Е. А. Русскевич*

Понятие вредоносной компьютерной программы

Аннотация. *В работе предпринята попытка пересмотра традиционного определения вредоносности компьютерной программы на основе ее способности создавать такие последствия, как несанкционированное уничтожение, блокирование, модификация либо копирование охраняемой законом информации. Автор обращает внимание, что господствующее толкование вредоносности компьютерной программы не позволяет отнести к таковым программы-шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а собирание сведений об активности пользователя в сети Интернет, программы «злые шутки» (Bad Jokes), конструкторы вирусов, а также программы, объективно приспособленные к совершению преступлений, но выполненные на основе легального программного обеспечения. Обосновывается вывод о том, что в свете современных угроз стремительно «виртуализующегося» общества понятие вредоносной программы должно быть расширено посредством использования более общего критерия — предназначение программы для осуществления противоправной деятельности в целом.*

Ключевые слова: *компьютерные преступления; информационно-коммуникационные технологии, информационная безопасность, вредоносная программа, компьютерный вирус.*

DOI: 10.17803/1994-1471.2018.96.11.207-215

В наше время, пожалуй, трудно найти пользователя современных информационно-коммуникационных технологий, который хотя бы раз не испытал на себе негативное воздействие вредоносных компьютерных программ. Некоторые из них относительно безобидны, другие могут причинить непоправимый вред не только информационным активам, но и самому компьютерному оборудованию. В отношении наиболее опасных авторы предлагают и вовсе использовать термины «информационное оружие»[1] или «киберору-

[1] *Фатьянов А. А.* Правовое обеспечение безопасности информации в Российской Федерации : учеб. пособие. М., 2001. С. 40.

[2] См.: *Казарин О. В.*, *Шаряпов Р. А.* Вредоносные программы нового поколения — одна из существующих угроз международной информационной безопасности // Вестник РГГУ. Серия : Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2015. № 12 (155). С. 9—23 ; *Mele S.* Legal consideration on cyber-weapons and their definition // Journal of Law & Cyber Warfare. 2014. Vol. 3. Iss. 1. P. 53.

* *Русскевич Евгений Александрович,* кандидат юридических наук, старший преподаватель кафедры уголовного права Московского университета МВД России имени В. Я. Кикотя
russkevich@mail.ru
117437, Россия, г. Москва, ул. Академика Волгина, д. 12

жие»[2]. Недавние атаки на информационную инфраструктуру ряда государств, в том числе России, вирусов-шифровальщиков WannaCry и Petya, не позволяют признавать такие оценки надуманными либо преувеличенными. В общей сложности только от WannaCry пострадало более 500 тыс. компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям в более чем 150 странах мира[3].

Парадоксально, но, несмотря на значимость проблемы, в отечественной уголовно-правовой науке так и не сложилось единообразного понимания «вредоносной программы» как конструктивного признака ст. 273 УК РФ.

Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации определяет вредоносную программу как созданную или существующую программу со специально внесенными изменениями, заведомо приводящую к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети[4].

В этом же ключе содержание вредоносной программы раскрывается в п. 2.6.5 и 2.6.6 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденного приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст[5]. Согласно государственному стандарту, вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Несанкционированное воздействие на информацию — воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Подобный подход, определяющий вредоносность программы ее функциональным предназначением — оказывать неправомерное (несанкционированное) воздействие исключительно на компьютерные данные и системы, — является наиболее распространенным и в доктрине уголовного права. Так, М. М. Малыковцев пишет, что «вредоносная программа — это программа, специально написанная на любом языке программирования, использование и распространение которой в информационной системе либо в информационно-телекоммуникационной сети приводит к неправомерному воздействию на информацию и (или) на средства компьютерной техники и связи, выражающемуся в незаконном уничтожении, копировании, повреждении, блокировании, искажении информации, и (или) иному нарушению установленного законным владельцем порядка работы указанных устройств»[6]. Похожим образом определяет вредоносность компьютерной программы Е. А. Маслакова, отмечая, что ее сущностным свойством выступает способность вызывать несанкционированное собственником уничтожение, блокирование, модификацию либо копирование компьютерной информации[7].

