УДК 343.1 doi: 10.20310/1819-8813-2017-12-6-463-468

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ЛОСКУТОВА ЕКАТЕРИНА СЕРГЕЕВНА
Тамбовский государственный технический университет,
г. Тамбов, Российская Федерация, e-mail: elters@crimeinfo.jesby.tstu.ru

ЧЕРНЫШОВ ВЛАДИМИР НИКОЛАЕВИЧ
Тамбовский государственный технический университет,
г. Тамбов, Российская Федерация, e-mail: elters@crimeinfo.jesby.tstu.ru

В современном мире информатизация общества идет довольно быстрыми темпами, и неправомерный доступ к информационным ресурсам, хранящимся в памяти компьютера, стал реальной угрозой безопасности личности, общества и государства, их правомерным интересам, в том числе и в связи с развитием информационно-телекоммуникационных технологий и сети Интернет. Следовательно, для правильной квалификации преступлений в сфере компьютерной информации необходимо проанализировать состав деяний, предусмотренных ст. 28 УК РФ. В представленной статье проведен анализ уголовного законодательства, рассмотрены все элементы состава преступлений, предусмотренных ст. 272-274 УК РФ. Также проанализирована практика применения рассматриваемых норм уголовного законодательства. Вопросы наступления уголовной ответственности за неправомерный доступ к информационным ресурсам, хранящимся в памяти компьютера, стали наиболее обсуждаемыми в теории и практике современного права с момента изменения уголовного законодательства в части определения средств доступа. Это стало необходимым в процессе совершенствования компьютерной техники, программного обеспечения и повсеместного внедрения телекоммуникационных сетей, в том числе и сети Интернет. Целью написания статьи является анализ состава преступлений, предусмотренных гл. 28 УК РФ для установления возможности их практического применения в реалиях современного технического прогресса. А именно с развитием технологий, в том числе и компьютерной техники и программного обеспечения, а также популяризации сети Интернет, при том что информация является наиболее популярным продуктом как на международном рынке, так и во внутригосударственном секторе предоставления услуг.

***Ключевые слова*: компьютерная информация, вредоносные программы, компьютерные системы и технологии, сеть Интернет**

В современном мире центральное место в развитии общественных отношений занимают информационные системы и компьютерные технологии. С информатизацией общества все больше общественных отношений переходит в информационную сферу. В сложившейся ситуации актуальной проблемой в обеспечении безопасности личности, общества и государства является охрана компьютерной информации.

Несмотря на все реформы уголовного законодательства, проведенные в последние годы, уголовно-правовая охрана компьютерной информации остается актуальной, с дополнениями, обусловленными научно-техническим прогрессом. Проведем подробный анализ норм, которые предусматривают уголовное наказание за неправомерный доступ к охраняемой законом компьютерной информации.

Таким образом, уголовное наказание установлено за «…Неправомерный доступ к охраняемой законом компьютерной информации» [1] устанавливает статья 272 УК РФ. В диспозиции статьи содержится указание на обязательное наступление последствий «…если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование компьютерной информации» [1]. Новая формулировка диспозиции рассматриваемой статьи предполагает возможность неправомерного доступа к компьютерной информации не только при помощи ЭВМ, как указывала ранее действующая редакция статьи, а любого устройства, при помощи которого возможно осуществить доступ к информации. Отметим, что в действующем УК РФ дается определение компьютерной информации, как предмета преступного посягательства

«…сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [1]. Непосредственный объект рассматриваемого преступления, это общественные отношения в сфере обеспечения и организации правомерного доступа, создания, хранения, модификация, использования компьютерной информации, как создателем, так и иными пользователями информационного пространства. В ч. 3 ст. 272 УК РФ сформулировано определение дополнительного объекта указанного преступного посягательства, а именно, общественные отношения, в сфере обеспечения интересов служебной деятельности.

Объективная сторона состава рассматриваемого деяния состоит из: действия, состоящего в доступе к охраняемой законом компьютерной информации, без соответствующего разрешения, либо без полномочий на такой доступ и последствий в форме уничтожения, модификации, блокирования, копирования компьютерной информации, а также причинно-следственной связи между указанным действием и любым из предусмотренных последствий. Согласно информационному законодательству, «…доступ к информации – возможность получения информации и ее использования» [2]. При этом охраняемая законом информация – это такие сведения, для которых законом установлен специальный режим правовой защиты.

