

ПОНЯТИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ЕГО ВЛИЯНИЕ НА КВАЛИФИКАЦИЮ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 272 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Автором рассматривается отдельное деяние статьи 272 «Неправомерный доступ к компьютерной информации» главы 28 Уголовного кодекса Российской Федерации (далее – УК РФ) с точки зрения того, как дефиниция «компьютерная информация» и диспозиция статьи в целом позволили сформировать ошибочную практику применения статьи. По мнению автора, причиной этого является неверная оценка степени бланкетности понятия компьютерной информации, которая влечет за собой ошибочное представление о способе совершения деяния, средствах его совершения и пр. Соотнося существующие трактовки названных дефиниций с действующим законом и техническими характеристиками, автор предлагает иной взгляд на содержание статьи 272 УК РФ и, соответственно, всей главы 28.

Ключевые слова: компьютерная информация; неправомерный доступ; регулирование компьютерной информации; преступления в сфере компьютерной информации; киберпреступления; квалификация; состав преступления; объект преступления; объективная сторона; уголовное право.

The author of the proposed article considers a separate act of Chapter 28 – Art. 272 «Illegal access to computer information» from the point of view of how the definition of «computer information» and the disposition of the article as a whole allowed to form an erroneous practice of using the article. According to the author, the reason for this is an incorrect assessment of the degree of blankness of the concept of computer information, which entails an erroneous idea of the method of committing an act, the means of committing it, and so on. st. 272 of the Criminal Code of the Russian Federation and, accordingly, the entire Chapter 28.

Keywords: computer information; illegal access; regulation of computer information; crimes in the field of computer information; cybercrime; qualification; crime; object of crime; objective side; criminal law.

В последнее время в науке уголовного права сформировалось отдельное направление, посвященное вопросам защиты прав, связанных с компьютерной информацией в той или иной форме, — киберпреступлений. Подавляющее большинство работ, касающихся этого вида деяний, затрагивают вопрос реформирования УК РФ, указывая, что глава 28 кодекса устарела и не соответствует современным правоотношениям. Другая категория авторов посвящает свои работы непосредственному рассмотрению составов преступлений главы 28 УК РФ и особенностей их квалификации, не затрагивая вопросы реформирования.

В Российской Федерации общественные отношения, связанные с использованием цифровых технологий, законодатель выделил задолго до возникновения термина «цифровая экономика» и интереса к кибербезопасности — в главе 28 УК РФ, устанавливающей ответственность за преступления в сфере компьютерной информации. Учитывая, что наименования разделов и глав Особенной части УК РФ содержат в себе перечень защищаемых уголовным законом однородных общественных от-

© Кучина Я.О. , 2019

ношений — объектов преступлений, то отношения в сфере компьютерной информации представляют собой один из них. Опыт правоприменительной практики в области защиты этих отношений и их объекта насчитывает уже более двадцати лет. Тем не менее, при проведении уголовно-правовой экспертизы материалов дел и приговоров часто можно наблюдать ошибочную квалификацию деяний, при совершении которых использовались те или иные компьютерные технологии.

Мы полагаем, что данное явление связано не с квалификацией правоприменителя, как иногда принято утверждать [8], но вызвано имеющейся в законе дефиницией самого объекта преступления, способами описания составов деяний и тем, как это соотносится с иными нормами отечественного законодательства, регулированием защищаемых правоотношений и техническими характеристиками предмета преступления. Рассмотрим подробнее, на чем мы основываем эту нашу позицию.

Глава 28 УК РФ содержит четыре состава преступления:

- 1) статья 272 «Неправомерный доступ к компьютерной информации»;
- 2) статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;
- 3) статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;
- 4) статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Системообразующей является статья 272 УК РФ, которая предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (часть 1). В примечании к статье компьютерная информация определена как *сведения (сообщения, данные), представляющие в форме электрических сигналов, независимо от средств их хранения, обработки и передачи*. То есть объектом преступления, предусмотренного статьей, выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение,

модификацию, использование компьютерной информации ее создателем, а также потребление этой информации иными пользователями.

До 7 марта 2011 года формулировка диспозиции статьи 272 была иной. В части 1 закреплялась ответственность за неправомерный доступ к информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Тем самым предыдущая редакция статьи, описывая объект преступления и его предмет, опиралась на ГОСТ 15971-90 [4] и ГОСТ 27201-87 [3]. Согласно им ЭВМ — это вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах; под персональной ЭВМ (персональным компьютером) подразумевается настольная микро-ЭВМ, имеющая эксплуатационные характеристики бытового прибора и универсальные функциональные возможности; а под системой ЭВМ — совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг.

