Преступления в сфере компьютерной безопасности

Предмет преступления

В теории уголовного права к предмету неправомерного доступа к компьютерной информации относят технические устройства, на которых эта информация хранится. Существует точка зрения, что предметом любого компьютерного преступления следует признать компьютер как информационную систему, носитель информации. Перекликается с ней позиция, в соответствии с которой предметом преступления выступает компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

Предмет преступления

Если признать предметом рассматриваемых преступлений технические устройства хранения компьютерной информации, то это может привести к трудностям при разграничении преступлений в сфере компьютерной информации и преступлений против собственности.

Предмет преступления

В юридической литературе существует точка зрения, относящая к предмету преступного посягательства «информационную среду, то есть деятельность субъектов, связанную с созданием, преобразованием и потреблением информации». Данная позиция отождествляет предмет неправомерного доступа к компьютерной информации с деятельностью субъектов отношений и неоправданно расширяет предмет преступного посягательства.

Предмет преступления

1) . Что такое компьютерная информация?
2) Какая компьютерная информация является предметом преступления?
3) Имеет ли компьютерная информация цену?
4) Влияет ли цена на уголовно-правовую квалификацию?

Предмет преступления

В ст. 272 УК упоминается охраняемая законом компьютерная информация. Существует ли неохраняемой информации в современном информационном поле в условиях развития информационного общества?

ФЗ от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации» разделил информацию в зависимости от доступа к ней на общедоступную информацию и на информацию, доступ к которой ограничен.

Предмет преступления

Согласно ст. 7 Закона "к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен", т.е. основными свойствами общедоступной информации являются общеизвестность и отсутствие ограничений на доступ к ней. П.3 ст. 3 Закона устанавливает право обладателя информации разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

Предмет преступления

Таким образом, в тот момент, когда обладатель компьютерной информации ограничивает к ней доступ или определяет его порядок, она начинает приобретать требуемое качество охраняемой законом в понимании ст. 272 УК. В случае если обладатель компьютерной информации не реализовал свое право на ограничение доступа к информации, то и рассматривать ее как охраняемую законом нет оснований.

Предмет преступления

Неправомерный доступ к компьютерной информации общего пользования, т.е. информации, адресованной неограниченному кругу лиц, не образует состава преступления, ответственность за совершение которого предусмотрена ст. 272 УК. Само существование такого разделения информации говорит об отсутствии уголовно-правовой защиты общедоступной информации от неправомерного доступа и о необходимости сохранения в диспозиции ст. 272 УК РФ категории "охраняемая законом".

Предмет преступления

Данная информация является предметом неправомерного доступа если:

1. это документированная информация, содержащая сведения, отнесенные законом к государственной тайне или конфиденциальной информации;

2. это информация ограниченного доступа, которая не только имеет специальный правовой статус, установленный соответствующими законами РФ или субъектов Федерации, но и по своему характеру предназначена для ограниченного круга лиц (пользователей), имеющих право на ознакомление и работу с ней.

Предмет преступления

Охраняемой законом по смыслу уголовного закона будет являться такая компьютерная информация, доступ к которой ограничен в соответствии с законом. Доступом к информации, как установлено в п. 6 ст. 2 ФЗ "Об информации, информационных технологиях и о защите информации", является возможность получения информации и ее использования.

Предмет преступления

Признакам информации ограниченного доступа:

1. ценность скрываемых сведений;
2. отсутствие свободного доступа к сведениям на законных основаниях;
3. наличие превентивных мер, принимаемых обладателем сведений для охраны их от доступа третьих лиц.

К информации ограниченного доступа можно отнести следующие виды информации:

Предмет преступления

Государственную тайну. Порядок отнесения сведений к государственной тайне, их засекречивания и рассекречивания регулируется Федеральным законом от 21 июля 1993 г. N 5485-1 "О государственной тайне". Государственная тайна - это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (ст. 2);

Предмет преступления

Банковскую тайну. В соответствии с Федеральным законом от 2 декабря 1990 г. N 395-1 "О банках и банковской деятельности» кредитные организации и их сотрудники обязаны гарантировать тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Это положение Закона также распространяется на операции с электронными денежными средствами, которые зачастую являются мишенью для компьютерных преступников;

Предмет преступления

Персональные данные. В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" персональными данными является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Право граждан на сохранность персональных данных в тайне может быть ограничено лишь в необходимых случаях и только федеральным законом;

Предмет преступления

Информацию, носящую конфиденциальный характер. Указом Президента РФ от 6 марта 1997 г. N 188 "Об утверждении Перечня сведений конфиденциального характера» утвержден Перечень сведений конфиденциального характера. Эти сведения могут быть распределены по следующим группам:
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.

Предмет преступления

В соответствии со ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются; органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Так, например, в соответствии со ст. 12 ФЗ от 15 ноября 1997 г. N 143-ФЗ "Об актах гражданского состояния»

Предмет преступления

сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат. В соответствии с данным Законом также должна обеспечиваться тайна усыновления: работники органов записи актов гражданского состояния не вправе без согласия усыновителей сообщать какие-либо сведения об усыновлении и выдавать документы, из содержания которых видно, что усыновители не являются родителями усыновленного ребенка.

Предмет преступления

Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства« и другими нормативными правовыми актами РФ. УПК РФ не содержит понятия "тайна следствия". В нем используются: "данные предварительного расследования" и "тайна совещания судей».

Предмет преступления

Государственная защита потерпевших, свидетелей и иных участников уголовного судопроизводства - это осуществление предусмотренных настоящим законом мер безопасности, направленных на защиту их жизни, здоровья и (или) имущества, а также мер социальной поддержки указанных лиц в связи с их участием в уголовном судопроизводстве уполномоченными на то государственными органами. По решению органа, осуществляющего меры безопасности, может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств.

Предмет преступления

Служебные сведения, доступ к которым ограничен органами государственной власти и федеральными законами (служебная тайна).

Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и ФЗ. В частности, к ним относятся:

- врачебная тайна - информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, его диагнозе и иные сведения, полученные при его обследовании и лечении (п. 1 ст. 13 ФЗ от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации");

Предмет преступления

- нотариальная тайна - в соответствии со ст. 16 Основ законодательства РФ о нотариате от 11 февраля 1993 г. N 4462-1 нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности;
- адвокатская тайна - любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю (ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре»;

Предмет преступления

- тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений - одна из разновидностей права на неприкосновенность частной жизни, которая гарантируется Конституцией и может быть ограничена только федеральным законом. В соответствии с ФЗ от 7 июля 2003 г. N 126-ФЗ «О связи» операторы связи обязаны обеспечить соблюдение тайны связи. Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

Предмет преступления

Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК и федеральными законами (коммерческая тайна). В соответствии с ФЗ от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне» коммерческой тайной является режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доход, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Предмет преступления

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Права на результаты интеллектуальной деятельности и средства индивидуализации охраняются в соответствии с требованиями части четвертой ГК .

Таким образом, все перечисленные виды информации, охраняемой законом, могут быть предметом преступления, предусмотренного ст. 272 УК. На основе анализа действующих федеральных законов исследователями был сделан вывод, что в настоящий момент существует более 30 видов тайн.

Предмет преступления

Проведенное исследование судебной практики по делам о привлечении к ответственности по ст. 272 УК после вступления в силу ФЗ "Об информации, информационных технологиях и о защите информации" позволило сделать вывод, что суды при вынесении приговоров зачастую дают неправильное определение охраняемой законом компьютерной информации, применяя утративший силу Федеральный закон "Об информации, информатизации и защите информации".

Предмет преступления

Так, Долгопрудненский городской суд Московской области в приговоре от 6 декабря 2011 г. по уголовному делу N 1-175/11 установил, что П., имея в своем пользовании установленный по месту его проживания персональный компьютер, являясь пользователем услуги ООО "ОК" - "МД" на основании заключенного им абонентского договора с ООО "ОК" о предоставлении услуг доступа в компьютерную сеть Интернет, имея умысел на неправомерный доступ к конфиденциальной информации о логинах и паролях абонентов услуги "МД", предоставляемой ООО "ОК", в нарушение ст. 21 ФЗ

Предмет преступления

"Об информации, информатизации и защите информации" в неустановленное время, обнаружив на неустановленном сайте компьютерной сети Интернет данные о логине и пароле абонента услуги "МД" Х., скопировал их в память на жесткий диск своего компьютера. После чего П., находясь по указанному адресу, осознавая возможность незаконного использования данных о логине и пароле абонента услуги "МД" Х., предвидя при этом наступление последствий в виде блокирования работы ЭВМ законного пользователя - Х., связанной с выходом в компьютерную сеть Интернет, и желая наступления

Предмет преступления

этих последствий, без разрешения Х., реализуя свой преступный умысел, направленный на неправомерный доступ к компьютерной информации, в определенный период времени без оплаты осуществлял неправомерный доступ к компьютерной информации, связанный с выходом в компьютерную сеть Интернет под учетными данными указанного абонента, что повлекло блокирование доступа к компьютерной информации для Х., создав условия, исключающие пользование информацией, находившейся в сети Интернет ее законным пользователем.

Предмет преступления

Как следует из приведенного приговора, суд в обоснование своих выводов применил нормы Закона "Об информации, информатизации и защите информации", который в момент рассмотрения дела уже более пяти лет не действовал.

Предмет преступления

Можно ли применить к информации категорию собственности? В науке существует точка зрения, согласно которой «категория собственности может быть применима только к материальным носителям нематериальных объектов, в частности информации», "право собственности относится не к информации, а к ее материальным носителям». Данную позицию сторонники этой точки зрения аргументируют отсутствием на законодательном уровне понятия «собственник информации» и использованием категории «обладатель информации».

Предмет преступления

В ст. 272 УК предусмотрена ответственность именно за неправомерный доступ к компьютерной информации, а не к средствам хранения компьютерной информации.

Понятия "собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения" и "владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения", использовавшиеся в Федеральном законе "Об информации, информатизации и защите информации", были заменены единым понятием "обладатель информации" (п. 2 ст. 2 ФЗ "Об информации, информационных технологиях и о защите информации»).

Предмет преступления

Действующее законодательство под обладателем информации понимает лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Категория "обладатель информации" объединяет в себе категорию "собственник информации" и категорию "владелец информации". Так, лицо, создавшее определенные данные, является собственником информации и может ограничить доступ к ней.

Предмет преступления

При получении на основании закона или договора информации от собственника лицо считается владельцем информации и обязано обеспечить условия ограничения доступа к ней, определенные собственником.

Представляется, что после введения в действие ФЗ "Об информации, информационных технологиях и о защите информации" для привлечения к уголовной ответственности необходимо определить, был ли нарушен установленный режим доступа к информации.

Предмет преступления

Судебная практика свидетельствует, что суды при квалификации деяний по ч.1 ст. 272 УК устанавливают, является ли компьютерная информация охраняемой законом, ограничен ли к ней доступ. Так, Ленинский районный суд г. Тюмени в приговоре от 17 июля 2012 г. установил следующее. Гражданин Г., имея преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, достоверно зная, что учетно-регистрационные данные - логин и пароль, необходимые для подключения ЭВМ к интернет-сайту: www.Educon.tsogu.ru, позволяют получить возможность ознакомления с информацией

Предмет преступления

ограниченного доступа (в соответствии со ст. 3,6,8,9,16 ФЗ "Об информации, информационных технологиях и о защите информации") и правомерно могут использоваться только лицом, их получившим на законных основаниях, осуществил неправомерный доступ к компьютерной информации.

Исследуя судебные приговоры, вынесенные после вступления в силу ФЗ "Об информации, информационных технологиях и о защите информации", можно сформулировать вывод, что суды все еще не используют понятие "обладатель" информации, а в приговорах указывают собственника и владельца информации.