Таким образом, неправомерным доступом к компьютерной информации можно считать возможность получения и использования сведений, составляющих государственную, либо иную, охраняемую законом тайну, хранящуюся в памяти компьютера, лицом, не имеющим на это специального разрешения и/или не обладающего такими полномочиями.

Если подробно рассмотреть формулировку диспозиции ст. 272 УК РФ, то станет очевидным, что состав рассматриваемого преступного деяния имеет материальную конструкцию, поскольку преступность деяния неразрывно связана с наступлением одного из следующих последствий:

– уничтожения информации, то есть такие действия с информацией, последствиями которых будет непригодность всего ресурса или его части для использования вне зависимости от возможности восстановления до прежнего состояния;

– блокирования информации – это такое воздействие на информационный ресурс или технологию его представляющую, результатом которого будет невозможность осуществлять операции над информационным ресурсом при помощи компьютерной техники и технологий полностью или в требуемом режиме;

– модификация информации, а именно внесение изменений в содержание или параметры отображения компьютерной информации;

– копирования информации, то есть создания дубликата информационного ресурса как на другой тип носителя, так и на аналогичный, но обособленный от системы, а также считывания информации путем перехвата.

Считаем необходимым обратить внимание на тот факт, что в результате настроек компьютера или отдельной программы работы с информацией, в процессе работы автоматически создается резервная копия информации, и такое действие не может иметь уголовно-правовых последствий, поскольку оно осуществляется независимо от волеизъявления лица, осуществляющего даже неправомерный доступ к компьютерной информации и не охватывается его умыслом, а также не имеет причинно-следственной связи с фактом неправомерного доступа к компьютерной информации.

Таким образом, при установлении причинно-следственной связи между неправомерным доступом и наступлением общественно-опасных последствий необходимо брать во внимание тот факт, что при работе с компьютерной техникой есть вероятность уничтожения, блокирования и модификации, хранящейся в ней или обрабатываемой ей информации в результате системных неисправностей или ошибок при функционировании операционной системы или иного программного обеспечения. В рассмотренных случаях субъект, совершивший неправомерный доступ к компьютерной информации, не подлежит ответственности по данной статье, поскольку отсутствует причинно-следственная связь между неправомерным действием субъекта и наступившими вредными последствиями.

Наряду с общим субъектом, ч. 3 ст. 272 УК РФ предусматривает возможность совершения преступного деяния специальным субъектом, который совершил преступление рассматриваемого вида с использованием своего служебного положения, то есть с использованием возможности доступа к компьютерной информации, которая входит в полномочия лица, подтвержденные трудовым соглашением или договором, либо посредством влияния на подчиненных, которые имеют доступ к указанным информационным ресурсам.

Уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ предусматривает ст. 273 УК РФ, в диспозиции которой указано, что ответственность установлена «…за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копи-

рования компьютерной информации или нейтрализации средств защиты компьютерной информации» [1]. Объектом рассматриваемого преступления выступают общественные отношения, действующие в сфере обеспечения безопасности компьютерной информации от вредоносных программных средств. Объективная сторона деяния может быть представлена несколькими альтернативными действиями:

– создание программных средств, причем для определенных целей, а именно для осуществления несанкционированного уничтожения, блокирования, модифицирования, а также для создания дубликата информационного ресурса, хранящегося в памяти компьютера или нейтрализации средств технической защиты, к которым, на наш взгляд, можно отнести и технические средства защиты авторских прав;

– распространение указанных программных средств, программных платформ и технологий или электронно-цифровых носителей информации с указанными технологиями;

– использование программ рассматриваемого вида.

Рассмотрим виды деятельности, указанные в диспозиции. Так, создание программ, разработанных с целью несанкционированного, то есть непредусмотренного законом для определенной категории лиц, доступа, равно как и уничтожения, блокирования, модифицирования, копирования информационных ресурсов, хранящихся в памяти компьютера. А также выведение из строя технических средств защиты информационных ресурсов представляет собой деятельность, направленную на разработку программного кода, подготовку программы к работе.

