации ЭВМ (системным

программистам, инженерам по обслуживанию, непосредственно работающим с данного вида носителями и др.) и программистам, которые обладают соответствующей квалификацией.

В приведJнных выше цитатах не сказано, какими именно специальными познаниями и какой именно квалификацией должны обладать специалисты, привлекаемые в качестве экспертов. Круг учреждений, специалисты из которых могут быть экспертами, весьма широк. Однако четко указано, что экспертами могут стать незаинтересованные специалисты. Поэтому налицо юридическая ошибка, возникающая при привлечении в качестве экспертов, при проведении следствия и суда, сотрудников антивирусных компаний. Сотрудники антивирусных компаний в принципе не могут выступать в качестве незаинтересованных специалистов при выдвинутом обвинении по статье 273 УК РФ. Пояснение к этому утверждению приведено в разделе «компьютерный вирус и троянский код» настоящей работы.

Основными ошибками рассматриваемых рекомендаций (в свете статьи 273 УК РФ) является необходимость выключения питания компьютеров и способы идентификации информации. Так, например, требуется «выключить компьютер, который подвергся воздействию, а при наличии сети требуется выключить все компьютеры в сети». Такие действия могут повлечь утерю основной улики, если компьютер или компьютерная сеть подверглись нападению бестелесного червя, существующего только в оперативной памяти компьютеров. К недостаткам рекомендаций также следует отнести использование термина «компьютерный вирус» при отсутствии общепризнанного определения такого класса программ (приведJнное авторами определение вызывает много нареканий). Кроме того, авторы вводят в заблуждение читателей ложной трактовкой других компьютерных терминов[11].

В рассматриваемых методических рекомендациях перечислены общие и обязательные обстоятельства, подлежащие установлению при расследовании компьютерных преступлений. Здесь сделан акцент на то, что, чтобы доказать опасность, исходящую от программы, необходимо определить, для каких систем она может представлять опасность, какую именно опасность и как много таких систем. Это является очень важным в применении термина «вредоносность» по отношению к компьютерным программам.

**4. Права вирмейкера как человека и гражданина**

Перед началом рассуждений следует отметить, что вирмейкеры не являются людьми «вне закона». Они имеют такие же права и свободы, как и любые другие люди и граждане своих государств. Эти права и свободы закреплены следующими документами:

- Всеобщая Декларация Прав Человека

· Каждый человек должен обладать всеми правами и всеми свободами, провозглашенными настоящей Декларацией, без какого бы то ни было различия… (статья 2)

· Все люди равны перед законом и имеют право, без всякого различия, на равную защиту закона (статья 7)

· Каждый человек, для определения его прав и обязанностей и для установления обоснованности предъявленного ему уголовного обвинения, имеет право, на основе полного равенства, на то, чтобы его дело было рассмотрено гласно и с соблюдением всех требований справедливости независимым и беспристрастным судом (статья 10)

· Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (статья 19)

· Каждый человек имеет право на социальный и международный порядок, при котором права и свободы, изложенные в настоящей Декларации, могут быть полностью осуществлены (статья 28)

· …

- Конституция Российской Федерации

· Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства (статья 2)

· Каждый гражданин Российской Федерации обладает на ее территории всеми правами и свободами… (статья 6)

· В Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права и в соответствии с настоящей Конституцией (статья 17 часть 1)

· Основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения (статья 17 часть 2)

· Каждому гарантируется свобода мысли и слова (статья 29 часть 1)

· Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них (статья 29 часть 3)

· Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (статья 29 часть 4)

· Российская Федерация… поддерживает различные формы образования и самообразования (статья 43 часть 5)

· Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания (статья 44 часть 1)

· Государственная защита прав и свобод человека и гражданина в Российской Федерации гарантируется (статья 45 часть 1)

· …

Необходимо обратить особое внимание на принятую иерархию законодательств. Так, Конституция РФ имеет юридическую силу выше, чем любой другой закон, принятый в РФ. Это закреплено в первой части статьи 15:

Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации. Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.