Отступив в 2011 году от терминологии ГОСТа и перейдя к использованию понятия «компьютерная информация», законодатель расширил возможность толкования содержания объекта и предмета преступления, исключив технические подробности и сосредоточившись на признаках защищаемого явления. Если выделять их непосредственно из примечания к статье 272 УК РФ, то компьютерная информация должна представлять собой сведения, сообщения или данные, выраженные в определенной форме — в форме электрических сигналов. Назначение и особенности работы с такими сведениями при установлении объекта преступления роли не играют.

При этом единообразного нормативно-правового разъяснения понятия «компьютерная информация» не существует. В научных работах часты ссылки [6, с. 42] на «Методические рекомендации по осуществлению прокурорского надзора за исполне-

нием законов при расследовании преступлений в сфере компьютерной информации» Генеральной прокуратуры Российской Федерации [9] (далее — Рекомендации). В них высказана правовая позиция, в соответствии с которой органы прокуратуры Российской Федерации осуществляют надзор за исполнением законодательства при расследовании преступлений из главы 28 УК РФ. То есть Рекомендации являются определяющими при поддержании государственного обвинения в процессе применения положений статьи 272 УК РФ и представляют в связи с этим особый интерес.

Объективная сторона преступления, предусмотренного частью 1 статьи 272 УК РФ, сформирована деянием в форме действия, последствиями и прямой причинно-следственной связью, т. е. согласно науке уголовного права рассматриваемый состав является материальным. Законодатель определил деяние как *неправомерный доступ к охраняемой законом компьютерной информации*. Это, в свою очередь, детерминирует способы совершения преступления, хотя они не перечислены в диспозиции статьи. Исчерпывающий перечень последствий включает в себя такой результат преступных действий, как *уничтожение, блокирование, модификацию либо копирование компьютерной информации*. Таким образом, на первый взгляд, диспозиция лаконична, а элементы состава преступления описаны в не требующей дополнительного пояснения форме. Однако, по нашему мнению, это упрощенный подход, в результате которого возникает устойчивая практика ошибочной квалификации. Для того чтобы подтвердить наш вывод, рассмотрим объект и объективную сторону части 1 статьи 272 УК РФ более подробно.

Необходимо начать с утверждения о том, что включенная в описательную часть формулировка «охраняемая законом компьютерная информация» делает объект преступления, предусмотренного частью 1 статьи 272 УК РФ, бланкетным, что, разумеется, вступает в некоторый конфликт с примечанием 1 к статье. Еще раз напомним, что общим объектом преступления выступают общественные отношения, гарантирующие *правомерный* доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. Со-

держание предмета преступления же более расплывчато.

Разъясняя особенности квалификации статьи 272 УК РФ, Генеральная прокуратура Российской Федерации ссылается на статью 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Федеральный закон № 149-ФЗ) [11], в пункте 1 которой информация определена как «сведения (сообщения, данные) независимо от формы их представления». То есть у защищаемой законом информации должно быть, как минимум, три формы выражения — это сведения, сообщения и данные, а примечание к статье 272 УК РФ добавляет еще одну — форму электрических сигналов, тем самым отграничивая компьютерную информацию от иных видов информации. Способ отграничения — это, как совершенно верно отмечает В.Б. Вехов, способ внешнего оформления информации, ее объективизация, а не внутреннее содержание [2, с. 78].

УК РФ говорит о компьютерной информации, охраняемой законом. Применительно к информации в целом, не только компьютерной, этот вопрос решается достаточно просто — виды охраняемой законом информации определены специальными нормативно-правовыми актами. В науке принято выделять понятие конфиденциальной информации, т. е. информации, не подлежащей разглашению [16, с. 17]. К примеру, статья 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» [12] устанавливает, что сведения о факте обращения гражданина за медицинской помощью, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляющие врачебную тайну, разглашение которой в какой-либо форме не допускается.

В части 2 статьи 9 Федерального закона № 149-ФЗ термин «конфиденциальная информация» используется при описании обязанности не разглашать информацию, доступ к которой ограничен, т. е. обязанности соблюдать ее конфиденциальность. В части 1 этой же статьи есть перечень информации, доступ к которой ограничен. Ограничение доступа к информации означает, что она подлежит охране. Такое ограничение устанавливается федеральными законами

в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности и безопасности государства, а к охраняемой законом относятся такие виды информации, как сведения, составляющие коммерческую тайну, служебную тайну и иную тайну (часть 4 статьи 9), информация о частной жизни физического лица, в том числе информация, составляющая личную или семейную тайну (часть 8 статьи 9), персональная информация (персональные данные).

