УДК 343.23

С.А. Стяжкина

УГОЛОВНО-ПРАВОВЫЕ ОСОБЕННОСТИ КВАЛИФИКАЦИИ НАРУШЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (статья 274 УК РФ)

В статье рассматриваются вопросы квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Раскрыты объективные и субъективные признаки данного состава преступления. Особое внимание уделено проблеме определения предмета нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Рассмотрен вопрос объективной стороны состава ст. 274 УК РФ, в частности, определены правила средств хранения, обработки и передачи компьютерной информации, в качестве которых следует рассматривать правила, как содержащиеся в нормативно-правовых актах, так и в локальных документах организаций, предприятий, учреждений. Проанализированы признаки субъективной стороны нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, которые вызывают немало споров в научной литературе. Также рассмотрены разные точки зрения относительно субъекта преступления, которым может быть физическое вменяемое лицо, достигшее 16-летнего возраста.

Ключевые слова: уголовное право, квалификация преступлений, уголовная ответственность, компьютерная информация, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации, преступления в сфере компьютерной информации.

DOI: 10.35634/2412-9593-2021-31-3-489-496

Проблемы обеспечения уголовно-правовой защиты компьютерной информации на сегодняшний день выходят на одно из лидирующих мест в сфере информационной безопасности. Переходя на новый формат создания, использования, хранения, передачи информации, необходимо обеспечить безопасность, сохранность информации, представленной в виде электрических сигналов. Широкое применение компьютерной информации во всех сферах жизнедеятельности человека требует адекватной реакции как со стороны общества, так и государства по вопросам обеспечения ее безопасного использования и хранения. Как показывает практика, в последние годы увеличился рост числа преступлений в сфере компьютерной информации, но гораздо большими темпами растет количество преступлений, которые совершаются с использованием и применением различного рода информационно-телекоммуникационных технологий. По официальным данным, содержащимся на сайте МВД РФ, в 2021 г. было зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Как отмечается на сайте, это почти на 70 % больше, чем за аналогичный период 2018 г. Более половины таких преступлений совершается с использованием сети «Интернет», а более трети – с использованием средств мобильной связи. В 2020 г. удельный вес преступлений, которые совершены с использованием информационно-телекоммуникационных сетей, а также в сфере компьютерной информации в общей структуре преступности составил 510 400, что составляет примерно 25% от общего числа зарегистрированных преступлений. Каждое четвертое преступление связано с компьютерной информацией или средствами ее обработки, хранения или передачи. По данным Генеральной Прокуратуры РФ, за последние пять лет количество преступлений, связанных с компьютерной информацией увеличилось более чем в 11 раз, а удельный вес в общей структуре преступности вырос с 2 % до 25 %. Большая часть киберпреступлений совершается с использованием сети «Интернет» (почти 58 % от всех киберпреступлений) или при помощи средств мобильной связи (42 %). Также среди способов совершения компьютерных преступлений фигурируют расчетные (пластиковые) карты, компьютерная техника, программные средства.

С расширением сферы применения компьютерных технологий и компьютерной информации неизбежен рост числа преступлений с использованием этих технологий. Следует отметить, что преступность в целом приобретает «информационный» характер» и все больше, и больше использует информационные ресурсы, находящиеся в цифровом пространстве. Кроме того, все чаще именно ин-

формация становится предметом и объектом посягательства. С массовым переходом населения на использование безналичных денежных средств, различных виртуальных кошельков, криптовалют и т.д. естественным образом увеличилось и количество преступлений, посягающих на данные ресурсы. Для совершения многих преступлений на сегодняшний день требуется доступ к компьютерной информации, ее незаконное использование.

О росте количества компьютерных преступлений свидетельствуют и данные официальной статистики. В сфере компьютерной информации в 2019 г. было зарегистрировано 2 883 преступления, что на 15,3 % больше, чем в предыдущем году. Но следует отметить, в 2019 г. осуждено по всем компьютерным преступлениям, содержащимся в гл. 28 УК РФ, всего 161 человек. Но еще больше преступлений остаются за рамками цифр официальной статистики, что свидетельствует о высокой латентности данного вида преступности.

