ПЕСКОВ П. Д., ПОМНИНА С. Н.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 272 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье обозначены проблемы, возникающие на практике при квалификации неправомерного доступа к компьютерной информации. Авторы указывают причины, обусловливающие типичные ошибки в квалификации рассматриваемого деяния. В этой связи предложены варианты правильного применения уголовно-правовых норм.

Ключевые слова: неправомерный доступ, компьютерная информация, компьютерные преступления, преступления в области компьютерной информации.

PESKOV P. D., POMNINA S. N.

CURRENT ISSUES OF QUALIFICATION OF THE CRIME COVERED BY ARTICLE 272 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Abstract. The article outlines the problems that arise in practice when qualifying unauthorized access to computer information. The authors indicate the reasons that determine typical errors in qualifying the act in question and offer options for the correct application of criminal law norms.

Keywords: unauthorized access, computer information, cybercrime, crimes in the field of computer information.

Преступления в сфере компьютерной информации являются достаточно распространенной группой преступных деяний в структуре преступности в целом. Согласно данным ГИАЦ МВД России, за период январь-сентябрь 2024 года в сфере компьютерной информации всего было совершено 78376 преступлений (65419 – не раскрыты). Из них 78059 – преступления (65323 – не раскрыты), предусмотренные ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ) [23]. Вместе с тем, за период январь-декабрь 2023 года всего было совершено 37101 преступление (26094 – не раскрыты), из них – 36788 преступлений (26023 – не раскрыты), предусмотренных ст. 272 УК РФ [24]. То есть, согласно данным уголовной статистики, за девять месяцев 2024 года количество преступлений, связанных с компьютерной информацией, превысило общее количество преступлений, предусмотренных главой 28 УК РФ, совершенных в 2023 году, на 41275 (111,26%). Количественные показатели нераскрытых преступлений за указанный период увеличились на 39325 (150,73%) по сравнению с 2023 годом. Это подтверждает, что вопросы противодействия компьютерной преступности сегодня особенно актуальны.

Возрастающее количество преступных посягательств в сфере персональных данных обусловило принятие законопроекта № 502113-8 [5]. Сможет ли данная новелла в УК РФ стать эффективным инструментом в борьбе с киберпреступностью? Это станет ясно только со временем и в процессе ее практического применения. Однако, учитывая масштабное распространение преступлений, подпадающих под действие ст. 272 УК РФ, на данном этапе невозможно полностью исключить ошибки в правоприменении.

Ошибки в квалификации возникают, в том числе, вследствие особенностей конструкции ст. 272 УК РФ. Остановимся на некоторых из них. Так, проблемным является вопрос отграничения ст. 272 УК РФ и ст. 138 УК РФ. В доктрине и судебной практике можно обнаружить различные подходы к квалификации деяний, подпадающих под указанные нормы. Если их систематизировать, то можно выделить три варианта квалификации.

Во-первых, содеянное квалифицируется только по ст. 272 УК РФ или по совокупности с иными преступлениями, кроме предусмотренных ст. 138 УК РФ. Подобный вариант является наиболее распространенным в правоприменительной практике, поскольку преступления, предусмотренные ст. 272 УК РФ, часто выступают способом совершения других преступных деяний (например, ст.ст. 159, 183 УК РФ и т.д.).

Кроме того, формулировка диспозиции ч. 1 ст. 272 УК РФ позволяет охватить преступные деяния, совершаемые во многих сферах общественных отношений. Так, под действие данной нормы подпадают, например, такие действия как: 1) оформление сим-карт на имя потерпевшего без его личного ведома, совершенное из корыстных побуждений [14]; 2) вход в аккаунт потерпевшего без его ведома и разрешения с одновременным изменением данных для авторизации [17]; 3) установка на игровой консоли компьютерных программ, предназначенных для преодоления мер защиты от использования нелицензионного софта [22]; 4) вход в личный кабинет клиентов банка с использованием персональных данных потерпевшего для изменения кредитного лимита и дальнейшего хищения денежных средств [15]; 5) внесение за денежное вознаграждение заведомо ложных сведений о прохождении вакцинации от новой коронавирусной инфекции (COVID–19) в государственную информационную систему здравоохранения [16]; 6) подключение за денежное вознаграждение непубличных опций на абонентские номера потерпевших [20] и т.п.