В свою очередь, М. А. Ефремова подчеркивает, что основное отличие вредоносных программ от иных, которые также могут производить копирование, уничтожение, модификацию информации, определяется тем, что все действия производятся без уведомления пользователя, скрытно от него, а сам пользова-

[3] Владимир Путин назвал спецслужбы США источником вируса WannaCry // URL: http://www.kommersant.ru/doc/3297338 (дата обращения: 20 ноября 2017 г.).

[4] СЗ РФ. 2009. № 13. Ст. 1460.

[5] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М. : Стандартинформ, 2008.

[6] *Малыковцев М. М.* Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дис. … канд. юрид. наук. М., 2007. С. 10.

[7] *Маслакова Е. А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук. Орел, 2008. С. 68.

тель зачастую и не подозревает о наличии такой программы на его компьютере[8].

А. П. Кузнецов также обосновывает, что вредоносность или полезность соответствующих компьютерных программ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это может являться технической функцией лицензионных (разрешенных) компьютерных программ), а тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает компьютерную программу вредоносной[9].

В. М. Быков, В. Н. Черкасов резюмируют, что для того, чтобы программа считалась вредоносной, она должна соответствовать следующим трем критериям: 1) направленность на уничтожение информации; 2) несанкционированный характер работы; 3) целью создания программы является оказание неправомерного воздействия на информационные ресурсы[10].

Нельзя не отметить спорный характер первого критерия, который неоправданно ограничивает вредоносность программы ее нацеленностью именно на уничтожение компьютерных данных.

По мнению В. Б. Вехова, для того, чтобы признать компьютерную программу вредоносной, необходимо доказать наличие совокупности следующих обстоятельств: 1) программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации; 2) программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий; 3) программа не запрашивает согласия (санкции) у собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно- телекоммуникационной сети на реализацию своего назначения (алгоритма)[11].

В судебно-следственной практике, пожалуй, наибольшее распространение получило признание вредоносными компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов (KEYGEN.exe и др.). Так, Р. был осужден по ч. 2 ст. 146 и ч. 1 ст. 273 УК РФ. Согласно приговору суда, Р., находясь в помещении общества с ограниченной ответственностью, из корыстной заинтересованности выполнил несанкционированное копирование (установку) с неустановленного следствием носителя информации программного продукта AutoCAD-2014 на системный блок электронно-вычислительной машины, принадлежащей организации, и для достижения работоспособности указанного программного продукта незаконно использовал вредоносную компьютерную программу X-Force с неустановленного следствием носителя информации. Таким образом, Р. умышленно использовал вредоносную программу X-Force, чем заведомо исключил возможность штатной установки лицензионного ключа программы AutoCAD-2014 и тем самым заведомо несанкционированно модифицировал (изменил) продукцию AutoCAD-2014, обеспечив

---

[8] *Ефремова М. А.* Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий : монография. М., 2015. С. 101.

[9] См.: *Кузнецов А. П.* Полный курс уголовного права : в 5 т. / под ред. д. ю. н., проф., заслуж. деятеля науки РФ А. И. Коробеева. СПб., 2008. Т. 4 : Преступления против общественной безопасности. С. 657.

[10] *Быков В. М.*, *Черкасов В. Н.* Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы : монография. М., 2015. С. 126.

[11] *Вехов В. Б.* Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8). С. 45.

нейтрализацию средств защиты и нормальное функционирование работы программного продукта AutoCAD-2014, неправомерно копированного (установленного) им с неустановленного следствием носителя[12].