Большинство из зарегистрированных преступлений, входящих в гл. 28 Уголовного кодекса РФ, составляет ст. 272 УК РФ, предусматривающая уголовную ответственность за неправомерный доступ к компьютерной информации. Удельный вес данного преступления среди киберпреступлений составляет 83,8 %. Второе место занимает состав преступления, содержащийся в ст. 273 УК РФ, в которой предусмотрена головная ответственность за создание, использование, и распространение вредоносных компьютерных программ, на которое приходится 15,4 % от всех компьютерных преступлений.

Обращаясь к ст. 274 УК РФ, предусматривающей ответственность за нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей, то их процент очень невелик, количество таких преступлений исчисляется единицами. Но проблема заключается не в том, что подобного рода деяния совершаются редко или совсем не совершаются, а в наличии сложностей, возникающих при их квалификации, при уголовно-правовой оценке содеянного. Много вопросов возникает при анализе и определении признаков объективной стороны ст. 274 УК РФ, а также при рассмотрении вопросов вины, характерной для нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также ее оценки.

Даже при определении объекта рассматриваемого преступления в литературе высказываются различные точки зрения. Одно из официальных определений содержится в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. В них указывается, что объектом преступления являются «общественные отношения, обеспечивающие безопасность в сфере компьютерной информации»[1]. Представляется, что данное определение не совсем точно отражает специфику рассматриваемого преступления.

Заслуживающим внимание является позиция К.Н.Евдокимова, который в качестве объекта преступления, предусмотренного ст. 274 УК РФ, рассматривает «охраняемые законом права и интересы пользователей и обладателей компьютерной информации в сфере безопасного создания, обработки, хранения, передачи, защиты компьютерной информации, а также безопасного функционирования компьютерных устройств, информационных систем, информационно-телекоммуникационных сетей и оконечного оборудования, автоматизированных систем управления, сетей электросвязи и иных средств создания, использования, распространения компьютерной информации»[2]. Но придерживаясь традиционного подхода к определению объекта преступления как общественного отношения, которое охраняется уголовным законом и которому причиняется вред, представляется, что интересы пользователей не могут быть объектом преступления.

Под объектом нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей следует понимать защищаемые уголовным законодательством общественные отношения, гарантирующие безопасную эксплуатацию средств хранения, обработки или передачи компьютерной информации, а также безопасное использование информационно-телекоммуникационных сетей и оконечного оборудования, и обществен-

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «Гарант».

[2] Евдокимов К.Н. Актуальные вопросы определения объекта преступного посягательства при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Ученые записки Крымского федерал. ун-та им. В.И. Вернадского. Юридические науки. 2018. Т. 4 (70), № 4. С. 188.

ные отношения, которые предусматривают порядок доступа к информационно-телекоммуникационным сетям.

Ряд авторов выделяют еще и дополнительный объект, в качестве которого называют общественные отношения, охраняемые Уголовным кодексом, обеспечивающие соблюдение и реализацию прав и законных интересов физических лиц, организаций, отношения, охраняющие собственность, а также интересы государственной, муниципальной и коммерческой службы, и даже отношения, обеспечивающие безопасность жизни, и здоровья человека[3]. Аналогичной позиции придерживаются и в Генеральной Прокуратуре Российской Федерации. В своих Рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации указывается, что дополнительный объект преступления, повлекшего причинение существенного вреда, − общественные отношения, обеспечивающие, в зависимости от характера последних, иные значимые социальные ценности (жизнь человека, здоровье многих людей, собственную безопасность и т.п.)[4]. Но в диспозиции ст.274 УК РФ нет указания на существенный вред как признак объективной стороны рассматриваемого состава. В ч.1 в качестве обязательного признака указан крупный ущерб, размер которого составляет 1 млн руб. Поэтому в качестве дополнительного объекта будут выступать только отношения, обеспечивающие охрану собственности. Соответственно, состав нарушения правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей является сложным составом с двумя объектами: основным и дополнительным.

Применительно к данному составу преступления имеет значение предмет преступления как факультативный признак объекта.

