

УДК 004.49

В.В. Воробьёв**V. Vorobyov**

О ПОНЯТИИ И ВИДАХ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

ON THE CONCEPT AND THE TYPES OF MALICIOUS SOFTWARE

В статье представлены различные точки зрения на определение понятия «вредоносная программа» в уголовном праве. Дана классификация и выявлены особенности как различных видов вредоносных программ, так и программ, которые могут быть использованы в этом качестве. Дано авторское определение термина «вредоносная компьютерная программа».

The article presents a different perspective on the definition of «malware» in criminal law. The classification and the peculiarities of the just-personal types of malicious programs and programs that can be used as such. The author's definition of the term «malicious computer program» is given.

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

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

В действующем УК РФ в составе ст.273 предусмотрена уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ. В частности, 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 г. в России к уголовной ответственности по ст. 273 было привлечено 210 человек, в 2013 г. – 200, а за первые 6 месяцев 2014 г. 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 в качестве лидеров в этом списке уже довольно давно закрепились и не собираются никого пропускать вперёд США и Россия. Что касается Нидерландов и Германии, то в этих странах просто легко и дешево регистрировать сайты, чем и пользуются владельцы сайтов из России, Украины, Белоруссии и пр.

Отдельно следует выделить Китай (он на 6-ом месте). В 2009 г. именно Китай был бесспорным

лидером по заражению компьютеров, однако сейчас здесь наблюдается сильнейший спад вирусной активности. Это связано с жестким регулированием властями регистрации доменных имён.

Пятёрка самых уязвимых стран сегодня выглядит следующим образом: Россия – 55,9%; Оман – 54,8%; США – 50,1%; Армения – 49,6% и Белоруссия – 48,7% [3].

Широкая распространённость и высокая общественная опасность указанных преступлений не вызывает сомнений, в то же время судебная статистика свидетельствует о низком уровне их раскрываемости. Основной причиной низкой результативности борьбы с оборотом вредоносных программ является специфичность состава ст.273 УК РФ, его связь с компьютерными науками. В указанной норме закреплён ряд компьютерных терминов, которые нуждаются в подробном разъяснении.

Из содержания диспозиции ч.1 ст.273 УК РФ следует, что общественная опасность деяния формируется в связи с созданием вредоносной программы, которая является продуктом преступной деятельности. Вредоносная программа не является предметом преступления, т.к. 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, т.к. законодатель связывает оборот именно вредоносных программ с опасностью нормального существования и функционирования компьютерной информации [4].

Таким образом, ключевым понятием, содержащимся в данной норме, является понятие «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 разрешённому 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].

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 её 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). 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 распространёнными видами вредоносных программ, по мнению М.М. Карелина, 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 спе-

циальные компьютерные программы, созданные с целью несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств её защиты, а также совершения иных противоправных деяний (например, рассылка спама, фишинг, кибершпионаж, кибершантаж, управление заражённым компьютером, создание ботнетов и др.) [9].

Таким образом, мы видим, что на данный момент нет единства мнений по формулированию юридического определения вредоносной программы. Аналогичная ситуация складывается и с нормативным закреплением этого термина.

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 внесёнными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети [10].

В инструкции 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 удалённых);
- 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 Постановлению Правительства РФ «Об утверждении Правил оказания телематических услуг связи» от 10.09.2007 № 575 вредоносное программное обеспечение – это программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и/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 неопределённому кругу лиц, доставленное абоненту и/или пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нём несуществующего или фальсифицированного адреса отправителя [12].

Типов вредоносных программ известно великое множество. В свою очередь, каждый из них состоит из огромного количества образцов, также отличающихся друг от друга. Для борьбы с ними нужно уметь однозначно классифицировать любую вредоносную программу и легко отличать её от других вредоносных программ.

«Лаборатория Касперского» классифицирует вредоносное программное обеспечение и потенциально нежелательные объекты в соответствии с их активностью на компьютерах пользователей (см. рис.).