Сравнительно реже правоохранительные органы выявляют случаи использования «компьютерных вирусов», «троянов» и т.п. Так, например, М. был осужден по ч. 1 ст. 273 УК РФ. В соответствии с приговором суда, М., обладая специальными познаниями в области работы с компьютерными программами, действуя умышленно, находясь по месту жительства, приобрел путем копирования с неустановленных интернет-ресурсов компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации, после чего посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов (серверов для хранения информации в сети Интернет) использовал указанные вредоносные компьютерные программы для заражения 50 компьютеров неустановленных пользователей сети Интернет и построения из них контролируемой сети, в результате чего без ведома и согласия указанных пользователей скопировал хранящуюся в памяти зараженных устройств компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных интернет-ресурсах, которую планировал использовать в личных целях. Согласно заключению эксперта, на жестком диске персонального компьютера М. обнаружены комплексы вредоносного программного обеспечения, предназначенного для построения «ботнетов» («бот-сетей»), то есть сетей из зараженных соответствующим вирусом компьютеров, с возможностью удаленного копирования информации назначенным владельцем указанной сети без ведома пользователя и без получения его согласия на применение указанных программ. Работа обнаруженного на жестком диске вредоносного программного обеспечения построена на использовании вирусов типа «троян» («троянская программа»)[13].

Господствующее толкование вредоносности компьютерной программы, к сожалению, имеет свои изъяны. Например, оно не позволяет отнести к таковым программы-шпионы (Spyware), целью которых является не причинение вреда информационным активам или инфраструктуре, а собирание сведений об активности пользователя в сети Интернет (о посещаемых сайтах, совершаемых покупках и т.п.), программы «злые шутки» (Bad Jokes)[14], так называемые «вирусные конструкторы» — программы, предназначенные не для осуществления атак на компьютерные ресурсы, а для генерирования новых вирусов. При общепринятом подходе нельзя отнести к вредоносным также программы, объективно приспособленные к совершению преступлений, но выполненные на основе легального программного обеспечения.

В связи с этим обоснованно возникает вопрос, может ли вредоносность программы выражаться в ее направленности на совершение посягательств в отношении иных охраняемых уголовным законом объектов? В. С. Комиссаров дает утвердительный ответ на этот вопрос, поскольку считает, что вредоносность может быть обусловлена не только самим алгоритмом действия про-

[12] Приговор Александровского городского суда Владимирской области от 19 августа 2015 г. по делу № 1-82/2015.

[13] Приговор Андроповского районного суда Ставропольского края от 6 апреля 2017 г. по делу № 1-31/2017.

[14] Такие программы не причиняют компьютеру прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен, предупреждают пользователя об опасности, которой на самом деле не существует. К Bad Jokes относятся, например, программы, которые пугают пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят сообщения, характерные для вирусов, и т.д. — в зависимости от «чувства юмора» автора такой программы. К этому классу также относятся программы, предназначенные для мошенничества, например путем распространения архивов с оплатой за смс (см. URL: https://threats.kaspersky.com/ru/threat/Hoax.JS.BadJoke/ (дата обращения: 22 ноября 2017 г.)).

граммы, направленным на уничтожение, блокирование, модификацию или копирование информации, но и «специфическими свойствами, предназначенными для выполнения неправомерных или даже преступных действий (хищения денег с банковских счетов, укрытия средств от налогообложения, хулиганства и т.д.)»[15].

В. А. Голуб и М. В. Овчинникова также расширительно толкуют содержание вредоносной программы, определяя ее как программу или фрагмент кода, специально созданную для выполнения или способствующую выполнению несанкционированных действий в информационной системе или информационно-телекоммуникационной сети, в результате которых возможно причинение вреда пользователям этой системы (сети) или другим лицам[16].

Пункт 2 Правил оказания телематических услуг связи, утвержденных постановлением Правительства РФ от 10 сентября 2007 г. № 575[17], вредоносное программное обеспечение раскрывает как *целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя* (выделено мной. — *Е. Р.*), 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.

Если исходить из подобного, более широкого понимания вредоносности как предназначения программы к заведомо противоправной (преступной) деятельности в целом, то изготовление и распространение программ-шпионов, Bad Jokes и конструкторов вирусов может быть квалифицировано по ст. 273 УК РФ. На наш взгляд, современный процесс непрерывного роста использования информационно-коммуникационных технологий во всех сферах жизни общества («виртуализация» жизнедеятельности»[18]) убедительно свидетельствует в пользу именно этого подхода. С течением времени вредоносные программные продукты всё 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.