Предмет преступления

Кезский районный суд Удмуртской Республики в приговоре от 10 февраля 2011 г. установил, что Л., используя свой персональный компьютер с процессором, сетевым оборудованием и установленной операционной системой, в комплект которой входит программное обеспечение для доступа в сеть Интернет при помощи ADSL-модема с зарегистрированным абонентским номером телефонной линии общего значения, обеспечивающего соединение для сеансов доступа в сеть Интернет с учетными данными (логином и соответствующим паролем), принадлежащими Х., в нарушение

Предмет преступления

ст. 2,4,6,10,12,13,17 ФЗ "Об информации, информационных технологиях и о защите информации", умышленно, с целью использования чужого логина и пароля для неправомерного доступа к охраняемой законом компьютерной информации, в виде безвозмездного незаконного пользования сетью Интернет, пренебрегая установленным в Российской Федерации режимом защиты компьютерной информации и стремясь удовлетворить личные интересы, осуществил без согласия собственника информации - провайдера и легального пользователя Х.

Предмет преступления

доступ к охраняемой законом компьютерной информации - логина и пароля и использовал эту информацию.

В целях реализации норм ФЗ «Об информации, информационных технологиях и о защите информации" и ФЗ от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне» утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения". В п. 2.5.2 вышеназванного Стандарта указано, что под защиту

Предмет преступления

подпадает "информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации».

Как предмет преступления информация должна помимо формы в виде документа обладать определенной ценностью. В настоящее время не существует единого критерия определения ценности информации.

Предмет преступления

Ее можно определить как максимальную пользу, которую может принести данное количество информации, или как те максимальные потери, к которым приведет утрата этого количества информации. Теоретически один и тот же информационный объект может иметь разную ценность для субъектов, поэтому такая категория, как "ценность информации", не может влиять на отнесение компьютерной информации к предмету преступления, предусмотренного ст. 272 УК . Ценность информации следует определять ее обладателю.

Объективная сторона преступления

Доступ к компьютерной информации – возможность получения информации и ее использование (ФЗ №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Так, в Постановлении президиума Свердловского областного суда от 30 сентября 2009 г. по делу N 44-У-286/2009 указано: "Объективная сторона заключается в неправомерном доступе к этой информации, означающем несанкционированное проникновение, взлом электронной системы защиты этой информации". В приговоре по делу N 1-125/2010 Алатырский районный суд Чувашской Республики определил

Объективная сторона преступления

неправомерный доступ к компьютерной информации как несанкционированный собственником информационной системы доступ к охраняемой законом компьютерной информации. Аналогичную позицию занял Чкаловский районный суд г. Екатеринбурга, который в приговоре по делу N 1-749/2011 отметил, что неправомерным является доступ, осуществленный «вопреки воле работодателей и без заключения договора с ними». Неправомерный доступ к компьютерной информации имеет место при отсутствии соответствующего разрешения со стороны обладателя, но всегда ли неправомерный доступ сопровождается преодолением средств защиты.

Объективная сторона преступления

На практике может возникнуть ситуация осуществления доступа к компьютерной информации лицом, не имеющим на это права, предоставленного обладателем информации, без преодоления средств защиты (например, осуществление доступа к информации на включенном другим лицом компьютере). Однако в любом случае, если был факт самовольного доступа к охраняемой законом компьютерной информации, то это безусловно нарушает права ее собственника или владельца по распоряжению данной информацией и ее использованию.

Объективная сторона преступления

В ст. 272 УК законодатель не ставит охрану информации в зависимость от ее технической защищенности. Уместно провести аналогию с составом преступления, предусмотренным ст. 158 УК. Государство защищает имущество в квартире как частную собственность независимо от того, установил ли собственник квартиры входную дверь, так и компьютерная информация подлежит охране государством безотносительно использования средств защиты информации. Таким образом, неправомерным является доступ к охраняемой законом информации и в случае, если информация на компьютере находится без средств защиты.

Объективная сторона преступления

Общественно опасные последствия. Уничтожение компьютерной информации является особенно опасным последствием неправомерного доступа к компьютерной информации, так как наносит наиболее существенный, а зачастую и невосполнимый вред компьютерной информации.

К настоящему времени сложилось несколько теоретических подходов к определению понятия "уничтожение":

а) удаление информации при невозможности восстановления;

Объективная сторона преступления

б) удаление информации вне зависимости от возможности восстановления;

в) уничтожение - это такой вид «воздействия на компьютерную информацию, при котором навсегда теряется возможность ее дальнейшего использования кем бы то ни было»;

г) потеря информации вообще, ее утрата при невозможности восстановления в первоначальном виде в конкретной информационной системе;

д) приведение информации или ее части в непригодное для использования состояние.

Объективная сторона преступления

Наступление преступных последствий будет налицо с того момента, когда файл или его часть станут "невидимыми" для средств программного обеспечения, используемого законным пользователем, и недоступными для их стандартных команд.

Для квалификации преступления по ч.1 ст. 272 УК не имеет значения, остались ли у собственника, владельца, пользователя второй образец или копия уничтоженной информации или нет.

Объективная сторона преступления

Что понимается под блокированием информации? Проведенный юридический анализ позволяет сформулировать вывод, что понятие "блокирование" с возможностью или невозможностью использования компьютерной информации:

а) блокирование - невозможность получить доступ в течение значимого промежутка времени к компьютерной информации ее законному пользователю при сохранности самой информации в информационной системе;

Объективная сторона преступления

б) блокирование - создание условий, при которых невозможно или существенно затруднено использование информации при сохранности такой информации; закрытие информации, характеризующееся недоступностью ее использования по прямому назначению со стороны законного пользователя, собственника или владельца; невозможность доступа к ней со стороны законного пользователя; создание препятствий к свободному доступу, при этом информация не подвергается уничтожению; полная или частичная временная невозможность доступа к компьютерной информации для дальнейшего ее использования;

Объективная сторона преступления

создание препятствий по правомерному доступу к компьютерной информации при ее сохранности; различные действия и манипуляции лица, которые приводят к тому, что владелец информации временно или постоянно лишается возможности использовать эту информацию и осуществлять с ней различные операции в своих интересах.

