Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2023-1-105-112

Вопросы квалификации преступлений в сфере компьютерной информации

Поздышев Роман Сергеевич
Нижегородская академия МВД России**,** Нижний Новгород, Россия, rmanpzdyshev@rambler.ru

Аннотация. В статье на основе анализа практики подразделений предварительного следствия органов внутренних дел обозначены проблемы квалификации преступлений в сфере компьютерной информации и предложены пути их решения. В частности, сделаны выводы о необходимости квалификации неправомерного доступа к учетным записям пользователей интернет-ресурсов и последующих хищений как совокупности соответствующих преступлений. Автором предложено внести изменения в законодательство для адекватной юридической реакции на киберпреступления, связанные с шифрованием компьютерной информации и последующими требованиями о выкупе паролей для расшифровки, поскольку действующей редакцией статьи 163 Уголовного кодекса Российской Федерации данное деяние не охватывается.

Ключевые слова: преступления в сфере компьютерной информации, киберпреступление, неправомерный доступ к компьютерной информации, мошенничество в сфере компьютерной информации, вредоносная компьютерная программа, вымогательство

Для цитирования: Поздышев Р. С. Вопросы квалификации преступлений в сфере компьютерной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 105—112. https://doi.org/10.36511/2078-5356-2023-1-105-112.

Original article

Issues of qualification of crimes in the sphere of computer information

Roman S. Pozdyshev
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, rmanpzdyshev@rambler.ru

Abstract. In the article, based on the analysis of the practice of the preliminary investigation units of the internal affairs bodies, the problems of qualifying crimes in the field of computer information are identified and ways to solve them are proposed. The author proposes to amend the legislation for an adequate legal response to cybercrimes related to encryption of computer information and subsequent demands for the ransom of passwords for decryption, since this act is not covered by the current version of Article 163 of the Criminal Code of the Russian Federation.

Keywords: crimes in the field of computer information, cybercrime, illegal access to computer information, fraud in the field of computer information, malicious software, extortion

For citation: Pozdyshev R. S. Issues of qualification of crimes in the sphere of computer information. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 1 (61), pp. 105—112 . (In Russ.). https://doi.org/10.36511/2078-5356-2023-1-105-112.

Правоприменительная практика в сфере уголовного судопроизводства не характеризуется единообразием. Схожие по фактическим обстоятельствам деяния могут квалифицироваться по-разному даже в рамках одного субъекта Российской Федерации. Преступления в сфере компьютерной информации не являются исключением [1—3]. В рамках данной статьи автором предпринята попытка унификации подходов к юридической квалификации рассматриваемой категории криминальных деяний в практике подразделений предварительного следствия органов внутренних дел.

Предваряя изложение результатов исследования, необходимо определить его предмет. Преступления в сфере компьютерной информации закреплены в главе 28 Уголовного Кодекса Российской Федерации (далее — УК РФ) и

представлены в виде четырех статей (ст. 272—274[1]), предусматривающих ответственность: за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. В рамках настоящего исследования круг данных преступлений расширен: в него включено мошенничество в сфере компьютерной информации (ст. 159[6] УК РФ), поскольку способ его совершения имеет общие признаки с рассматриваемой категорией криминальных деяний.

Эмпирическая база исследования представлена материалами судебно-следственной практики по противодействию преступлениям в сфере компьютерной информации, представленными Следственным департаментом МВД России в 2022 году в рамках подготовки заказного научного исследования «Аналитический обзор результатов работы органов предварительного следствия по уголовным делам о преступлениях в сфере компьютерной информации по итогам 2021 года». Кроме того, в ходе исследования осуществлено интервьюирование 48 сотрудников органов внутренних дел, проходящих службу в разных регионах Российской Федерации, в чьи обязанности входит противодействие преступлениям в сфере компьютерной информации.

Для демонстративности наиболее проблемные вопросы, выявленные в результате изучения обвинительных заключений, приговоров и иных процессуальных документов, агрегированы в условные группы.

