Вестник Томского государственного университета. Право. 2022. № 44. С. 5–16
Tomsk State University Journal of Law. 2022. 44. pp. 5–16

Проблемы публичного права

Научная статья
УДК 343.3/.7
doi: 10.17223/22253513/44/1

К вопросу об общественной опасности неправомерного доступа к компьютерной информации

Антон Геннадьевич Антонов[1], Елена Андреевна Зорина[2], Дмитрий Витальевич Крюков[3]

[1, 3] Ленинградский государственный университет им. А.С. Пушкина, Санкт-Петербург, Россия
[2] Санкт-Петербургский университет государственной противопожарной службы, Санкт-Петербург, Россия
[1] antonovanton1@mail.ru
[2] zorina_lena@mail.ru
[3] kryukov48@mail.ru

Аннотация. Исследуется общественная опасность неправомерного доступа к компьютерной информации, в том числе характер причинения таким деянием вреда общественным отношениям и угрозы его причинения. Обосновывается тезис, что такие последствия неправомерного доступа к компьютерной информации, как копирование, блокирование, модификация или уничтожение, сами по себе не всегда являются общественно опасными. Общественная опасность этого преступления проявляется в «кумулятивном эффекте» – способности повлечь за собой причинение вреда другим объектам уголовно-правовой охраны.

Ключевые слова: общественная опасность, неправомерный доступ, компьютерная информация, кумулятивная опасность, копирование, модификация, блокирование, уничтожение компьютерной информации

Для цитирования: Антонов А.Г., Зорина Е.А., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестник Томского государственного университета. Право. 2022. № 44. С. 5–16. doi: 10.17223/22253513/44/1

Problems of the public law

Original article
doi: 10.17223/22253513/44/1

On the public danger of illegal access to computer information

Anton G. Antonov[1], Elena A. Zorina[2], Dmitry V. Kryukov[3]

[1, 3] *Leningrad State University named after A.S. Pushkin, St. Petersburg, Russian Federation*
[2] *Saint Petersburg University of the State Fire Service, St. Petersburg, Russian Federation*
[1] *antonovanton1@mail.ru*
[2] *zorina_lena@mail.ru*
[3] *kryukov48@mail.ru*

Abstract. The article examines the public danger of unauthorised access to computer information, including the nature of the damage caused by such an act to social relations and the threat of its infliction. The authors of the article consider that consequences of illegal access to computer information, such as copying, blocking, modification or destruction are not always socially dangerous. Public danger of this crime lies in its "cumulative effect" – its ability to cause damage to other objects of criminal protection. At the same time, the nature and degree of social danger of encroaching on information does not depend on the fact that it is in electronic form, but on its content and value. The authors conducted a sociological survey, according to which a significant proportion of the population recognises the danger of computer crimes as insignificant. The analysis of judicial practice reveals that the harm caused by such crimes is, in most cases, insignificant. The negative consequences for the convicted person, expressed in the imposition of a real sentence and a criminal record, are disproportionate to the extent of the harm caused. This raises doubts as to the validity of the criminalisation of the act under Article 272 of the Criminal Code of the Russian Federation.

Public danger of the crime provided for by part 1 of article 272 of the Criminal Code of the RF consists in the ability to cause harm to public relations and in the threat of committing other crimes. Therefore, we refer it to the crimes of cumulative danger, public danger of which increases due to the cumulative effect - the potential probability of causing harm to other objects of criminal-legal protection. In this case, the considered crimes will have public danger in case of infliction of substantial harm to public relations, which, in fact, causes its further development.

In such circumstances, there are reasonable doubts as to whether the criminalization of the deed stipulated by part 1 of article 272 of the Criminal Code of the RF as an independent crime is justified. At the same time, if we refer to the Code on Administrative Offences of the Russian Federation, in it can be found such unlawful acts, the public danger of which is more obvious. These include, for example, violation of sanitary and epidemiological requirements for drinking water, as well as drinking and domestic water supply (article 6.5), concealment by a person suffering from HIV or venereal disease of the source of infection (article 6.1), non-compliance with the rules and regulations on prevention and liquidation of emergency situations (article 20.6).

