**Содержание**

[**Введение** 3](#_Toc260392114)

[**1.** **Правовые аспекты регулирования преступлений в сфере компьютерной информации** 6](#_Toc260392115)

[**1.1.** **Правовое регулирование понятия преступления в сфере компьютерной информации** 6](#_Toc260392116)

[**1.2.** **Общая характеристика преступлений в сфере компьютерной информации** 12](#_Toc260392117)

[**2. Правоприменительная практика в сфере компьютерной информации** 15](#_Toc260392118)

[**2.1. Неправомерный доступ к компьютерной информации** 15](#_Toc260392119)

[**2.2. Создание, использование и распространение вредоносных программ для ЭВМ** 19](#_Toc260392120)

[**2.3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети** 21](#_Toc260392121)

[**3. Проблемы и перспективы развития отношений в сфере компьютерной информации** 24](#_Toc260392122)

[**3.1. Неправомерный доступ к компьютерной информации** 24](#_Toc260392123)

[**3.2. Разработка и распространение компьютерных вирусов** 26](#_Toc260392124)

[**3.3. Виды компьютерных преступлений** 28](#_Toc260392125)

[**Заключение** 37](#_Toc260392126)

[**Глоссарий** 41](#_Toc260392127)

[**Библиографический список** 43](#_Toc260392128)

[**Приложение -1** 46](#_Toc260392133)

**Введение**

Современную жизнь уже просто не возможно представить без персонального компьютера. В каждом доме, офисе, предприятии обязательно присутствует компьютер. Информация различного характера, в том числе, финансовая и содержащая персональные данные храниться на специальных носителях. Все сферы жизни пронизаны и связаны между собою посредством компьютера. В данной ситуации и крупное предприятие и простой пользователь оказываются беззащитны перед угрозой исходящей от преступников, использующих новые технологии. Данная сфера преступлений еще достаточно «молода» в силу того, что компьютер только в последние десять-пятнадцать лет получил столь широкое распространение. Раз имеют место нарушение норм права в сфере компьютерной информации, следовательно, законодательство должно поспевать за развитием общественных отношений и регулировать и данную сферу преступлений.

Новый Уголовный кодекс Российской федерации, по существу, вводит понятие «компьютерной преступности».

Таким образом, одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных.

Другой – «реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности.

Ситуация, в которой пользователь становиться потерпевшим в результате преступления, потребовала принятия норм уголовного права, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации.

Это и нашло воплощение в новом Уголовном кодексе РФ. Глава 28 «Преступления в сфере компьютерной информации» содержит три статьи: «Неправомерный доступ к компьютерной информации» (ст.272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст.273), «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст.274)»[[1]](#footnote-1).

В данном контексте тема предложенного исследования представляется актуальной.

Цели и задачи исследования.

Целью курсовой работы является комплексное исследование преступлений в сфере компьютерной информации.

Поставленная цель предопределила решение следующих задач:

* проанализировать нормативно-правовые акты в сфере компьютерной информации;
* дать развернутый анализ состава преступления в сфере компьютерной информации;
* охарактеризовать виды преступления в сфере компьютерной информации;
* рассмотреть проблемы и перспективы развития отношений в сфере компьютерной информации.

Объект и предмет исследования.

Объектом курсового исследования являются преступления в сфере общественной безопасности и общественного порядка.

Предметом исследования являются преступления в сфере компьютерной информации.

В исследовании были использованы следующие общенаучные и частнонаучные методы.

* общелогические метод позволил провести анализ и синтез исследуемых явлений;
* сравнительный – в результате, которого происходило сравнение двух или более исследуемых явлений, «выявлялись общие или особенные черты, этапы и тенденции развития»[[2]](#footnote-2);
* исторический позволивший рассматривать процессы возникновения и развития социальных явлений;
* формально-юридический – позволяющий изучать правовое явление в «чистом» виде, вне связи с другими сферами общественной жизни.
1. **Правовые аспекты регулирования преступлений в сфере компьютерной информации**
	1. **Правовое регулирование понятия преступления в сфере компьютерной информации**

Глава 28 «Преступления в сфере компьютерной информации» УК РФ включена в отечественное уголовное законодательство впервые. «Страны, уже прошедшие период компьютерного переоснащения, накопили свой криминальный опыт. Например, бухгалтер одной из зарубежных пароходных компаний вычислил, что незначительное искажение отчетности не будет замечено ревизионной службой. Организовав 17 подставных фирм, он похитил значительные суммы без каких-либо видимых нарушений финансовой деятельности компании. Другой пример: преступник открывает не менее двух счетов в банках, перечисляя денежные суммы с процентами со счета на счет, в конечном итоге он исчезает с похищенной суммой.

Заполучила своих компьютерных взломщиков и Россия. Вспомним хотя бы нашумевшее дело Левина, проникшего в банковские счета зарубежных банков. Двадцатичетырехлетний математик с сообщниками проник в компьютерную систему Ситибанка, похищая денежные средства со счетов вкладчиков.

Не исключено, что в Российской Федерации компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний»[[3]](#footnote-3).

Таким образом, необходимость этого решения законодателя объясняется тем, что вслед за распространением в странах Запада посягательств на сохранность информации и ее компьютерных носителей эта тенденция проявилась и в России. «Указанные преступления нацелены на жизненно важные интересы личности, общества, государства, связанные с формированием и использованием автоматизированных информационных ресурсов, созданием, сбором, обработкой, накоплением, хранением, поиском, распространением информации; созданием и использованием информационных технологий и средств их обеспечения. Даже локальные посягательства на компьютерную информацию и ее носителей способны вызвать (с учетом места, которое занимает в социальной жизни эксплуатация компьютеров) хаос в финансово-банковских операциях, производстве, образовании, социальной помощи, обороне и т.д., огромные имущественные потери, нарушение конституционных прав»[[4]](#footnote-4).

Первоначально необходимо определить понятие компьютерной информации. Согласно международно-правовому определению к компьютерным преступлениям относятся любые деяния, незаконно затрагивающие автоматизированную обработку либо передачу данных.

Так компьютерной называется информация, содержащаяся:

«на машинном носителе. К последним относятся дискеты, лазерные диски и другие носители информации, которые позволяют воспроизводить, редактировать, обрабатывать, декомпилировать, распространять и т.д. имеющуюся на них информацию исключительно с помощью ЭВМ;

на жестком диске ЭВМ, например, в виде программ (т.е. объективной формы представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата), баз данных, их адаптации, модификации (ст. 1261-1262 ГК, а до 01.01.08 - ст. 1 Закона об ЭВМ);

в системе ЭВМ или их сети, способной обрабатывать эту информацию одновременно либо осуществлять с ней любые манипуляции (адаптация, модификация, воспроизведение, распространение и т.д.)»[[5]](#footnote-5);

По мнению Богомолова М.В. в работе «Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации», под информацией вообще понимается «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые и передаваемые человеком или специальными устройствами»[[6]](#footnote-6). Богомолов М.В. приводит точку зрения В.В. Крылова, который, считает, что «термин «информация» может интерпретироваться и как совокупность формализованных сведений (знаний), предназначенных для передачи в качестве сообщения. Понимая под «сообщением» активные волевые действия лица по передаче информации вовне, под «знанием» упорядоченное мысленное представление о конкретном объекте, факте (или их совокупности), о способах его (их) взаимодействия и взаимосвязи с другими объектами, фактами, поддающееся описанию, приему и передаче формальным (вербальным или символьным) образом, превращаясь в «сообщение». Но законодатель в Федеральном законе «Об информации, информатизации и защите информации», в котором регулируются отношения по формированию и использованию большей части информации, так определил данное понятие:

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»[[7]](#footnote-7).