К. Н. Евдокимов делает вывод, что вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в ст. 273 УК РФ[19]. Полагаем, что автор необоснованно смешивает вредоносные программы и легальное программное обеспечение, которое достаточно часто используется при совершении посягательств на объекты уголовно-правовой охраны. Известно, что многие разрешенные к обороту программные продукты применяются злоумышленниками для совершения преступлений. Так, например, программы для записи дисков (InfraRecoder, BurnAware, Nero и др.) используются злоумышленниками для изготовления контрафактной продукции (неправомерного копирования информации), программное обеспечение для удаленного администрирования (RDP, VNC, DameWare, TeamViewer, Remote Office Manager, Hamachi, и т.д.) довольно часто применяется при совершении хищений, связанных с неправомерным вмешательством в системы дистанционного банковского обслуживания. Вместе с тем вредоносными их признавать нельзя, поскольку такие программы по факту остаются аутентич-

---

[15] Уголовное право : Особенная часть / под ред. А. И. Рарога. М., 2009. С. 532—533.

[16] *Голуб В. А.*, *Овчинникова М. В.* Проблема корректного определения термина «вредоносная программа» // Вестник Воронеж. гос. ун-та. Серия : Системный анализ и информационные технологии. 2008. № 1. С. 141.

[17] СЗ РФ. 2007. № 38. Ст. 4552.

[18] См.: *Гилинский Я. И.* Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права : материалы X Российского конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. д-р юрид. наук, проф. В. С. Комиссаров. М., 2016. С. 296.

[19] *Евдокимов К. Н.* Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : монография. Иркутск, 2013. С. 60.

ными, сохраняют стандартный набор настроек и возможностей, заложенный разработчиком.

Другое дело, когда центральную часть легальной программы (так называемый «движок») приспосабливают для совершения конкретных преступлений. Например, для незаконного пополнения баланса проездных билетов злоумышленник использует одну из многих компьютерных программ, предназначенных для записи информации с одного носителя на другой, но меняет ее интерфейс таким образом, чтобы можно было выбрать перевозчика, количество поездок, срок действия и т.п. В этом случае, на наш взгляд, можно говорить о наличии признаков изготовления вредоносной компьютерной программы, поскольку в окончательном виде полученное программное обеспечение обладает уже другими характеристиками, напрямую указывающими на ее предназначение для осуществления противоправной деятельности.

Следует упомянуть об общепринятом в доктрине уголовного права положении: вредоносность программного обеспечения — категория юридическая и находится в компетенции правоприменителя. Программно-техническая экспертиза должна решать свои задачи — раскрыть общий алгоритм и особенности действия программы, предоставить значимую для следствия информацию о ее работе и т.п. Так или иначе, выводы эксперта будут иметь лишь ориентирующий характер в разрешении вопроса о вредоносности программы. В свете современных угроз стремительно «виртуализующегося» общества полагаем, что единственно верным будет избрать в качестве основного критерия вредоносности программы ее изначальное и основное предназначение — осуществление противоправной деятельности. В какой сфере такая деятельность будет осуществляться, будет ли работа программы носить не санкционированный пользователем или разрешенный характер (как с конструктором вирусов), имеет второстепенное значение. Таким образом, под вредоносной следует понимать компьютерную программу, созданную (в том числе путем модификации легальной программы) для осуществления противоправной деятельности.

Подобное толкование, на наш взгляд, позволит предупредить в будущем возможные проблемы применения такого оперативно-розыскного мероприятия, как получение компьютерной информации (было внесено в Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» в июле 2016 г.[20]). А. Л. Осипенко совершенно справедливо отмечает, что законодатель вряд ли связывает проведение данного оперативно-розыскного мероприятия с простейшими формами обращения к компьютерным ресурсам, находящимся в открытом доступе. Такие действия, осуществляемые, как правило, гласно и не подразумевающие необходимости преодоления определенных препятствий, следует оформлять как наведение справок, сбор образцов для сравнительного исследования и т.д. Основу же получения компьютерной информации как оперативно-розыскного мероприятия составляют достаточно сложные в техническом плане и требующие специальной подготовки действия по добыванию хранящейся в компьютерных системах или передаваемой по техническим каналам связи информации о лицах и событиях, вызывающих оперативный интерес[21].

