УДК 343.8
Код РИНЦ 10.81.71

К ВОПРОСУ О ПОНЯТИИ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ НА СОВРЕМЕННОМ ЭТАПЕ

© 2019 Шаповалова Анастасия Валериевна
студент
© 2019 Якубов Никита Александрович
студент
© 2019 Осипов Данила Денисович
преподаватель
Самарский государственный экономический университет
E-mail: proof-mast@mai.ru

Ключевые слова: вредоносная программа, компьютерная программа, компьютерные преступления.

В статье обращается внимание на неоднозначное толкование термина «вредоносная компьютерная программа»; выявляются отличительные признаки программ, приспособленных для совершения несанкционированных действий (даже если они являются легальными), а также предлагаются предупредительные меры в целях защиты информации от ее уничтожения, блокирования, модификации, копирования или нейтрализации.

Развитие информационных технологий, активное применение электронного документооборота привело к изменению способа хранения информации. Использование программных продуктов в значительной степени упрощает работу с массивом данных, что особенно актуально для крупных организаций.

Общественные отношения, складывающиеся по поводу создания, использования и распространения компьютерных программ, продолжают стремительно развиваться, и, вместе с этим, влекут появление новых преступных схем.

Считаем необходимым обратиться к норме-дефиниции и ее толкованию. В примечании 1 к ст. 272 Уголовного кодекса Российской Федерации (далее - УК РФ), содержится следующая формулировка: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Действия, направленные на несанкционированное уничтожение, блокирование, модификацию, копирование или нейтрализацию средств защиты[1] такой информации являются противоправными.

Проблема, связанная с применением норм ст. 272 и 273 УК РФ, связана в основном с отсутствием единого понимания вредоносной компьютерной программы, позволяющей совершить одно или несколько вышеуказанных действий.

Согласно п. п. 2.6.5 и 2.6.6 Национального стандарта "Защита информации. Основные термины и определения Protection of Information. Basic Terms and Definitions ГОСТ Р 50922-2006", утвержденного Приказом Ростехрегулирования от 27 декабря 2006 г.

№ 373-ст вредоносная программа определяется как «программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы».

В соглашении о сотрудничестве государств-членов Содружества Независимых Государств закрепилось иное толкование термина «вредоносная программа», а именно: «созданная или существующая программа со специально внесенными, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети»[2].

Е. А. Ефремова по-иному трактует понятие «вредоносная программа», выделяя такой признак как способность к осуществлению противоправных действий без ведома пользователя.

А. П. Кузнецов, частично соглашаясь с Е. А. Ефремовой отмечает, что операции по уничтожению, блокированию и т.д. информации способны выполнить и лицензионные программы, установленные на ЭВМ пользователя. Принимая во внимания такое обстоятельство, А. П. Кузнецов выделил два критерия, по одному из которых можно определить компьютерную программу как вредоносную. Во-первых, отсутствие сведений о наличии такой программы на ЭВМ добросовестного пользователя, а, во-вторых, отсутствие согласия на использование такой программы.

М. М. Малыковцев дает иное определение «вредоносной программы». По его мнению, это программа, написанная на любом языке программирования, использование которой влечет неправомерное воздействие как на информацию, так и на сами технические средства и связь.

Все перечисленные определения понятия компьютерной программы различны и не отражают всех признаков данной категории.

Думается, что со стремительным развитием IT-технологий, появлением новых способов несанкционированного уничтожения и изменения компьютерной информации, введение единого определения с конкретным набором признаков почти бессмысленно.

Во-первых, потому, что потенциальный субъект преступления обладает специальными знаниями и способен создать такую компьютерную программу, которая хотя и не будет отвечать признакам, указанным в УК РФ и иных нормативно-правовых актах, но нанесет существенный ущерб. То есть будут совершены приносящие вред действия, но квалифицироваться как преступление не будут. Соответственно, такие действия останутся безнаказанными.

Во-вторых, законодательство, скорее всего, не будет успевать вносить изменения в определение понятий, внося дополнительные критерии и характеристики.

Таким образом, наиболее рациональным представляется обратить особое внимание не на детальную характеристику вредоносной компьютерной программы либо информации, а именно на степень ущерба, который был принесен. При этом необходимо выделить один основной признак вредоносной программы - совершение противоправного деяния путем применения такого программного продукта.

Более того, с появлением систем «умный дом» и пр. подобным угрозам подвержены не только компьютерные устройства, но и потребительская бытовая техника. Совре-

менное бытовое оборудование во многом технически приравнивается к компьютерным устройствам, подверженные взлому и заражению[3].