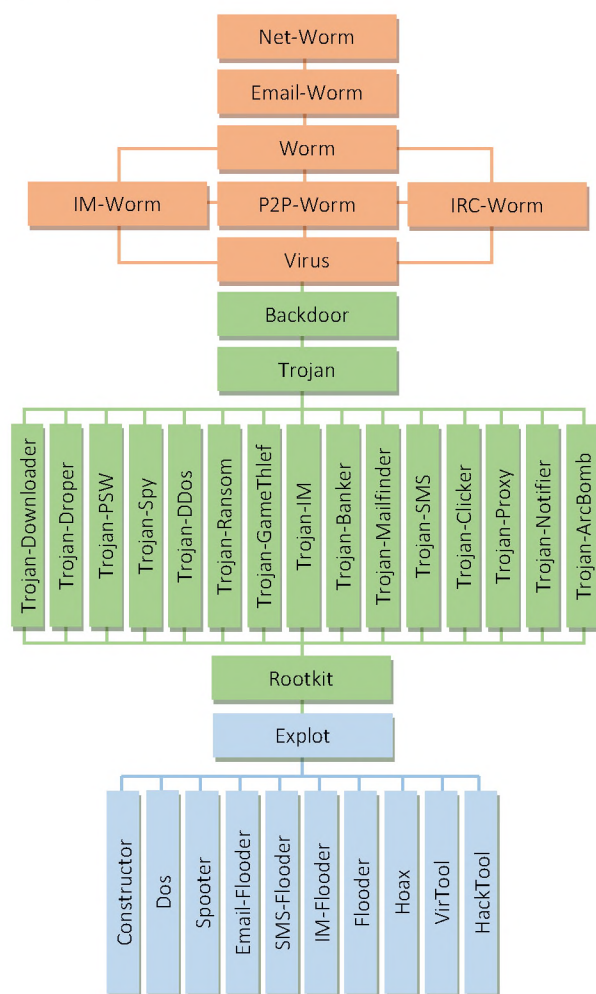


Рис. Виды вредоносного программного обеспечения и потенциально нежелательных объектов в соответствии с их активностью на компьютерах пользователей [13]

Типы поведения, представляющие наименьшую опасность, показаны в нижней области диаграммы, а типы поведения с максимальной опасностью отображаются в её верхней части.

Вредоносные программы зачастую выполняют несколько вредоносных функций и распространяются несколькими способами.

Например, существуют вредоносные программы, которые занимаются сбором адресов электронной почты на заражённом компьютере без ведома пользователя. При этом они распространяются как в виде вложений в сообщения электронной почты, так и в виде файлов через сети P2P. Следовательно, 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 рассматриваются 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 множество типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Вредоносное программное обеспечение из подкласса вирусов и червей включает в себя следующие программы: *Email-Worm*, *IM-Worm*, *IRC-Worm*, *Net-Worm*, *P2P-Worm*, *Virus*.

Большинство известных компьютерных червей распространяется следующими способами:

- в виде файла, отправленного во вложении в электронном письме;
- в виде ссылки на интернет или *FTP*-ресурс;
- в виде ссылки, переданной через сообщение *ICQ* или *IR*;
- через пиринговые сети обмена данными P2P (*peer-to-peer*);
- некоторые черви распространяются как сетевые пакеты. Они проникают прямо в компьютерную память, затем активируется код червя.

Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или бреши в защите операционной системы и приложений. Многие черви распространяют свои копии через сеть несколькими способами.

Вирусы можно классифицировать в соответствии с тем, каким способом они заражают компьютер: файловые вирусы, вирусы загрузочного сектора, макровирусы, вирусные скрипты [14].

Любая программа данного подкласса вредоносного программного обеспечения в качестве

дополнительных может иметь и функции троянской программы.

Троянские программы – это вредоносные программы, выполняющие не санкционированные пользователем действия. Такие действия могут включать в себя удаление, блокирование, изменение и копирование данных, замедление работы компьютеров и компьютерных сетей. В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на компьютере.

Backdoor (бэкдор). Троянская программа *Backdoor* предоставляет злоумышленникам возможность удалённого управления заражёнными компьютерами. Такие программы позволяют автору выполнять на заражённом компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера. Троянцы-бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.

Exploit (эксплойт). Эксплойты – это программы с данными или кодом, использующие уязвимость в работающих на компьютере приложениях.

Rootkit (руткит). Руткиты – это программы, предназначенные для сокрытия в системе определённых объектов или действий. Часто их основная цель – предотвратить обнаружение вредоносных программ, чтобы увеличить время их работы на заражённом компьютере.

Trojan-Banker (банковские троянцы). Банковские троянцы предназначены для кражи учётных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.

DDoS-троянцы. Это программы для проведения атак типа «отказ в обслуживании» (*Denial of Service, DoS*) по целевым веб-адресам. При такой атаке с заражённых компьютеров системе с определённым адресом отправляется большое количество запросов, что может вызвать её перегрузку и привести к отказу в обслуживании.

Trojan-Downloader. Данные программы способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ, включая троянские и рекламные программы.