Предметом преступления в соответствии с диспозицией ст. 274 УК РФ выступают средства хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование. К средствам обработки, хранения и передачи компьютерной информации можно отнести большое количество различного рода предметов, начиная от ЭВМ, ПК, смартофонов, ноутбуков и заканчивая банкоматами, флешкартами и картами памяти. Фактически – это любые предметы, на которых может содержаться компьютерная информация, то есть «любые сведения, сообщения или данные, представленные в форме электрических сигналов»[5]. Таким образом, к таким средствам могут относиться и пластиковые карты со встроенными чипами и магнитными полосами, иммобилайзеры, датчики и т. д. Надо сказать, что эти средства получают все более широкую сферу применения как среди лиц, осуществляющих свои профессиональные функции, связанные с обеспечением безопасности компьютерной информации, так и среди обычных граждан, использующих данные предметы в повседневной жизни. Такое активное применение рассматриваемых средств и их совершенствование может привести в дальнейшем к проблемам квалификации рассматриваемого состава, связанных с широкой трактовкой вышеуказанных предметов.

Определение информационно-телекоммуникационных сетей есть в Федеральном законе 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», где сказано, что «информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»[6]. Подобного рода системы могут быть локальными и глобальными, к которой относится и Интернет. Интернет очень активно входит в жизнь людей и на сегодняшний день большая часть населения пользуется его услугами. По данным официальной статистики, удельный вес населения, использующего сеть Интернет, в общей численности населения Российской Федерации с 77,7 % в 2015 г. вырос до 88,9 в 2019 г., а удельный вес организаций, использующих сеть Интернет, в общем числе организаций вырос с 88,1 % в 2015 г. до 91,2 % в 2019 г.

Оконечное оборудование в соответствии с ФЗ от 7 июля 2003 «О связи» № 126-ФЗ – 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[7].

---

[3] Там же.

[4] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «Гарант».

[5] Уголовный Кодекс РФ // СПС «Гарант».

[6] ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Гарант»

[7] ФЗ от 07.07.2003 № 126-ФЗ «О связи» // СПС «Гарант».

Много вопросов как в теории, так и в правоприменительной практике вызывает проблема определения признаков объективной стороны нарушения правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей. Обращаясь к диспозиции ст. 274 УК РФ, можно выделить две формы деяния состава нарушения правил эксплуатации средств обработки, хранения или передачи компьютерной информации и информационно-телекоммуникационных сетей.

К первой форме будет относиться нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования.

Второй формой будет выступать нарушение правил доступа к информационно-телекоммуникационным сетям.

Для правильной квалификации действий мы должны выяснить, о каких правилах идет речь в статье и где они содержаться. По этому поводу в специальной литературе, посвященной проблемам компьютерных преступлений, существуют различные подходы к определению 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. На основе их анализа можно сделать вывод, что рассматриваемые правила эксплуатации и хранения могут содержаться как в нормативных правовых актах, так и в общих требованиях, предъявляемых к технике безопасности и правилам эксплуатации компьютерного оборудования. Кроме того, правила эксплуатации, обработки и хранения компьютерной информации могут быть и должны быть предусмотрены изготовителями и производителями компьютерного оборудования и прилагаться в виде инструкций и различного рода правил эксплуатации. Особая роль в сфере защиты компьютерной информации и средств ее хранения и передачи принадлежит обладателям такой информации. В организациях должны быть разработаны локальные акты, регламентирующие правила работы с компьютерной информацией и ее носителями.

В вышеуказанных Методических рекомендациях сказано, что «норма, содержащаяся в ст.274 УК РФ является бланкетной и отсылает правоприменителя к конкретным правилам инструкциям, которые устанавливают порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Каких-то общих правил эксплуатации, которые распространялись бы на неограниченный круг пользователей глобальной сети Интернет, не существует»[8]. Также указывается, что 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[9].

Подобного рода правила могут содержаться как в нормативно-правовых актах, технических регламентах, СНИПах, так и в локальных документах, разработанных в конкретных организациях по защите своих информационных ресурсов, кроме того, правила эксплуатации содержатся в технической документации, инструкциях, исходящих от заводов изготовителей этих средств.