Имеющееся в законодательных актах определение термина «вредоносная программа» не позволяет отнести к таковым программы-шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а сбор сведений об активности пользователя в сети Интернет (о посещаемых сайтах, совершаемых покупках и т.п.), программы "злые шутки" (Bad Jokes)[4], так называемые "вирусные конструкторы" - программы, созданные, главным образом, не в целях осуществления атак на компьютерные ресурсы, а для генерирования новых вирусов.

Общепринятый подход не позволяет отнести к вредоносным также программы, объективно приспособленные к совершению преступлений, но при этом созданные на основе легального программного обеспечения.

Однако наиболее важно предупредить создание, использование и распространение вредоносных компьютерных программ, прежде чем будет совершено преступление посредством их применения.

Некоторые разрешенные к обороту программы часто становятся инструментом для совершения злоумышленниками преступлений. Например, программы для записи дисков (InfraRecoder, BurnAware, Nero и др.) применяются злоумышленниками в целях изготовления контрафактной продукции (неправомерного копирования информации), программное обеспечение для удаленного администрирования (RDP, VNC, DameWare, TeamViewer, Remote Office Manager, Hamachi и т.д.), как правило, применяется при совершении хищений, связанных с неправомерным вмешательством в системы дистанционного банковского обслуживания. Однако вредоносными их признавать нельзя, так как такие программы по факту остаются аутентичными, сохраняют стандартный набор настроек и возможностей, заложенный разработчиком.

В целях защиты компьютерных сведений служат технические, программные средства и криптосистемы. Например, 1) антивирус; 2) программа, устраняющая незаконное дублирование сведений; 3) защита, встроенная в операционную систему.

Предприятиям, организациям и пр. следует предпринять усиленные меры защиты. Как правило, на их ЭВМ хранятся наиболее крупные и ценные массивы данных, ведется бухгалтерский учет. Наиболее эффективным представляется привлечение квалифицированных специалистов в области IT-технологий, которые создадут для конкретной организации индивидуальный программный продукт, препятствующий совершению несанкционированных действий. Такая программа будет предназначена лишь для одного потребителя.

Применение таких известных антивирусных программ как «Kaspersky», «Dr. Web» и пр. могут оказаться малоэффективными, поскольку предназначены для приобретения и использования любым желающим, а значит, становятся наиболее изученными потенциальными преступниками.

Создание индивидуальных антивирусных систем, возможно, потребует крупных материальных вложений пользователя, больших временных затрат. Однако такие издержки будут полностью оправданы, если велика ценность информации, которая может быть уничтожена, скопирована либо изменена из-за несанкционированных действий.

С развитием IT-индустрии стало возможным применение «cloud technologies» или «облачных технологий». С помощью «облачного хранилища» можно создать общую папку для всех персональных компьютеров и даже смартфонов. В целях надежной защиты доступа к информации посторонних лиц станет полное удаление таковой информации с компьютера пользователя, например, после второй неудачной попытки доступа. Таким образом, постороннее лицо не сможет получить какие-либо данные, а после выяснения подозрительных причин входа в систему, владелец сможет восстановить эти данные, синхронизировав их.

Не исключено, что в будущем вредоносные программные продукты все больше будут направлены не на отношения информационной безопасности как таковые, а на иные социально значимые сферы - жизнь, здоровье, честь и достоинство личности, неприкосновенность частной жизни, отношения собственности, общественный порядок и др. Наша задача - предпринять необходимые меры для предотвращения неблагоприятных последствий и минимизации риска применения таких программ.

---

[1] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 02.08.2019) // СПС Консультант Плюс (дата обращения 25.09.2019 г.);

[2] «Собрание Законодательства Российской Федерации», 2009. №13;

[3] Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: Дис. … канд. юрид. наук / Е.А. Маслакова. Орел, 2018. 412 с.

[4] Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. 2019. № 3 (79). 273 с.

TO THE QUESTION OF THE CONCEPT OF MALICIOUS COMPUTER PROGRAMS AT THE MODERN STAGE

© 2019 Shapovalova Anastasiya Valerievna
Student
© 2019 Yakubov Nikita Alexsandrovich
Student
© 2019 Osipov Danila Denisovich
Lecturer
Samara State University of Economics
E-mail: proof-mast@mail.ru

Keywords: malware, computer program, computer crimes.

The article draws attention to the ambiguous interpretation of the term "malicious computer program"; identifies the distinctive features of programs designed to perform unauthorized actions (even if they are legal), and proposes preventive measures to protect information from its destruction, blocking, modification, copying or neutralization.