СТАТЬИ

УГОЛОВНОЕ ПРАВО И ПРОЦЕСС

УДК 343.2/.7

В.В. Воробьёв

V. Vorobyov

ВОПРОСЫ ПРИМЕНЕНИЯ СОСТАВА ст.274 УК РФ

QUESTIONS OF APPLICATION COMPOSITION ARTICLE 274 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

В статье проанализированы объективная и субъективная стороны нарушения 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. Рассмотрены причинно-следственная связь и её разновидности в этом преступлении, особенности вины в различных вариантах совершения этого преступления.

In article the objective and subjective parties of violation of the rules of operation of means of storage, processing or transfer of the protected computer information or information and telecommunication networks and the terminal equipment, and also rules of access to information and telecommunication networks are analysed. It is considered cause and effect and its versions in this crime, and also feature of fault in various options of commission of this crime.

Ключевые слова: преступления в сфере компьютерной информации, компьютерные преступления, нарушение правил эксплуатации компьютера, компьютерная информация, уничтожение, блокирование, модификация, копирование компьютерной информации, состав преступления, вина, тяжкие последствия.

Keywords: crimes in the sphere of computer information, computer crimes, violation of the rules of operation of the computer, computer information, corpus delicti, wine, heavy consequences, destruction, blocking, modification, copying of computer information.

В современном обществе создаётся разветвлённая система общественных отношений, «ядром» которых является информация, циркулирующая, хранящаяся и обрабатываемая как в отдельных компьютерах, так и телекоммуникационных сетях. В Доктрине информационной безопасности РФ говорится о том, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации [1].

В связи с тем, что компьютер представляет собой программно-технический комплекс, его эксплуатация должна быть регламентирована специальными правилами, устанавливающими порядок:

1) доступа к компьютерной информации, её обработки и хранения;

2) работы с программными продуктами;

3) эксплуатации средств хранения, обработки и передачи компьютерной информации.

Так как компьютерные технологии используются в различных сферах деятельности человека, то указанные правила должны быть как унифицированными, так и учитывающими особенности этих сфер.

Согласно данным судебной статистики, в Российской Федерации число лиц, осуждённых за преступления в сфере компьютерной информации, до 2010 г. росло, а начиная с 2011 г. стало уменьшаться. Так, в 2003 г. за преступления, предусмотренные ст.272–274 УК РФ, число осуждённых составило 152 человека, в 2004 г. – 137, в 2005 г. – 203, в 2006 г. – 191, в 2007 г. – 241, в 2008 г. – 257, в 2009 г. – 347, в 2010 г. – 321, в 2011 г. – 258, в 2012 г. – 280, в 2013 г. – 268,

в 2014 г. – 218 и за I полугодие 2015 г. – 109 человек (см. *рис. 1*) [2].

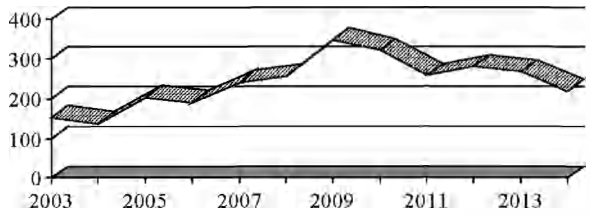

Рис. 1. Количество осуждённых за преступления, предусмотренные ст.272–274 УК РФ

В 2014 г., по данным МВД, в России зарегистрировано 11 тыс. компьютерных преступлений. Эксперты говорят о том, что вести учёт компьютерных преступлений непросто, поэтому общее их число во много раз превышает данные из статистики МВД. По мнению гендиректора компании *Digital Security* (анализ защищённости компьютерных систем), реальное количество киберпреступлений в России минимум в 5 раз больше. Например, как сообщает руководитель департамента расследований инцидентов *Group-IB* (расследование киберпреступлений), только количество взломов почты исчисляется миллионами. Попытки хищения денег происходят намного реже, чем взломы почты, но не менее 100 тыс. в год, и часть из них блокируется банками [3].

Такое расхождение в официальной статистике связано с тем, что учитываются только те преступления, по которым поданы заявления от потерпевших. Последние крайне редко пишут заявления в случае *DDoS*-атак, кражи логинов и паролей, а также установки вредоносных программ. Данные судебной статистики также сильно отличаются от статистики МВД. Так, только за первое полугодие 2015 г. от уголовной ответственности за преступления в сфере компьютерной информации освобождено 68 человек, тогда как привлечено 109 [4]. Основаниями для освобождения от уголовной ответственности за эти преступления чаще всего выступают деятельное раскаяние и примирение с потерпевшим, реже – истечение сроков давности. Кроме того, как правило, привлекаемое к уголовной ответственности лицо до задержания успевает совершить несколько компьютерных преступлений, которые регистрируются отдельно. Таким образом, расхождение в статистических данных вызвано рядом объективных и субъективных причин.