Keywords: public danger, illegal access, computer information, cumulative danger, copying, modification, blocking, destruction of computer information

For citation: Antonov, A.G., Zorina, E.A. & Kryukov D.V. (2022) On the public danger of illegal access to computer information. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo – Tomsk State University Journal of Law.* 44. pp. 5–16. (In Russian). doi: 10.17223/22253513/44/1

Информация, обрабатываемая с помощью электронно-вычислительной техники, как объект законодательного регулирования в отечественное правовое поле попала сравнительно недавно. Несмотря на бурное развитие компьютерных технологий и информационно-коммуникационных сетей, преступления в сфере компьютерной информации, предусмотренные Главой 28 Уголовного кодекса Российской Федерации (УК РФ), явление относительно нераспространенное. В производстве районных судов Российской Федерации за период с 2015 г. по настоящее время, по данным ГАС «Правосудие» [1], находилось лишь 2 156 уголовных дел по обвинению в преступлениях, предусмотренных статьями данной главы УК РФ. При этом приговоры вынесены лишь по 1 160 делам. Если говорить о ст. 272 УК РФ, то за пятилетний период в производстве судов находилось 1 128 уголовных дел по обвинению в преступлении, предусмотренном данной статьей, и по таким делам было вынесено лишь 622 приговора. Для сравнения, за этот же период в производстве судов находилось по одной только ст. 158 УК РФ (кража) более 990 тыс. уголовных дел, по которым вынесено более 540 тыс. приговоров.

Вместе с тем законодатель, криминализуя соответствующие деяния, признает их общественно опасными. Несомненно, в XXI в. значимость компьютерной информации сложно переоценить, и общественные отношения в сфере безопасности компьютерной информации нуждаются в уголовно-правовой охране. Однако формирование и формулирование уголовно-правовых запретов в данной области не могут строиться без учета характера и степени общественной опасности деяний.

Как известно, общественная опасность преступления проявляется в двух формах: причинении существенного вреда общественным отношениям, охраняемым уголовным законом, или создании угрозы причинения такого вреда [2. С. 107]. Преступление «не только как уже произошедшее нарушение общественных отношений, но и как источник опасности, грозящей охраняемому уголовным правом объекту, опасности, реализацию которой во многих случаях еще можно предотвратить» [3. С. 44].

Тем самым при совершении преступления его общественная опасность реализуется относительно нарушенных общественных отношений, которым причинен вред или создана угроза его причинения. При этом она продолжает развиваться относительно аналогичных нарушенных общественных отношений и относительно всех общественных отношений, входящих в сферу уголовно-правовой охраны.

Таким образом, преступление в случае его совершения не только общественно опасно, но и общественно вредно. Вред следует рассматривать как результат реализации общественной опасности преступления относительно нарушенных общественных отношений. Опасность же остается таковой применительно к ненарушенным общественным отношениям. Очевидно, поэтому категория вреда отличается от категории опасности. Вред – это явление, состоявшееся в сущности, а опасность – вероятность наступления вреда в будущем. Опасность – однопорядковое понятие категории «угро-

за». Угроза причинения вреда общественным отношениям является не только результатом реализации общественной опасности преступления, но и ее частным проявлением. Следовательно, данную категорию необходимо рассматривать в узком и широком смыслах. В первом случае имеет место угроза причинения вреда конкретным ненарушенным общественным отношениям как последствие преступления и вред нарушенным общественным отношениям. Во втором случае можно констатировать наличие угрозы всем или аналогичным общественным отношениям в случае нарушения уголовно-правового запрета. Опасность применительно к аналогичным нарушенным общественным отношениям наступает при совершении преступления, до этого она сохраняется для всех общественных отношений, находящихся под уголовно-правовой охраной.

Общественная опасность преступления в широком смысле слова состоит:

1. В угрозе (вероятности) повторения конкретного преступления (его прецедентности) или любого другого преступления. Поэтому преступление не только причиняет конкретный вред (например, здоровью потерпевшего) – оно еще и общественно опасно. Если же исходить только из состоявшегося вреда конкретным общественным отношениям, то останутся непонятными основания наказуемости некоторых преступлений (например, предусмотренных ст. 222 УК РФ). Опасность заключается и в том, что преступление представляет собой элемент негативной социальной практики, имеющий прецедентный характер, в том, что общество способно воспринять его как возможный вариант поведения в случае, если государство не даст ему отрицательной оценки [4. С. 8–9].

2. В угрозе совершения дополнительного, смежного преступления. Общественная опасность одних преступлений заключается лишь в возможности повторения аналогичных деяний другими людьми. К таковым относится, например, кража. Здесь общественная опасность нашла свою полную реализацию в виде причинения ущерба собственнику и не предполагает дальнейшего развития. Условно обозначим ее простой. Другие преступления предполагают второй уровень опасности, заключая в себе возможность развития цепочки событий, которая может повлечь не только повторение преступления, но и совершение нового преступления как результат продолжения начатой преступной деятельности, причем второе преступление может быть гораздо более тяжким, нежели первое. Прибегнув к технической терминологии, условно отнесем такие противоправные деяния к преступлениям кумулятивной опасности. С одной стороны, они опасны тем, что как элемент социальной практики могут быть повторены, с другой – тем, что имманентно содержат опасность совершения иного, более тяжкого преступления. К примеру, при неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ), с одной стороны, опасность состоит в том, что окружающие видят, что можно совершать указанные деяния (например, блокировать компьютерную информацию), а с другой – в том, что эти дея-

ния могут причинить существенный вред общественным отношениям (это отражено в квалифицирующих признаках рассматриваемой нормы).