Trojan-Droper. Эти программы используются хакерами, чтобы установить троянские программы и/или вирусы или предотвратить обнаружение вредоносных программ. Не каждая антивирусная программа способна выявить все компоненты троянских программ данного типа.

Trojan-FakeAV. Программы этого типа имитируют работу антивирусного программного обеспечения. Они созданы, чтобы вымогать деньги

у пользователя в обмен на обещание обнаружения и удаления угроз, хотя угроз, о которых они сообщают, в действительности не существует.

Игровые троянцы. Программы для кражи информации об учётных записях участников сетевых игр.

IM-троянцы. Программы *Trojan-IM* крадут логины и пароли к программам мгновенного обмена сообщениями, таких как *ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype* и многие другие.

Trojan-Ransom. Троянские программы этого типа могут изменить данные на компьютере таким образом, что он перестаёт нормально работать, а пользователь лишается возможности использовать определённые данные. Злоумышленник обещает восстановить нормальную работу компьютера или разблокировать данные после уплаты запрашиваемой суммы.

SMS-троянцы. Такие программы отправляют текстовые сообщения с мобильного устройства на платные телефонные номера с повышенным тарифом, тратя ваши деньги.

Trojan-Spy (шпионские программы). Способны скрыто наблюдать за использованием компьютера, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана и получая список работающих приложений.

Trojan-Mailfinder. Способны собирать на компьютере адреса электронной почты.

Встречаются и такие виды троянских программ, как *Trojan-ArcBomb, Trojan-Clicker, Trojan-Notifier, Trojan-Proxy, Trojan-PSW* [15].

Помимо вирусов и троянских программ выделяется шпионское программное обеспечение. Категория *Adware, Pornware u Riskware* включает в себя легально разработанные программы, которые в определённых случаях могут представлять особую опасность для пользователей компьютеров (действуя так же, как шпионское программное обеспечение) [16].

Adware – это программы, предназначенные для показа рекламы на компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о пользователе (например, какого рода сайты он посещает), чтобы реклама соответствовала определённым интересам.

Adware-программы собирают данные с согласия пользователя, поэтому не следует их путать с троянскими программами-шпионами, которые собирают информацию без разрешения и ведома пользователя. Если же **Adware-программа** не уведомляет о сборе информации, она становится вредоносной. Например, вредоносная программа троянец-шпион (*Trojan-Spy*).

За исключением показа рекламы и сбора данных такие программы, как правило, не проявля-

ют своего присутствия в системе. Обычно у такой программы отсутствует значок на панели задач, и в меню программ она тоже отсутствует.

Adware-программы могут попасть в компьютер двумя основными путями:

1. С бесплатным или условно-бесплатным программным обеспечением *Adware*-программы могут входить на вполне законных основаниях в состав некоторых бесплатных или условно-бесплатных программ в качестве рекламной составляющей. Доходы от такой рекламы помогают финансировать их разработку.

2. Через заражённые веб-сайты. Посещение заражённого веб-сайта может привести к несанкционированной установке *Adware*-программы на компьютер. В этих целях часто используются хакерские технологии. Например, для проникновения в компьютер может использоваться уязвимость браузера и троянская программа, предназначенная для незаметной установки *Adware*. Действующие таким образом *Adware*-программы часто называют *Browser Hijackers* [17].

Pornware – это программы, отображающие на устройстве порнографический контент. Кроме программ, намеренно устанавливаемых некоторыми пользователями на свои компьютеры и мобильные устройства для поиска и отображения порнографического контента, категория *Pornware* также включает программы, установленные со злонамеренной целью без уведомления пользователя об их присутствии (обычно для рекламирования платных порнографических веб-сайтов и сервисов).

Вирусописатели могут использовать неисправленные уязвимости в популярных приложениях и операционных системах для установки *Pornware*-программ на компьютер, планшет или смартфон. Кроме того, заражение ими устройств возможно с помощью троянских программ, таких как *Trojan-Downloader* и *Trojan-Dropper*. Например, *Pornware*-программы, дозванивающиеся до телефонных служб «для взрослых», телефонные номера и/или специальный код которых сохранены в теле таких программ. В отличие от вредоносных программ программы дозвона уведомляют пользователя о совершаемых ими действиях.

Porn-Downloader – программы, которые загружают из Интернета в компьютер пользователя порнографические мультимедийные файлы. В отличие от вредоносных программ они уведомляют пользователя о совершаемых ими действиях.

Porn-Tool – программы, осуществляющие поиск и отображение порнографического контента на компьютере пользователя. Это могут быть специальные панели инструментов для веб-браузеров и специальные проигрыватели видеороликов [18].