Как видно из *таблицы*, удельный вес преступлений, предусмотренных ст.274 УК РФ, в общей группе компьютерных очень мал. В причинах такого положения необходимо разбираться, т.к. подобная картина наблюдается на протяжении 19 лет действия современного УК РФ. Такие составы

Таблица

Данные о компьютерных преступлениях по составам [5]

Статья УК РФ	2010 г.	2011 г.	2012 г.	2013 г.
ст.272	6 132	2 005	1 930	1 799
ст.273	1 010	693	889	764
ст.274	0	0	1	0

в уголовном праве принято называть «мёртвыми». Невысокая активность по исследованию этой проблемы наблюдается и в научной среде.

Для того, чтобы понять причины такой «плохой» статистики, в первую очередь необходимо проанализировать состав ст.274 УК РФ.

Объективная сторона преступления, ответственность за которое предусмотрена ст.274 УК РФ, состоит в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей (далее – ИТС) и оконечного оборудования, а также правил доступа к ИТС, повлекшее за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб [6]. Данная редакция состава ст.274 УК РФ была введена в декабре 2011 г., до этого времени была иная редакция, звучавшая следующим образом: «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети... повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред» [7].

Нарушение правил эксплуатации может выражаться как в полном игнорировании, так и в ненадлежащем соблюдении правил. Нарушение может быть выражено в форме действия или бездействия (совершение запрещённых действий или невыполнение виновным действий, предписанных правилами). Термины «нарушение правил» и «несоблюдение правил» в контексте данной статьи следует рассматриваться как равнозначные (синонимы).

Статья 274 УК РФ не содержит конкретных требований и отсылает к правилам, определяющим порядок эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо ИТС и оконечного оборудования, а также правил доступа к ИТС.

Основной проблемой применения данной нормы является отсутствие какой-либо системы правил и инструкций в этой области, а также процедуры их принятия и доведения до исполнителей.

Очевидно, что правила должны устанавливаться специально уполномоченным лицом или органом и доводиться до исполнителей, на которых

возлагается ответственность за нарушение этих правил в соответствии со ст.274 УК РФ.

Можно выделить 2 вида правил эксплуатации, которыми должны руководствоваться в своей деятельности ответственные лица. Первый вид правил – инструкции, разработанные изготовителем компьютера, оконечного оборудования и иных устройств. Эти правила обязательны для соблюдения пользователем под угрозой, как правило, потери прав на гарантийное обслуживание. Второй вид – правила, установленные собственником или иным владельцем информационных ресурсов, информационных сетей, средств хранения, обработки или передачи информации, а также установленные субъектом, обеспечивающим доступ к ИТС.

Ответственность за нарушение второго вида правил может наступить только в случае, если они были приняты уполномоченным лицом (органом) с соблюдением порядка принятия и доведены до ответственного лица (например, под роспись).

Таким образом, к правилам, нарушение которых влечёт за собой уголовную ответственность по ст.274 УК РФ, следует относить требования как к эксплуатации аппаратной части, так и к работе с программами, базами данных, иной охраняемой информацией, а в некоторых случаях – организационного характера.

Согласно методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, правила, о которых идёт речь в ст.274 УК РФ, должны быть направлены только на обеспечение информационной безопасности. В ст.274 УК РФ говорится о нарушении правил, которое может повлечь за собой уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, т.е. такие же последствия, что и при неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных программ для ЭВМ.

Правила доступа и эксплуатации, относящиеся к обработке информации, содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах [8].

В связи с тем, что данный состав по конструкции является материальным, помимо деяния (нарушение правил эксплуатации) особое внимание следует обратить на такой элемент объективной стороны преступления, как преступные последствия, наступление которых для данного преступления обязательно.

Для окончания этого преступления необходимо уничтожение, блокирование, модификация или копирование такого количества информации или такой информации, утрата (или распространение) которой причинила бы законному пользователю или владельцу компьютерной информации крупный ущерб.

Диспозиция ст.274 УК РФ предусматривает причинение крупного ущерба. Согласно примечанию 2 к ст.272 УК РФ, крупным ущербом в статьях гл.28 УК РФ признаётся ущерб, сумма которого превышает 1 млн рублей.

В ч.2 рассматриваемой статьи Уголовного кодекса установлена ответственность за нарушение правил, причинившее тяжкие последствия или создавшее угрозу их наступления.