Проблемы квалификации неправомерного доступа к учетным записям пользователей интернет-ресурсов и последующих хищений

В большинстве субъектов Российской Федерации сложилась практика квалификации подобных деяний как совокупности преступлений: по части 2 статьи 272 УК РФ за неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности, и по соответствующей статье УК РФ за последующее хищение.

В производстве следственных подразделений по Оренбургской области находилось уголовное дело по обвинению М. в совершении ряда преступлений, предусмотренных частью 2 статьи 272 и частями 1 и 2 статьи 159 УК РФ. Согласно полученным доказательствам, М., имея умысел на хищение денежных средств граждан, используя заранее приобретенные логины и пароли, осуществил неправомерный доступ к персональным страницам пользователей социальной сети, после чего изменил их, тем самым заблокировав компьютерную информацию для законных владельцев учетных записей. Затем, действуя от имени последних, направил их подписчикам сообщения с просьбой одолжить денежные средства. Получатели указанных писем, будучи введенными в заблуждение относительно авторства сообщений, перечисляли различные суммы на подконтрольные М. счета. Преступными действиями М. потерпевшим причинен материальный ущерб в размере 180 000 рублей [4].

Согласно справкам, представленным территориальными следственными подразделениями в системе МВД России, в ряде регионов сложилась другая практика. Так, в соответствии с информацией, направленной Следственным управлением МВД по Республике Бурятия, позиция прокуратуры заключается в рассмотрении неправомерного доступа к учетным записям пользователей интернет-ресурсов как способа совершения мошенничества, и дополнительно по статье 272 УК РФ не квалифицируется.

Аналогичной позиции придерживается Главное следственное управление МВД по Республике Татарстан. Здесь, в отличие от предыдущего субъекта, эта позиция идет вразрез с мнением местного надзорного ведомства по данному вопросу. С точки зрения Прокуратуры Республики Татарстан, мошенничества, связанные со взломом страницы в социальных сетях, должны квалифицироваться не только по статье 159 УК РФ, но и по статье 272 УК РФ. Однако орган предварительного следствия с данной позицией не согласен, обосновывая это тем, что аккаунты в социальных сетях не относятся к категории охраняемой законом компьютерной информации, поскольку не представляют ни государственную, ни коммерческую тайну, все персональные данные, которые размещаются на таких страницах, являются общедоступными в силу пункта 2 части 2 статьи 10 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в связи с чем применение такого понятия, как «тайна связи», и статьи 63 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи» невозможно.

Подобную, по мнению автора, ошибочную позицию, можно встретить и в правоприменительной практике других регионов Российской Федерации.

В ходе предварительного следствия по уголовному делу, возбужденному следственным органом МВД по Республике Адыгея по части 2 статьи 272 УК РФ, установлено, что неизвестное лицо в 2021 году путем подбора логина и пароля от аккаунта в социальной сети Instagram и электронного почтового ящика ООО «Мэйл.Ру», принадлежащих С., заблокировало правомерный доступ последней к указанным учетным записям с целью публикаций не соответствующих действительности сведений о сборе денежных средств. Довести свой преступный умысел до конца неустановленное лицо не смогло по не зависящим от него обстоятельствам. В связи с позицией прокуратуры об ошибочности отнесения содержащейся в аккаунте социальной сети и электронном почтовом ящике информации к категории охраняемой законом, данное преступление переквалифицировано на часть 3 статьи 30, часть 1 статьи 159[6] УК РФ [5].

Приведенная аргументация противоречит требованиям закона и сложившейся на большей части России юридической практике. В соответствии со статьей 23 Конституции Российской Федерации каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Очевидно, что нарушение данных прав человека происходит при неправомерном доступе к учетной записи в социальных сетях, где содержится как личная информация, так и переписка пользователя с иными лицами, соответственно, подобная информация охраняется законом. Согласно законодательству и юридической доктрине, вышеуказанные преступные действия следует квалифицировать как совокупность преступлений, предусмотренных частью 3 статьи 30, частью 2 статьи 272 и соответствующей частью статьи 159 УК РФ.