Вместе с тем, на практике можно встретить ситуации, подобные следующей. Подсудимый, занимавший должность специалиста офиса ПАО «ВымпелКом», за денежное вознаграждение незаконно скопировал и передал неустановленному лицу сведения о детализации телефонных переговоров абонентов компании. Приговором Суксунского районного суда Пермского края от 18.11.2022 подсудимый признан виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, и ему назначено наказание в виде

ограничения свободы сроком на 1 год [21] (см. также приговор Самарского районного суда г. Самары от 18.08.2022 по делу № 1-139/2022 [18], приговор Серпуховского городского суда Московской области от 14.01.2019 по делу № 1-27/2019 [19]).

На наш взгляд, данная квалификация является недостаточной по следующим причинам. Содержанием компьютерной информации, неправомерный доступ к которой совершает виновный, в данном случае выступает детализация телефонных переговоров, которая, согласно п. 2 постановления Конституционного Суда РФ от 26.10.2017 № 25-П, составляет тайну телефонных переговоров [6]. Учитывая позицию Пленума Верховного Суда РФ, выраженную в п. 4 постановления от 25.12.2018 № 46 [9] и п. 16 постановления от 15.12.2022 № 37 [8], в этом случае квалификация деяния должна осуществляться по совокупности соответствующих частей ст.ст. 272 и 138 УК РФ. В науке уголовного права справедливо отмечается, что иной подход будет означать поглощение ч. 1 ст. 272 УК РФ предмета преступления, предусмотренного ч. 1 ст. 138 УК РФ, и наказание за неправомерный доступ к компьютерной информации должно быть больше, чем 2 года лишения свободы [2, с. 78].

Во-вторых, деяние квалифицируется только по ст. 138 УК РФ. Например, подсудимая, используя служебное положение и действуя из корыстных побуждений, скопировала и передала через мессенджер «Telegram» сведения о телефонных соединениях абонента компании. Постановлением Октябрьского районного суда г. Уфы от 23.09.2021 по делу № 1-386/2021 подсудимая была освобождена от уголовной ответственности за совершение преступления, предусмотренного ч. 2 ст. 138 УК РФ, с назначением судебного штрафа в размере 20 000 рублей [7].

Приведенный вариант квалификации также следует признать недостаточным. В уголовно-правовой доктрине имеется позиция, согласно которой квалификация только по ст. 138 УК РФ привела бы к значительному ослаблению ответственности и, ввиду этого, если санкция соответствующей статьи УК РФ ниже, чем санкция ст. 272 УК РФ во всех случаях необходимо квалифицировать данные преступления по совокупности [3, с. 160].

Квалификация исключительно в рамках ст. 138 УК РФ представляется возможной в случае, если она будет дополнена частью третьей, которая установила бы такой квалифицированный состав преступления, как «деяние, предусмотренное частью первой, совершенное путем неправомерного доступа к компьютерной информации». Однако это нецелесообразно, поскольку возникает проблема определения максимального размера наказания за содеянное. Более того, эта формулировка носит общий характер и не позволит индивидуализировать наказание лицу, взломавшему чей-либо аккаунт в социальной сети и ознакомившемуся с содержанием переписок, и лицу, занимающему должность специалиста в салоне сотовой связи и продавшему сведения о детализации телефонных соединений.

Общественная опасность этих деяний различна, как минимум по признаку использования виновным служебного положения. Всё же вариант квалификации по совокупности является наиболее оптимальным и соответствующим положению ч. 2 ст. 17 УК РФ.

В-третьих, деяние квалифицируется по совокупности ст.ст. 138 и 272 УК РФ. Так, подсудимый, будучи сотрудником салона сотовой связи, скопировал персональные данные и сведения о детализации телефонных переговоров абонентов компании. Приговором Автозаводского районного суда г. Нижнего Новгорода от 26.04.2022 по делу № 1-335/2022 подсудимый признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 138, ч. 3 ст. 272 УК РФ [11].

Таким образом, последний вариант квалификации является единственно верным и соответствующим положениям действующего уголовного законодательства. В то же время мы убедились, что, несмотря на имеющиеся разъяснения Пленума Верховного Суда РФ [8], в правоприменительной практике возникают сложности при юридической оценке судом действий подсудимых.

Следующая проблема заключается в правильном отграничении ст. 272 и ст. 274.1 УК РФ при квалификации преступных посягательств, совершенных работниками салонов связи. Необходимо отметить, что признаки состава преступления, предусмотренного ст. 274.1 УК РФ, уже становились предметом научного исследования [1]. В связи с этим целесообразно сделать акцент на проблемах, возникающих при рассмотрении уголовных дел в суде.

