УДК 004.491.22

ПРОБЛЕМА КОРРЕКТНОГО ОПРЕДЕЛЕНИЯ ТЕРМИНА «ВРЕДОНОСНАЯ ПРОГРАММА»

В. А. Голуб, М. В. Овчинникова

Воронежский государственный университет

Рассматривается проблема корректного определения термина «вредоносная программа». Дан анализ достоинств и недостатков определений, имеющихся в настоящее время. Сформулированы требования, которым должно удовлетворять такое определение. Предложено определение термина «вредоносная программа», в наиболее полной мере удовлетворяющее этим требованиям.

Каждый пользователь компьютера постоянно сталкивается с необходимостью защиты от вредоносных программ, обычно называемых компьютерными вирусами. В последние три года вредоносные программы распространились и на сферу мобильной связи и стали способны инфицировать сотовые телефоны и другие мобильные устройства, использующие радиоканал для передачи данных, в частности, систему Bluetooth. Угрозы информационной безопасности, обусловленные воздействием вредоносных программ могут быть чрезвычайно серьезными. В то же время, как это не парадоксально, до настоящего времени отсутствует корректное и достаточно общее определение вредоносной программы, необходимость которого очевидна не только для программистов и юристов, но и для пользователей любых компьютеризированных информационных систем, подверженных воздействию вредоносных программ. При этом следует отметить, что, по мнению ряда авторов, в том числе специалистов по компьютерной вирусологии, дать исчерпывающее и точное определение термина «вредоносная программа» крайне сложно, если вообще возможно. Сложность решения этой задачи связана, в частности, с тем, что и полезные программы могут нанести вред в результате программных ошибок, либо в результате неправильного применения.

Чрезвычайно важным является и юридический аспект корректного определения вредоносного программного обеспечения. Так, значительная часть преступлений, совершаемых в информационной сфере — это преступления, ответственность за которые предусмотрена ст. 273 Уголовного Кодекса Российской Федерации «Создание, использование и распространение вредоносных программ для ЭВМ». Однако в ст. 273 УК РФ не содержится определение понятия «вредоносная программа», а лишь указываются конкретные деструктивные действия, связанные с использованием такой программы, что следует считать одним из пробелов в законодательстве РФ.

В этой связи появляется насущная потребность иметь выверенное корректное как с «программистской», так и с юридической точки зрения определение вредоносной программы, что и является целью данной работы.

Анализ материалов по рассматриваемому вопросу, включая публикации по информационным технологиям, программированию, вопросам, связанным с разработкой средств защиты от вредоносных программ, а также анализ нормативно-правовых актов Российской Федерации и других стран, международных актов, комментариев к законодательству, материалов судебной практики и т.п., дает возможность выявить достоинства и недостатки различных определений вредоносных программ и, на этой основе, сформулировать наиболее точное и полное определение.

Так, наиболее приемлемым на данный момент следует считать определение термина «вредоносная программа», содержащееся в тексте Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.), которое подразумевает под *вредоносной программой — «созданную или существующую программу со специально внесенными изменениями, заведомо приводящую к несанкционированному уничтожению, блокированию, модифика-*

ции либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети».

В то же время указанное определение, как и текст, закрепленный как диспозиция ст. 273 УК РФ, не является полным и корректным, так как, в частности, не учитывает всех возможных последствий действия вредоносных программ. Такое определение не охватывает, например, такие программы, как программы-шпионы (Spyware), целью которых является отслеживание действий пользователя компьютера, программы-злые шутки (Bad Jokes) и т.п.

Законодательство Российской Федерации ни в одном нормативном акте, кроме упомянутых выше, не дает определение «вредоносной программы» или «компьютерный вирус» и даже не содержит бланкетных норм. Это приводит к тому, что в ряде документов этот термин используется как известный и не определяется, что приводит к юридической некорректности этих документов. Примером тому является Инструкция Центрального Банка Российской Федерации от 22 июля 2002 г. № 102-и «О правилах выпуска и регистрации ценных бумаг кредитными организациями на территории Российской Федерации», где в главе 23 «Порядок представления документов на магнитном носителе» говорится, что «*Полученные регистрирующими органами магнитные носители проверяются на отсутствие компьютерных вирусов…*». Данный документ не дает определение термину «компьютерный вирус», также не говорит, где его можно найти.

Другим примером является Постановление Правительства Москвы от 28 сентября 2004 г. № 670-пп «О концепции создания городской интегрированной системы районных социально ориентированных информационных ресурсов и услуг (проект «инфоград»)» в пункте 7.1. «Модель нарушителя безопасности», в котором говорится, что «*В соответствии с РД Гостехкомиссии НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа. НСД к информации может осуществляться злоумышленником как непосредственно, при помощи штатных средств системы либо с использованием специализированных программно-технических средств, так и опосредованно, путем внедрения в систему вредоносных программных кодов (вирусов, компьютерных червей, «троянских» программ)*». Здесь идет речь только о вредоносных программных кодах, определяя, что к ним относятся лишь вирусы, компьютерные черви и «троянские» программы.