Следовательно, все противоречащие Конституции РФ законы (например, в силу их несовершенства) не могут быть применены. Кроме того, в случае подписания Россией международных договоров, эти договора получают юридическую силу выше, чем даже сама Конституция РФ. Это закреплено в четвJртой части статьи 15:

Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Одним из таких международных договоров как раз и является Всеобщая Декларация Прав Человека, принятая и провозглашJнная резолюцией 217 A (III) Генеральной Ассамблеей ООН 10 декабря 1948 года. Кроме того, в статье 55 (части 1 и 2) Конституции РФ утверждается:

1. Перечисление в Конституции Российской Федерации основных прав и свобод не должно толковаться как отрицание или умаление других общепризнанных прав и свобод человека и гражданина.

2. В Российской Федерации не должны издаваться законы, отменяющие или умаляющие права и свободы человека и гражданина.

Исходя из вышесказанного, вирмейкер имеет право «беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ». В данном случае имеется ввиду информация из области компьютерной безопасности и информация, касающаяся создания и функционирования компьютерных вирусов. До тех пор, пока использование этой информации вирмейкером не ущемляет права и свободы других людей или не ограничивается на законном основании (законным основанием является отнесение информации к государственной, коммерческой или личной [конфиденциальная информация] тайне), деятельность вирмейкера имеет правовую основу и защиту. Также вирмейкер «не может быть принужден» к отказу от своих мнений и убеждений, ибо такое принуждение будет противоречить Российскому законодательству. И ещJ, вирмейкер «имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» до тех пор, пока эта информация не имеет ограничения по доступу либо осуществление этого права не наносит прямого ущерба другим людям.

Во введении к настоящей работе было указано, что нанесения ущерба другим людям (независимо от того, с помощью вируса или с помощью молотка, кирпича или чего-то ещJ) является противозаконным и в данной работе обсуждению не подлежит. Поэтому будем в дальнейшем рассматривать законность действий только той части вирмейкерского сообщества, использующей информацию из области компьютерных вирусов исключительно для самообразования («Российская Федерация… поддерживает различные формы образования и самообразования»), исследований в области безопасности и литературного творчества («гарантируется свобода литературного, .. научного, ... и других видов творчества»), например, программирования в качестве хобби. Таким образом осуществляется право вирмейкера на творчество и самообразование, закреплJнное Конституцией РФ.

**5. Компьютерный вирус и троянский код**

Законодательство РФ не определяет понятие «компьютерный вирус», а значит «вредоносность» каждого вируса должна рассматриваться для каждого конкретного случая. По наличию формальных признаков, компьютерный вирус может быть отнесJн законодательством к

· информации;

· программа для ЭВМ;

· документ (опубликование, с некоторыми допущениями);

· массовая информация (с некоторыми допущениями);

· информационный продукт;

· архивный документ (с некоторыми допущениями);

· произведение литературы;

· средство защиты информации.

Только в случае признания компьютерных вирусов программами для ЭВМ, к их создателям и обладателям может быть применена статья 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» и то, только в случае признания всех компьютерных вирусов вредоносными программами. При этом возникают очень большие претензии к формулировке самой статьи и правомерности eJ применения. Кроме того, в мировой юридической практике есть прецедент оправдания лица, публиковавшего вирусы на страницах Internet. Решающим доводом послужило то, что запакованный в архив вирус уже вирусом не является.

Что же такое «компьютерный вирус»?