Из позиций такого понимания общественной опасности преступления мы будем исходить и при дальнейшем изложении вопроса относительно состава преступления, предусмотренного ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), которое относится к преступлениям в сфере компьютерной информации. Вместе с тем для более полного анализа необходимо выяснить, признает ли население такие деяния общественно опасными.

Согласно проведенному опросу, такие деяния, как копирование, изменение или удаление компьютерной информации без разрешения владельца, признают общественно опасными 81,7% респондентов, 18,3% назвали таковые неопасными для общества. Создание компьютерных «вирусов», их использование и распространение также большинством респондентов было признано общественно опасными: 83,7% против 16,3%. Несанкционированный доступ к компьютерной информации, «взлом» чужих аккаунтов и подобные деяния общественно опасными признали 78,7% опрошенных. Противоположную точку зрения заняли лишь 21,3% респондентов.

Какое положение общественная опасность преступлений в сфере компьютерной информации занимает относительно других преступлений? Для ответа на этот вопрос респондентам было предложено распределить по уровням общественной опасности не только компьютерные преступления, но и иные общественно опасные деяния. Так, чрезвычайно опасными были признаны террористический акт, похищение человека, захват заложника (к таковым их отнесли 93,9% опрошенных). Немного меньше респондентов отнесли к таковым убийства и причинение вреда здоровью человека (89,8%) и примерно столько же (87,8%) респондентов признали чрезвычайно опасным намеренное заражение ВИЧ-инфекцией или венерическим заболеванием.

Что касается предмета нашего исследования, компьютерные преступления признали наименее опасными или совершенно не опасными для общества деяниями примерно 20% опрошенных. Большинство же признают такие деяния опасными для общества. Однако очевидно, что в сравнении с иными преступными деяниями компьютерные преступления часто представляются обычному человеку наименьшим из зол.

В чем же заключается общественная опасность преступления в сфере компьютерной информации, предусмотренного ст. 272 УК РФ? Как отмечалось ранее, общественная опасность преступления проявляется в двух формах: реальном причинении вреда и возникновении реальной угрозы его причинения. С этих позиций ст. 272 УК РФ не является исключением. Общественная опасность этого преступления заключается в реальном причинении вреда общественным отношениям и опасности его повторения (прецедентности).

Часть 1 ст. 272 УК РФ закрепляет уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо ко-

пирование компьютерной информации. Общественная опасность данного деяния не является завершенной и предполагает свое дальнейшее развитие. Такой вид общественной опасности мы относим к кумулятивному по следующим причинам.

Данное преступление можно признать оконченным только тогда, когда неправомерный доступ к определенной компьютерной информацией повлек определенные последствия в виде конкретного вреда общественным отношениям: уничтожение, копирование, блокирование, модификацию компьютерной информации. При этом общественная опасность преступления не находит в данном случае своей полной реализации. Перспектива такой реализации отражена в квалифицирующих признаках ст. 272 УК РФ. Так, например, общественная опасность рассматриваемого преступления может найти свое завершение при причинении крупного ущерба и наступлении тяжких последствий.

Уголовный закон не раскрывает значения терминов «уничтожение», «копирование», «блокирование» и «модификация» компьютерной информации. Однако, согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» Генеральной прокуратуры Российской Федерации (далее – Методические рекомендации) уничтожение компьютерной информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления [5]. Вред в таком случае выражается в физической утрате информации. Если следовать данной логике, даже если информация может быть восстановлена, она считается уничтоженной. Однако в случае ее восстановления физические, осязаемые последствия исчезают. Поэтому если и говорить о вреде, то уничтожением компьютерной информации стоит признавать только ее утрату без возможности восстановления. Соответственно, вред, причиняемый преступлением, выражается в безвозвратной утрате компьютерной информации. Однако в таком случае встает резонный вопрос: как определить ту самую «безвозвратность»? Представим себе простую ситуацию.