Разные определения термина «вредоносная программа» или «компьютерный вирус» даются и в различных комментариях к УК РФ. В целом можно выделить следующие неточности, содержащиеся в ряде определений.

1. Определение компьютерного вируса как *совокупности машинного кода* [1], не является правильным. Существуют вирусы, распространяющиеся только в виде исходных кодов (исходные коды машинными инструкциями не являются).

2. Такое действие вируса, как *создание копий и внедрение в файлы* [1], не специфично для вирусов и может быть присуще и другим программам. Внедряться в файлы могут, например, антивирусные вакцины, средства защиты программ от несанкционированного доступа, архиваторы (при создании самораспаковывающихся архивов) и т.п.

3. В своих работах В. Я. Кожинов и В. А. Копылов [2, 3] компьютерный вирус характеризуют как программу для ЭВМ, миниатюрную или небольшую по объему, что представляется некорректным, так как понятие «небольшой объем» — оценочное, и не понятно, по сравнению с каким объемом размер вирусной программы мал, а кроме того, объем памяти, который занимают компоненты вредоносных программ может быть сравнительно большим (например лог-файл трояна-кейлоггера может занимать сотни КБ).

4. Указание на то, что целью компьютерного вируса является разрушение хранимой в ЭВМ информации и программного обеспечения, как это сделано в «Информационном праве» В. А. Копылова [3] не позволяет значительное количество вредоносных программ, например, таких как программы-шпионы (Spy-ware), ряд троянских программ (парольные воры, клавиатурные мониторы и т.п.), а также программы Ad-Ware, целью которых является реклама.

5. Определять вредоносную программу как специально созданную *для нарушения нормального функционирования компьютерных программ*, как сформулировано в комментарии к УК РФ под редакцией С. А. Разумова, Г. Н. Борзенкова и В. П. Верина [4], неправильно. Часто вредоносные программы специально разрабатываются так, чтобы они не нарушали нормальную работу именно программ,

но нарушали бы функционирование компьютерной системы, либо, просто обеспечивали вывод на экран ненужной пользователю информации, которая лишь отвлекает пользователя либо способна наносить ему моральный вред, как это делают программы классов Ad-Ware и Bud-jouks.

6. Определение компьютерного вируса как «*программы, которая самопроизвольно присоединяется к другим программам и при запуске последних выполняет различные нежелательные действия (порча файлов и каталогов, искажение и уничтожение информации и т.д.)*» [5] некорректно, т. к. компьютерные вирусы могут активизироваться не только при запуске зараженных программ, но, например, при копировании на компьютер вирусных файлов с носителя, посещение зараженных веб-сайтов и т. д. Выражение «нежелательные действия» является неоднозначным, т. к., например, некоторые процессы, исполняющиеся в компьютере, могут быть нежелательны для пользователя, неспособного грамотно настроить систему.

7. Употребление терминов «программа-вирус» и «компьютерный вирус» как эквивалентных, в частности, приведенное в словаре-справочнике «Операции информационно-психологической войны» [5]: «*Программа-вирус (компьютерный вирус)*», является ошибочным, т. к. в этом случае определение не может быть распространено на многочисленный класс вредоносных программ для мобильных устройств, таких как сотовые телефоны, которые, имея встроенный микропроцессор, не являются в прямом смысле компьютером.

Некорректность определения программы-вируса часто связана с неполным или неверным указанием на характер деструктивных действий, совершаемых такими программами. Например, в словаре-справочнике «Операции информационно-психологической войны» [5] приведено следующее определение: «*программа-вирус — это вредоносная программа, приводящая к поражению или к полной утрате информации, которая «инфицирует» компьютерные файлы, вставляя в них свои копии, осуществляя это так, что копии будут выполняться, когда файл загружается в память компьютера, позволяя им инфицировать еще и другие файлы и т.д.*». Из этого определения следует, что программа-вирус приводит к *поражению или полной утрате информации*, хотя блокирование информации, засорение памяти или вывод на экран монитора посторонних сообщений могут быть совершены и без этих действий. Более правильным следует считать употребление терминов «модификация» и «уничтожение информации», а не «поражение» или «полная утрата информации».

Утверждение, что «программа-вирус вставляет свои копии в компьютерные файлы, чем и «инфицирует» их отражает особенности действий лишь нескольких видов вирусов. В большинстве случаев заражение компьютерной системы происходит иначе. Например, вирус может создавать видоизмененную копию только своего тела.