Перечня тяжких последствий уголовный закон не содержит. Отличие крупного ущерба от тяжких последствий зависит от величины ущерба, которая, в свою очередь, во многом зависит от важности информации. В зависимости от этого можно выделить следующие её виды:

- *жизненно важная информация* – незаменимая информация, наличие которой обеспечивает функционирование компьютера, системы ЭВМ или их сети и, как следствие, функционирование физического либо юридического лица;

- *важная информация* – информация, которая может быть заменена или восстановлена, но этот процесс связан с большими затратами и серьёзными трудностями;

- *полезная информация* – информация, которая приносит очевидную пользу и которую довольно трудно восстановить, хотя юридическое или физическое лицо может нормально функционировать и без неё [9].

К тяжким последствиям можно причислить такие, как:

- гибель человека или причинение тяжкого вреда здоровью хотя бы одного человека;

- крупные аварии (в том числе приводящие к экологическим и другим катастрофам);

- дезорганизация работы предприятия или организации;

- осложнение дипломатических отношений;

- возникновение вооружённого конфликта либо реальная угроза его возникновения;

- причинение имущественного ущерба в сумме, превышающей 10 млн руб. (в том числе в виде упущенной выгоды);

- утрата уникальной либо особо ценной информации.

Приведённый перечень тяжких последствий не является исчерпывающим, поэтому судом может быть признано тяжким и иное общественно опасное последствие.

Нарушение правил эксплуатации будет оконченным преступлением только в случае наступления определённых неблагоприятных последствий

в виде уничтожения, блокирования, модификации или копирования охраняемой компьютерной информации. Но ответственность по ст.274 наступает лишь при наличии крупного ущерба или при наступлении тяжких последствий. Таким образом, именно в результате уничтожения, блокирования, модификации или копирования охраняемой компьютерной информации причиняется крупный ущерб или наступают тяжкие последствия.

Представляется, что причинно-следственная связь в данной норме развивается в 2 этапа. Схематически это можно представить следующим образом (см. *рис. 2*).

Как показано на схеме, первый этап развития причинной связи находится между нарушением правил эксплуатации и первичными неблагоприятными последствиями, такими как уничтожение, блокирование, модификация или копирование информации. Второй этап развития причинной связи при нарушении правил эксплуатации развивается, когда в результате наступления первичных вредных последствий возникают вторичные – в виде крупного ущерба или тяжких последствий.

Таким образом, из содержания диспозиции ст.274 УК РФ видно, что уничтожение, блокирование, модификация или копирование компьютерной информации является необходимым условием для причинения крупного ущерба. Во многих случаях первичные и вторичные последствия могут наступать одновременно или почти одновременно, хотя в некоторых случаях они наступают через длительный промежуток времени. Например, уничтожение дорогостоящей базы данных бывшим сотрудником организации. Здесь крупный ущерб причиняется одновременно с уничтожением информации. А в результате блокирования антивирусной программы, производящей периодическое антивирусное тестирование компьютера, через определённое время происходит заражение вредоносной программой, что впоследствии приводит к уничтожению важной информации.

Подытоживая вышеизложенное, следует отметить, что преступление, ответственность за которое предусмотрена ст.274 УК РФ, будет окончено только при причинении крупного ущерба или наступления тяжких последствий либо возникновения реальной угрозы их наступления, независимо от того, одновременно или в разное время наступили первичные и вторичные последствия. Другими словами, когда нарушаются правила эксплуатации, в результате чего уничтожается, блокируется, модифицируется или копируется информация, но крупный ущерб ещё не причинён, говорить об оконченном преступлении преждевременно. В зависимости от причин недоведения преступления до конца и последующего поведения виновного квалифицировать деяние следует как покушение на преступление или как добровольный отказ от доведения преступления до конца.

Однако всё изложенное выше является результатом доктринального толкования уголовно-правовой нормы. Полагаем, что для более эффективной борьбы с этим видом компьютерных преступлений необходимо осуществление судебного толкования этой нормы в виде разъяснений, даваемых Пленумом Верховного Суда РФ.