**5.1. Живое существо**

В монографии «Биофизика полей и излучений и биоинформатика» [16] (отрывок из которой «Компьютерный вирус – живое существо?» публиковался в четвJртом выпуске электронного журнала «Земский Фершал» [http://www.karimov.ru/zf/]) представлены научно обоснованные определение и совокупность свойств живого объекта. Такими свойствами, например, являются:

- способности воспроизводить себе подобные или имеющие качественные отличия объекты: (+)

- способности управлять процессами материального, энергетического и информационного обмена с окружающей средой. (++)

Также показано, «что разум, как сторона человека, проявляющаяся в системе отношений между человеком и изменяемой им природой, является свойством человека все более углубленно и целенаправленно управлять процессами материального, энергетического и информационного обмена в окружающей среде и между человеком и окружающей средой (+++)». УчJные утверждают, что «человек, обладая свойствами (+) и (+++), имеет потенциальную возможность породить качественно новые живые объекты с новой формой организации жизни». В этой работе на примере компьютерных вирусов показано, «что человек уже в настоящее время способен выполнять функции Творца». Таким образом, выдвинута научно-обоснованная гипотеза того, что компьютерный вирус является живым существом.

Не согласиться с авторами трудно, так как поведение современного человека по отношению к природе практически ничем не отличается от поведения троянских программ и вирусов по отношению к информационной среде. В такой трактовке биологические вирусы можно отождествлять с антивирусными программами, создаваемыми Творцом для борьбы с биологической опасностью, представляемой Человеком.

**5.2. Принцип воспроизводства и внедрения в объекты**

В работе «Создание, использование и распространение вредоносных программ для ЭВМ» (http://download.referat.su/15985.zip) дано следующее определение:

- под «компьютерным вирусом» в теории программирования понимается такая совокупность машинного кода, которая сама может создавать свои копии и внедрять их в файлы, системные области ЭВМ, вычислительные сети и т.д. При этом копии не обязательно полностью совпадают с оригиналом, могут становиться совершеннее его и сохраняют способность дальнейшего самораспространения.

Вызывает большое сомнение то, что в «теории программирования» (computer science – англ., состоит из теории алгоритмов, теории автоматов, теории групп, теории баз данных и т.д.) существует определение термину «компьютерный вирус». Дело в том, что

- Вирус, как и любая другая программа, является совокупностью данных и команд. При этом существуют вирусы, распространяющиеся только в виде исходных кодов (исходные коды машинными инструкциями не являются).

- Свои копии могут создавать и файловые менеджеры (Norton Commander, Volcov Commander, Dos Navigator и др.) при копировании их самих встроенными в них средствами из одного каталога или диска в другой. Например, при случайном стечении обстоятельств. К слову сказать, многие почтовые черви могут инфицировать компьютер только в том случае, если пользователь сам сохранит на диске архив-приложение к письму, разархивирует этот архив и запустит файл червя на исполнение (некоторые вирусы дополнительно закрывают архив паролем).

- Внедряться в файлы могут антивирусные вакцины, средства защиты программ от несанкционированного доступа, архиваторы (при создании самораспаковывающихся архивов).

- Утверждение о том, что копии вирусов могут становиться совершеннее оригиналов, вызывает большие сомнения. На сегодняшний день более известны те вирусы, которые либо не изменяются с точки зрения функциональности, либо становятся хуже (примитивнее) от копии к копии в результате программных ошибок и заложенных в них алгоритмов. Некоторые вирусы в своих поколениях (копиях, созданных копиями) вообще теряют способность к размножению.

- Не дано определение термину «самораспространение». Действия операционной системы при инсталляции на диск (например, как показано в примере с MS DOS в книге Е. Касперского [8]) также можно назвать самораспространением. При этом и оригинал операционной системы и eJ копия, установленная на диске, будут отвечать всем признакам вируса, приведJнным в указанном определении компьютерного вируса.

В данном определении не приведено ни одного свойства вируса, которое бы приносило вред, и вследствие чего вирус можно было бы отнести к разряду «вредоносных» программ. Кроме того, в подавляющем большинстве своJм вирусы специально разрабатываются так, чтобы они не нарушали нормального функционирования компьютерных программ. Иначе этот вирус будет быстро обнаружен и удалJн из системы. Если же автор данного определения имел в виду выполнение перечисленных действий несанкционированно, на что указывает термин «самораспространение», то и в этом случае он окажется не прав. Например, если владелец компьютера санкционирует выполнение вирусом всех действий на своJм компьютере, то вирус от этого вирусом быть не перестаJт. А часто ли спрашивают другие программы, например операционная система, у пользователя санкции на выполнение тех же самых действий, что перечислены в определении? Если использование термина «самораспространение» указывает на то, что вирус имеет в себе все средства для создания своего дубликата, то это заблуждение. Существуют вирусы, не имеющие средств для создания дубликатов.