Объективная сторона преступления

Суды при определении понятия "блокирование" используют ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения». В соответствии с п. 3.3.8 вышеназванного документа "блокирование доступа (к информации): прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей)".

Объективная сторона преступления

Так, 12 мая 2012 г. Ленинским районным судом г. Курска вынесен приговор по уголовному делу N 1-81/7-2012 в отношении В., обвиняемого в совершении преступлений, предусмотренных ч. 1 ст. 272, ч. 2 ст. 272, ч.3 ст. 272, ч. 4 ст. 272 УК. Суд установил: "В. совершил неправомерный доступ к охраняемой законом компьютерной информации... и это деяние повлекло блокирование информации. В июне 2010 г. В., имея навык обращения с компьютерным и сетевым оборудованием, а также имея в собственности портативный компьютер, будучи активным пользователем сети Интернет, услуги по доступу к которой ему были предоставлены согласно

Объективная сторона преступления

абонентскому договору о предоставлении услуг связи на условиях предварительной оплаты филиалом ООО "И", в котором он работал до февраля 2010 г. по договору подряда на должности системного администратора, обнаружил, что доступ к сети Интернет работает некорректно.

В этот момент, т.е. в июне 2010 г., с целью обеспечения подключения к корректно работающей сети Интернет, у В. возник умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, находящейся на VPN-сервере, расположенном по адресу, принадлежащему филиалу ООО "И".

Объективная сторона преступления

Для осуществления своих преступных намерений В., по роду деятельности системный администратор в филиале ООО "И", зная логин и пароль к доступу на VPN-сервер этого филиала, в июне 2010 г. посредством корректно работающей локальной сети филиала ООО "И" и используя для связи с VPN-сервером (с IP-адресом N), принадлежащим филиалу ООО "И", свой портативный компьютер с установленным программным обеспечением ввел логин и пароль, принадлежащие легальному пользователю - работнику филиала ООО "И", при этом осознавая, что указанный логин и пароль ему не принадлежат, осуществил

Объективная сторона преступления

неправомерный доступ к VPN-серверу, принадлежащему филиалу ООО "И", на котором находилась охраняемая законом компьютерная информация.

В результате указанных умышленных неправомерных действий В. в 15 часов 30 минут 49 секунд, в 22 часов 15 минут 18 секунд, в 23 часа 45 минут 38 секунд произошло блокирование информации, т.е. прекращение и затруднение доступа к информации лиц, имеющих на это право (согласно п. 3.3.8 ГОСТ Р 53114-2008). В результате неправомерных действий В., законный (легальный) пользователь, работающий в должности ведущего менеджера по работе с

Объективная сторона преступления

корпоративными клиентами филиала ООО "И", при исполнении своих служебных обязанностей в указанный период не смог осуществить правомерный доступ к охраняемой законом компьютерной информации, расположенной на VPN-сервере (с IP-адресом N), расположенном по адресу, принадлежащему филиалу ООО "И", что повлекло за собой причинение вреда деловой репутации филиалу ООО "И».

Объективная сторона преступления

В ст.14 УК определено "не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного УК, но в силу своей малозначительности не представляющее общественной опасности". Таким образом, блокирование информации, длящееся от нескольких секунд до нескольких минут и не повлекшее последствий, кроме невозможности ее использования в течение нескольких минут, не может признаваться преступлением в силу своей малозначительности.

Объективная сторона преступления

Подводя итог анализу понятия "блокирование компьютерной информации", можно заключить, что ученые и правоприменители в качестве основного признака исследуемого последствия неправомерного доступа к компьютерной информации называют невозможность доступа к компьютерной информации со стороны законного обладателя для ее использования.

Коммерческая тайна

В РФ Постановление Правительства РСФСР от 5 декабря 1991 г. N 35 "О перечне сведений, которые не могут составлять коммерческую тайну». Учетно-регистрационные данные в этом перечне отсутствуют. В соответствии с п. 1 ст. 4 ФЗ от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне» право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю данной информации.

Коммерческая тайна

Суды при квалификации незаконного получения чужих регистрационных данных для доступа в сеть Интернет определяют юридически значимые обстоятельства, а именно отнесены ли учетно-регистрационные данные абонентов к коммерческой тайне.

В качестве примера приведем выдержки из приговора Тавдинского районного суда Свердловской области от 5 апреля 2011 г.. Ф. собирал сведения, составляющие коммерческую тайну, совершил неправомерный доступ к охраняемой законом компьютерной информации. В соответствии с ФЗ "О коммерческой

Коммерческая тайна

тайне", с перечнем сведений, составляющих конфиденциальную информацию ОАО "ХХХ", утвержденным советом директоров ОАО "ХХХ", и перечнем сведений, составляющих коммерческую тайну ОАО "ХХХ", утвержденным советом директоров, сведения об абонентах, позволяющие идентифицировать абонента или оконечное оборудование, сведения о настройках и паролях доступа, используемых в средствах защиты информационных ресурсов и автоматизированных системах управления ОАО "ХХХ", отнесены к коммерческой тайне ОАО "ХХХ".

Коммерческая тайна

В соответствии с п. 1.12 Перечня сведений, составляющих коммерческую тайну, Положением о конфиденциальной информации МУП "ХХХХ" сведения о состоянии программного и компьютерного обеспечения, каковыми являются логин и пароль для доступа в сеть Интернет, отнесены к коммерческой тайне МУП "ХХХХ". Незаконно получив учетно-регистрационные данные абонента ОАО "ХХХ", Ф. в период с ХХХХ г. в дневное, вечернее и ночное время, используя учетно-регистрационные данные абонента ОАО "ХХХ", неоднократно осуществлял неправомерный доступ к сети Интернет.