Конституция РФ закрепляет право граждан на защиту информации в рамках 23 статьи, где говориться о неприкосновенности частной жизни, личную и семейную тайну, а также защиту своей чести и доброго имени. Дополнительно в ст.24 Конституции РФ устанавливается обязанность соблюдать «порядок сбора, хранения, использования и распространения информации о частной жизни лица. Эта обязанность возлагается не только на государственные органы власти и управления, предприятия и организации, но и на коммерческие и общественные организации и предприятия, а также граждан»[[8]](#footnote-8).

Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (определяет понятие информации как то, что: 1) «информация - сведения (сообщения, данные) независимо от формы их представления; 2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов; 3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; 4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники; 5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам; 6) доступ к информации - возможность получения информации и ее использования; 7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя; 8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц; 9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц; 10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети; 11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель»[[9]](#footnote-9).

В Указе Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера» установлен объем информации носящей конфиденциальный характер и требующей правовой защиты. К такой информации отнесены следующие сведения:

* Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;
* Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
* Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
* Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);
* Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Законность операций с информацией вообще и компьютерной в частности определяется:

а) инициативой или согласием собственника или иного частного владельца информации;

б) наличием законного допуска к осуществлению операций;

в) соблюдением правовых предписаний об операциях с конфиденциальной информацией различных видов;

г) соблюдением правовых требований эксплуатации компьютеров, их систем и сетей;

д) «вынужденной необходимостью в области борьбы с преступностью;

е) при защите здоровья граждан;

ж) в условиях объявления чрезвычайного и военного положения»[[10]](#footnote-10).

«Закон об информации имеет специальную главу о защите информации и прав субъектов, участвующих в работе с ней. Целями защиты провозглашаются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства, в том числе защита конституционных прав граждан, сохранение государственной, служебной, иной тайны, предусмотренной законом; обеспечение прав информационных процессов. Способы защиты информации и прав субъектов работы с нею различаются «с учетом специфики правонарушений и нанесенного ущерба». Этот критерий использован и при определении границ уголовно-правового регулирования борьбы с преступлениями в сфере компьютерной информации. А именно установление уголовной ответственности предполагает материальные составы, связанные с наличием существенного или тяжкого вреда.

Отсутствие этого признака деяния влечет невозможность признания его преступлением и необходимость использования механизма защиты информации и прав субъекта в работе с нею через арбитражный суд, суд общей юрисдикции в соответствии с гражданским законодательством или законодательством об административных правонарушениях.

Глава о преступлениях в сфере компьютерной информации входит в раздел «Преступления против общественной безопасности и общественного порядка» УК РФ. Тем самым определяется и родовой объект составов преступлений, включенных в рассматриваемую главу[[11]](#footnote-11).

Таким образом, компьютерная информация - вся информация, циркулирующая на компьютере или в сети компьютеров, как записанная на машинных носителях, так и загруженная в оперативную память компьютера как следствие нанесение ущерба, лицу незаконно используя информации или незаконный доступ к ней, является определяющим для регулирования борьбы преступлений в сфере компьютерной информации. Любое преступление имеет состав элементов позволяющих говорить о наличии самого преступления. В связи с этим необходимо дать общую характеристику преступлений в сфере компьютерной информации.

* 1. **Общая характеристика преступлений в сфере компьютерной информации**

Первоначально попробуем рассмотреть различные точки зрения на понятие «компьютерного преступления». Есть точка зрения, высказанная Богомоловым М.В. «в рамках которой к «компьютерным преступлениям» относятся все противоправные деяния, так или иначе связанные с компьютерной техникой»[[12]](#footnote-12).

Более узкой по объекту регулирования является точка зрения Вехова Б.В., представленная в работе Богомолова М.В. «Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации», который считает, что «что под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства»[[13]](#footnote-13).

Таким образом, видовым объектом являются общественные отношения, нарушающие формирование и использование автоматизированных информационных ресурсов и средств их обеспечения. «По самому своему характеру видовой объект является сложным. В него в свою очередь входят несколько объектов, охватывающих права и законные интересы:

а) владельцев (в том числе собственников) и пользователей информации, компьютеров, их систем и сетей, средств обеспечения;

б) физических и юридических лиц, сведения о которых имеются в автоматизированных информационных ресурсах (банках данных);

в) общества и государства, в том числе интересы национальной безопасности. В частности, применительно к гражданам объектом посягательства могут быть здоровье (например, при нарушении правил эксплуатации ЭВМ), имущественные права, право на личную тайну и тайну сообщений, честь и достоинства личности»[[14]](#footnote-14).

Конкретно эти преступления направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. «Выяснение данного обстоятельства важно для того, чтобы отграничить преступления, предусмотренные статьями 272 — 274 УК, от других преступлений, связанных с использованием ЭВМ, системы ЭВМ и их сети для совершения других преступлений. В тех случаях, когда компьютерная аппаратура является предметом преступлений против собственности, соответственно ее хищение, уничтожение или повреждение подлежат квалификации по ст. 158 — 168 УК. Информационная же структура (программы и информация) не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных признаков предмета преступлений против собственности, в частности не обладает физическим признаком.

Предметом компьютерной информации являются информационные ресурсы, которые рассматриваются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных. Эти ресурсы содержат сведения (сообщения, данные) независимо от формы их представления»[[15]](#footnote-15).

Основные составы, сформулированные в ст. 272-274 УК РФ, предполагают наличие умысла. Квалифицированные составы, связанные с созданием, использованием и распространением вредоносных программ или с нарушением правил эксплуатации ЭВМ (систем, сетей), предусматривают неосторожную форму вины в отношении тяжких последствий. Умысел же в отношении тяжких последствий влечет необходимость квалификации деяния по совокупности - по соответствующим статьям о компьютерных преступлениях, чтобы полно охарактеризовать способ совершения деяния и создать возможность для сложения наказания.

**2. Правоприменительная практика в сфере компьютерной информации**

**2.1. Неправомерный доступ к компьютерной информации**

Базовым понятием в «данной норме является термин «доступ». Он взят из профессиональной терминологии; с точки зрения смысловой характеристики точнее было бы говорить о «проникновении». Имеется в виду неправомерное проникновение (вторжение) в охраняемую законом информацию, находящуюся в памяти ЭВМ, в машинном носителе либо циркулирующую по коммуникационным каналам в системе или сети ЭВМ»[[16]](#footnote-16).

Объектом преступления являются отношения в сфере охраны компьютерной информации.