Имущественные преступления, следующие за неправомерным доступом к учетным записям пользователей интернет-ресурсов, не всегда осуществляются в виде мошеннических действий.

В производстве следователей по Тамбовской области находилось уголовное дело по обвинению П. в совершении серии преступлений, предусмотренных частью 1 статьи 272 и частью 1 статьи 163 УК РФ. Установлено, что в 2020 году П. путем введения полученных при неустановленных обстоятельствах логинов и паролей осуществил неправомерный доступ к закрытой информации страниц граждан в социальной сети «ВКонтакте», после чего произвел копирование частных видеозаписей, изображений и переписки их владельцев. Далее под угрозой распространения указанных сведений, позорящих потерпевших и способных причинить существенный вред их правам и законным интересам, путем переписки П. незаконно требовал перевести ему денежные средства в различных суммах на принадлежащий ему счет биткоин-кошелька. Ленинским районным судом г. Тамбова уголовное дело в отношении П. прекращено по статье 25[1] УПК РФ с назначением судебного штрафа [6].

В приведенном примере квалификация действий обвиняемого, связанных с неправомерным доступом к компьютерной информации, представляется ошибочной, поскольку в деяниях прослеживается корыстная заинтересованность, соответственно, их необходимо квалифицировать по части 2 статьи 272 УК РФ.

Проблемы квалификации киберпреступлений, связанных с шифрованием компьютерной информации и последующими требованиями о выкупе паролей для расшифровки

Преступления, связанные с шифрованием компьютерной информации и последующим требованием выкупа за ее расшифровку, имеют широкое распространение во всем мире. Органы предварительного следствия МВД России квалифицируют такие преступления по статье 272 или статье 273 УК РФ.

Следственным органом Управления на транспорте МВД России по Северо-Западному федеральному округу возбуждено уголовное дело по части 2 статьи 273 УК РФ в отношении неустановленного лица, которое распространило вредоносное программное обеспечение, а также выполнило несанкционированное кодирование и блокировку информации, находящейся в персональном компьютере АО «К», нарушив деятельность предприятия. В последующем в АО «К» посредством электронной почты поступило предложение неустановленного лица о приобретении программного обеспечения, позволяющего разблокировать закодированную информацию за криптовалюту, эквивалентную 4 000 долларов США. В ходе расследования установить лицо, подлежащее

привлечению в качестве обвиняемого, не представилось возможным, в связи с чем предварительное следствие приостановлено [7].

Существует практика квалификации подобных преступлений по части 2 статьи 272 УК РФ.

В производстве следственных подразделений по Алтайскому краю находилось уголовное дело по обвинению П. в совершении двух преступлений, предусмотренных частью 2 статьи 272 УК РФ. Расследованием установлено, что П. приобрел на неустановленных интернет-ресурсах информацию, необходимую для удаленного доступа к персональным компьютерам бухгалтеров организаций в Челябинской области и Краснодарском крае. Используя эти сведения (IP-адрес, логин, пароль), П. осуществил неправомерный доступ к данным бухгалтерии, заархивировал их, удалив оригинальные файлы, и установил пароли для доступа к архивам. За предоставление паролей доступа к заблокированной информации П. получил от представителей организаций выкуп в криптовалюте DASH. Приговором Армавирского городского суда Краснодарского края П. назначено наказания в виде исправительных работ на срок 1 год 2 месяца с удержанием 10 % заработной платы в доход государства [8].

Принципиальным обстоятельством, влияющим на выбор той или иной нормы права, является способ проникновения в компьютерную инфраструктуру потерпевшего. Если доступ к информации совершен посредством приобретения необходимых для этого сведений (*IP*-адреса, логина, пароля и др.) на сторонних интернет-ресурсах, а затем они использованы в обычном для всех пользователей порядке через сеть «Интернет» без применения каких-либо вредоносных программ, то содеянное квалифицируется по части 2 статьи 272 УК РФ. Если же доступ к информации, которую злоумышленник планирует зашифровать, осуществляется посредством использования вредоносной программы, то деяние подпадает под действие части 2 статьи 273 УК РФ.

