Воробьёв В. В.

кандидат юридических наук, доцент,
заведующий кафедрой «Уголовное право и криминология»,
ГОУ ВО «Коми республиканская академия
государственной службы и управления»

Вредоносные компьютерные программы в уголовном законодательстве Российской Федерации

В статье представлены различные точки зрения на определение вредоносной программы в уголовном праве. Дана классификация и выявлены особенности различных видов вредоносных программ и программ, которые могут быть использованы как вредоносные. Дано авторское определение вредоносной компьютерной программы.

Ключевые слова: *вредоносная компьютерная программа, компьютерная информация, вирус, троянская программа.*

Vorobyov V. V.

PhD (Jurisprudence), associate professor, head of the department
of criminal law and criminology of Public Educational Institution
«Komi republican academy of public service and management»

Harmful computer programs in the criminal legislation of the Russian Federation

Various points of view on definition of the harmful program in criminal law are presented in the present article. Classification is given and features of different types of harmful programs and programs which can be used as harmful are revealed. Author's definition of the harmful computer program is given.

Keywords: *harmful computer program, computer information, virus, Trojan program.*

В действующем уголовном кодексе Российской Федерации в составе ст. 273 предусмотрена уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ. В ч. 1 ст. 273 УК РФ законодатель предусмотрел ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо

предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [1].

Согласно судебной статистике, в 2012 году в России к уголовной ответственности по ст. 273 было привлечено 210 человек, в 2013 – 200, а за первые 6 месяцев 2014 года осуждено 68 человек [2].

Список стран, которые распространяют вредоносный код выглядит следующим образом: США – 240022553 атаки; Россия – 138554755; Нидерланды – 92652499; Германия – 82544498; Украина – 47886774 атаки. Следует отметить, что на первых двух строчках этого списка уже довольно давно закрепились в лидерах и не собираются никого пропускать вперед США и Россия. Что касается Нидерландов и Германии, то в этих странах просто легко и дешево регистрировать сайты. Этим и пользуются владельцы сайтов из России, Украины, Белоруссии и пр.

Отдельно следует выделить Китай (он на 6-м месте). В 2009 г. именно Китай был бесспорным лидером по заражению компьютеров. Однако сейчас идет сильнейший спад вирусной активности в данной стране. Причиной этому стало жесткое регулирование властями регистрации доменных имен.

Пятерка самых уязвимых стран в настоящее время выглядит так: Россия – 55,9%; Оман – 54,8%; США – 50,1%; Армения – 49,6% и Белоруссия – 48,7% [3].

Широкая распространенность и высокая общественная опасность этих преступлений не вызывает сомнений, однако судебная статистика свидетельствует о низком уровне раскрываемости этой категории преступлений. Основной причиной такого низкого уровня борьбы с оборотом вредоносных программ является специфичность состава ст. 273 УК РФ, его связь с компьютерными науками. В указанной норме закреплен ряд компьютерных терминов, которые нуждаются в подробном разъяснении.

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.02.2015) // Собрание законодательства РФ. 17.06.1996. – № 25. Ст. 2954.

[2] Сводные статистические сведения о состоянии судимости в России за 2012 год // http://www.cdep.ru/index.php?id=79&item=1776; Сводные статистические сведения о состоянии судимости в России за 2013 год // http://www.cdep.ru/index.php?id=79&item=2362; Сводные статистические сведения о состоянии судимости в России за первое полугодие 2014 г. // http://www.cdep.ru/index.php?id=79&item=586.

[3] Быков В.М., Черкасов В.Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. – 2012. – № 7. – С. 16–21.

Из содержания диспозиции ч. 1 ст. 273 УК РФ мы видим, что общественная опасность деяния формируется в связи с созданием вредоносной программы, которая является продуктом преступной деятельности. Вредоносная программа не является предметом преступления, так как именно она оказывает на него разрушительное воздействие. Поэтому, вредоносные компьютерные программы не могут выступать в качестве факультативного признака объекта преступления состава ст. 273 УК РФ, а являются продуктами преступной деятельности, которые следует относить к такому элементу состава преступления как объективная сторона. Информация же, блокирование, модификация или копирование которой может произойти при использовании вредоносной программы должна признаваться предметом преступления, так как законодатель связывает оборот именно вредоносных программ с опасностью нормального существования и функционирования компьютерной информации [4].

Таким образом, ключевым понятием, содержащимся в данной норме, является «вредоносная программа». Этот термин имеет как доктринальное, так и нормативное толкование.

Так, по мнению И.А. Клепицкого, вредоносная программа – это программа, приводящая к несанкционированному (т.е. не разрешенному владельцем информации, пользователем, иным уполномоченным лицом) уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети [5].