Объективную сторону преступления образует неправомерный доступ к охраняемой законом компьютерной информации, т. е. «информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать самовольное получение информации без разрешения ее собственника или владельца. В связи с тем, что речь идет об охраняемой законом информации, неправомерность доступа к ней потребителя характеризуется еще и нарушением установленного порядка доступа к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие ее собственника или владельца не исключает неправомерности доступа к ней. Собственником информационных ресурсов, информационных систем, технологии и средств их обеспечения является субъект, в полном объеме реализующий права владения, пользования распоряжения указанными объектами. Владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения является субъект, осуществляющий владение и пользование указанными объектами и реализующий права распоряжения в пределах, установленных законом. Пользователем (потребителем) информации является субъект, обращающийся к информации.

Информация (сведения различного характера) содержится в базе данных, которая является объективной формой представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Гибкие диски (дискеты), жесткие диски и компакт-диски позволяют переносить документы и программы с одного компьютера на другой, хранить информацию, не используемую постоянно на компьютере, делать архивные копии информации, содержащейся на жестком диске.

Доступ к информации на машинном носителе имеют законные пользователи, т. е. лица, имеющие разрешение пользоваться компьютерными системами., Такое разрешение может быть дано, например, администратором базы данных.

Неправомерным следует признать доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией. Способы такого доступа: использование чужого имени, модификация программного и информационного обеспечения, изменение физических адресов технических устройств в результате системной поломки компьютера, установка аппаратуры записи, подключаемой к каналам передачи данных, и т. п»[[17]](#footnote-17).

Обязательный элемент объективной стороны данного состава - последствия.

Уничтожение информации заключается в удалении файла (поименованной области на диске или другом машинном носителе) без технической возможности восстановления. «Формы уничтожения также могут быть разнообразными: от самых банальных (сжигание дискет, подача команды на «стирание» программы) до более изощренных (искажение компьютерной информации, уничтожение важнейших фрагментов компьютерной информации и т.д.). Главный признак уничтожения - информацию невозможно восстановить»[[18]](#footnote-18);

Модификация - внесение любых изменений, за исключением необходимых для функционирования программы или базы данных на конкретных технических средствах пользователя или под управлением его конкретных программ. Т.е. «внесением изменений, осуществляемых исключительно с целью обеспечить функционирование программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя»[[19]](#footnote-19).

Блокирование информации - это создание препятствий к свободному доступу; при этом информация не подвергается уничтожению. «В отличие от уничтожения при блокировании - информация сохраняется, однако доступ к ней стал для данного пользователя недоступным (например, применили систему паролей и ключей, перевели программу на другой, неизвестный пользователю язык программирования)»[[20]](#footnote-20);

Копирование информации - создание копий файлов и системных областей дисков.

Нарушение работы ЭВМ (систем ЭВМ, их сети) выражается в снижении работоспособности отдельных звеньев ЭВМ, отключении элементов компьютерной сети.

Преступление считается, окончено с момента осуществления неправомерного доступа к информации, повлекшего ее уничтожение, модификацию, блокирование, копирование либо нарушение работы ЭВМ (систем ЭВМ, их сети). «Состав преступления - материальный. Для квалификации деяния как оконченного необходимо, чтобы наступило хотя бы одно из последствий, упомянутых в исчерпывающем перечне, который дается в ч. 1 данной статьи: уничтожение, блокирование, модификация, копирование информации либо нарушение работы с ней»[[21]](#footnote-21).

«С субъективной стороны преступление характеризуется только умышленной формой, вины. При этом по отношению к действию умысел может быть только прямым, о чем свидетельствует и использование законодателем термина «неправомерный», а к факту наступления последствий - как прямым, так и косвенным.

Субъектом преступления, предусмотренного ч. 1 ст. 272 УК, могут быть лица, достигшие 16 лет, в том числе и законный пользователь, который не имеет разрешения для работы с информацией определенной категории.

Частью 2 ст. 272 УК предусмотрена уголовная ответственность за данное преступление, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Совершение преступления группой лиц по предварительному сговору будет иметь место, когда неправомерный доступ осуществили два лица, заранее договорившиеся о совместном его совершении.

Признак организованной группы вменяется при совершении преступления двумя или более лицами, вне зависимости от формы соучастия - простое (соисполнительство) или сложное (с функциональным распределением ролей); причем действия виновных квалифицируются без ссылки на ст. 33 УК»[[22]](#footnote-22) .

2.2. Создание, использование и распространение вредоносных программ для ЭВМ

 Под вредоносными программами понимаются те из них, которые специально созданы для нарушения нормального функционирования компьютерных систем и программ.

Объектом преступления являются отношения в сфере обеспечения компьютерной безопасности.

Объективная сторона преступления выражается в «создании программ для ЭВМ или внесении изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, использовании таких программ; распространении таких программ или машинных носителей с такими программами.

В данной статье речь идет о разработке, распространении компьютерных вирусов путем создание программ для ЭВМ или внесения изменений в существующие программы. Опасность компьютерного вируса состоит в том, что он может привести к полной дезорганизации системы компьютерной информации и при этом, по мнению специалистов в данной области, может бездействовать достаточно длительное время, затем неожиданно «проснуться» и привести к катастрофе. Вирус может оказаться причиной катастрофы в таких областях использования компьютерной информации, как оборона, космонавтика, государственная безопасность, борьба с преступностью и т. д. К тяжким последствиям, наступившим по неосторожности, могут быть отнесены, например, гибель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или отрасли промышленности, осложнение дипломатических отношений с другим государством, возникновение вооруженного конфликта»[[23]](#footnote-23).

Программа для ЭВМ – «это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата»[[24]](#footnote-24).

Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки и порождаемые ею аудиовизуальные отображения. «Под созданием и распространением вредоносных программ для ЭВМ следует понимать воздействие вирусов, т. е. программ, преднамеренно и без санкции соответствующих лиц изменяющих хранящиеся в компьютере данные или программы.

Под использованием программы понимается воспроизведение, распространение (предоставление экземпляров программы неопределенному кругу лиц) и иные действия по ее введению в оборот.

Распространением программы признается предоставление доступа к воспроизведенной в любой материальной форме программе, в том числе сетевым и иным способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.

Окончено это преступление с момента совершения действий, указанных в диспозиции статьи»[[25]](#footnote-25).

«Предметом преступления, как и применительно к ст. 272 УК РФ, является охраняемая законом компьютерная информация, находящаяся на машинном носителе, в ЭВМ, сети ЭВМ»[[26]](#footnote-26).

С субъективной стороны преступление может быть совершенно как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил виновный, а когда наступили последствия, к достижению которых он стремился, - и зависимости от наступивших последствий. Лицо сознает, что создает программу, зараженную «вирусом», либо внедряет «вирус» в чужую программу или распространяет и использует его, и желает совершить эти действия. В этом случае действия, предусмотренные ст. 273 УК, оказываются лишь способом достижения поставленной цели. Совершенное деяние подлежит квалификации по совокупности совершенных преступлений.