Психическое отношение к деянию, ответственность за которое предусмотрена ст.274 УК РФ, выражается как в форме умысла, так и в форме неосторожности. При нарушении правил лицо осознаёт общественную опасность этого деяния, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления либо сознательно их допускает

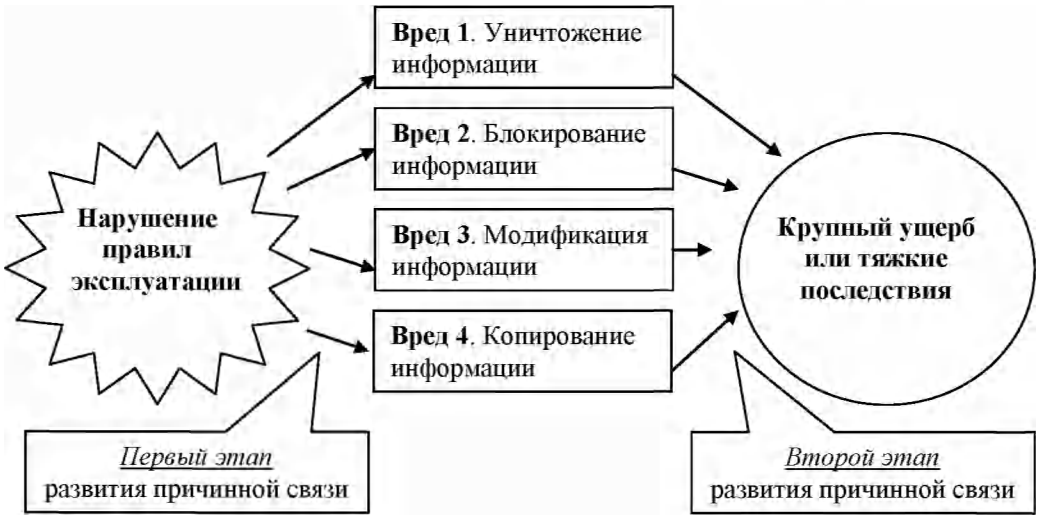

Рис. 2. Развитие причинной связи при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ)

или относится к ним безразлично. Иными словами, это преступление может быть совершено как с прямым, так и с косвенным умыслом. А равно, когда лицо предвидит возможность наступления последствий, но самонадеянно рассчитывает на их предотвращение или когда лицо не предвидит возможности наступления последствий, но при необходимой внимательности и предусмотрительности должно было и могло их предвидеть, т.е. совершение преступления по легкомыслию или небрежности.

Необходимо провести разделение по видам умысла и неосторожности по отношению к первичным и вторичным последствиям (см. *рис. 3*).

Двойственность вины в данном преступлении может состоять и в том, что по отношению к деянию и первичным последствиям имеется умышленная форма вины, а по отношению к вторичным – неосторожность. Первым неблагоприятным последствием является факт умышленного уничтожения, блокирования, модификации или копирования охраняемой компьютерной информации (первичные последствия). Однако наступление только этого последствия будет свидетельствовать о неоконченности уголовно наказуемого деяния. Оконченным оно будет только при наступлении вторичного общественно опасного последствия.

Справедливым, по нашему мнению, является суждение П.Н. Панченко, полагающего, что в зависимости от того, как соотносятся первичные и вторичные последствия, различают разные комбинации умысла и неосторожности. В одном случае последствия могут как бы вытекать друг из друга (умышленное причинение тяжкого вреда здоровью, повлёкшее по неосторожности смерть потерпевшего). В другом – последствия параллельно наступают в результате совершения одного деяния (изнасилование, повлёкшее по неосторожности тяжкий вред здоровью, например, психическое заболевание) [10].

При нарушении правил эксплуатации, повлёкшем по неосторожности тяжкий вред, соотношение первичных и вторичных (дальних) последствий может заключаться как в последовательном их наступлении, так и в параллельном.

Примером первого варианта двух форм вины может послужить умышленное нарушение правил эксплуатации компьютера, повлёкшее по неосторожности остановку предприятия. Последовательность наступления последствий в этом преступлении представлена на *рис. 4*.

Последовательность наступления последствий наглядно демонстрируется при умышленном нарушении правил эксплуатации компьютера, повлекшем за собой модификацию компьютерной информации, к которой виновное лицо относилось также умышленно (первичное последствие 1), модификация компьютерной информации влечёт остановку конвейера завода (первичное последствие 2), а остановка конвейера является причиной остановки предприятия (вторичное последствие).

В качестве примера второго варианта двух форм вины можно представить умышленное нарушение правил эксплуатации ЭВМ, повлекшее по неосторожности уничтожение особо ценной информации.