На сегодняшний день многие организации, учреждения предусматривают свои правила эксплуатации средств хранения, обработки, передачи компьютерной информации, к которым, в частности, относятся, запреты на использование ресурсов Интернета во внеслужебных целях, запрет менять и обновлять программное обеспечение, использовать при работе на служебных компьютерах собственные носители информации (флешкарты, диски), нельзя допускать к работе с компьютерной информацией лиц, не обладающих соответствующими правами, и т. д.

Естественно, что лицо, нарушающее правила, должно быть ознакомлено с ними. Как правило, это указывается в должностной инструкции либо в договоре.

Законодатель также предусмотрел ответственность за нарушение правил доступа к информационно-телекоммуникационным сетям, тем самым расширив сферу применения данной статьи. Сегодня мы уже не представляем жизнь без Интернета, и подавляющее большинство населения имеет доступ

[8] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «Гарант».
[9] Там же.

к Интернету. Но, к сожалению, мало кто знает о правилах доступа. Хотя, заключая договор с провайдером, каждый ставит отметку о том, что он ознакомлен с правилами и с ответственностью за нарушение данных правил. Следует отметить, что уже появилась судебная практика по привлечению лица к уголовной ответственности по ст. 274 УК РФ за нарушение именно правил доступа к информационно-телекоммуникационным сетям, к которым относится Интернет. В частности, привлекают к ответственности лиц, которые предоставляют возможность неограниченному кругу лиц, являющихся пользователями систем, копировать и приобретать файлы, содержащие материалы порнографического характера, в целях зарабатывания рейтинга пользователей абонентов сети.

Помимо деяния, заключающегося в нарушении 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 обязательным признаком объективной стороны ст. 274 УК РФ, выступают последствия.

Последствия в виде уничтожения, блокирования, модификации и копирования компьютерной информации предусмотрены не только в ст. 274 УК РФ, но и в ст. 272 УК РФ. В литературе эти понятия достаточно полно раскрыты и, как правило, их установление не представляет существенной сложности.

Под уничтожением информации понимается приведение компьютерной информации полностью или частично в непригодное для использования состояние. Следует учесть, что для квалификации не имеет значения, сохранились ли копии этой информации на других носителях. Блокирование информации представляет собой отсутствие возможности в течение определенного периода времени или постоянно осуществлять нужные операции над компьютерной информацией полностью или в требуемом режиме, то есть можно говорить о закрытии доступа или его ограничения к компьютерной информации, целенаправленное затруднение доступа законных пользователей к компьютерной информации при сохранности таковой. Модификацией информации являются любые видоизменения информации по сравнению с первоначальным вариантом. Под копированием информации предполагается создание копии имеющейся информации на другом носителе, то есть перенос данной информации на обособленный носитель при сохранении неизменной первоначальной информации. Копирование может быть осуществлено на любой носитель: бумажный, электронный, переписанный от руки с дисплея монитора и т. д.

Указание на эти последствия в качестве обязательного признака объективной стороны, на мой взгляд, является излишним. Для квалификации достаточно наличия крупного ущерба в результате нарушения правил эксплуатации средств хранения, передачи и обработки компьютерной информации. Размер крупного ущерба определен в примечании к ст. 272 УК РФ, он составляет сумму свыше 1 млн рублей. Представляется, что относительно небольшое количество случаев привлечения к уголовной ответственности по ст. 274 УК РФ обусловлено как раз проблемами доказывания последствий в виде крупного ущерба.

Очень часто нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации выступает одним из этапов совершения других преступлений, в частности, хищений, собирания сведений, составляющих коммерческую, банковскую тайну. В таких случаях правоохранительные органы не считают необходимым квалифицировать действия лица по ст.274 УК РФ, ограничиваясь привлечением к ответственности по ст. 159, 159.6, 158, 183 УК РФ.

По моему мнению, к крупному ущербу следует относить не только прямой ущерб, который был причинен в результате нарушения правил, но и упущенную выгоду, затраты, необходимые на восстановление систем или информации, которая хранилась на средствах хранения, обработки и передачи информации, затраты на приобретение и установку нового программного обеспечения и т. д.