Некоторые авторы полагают данный перечень исчерпывающим, считая Федеральный закон № 149-ФЗ основным актом, регулирующим охрану информации [6, с. 44], а установление критериев конфиденциальности — единственным признаком [18, с. 179–180]. Это мнение более чем спорно, достаточно привести примеры такой информации, как профессиональная тайна (адвокатская, врачебная) или объекты авторских и смежных прав, которые часто по своей внешней форме являются данными. То есть исчерпывающий перечень и отграничение видов охраняемой информации от неохраняемой определяются специальными нормативно-правовыми актами [12], Гражданским и Семейным кодексами Российской Федерации, в некоторых случаях — правоприменителем. Согласно постановлению Пленума Верховного суда Российской Федерации от 13 декабря 2012 года вопросы частной жизни лиц, не являющихся участниками дела, не могут подлежать оглашению среди неопределенного круга лиц, а вопросы, затрагивающие права и законные интересы несовершеннолетних, рассматриваются в открытом судебном заседании только при наличии согласия их законных представителей [15]. В этом случае информация становится охраняемой законом по решению суда, которое конкретизирует ее из общего объема всей подобной информации.

Отсюда мы можем сделать вывод, что под информацией, охраняемой законом, надо понимать не только информацию, которую законодатель целенаправленно наделил признаками конфиденциальности и в отношении которой установил режим охраны. Охраняемая законом информация — это любая информация, признаваемая законом, определенная законом, если в ее отноше-

нии установлен любой правовой режим, т. е. если она признана объектом правоотношения. Актом, содержащим наиболее полный перечень охраняемой информации, является Конституция Российской Федерации (далее — Конституция РФ). Наличие такого признания, исходя из положений действующего на территории Российской Федерации законодательства, позволяет прибегнуть к общим и специальным средствам защиты объекта правоотношения, например, согласно статьям 17 и 23 Конституции РФ, статьям 1, 11, 150 и 152.2 Гражданского кодекса Российской Федерации (далее — ГК РФ) [5] и пр. Следовательно, охраняемая законом компьютерная информация — это вся подобная информация, если она имеет форму электрических сигналов; и именно эта информация, по смыслу статьи 272 УК РФ, и должна составлять предмет преступления. Сужение предмета преступления статьи 272 УК РФ, на наш взгляд, влечет существенное снижение качества государственной защиты этой категории правоотношений от преступных посягательств.

Таким образом, как мы видим, толкование понятия компьютерной информации, которое содержится в Рекомендациях и часто встречается в приговорах судов и материалах уголовных дел, не учитывает бланкетного характера статьи 272 УК РФ, а является толкованием примечания к ней. Кроме того, довольно часто правоприменитель не учитывает мнение, содержащееся в постановлении Конституционного Суда Российской Федерации от 26 октября 2017 года № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» [15], которым пункт 5 статьи 2 Федерального закона № 149 признан не противоречащим Конституции РФ. В нем, во-первых, Конституционный Суд признал лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, не противоречащим Конституции РФ, *обладателем информации*. Во-вторых, постановил, что передача подобной информации (а следовательно и иные действия с ней) вопреки запрету, установленному *правовыми*,

в том числе локальными, актами или договором, представляет собой нарушение прав и законных интересов обладателя информации. Это мнение полностью подтверждает сделанный нами вывод о бланкетном характере статьи 272 УК РФ.

Однако неверное определение объекта и предмета преступления в силу сужения бланкетной нормы не является единственной ошибкой правоприменителя. Еще об одной, о которой необходимо сказать, является определение дефиниции «компьютерная информация» в целом. Для ее описания требуется ответить на вопрос, какие именно действия должны включаться в объективную сторону преступления и какие последствия признаваться общественно-опасными.

Формулировка диспозиции части 1 статьи 272 УК РФ позволяет нам сделать очевидный вывод о том, что объективная сторона деяния полностью продиктована особой формой предмета преступления. Деяние, согласно диспозиции статьи, должно представлять из себя неправомерный доступ, который повлечет определенные последствия: уничтожение, блокирование, модификацию либо копирование компьютерной информации. Как мы уже отмечали выше, перечень последствий является исчерпывающим.