Коммерческая тайна

Своими действиями Ф. ввел ОАО "ХХХ" в заблуждение относительно того, что доступ к сети Интернет осуществлял правомерный пользователь МУП "ХХХХ", в связи с чем Ф. были оказаны услуги по предоставлению доступа в сеть Интернет, а расходы по их оплате на сумму ХХХХ руб. отнесены на счет МУП "ХХХХ". В судебном заседании нашел свое подтверждение сбор Ф. сведений, составляющих коммерческую тайну. Получение законным способом логина и пароля пользователя услуг сети Интернет возможно только в результате заключения договора с провайдером или получения сведений с согласия

Коммерческая тайна

собственника. Ф., зная, что он не заключал договор, в результате которого мог законно получить логин и пароль, получил их из сети Интернет, осознавая, что права на получение указанных сведений у него нет. Указанные обстоятельства подтверждаются показаниями Ф., из которых следует, что он понимал, что это чужие логины и пароли. Суд приговорил признать Ф. виновным в совершении преступлений, предусмотренных ч. 1 ст. 183, ч. 1 ст. 272, ч. 1 ст. 165 УК. Как следует из приведенного выше приговора, суд для квалификации деяния по ст. 183 УК установил, относятся ли учетно-регистрационные сведения абонентов к коммерческой тайне.

Копирование компьютерной информации

В настоящее время сложилось несколько подходов к решению вопросов о том, что такое копирование компьютерной информации и какие способы ее копирования существуют. Проведенный анализ следственно-судебной практики позволил нам сделать вывод, что суды определяют "копирование компьютерной информации" как перенос с одного носителя информации на другой.

Например, Егорьевский городской суд Московской области от 3 марта 2011 г. установил, что подсудимый Р. совершил неправомерный доступ к охраняемой законом компьютерной информации. Это деяние повлекло копирование информации. Подсудимый Р., имея единый преступный умысел, направленный на осуществление неправомерного доступа к охраняемой законом информации и ее копирование,

Копирование компьютерной информации

незаконно приобрел путем скачивания на компьютер из сети Интернет и последующей записи на цифровой носитель нелицензионные версии программных продуктов. После этого подсудимый Р. с целью реализации своего преступного умысла, направленного на осуществление неправомерного доступа к охраняемой законом информации и ее копирование, действуя умышленно, вставил в установленный там же компьютер цифровой носитель, содержащий ранее незаконно приобретенные им нелицензионные версии программных продуктов, после чего, доводя свой преступный умысел до конца, произвел копирование с

Копирование компьютерной информации

указанного цифрового носителя на жесткий диск компьютера, тем самым совершив неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, повлекший ее копирование с цифрового накопителя на жесткий диск компьютера. Таким образом, подсудимый Р. совершил преступление, предусмотренное ч. 1 ст. 272 УК.

Из приведенного приговора следует, что судом под копированием компьютерной информации признается перенос информации с оригинального носителя информации на другой.

доступ и последствия

Проведенный анализ судебных дел, связанных с привлечением виновных к ответственности за неправомерный доступ к компьютерной информации, показал, что суды не всегда правильно понимают понятия "доступ" и "последствия", отождествляя их, что приводит к ошибкам в толковании норм Уголовного кодекса РФ.

Доступ и последствия

В качестве примера приведем Постановление от 14 марта 2012 г. о прекращении уголовного дела N 1-155/12, принятое Первомайским районным судом г. Ижевска Удмуртской Республики. Дело прекращено в соответствии со ст. 25 УПК в связи с примирением сторон. "Обвиняемый Х. совершил неправомерный доступ к охраняемой законом компьютерной информации при следующих обстоятельствах. С 8 февраля 2008 г. по договору N Х провайдером ООО "Н" был предоставлен доступ к сети Интернет. В силу ст. 2,6 ФЗ "Об информации, информационных

Доступ и последствия

технологиях и о защите информации" К., создав информацию на Г@mail.ru, является обладателем данного аккаунта и вправе разрешать или ограничивать доступ к принадлежащей ей информации, защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования другими лицами. Разрешения для пользования указанным аккаунтом К. никому не давала, в том числе иДо 20 часов 55 минут 22 октября 2011 г. у Х. возник преступный умысел, направленный на неправомерный доступ Х. к

Доступ и последствия

охраняемой законом компьютерной информации - к принадлежащему К. аккаунту. Реализуя свой преступный умысел, действуя умышленно, осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно опасных последствий в виде неправомерного доступа к охраняемой законом компьютерной информации, ее блокирование и модификацию, К. осуществил несанкционированный доступ к аккаунту, принадлежащемуК.».Постановление Первомайского районного суда г. Ижевска от 14 марта 2012 г. о прекращении уголовного дела N 1-155/12.

Доступ и последствия

Законодатель не дает определения понятия «удаление информации».

Под ним можно понимать – совершение действий, в результате которых становится невозможно восстановить содержание компьютерной информации, и(или) в результате которых уничтожаются носители компьютерной информации.

Большинство правоведов недоработкой законодателя считают отсутствие в нормах УК РФ указания на "ознакомление с компьютерной информацией" как на общественно опасное последствие неправомерного доступа к компьютерной информации. Сам факт того, что информация становится известна третьему лицу, причиняет существенный вред ее обладателю
Получается, что если информация была скопирована, то все признаки состава преступления есть, а если она была просто прочитана – нет. Ознакомление с информацией путем ее прочтения не менее опасно, чем ее копирование. В некоторых случаях злоумышленнику достаточно увидеть и прочитать

информацию, и она теряет свою ценность или может быть применена им в дальнейшем без всякого копирования. Независимо от того, наступили ли указанные последствия или нет, сам по себе факт неправомерного доступа уже представляет собой грубейшее нарушение прав собственника на владение компьютерной информацией.

Неправомерный доступ может быть осуществлен двумя способами:

либо путем хищения самих носителей компьютерной информации (например, кража диска, флеш-накопителя и т.п.) и последующего доступа к хранящейся на них компьютерной информации;

либо путем перехвата информации с использованием компьютерной техники.

Большинство преступлений совершается вторым способом. Методы несанкционированного доступа и перехвата компьютерной информации:

- "жучок" (bugging) - характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;

- "откачивание данных" (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
- "уборка мусора" (scavening) - характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.п. Электронный вариант требует исследования данных, оставленных в памяти машины;

- метод следования "за дураком" (piggbacking) - характеризует несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если взять в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;
- метод "поиск бреши" (trapdoorentry) - используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

- метод "мистификация" (spoofing) - используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать полезную для него информацию, например коды пользователя.