Естественно, должна быть причинно-следственная связь между нарушением правил и наступившими последствиями.

Таким образом, состав ст. 274 УК РФ является материальным составом и преступление считается оконченным с момента наступления неблагоприятных последствий.

В правоприменительной практике возникают сложности с определением субъективной стороны рассматриваемого преступления. Ряд авторов придерживается точки зрения, согласно которой субъективная сторона нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей характеризуется только

неосторожной формой вины[10]. Другие исследователи проблем квалификации ст. 274 УК РФ полагают, что субъективная сторона рассматриваемого преступления характеризуется как умыслом, так и неосторожной формой вины. Некоторые указывают на то, что «субъективная сторона преступного 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 характеризуется двумя формами вины»[11].

Исходя из анализа нормы, которая относится к числу бланкетных, можно прийти к выводу, что виновное лицо, нарушая правила, предвидит возможность наступления последствий, но самонадеянно рассчитывает на их предотвращение либо не предвидит возможные последствия, хотя при необходимой внимательности и предусмотрительности должно и могло их предвидеть. Следует отметить, что большинство бланкетных норм описывают составы с неосторожной формой вины, такие как ст. 264 УК РФ, 216 УК РФ, 143 УК РФ и т. д. Представляется, что данное преступление должно относиться к числу неосторожных преступлений. Если допустить возможность совершения данного преступления с умышленной формой вины, то, как мне представляется, это создаст сложности в отграничении от других преступлений, которые посягают на отношения собственности, общественную безопасность и т.д. В частности, если предположить, что лицо желает причинить крупный ущерб потерпевшим, сознательно выводя из строя дорогостоящее компьютерное оборудование, то квалифицировать необходимо по ст. 167 УК РФ, предусматривающей ответственность за умышленное уничтожение чужого имущества.

В содержание интеллектуального момента вины в качестве обязательного условия должно входить знание лица о правилах, которые оно нарушает. Виновное лицо должно быть ознакомлено с данными правилами, о чем указывается либо в договоре, инструкции, пользовательском соглашении и т. д.

Субъектом рассматриваемого преступления, согласно ст. 274 УК РФ, является физическое, вменяемое лицо, достигшее возраста 16 лет. Следует отметить, что по вопросу определения субъекта преступления, предусмотренного ст. 274 УК РФ, высказываются различные точки зрения. В частности, ряд исследователей считает, что в данном составе преступления субъект должен быть специальный, указывая на то, что «специализация субъекта здесь может определяться не только тем, что на лицо конкретными инструкциями или договорами возложены обязанности по соблюдению соответствующих правил, но и самим фактом использования лицом соответствующих ресурсов и (или) оборудования, т.е. определяться фактической включенностью лица в специфическую группу общественных отношений. Присоединение к любому пользовательскому соглашению, которое, как известно, осуществляется лицом путем проставления соответствующей отметки при прохождении регистрации на том или ином ресурсе, автоматически включает его в такие отношения»[12]. Скорее всего, речь здесь идет не о признаках субъекта преступления, а о признаках субъективной стороны, содержание которой включает в себя осознание лицом того факта, что оно нарушает определенные правила, содержащиеся в нормативно-правовых актах, инструкциях, договорах, соглашениях и т.д.

На практике вызывают сложности вопросы отграничения нарушения правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей от такого смежного состава преступления, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ), так как на практике складывается неоднозначная ситуация квалификации действий лица, имеющего доступ к компьютерной информации в силу занимаемой должности, профессиональной принадлежности и использующего такую информацию, по ч. 3 ст. 272 УК РФ. Если обратиться к сложившейся судебной практике толкования такого квалифицирующего признака, как использование своего служебного положения, то под этим признаком принято понимать совершение преступления должностным лицом, государственным или муниципальным служащим, не являющимся должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации. Но в Методических рекомендациях под использованием своих служебных полномочий применительно к ч. 2 ст. 272 УК РФ понимается использование возможности

[10] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. … канд. юрид. наук. Казань, 2017. С. 136.
[11] Русскевич В.Е. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации // Уголовное право. 2020. № 5. С. 22.
[12] Русскевич В.Е. Указ. соч. С. 24.