Далее в тексте работы автор намеревался привести перечень вредоносных программ, однако дал лишь размытые определения незаконного применения абсолютно любых программ. Хочется пояснить, что в случае применения программы для выполнения преступного деяния, программа вредоносной стать не может. Вредоносным будет конкретное деяние конкретного человека. Позволю себе привести пример: если с помощью графического редактора MS PaintBrush пользователь нарисовал неприличную картинку и использует

eJ в хулиганских целях, то программа MS PaintBrush от этого вредоносной не становится.

Если же рассматривать возможность транспортировки вирусами троянского (вредоносного) кода, например удаляющего информацию с диска, в качестве вредоносной функции, то и это ещJ не может стать основанием для причисления компьютерных вирусов к разряду вредоносных программ. Вредоносный код может транспортироваться и другими носителями. Например, если человек распространяет троянский код в виде приложений к сообщениям электронной почты, то ни само сообщение, ни почтовая программа от этого вредоносными не становятся. ЕщJ один пример: многие программы содержат в себе графические изображения, выводимые ими в качестве заставки. Однако сами программы не становятся от этого графическими изображениями, а остаются программами.

Сам же вирус, как и любая другая программа, может содержать ошибки, конфликтовать с другими программами или устройствами, занимать системные ресурсы (попробуйте доказать оправданность всех занимаемых ресурсов операционной системой Windows и у вас ничего не получится). Поэтому такие возможные свойства вирусов, которыми обладают и другие программы, не могут являться критериями «вредоносности».

**5.3. Принцип Касперского**

В книге Е. Касперского «Компьютерные вирусы» [8] целый раздел посвящен «попытке дать “нормальное” определение» компьютерному вирусу. Касперский признаJт, что «строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно». Указано, что все отличительные черты вируса либо присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных отличительных черт, за исключением возможности распространения. Акцент поставлен правильный, так как существуют вирусы, имеющие возможность распространения, но при этом не имеющие возможности самораспространения. Например, вирус может работать в диалоговом режиме с пользователем:

> Введите имя инфицируемого файла: c: empgoat.exe

> Файл “c: empgoat.exe” найден. Инфицировать его [Y/N]? Y

> Файл успешно инфицирован.

Такие действия вируса уже трудно назвать самораспространением. Однако это всJ равно будет вирус, хотя и в примитивной, вырожденной форме. Дальше Касперский признаJт: «Основная же проблема компьютерных вирусов – возможность их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами». Стало быть, по этой особенности нельзя выделить группу «компьютерные вирусы» из общего числа компьютерных программ.

Далее сообщается, что «представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом» и приведено такое условие:

- ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Хочется возразить, что это свойство не является ни обязательным ни необходимым. Например, резидентный вирус может перехватывать функцию операционной системы «Запись в файл» и при вызове этой функции настраивать регистры процессора таким образом, чтобы операционная система брала в качестве источника данных копию вируса из памяти. Или другой пример, нерезидентный компаньон-вирус может вызывать командный процессор COMMAND.COM с некоторыми параметрами, в результате чего будет создан дубликат вируса средствами командного процессора. Таким образом, вирус не всегда будет иметь в себе даже возможность создавать свои дубликаты (например, при попадании в другую операционную среду), но вирусом от этого быть не перестанет. Кроме того, возможность создавать свои дубликаты, как было правильно замечено Касперским, имеют и другие программы, вирусами не являющиеся. Например, операционная система MS DOS.