Представляется очевидным, что правоохранительными органами при получении компьютерной информации, как правило, будут использоваться «заблаговременно внедренные программные продукты»[22] — практика,

[20] Федеральный закон от 06.07.2016 № 374 ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС «КонсультантПлюс».

[21] *Осипенко А. Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 86.

[22] *Баженов С. В.* Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. 2017. № 2 (65). С. 32.

которая апробирована силовыми структурами многих зарубежных стран и уже получила освещение в печати[23]. Несмотря на то что такие программные продукты обладают функционалом к преодолению средств защиты информации и ее скрытой фиксации (не санкционированного пользователем копирования), их предназначение для правомерного использования при проведении оперативно-розыскных мероприятий не позволит признавать их вредоносными по смыслу ст. 273 УК РФ.

БИБЛИОГРАФИЯ

1. *Баженов С. В.* Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. — 2017. — № 2 (65). — С. 31—33.
2. *Быков В. М.*, *Черкасов В. Н.* Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы : монография. — М., 2015. —325 с.
3. *Вехов В. Б.* Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. — 2015. — № 2 (8). — С. 43—46.
4. *Гилинский Я. И.* Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права : материалы X Российского конгресса уголовного права, состоявшегося 26—27 мая 2016 г. / отв. ред. д-р юрид. наук, проф. В. С. Комиссаров. — М., 2016. — С. 294—298.
5. *Голуб В. А.*, *Овчинникова М. В.* Проблема корректного определения термина «вредоносная программа» // Вестник Воронежского государственного университета. Серия : Системный анализ и информационные технологии. — 2008. — № 1. — С. 138—141.
6. *Евдокимов К. Н.* Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : монография. — Иркутск, 2013. — 267 с.
7. *Ефремова М. А.* Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий : монография. — М., 2015. — 200 с.
8. *Казарин О. В.*, *Шаряпов Р. А.* Вредоносные программы нового поколения — одна из существующих угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. — 2015. — № 12 (155). — С. 9—23.
9. *Кузнецов А. П.* Полный курс уголовного права : в 5 т. / под ред. д. ю. н., проф., заслуж. деятеля науки РФ А. И. Коробеева. — СПб., 2008. — Т. 4 : Преступления против общественной безопасности. — 672 с.
10. *Малыковцев М. М.* Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дис. … канд. юрид. наук. — М., 2007. — 186 с.
11. *Маслакова Е. А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук. — Орел, 2008. — 198 с.
12. *Осипенко А. Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. — 2016. — № 3. — С. 83—90.
13. Уголовное право : Особенная часть / под ред. А. И. Рарога. — М., 2009. — 704 с.
14. *Фатьянов А. А.* Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие. — М., 2001. — 421 с.
15. *Kaspersky E.* What is wrong with «legal malware»? // Forbes. — 22 dec. —2014.
16. *Mele S.* Legal consideration on cyber-weapons and their definition // Journal of Law & Cyber Warfare. — 2014. — Vol. 3. — Iss. 1. — P. 53—69.

Материал поступил в редакцию 2 февраля 2018 г.

[23] *Kaspersky E.* What is wrong with «legal malware»? // Forbes. 22 dec. 2014.

MALICIOUS COMPUTER PROGRAM

RUSSKEVICH Evgeny Aleksandrovich, PhD in Law, Senior Lecturer of the Department of Criminal Law of the Kikot Moscow University of the Ministry of the Interior of Russia
russkevich@mail.ru
117437, Russia, Moscow, ul. Akademika Volgina, d. 12