Если документ, удаленный с компьютера, был цифровой копией бумажного документа, то формально компьютерная информация была уничтожена. Вместе с тем бумажный, «аналоговый» вариант никуда не исчез и, более того, может быть скопирован в память компьютера заново. С технической точки зрения, это будет уже новый цифровой документ, хотя и содержание его будет тем же, и создать новый документ с помощью сканера не составит труда. В этом случае безвозвратно компьютерная информация не была утрачена. Безвозвратность имела бы место при отсутствии бумажного, физического варианта информации. В последнем случае общественная опасность деяния налицо. Только при таком развитии событий общественная опасность исследуемого преступления находит свое отражение, но не завершение. Ведь далее она может получить развитие относительно ряда других общественных отношений. Например, уничтожение

информации по уголовному делу в электронном виде наносит ущерб правосудию и может являться отдельным преступлением.

Блокирование информации, согласно Методическим рекомендациям, – это результат воздействия на компьютерную информацию или технику, последствием которого является 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. Такая формулировка довольно спорна, особенно в части, где под блокированием понимается невозможность постоянно совершать операции над информацией, поскольку в таком случае с точки зрения пользователя нет никакой разницы с уничтожением информации. Если же говорить о временном нарушении доступа к информации, то, по сути, вред в таком случае отсутствует ввиду возможности восстановления доступа к информации и дальнейшего ее использования. Иными словами, преступным последствием признаются некие временные неудобства, связанные с доступом к информации, и не более того.

Осужденный в 2015 г. Сарапульским городским судом Удмуртской Республики гражданин Ш. на почве личных неприязненных отношений с помощью заранее известных ему логина и пароля зашел в аккаунт своей подруги в социальной сети и выложил там ее фотографию интимного содержания, после чего поменял пароль, заблокировав ей доступ к странице. Подсудимый был признан виновным в совершении неправомерного доступа к компьютерной информации, повлекшего ее модификацию и блокирование (ч. 1 ст. 272 УК РФ), и ему было назначено наказание в виде штрафа в размере 20 тыс. руб. При этом мера пресечения в виде подписки о невыезде была оставлена без изменения до вступления решения суда в законную силу [6].

Всем пользователям социальных сетей известно, что в случае «взлома» страницы у владельца аккаунта есть абсолютно реальная возможность восстановить доступ к заблокированной странице с помощью номера телефона или адреса электронной почты, на которые высылается либо новый пароль, либо ссылка, пройдя по которой пользователь устанавливает свой пароль. Описанный выше пример иллюстрирует крайне неприятную с этической точки зрения ситуацию. Однако для восстановления социальной справедливости в таких случаях имеется гражданско-правовой механизм, а именно предъявление иска о защите чести и достоинства. Сама же процедура восстановления доступа к своей странице и удаления неприемлемого контента занимает не более пяти минут и не требует особых усилий от пострадавшего.

Таким образом, встает вопрос о соразмерности правовых последствий для самого осужденного и степени нанесенного им вреда. Осужденному назначено реальное наказание в виде штрафа, а самое главное – оно влечет

судимость, которая, в соответствии с п. «б» ч. 3 ст. 86 УК РФ, погашается лишь по истечении года после исполнения наказания. В данном случае поражение в правах осужденного выглядит намного более весомым в сравнении с последствиями его деяния, что явно противоречит принципу справедливости, установленному ст. 6 УК РФ. Если предположить, что блокируется не компьютерная информация... Один студент взял и не отдает другому дневник (содержащий сведения о личной жизни) в течение двадцати минут. Информация заблокирована. Есть ли здесь общественная опасность? В связи с этим сам по себе неправомерный доступ к компьютерной информации, повлекший ее блокирование, не всегда может свидетельствовать о наличии общественной опасности. Таковую можно рассматривать при причинении существенного ущерба общественным отношениям, который напрямую зависит от ценности и востребованности заблокированной информации. Общественная опасность в данном случае является кумулятивной. Это отражено в квалифицирующих признаках ст. 272 УК РФ, которые предусматривают, наряду с другими, тяжкие последствия или причинение крупного ущерба в результате совершения преступления. При этом блокирование компьютерной информации может повлечь совершение другого преступления. Например, мошенничества.

Под модификацией информации в упомянутом документе понимается внесение изменений в компьютерную информацию (или ее параметры). Однако всякая ли модификация компьютерной информации общественно опасна? Показателен в этом смысле следующий пример.

В 2016 г. Волжский городской суд Волгоградской области рассматривал уголовное дело в отношении бывшего администратора сайта, который, использовав имевшиеся у него логин и пароль, разместил на этом сайте изображение флага с арабской вязью. При этом деяние не было совершено из каких-либо экстремистских побуждений и не имело целью разжигание национальной розни. Подсудимый был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ, ему был назначен штраф в размере 20 тыс. руб. [7].