Под распространением программ рассматриваемого вида понимается предоставление доступа к ним любому лицу каждым из имеющихся возможностей, например, продажу или бесплатное ознакомление посредством электронной почты или социальных сетей. Таким образом, это любые действия по предоставлению доступа к программе, в том числе и посредством удаленного доступа. Деятельность по использованию программ – это работа с ней в той области, для функционирования в которой она была разработана, либо проведение с ней других, сходных действий по осуществлению в отношении ее гражданско-правовых сделок, независимо от формы предоставления программы. Под использованием вредоносных программных средств, платформ и технологий обычно рассматривается их применение (любым лицом), посредством которого проявляются их свойства, а именно вредоносная направленность деятельности. Конструкция состава рассматриваемого деяния формальная, то есть преступление будет считаться оконченным с момента разработки программного кода, применения по назначению или передачи третьим лицам указанных выше программных средств. Или информационных продуктов, которые своим дальнейшим функционированием предусматривают возможность наступления последствий, предусмотренных уголовным законом вне зависимости от того, был ли в результате причинен реальных вред. Если говорить о субъективной стороне рассматриваемого состава, то в данном случае виновный должен осознавать, что использование разработанного или используемого им программного средства, платформы или технологии приведет к общественно опасным последствиям, предусмотренным уголовным законом.

Отметим, что ст. 273 УК РФ устанавливает уголовное наказание за противоречащие закону действия с компьютерными программами, платформами и технологиями независимо от формы их представления, это может быть как электронный, так и бумажный носитель. В связи с этим наличие рукописных исходных алгоритмов вредоносных компьютерных программ также будет считаться основанием для привлечения лица к уголовной ответственности по ст. 273 УК РФ. Однако использование вредоносной компьютерной программы для личных нужд (например, для уничтожения собственной компьютерной информации) ненаказуемо. Однако, когда работа вредоносной программы явилось базой для совершения другого преступного деяния, то такое деяние должно быть квалифицировано по совокупности преступлений вне зависимости от степени тяжести другого преступления.

Обратим внимание, что диспозиция ч. 1 ст. 273 УК РФ ранее была изложена следующим образом: «создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами». Однако понятие ЭВМ слишком узкое и современные технологии ушли далеко вперед, сейчас необходимо охватить и мобильные устройства. Учитывая тот факт, что использование программ для ЭВМ сейчас остается актуальным в некоторых областях деятельности, в действующем законодательстве дано их определение, как «…программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные ото-

бражения» [3]. В связи с этим в УК РФ действующей редакции диспозиция ч. 1 ст. 273 УК РФ предусматривает ответственность за «…создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации» [1]. Такая формулировка, на наш взгляд, является более практически значимой, поскольку охватывает все компьютерные программы и компьютерную информацию, независимо от вида устройств, их использующих. Также, уголовное законодательство РФ дает определение вредоносным компьютерным программам, в то время как специальное законодательство определяет средства защиты информации, к которым относятся «...технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации» [4].

Уголовное наказание за преступные посягательства в сфере соблюдения правил эксплуатации программных средств хранения, обработки данных и распространения информационных ресурсов, хранящихся в памяти компьютера и информационно-телекоммуникационных сетях, в том числе и в сети Интернет установлена ст. 274 УК РФ. Диспозиция ч. 1 ст. 274 УК РФ ранее предусматривала уголовную ответственность за «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред». Однако, в действующей редакции уголовного закона, законодатель изменил формулировку диспозиции, также заменив узкое понятие ЭВМ на более расширенное «средства хранения и обработки компьютерной информации», что, на наш взгляд, также является стремлением обеспечить безопасность компьютерной информации в условиях быстрого развития сегмента компьютерных технологий и количественного роста пользователей информационно-телекоммуникационных сетей, в том числе и сети Интернет. Таким образом, диспозиция ст. 274 представлена в такой трактовке: «…Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации» [1]. Непосредственным объектом рассматриваемых преступных посягательств являются общественные отношения, складывающиеся в сфере обеспечения безопасности оборота и хранения компьютерной информации-информационных ресурсов. Как дополнительный объект рассматриваемая норма устанавливает общественные отношения, обеспечивающие безопасность материально-ценностным объектам общества и государства. Предметом рассматриваемого преступного деяния выступают программные и технические средства сбора, хранения и обработки охраняемых информационных ресурсов, хранящихся в памяти компьютерной техники и информационно-телекоммуникационные сети, в том числе и сети Интернет. Рассматриваемая уголовно-правовая норма имеет бланкетный характер. Организация деятельности сотрудников по работе со средствами хранения информационных ресурсов, обработки или распространения охраняемых информационных ресурсов, хранящихся в памяти компьютера, информационно-телекоммуникационными сетями, в том числе и сетью Интернет в каждой отдельной организации или подразделении устанавливают конкретные локальные инструкции и правила.