Abstract. *This paper attempts to revise the traditional definition of the harmfulness of a computer program based on its ability to create such consequences as unauthorized destruction, blocking, modification or copying of information protected by law. The author points out that the prevailing interpretation of the harmfulness of a computer program does not make it possible to classify as spyware programs (Spyware), the purpose of which is not to harm information assets or infrastructure, but to gather information about the user's activity on the Internet, the program "Bad Jokes", virus constructors, as well as programs that are objectively adapted to commit crimes, but executed on the basis of legal software. The author justifies the conclusion that in the light of today's threats of a rapidly "virtualizing" society, the concept of a malicious program should be expanded by using a more general criterion — the purpose of the program for carrying out illegal activities in general.*

Keywords: *computer crimes, information and communication technology, information security, malware, computer virus.*

REFERENCES (TRANSLITERATION)

1. *Bazhenov S. V.* Operativno-rozysknoe meropriyatie «Poluchenie komp'yuternoy informatsii» // Nauchniy vestnik Omskoy akademii MVD Rossii. — 2017. — № 2 (65). — S. 31—33.
2. *Bykov V.* M., *Cherkasov V. N.* Prestupleniya v sfere komp'yuternoy informatsii: kriminologicheskie, ugolovno-pravovye i kriminalisticheskie problemy : monografiya. — M., 2015. —325 c.
3. *Vekhov V. B.* Vredonosnye komp'yuternye programmy kak predmet i sredstvo sovershenia prestupleniya // Rassledovanie prestupleniy: problemy i puti ikh resheniya. — 2015. — № 2 (8). — S. 43—46.
4. *Gilinskiy Ya. I.* Kriminologicheskie osnovy ugolovnogo prava v epokhu postmoderna // Kriminologicheskie osnovy ugolovnogo prava : materialy X Rossiyskogo kongressa ugolovnogo prava, sostoyavshegosya 26—27 maya 2016 g. / otv. red. d-r yurid. nauk, prof. V. S. Komissarov. — M., 2016. — S. 294—298.
5. *Golub V. A., Ovchinnikova M. V.* Problema korrektnogo opredeleniya termina «vredonosnaya programma» // Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya : Sistemniy analiz i informatsionnye tekhnologii. — 2008. — № 1. — S. 138—141.
6. *Evdokimov K. N.* Sozdanie, ispol'zovanie i rasprostranenie vredonosnykh komp'yuternykh programm: ugolovno-pravovye i kriminologicheskie aspekty : monografiya. — Irkutsk, 2013. — 267 c.
7. *Efremova M. A.* Ugolovnaya otvetstvennost' za prestupleniya, sovershaemye s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologiy : monografiya. — M., 2015. — 200 c.
8. *Kazarin O. V., Sharyapov R. A.* Vredonosnye programmy novogo pokoleniya — odna iz sushchestvuyushchikh ugroz mezhdunarodnoy informatsionnoy bezopasnosti // Vestnik RGGU. Seriya: Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaya bezopasnost'. — 2015. — № 12 (155). — S. 9—23.
9. *Kuznetsov A. P.* Polniy kurs ugolovnogo prava : v 5 t. / pod red. d. yu. n., prof., zasluzh.o deyatelya nauki RF A. I. Korobeeva. — SPb., 2008. — T. 4 : Prestupleniya protiv obshchestvennoy bezopasnosti. — 672 s.
10. *Malykovtsev M. M.* Ugolovnaya otvetstvennost' za sozdanie, ispol'zovanie i rasprostranenie vredonosnykh programm dlya EVM : dis. … kand. yurid. nauk. — M., 2007. — 186 s.

11. *Maslakova E. A.* Nezakonniy oborot vredonosnykh komp'yuternykh programm: ugolovno-pravovye i kriminologicheskie aspekty : dis. … kand. yurid. nauk. — Orel, 2008. — 198 s.
12. *Osipenko A. L.* Novoe operativno-rozysknoe meropriyatie «poluchenie komp'yuternoy informatsii»: soderzhanie i osnovy osushchestvleniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2016. — № 3. — S. 83—90.
13. Ugolovnoe pravo : Osobennaya chast' / pod red. A. I. Raroga. — M., 2009. — 704 s.
14. *Fat'yanov A. A.* Pravovoe obespechenie bezopasnosti informatsii v Rossiyskoy Federatsii : uchebnoe posobie. — M., 2001. — 421 c.