К категории *Riskware* относят легальные программы, которые могут причинить вред компью-

теру, если используются злоумышленниками для удаления, блокирования, изменения или копирования данных, а также для нарушения работы компьютеров и сетей. В категорию *Riskware* входят следующие виды программ, которые широко используются в легальных целях: утилиты удалённого администрирования; программы-клиенты *IRC*; программы дозвона; программы для загрузки файлов; программное обеспечение для мониторинга активности компьютеров; утилиты управления паролями; серверные веб-службы, такие как *FTP*, *Web*, *Proxy* и *Telnet*.

По своему назначению это не вредоносные программы, но некоторые их функции могут быть использованы в преступных целях.

При таком большом количестве легальных программ, которые злоумышленники могут использовать в незаконных целях, нелегко решить, какие из программ представляют угрозу. Например, программы удалённого администрирования часто используются системными администраторами и службами поддержки клиентов для диагностики и устранения неполадок, возникающих на компьютерах пользователей. Однако если такая программа установлена на вашем компьютере злоумышленником (без вашего ведома), он получит удалённый доступ к вашему компьютеру. Полностью контролируя ваш компьютер, злоумышленник сможет использовать его практически в любых нужных ему целях.

Специалистами «Лаборатории Касперского» выявлены случаи секретной установки легальных программ удалённого администрирования, таких как *WinVNC*, для получения полного удалённого доступа к компьютеру.

В качестве другого примера можно взять утилиту *mIRC* – легальную сетевую программу-клиент *IRC*, которая может использоваться злоумышленниками в незаконных целях. Часто вредоносные программы устанавливают программу-клиент *mIRC* для последующего вредоносного использования. В таких случаях *mIRC* обычно сохраняется в папке *Windows* и вложенных в неё папках.

Существуют следующие виды *Riskware*-программ: *Client-IRC*; *Client-P2P*; *Client-SMTP*; *Dialer*; *Downloader*; *Fraud Tool*; *Monitor*; *NetTool*; *PSWTool*; *RemoteAdmin*; *RiskTool*; *Server-FTP*; *Server-Proxy*; *Server-Telnet*; *Server-Web*; *WebToolbar* [19].

Из приведённого перечня 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 предназначенные для несанкционированного воздействия» 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. Например, виновный совершил несанкционированное уничтожение или копирование персональных данных при помощи программы категории *Riskware*, в частности, утилиты удалённого 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 «бэкдор» следует квалифицировать по совокупности преступлений, предусмотренных ст.272 и 273 УК РФ. В этом случае соответствующую троянскую программу целесообразно рассматривать в качестве орудия 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.

* * *

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.02.2015) // Собр. законодательства РФ. – 1996. – № 25. – Ст.2954.

2. Сводные статистические сведения о состоянии судимости в России за 2012 год. – URL: <http://www.cdep.ru/index.php?id=79&item=1776>; Сводные статистические сведения о состоянии судимости в России за 2013 год. – URL: <http://www.cdep.ru/index.php?id=79&item=2362>; Сводные статистические сведения о состоянии судимости в России за первое полугодие 2014 года. – URL: <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.

4. Воробьев В.В. О предмете преступления и его особенностях в компьютерных преступлениях // Общественная безопасность как научная категория: уголовно-правовой и криминологический аспекты: материалы науч.-практ. конф. (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.

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.

10. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001; вступило в силу для России 17.10.2008) // Собр. законодательства РФ. – 2009. – № 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 // СПС «Консультант-Плюс». – [Не опублик.].

12. Об утверждении Правил оказания телематических услуг связи: Постановление Правительства РФ от 10.09.2007 № 575 (ред. от 16.02.2008) // Собр. законодательства РФ. – 2007. – № 38. – Ст.4552.

12. Классификация вредоносных программ. – URL: <http://www.kaspersky.ru/internet-security-center/threats/malware-classifications>

14. Что такое компьютерный вирус и компьютерный червь? – URL: www.kaspersky.ru/internet-security-center/threats/viruses-worms

15. Что такое троянская программа? – URL: www.kaspersky.ru/internet-security-center/threats/trojans

16. Виды шпионского ПО. – URL: www.kaspersky.ru/internet-security-center/threats/adware-pornware-riskware

17. Что такое Adware? – URL: www.kaspersky.ru/internet-security-center/threats/adware

18. Что такое Pornware? – URL: www.kaspersky.ru/internet-security-center/threats/pornware

19. Что такое Riskware? – URL: www.kaspersky.ru/internet-security-center/threats/riskware