То есть, общих правил эксплуатации, распространяющихся на неограниченный круг пользователей телекоммуникационных сетей, в том числе и сети Интернет, не существует на данный момент. Объективная сторона представлена действиями: «…нарушением правил хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если такое нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб» [1]. При этом, любые нарушения и наступившие общественно опасные последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации должны быть взаимосвязаны между собой причинно-следственной связью. И необходимо доказать, что наступившие общественно-опасные последствия есть результат нарушения правил эксплуатации, а не системной ошибки или действиями, предусмотренными объективной стороной ст. 272 и 273 УК РФ. Регламент, о соблюдении которого говорится в ст. 274 УК РФ, должен быть соблюден в целях обеспечения безопасности информационных ресурсов, хранящихся в памяти компьютера.

Обратим внимание, что ранее действующая редакция статьи в своем применении вызывала сложности. Это касалось установления субъекта преступного деяния, которым могло быть только спе-

циальное лицо, обязанное в силу занимаемой должности реализовывать полномочие по соблюдению установленных правила эксплуатации ЭВМ, системы ЭВМ или их сети. Если же рассматривать диспозицию ст. 274 в действующей редакции, то при квалификации возникает вопрос в области обеспечения безопасности доступа к телекоммуникационным сетям, определение которых можно сформулировать следующим образом «…технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» [2]. Указанной дефиницией можно определить любую «…компьютерную или глобальную, трансграничную сеть, а также локальные сети, создаваемые по территориальному принципу» [5]. Следовательно, субъект преступления будет общий, а не специальный, как было в ранее действующем законодательстве.

Таким образом, сложность компьютерных технологий и телекоммуникационных сетей, а также проблемы квалификации, связанные, например, с установлением места преступления, как и трудность сбора доказательственной информации о совершенных действиях приводит к тому, что уголовные дела по преступлениям, предусмотренным ст. 272-274 УК, либо не возбуждаются, либо не доходят до стадии судебного разбирательства. Однако, предусмотренные составы охватывают значительно больше видов совершения неправомерных посягательств на компьютерную информацию. Тем более что правоприменитель зачастую использует рассматриваемые нормы для квалификации деяний по совокупности, например ст. 146 и ст. 273 УК РФ или ст. 146 и ст. 272 УК РФ [6].

Таблица 1

Статистика правоприменения ст. 146 и 272 УК РФ

ч. 2 ст. 146, ч. 1 ст. 272 УК РФ	Прекращено	Обвинительный приговор	Всего
2017	114	4	118
2016	127	2	129
2015	87	0	87
2014	63	0	63

Таблица 2

Статистика правоприменения по ст. 146 и 273 УК РФ

ч. 2 ст. 146, ч. 1 ст. 273 УК РФ	Прекращено	Обвинительный приговор	всего
2017	154	2	156
2016	142	3	145
2015	196	3	199
2014	273	5	278

Также мы считаем, что в связи с происходящими процессами глобализации и информатизации и все большее распространение сети Интернет, как их последствие, необходимо ввести в УК РФ составы, предусматривающие ответственность за распространение информации, а также за неправомерный доступ к компьютерной информации посредством сети Интернет.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 17.04.2017) // Собрание законодательства РФ. 2017. № 25. Ст. 2954.

2. Об информации, информационных технологиях и о защите информации: федер. закон № 149-ФЗ от 27 июля 2006 г. // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (Ч. I) ст. 3448.

3. Часть четвертая Гражданского кодекса Российской Федерации от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства Российской Федерации от 25 декабря 2006 г. № 52 (Ч. I) ст. 5496.

4. О государственной тайне Закон РФ от 21 июля 1993 г. № 5485-I // Российская газета от 21 сент. 1993 г. № 182.