В последнем случае статьей 273 УК РФ охватываются лишь действия по использованию компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. При этом упускаются из виду действия преступника по неправомерному доступу к охраняемой законом информации и общественно опасные последствия в виде блокирования данной информации. Таким образом, квалификация действий шифровальщиков-вымогателей по статье 272 УК РФ представляется необходимой во всех случаях. Если для неправомерного доступа использовалась вредоносная программа, то деяние следует квалифицировать как совокупность преступлений и дополнительно вменять статью 273 УК РФ.

Другим проблемным моментом в квалификации данных преступлений является определение юридической природы требований о выкупе паролей или иных средств для возобновления доступа к зашифрованной информации. Подобные требования не охватываются действием статей 272 или 273 УК РФ и при этом также представляются преступными, а значит требующими отдельной квалификации. К данному умозаключению можно прийти при системном анализе уголовного закона, актов его официального толкования и теории уголовного права. Здесь можно провести аналогию с иными схожими по логике совершения криминальными деяниями.

Так, в соответствии с пунктом 20 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое», если лицо, совершая кражу, грабеж или разбой с незаконным проникновением в жилище, помещение либо иное хранилище, умышленно уничтожило или повредило двери, замки и т. п., а равно иное имущество потерпевшего, не являвшееся предметом хищения (например, мебель, бытовую технику и другие вещи), содеянное в случае причинения значительного ущерба следует дополнительно квалифицировать по статье 167 УК РФ.

Также в соответствии с пунктом 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274[1] УК РФ.

Таким образом, разумным и обоснованным видится необходимость правовой реакции не только на неправомерный доступ к компьютерной информации и ее шифрование, являющееся лишь способом незаконного обогащения, но и на действия лица, требующего выкуп за расшифровку этой информации. На первый взгляд,

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 1 (61)

подобные действия схожи с составом преступления, предусмотренного статьей 163 УК РФ. Однако, вымогательство не предусматривает такой признак объективной стороны как требование передачи чужого имущества под угрозой уничтожения или блокирования компьютерной информации. Таким образом, можно говорить о правовом пробеле, так как рассматриваемые общественные отношения не урегулированы в достаточной степени. Преодоление данного пробела предпринималось правоприменительной практикой.

Расследование по уголовному делу, находившемуся в производстве следственных подразделений по Томской области, показало, что Д., используя приобретенные им логины и пароли к административным учетным записям ООО «Л», осуществил неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей данной организации. После этого, применяя специализированное программное обеспечение, обвиняемый произвел блокирование указанной информации путем ее шифрования и направил электронное письмо в адрес ООО «Л», в котором под угрозой сохранения блокировки, уничтожения и повреждения компьютерных систем организации выдвинул требования о перечислении ему 2 биткоинов, что эквивалентно 1 261 838,3 рублям. В ходе переписки с представителем ООО «Л» Д. согласился предоставить ключи для снятия блокировки серверов за 0,8 биткоина, то есть за 504 640 рублей. После получения указанного имущества Д. предоставил ключи для расшифровки компьютерной информации. Его действия квалифицированы по части 4 статьи 272, пункту «б» части 3 статьи 163 УК РФ [9].

Данный пример является показательным, поскольку убедительно демонстрирует высокую общественную опасность данного вида преступлений. Необходимость квалификации подобных деяний как совокупности неправомерного доступа к компьютерной информации и соответствующего преступления против собственности представляется очевидной. Однако, в связи с принципом законности практическая реализация данной идеи на сегодняшний момент невозможна. В приведенном выше примере непосредственных угроз уничтожения или повреждения чужого имущества преступником не высказывалось. Кроме того, представитель потерпевшего ООО «Л» в ходе допроса пояснил, что действия преступника были связаны только с блокировкой информации, хранящейся на серверах, к физическому уничтожению или повреждению самих серверов данные обстоятельства привести не могли. Тем не менее работа всей информационной системы предприятия была полностью остановлена. Ущерб, причиненный данной организации от преступных действий Д. не имел реальной формы, а выражался лишь в упущенной выгоде в связи с вынужденным простоем в производстве.