Отдельно следует выделить грубую ошибку, которую содержат многие источники — термины «вредоносная программа» и «компьютерный вирус» некорректно употребляются как синонимы. На самом деле, понятие «вредоносная программа» намного шире, чем термин «компьютерный вирус», т. к. многие программы, являющиеся вредоносными, не могут относиться к компьютерным вирусам, не обладая характерными для вирусов свойствами. Например, «логические бомбы» (программа, выполняемая периодически или однократно в определенный момент времени при наступлении определенных условий) не способны к размножению и не относятся к классу компьютерных вирусов, но являются вредоносными программами, т. к. способны нанести серьезный ущерб. Примерами тому являются следующие юридические документы: Концепция региональной информатизации до 2010, Приказ МНС РФ от 25 февраля 2004 г. № БГ-3-18/143 «Об утверждении Положения об обмене информацией по электронной почте в системе Министерства Российской Федерации по налогам и сборам при взаимодействии со сторонними организациями и Правил пользования автономными средствами электронной цифровой подписи и ключами электронной цифровой подписи», Решение коллегии ГТК РФ от 28 сентября 2001 г. «О Концепции информационно-технической политики Государственного таможенного комитета Российской Федерации», отраслевой руководящий документ «Порядок сбора, контроля, передачи и обработки первичной таможенной информации для формирования баз данных на всех уровнях таможенной службы» и т.д. Для того,

чтобы обеспечить единство терминологии, в документах и нормативно-правовых актах следует заменить термин «компьютерный вирус» на «вредоносная программа», указав его определение, которое будет едино для всех юридических документов.

Определение термина «вредоносная программа» должно удовлетворять следующим требованиям:

1) охватывать все известные разновидности вредоносных программ;

2) содержать конкретные признаки, в соответствии с которыми программа будет являться вредоносной;

3) распространяться не только на собственно вредоносные программы, но и те программы, которые способствуют их созданию (например, вирусные конструкторы, полиморфные генераторы и т.п.);

4) указывать, что вредоносные программы направлены на выполнение именно несанкционированных действий;

5) определять область, в которой производятся указанные выше действия, которая охватывает не только ЭВМ, системы ЭВМ и компьютерные сети, но и информационно-телекоммуникационные сети, в частности, сотовые сети связи;

6) указывать на то, что несанкционированные действия, связанные с вредоносными программами, носят материальный характер, то есть, в результате таких действий возможно причинение вреда;

7) определять субъекта, которому причиняется или может быть причинен вред в результате действий вредоносной программы;

8) соответствовать не только современным условиям, но и учитывать возможное появление в будущем новых видов вредоносных программ.

Исходя из изложенного выше, можно предложить следующее определение вредоносной программы:

«Вредоносная программа — это программа или фрагмент кода, специально созданная для выполнения или способствующая выполнению несанкционированных действий в информационной системе или информационно-телекоммуникационной сети, в результате которых возможно причинение вреда пользователям этой системы (сети) или другим лицам».

Следует отметить, что предложенное определение термина «вредоносная программа» в максимальной степени отвечает приведенным выше требованиям. Для программистов оно может рассматриваться как ориентир, определяющий возможное вольное или невольное нарушение закона, с учетом того, что, с юридической точки зрения, ответственность за создание, распространение и использование вредоносных программ наступает только после наступления последствий, указанных в ст. 273 УК РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Создание, использование и распространение вредоносных программ для ЭВМ. — (http://download.referat.ru).

2. *Кожинов В.Я.* Основы бухгалтерского учета / В. Я. Кожинов // Система Гарант. — 2003. — 364 с.

3. *Копылов В.А.* Информационное право / В. А. Копылов. — М. : Юристъ. 1997. — 24 с.

4. *Разумов С.А.* Комментарий к УК РФ / С. А. Разумов, Г. Н. Борзенков, В. П. Верин и др.; отв. ред. В. М. Лебедев 3-е изд., доп. и испр. — М. : Юрайт-Издат 2004. — 223 с.

5. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В. Б. Вепринцев, А. В. Манойло, А. И. Петренко, Д. Б. Фролов; под ред. А. И. Петренко. — М. : Горячая линия — Телеком, 2005. — 495 с.

6. Вирусная энциклопедия. — (http://www.viruslist.com/ru/viruses/encyclopedia).

7. *Евгений Касперский.* Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения. — (http://www.jetinfo.ru/2003/12/2/article2.12.2003.html).

8. Информационная безопасность и защита информации в информационных системах. / А. С. Дубровин, М. Г. Матвеев, Е. А. Рогозин, В. И. Сумин. — Воронеж. гос. технол. акад., Воронеж, 2005. — 292 с.

9. *Уоллес Ванг.* Безопасная работа в Интернет / Ванг Уоллес. — М. : Диа СофтЮП, 2005. — 400 с.

10. Энциклопедия компьютерных вирусов — Virus Encyclopedia. (http://kgk.bashnet.ru/comp/avp/sub.htm).