Ранее нами предлагалось под вредоносной программой понимать такое программное средство, которое было создано для выполнения не санкционированных собственником и другими законными пользователями информации, ЭВМ, системы ЭВМ или их сети функций. Под нежелательными функциями подразумевалось несанкционированное уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сетей, а также вывод из строя системы защиты информации [6].

---

[4] Воробьев В.В. О предмете преступления и его особенностях в компьютерных преступлениях // Общественная безопасность как научная категория: уголовно-правовой и криминологический аспекты: Материалы научно-практической конференции (Н. Новгород, 14 марта 2014 г.). – Н Новгород, 2014. – С. 14–19.

[5] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. – М., 2006. – С. 491.

[6] Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.Т. Томина, В.В. Сверчкова. – 7-е изд., перераб и доп. – М., 2011. – С. 1117–1118.

Вредоносной программой следует считать уже компилированный (иначе – машиночитаемый) текст программы, т.е. программа должна находиться в электронном виде и быть способной осуществлять вредоносные функции. Написание же текста программы без ее компилирования следует квалифицировать как покушение на создание вредоносной программы.

Ранее, нами, также отмечалось, что вредоносность программы определяется не только способностью уничтожать, блокировать, модифицировать или копировать информацию (это рабочие функции большого количества вполне легальных программ), а основной особенностью вредоносных программ является то, что они выполняют эти функции без предварительного уведомления или получения согласия (санкции) собственника или другого законного владельца информации [7].

Наиболее распространенными, по мнению М.М. Карелина, видами вредоносных программ являются компьютерные вирусы, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации и программы-патчеры [8].

К.Н. Евдокимов предлагает вредоносные компьютерные программы рассматривать как специальные компьютерные программы, созданные с целью несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а также совершения иных противоправных деяний (например, рассылка спама, фишинга, кибершпионажа, кибершантажа, управление зараженным компьютером, создание ботнетов и др.) [9].

Таким образом, мы видим, что единства мнений по формулированию юридического определения вредоносной программы не наблюдается. Аналогичная ситуация складывается и в нормативном закреплении этого термина.

---

[7] Комментарий к уголовному кодексу Российской Федерации / Отв. ред. А.А. Чекалин; Под ред. В.Т. Томина, В.В. Сверчкова. 4-е изд., перераб. и доп. – М., 2007. – С. 1038.

[8] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.М. Лебедев. – М., 2010. – С. 687.

[9] Евдокимов К.Н. К вопросу о совершенствовании объективной стороны состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. – 2013. – № 7. – С. 18–24.

Так, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации устанавливает, что вредоносная программа – это созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети [10].

В инструкция по проведению антивирусного контроля в информационных системах персональных данных территориального органа Росреестра говорится, что вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции (сервера);
- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных [11].

Согласно постановления Правительства РФ от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи», вредоносное программное обеспечение – это программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и

[10] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Заключено в г. Минске 01.06.2001) Соглашение вступило в силу для России 17.10.2008 // Собрание законодательства РФ. 30 марта 2009 г. – № 13. Ст. 1460.

[11] Инструкция по проведению антивирусного контроля в информационных системах персональных данных территориального органа Росреестра: Приказ Росреестра от 29.01.2013 № П/31 (Документ не был опубликован).

(или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи. Спам – это телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя [12].

Типов вредоносных программ известно великое множество, а каждый тип состоит из огромного количества образцов, также отличающихся друг от друга. Для борьбы с ними нужно уметь однозначно классифицировать любую вредоносную программу и легко отличить ее от других вредоносных программ.

«Лаборатория Касперского» классифицирует все виды вредоносного программного обеспечения и потенциально нежелательных объектов в соответствии с их активностью на компьютерах пользователей.

Отдельные вредоносные программы часто выполняют несколько вредоносных функций и используют несколько способов распространения.

Например, существуют вредоносные программы, которые занимается сбором адресов электронной почты на зараженном компьютере без ведома пользователя. При этом они распространяется как в виде вложений электронной почты, так и в виде файлов через сети P2P. Тогда эти программы можно классифицировать и как Email-Worm, и как P2P-Worm или Trojan-Mailfinder. Такие программы принято называть «Многофункциональные вредоносные программы».

Компьютерные вирусы и компьютерные черви рассматривается как вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

[12] Об утверждении Правил оказания телематических услуг связи: Постановление Правительства РФ от 10.09.2007 № 575 (ред. от 16.02.2008) // Собрание законодательства РФ. 17.09.2007. – № 38. Ст. 4552.

Любая программа данного подкласса вредоносного ПО в качестве дополнительных может иметь и функции троянской программы.