На практике возможна ситуация, когда деяния, соответствующие признакам преступления, предусмотренного ч. 1 или ч. 3 ст. 272 УК РФ, квалифицируются по ч. 2 или ч. 4 ст. 274.1 УК РФ соответственно. Основания такой квалификации исключительно формальные – причинение вреда информационной системе, базе данных и т.п., которые включены в реестр значимых объектов критической инфраструктуры Российской Федерации (далее – Реестр) без учета характера причиненного вреда. Так, подсудимый, будучи сервисным инженером ПАО «Ростелеком», по просьбе соседки, действуя из корыстной заинтересованности и используя учетные данные клиентов компании, подключил ее квартиру к сети «Интернет» и впоследствии внес данные о подключенной услуге в базы данных «Старт IP» и «Радиус». Приговором Ленинского районного суда г. Саранска от 31.01.2023 г. по делу № 1-65/2023 подсудимый признан виновным в совершении преступления, предусмотренного ч. 4 ст. 274.1 УК РФ и ч. 3 ст. 274.1 УК РФ [13].

Ключевым признаком, по которому следует отграничивать составы преступлений, предусмотренных ч. 4 ст. 274.1 УК РФ и ч. 3 ст. 272 УК РФ, является причинение вреда критической информационной инфраструктуре Российской Федерации (далее – КИИ РФ). Следовательно, суду надлежит не только указать на включение той или иной информационной

системы, содержащей компьютерную информацию, к которой совершен неправомерный доступ, в Реестр, но и описать, какой именно вред был причинен КИИ РФ, в чем он выражается.

Вместе с тем, в правоприменительной практике суды при описании вреда, причиненного КИИ РФ, нередко используют самые общие формулировки. Так, Ленинским районным судом г. Саранска в вынесенном приговоре указано, что причиненный вред выразился в модификации компьютерной информации, в результате чего в базах данных ПАО «Ростелеком», которые включены в Реестр, содержится недостоверная и необъективная информация [13]. Аналогичное описание можно обнаружить в приговоре Армянского городского суда Республики Крым от 19.10.2022 г. по делу № 1-89/2022, которым несколько лиц признаны виновными в совершении преступлений, предусмотренных ч. 4 ст. 274.1 УК РФ, в связи с внесением недостоверных сведений в государственную базу данных Минздрава России о вакцинированных от COVID-19 лицах [12]. В другом случае суд указал на нарушение безопасности информации и дискредитацию деловой репутации компании, которая владеет объектами, включенными в Реестр [10].

На наш взгляд, в обоснование причинения вреда КИИ РФ недостаточно сослаться на нахождение базы данных и подобных объектов в Реестре. Необходимо, чтобы этот вред был существенным (например, чтобы он создавал угрозу жизни и (или) здоровью неограниченного круга лиц).

Подобный подход будет соответствовать цели принятия Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», которую можно вывести из пояснительной записки к проекту указанного закона [4]: защита критической инфраструктуры от хакерских атак, сопоставимых с теми, что повлекли остановку центрифуг иранской атомной станции в сентябре 2010 года или паралич деятельности банков Южной Кореи в марте 2013 года.

В приведенных примерах обоснованным можно признать лишь приговор в отношении медработников из Республики Крым [12]. Это обусловлено тем, что внесение недостоверных сведений о вакцинированных от COVID-19 в период пандемии не только означает циркуляцию заведомо недостоверной информации в единой базе данных Минздрава России, но и является препятствием для объективной оценки масштабов распространения болезни, количества инфицированных, ставя под угрозу здоровье и жизни неограниченного круга лиц. В других приведенных случаях совершенные деяния необходимо было квалифицировать по ст. 272 УК РФ.

Следует также обратить внимание на то, что наказание за совершение преступления, предусмотренного ч. 4 ст. 274.1 УК РФ, составляет от 3 до 8 лет лишения свободы. В то же

время за совершение преступления, предусмотренного ч. 3 ст. 272 УК РФ, наказание в виде лишения свободы, во-первых, не является единственным основным возможным наказанием, и, во-вторых, срок лишения свободы, назначаемого за данное преступление, составляет до 5 лет. Таким образом, вследствие использования оценочных понятий (вред, причиненный КИИ РФ), отсутствия разъяснений высших судов по данной категории дел возникла ситуация, при которой виновным лицам, совершившим преступные деяния при аналогичных фактических обстоятельствах, может быть назначено несправедливое наказание по обозначенному формальному признаку.