Таким образом, представляется, что единственно верным способом преодоления выявленного пробела в праве является внесение соответствующих изменений в статью 163 УК РФ.

Проблемы соотношения статей 159 и 159^6 УК РФ

В правоприменительной практике органов предварительного следствия МВД России нередко встречается неправильное разграничение мошенничества, предусмотренного статьей 159 УК РФ, и мошенничества в сфере компьютерной информации, предусмотренного статьей 159^6 УК РФ.

В 2021 году следователями по Калужской области окончено расследование по уголовному делу по части 1 статьи 159^6, части 2 статьи 272 УК РФ. Установлено, что в 2019—2020 годах Э., действуя с целью хищения денежных средств пользователей сети «Инстаграмм», зная логин и пароль одного из аккаунтов, осуществил вход в него, после чего произвел замену пароля для последующего доступа к нему, тем самым заблокировав компьютерную информацию для ее законного владельца. Далее от имени владельца указанной учетной записи направил ее знакомой Х. сообщение с просьбой одолжить денежные средства в сумме 7 000 рублей, которые последняя, будучи введенной в заблуждение относительно авторства просьбы, перевела на подконтрольный Э. банковский счет. Сухиничским районным судом Калужской области уголовное дело в отношении Э. прекращено по основанию, предусмотренному статье 25 УПК РФ [10].

Квалификация действий Э., связанных с хищением денежных средств, представляется ошибочной. В соответствии с пунктом 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в сети

«Интернет», то такое мошенничество следует квалифицировать по статье 159, а не 159[6] УК РФ.

Способом совершения мошенничества, предусмотренного статьей 159[6] УК РФ, является не обман или злоупотребление доверием, а вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Под таким вмешательством следует понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) — ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Отрицательные примеры правоприменительной практики расследования преступлений в сфере компьютерной информации

Институт возбуждения уголовного дела в российском уголовном процессе играет роль своеобразного фильтра, позволяющего отсеивать деяния, которые в соответствии с уголовным законом не являются преступлениями. На данной стадии в том числе необходимо проверять лицо, совершившее преступные действия, на соответствие требованиям уголовного закона, предъявляемым к признакам субъекта преступления.

Следственными подразделениями по Республике Коми возбуждено уголовное дело по части 2 статьи 272 УК РФ по факту внесения неустановленным лицом в электронный журнал одной из школ города ложной информации об оценках учащихся пятого «А» класса. При допросе ученика этого класса, мобильный телефон которого использовался для входа в учетную запись преподавателя и исправления отметок, стало известно, что логин и пароль ученик подсмотрел у учителя, модификацию информации произвел по причине получения неудовлетворительной оценки. В сентябре 2021 года уголовное дело прекращено в связи с недостижением виновным возраста уголовной ответственности, то есть на основании пункта 2 части 1 статьи 24 УПК РФ [11].

Безусловно, не всегда возможно в ходе проверки сообщения о преступлении установить лицо его совершившее, однако в данном случае достаточной стала бы своевременная проверка IP-адреса, с которого осуществлен неправомерный доступ к электронному журналу. Кроме того, на совершение деяния лицом, не достигшим возраста 16 лет, указывали фактические обстоятельства, а именно: исправление оценок в журнале пятого класса. Также вызывает сомнение квалификация деяния по части 2 статьи 272 УК РФ, как совершенного из корыстной заинтересованности. Содержание данного квалифицирующего признака в законе не раскрывается, однако юридическая наука и практика под корыстной заинтересованностью понимают стремление лица путем совершения неправомерных действий получить для себя или других лиц выгоду имущественного характера.

Еще одной проблемой являются провокации совершения преступления сотрудниками, осуществляющими оперативно-розыскную деятельность.