Квалифицированный вид неправомерного доступа к компьютерной информации (ч. 2 ст. 272 УК РФ) представляет собой деяние, предусмотренное ч. 1 данной статьи, причинившее крупный ущерб или совершенное из корыстной заинтересованности.

Крупный ущерб определен в примечании к ст. 272 УК РФ и применяется для всех составов преступлений гл. 28 УК. Крупным ущербом признается ущерб, сумма которого превышает 1 млн. руб.

Содержание понятия "корыстная заинтересованность законодатель не раскрывает. В русском языке слово "корысть" понимается как стремление получить материальную выгоду любым путем. Также это понятие толкуется как страсть к приобретению и наживе, жадность к деньгам, богатству и падкость на барыш, стремление к богатству. В Постановлении Пленума Верховного Суда РФ от 16 октября 2009 г. N 19 "О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий« корыстная заинтересованность определяется как стремление путем совершения неправомерных действий получить

для себя или других лиц выгоду имущественного характера либо избавиться от материальных затрат (освобождение от каких-либо имущественных затрат, погашение долга, оплаты услуг, уплаты налогов и т.п.). Часть 3 ст. 272 устанавливает ответственность за деяния, предусмотренные ч. 1 и 2 данной статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

Для квалификации преступления по ч. 3 ст. 272 УК суды устанавливают возникновение сговора до осуществления неправомерного доступа к охраняемой законом компьютерной информации.

В Кассационном определении от 26 апреля 2012 г. по делу N 22-475/2012 судебная коллегия по уголовным делам суда Ямало-Ненецкого автономного округа, рассмотрев в открытом судебном заседании уголовное дело по кассационному представлению государственного обвинителя и кассационной жалобе осужденного Ю. на приговор Новоуренгойского городского суда Ямало-Ненецкого автономного округа

от 23 января 2012 г., установила следующее: "По приговору суда Ю., М., С. признаны виновными и осуждены за:

- причинение имущественного ущерба ОАО "У" путем обмана при отсутствии признаков хищения, совершенное группой лиц по предварительному сговору, причинившее особо крупный ущерб;

-Ю. и М. за неправомерный доступ к охраняемой законом компьютерной информации, совершенный группой лиц по предварительному сговору; С. за те же действия с использованием своего служебного положения".

В качестве доказательства совершения неправомерного доступа к охраняемой законом компьютерной информации группой лиц по предварительному сговору суд обоснованно принял "многочисленную переписку виновных лиц между собой, осуществляемую посредством сети Интернет и обнаруженную на технических устройствах Ю., С., М., в ходе которой осужденные обсуждали факт выявления их преступной деятельности, возможную уголовную ответственность, а также тактику

поведения, которой следует придерживаться с целью избежания такой ответственности».

При совершении преступления организованной группой необходимо установить, что она состоит не из случайных людей, а функционирует на взаимном доверии, имеет лидера, который является "мозговым центром", обеспечивает целенаправленную, спланированную и слаженную деятельность как группы в целом, так и каждого ее участника.

Организованная преступная группа может создаваться для совершения как одного, так и нескольких преступлений.

В качестве примера осуществления неправомерного доступа к охраняемой законом компьютерной информации, совершенного организованной преступной группой, приведем уголовное дело в отношении одного из участников организованной преступной группы. 10 марта 2011 г. следователем ГСУ ГУ МВД России по г. Москве возбуждено уголовное дело по ч. 2 ст. 272 УК РФ (неправомерный

доступ к компьютерной информации).

В 2010 г. организатор преступной группы, находящийся в федеральном розыске за побег из исправительной колонии в Смоленской области, приобрел за 550 тыс. долларов в одной из компаний в г. Дубае (ОАЭ) и незаконно ввез в Россию комплекс технических средств, который позволял негласно контролировать каналы связи.

Под его руководством четыре участника организованной преступной группы установили данный комплекс в автомобиль ГАЗ, замаскированный надписями о ремонтных работах. Затем с помощью этого устройства члены ОПГ осуществляли

неправомерный доступ к компьютерной информации операторов сотовой связи, затем копировали данные с мобильных телефонов проходящих мимо машин граждан и путем инициирования исходящих вызовов и СМС-сообщений определенным образом модифицировали в системах ЭВМ информацию. Таким образом, злоумышленники незаконно завладевали денежными средствами граждан в различных районах Москвы, а также Брянской, Московской, Орловской и Смоленской областях.

Официальный сайт ГУВД по г. Москве.

Как следует из приведенного примера, у организованной преступной группы был руководитель, распределявший роли между соучастниками, всех соучастников объединял единый умысел, направленный на совершение преступления, предусмотренного ст. 272 УК РФ.

В настоящее время существует и другая тенденция принципов структурно-функционального построения преступных групп. Например, при организации организованных преступных групп в сетевом информационном пространстве практически отсутствуют группы, создающиеся на длительное время, для которых характерны устойчивость,

---

сплоченность, основанные на организационно-иерархических связях; такие группы объединяются на основе сетевой формы организации. Как правило, преступные группы в сетевом информационном пространстве организовываются для осуществления конкретной задачи, в связи с этим их составу свойствен достаточно высокий уровень изменчивости. Участники таких групп порой лично незнакомы.

На практике могут возникнуть трудности при квалификации неправомерного доступа к компьютерной информации по ч. 2 ст. 272 УК в случае, когда один из соучастников осуществляет неправомерный доступ к компьютерной информации,

а другие нет. Очевидно, разграничение должно идти по направленности умысла. Если умысел един, то действия всех соучастников квалифицируются по ч. 3 ст. 272 УК.

Если умысел направлен не на компьютерную информацию, а на другой объект уголовно-правовой охраны, а неправомерный доступ выступает лишь в качестве способа совершения преступления, то по ст. 272 УК должно нести ответственность только лицо, чьим умыслом охватывается неправомерный осуществлявшее доступ к компьютерной информации. Как правило, это имеет место при совершении хищений с использованием компьютерных технологий.