Субъект преступления - лицо, достигшее 16 лет. «Квалифицирующим обстоятельством данного преступления является наступление тяжких последствий (ч. 2 ст. 273 УК). При фиксации последствий в данном составе преступления законодатель использует оценочное понятие. Следовательно, их тяжесть должна определяться с учетом конкретных обстоятельств дела: имущественный ущерб, сопряженный с восстановлением информации; упущенная выгода при срыве заключения крупного контракта или соглашения; дезорганизация работы предприятий или учреждений и т. п. Форма вины по отношению к тяжким последствиям может быть только неосторожной»[[27]](#footnote-27).

2.3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Объектом преступления являются отношения в сфере обеспечения безопасности.

Объективную сторону преступления образует нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это причинило существенный вред.

К такого вида нарушениям можно отнести несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации ЭВМ. Выделяют два основных средства защиты: копирование информации и ограничение доступа к информации. Нарушение режима эксплуатации ЭВМ образуют, например, несанкционированные изменение, уничтожение или передача информации. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями. «Эти правила обычно излагаются в инструкциях заводов-изготовителей, в различных руководствах по эксплуатации ЭВМ. Кроме того, в организациях локальными нормативными актами (такими, как Правила внутреннего трудового распорядка, Правила пожарной безопасности, Правила техники безопасности при обращении с ЭВМ) также устанавливаются общеобязательные для работников данной организации (а в соответствующих случаях - и для работников данного индивидуального предпринимателя) требования, которые они должны соблюдать при работе с ЭВМ»[[28]](#footnote-28).

Под охраняемой законом информацией следует понимать информацию, «изъятую из публичного оборота на основании закона, других нормативных актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования. Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать ограничительные грифы в целях сохранения коммерческой или банковской тайны.

Под существенным вредом (оценочное понятие) следует пони- мать причинение как материального, так и нематериального вреда.

Обязательным признаком объективной стороны преступления является наличие прямой (непосредственнной) причинной связи между уничтожением, модификацией или блокированием охраняемой законом информации и наступлением последствий в виде причинения существенного вреда»[[29]](#footnote-29).

С субъективной стороны преступление может быть совершено как умышленно так и по неосторожности в виде как небрежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации ЭВМ, системы ЭВМ и сети деяние, предусмотренное ст. 274 УК, становится лишь способом совершения преступления. Преступление в этом случае подлежит квалификации по наступившим последствиям, которые предвидел виновный, по совокупности с преступлением, предусмотренным данной статьей УК.

Субъект преступления специальный — лицо, имеющее законный доступ к эксплуатации упомянутых технических средств, достигший 16 лет. Это могут быть программисты, операторы ЭВМ, техники-наладчики и другие лица, имеющие к ним доступ по работе. О тяжких последствиях, наступивших по неосторожности, сказано выше в ст. 273

Квалифицирующим признаком ч. 2 ст. 274 УК является наступление тяжких последствий, а субъективная сторона характеризуется неосторожной формой вины по отношению к этим последствиям.

**3. Проблемы и перспективы развития отношений в сфере компьютерной информации**

**3.1. Неправомерный доступ к компьютерной информации**

Неправомерный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры «электронные корсары», «компьютерные пираты» - так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети. Внедрение в чужой компьютер происходит различными способами. Так применятся системы подбора паролей пользователей. «Стоит обратить внимание, что существует множество программ- «взломщиков», называемых на профессиональном языке HACK TOOLS (инструмент взлома). Но эти программы становятся малоэффективными в компьютерных системах, обладающих программой - «сторожем» компьютерных портов. Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора», основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности.

В этом случае программе – «взломщику» передаются некоторые исходные данные о личности автора пароля. Как показывают многочисленные эксперименты, вручную с использованием метода «интеллектуального перебора» вскрывается 42% от общего числа паролей. Интересны результаты экспериментов которые показали, что использование в качестве пароля имени, фамилии и производных позволят взломать около 54,5% паролей (приложение 1)»[[30]](#footnote-30).

Несанкционированный противоправный «доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, преступник может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, подобно покупателю, изучающему товары на витрине.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей компьютерной логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению возможности совершения противоправного деяния. Обычно они всетаки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что правонарушитель проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого способа преступления. Самый простейший путь его осуществления - это получить коды и другие идентифицирующие шифры законных пользователей. Это возможно:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;

-незаконным, несанкционированным подслушиванием через телефонные линии»[[31]](#footnote-31).

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом незаконно получить некоторую ценную информацию, в частности коды.

**3.2. Разработка и распространение компьютерных вирусов**

Трудно найти хоть одного человека, который пользуются компьютером, что бы он не сталкивался с вирусами. Автор исследования, не являясь заядлым пользователем, и то частенько попадает под вирусные атаки различного характера. «На сегодняшний день по оценкам западных специалистов дополнительно к тысячам уже известных вирусов появляется 100-150 новых видов ежемесячно.

Опасность компьютерного вируса состоит в том, что он может привести к полной дезорганизации работы компьютера и программного обеспечения и при этом, по мнению специалистов в данной области, может бездействовать достаточно длительное время, затем неожиданно активизироваться и привести к катастрофе. Вирус может оказаться причиной неустранимых нарушений в работе программного обеспечения и компьютерных сетей в таких важных национальных областях использования компьютерной информации, как оборона, космонавтика, государственная безопасность, банковская система, организованная борьба с преступностью. Именно высокой степенью общественной опасности объясняется, что УК РФ преследует достаточно строго за сам факт создания, распространения и использования вредоносных компьютерных программ для ЭВМ, не оговаривая наступления каких-либо тяжких последствий. При этом преступление считается оконченным, когда вредоносная программа создана или были внесены изменения. Под использованием (распространением) вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в компьютер, систему, сеть компьютеров, а также продажа, обмен, дарение, безвозмездная передача. Можно предположить, что под распространением следует понимать и их копирование. Яркий пример этому - произведение американского писателя Дэвида Бишофа под названием «Военные игры», написанного на основе реально происходивших событий. Чрезвычайно одаренный подросток взломал компьютерную сеть Пентагона и едва не развязал Третью мировую войну. Вирусы, действующие по принципу: «сотри все данные этой программы, перейди в следующую и сделай то же самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как самое настоящее вирусное заболевание. Причем выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с вредоносной программой типа «логической бомбы» или «временной бомбы». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека. Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь персонального компьютера ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер «заболевает»[[32]](#footnote-32).

Варианты вирусов зависят от противоправных целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея. Признаки могут быть эволютивными, и «болезнь» будет обостряться по мере своего течения. Так по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения. Американскими экспертами собрано досье писем от шантажистов требующих перечисления крупных сумм денег в одно из отделений американской фирмы «ПК Сиборг»; в случае отказа преступники грозятся вывести компьютеры из строя. По данным журнала «Business world», дискеты-вирусоносители получены десятью тысячами организаций, использующих в своей работе компьютеры. Для поиска и выявления компьютерных преступлений созданы специальные отряды американских детективов.