5. Искевич И. С., Кочеткова М. Н., Попов А. М. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект // ППД. 2016. № 4. С. 54-58

6. Росправосудие. URL: https://rospravosudie.com/

References

1. Ugolovnyj kodeks Rossijskoj Federatsii ot 13.06.1996 g. № 63-FZ (red. ot 17.04.2017) [Criminal Code of the Russian Federation on 13.06.1996 № 63-FL

(edition on 17.04.2017)] // Sobraniye zakonodatel'stva RF. 2017. № 25. St. 2954.

2. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: Feder. zakon № 149-FZ ot 27 iyulya 2006 g. [About information, information technologies and information security: Federal law № 149-FL on July 27, 2006] // Sobraniye zakonodatel'stva Rossijskoj Federatsii ot 31 iyulya 2006 g. № 31 (chast' I) st. 3448.

3. Chast' chetvertaya Grazhdanskogo kodeksa Rossijskoj Federatsii ot 18 dekabrya 2006 g. № 230-FZ [Fourth part of the Civil code of the Russian Federation on December 18, 2006 № 230-FL] // Sobraniye zakonodatel'stva Rossijskoj Federatsii ot 25 dekabrya 2006 g. № 52 (chast' I) st. 5496

4. O gosudarstvennoj tajne Zakon RF ot 21 iyulya 1993 g. № 5485-I [About the state secret Act of the Russian Federation on July 21, 1993 № 5485-I] // Rossijskaya gazeta ot 21 sentyabrya 1993 g. № 182.

5. Iskevich I. S., Kochetkova M. N., Popov A. M. Aktual'nye problemy opredeleniya yurisdiktsii pri rassledovanii prestuplenij v informatsionnom prostranstve: mezhdunarodno-pravovoj aspect [Current problems of definition of jurisdiction at investigation of crimes in information space: international legal aspect] // PPD. 2016. № 4. S. 54-58

6. Rospravosudiye. [Rospravosudiye]. URL: https://-rospra-vosudie.com/

* * *

PROBLEMS OF CRIMINAL LEGAL PROTECTION OF COMPUTER INFORMATION

LOSKUTOVA EKATERINA SERGEEVNA
Tambov State Technical University,
Tambov, the Russian Federation, e-mail: elters@crimeinfo.jesby.tstu.ru

CHERNYSHOV VLADIMIR NIKOLAEVICH
Tambov State Technical University,
Tambov, the Russian Federation, e-mail: elters@crimeinfo.jesby.tstu.ru

In the modern world informational support of society goes enough in high gear and illegal access to the information resources stored in memory of the computer became real threat to security of the personality, society and state, to their lawful interests including in connection with development of information and telecommunication technologies and the Internet. Therefore, for the correct qualification of crimes in the sphere of computer information it is necessary to analyze structure of the acts provided by Art. 28 of the Criminal Code of the Russian Federation. In the submitted article authors carried out the analysis of the criminal legislation, considered all elements of corpus delicti, provided by Art. 272-274 of the Criminal Code of the Russian Federation and also analyzed practice of use of the considered standards of the criminal legislation. Questions of occurrence of a criminal responsibility for illegal access to the information resources stored in memory of the computer became the most discussed in the theory and practice of the modern right from the moment of change of the criminal legislation regarding definition of accessors. It became necessary in the course of improvement of the computer equipment, the software and universal introduction of telecommunication networks including the Internet. The purpose of writing of article is the analysis of corpus delicti, the provided by chapter 28 of Criminal Code of the Russian Federation for establishment of a possibility of their practical application in realities of modern technical progress. Exactly with development of technologies, including computer equipment and software and also promoting of the Internet, thus that information is the most popular product both at the international market, and in the interstate sector of rendering of services.

Key words: computer information, malicious applications, computer systems and technologies, Internet

Об авторах:

Лоскутова Екатерина Сергеевна, аспирант кафедры уголовного права и прикладной информатики в юриспруденции Тамбовского государственного технического университета, г. Тамбов

Чернышов Владимир Николаевич, доктор технических наук, профессор, зав. кафедрой уголовного права и прикладной информатики в юриспруденции Тамбовского государственного технического университета, г. Тамбов

About the authors:

Loskutova Ekaterina Sergeevna, Post-graduate Student of the Penal Law and Applied Informatics in Law Department, Tambov State Technical University, Tambov

Chernyshov Vladimir Nikolaevich, Doctor of Engineering, Professor, Head of the Penal Law and Applied Informatics in Law Department, Tambov State Technical University, Tambov