Непонятно утверждение «не обязательно совпадающие с оригиналом». Насколько несовпадающие? Несовпадающие в чJм? Дело в том, что существуют вирусы (ACG[12], VCG[13]), которые создают дубликаты, несовпадающие с оригиналом ни на один байт, а есть вирусы, полностью меняющие свою функциональность

от копии к копии. Примером вирусов, меняющих свою функциональность (под функциональностью подразумевается весь тот набор «умений», которые вирус потенциально может реализовать) может являться двуполый вирус RMNS[14] (в результате соединения «полов» получается совершенно новый вирус) или вирусы, использующие плагины[15] (Plug In – англ.), заботливо раскладываемые автором вируса на WEB-страницах или в электронных конференциях. Кроме того, возможно, что на определJнном этапе, вирус начнJт инфицировать объекты такими своими дубликатами, которые не будут больше иметь способность к дальнейшему размножению, а будут воспроизводить только заложенные в вирус аудиовизуальные эффекты или исполнять заложенный автором троянский код. Будет ли являться такой вирус вирусом?

Кроме того, непонятна опасность (вред) от способности программ создавать свои дубликаты. Пример вырожденных вирусов:

- Вирус представляет собой исполняемый файл на диске. При запуске вируса, он создаJт единственный свой дубликат и перезаписывает им тот файл, из которого он стартовал, то есть, перезаписывает сам себя. Это свойство собственной перезаписи использовали раньше созданные в виде COM-программы антивирусы, написанные на языке ассемблера (например, при нарушении целостности COM-файла антивируса в результате воздействия вируса или сбоя на диске, антивирус мог восстановить этот файл записью своей копии из памяти) и при этом вирусами не являвшиеся.

- Вирус создает свой дубликат всегда в единственный файл на диске, имеющий всегда одно и то же имя (например, записывает свой дубликат в файл VIRUS.TXT). Более того, такой дубликат теряет возможность дальнейшего распространения, так как файлы с расширением .TXT не являются исполняемыми. Для того, чтобы дубликат вновь приобрJл способность к размножению, пользователь должен самостоятельно изменить расширение файла на соответствующее формату файла, содержащего оригинал вируса.

Внедрение же своих дубликатов в системные области компьютера характерно и для программ, не являющихся вирусами. Примером тому может служить резидентный монитор антивирусной программы. Непонятен вред от этой способности программ, но польза очевидна.

В дальнейшем Касперский частично соглашается с несостоятельностью данного определения: «следует отметить, что это условие не является достаточным» и приводит пример с операционной средой MS DOS, которая удовлетворяет данному свойству, но вирусом не является.

Здесь следует высказать ещJ одно замечание. Нельзя приписывать программам, как и вещам материального мира, какие-либо функции. Вещи и программы существуют сами по себе, независимо от цели их применения человеком. Как не бывает хороших вещей или плохих вещей (бывает хорошее или плохое применение этим вещам), так не бывает хороших или плохих (вредоносных) программ. Бывают преступные цели, намерения и деяния. Преступное деяние может быть совершено с помощью хорошей (полезной) вещи и будет являться преступлением. А может быть и так, что хорошее деяние будет совершено с помощью «плохой» вещи и при этом преступлением являться не будет. Было бы неправильным объявлять какие-либо вещи преступными только потому, что существует возможность совершения с помощью этих вещей преступления. Молоток не является ни хорошей, ни вредоносной вещью, он просто молоток, независимо от того, забивают им гвозди, раскалывают орехи, разбивают окно соседу или причиняют тяжкие телесные повреждения сопернику. На основании лишь того, что кто-то использовал молоток для совершения проступка или преступления, нельзя относить молотки к вредоносным вещам и запрещать их производство, применение или распространение (например, розничную продажу). Наказывать нужно не вещи и не лица их создавшие, а лица их применившие в преступных целях. Это было бы справедливо.