По-видимому, в будущем следует ожидать появление принципиально новых видов вирусов. Например, можно себе представить вредоносной программы вирусного типа в логических электронных схемах компьютера. В самом деле, пока речь идет только о заражении компьютеров. А почему бы - не микросхем? Ведь они становятся все более мощными и превращаются в некое подобие мини-ЭВМ. И их также необходимо программировать. Конечно, ничто не может непосредственно «заразить» микросхему. Но ведь можно заразить компьютер, используемый как программатор для тысячи микросхем.

**3.3. Виды компьютерных преступлений**

Все способы совершения компьютерных преступлений классифицируются в 5 основных групп. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, которые направлены на получение доступа к средствам компьютерной техники с различными намерениями. Руководствуясь этим признаком, Ю.М. Батурин в статье «Криминалистическая характеристика компьютерных преступлений» предлагает подход, согласно которому выделяет следующие общие группы:

1) изъятие средств компьютерной техники (СКТ);

2) перехват информации;

3) несанкционированный доступ к СКТ;

4) манипуляция данными и управляющими командами;

5) комплексные методы[[33]](#footnote-33).

Рассмотрим наиболее распространенные преступления в сфере компьютерной информации.

К первой группе относятся традиционные способы совершения обычных видов («некомпьютерных») преступлений, в которых действия преступника направлены на изъятие чужого имущества.

С уголовно-правовой точки зрения подобные преступления будут квалифицироваться соответствующими статьями Уголовного законодательства, например, шпионаж, хищение, разбой, вымогательство и т.п. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления будут использоваться иные инструменты, технические устройства и приспособления (или без их использования), не являющиеся средствами компьютерной техники.

«Например, по материалам уголовного дела, расследованного следственным отделом ГУВД г. В. Волгоградской области, возбужденного по факту кражи чужого имущества, было установлено, что 3 мая 1994 года в 3:00 неизвестные лица, перепилив с помощью ножовки по металлу прутья оконных металлических решеток, проникли в необорудованный охранной сигнализацией операционный зал государственного сбербанка, откуда похитили 2 системных блока персональных компьютеров стандартной модификации типа IBM PC/AT - 386 и PC/AT - 286, содержащих в своей постоянной памяти банк данных на всех вкладчиков сбербанка, физических и юридических лиц, кредиторов с полными установочными данными, зафиксированными электромагнитным способом на жестком магнитном диске (винчестере)»[[34]](#footnote-34). Как видно из приведенного примера, способ совершения компьютерного преступления достаточно прост и традиционен. Именно подобные ему способы совершения компьютерных преступлений и относятся к рассматриваемой группе.

Данные способы совершения преступлений в большей степени поддаются общим методам расследования, наибольший интерес представляют преступления, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов.

Назовем некоторые из таких способов:

1. Непосредственный (активный) перехват. Осуществляется с помощью непосредственного подключения и телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера.

2. Электромагнитный (пассивный) перехват. Не всегда перехватывающие устройства требуют непосредственного подключения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них.

Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излучение, возникающее при функционировании многих средств компьютерной техники, включая и средства коммуникации. Ведь работа всех без исключения электронных устройств сопровождается электромагнитным излучением, в результате чего в различных электронных приемных устройствах возникают нежелательные помехи.

Например, для осуществления преступных целей иногда достаточно смонтировать приемную антенну по типу волнового канала и имеющую более острую, несимметричную диаграмму направленности. После чего разработать (или использовать готовую) программу расшифровки «снятых» данных.

3. Аудиоперехват или снятие информации по виброакустическому каналу. Данный способ является наиболее опасным и достаточно распространенным. Защита от утечки по этому каналу очень сложна.

4. Видеоперехват. Данный способ совершения преступления заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники.

5. «Уборка мусора». Этот способ совершения преступления заключается в неправомочном использовании преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой.

Он осуществляется в двух формах: физической и электронной.

В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, емкостей для технологических отходов и сбору оставленных или выброшенных физических носителей информации.

Электронный вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования СКТ. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы.

К еще одной группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие:

1. «За дураком». Типичный прием физического проникновения хорошо известен специалистам, занимающимся вопросами совершенствования оперативно-розыскной деятельности. Он заключается в следующем: держа в руках предметы, связанные с работой на компьютерной технике (элементы маскировки), нужно ожидать кого-либо, имеющего санкционированный доступ, возле запертой двери, за которой находится предмет посягательства. Когда появляется законный пользователь, остается только войти внутрь вместе с ним или попросить его помочь донести якобы необходимые для работы на компьютере предметы. Этот вариант способа рассчитан на низкую бдительность сотрудников организации и лиц, ее охраняющих. При этом преступником может быть использован прием легендирования.

2. «За хвост». Этот способ съема информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе.

3. «Компьютерный абордаж». Данный способ совершения компьютерного преступления осуществляется преступником путем случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата.

4. «Неспешный выбор». Преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.

Обычно такой способ используется преступником в отношении тех, кто не уделяют должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы.

5. «Брешь». В отличие от «неспешного выбора» при данном способе преступником осуществляется конкурентизация слабых мест в защите компьютерной системы: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены.

6. «Маскарад». Преступник проникает в компьютерную систему, выдавал себя за законного пользователя. Системы защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации (по отпечаткам пальцев, рисунку сетчатки глаза, голосу и т.п.), оказываются незащищенными от этого способа. Самый простейший путь к проникновению в такие системы - получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путем подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу[[35]](#footnote-35).

Ряд программ заслуживает особого внимания, так как, к сожалению, с ними сталкивается и обычный пользователь. Как таковой реальной защиты от подобных преступлений трудно представить. В России еще не сформировался уровень правовой культуры, позволяющий любому пострадавшему от подобного преступления обратиться за помощью и привлечь преступника к ответственности.

Самой распространенной на сегодняшний день, по мнению автора, вредоносной программой является «Троянский конь". Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем принимающей «троянского коня» программы, с одновременным сохранением прежней ее работоспособности.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом перерасчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты.

«Дропперы» могут содержать в себе уже известную вредоносную программу или наоборот - устанавливать новую ее версию. Также «дропперы» могут устанавливать не одну, а сразу несколько вредоносных программ, принципиально отличающихся по поведению и даже написанных разными людьми.

Фактически «дропперы» являются своеобразными архивами, внутрь которых может быть помещено все что угодно. Очень часто они применяются для установки в систему уже известных «троянцев», поскольку написать «дроппер» гораздо проще, чем переписывать «троянца», пытаясь сделать его недетектируемым для антивируса. Весьма значительную часть «дропперов» составляют их реализации на скрипт-языках VBS и JS, что объясняется сравнительной простотой программирования на них и универсальностью подобных программ.

Даунлоадеры, или загрузчики, активно используются вирусописателями как по причинам, описанным выше для «дропперов» (скрытая установка уже известных троянцев), так и по причине их меньшего по сравнению с «дропперами» размера, а также благодаря возможности обновлять устанавливаемые троянские программы. Оба эти класса вредоносных программ используются для установки на компьютеры не только троянских программ, но и различных рекламных (adware) или порнографических (pornware) программ»[[36]](#footnote-36).