Квалифицированный вид неправомерного доступа к компьютерной информации (ч. 4 ст. 272 УК РФ) представляет собой деяния, предусмотренные ч. 1 - 3 данной статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Законодатель не раскрывает понятие "тяжкие последствия" не раскрывается, оно является оценочным и должно определяться судом в каждом конкретном случае в зависимости от обстоятельств дела.

Включение преступного вреда посредством оценочных понятий в основные составы преступлений делает неясными рамки преступных и непреступных форм поведения и дает настолько широкую свободу правоприменителям, что они вынуждены в своей практической деятельности подменять законодателя и самостоятельно решать вопрос о пределах криминализации деяний.

К тяжким последствиям неправомерного доступа к компьютерной информации могут быть отнесены внедрение в системы, регулирующие безопасность жизни и здоровья граждан (например, в диспетчерские системы на транспорте, особенно воздушном,

системы, обеспечивающие обороноспособность страны, отвечающие за экологическую безопасность), случаи гибели людей либо причинения тяжкого вреда здоровью, а также значительного экономического ущерба государству, юридическим и физическим лицам в результате дезорганизации работы производственных комплексов, нарушения организованной работы транспорта, уничтожения или повреждения имущества.

Статья 273 УК

Статья 273 УК предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты компьютерной информации.

Вредоносная программа

а) вредоносная программа - это программа, приводящая к несанкционированным уничтожению, блокированию, модификации либо копированию информации ;

б) вредоносная программа - компьютерная программа, функционирование которой вызывает не санкционированные собственником компьютерной информации ее уничтожение, блокирование, модификацию либо копирование;

в) вредоносная программа - это программа, специально созданная или модифицированная компьютерная программа, способная совершать

действия, приводящие к не санкционированным собственником информационной системы уничтожению, блокированию, модификации либо копированию информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях;

г) вредоносной программой является "программное средство, которое было создано для выполнения не санкционированных собственником и другими законными владельцами информации, ЭВМ, системы ЭВМ или их сети функций».

В связи с тем что вредоносная компьютерная программа является разновидностью компьютерной программы, необходимо более подробно рассмотреть толкование понятия "программа для ЭВМ". Согласно ст. 1261 ГК. В ней под понятием "программа для ЭВМ" понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, таким образом, чтобы достигался определенный результат, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Действующий ГК РФ использует весьма устаревшее понятие "ЭВМ", в то время как УК РФ оперирует понятием «компьютерная программа».
Определение вредоносной программы дается в п. 2.6.5 ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", утвержденного Приказом Ростехрегулирования от 27 декабря 2006 г. N 373-ст. Вредоносной является программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

В свою очередь, несанкционированное воздействие на информацию представляет собой 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.

Определение понятия "вредоносная программа" содержится в Соглашении о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

Согласно п. "в" ст. 1 данного документа "вредоносная программа - созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированным уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети".

В Постановлении Правительства РФ от 10 сентября 2007 г. N 575 «Об утверждении Правил оказания телематических услуг связи» дается определение вредоносного программного обеспечения, под которым понимается программное обеспечение, целенаправленно приводящее к нарушению законных

прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя либо к ухудшению параметров функционирования абонентского терминала или сети связи. Результатом запуска вредоносной программы является нарушение нормального порядка работы программ, что может выражаться в невыполнении команд пользователя, невозможности запуска программ, открытия тех или иных файлов.

Мобильные телефоны

Суды признают лиц, создавших, распространивших или использовавших вредоносные программы для мобильных телефонов, виновными в совершении преступлений по ст. 273 УК РФ.

Например, Басманным районным судом г. Москвы 12 июля 2011 г. вынесен приговор по уголовному делу N 1-190/11 по обвинению гражданина В. в совершении преступления, предусмотренного ч. 1 ст. 273 УК. Суд установил, что В. занимался созданием и распространением программ для ЭВМ, заведомо приводящих к несанкционированным уничтожению, блокированию, модификации либо копированию

Мобильные телефоны

информации. Находясь по месту жительства, он, действуя с целью сбыта, осуществлял создание вредоносных программ для мобильных телефонов, а именно:

- программы, позволяющей мобильному телефону (контролирующему) совершать в скрытом от пользователя контролируемого телефона режиме следующие действия: получать информацию - СМС-сообщения о начале разговора по контролируемому телефону, копии входящих и исходящих СМС-сообщений, отправляемых с контролируемого телефона; записывать аудиосигналы, поступающие на

Мобильные телефоны

контролируемый мобильный телефон (звуки около телефона); получать информацию о телефонном аппарате, его текущем состоянии и местонахождении; прослушивать телефонные переговоры;

программы, позволяющей накапливать во внутренней памяти контролируемого телефона записи входящих и исходящих разговоров, входящих и исходящих СМС-сообщений, звуков вокруг телефона, контактов из памяти телефона, определять его точное местонахождение, если мобильный телефон поддерживает GPS-приемник, после накопления информации получать информацию с контролируемого

Мобильные телефоны

мобильного телефона посредством передачи данных через связь без ведома и негласно для пользователя; программы, позволяющей изменять индивидуальный идентификационный номер телефона IMEI.

После установки указанных вредоносных программ в мобильные телефоны различных марок и модификаций телефоны приобретали способность без ведома пользователя выполнять следующие функции: управление вызовами; прием входящих СМС-сообщений; отправка СМС-сообщений; удаление СМС-сообщений; блокирование уведомления о входящих СМС-сообщениях; блокирование сообщения о

Мобильные телефоны

входящих вызовах; включение диктофона; создание и удаление файлов в памяти телефона; запись переговоров, ведущихся с использованием телефона. Каждый мобильный телефон с установленными на нем вредоносными программами, разработанными и распространяемыми В., являлся специальным техническим средством, предназначенным для негласного съема акустической информации (съема акустических сигналов, поступающих на микрофон телефона) и прослушивания телефонных разговоров лица, использующего данный телефонный аппарат.