Кажется очевидным, что авторы подобных определений идут по принципу: «всJ, что не полезно с моей точки зрения для других людей – вредно». Это абсолютно недопустимый принцип для отнесения компьютерных программ к разряду вредоносных. Если конкретному человеку, даже обладающему властными полномочиями, непонятен смысл какого-либо литературного или художественного произведения, то его непонимание не может являться причиной расценивать это произведение как бесполезное и вредное[16]. Приведу пример: в чJм заключается вред от стихов Баркова[17] или от известной картины[18] Казимира Малевича[19]?

В результате очень спорных рассуждений Касперский приходит к таким выводам:

- Точного определения нет до сих пор, и вряд ли оно появится в обозримом будущем.

- Нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов».

- Иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Поскольку Касперский пытается отнести вирусы к вредоносным программам, разделяя файлы на «хорошие» и «вирусы», то в отношении лиц создающих, распространяющих или использующих вирусы, должна применяться статья 273 УК РФ. Однако первые два вывода автора показывают, что возникает противоречие трJм принципам применения уголовного закона, указанным в разделе 3.1 настоящей работы. Тем самым ещJ раз подтверждается правильность основной цели данной работы – показать недопустимость применения статьи 273 УК РФ по отношению к лицам создающим, публикующим или использующим компьютерные программы, которые именуются этими же лицами (или антивирусными компаниями) как «компьютерные вирусы».

Третий вывод наиболее интересен с точки зрения уголовного законодательства. Он в явной форме говорит о недопустимости применения статьи 273 УК РФ из-за отсутствия значимых критериев определения вредоносных программ.

Дальше Евгений Касперский показывает на примере программ KOH и ALREADY.COM свой принцип отнесения той или иной программы к разделу компьютерных вирусов. Мало того, что этот принцип является абсолютно субъективным (абсолютно не вредоносная программа KOH отнесена к разделу вредоносных программ), но и:

- Если бы, конечно, автором KOH был бы не безызвестный программист, а скажем, Симантек, или Sierra, или даже сам Microsoft, то никто бы и не посмел назвать это вирусом…

Хотелось бы напомнить автору этих строк, что в соответствии со следующими Законами данное публичное признание само является уголовно наказуемым преступлением по статье 136 УК РФ в части 2:

- Всеобщая декларация прав человека, статья 7: «Все люди равны перед законом и имеют право, без всякого различия, на равную защиту закона».

- Конституция РФ, статья 19 часть 1: «Все равны перед законом и судом».

- Уголовный Кодекс РФ, статья 4: «Лица, совершившие преступления, равны перед законом и подлежат уголовной ответственности независимо от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств».

Дело вот в чJм. Если допустить, что вирус является вредоносной программой, то автора программы KOH можно было бы осудить по статье 273 УК РФ. Представьте себе, что было бы, если бы на момент создания программы KOH эта статья бы действовала, а автором еJ был бы не безызвестный программист, а вполне реальный российский программист. Речь то идJт об уголовном преступлении!

Если суд будет ориентироваться при отнесении программ к разряду «вредоносных» по наличию соответствующих записей в антивирусных базах таких антивирусов, как KAV (http://www.avp.ru/products.html), то можно будет лишать свободы людей за создание и использование абсолютно любых программ, которые по каким то причинам (или их автор) не понравились разработчикам. Этот пример демонстрирует, что следствию и суду (собственно, вообще никому) недопустимо ориентироваться на записи в базах данных антивирусных программ и недопустимо привлекать сотрудников антивирусных компаний в качестве экспертов по уголовным делам, касающихся компьютерных преступлений.

Кроме явной субъективности мнения разработчиков антивирусных программ о «вредоносности», существует ещJ одна особенность – возможность отключения отдельных таблиц из вирусной базы на усмотрение пользователя (например, отключение eicar.avc или malware.avc от базы данных антивирусной программы KAV). Точно также возможно создание индивидуальной таблицы (вероятно на коммерческой основе) с записями для тех программ, которые конкретный пользователь по тем или иным причинам не желает видеть на своJм компьютере (например отец хочет запретить сыну играть в определJнные компьютерные игры). Этот произвол ещJ раз подчJркивает о недопустимости использования в качестве критерия «вредоносности» конкретной программы наличие о ней записи в антивирусной базе данных.