Интересен способ «Салями». Такой способ совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях. Данный способ основан на методике проведения операций перебрасывания на подставной счет мелочи - результата округления, которая на профессиональном бухгалтерском языке называется «салями».

С точки зрения преступников, это один из простейших способов совершения преступления. Он используется, как правило, при хищении денежных средств в тех бухгалтерских операциях, в которых отчисляются дробные (меньше, чем одна минимальная денежная единица) сумма денег с каждой операции, т.к. в этих случаях всегда делается округление сумм до установленных целых значений. Ставка преступников делается на том, что при каждой проверке потерпевший теряет так мало, что это практически не фиксируется документально[[37]](#footnote-37).

Bad-Joke, Hoax - злые шутки, введение пользователя в заблуждение

К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. - в зависимости от чувства юмора автора такой программы.

Социальный инжиниринг не относится к вредоносным программам или вирусам. Он призвана запутать пользователей, усыпить их бдительность, замаскировать вредоносную программу под какой либо патч или полезную программу, заманить пользователя на заведомо зараженный сайт.

В первую очередь на уловки соц. Инжиниринга попадаются не опытные пользователи всемирной паутины, но в последнее время вирусописатели идут на всевозможные хитрости, что даже опытные пользователи не всегда способны распознать уловку от правды.

Примерами данной технологии являются: всевозможные письма с текстом открыть прикрепленный к письму файл или зайти на сайт по указанной ссылке, для скачивания обновлений, патчей, просьбы якобы от службы технической поддержки или администраторов почтового сервера отослать свой пароль к вашему электронному ящику и пр..

Так, например червь Swen, выдавал себя за специальный патч от компании Microsoft, якобы устраняющий все известные уязвимости. Письмо, содержало легко узнаваемые элементы официального сайта Microsoft, ссылки на другие ресурсы данной компании и грамотно составленный текст.

Социальный инжиниринг активно используется не только в вирусах, но и самими хакерами для получения конфиденциальной информации от пользователей.

К программам класса Pornware, по мнению экспертов Лаборатории Касперского, относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера.

На данный момент в классе выделяется три поведения: Porn-Dialer, Porn-Downloader и Porn-Tool. Дайлеры дозваниваются до порнографических телефонных служб, а даунлоадеры скачивают на пользовательский компьютер порнографические материалы. К последнему поведению класса Pornware относятся всевозможные утилиты, так или иначе связанные с поиском и показом порнографических материалов (например, специальные панели инструментов для интернет-браузера и особые видеоплееры).

Программы класса Pornware могут быть установлены пользователем на свой компьютер сознательно, с целью поиска и получения порнографической информации. В этом случае они не являются вредоносными»[[38]](#footnote-38).

**Заключение**

В настоящее время в отечественной криминалистической науке не существует сколько-нибудь обобщенных данных для формирования понятий основных элементов криминалистической характеристики компьютерных преступлений.

«Как показывают проведенные исследования, 55% опрошенных респондентов не имеют об этих категориях ни малейшего понятия, а 39% - лишь частично знакомы с криминалистической характеристикой лиц, склонных к совершению компьютерных преступлений по ненаучным источникам, из которых 66% - средства массовой информации, 28% кино- и видеофильмы (как правило, зарубежного производства).

И при этом в качестве респондентов выступали в основном начальники городских и районных отделов и управлений органов внутренних дел и их заместители (начальники следственных отделов), которые в первую очередь должны обладать именно научной информацией о том, с чем им приходится сталкиваться в своей непосредственной практической работе. Такое положение, естественно, нельзя признать положительным. Поэтому весьма актуальной как с научной, так и с практической точки зрения, является разработка проблемы криминалистической характеристики данных видов преступных деликтов.

Как известно, криминалистическая характеристика преступления представляет собой систему описания криминалистически значимых признаков вида, группы и отдельного преступления, проявляющихся в особенностях способа, механизма и обстановки его совершения, дающую представление о преступлении, личности его субъекта и иных его обстоятельствах, об определенной преступной деятельности и имеющую своим назначением обеспечение успешного решения задач раскрытия, расследования и предупреждения преступлений.

Преступления в сфере компьютерной информации известны сравнительно недавно. Отечественная практика расследования таких преступлений пока весьма невелика, поскольку лишь в последние годы в результате развития программно-технических средств и повышения так называемой “компьютерной граммотности”, информационные системы внедрены в такие отрасли, как бухгалтерский учет, экономические расчеты, планирование и др»[[39]](#footnote-39).

Общественная опасность преступных действий в указанной сфере становится все более очевидна и опыт формализации законодателем главным образом зарубежных криминалистических знаний о “компьютерных преступлениях” происходит на наших глазах.

Недостатки правовой регламентации в данной области и дефицит у следователей знаний о современных информационных технологиях в значительной мере способствуют сохранению высокого уровня латентности противоправных действий в области информационных отношений и их безнаказанности.

За первое полугодие 2008 года аналитики «Лаборатории Касперского» обнаружили 367 772 новые вредоносные программы - в 2,9 раз больше, чем во втором полугодии 2007 года. Среднее число новых вредоносных программ, обнаруживаемых за месяц, составило 61 295,33. По сравнению со второй половиной 2007 года число новых программ увеличилось на 188,85%. Такие темпы роста значительно превосходят итоги 2007 года, когда было обнаружено на 114% вредоносных программ больше, чем в 2006 году.

2008 год не внес значительных изменений в соотношение классов вредоносных программ. Абсолютным лидером по-прежнему являются троянские программы, на которые приходится более 92% всех вредоносных программ. При этом доля троянов выросла лишь на 0,43% - это значительно меньше, чем их рост на два с лишним процента в 2007 году. Число новых троянских программ, обнаруженных в первом полугодии 2008 года, увеличилось на 190,2% по сравнению с предыдущим полугодием[[40]](#footnote-40).

Данная динамика прекрасно показывает, что преступления, направленные на сферу компьютерной информации, будут только увеличиваться в доле других преступлений. Если на сегодняшний момент статьи, посвященные данной группе преступлений, являются новым явлением для уголовной практики. Можно предположить, что данные преступления будут наращиваться вместе с ростом высоких технологий и развитием инновационных технологий. Президент России Д.А. Медведев заявил, что развитие России без развития инновационных технологий невозможно, но в тоже время следует добавить, по мнению автора, что это развитие должно сопровождаться адекватным реагированием специалистов на угрозы исходящие от компьютерных преступников.

Реально применять нормы Уголовного кодекса в сфере компьютерной информации, на сегодняшний день, могут себе позволить только серьезные компании и специальные службы. Простой пользователь остается незащищенным в данной сфере и зачастую оказывается объектом мошенничества и вымогательства денежных средств.

Как следствие, необходимо развивать законодательство преступлений в сфере компьютерной информации, стремиться к тому, что нормы права реально выполняли свою функцию защиты и восстановления нарушенных прав.

В условиях современного мира, где жизнь любого человека сопряжена с использованием технических средств очень важно стремиться к соблюдению ключевых прав и свобод человека – его правом на тайну информации.