доступа к компьютерной информации, которая возникла в результате выполняемой работы (по трудовому договору, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ, то есть на тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие)[13].

При таком подходе ч. 1 ст. 272 УК РФ вступает в противоречие с ч.2 этой же статьи. Объективная сторона ст. 272 УК РФ заключается в неправомерном доступе к компьютерной информации, то есть речь идет о незаконном либо не разрешенном собственником или иным законным обладателем информации ее использовании, о возможности получения такой информации. Таким образом, получается, что с одной стороны, доступ должен быть неправомерным, а с другой – у лица имеется возможность доступа к охраняемой компьютерной информации. Выход из сложившейся ситуации видится в разграничении составов преступлений, предусмотренных ст. 272 УК РФ и ст. 274 УК РФ. В частности, если лицо имеет доступ к охраняемой компьютерной информации, но совершает незаконные действия с этой информацией, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи информации, что приводит к ее уничтожению, блокированию, модификации или копировании, то данные действия следует квалифицировать по ст. 274 УК РФ. А по ст. 272 УК РФ квалифицировать в тех случаях, когда субъект не имеет права доступа к компьютерной информации.

В заключение хотелось бы отметить, что в связи с активным ростом киберпреступности и кардинальными изменениями в средствах и способах совершения многих преступлений, связанных прежде всего с компьютерными технологиями, информационными ресурсами, информационно-телекоммуникационными системами, необходимо решить проблемы применения статей, предусматривающих уголовную ответственность за преступления в сфере компьютерной информации. Как показывает практика, преступления в сфере компьютерной информации в основном являются способами совершения других преступлений, посягающих на собственность, общественную безопасность, здоровье населения и т.д. Преступность, как и другие социальные явления, все больше и больше переходит в киберпространство, что существенно усложняет процесс раскрытия такого рода преступлений. Многие преступления совершаются, не выходя из дома с использованием различного рода технических средств, позволяющих проникать в средства хранения, передачи, обработки компьютерной информации.

Для эффективной борьбы с киберпреступлениями необходимо совершенствовать систему применения норм уголовного законодательства и разработать единые подходы к правилам квалификации этого вида преступлений.

Поступила в редакцию 23.03.2021

Стяжкина Светлана Александровна, кандидат юридических наук,
доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 4)
E-mail: styazhkina.sv@yandex.ru

S.A. Styazhkina

CRIMINAL-LEGAL FEATURES OF THE QUALIFICATION OF VIOLATIONS OF THE RULES OF OPERATION OF MEANS OF STORAGE, PROCESSING OR TRANSMISSION OF COMPUTER INFORMATION AND INFORMATION AND TELECOMMUNICATIONS NETWORKS (ARTICLE 274 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)

DOI: 10.35634/2412-9593-2021-31-3-489-496

The article deals with the issues of qualification of violations of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunications networks (Article 274 of the Criminal Code of the Russian Federation). The objective and subjective features of this corpus delicti are revealed. Special

[13] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «Гарант».

attention is paid to the problem of determining the subject of violation of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunications networks. The question of the objective side of the Article 274 of the Criminal Code of the Russian Federation is considered, in particular, the rules of means of storage, processing and transmission of computer information are defined, as which the rules should be considered, both contained in regulatory legal acts and in local documents of organizations, enterprises, institutions. The author analyzes the signs of the subjective side of the violation of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunications networks, which cause a lot of controversy in the scientific literature. Different points of view regarding the subject of the crime, which can be a physical sane person who has reached the age of 16, are also considered.

Keywords: criminal law, qualification of crimes, criminal liability, computer information, information and telecommunications networks, means of storing, processing and transmitting computer information, crimes in the field of computer information.

Received 23.03.2021

Styazhkina S.A., Candidate of Law, Associate Professor
Udmurt State University
Universitetskaya st., 1/4, Izhevsk, Russia, 426034
E-mail: styazhkina.sv@yandex.ru