Также возникает резонный вопрос, каким образом можно определить, что bootstrap loader программы KOH совпадает практически на 100% с вирусом Havoc? Может быть, это вирус Havoc совпадает практически на 100% с bootstrap loader программы KOH? Если пользоваться принципом Касперского, то любого автора программы можно наказать по статье 273 УК РФ только за то, что кто-то использовал код его программы для создания вируса.

Пример с программой KOH не является исключением. Вот другой пример абсолютно безобидной программы

на языке Ассемблер. Программа GOAT никаких вредоносных деяний не совершает. Она проверяет наличие параметра «R» в командной строке и завершает свою работу. В случае, если пользователь запустил программу GOAT с параметром «R», она запишет свой образ из памяти в тот файл на диске, из которого стартовала и таким образом восстановит собственный код из памяти. Действие программы является санкционированным (санкцией является параметр «R», санкционирует пользователь) и не имеет отношения к самораспространению (здесь больше подходит термин «самовосстановление»). Однако, по принципу Касперского, эта программа является «страшным» вирусом с названием SillyOC.2000.

```
PSP_envirn_seg equ 2Ch

PSP_cmd_tail+1 equ 82h

org 100h

start proc near

mov al, PSP_cmd_tail+1 ; (DS:0082=0)

cmp al, 52h ; `R`

jnz locret_0_13E ; Jump if not equal

mov ax, ds:PSP_envirn_seg ; (DS:002C=0)

mov ds, ax

xor bx, bx ; Zero register

loc_0_10E: ; xref DS:0115, 011C

mov al, [bx]

or al, 0

jz loc_0_117 ; Jump if zero

inc bx

jmp short loc_0_10E

loc_0_117: ; xref DS:0112

inc bx

mov al, [bx]

or al, al ; Zero ?

jnz loc_0_10E ; Jump if not zero

add bx, 3

mov ah, 3Ch ; DOS Services, ah=function 3Ch

mov cx, 0

mov dx, bx

int 21h ; DOS - 2+ - CREATE A FILE WITH HANDLE (CREAT)

; CX = attributes for file

; DS:DX -> ASCIZ filename

;(may include drive and path)
```

```
jb locret_0_13E ; Jump if carry Set

mov bh, 40h ; DOS Services ah=function 40h

xchg ax, bx

push cs

pop ds

mov cx, 7D0h

nop

cwd

inc dh

int 21h ; DOS - 2+ - WRITE FILE WITH HANDLE (WRITE)

; BX = file handle

; CX = count bytes from ds:dx buffer

; DS:DX buffer

mov ah, 3Ch ; DOS Services ah=function 3Ch

int 21h ; DOS - 2+ - CREATE A FILE WITH HANDLE (TRUNC)

; CX = attributes for file

; DS:DX -> ASCIZ filename

;(may include drive and path)

locret_0_13E: ; xref DS:0105, 012A

retn

start endp

db 1937 dup (90h) ; NOP

seg000 ends

end start
```

Поскольку мы рассматриваем приведJнные в книге известного вирусолога примеры применительно к уголовному закону, то все его выводы оказываются, мягко говоря, спорными и не могут применяться в качестве экспертной оценки в следственной и судебной практике в силу принципов применения законов, и в первую очередь IN DUBIO PRO REO.

«Попытка дать “нормальное” определение» известного в мире вирусолога заканчивается следующими словами: «Посему тема “нормального” определения компьютерного вируса остается открытой».

В этой же книге приведено «Объяснение для домохозяйки» термина «компьютерный вирус» не менее известного вирусолога Д.Н. Лозинского. Мало того, что это определение не применимо для уголовного закона в силу сплошной аналогии, но и правомерность самой аналогии может являться темой для большой дискуссии, выходящей за рамки данной работы.



ОКОНЧАНИЕ

Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ, МИР 4610 31.03.2004, 13:15 386