По мнению С.А. Середы, «сложившаяся сегодня практика привлечения к уголовной ответственности по ст. 272 и 273 УК РФ за деяния, заключающиеся в нарушении авторских прав на программы для ЭВМ, не соответствует закону. Эти статьи ошибочно применяются к правоотношениям, не входящим в сферу действия гл. 28 УК РФ. Люди, осужденные по этим статьям, фактически, невиновны в неправомерном доступе к компьютерной информации или использовании вредоносных программ для ЭВМ. Следовательно, можно даже поднимать вопрос о фактах привлечения к уголовной ответственности заведомо невиновных лиц.

Для исправления сложившейся ситуации можно предложить следующее:

инициировать рассмотрение одного из судебных дел с вменением состава преступления по ст. 272 и (или) 273 УК РФ нарушителям авторских прав Верховным Судом РФ с целью получения соответствующего постановления;

инициировать публикацию Верховным Судом России разъяснений терминов, используемых в ст. 272 и 273 УК РФ;

проводить разъяснительную работу (например, посредством публикации соответствующих материалов) среди представителей правоохранительных органов, а также потенциальных нарушителей авторских прав (системных администраторов, программистов, «настройщиков» вычислительной техники и программного обеспечения);

разработать и ввести в действие новую редакцию гл. 28 УК РФ, соответствующую текущей практике информационной безопасности и современному уровню техники (например, на базе уголовного законодательства зарубежных стран)»[[41]](#footnote-41).

**Глоссарий**

|  |  |  |
| --- | --- | --- |
| **№** | **Понятие** | **Значение** |
|  | Блокирование информации  | это создание препятствий к свободному доступу информации |
|  | Вредоносная программа | (буквальный перевод англоязычного термина Malware, mal icious -вредоносный |
|  | Запоминающее устройство  | носитель информации , предназначенный для записи и хранения информации |
|  | Информация | от лат. informatio — осведомление, разъяснение, изложение, от лат. informare — придавать форму) — в широком смысле абстрактное понятие, имеющее множество значений, в зависимости от контекста. В узком смысле этого слова — сведения (сообщения) независимо от формы их представления |
|  | Компьютерный вирус  | разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. |
|  | Компьютерное преступление | любое деяние, незаконно затрагивающие автоматизированную обработку либо передачу данных. |
|  | Пользователь  | лицо или организация, которое использует действующую систему для выполнения конкретной функции |
|  | Троянская программа | (также - троян, троянец, троянский конь, трой) -вредоносная программа , проникающая на компьютер под видом безвредной |
|  | Уголовное преступление | это правонарушение , совершение которого влечёт применение к лицу мер уголовной ответственности. |
|  | Уничтожение компьютерной информации | невозможность ее восстановления вследствие неправомерных действий; |

**Библиографический список**

**Нормативно-правовые акты**

1. Конституция Российской Федерации СПС «Консультант +» Выпуск №13
2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996) (ред. от 07.04.2010) (с изм. и доп., вступающими в силу с 18.04.2010)
3. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД ФС РФ 08.07.2006)
4. Федеральный закон от 20.08.2004 N 119-ФЗ (ред. от 05.04.2010) "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" (принят ГД ФС РФ 31.07.2004)
5. Указ Президента РФ от 06.03.1997 №188 (в ред. 23.09.2005) «Об утверждении перечня сведений конфиденциального характера»

**Учебная литература**

Бархатова Е.Ю. Комментарий к Конституции Российской Федерации. –М.: Изд-во Проспект, 2005 256-с.

Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru

1. Ветров Н.И. Уголовное право. Особенная часть: Учебник для вузов.-М.: Юнита-Дана

# Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.

Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция 1997 №10 СПС «Гарант»

# Дащян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет СПС Гарант

# Комментарий к Уголовному кодексу Российской Федерации (под ред. В.Т. Томина, В.В. Сверчкова). - 6-е изд., перераб. и доп. - "Юрайт-Издат", 2010 г.

# Комментарий к Закону РФ от 23 сентября 1992 г. N 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных»

Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru

1. С.А. Середа Ответственность за распространение вредоносных программ //Право и экономика 2007 №3
2. С.А. Середа Расширенное толкование терминов «вредоносная программа» и «неправомерный доступ» // Закон 2007 №7
3. Теория государства и права: Учебное пособие. Конспект лекций в схемах и определениях / Под ред. доцента Л.В. Смирновой. М.: Книжный мир, 2004.
4. Уголовное право. Общая и Особенная части: Учебник для вузов / Под общей ред. д.ю.н. М.П. Журавлева и к.ю.н. С.И. Никулина – М.: Норма, 2007 – 816 с.
5. Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. проф. Б.В. Здравомыслова. - М.: Юрист. 2000 – 552с
6. Уголовное право. Особенная часть: Учебник / Под общ. ред. проф. Л.Д. Гаухмана и С.В. Максимова. – М.: Форум: ИНФРА-М, 2003. – 400с

Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г

**Интернет - источники**

1. <http://www.itpedia.ru>
2. http://partnerstvo.ru
3. <http://www.whatis.ru>
4. http://copyright.samara.ru
5. http://www.best-lawyers.ru/
6. <http://www.allpravo.ru>
7. <http://www.itpedia.ru>
8. http://www.sir35.ru

**Приложение - 1**

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И ИНТЕРНЕТ

Мосин О.В.

ГЛАВА 2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Уголовный Кодекс Российской Федерации установил нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие уголовную ответственность за их совершение. Такие нормы появились в российском законодательстве впервые. К уголовно-наказуемым отнесены 1) неправомерный доступ к компьютерной информации (ст. 272 УК РФ), 2) создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) и 3) нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ).

Видовым объектом преступлений в сфере компьютерной информации являются информационные отношения, т. е. отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации. Из этого определения следует, что и информационные отношения стали новым объектом преступления. Конкретно эти преступления направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. Выяснение данного обстоятельства важно для того, чтобы отграничить преступления, предусмотренные статьями 272 — 274 УК, от других преступлений, связанных с использованием ЭВМ, системы ЭВМ и их сети для совершения других преступлений. В тех случаях, когда компьютерная аппаратура является предметом преступлений против собственности, соответственно ее хищение, уничтожение или повреждение подлежат квалификации по ст. 158 — 168 УК. Информационная же структура (программы и информация) не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных при- знаков предмета преступлений против собственности, в частности не обладает физическим признаком.

Предметом компьютерной информации являются информационные ресурсы, которые в ст. 2 Федерального закона от 20 февраля 1995 г. «Об информации, информатизации и защите информации» рассматриваются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных. Эти ресурсы согласно ст. 2 Закона содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления.

**Приложение - 2**

Способ компьютерных преступлений: метод "интеллектуального перебора", основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности.