Исходя из процитированного постановления Конституционного Суда Российской Федерации, а также анализа норм Конституции РФ и иных норм права Российской Федерации, критерии неправомерности нами уже установлены — это нарушение запрета на получение доступа к компьютерной информации. Запрет может быть установлен законом, иным актом, в том числе локальным или правоприменительным, или договором. Последняя формулировка влечет за собой очень важное правовое последствие, которое становится очевидным только при рассмотрении его вкупе с понятием «компьютерная информация». Для этого нам вновь необходимо вернуться к содержанию этого термина.

Итак, *компьютерная информация* — это вид информации, выраженный в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В этой статье мы не будем уделять внимания технической обоснованности такого описания предмета преступления и его соответствия современному этапу развития инфор-

мационных технологий, поскольку вопреки устоявшемуся мнению [17, с. 656] для действия статьи 272 УК РФ в ее нынешнем виде это не имеет значения. С точки зрения уголовного права примечание 1 к статье 272 выполняет свою функцию и не ставит применение статьи в зависимость от определения устройства обработки и передачи компьютерной информации или тонкого клиента. Спорность формулировки, на наш взгляд, в другом, а именно, в проанализированном выше признаке «охраняемая законом» и его толковании, а также разграничении компьютерной информации на охраняемую и неохраняемую.

Анализируя Рекомендации, судебную практику и позиции ученых, мы должны отметить сформировавшееся устойчивое мнение о том, что охраняемая законом компьютерная информация — это та же информация (сведения, сообщения, данные), что охраняется законом в иных формах (визуальной, вербальной, письменной и пр.). На практике часто подразумевается, что это охраняемая информация, например, содержащая государственную тайну, только размещенная в компьютере или в ином равнозначном устройстве, в сети Интернет и т. д., которую законодатель назвал информацией в форме электрических сигналов, а современные источники чаще называют цифровой, компьютерной и т. д.

При этом, толкуя термин, правоприменитель часто полагает, что есть неохраняемая и охраняемая законом компьютерная информация. Здесь вступает в действие аналогия правоприменения, к примеру, положений об охраняемой законом тайне телефонных переговоров от незаконного вторжения. В этом случае незаконным будет считаться доступ к самим переговорам посредством технического или иного вторжения в телефонную сеть без наличия на то предусмотренных правовых и процессуальных оснований [13]. Простое физическое подслушивание речи говорящего по телефону лица другим лицом, скрывающимся за углом дома, таковым не признается. Граница, разделяющая охраняемую законом тайну вербальной информации от неохраняемой, а преступное посягательство от сомнительного, с моральной точки зрения действия проходит, в буквальном смысле, по телефонному проводу и подразумевает совокупность определенных правовых и технических признаков, устоявшихся

как в силу длительного существования телефонного общения, так и института его правовой охраны.

В случае с компьютерной информацией такой практики еще не возникло. Законодатель, а вслед за ним и правоприменитель, проводят аналогии с другими видами информации и не задаются вопросом, насколько это оправданно. Но от других видов компьютерная информация отличается несколькими существенными признаками, основным из которых (для толкования статьи 272 УК РФ) является осознанный характер ее размещения. Информация становится компьютерной в силу совершения ряда технических действий, так как она не может приобрести «форму электрических сигналов» самостоятельно, или в результате бессознательной деятельности человека. Законодатель внес в статью признак независимости компьютерной информации от средств ее хранения, обработки и передачи, однако не учел, что современные правоотношения в сфере информационных технологий подразумевают практически полную правовую определенность, установленную законом или договором.

Способы оборота компьютерной информации четко оговорены, равно как и способы ее обработки, передачи и, тем более, хранения. Даже если информация становится доступной в силу совершения преступления, технического сбоя, неосторожности пользователя или собственника, она все равно подлежит охране, а ее использование незаконно. Это означает, что в случае совершения преступления, предусмотренного статьей 272 УК РФ, вопрос о наличии либо отсутствии в составе предмета преступления должен решаться проведением правовой экспертизы и установлением признака «охраны законом» — в том смысле, в котором об этом заявил Конституционный Суд Российской Федерации, — относительно каждого вида компьютерной информации. Более того, учитывая сложность и многослойность современных цифровых технологий, которые сведены в статье 272 УК РФ к этому простому термину, пределы охраны могут (и должны) устанавливаться несколько раз применительно к одному и тому же объекту преступления.