Нейтрализация средств защиты компьютерной информации

Определение понятия "защита информации" содержится в ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", утвержденном Приказом Ростехрегулирования от 27 декабря 2006 г. N 373-ст. Согласно п. 2.1.1 названного документа под защитой информации следует понимать деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Нейтрализация средств защиты компьютерной информации

Защита информации - это совокупность мер, обеспечивающих безопасность прав владельцев информационной продукции, в первую очередь программ, баз и банков данных, от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.

Нейтрализация средств защиты компьютерной информации

Статья 2 Федерального закона от 21 июля 1993 г. N 5485-1 "О государственной тайне» содержит приблизительный перечень средств защиты информации: технические, криптографические, программные и другие средства, предназначенные для защиты сведений.

К техническим средствам относятся изделия, оборудование, аппаратура и (или) их составные части, функционирующие на основании законов электротехники, радиотехники и (или) электроники и содержащие электронные схемы и (или) компоненты.

Нейтрализация средств защиты компьютерной информации

К криптографическим средствам защиты можно отнести любые способы секретной записи и механическое либо электрическое устройство, используемые в целях маскировки или сокрытия содержания, значимости или смысла передаваемой информации. ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", утвержденный Приказом Ростехрегулирования от 27 декабря 2006 г. N 373-ст, относит к криптографическим такое средство защиты

Нейтрализация средств защиты компьютерной информации

информации, которое реализует алгоритмы криптографического преобразования информации.

Программные средства - это средства, предусматривающие определенную последовательность процедур, направленных на защиту компьютерной информации. Программные средства в компьютерном смысле - это объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерных устройств, с целью получения

Нейтрализация средств защиты компьютерной информации

определенного результата, включая подготовительные материалы, полученные в ходе разработки компьютерной программы, и порождаемые ею аудиовизуальные отображения.

Деятельность по технической защите информации подлежит лицензированию в соответствии с Постановлением Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации».

Нейтрализация средств защиты компьютерной информации

В соответствии с абз. 3 п. 1 Положения о сертификации средств защиты информации, утвержденного Постановлением Правительства РФ от 26 июня 1995 г. N 608, указанные средства защиты подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности.

Нейтрализация средств защиты компьютерной информации

Сертификация на соответствие требованиям по безопасности информации осуществляется органом по сертификации и представляет собой форму подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров (п. 2.8.3 ГОСТ Р 50922-2006). Одним из распространенных сертифицированных средств защиты информации является система "SecretNet", которую используют для защиты конфиденциальной информации и государственной тайны.

Нейтрализация средств защиты компьютерной информации

Программные средства защиты содержат механизм мандатного разграничения доступа. Система принимает решение о возможности доступа субъекта к объекту или о запрете доступа, принимая за основание тип операции, связанный с каждым субъектом, и мандатную метку, связанную с объектом. Как правило, средства защиты информации содержатся в ядре операционной системы, но идентификация, аутентификация и контроль целостности файлов являются отдельными программными компонентами.

Нейтрализация средств защиты компьютерной информации

Помимо очевидного взлома программ антивирусной защиты под нейтрализацию может подпасть и следующая ситуация. Зачастую пользователи выкладывают лицензионное программное обеспечение вместе с программами, с помощью которых можно взломать защиту лицензионного программного обеспечения и использовать его несколько раз. К таким программам относятся:

Нейтрализация средств защиты компьютерной информации

1) "кейген" (от англ. keygen - keygenerator - генератор ключей) - это программа, которая генерирует либо криптографические ключи для шифрования данных, либо псевдоподлинные CD-ключи или серийные, регистрационные или активационные номера для регистрации или активирования программного обеспечения;

Нейтрализация средств защиты компьютерной информации

2) "крэк" (от англ. crack - разламывать, раскалывать) - специальная программа для взлома программного обеспечения. Формально под действие ст. 273 УК РФ может подпасть очень большое количество пользователей сети Интернет, которые используют "взломанное" программное обеспечение.

Нейтрализация средств защиты компьютерной информации

Анализ судебной практики подтверждает, что использование компьютерных программ нейтрализации средств защиты есть средство к получению неправомерного доступа к компьютерной информации. Снежинским городским судом Челябинской области за использование компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации (ч. 1 ст. 273 УК РФ), осужден гражданин Г. Как установлено, в апреле 2012 г. в дневное время Г., находясь в

Нейтрализация средств защиты компьютерной информации

гостинице г. Снежинска, установил на три компьютера другого лица за вознаграждение в 1000 руб. программу "Компас 3D V-13", правообладателем которой является ЗАО "А".

При установке программного обеспечения "Компас 3D V-13" подсудимый использовал компьютерную информацию, файл "KOMPAS 3D V13 antiHASP v 1.0 exe", который заведомо для виновного был предназначен для нейтрализации средств защиты указанного программного обеспечения. При запуске этого файла часть оригинальных файлов программного продукта "Компас 3D V-13" была

Нейтрализация средств защиты компьютерной информации

модифицирована, что позволило использовать этот программный продукт без электронного ключа защиты. Была осуществлена нейтрализация средств защиты компьютерной информации, получен неправомерный доступ к указанному программному обеспечению.

Разработка и использование программных средств защиты информации являются необходимыми условиями обеспечения информационной безопасности. Думается, что именно обладатель компьютерной информации должен в первую очередь принимать все необходимые меры, направленные на ее защиту от неправомерного воздействия.

Нейтрализация средств защиты компьютерной информации

На сегодняшний день разработка и использование программных средств защиты информации являются необходимыми условиями обеспечения информационной безопасности. Думается, что именно обладатель компьютерной информации должен в первую очередь принимать все необходимые меры, направленные на ее защиту от неправомерного воздействия.

Информационно-телекоммуникационная сеть.

Статья 2 ФЗ "Об информации, информационных технологиях и о защите информации» понимает под информационно-телекоммуникационной сетью технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Согласно ст. 2 ФЗ «О связи» оконченное (пользовательское) оборудование - это технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.