Вот результаты экспериментов:

|  |  |  |
| --- | --- | --- |
| Тематические группы паролей | % частоты выбора пароля человеком | % вскрываемости |
| Имена, фамилии и производные | 22,2 | 54,5 |
| Интересы (хобби, спорт, музыка) | 9,5 | 29,2 |
| Даты рождения, знаки зодиака свои и близких; их комбинации | 11,8 | 54,5 |
| Адрес жительства; место рождения | 4,7 | 55 |
| Номера телефонов | 3,5 | 66,6 |
| Последовательность клавиш ПК, повтор символа | 14,1 | 72,3 |
| Номер документов (паспорт, удостоверение) и т.д. | 3,5 | 100,0 |
| Прочие | 30,7 | 5,7 |

**Приложение - 3**

**Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.**

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

 1. Объектом преступления, упомянутого в ст. 274 УК, являются правила эксплуатации ЭВМ (их систем или сетей ЭВМ, см. комментарий к ст. 272 УК).

 2. Объективная сторона анализируемого деяния состоит:

 а) в нарушении правил эксплуатации ЭВМ. Эти правила обычно излагаются в инструкциях заводов-изготовителей, в различных руководствах по эксплуатации ЭВМ. Кроме того, в организациях локальными нормативными актами (такими, как Правила внутреннего трудового распорядка, Правила пожарной безопасности, Правила техники безопасности при обращении с ЭВМ) также устанавливаются общеобязательные для работников данной организации (а в соответствующих случаях - и для работников данного индивидуального предпринимателя) требования, которые они должны соблюдать при работе с ЭВМ.

 Безусловно, к числу упомянутых в ст. 274 УК относятся также правила, предусмотренные законами (например, Законом об ЭВМ), различными ведомственными положениями и инструкциями;

 б) в том, что упомянутые нарушения влекут:

 уничтожение охраняемой законом информации ЭВМ (см. о том, что относится к "охраняемой законом информации" комментарий к ст. 272 УК). В результате деяния виновного уничтожается либо сама ЭВМ (например, при пожаре), а вместе с ней и охраняемая информация, либо дискеты, лазерные диски с этой информацией, либо только информация (хотя ЭВМ, машинные носители информации могут и не пострадать). При этом восстановить охраняемую законом информацию не представляется возможным;

 блокирование или модификацию компьютерной информации (о понятиях "блокирование" и "модификация" см. комментарий к ст. 272, 273 УК). В отличие от уничтожения в данном случае компьютерная информация в принципе сохраняется (и даже восстановима), однако доступ к ней законного владельца затруднен или невозможен;

 в) в том, что деяние, предусмотренное в ст. 274 УК:

 либо причиняет собственнику (иному законному владельцу исключительных прав, например пользователю) компьютерной информации существенный вред. Закон не дает его легального определения. Чтобы судить о том, относится вред к "существенному" или нет, необходим анализ конкретных обстоятельств дела (размер убытков, в т.ч. упущенной выгоды, которые понес потерпевший, затраты на приобретение либо создание новой программы, степень повреждения ЭВМ (их систем и сетей), значение информации для обороны, охраны государственной тайны и т.д.);

 либо влечет за собой тяжкие последствия. Последнее обстоятельство относится к квалифицирующим (т.е. отягчающим). Формы тяжких последствий могут быть разнообразными (например, причинение вреда здоровью человека, скажем пациенту, находящемуся на излечении; гибель людей, паника на товарном рынке, обвальное падение курса национальной валюты, разорение кредитной организации, принимающей вклады граждан).

 3. Субъективная сторона совершенного преступления состоит в неосторожной форме вины. Иначе говоря, виновный, нарушая упомянутые в ст. 274 УК правила, действует:

 либо по легкомыслию, т.е. предвидит, что могут наступить такие общественно опасные последствия, как уничтожение, блокирование и т.п. компьютерной информации, но без достаточных к тому оснований рассчитывает такие последствия предотвратить (ч. 2 ст. 26 УК);

 либо по небрежности, т.е. не предвидит наступления указанных в ст. 274 УК последствий, хотя должен и мог их предвидеть (ч. 3 ст. 26 УК).

 Субъектом преступления, предусмотренного в ст. 274 УК, является вменяемое физическое лицо, достигшее 16 лет (ст. 20, 21 УК). Чаще всего такими лицами являются работники ЮЛ и индивидуальных предпринимателей (например, программисты, операторы ЭВМ, бухгалтеры - пользователи ЭВМ). Реже к ним относятся индивидуальные предприниматели, иные граждане, оказывающие услуги заказчику (ЮЛ или индивидуальному предпринимателю) по гражданско-правовым договорам.

 Деяние, упомянутое в ч. 1 ст. 274 УК, относится к преступлениям небольшой, а предусмотренное в ч. 2 ст. 273 УК, - средней тяжести (ст. 15 УК).

1. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция 1997 №10 СПС «Гарант» [↑](#footnote-ref-1)
2. Теория государства и права: Учебное пособие. Конспект лекций в схемах и определениях / Под ред. доцента Л.В. Смирновой. М.: Книжный мир, 2004. с.26 [↑](#footnote-ref-2)
3. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция 1997 №10 СПС «Гарант» [↑](#footnote-ref-3)
4. Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г [↑](#footnote-ref-4)
5. #  Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.

 [↑](#footnote-ref-5)
6. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru [↑](#footnote-ref-6)
7. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru [↑](#footnote-ref-7)
8. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации. –М.: Изд-во Проспект, 2005 с-40 [↑](#footnote-ref-8)
9. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» [↑](#footnote-ref-9)
10. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации. –М.: Изд-во Проспект, 2005 с-37 [↑](#footnote-ref-10)
11. # Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г.

 [↑](#footnote-ref-11)
12. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru [↑](#footnote-ref-12)
13. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации // http://pu.boom.ru [↑](#footnote-ref-13)
14. #  Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г.

 [↑](#footnote-ref-14)
15. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-15)
16. Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г. [↑](#footnote-ref-16)
17. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-17)
18. #  Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.

 [↑](#footnote-ref-18)
19. #  Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.

 [↑](#footnote-ref-19)
20. #  Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г.

 [↑](#footnote-ref-20)
21. Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г. [↑](#footnote-ref-21)
22. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-22)
23. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-23)
24. Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г. [↑](#footnote-ref-24)
25. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-25)
26. Уголовное право России. Особенная часть. Учебник. 2-е изд., испр и доп. (под редакцией В.П. Ревина, доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации). - "Юстицинформ", 2009 г. [↑](#footnote-ref-26)
27. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-27)
28. Гуев А.Н. Комментарий к Уголовному кодексу Российской Федерации для предпринимателей. - Система ГАРАНТ, 2009 г. [↑](#footnote-ref-28)
29. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-29)
30. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-30)
31. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-31)
32. Мосин О.В. Компьютерная преступность в Интернете http://www.yurclub.ru [↑](#footnote-ref-32)
33. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-33)
34. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-34)
35. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-35)
36. <http://www.whatis.ru> [↑](#footnote-ref-36)
37. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-37)
38. <http://www.whatis.ru> [↑](#footnote-ref-38)
39. Криминалистическая характеристика компьютерных преступлений // http://melik.narod.ru [↑](#footnote-ref-39)
40. http://www.itpedia.ru [↑](#footnote-ref-40)
41. С.А. Середа Отвественность за распространение вредоносных программ //Право и экономика 2007 №3 [↑](#footnote-ref-41)