Потому бесспорна третья проблема квалификации деяния по статье 272 УК

РФ. Если неправомерный доступ, т. е. само действие и способ его совершения, производны от вида компьютерной информации, то таковы и общественно-опасные последствия этого действия. Если опять обратиться к Рекомендациям, то там можно увидеть, что последствия определены довольно ясно. Под ними подразумевается следующее:

1) уничтожение информации — приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления;

2) блокирование информации — невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, т. е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

3) модификация информации — незаконное внесение изменений в компьютерную информацию (критерий незаконности определен в соответствии со статьей 1280 ГК РФ по формуле «от противного»);

4) копирование информации — создание копии имеющейся информации на другом носителе, т. е. перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, или воспроизведение информации в любой материальной форме — от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т. п.

Все сказанное подразумевает, что, вопреки, вопреки некоторым научным мнениям [7, с. 200] наступивший преступный результат должен охватываться умыслом субъекта преступления. Как совершенно верно указано в Рекомендациях, не будет иметь уголовно-правовых последствий действие, которое «осуществляется независимо от волеизъявления лица и, соответственно, в прямой причинной связи с его действиями не состоит». Во-вторых, как и способ совершения, так и наступившие последствия должны соответствовать виду компьютерной информации, ее техническим характеристикам и особенностям.

С учетом того, что, компьютерной становится любая информация, если ей придана соответствующая форма, то установление наличия либо отсутствия состава преступления в действиях лица целиком зависимо от этой формы. Этот вывод, основанный на всех вышеприведенных доводах, позволяет признать статью 272 УК РФ в ее нынешней редакции казуальной, т. е. требующей разъяснения ее смысла для каждого конкретного дела. Отсутствие такого толкования может привести как к неправомерному отказу в возбуждении уголовного дела, так и к привлечению к уголовной ответственности лица, в действиях которого нет состава преступления, либо им совершено иное деяние, запрещенное УК РФ.

Рассмотрим конкретный пример.

П. был 2 раза осужден за совершение преступления, предусмотренного частью 1 статьи 159 УК РФ, 2 раза — частью 2 статьи 159 УК РФ, и 5 раз — частью 2 статьи 272 УК РФ. Итого, по совокупности преступлений различными судами первой инстанции было вынесено 9 приговоров, признан рецидив преступлений. П. приговорен к 1 году 6 месяцам лишения свободы в колонии общего режима и двум штрафам по двадцать тысяч рублей каждый.

Согласно приговорам судов П., скопировав из выложенного в сети Интернет документа логины и пароли к электронной почте ряда лиц, использовал их, чтобы получить доступ к содержимому почтовых ящиков потерпевших. Изучив хранящуюся там информацию, он использовал ее при написании писем, в которых от имени владельцев паролей просил оказать материальную помощь. Сведения личного характера он использовал, чтобы ввести получателей писем в заблуждение относительно личности отправителя. Кроме того, П. осуществлял рассылку согласно перечню контактов использованных им почтовых ящиков. В итоге на счет, который П. указал в письме, один из получателей перевел сумму в 500 руб., иных преступных результатов все перечисленные действия не повлекли. П. был обвинен в совершении неправомерного доступа к компьютерной информации из корыстной заинтересованности, повлекшего модификацию этой информации, а также в совершении мошенничества группой лиц по предварительному сговору, поскольку счет, на

который переводили деньги, принадлежал другому лицу [1].

Анализируя это дело, мы можем заключить, что квалификация совершенных П. деяний изначально осуществлялась неправильно. Не подлежит сомнению, что, копируя логины и пароли, оказавшиеся в свободном доступе из-за нарушения безопасности почтового сервиса, П. намеревался использовать их для совершения мошенничества. Обман заключался во введении в заблуждение получателей писем относительно личности автора текста, а достоверность достигалась посредством использования обстоятельств, касающихся личной жизни потерпевших. При этом очевидно, что деяние П. состояло из двух действий:

- 1) получение незаконного доступа к содержимому переписки путем введения логина и пароля в адресные строки почтового клиента;

- 2) рассылка написанного текста согласно перечню контактов, хранившемуся в почтовом сервисе.

Действия не повлекли за собой никаких последствий для содержимого почтовых ящиков. Это подтверждается показаниями одной из потерпевших, указавшей, что факт «взлома» почты она обнаружила, лишь когда нашла в перечне отправленных сообщений письмо, которое не писала и не отправляла.