Следственным органом Управления на транспорте МВД России по Приволжскому федеральному округу окончено уголовное дело по обвинению Б. в совершении преступлений, предусмотренных части 3 статьи 30, части 2 статьи 146, части 3 статьи 30 части 1 статьи 273 УК РФ. Предварительным расследованием установлено, что Б. в 2020 году разместил на торговой интернет-площадке «Авито» объявление об установке и переустановке операционной системы Windows и установке дополнительных систем с выездом на дом. Затем, выполняя заказ одного из своих клиентов, из сети «Интернет» скопировал (приобрел) с целью сбыта и перенес на оптический диск контрафактный инсталляционный экземпляр узкоспециализированной компьютерной программы, а также файлы, предназначенные для нейтрализации путем модификации информации установленных правообладателем средств ее защиты. Далее указанный оптический диск, содержащий контрафактную продукцию и вредоносную компьютерную программу, Б. реализовал участвовавшему в проведении оперативно-розыскного мероприятия «проверочная закупка» Ш. за 500 рублей. В связи с тем, что приобретение программного продукта проводилось под контролем правоохранительных органов лицом, осуществлявшим проверочную закупку, преступления Б. не были доведены до конца по независящим от него обстоятельствам [12].

Бугульминский городской суд Республики Татарстан счел обвинение, предъявленное Б., несостоятельным, поскольку собранные по уголовному делу доказательства свидетельствуют, что участвующий в проверочной закупке Ш. сам попросил Б. скачать программу, указав ее название. Следовательно, инициатива по установке программы исходила не от подсудимого Б., а от свидетеля Ш. Таким образом, суд пришел к выводу, что умысел на совершение указанных преступлений у Б. возник в результате деятельности оперативных сотрудников, что является нарушением требований статьи 5 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности». В результате Б. признан невиновным и оправдан приговором суда.

Кроме того, вызывает сомнения правильность квалификации действий Б., как покушения на преступление. Юридической практикой, основывающейся на законе и актах официального толкования норм права, факт совершения преступления с формальным составом под контролем правоохранительных органов не влияет на его квалификацию как оконченного. Например, согласно пункту 13 постановления Пленума Верховного Суда Российской Федерации от 9 июля 2013 года № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» получение или дача взятки, если указанные действия осуществлялись в условиях оперативно-розыскного мероприятия, должны квалифицироваться как оконченное преступление вне зависимости от того, были ли ценности изъяты сразу после их принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации. Аналогичные позиции можно встретить и в других правоинтерпретационных актах.

Резюмируя изложенное, следует заключить, что сложившаяся ситуация в области применения правовых норм, регламентирующих уголовную ответственность за преступления в сфере компьютерной информации, не в полной мере соответствует концепции правового государства, поскольку отсутствует единое понимание данной разновидности правонарушений и юридические предписания действуют по-разному в разных регионах Российской Федерации. Результаты проведенного исследования могут способствовать унификации подходов к квалификации рассматриваемой категории преступлений и обеспечению предсказуемости юридической практики.

Список источников

1. Летелкин Н. В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции, Москва, 25—26 января 2018 года. Москва: РГ-Пресс, 2018. С. 617—619.

2. Ушаков А. Ю. Некоторые вопросы правового обеспечения противодействия преступлениям, совершаемым с использованием it-технологий // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. 2022. № 1. С. 32—36.

3. Долгачева О. И., Потапова Н. Н. К вопросу о противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Дискуссионные аспекты развития уголовно-процессуального законодательства и его применения сборник статей по материалам всероссийской конференции, Нижний Новгород, 12 ноября 2020 года. Нижний Новгород: Нижегородская академия Министерства внутренних дел Российской Федерации, 2021. С. 73—79.

4. Уголовное дело № 12101530021000057 // Надзорное производство Следственного управления УМВД России по Оренбургской области. 2021.

5. Уголовное дело № 12101790004000459 // Надзорное производство Следственного управления МВД по Республике Адыгея. 2021.

6. Уголовное дело № 12001680032001073 // Надзорное производство Следственного управления УМВД России по Тамбовской области. 2021.