Троянские программы — это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать: удаление данных; блокирование данных; изменение данных; копирование данных; замедление работы компьютеров и компьютерных сетей.

В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

Помимо вирусов и троянских программ, выделяется шпионское программное обеспечение. Категория Adware, Pornware и Riskware включает легально разработанные программы, которые в определенных случаях могут представлять особую опасность для пользователей компьютеров (действуя так же, как шпионское программное обеспечение) [13].

Из приведенного перечня и разнообразия программных продуктов, изначально созданных для причинения вреда, а также программ, предназначенных для выполнения полезных функций, но могущих быть использованными в преступных целях, видно, что уголовное законодательство нуждается в закреплении единого легального определения вредоносной программы.

Так, исходя из смысла диспозиции ч. 1 ст. 273 УК РФ видно, что уголовная ответственность наступает за манипуляции с программами, заведомо предназначенными для несанкционированного воздействия на компьютерную информацию. Словосочетание «заведомо предназначенных для несанкционированного» означает, что программа была изначально создана как вредоносная. Таким образом, законодатель исключил возможность признать программу вредоносной, если злоумышленник применил легальную, изначально полезную программу в преступных целях. К примеру, виновный совершил несанкционированное уничтожение или копирование персональных данных при помощи программы категории Riskware, например, утилиты удаленного администрирования. В этом случае квалификация должна проводиться лишь по ст. 272 УК РФ, а использование вредоносной программы, ответственность за которое предусмотрена ст. 273 УК РФ отсутствует. Данную утилиту необходимо рассматривать как предмет, используемый в качестве орудия преступления. Тогда как использование для совершения этого же преступления троянской программы типа «Бэк-

[13] Виды шпионского ПО // www.kaspersky.ru/internet-security-center/threats/adware-pornware-riskware.

дор» следует квалифицировать по совокупности преступлений, предусмотренных ст.ст. 272 и 273 УК РФ. В этом случае, соответствующую троянскую программу следует определить, как орудие совершения преступления.

Подводя итог исследования и руководствуясь вышеизложенным предлагается под вредоносной программой понимать такую программу, которая изначально предназначена для выполнения не санкционированных собственником либо другим законным пользователем или владельцем информации функций в виде уничтожения, блокирования, модификации или копирования компьютерной информации, а также нейтрализации средств защиты компьютерной информации.

Используемые источники

1. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Заключено в г. Минске 01.06.2001) Соглашение вступило в силу для России 17.10.2008 // Собрание законодательства РФ. 30 марта 2009 г. – № 13. Ст. 1460.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.02.2015) // Собрание законодательства РФ. 17.06.1996. – № 25. Ст. 2954.
3. Об утверждении Правил оказания телематических услуг связи: Постановление Правительства РФ от 10.09.2007 № 575 (ред. от 16.02.2008) // Собрание законодательства РФ. – 17.09.2007. – № 38. Ст. 4552.
4. Инструкция по проведению антивирусного контроля в информационных системах персональных данных территориального органа Росреестра: Приказ Росреестра от 29.01.2013 № П/31 (Документ не был опубликован).
5. Быков В.М., Черкасов В.Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. – 2012. – № 7.
6. Виды шпионского ПО // www.kaspersky.ru/internet-security-center/threats/adware-pornware-riskware.
7. Воробьев В.В. О предмете преступления и его особенностях в компьютерных преступлениях // Общественная безопасность как научная категория: уголовно-правовой и криминологический аспекты: Материалы научно-практической конференции (Н. Новгород, 14 марта 2014 г.). – Н. Новгород, 2014.

8. Евдокимов К.Н. К вопросу о совершенствовании объективной стороны состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. – 2013. – № 7.
9. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. А.И. Рарог. – М., 2006.
10. Комментарий к уголовному кодексу Российской Федерации / отв. ред. А.А. Чекалин; Под ред. В.Т. Томина, В.В. Сверчкова. 4-е изд., перераб. и доп. – М., 2007.
11. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В.М. Лебедев. – М., 2010.
12. Комментарий к Уголовному кодексу Российской Федерации / под ред. В.Т. Томина, В.В. Сверчкова. – 7-е изд., перераб и доп. – М., 2011.
13. Сводные статистические сведения о состоянии судимости в России за 2012 год // http://www.cdep.ru/index.php?id=79&item=1776; Сводные статистические сведения о состоянии судимости в России за 2013 год // http://www.cdep.ru/index.php?id=79&item=2362; Сводные статистические сведения о состоянии судимости в России за первое полугодие 2014 г. // http://www.cdep.ru/index.php?id=79&item=586.