Учитывая, что причиненный вред составил 500 руб., переведенных на счет П., факт квалификации всех совершенных действий по отдельности, по части 1 и части 2 статьи 159 УК РФ уже является неверным, так как все действия совершались им в комплексе и охватывались единым умыслом. Кроме того, малозначительное деяние, хоть и содержащее в себе признаки мошенничества, не влечет уголовной ответственности [10], что было отдельно разъяснено в Пленуме Верховного Суда РФ в 2017 году.

Что касается квалификации по части 2 статьи 272 УК РФ, то мнение суда основано на заключении эксперта. Под модификацией суд подразумевал не только использование логинов и паролей, но и процесс написания и отправки электронных писем. Однако если мы опять обратимся к определению модификации, то увидим, что в него включены такие действия, как «внесение изменений». Ссылка на статью 1280 ГК РФ позволяет истолковать этот термин шире, согласно ко-

торой модификация осуществляется в трех видах: исправление явных ошибок; внесение изменений в программы, базы данных для их функционирования на технических средствах пользователя; частная декомпиляция программы для достижения способности к взаимодействию с другими программами. Для определения модификации согласно статье 272 УК РФ достаточно лишь, чтобы эти три вида действий были совершены незаконно. Но, как мы видим, П. их не совершал, названных последствий его деяние для содержащейся в почтовом сервисе информации не повлекло.

Таким образом, при квалификации деяния П. совершена ошибка, вызванная неправильным определением объекта преступления. Посчитав, что если действия были совершены с использованием почтового сервиса и связаны с получением доступа к информации в форме электронных сигналов, и приняв отправку электронного письма за модификацию компьютерной информации, суд счел, что речь идет о преступлении, запрещенном главой 28. Тогда как совершенно очевидно, что объектом этого преступления выступила тайна личной жизни, обстоятельства которой стали известны П. незаконно и которые он намеревался использовать для совершения мошенничества. То есть деяние должно было быть квалифицировано или по статье 137 УК РФ «Нарушение неприкосновенности частной жизни» или по статье 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» в зависимости от обстоятельств, которые были бы установлены в ходе расследования.

Приведенный пример как нельзя более наглядно демонстрирует всю сложность применения статьи 272 УК РФ на практике. Полагаем, что причина этой сложности заключается в намерении законодателя закрепить в качестве охраняемого правоотношение,

суть которого определена неверно. Диспозиция статьи 272 УК РФ даже в измененном виде наследует цель предыдущей ее версии, которая, в свою очередь, представляла собой аналог деяния, связанного с умышленным уничтожением или повреждением чужого имущества. Исключение составляла лишь форма такого имущества — «содержание» цифрового устройства, выделенное в качестве предмета преступления, которому действиями лица причиняется вред. Разрушительный или уничтожающий характер этого вреда не подлежит сомнению, потому что способ, которым преступление совершается, так или иначе влечет имущественный ущерб в силу наличия материальной ценности как у самой компьютерной информации, так и у ее носителей.

Следовательно, поднимая вопрос о проблемах защиты правоотношений в сфере компьютерной информации, нужно изначально исходить из вопроса возможности квалифицировать деяние в соответствии с той целью, с которой законодатель вводил статью в состав УК РФ. Как мы только что объяснили, достижение этой цели при применении статьи 272 проблематично, поскольку требует слишком большой совокупности знаний, как специальных, так и юридических. Сложность защиты правоотношений в сфере компьютерной информации заключается не только в эволюции технологий ее оформления и передачи, но и в эволюции самих правоотношений, кардинально изменившихся и с 1996, и с 2011 годов. Отсталость статьи 272 УК РФ и проблемы квалификации деяний по этой статье, существующие в современной судебной практике, не могут быть решены лишь изменением диспозиции состава. Учитывая, какой законодательный и правоприменительный пласт скрывается за простыми с виду терминами, проблема требует иного, гораздо более комплексного решения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Апелляционное постановление Свердловского областного суда от 18 декабря 2017 г. по делу № 22-9487/2017 // Архив суда.
2. Вехов В.Б. Преступления, связанные с неправомерным использованием баз данных и содержащейся в них компьютерной информации // Защита информации. Инсайд. — 2008. — № 2 (20). — С. 78 — 81.
3. Государственный стандарт Союза ССР ГОСТ 27201-87. Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования : постанов-

ление Госстандарта СССР от 28 января 1987 г. № 124 (в ред. от 1 мая 1988 г.). — М. : Изд-во стандартов, 1989.