В предложенной ситуации умышленное нарушение правил эксплуатации влечёт за собой умышленное уничтожение всей компьютерной информации, однако уничтожение особо ценной информации, являющейся частью всей компьютерной

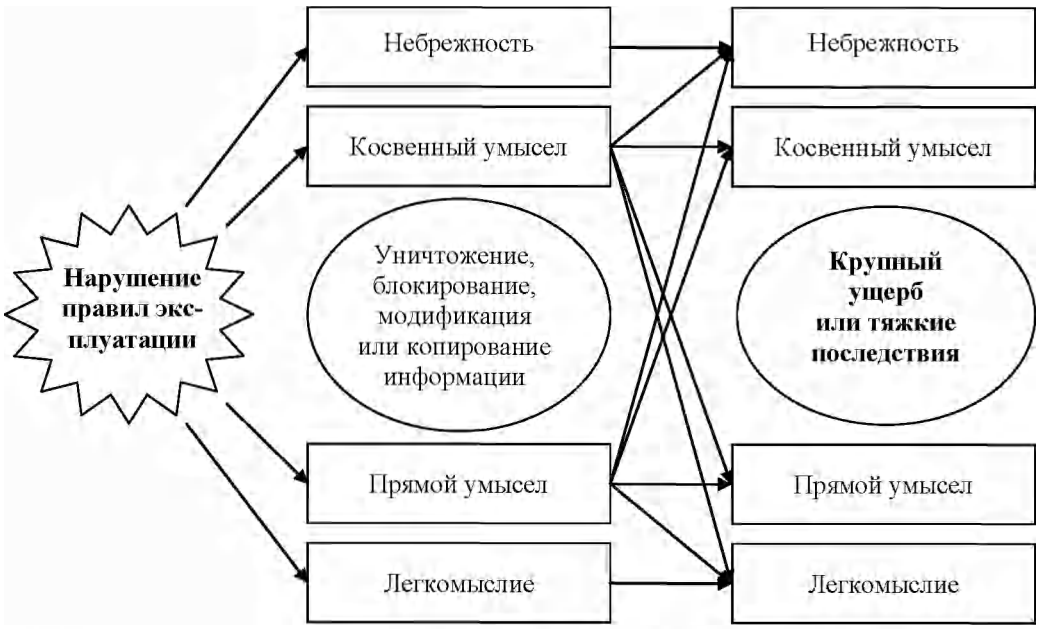

Рис. 3. Виды умысла и неосторожности по отношению к первичным и вторичным последствиям при нарушении правил эксплуатации

Рис. 4. Последовательное наступление последствий в преступлении с двумя формами вины (на конкретном примере)

информации (например, в научно-исследовательском институте), не охватывается умыслом виновного, а уничтожается им по неосторожности. При таком причинении тяжкого вреда первичные и вторичные последствия наступают параллельно (одновременно) (см. *рис. 5*).

Правила эксплуатации нарушаются умышленно, причём умысел может быть как прямым, так и косвенным. Психическое отношение к вторичным последствиям (тяжкий вред) характеризуется виной в форме неосторожности, которая может выражаться как в легкомыслии, так и в небрежности.

Факультативные признаки субъективной стороны состава преступления (мотив, цель, особое эмоциональное состояние) на квалификацию анализируемого вида компьютерных преступлений влияния не оказывают и могут быть учтены судом при назначении наказания.

Субъект данного преступления является специальным. Наличие специального субъекта в анализируемом составе преступления вызвано объективными причинами. Привлекать к ответственности за нарушение правил эксплуатации можно только в том случае, если лицо было ответственно за соблюдение этих правил.

Рис. 5. Параллельное (одновременное) наступление последствий в преступлении с двумя формами вины (на конкретном примере)

* * *

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 № Пр-1895) // Рос. газета. – 2000. – 28 сент.

2. Основные статистические показатели состояния судимости в России за 2003–2007 годы и 2008–2014 годы. – URL: http://www.cdep.ru/index.php?id=79&item=2074; Сводные статистические сведения о состоянии судимости в России за первое полугодие 2015 года. – URL: http://www.cdep.ru/index.php?id=79&item=3212

3. МВД зарегистрировало около 11 000 киберпреступлений в 2014 году. – URL: http://www.vedomosti.ru/technology/articles/2015/02/06/kiberprestupniki-v-spiskah-ne-znachatsya

4. Сводные статистические сведения о состоянии судимости в России за первое полугодие 2015 года…

5. *Евдокимов К.Н.* Политические факторы компьютерной преступности в России. – URL: http://отрасли-права.рф/article/8285

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.12.2015) // Собр. законодательства РФ. – 1996. – № 25. – Ст.2954.

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.11.2011) // Собр. законодательства РФ. – 1996. – № 25. – Ст.2954.

8. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. – URL: http://genproc.gov.ru/documents/nauka/execution/document-104550

9. Научно-практический комментарий к Уголовному кодексу Российской Федерации: в 2 т. / под ред. П.Н. Панченко. – Н. Новгород, 1996. – Т.2. – С.242.

10. *Панченко П.Н.* Уголовное право России. Общая часть: учеб. пособие. – Н. Новгород, 1995. – С.178.