7. Уголовное дело № 12001009719000266 // Надзорное производство Следственного управления УТ МВД России по Северо-западному федеральному округу. 2021.

8. Уголовное дело № 12001010001000278 // Надзорное производство Главного следственного управления ГУ МВД России по Алтайскому краю. 2021.

9. Уголовное дело № 12001690024000209 // Надзорное производство Следственного управления УМВД России по Томской области. 2021.

10. Уголовное дело № 12101290003000031 // Надзорное производство Следственного управления УМВД России по Калужской области. 2021.

11. Уголовное дело № 12101870007000585 // Надзорное производство Следственного отдела ОМВД России по г. Ухте. 2021.

12. Уголовное дело № 12001000149000163 // Надзорное производство Следственного управления Управления на транспорте МВД России по Приволжскому федеральному округу. 2021.

References

1. Letelkin N. V. On the issue of defining the concept of crimes committed using information and telecommu-

nication networks (including the Internet). Criminal law: development strategy in the XXI century: Proceedings of the XV International Scientific -practical conference, Moscow, January 25—26, 2018. Moscow: RG-Press Publ., 2018. Pp. 617—619. (In Russ.)

2. Ushakov A. Yu. Some issues of legal support for counteraction to crimes committed with the use of it-technologies. *Vestnik of Putilin Belgorod law institute of the Ministry of the interior of Russia*, 2022, no. 1, pp. 32—36. (In Russ.)

3. Dolgacheva O. I., Potapova N. N. On the issue of counteraction to crimes committed with the use of information and telecommunication technologies. Discussion aspects of the development of criminal procedure legislation and its application: collection of articles based on materials All-Russian Conference, Nizhny Novgorod, November 12, 2020. Nizhny Novgorod: Nizhny Novgorod Academy of the Ministry of Internal Affairs of the Russian Federation, 2021. Pp. 73—79. (In Russ.)

4. Criminal case no. 12101530021000057. Supervisory proceedings of the Investigation Department of the Ministry of Internal Affairs of Russia for the Orenburg Region, 2021. (In Russ.)

5. Criminal case no. 12101790004000459. Supervisory proceedings of the Investigation Department of the Ministry of Internal Affairs for the Republic of Adygea, 2021. (In Russ.)

6. Criminal case no. 12001680032001073. Supervisory proceedings of the Investigation Department of the Ministry of Internal Affairs of Russia for the Tambov Region, 2021. (In Russ.)

7. Criminal case no. 12001009719000266. Supervisory proceedings of the Investigation Department of the UT of the Ministry of Internal Affairs of Russia for the Northwestern Federal District, 2021. (In Russ.)

8. Criminal case no. 12001010001000278. Supervisory proceedings of the Main Investigation Department of the Main Directorate of the Ministry of Internal Affairs of Russia for the Altai Territory, 2021. (In Russ.)

9. Criminal case no. 12001690024000209. Supervisory proceedings of the Investigation Department of the Ministry of Internal Affairs of Russia for the Tomsk Region, 2021. (In Russ.)

10. Criminal case no. 12101290003000031. Supervisory proceedings of the Investigation Department of the Ministry of Internal Affairs of Russia for the Kaluga Region, 2021. (In Russ.)

11. Criminal case no. 12101870007000585. Supervisory proceedings of the Investigative Department of the OMVD of Russia for the city of Ukhta, 2021. (In Russ.)

12. Criminal case no. 12001000149000163. Supervisory proceedings of the Investigation Department of the Transport Administration of the Ministry of Internal Affairs of Russia for the Volga Federal District, 2021. (In Russ.)

Информация об авторе

Р. С. Поздышев — кандидат юридических наук.

Information about the author

R. S. Pozdyshev — Candidate of Sciences (Law).

Статья поступила в редакцию 21.01.2023; одобрена после рецензирования 15.02.2023; принята к публикации 05.03.2023.

The article was submitted 21.01.2023; approved after reviewing 15.02.2023; accepted for publication 05.03.2023.