4. Государственный стандарт СССР ГОСТ 15971-90. Системы обработки информации. Термины и определения : постановление Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698. — М. : Изд-во стандартов, 1991.

5. Гражданский кодекс Российской Федерации : федер. закон от 30 ноября 1994 г. № 51-ФЗ (в ред. от 3 августа 2018 г.) // Собрание законодательства РФ. — 1994. — № 32. — Ст. 3301; СПС «Консультант-Плюс».

6. Евдокимов К.Н. Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. — 2009. — № 2 (10). — С. 42 — 46.

7. Зайцев В.С., Горбань В.С. Проблемы квалификации преступления, предусмотренного ст. 272 УК РФ // Научное и образовательное пространство: перспективы развития : материалы III Междунар. науч.-практ. конф. (Чебоксары, 13 нояб., 2016 г.) : в 2 т. — Чебоксары, 2016. — Т. 2. — С. 200 — 201.

8. Захарцев С.И., Медведев В.Н., Сальников В.П. Снятие информации с технических каналов связи: правовые вопросы. — СПб. : Фонд «Университет», 2004. — 256 с.

9. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации : утв. Генпрокуратурой России // СПС «КонсультантПлюс».

10. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Российская газета. — 2017. — 11 дек.

11. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 18 марта 2019 г.) // ИПС «Гарант».

12. Об основах охраны здоровья граждан в Российской Федерации : федер. закон от 21 ноября 2011 г. № 323-ФЗ (в ред. от 6 марта 2019 г.) // Собрание законодательства РФ. — 2011. — № 48. — Ст. 6724; Официальный интернет-портал правовой информации www.pravo.gov.ru 06.03.2019.

13. Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации : определение Конституционного Суда РФ от 28 июня 2012 г. № 1253-О // www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1908262149012375988447029185&cacheid=55654D34919807BF5668DC89C6A51D0A&mode=splus&base=LAW&n=133029&rnd=09B87D08A61CE8B72A355AC9FEDCD4F8#07215043222330684 (дата обращения: 01.10.2018).

14. Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов : постановление Пленума Верховного Суда РФ от 13 декабря 2012 г. № 35 // Бюллетень Верховного Суда РФ. — 2013. — № 3.

15. По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова : постановление Конституционного Суда РФ от 26 октября 2017 г. № 25-П // ИПС «Гарант.РУ».

16. Старищев М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. — 2014. — № 1 (68). — С. 16 — 20.

17. Чирков П.А., Кашковский В.В. Российское уголовное право нуждается в уточнении объекта преступлений в сфере компьютерной информации // Сборник статей по материалам V Всероссийской научно-практической конференции / под ред. Н.В. Иванцовой, Н.М. Швецова. — 2015. — С. 655 — 659.

18. Шкиль Д.А., Китаева А.В. К вопросу о видах ответственности работников, допустивших распространение охраняемой законом информации // Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов : в 2 т. — Самара, 2018. — Т. 1. — С. 179 — 182.

REFERENCES (TRANSLITERATED)

1. Apellyacionnoe postanovlenie Sverdlovskogo oblastnogo suda ot 18 dekabrya 2017 g. po delu № 22-9487/2017 // Arhiv suda.

2. Vekhov V.B. Prestupleniya, svyazannye s nepravomernym ispol'zovaniem baz dannyh i sodержashchejsya v nih komp'yuternoj informacii // Zashchita informacii. Insajd. — 2008. — № 2 (20). — S. 78 — 81.

3. Gosudarstvennyj standart Soyuzs SSR GOST 27201-87. Mashiny vychislitel'nye elektronnye personal'nye. Tipy, osnovnye parametry, obshchie tekhnicheskie trebovaniya : postanovlenie Gosstandarta SSSR ot 28 yanvarya 1987 g. № 124 (v red. ot 1 maya 1988 g.). — M. : Izd-vo standartov, 1989.

4. Gosudarstvennyj standart SSSR GOST 15971-90. Sistemy obrabotki informacii. Terminy i opredeleniya : postanovlenie Gosudarstvennogo komiteta SSSR po upravleniyu kachestvom produkcii i standartam ot 26 oktyabrya 1990 g. № 2698. — M. : Izd-vo standartov, 1991.