В заключение можно констатировать, что вновь введенные в уголовный закон нормы, закрепляющие уголовную ответственность за преступные посягательства на КИИ РФ, лишь создали конкуренцию между статьями 272 и 274.1 УК РФ, которая является трудноразрешимой на практике. Мы считаем, что вместо осуществленной криминализации целесообразно было бы дополнить ст. 272 УК РФ квалифицированным составом, предусматривающим ответственность за «неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, если это деяние повлекло причинение существенного вреда критической информационной инфраструктуре Российской Федерации» (аналогично со ст.ст. 273 и 274 УК РФ); дать толкование существенного вреда и закрепить правила квалификации таких преступлений в постановлении Пленума Верховного Суда РФ от 15.12.2022 г. № 37.

Кроме того, в случае введения в УК РФ ст. 272.1 возникнет ситуация, когда большинство преступлений, связанных с неправомерным доступом к компьютерной информации, будут квалифицироваться по новой норме, поскольку в базах данных (мобильных операторов, различных государственных банках информации и т.п.) содержатся именно персональные данные граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Бражник С. Д. Технико-юридический анализ нормы о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Евразийское Научное Объединение. – 2019. – № 8-3 (54). – С. 198–201.

2. Винокуров В. Н. Пределы действия нормы, предусмотренной статьей 272 Уголовного кодекса РФ // Российский юридический журнал. – 2021. – № 4 (139). – С. 73–82.

3. Гребеньков А. А. Проблемы разграничения неправомерного доступа к компьютерной информации с другими составами преступлений // Известия Юго-Западного государственного университета. – 2012. – № 2-1. – С. 159–163.

4. О безопасности критической информационной инфраструктуры Российской Федерации: Законопроект № 47571-7 [Электронный ресурс]. – Режим доступа: https://sozd.duma.gov.ru/bill/47571-7 (дата обращения: 20.10.2024).
5. О внесении изменений в Уголовный кодекс Российской Федерации (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: Законопроект № 502113-8 [Электронный ресурс]. – Режим доступа: https: //sozd.duma.gov.ru/bill/502113-8#bh_e (дата обращения: 20.10.2024).
6. Постановление Конституционного Суда Российской Федерации № 25-П от 26 октября 2017 г. [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
7. Постановление Октябрьского районного суда г. Уфы Республики Башкортостан №1-386/2021 от 23.09.2021 [Электронный ресурс]. – Режим доступа: http: //www.consultant.ru (дата обращения: 20.10.2024).
8. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 г. [Электронный ресурс]. – Режим доступа: http: //www.consultant.ru (дата обращения: 20.10.2024).
9. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации: Постановление Пленума Верховного Суда Российской Федерации № 46 от 25 декабря 2018 г. [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
10. Приговор Абаканского городского суда Республики Хакасия № 1-805/2020 от 29.07.2020 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
11. Приговор Автозаводского районного суда города Нижнего Новгорода № 1-335/2022 от 11.05.2022 [Электронный ресурс]. – Режим доступа: http:// www.consultant.ru (дата обращения: 20.10.2024).
12. Приговор Армянского городского суда Республики Крым № 1-89/2022 от 19.10.2022 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
13. Приговор Ленинского районного суда города Саранска Республики Мордовия №1-

65/2023 от 31.01.2023 [Электронный ресурс]. – Режим доступа: http:// www.consultant.ru (дата обращения: 20.10.2024).
14. Приговор Ленинского районного суда города Саранска Республики Мордовия №1-372/2023 от 26.11.2023 [Электронный ресурс]. – Режим доступа: http:// www.consultant.ru (дата обращения: 20.10.2024).
15. Приговор Октябрьского районного суда города Рязани № 1-32/2023 от 23.06.2023 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
16. Приговор Первомайского районного суда города Пензы № 1-178/2022 от 07.06.2022 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
17. Приговор Пролетарского районного суда города Саранска Республики Мордовия № 1-186/2021 от 29.06.2021 [Электронный ресурс]. – Режим доступа: http:// www.consultant.ru (дата обращения: 20.10.2024).
18. Приговор Самарского районного суда города Самары № 1-139/2022 от 18.09.2022 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
19. Приговор Серпуховского городского суда Московской области № 1-27/2019 от 14.01.2019 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
20. Приговор Советского районного суда города Нижнего Новгорода № 1-410/2023 от 22.11.2023 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
21. Приговор Суксунского районного суда Пермского края № 1-64/2022 от 18.10.2022 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
22. Приговор Тамбовского районного суда Тамбовской области № 1-46/2023 от 08.02.2023 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (дата обращения: 20.10.2024).
23. Состояние преступности в России за январь-сентябрь 2024 г. [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/56672721/ (дата обращения: 10.11.2024).
24. Состояние преступности в России за январь-декабрь 2023 г. [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/47055751/ (дата обращения: 10.11.2024).