5. Grazhdanskiy kodeks Rossijskoj Federacii : feder. zakon ot 30 noyabrya 1994 g. № 51-FZ (v red. ot 3 avgusta 2018 g.) // *Sobranie zakonodatel'stva RF*. — 1994. — № 32. — St. 3301; SPS «Konsul'tantPlyus».
6. *Evdokimov K.N.* Voprosy ugovolno-pravovoy kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii i ego ogranicheniya ot smezhnyh sostavov prestuplenij // *Vestnik Akademii General'noj prokuratury Rossijskoj Federacii*. — 2009. — № 2 (10). — S. 42 — 46.
7. *Zajcev V.S., Gorban' V.S.* Problemy kvalifikacii prestupleniya, predusmotrennogo st. 272 UK RF // *Nauchnoe i obrazovatel'noe prostranstvo: perspektivy razvitiya : materialy III Mezhdunar. nauch.-prakt. konf. (Cheboksary, 13 noyab., 2016 g.)* : v 2 t. — Cheboksary, 2016. — T. 2. — S. 200 — 201.
8. *Zaharcev S.I., Medvedev V.N., Sal'nikov V.P.* Snyatie informacii s tekhnicheskikh kanalov svyazi: pravovye voprosy. — SPb. : Fond «Universitet», 2004. — 256 s.
9. Metodicheskie rekomendacii po osushchestvleniyu prokurorskogo nadzora za ispolneniem zakonov pri rassledovanii prestuplenij v sfere komp'yuternoj informacii : utv. Genprokuratury Rossii // SPS «Konsul'tantPlyus».
10. O sudebnoj praktike po delam o moshennichestve, prisvoenii i rastrate : postanovlenie Plenuma Verhovnogo Suda RF ot 30 noyabrya 2017 g. № 48 // *Rossiyskaya gazeta*. — 2017. — 11 dek.
11. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii : feder. zakon ot 27 iyulya 2006 g. № 149-RF (v red. ot 18 marta 2019 g.) // IPS «Garant».
12. Ob osnovah ohrany zdorov'ya grazhdan v Rossijskoj Federacii : feder. zakon ot 21 noyabrya 2011 g. № 323-FZ (v red. ot 6 marta 2019 g.) // *Sobranie zakonodatel'stva RF*. — 2011. — № 48. — St. 6724; Oficial'nyj internet-portal pravovoj informacii www.pravo.gov.ru 06.03.2019.
13. Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Supruna Mihaila Nikolaevicha na narushenie ego konstitucionnyh prav stat'ej 137 Ugolovnogo kodeksa Rossijskoj Federacii : opredelenie Konstitucionnogo Suda RF ot 28 iyunya 2012 g. № 1253-O // www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1908262149012375988447029185&cacheid=55654D34919807BF5668DC89C6A51D0A&mode=splus&base=LAW&n=133029&rnd=09B87D08A61CE8B72A355AC9FEDCD4F8#07215043222330684 (data obrashcheniya: 01.10.2018).
14. Ob otkrytosti i glasnosti sudoproizvodstva i o dostupe k informacii o deyatelnosti sudov : postanovlenie Plenuma Verhovnogo Suda RF ot 13 dekabrya 2012 g. № 35 // *Byulleten' Verhovnogo Suda RF*. — 2013. — № 3.
15. Po delu o proverke konstitucionnosti punkta 5 stat'i 2 Federal'nogo zakona «Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii» v svyazi s zhaloboj grazhdanina A.I. Sushkova : postanovlenie Konstitucionnogo Suda RF ot 26 oktyabrya 2017 g. № 25-P // IPP «Garant.RU».
16. *Starichkov M.V.* Ponyatie «komp'yuternaya informaciya» v rossijskom ugovolnom prave // *Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennih del Rossii*. — 2014. — № 1 (68). — S. 16 — 20.
17. *Chirkov P.A., Kashkovskij V.V.* Rossijskoe ugovolnoe pravo nuzhdaetsya v utochnenii ob"ekta prestuplenij v sfere komp'yuternoj informacii // *Sbornik statej po materialam V Vserossijskoj nauchno-prakticheskoj konferencii / pod red. N.V. Ivancovoj, N.M. Shvecova*. — 2015. — S. 655 — 659.
18. *Shkil' D.A., Kitaeva A.V.* K voprosu o vidah otvetstvennosti rabotnikov, dopustivshih rasprostranenie ohranyaemoj zakonom informacii // *Materialy Mezhdunarodnoj nauchnoj konferencii ad'yunktov, aspirantov, kursantov i studentov* : v 2 t. — Samara, 2018. — T. 1. — S. 179 — 182.