Конечно, своими действиями обвиняемый модифицировал компьютерную информацию, однако эти действия вряд ли можно признать общественно опасными, поскольку сама по себе демонстрация такого флага в отсутствие каких-либо экстремистских побуждений не может расцениваться как преступление, и нельзя увязывать наличие вреда лишь с тем фактом, что такая демонстрация осуществлена посредством размещения на сайте в сети Интернет. Достаточно представить, что то же самое было проделано «в офлайне»: если бы, например, подсудимый вывесил этот флаг, допустим, на стене у парадной собственного многоквартирного дома со стороны улицы. Эффект абсолютно тот же: любой прохожий видит этот флаг, однако владелец этого флага не несет за свои действия уголовной ответственности.

Исходя из кумулятивного характера общественной опасности рассмотренного деяния, можно сделать вывод о том, что таковая появляется в слу-

чае существенной модификации информации, представляющей какую-либо ценность. При этом модификация ценной и значимой информации может повлечь существенный вред другим объектам уголовно-правовой охраны. Например, модификация базы данных для проведения выборов различного уровня может повлечь нарушение конституционных прав человека и гражданина, т.е. обусловить совершение другого преступления.

Копирование информации, согласно Методическим рекомендациям, – это создание копии имеющейся информации на другом носителе, т.е. перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – «от руки», фотографированием текста с экрана дисплея, а также считывание информации путем любого ее перехвата и т.п.

В данном случае общественная опасность заключается в том, что компьютерная информация становится доступной третьим лицам. Действительно, в электронном виде сейчас записано множество конфиденциальных данных: личная переписка, пароли от банковских карт, персональные данные. Но в таком случае общественная опасность заключается не только в копировании информации как таковом, но и в потенциальной возможности нанести вред иным общественным отношениям. То есть общественная опасность копирования информации видоизменяется, когда оно выступает в качестве способа причинения существенного вреда общественным отношениям.

Октябрьским районным судом г. Архангельска в 2017 г. был вынесен приговор в отношении К. Молодой человек поссорился со своей подругой и, найдя дома ее ноутбук с незакрытыми страницами в соцсети и электронной почте, скопировал ее личную переписку на флеш-карту, после чего разослал эту переписку и личные фотографии потерпевшей ее знакомым и коллегам. Умысел К. был направлен на нарушение неприкосновенности частной жизни и нарушение тайны переписки, что и было установлено судом. Вместе с тем государственное обвинение квалифицировало его действия не только по ст. 137 и 138 УК РФ, но и по ч. 1 ст. 272 УК РФ, поскольку подсудимым был осуществлен неправомерный доступ к компьютерной информации, повлекший ее копирование. Однако суд признал подсудимого виновным только в совершении нарушения неприкосновенности частной жизни и нарушении тайны переписки, в отношении других деяний был постановлен оправдательный приговор. При этом суд в мотивировочной части приговора указывает, что неправомерный доступ к компьютерной информации и ее копирование имели место, однако «взлома» аккаунта с помощью специальных программных инструментов подсудимый не осуществлял, что позволяет в этой части постановить оправдательный приговор [8].

Явный кумулятивный характер общественной опасности рассмотренного преступления не свидетельствует о том, что любое копирование информации можно считать общественно опасным. Сама по себе скопированная информация должна представлять собой достаточную ценность для при-

знания деяния преступным без наступления каких-либо дополнительных последствий в виде ущерба другим объектам уголовно-правовой охраны.

Тем самым неправомерный доступ к компьютерной информации, повлекший ее уничтожение, блокирование, модификацию или копирование, условно можно отнести к виду преступлений кумулятивной опасности, т.е. таким, которые влекут за собой, с определенной степенью вероятности обусловливают совершение другого преступления. При этом сами деяния, закрепленные в ч. 1 ст. 272 УК РФ, могут и не обладать общественной опасностью в полном понимании этой категории, не всегда могут причинять существенный вред общественным отношениям. Чтобы это определить, необходимы дополнительные исследования относительно ценности компьютерной информации. Видимо, этим и объясняется отношение значительного количества опрошенных, которые признали компьютерные преступления наименее опасными или совершенно не опасными. Поэтому необходимо учесть, что информация может представлять разную ценность, в том числе и для самого потерпевшего, и именно поэтому от ценности такой информации зависит и общественная опасность преступления.

Неочевидность общественной опасности проявляется в ч. 1 ст. 272 УК РФ, однако она приобретает зримые очертания благодаря квалифицирующим признакам, где в качестве общественно опасных последствий отражены, например, причинение крупного ущерба или наступление тяжких последствий. Отсюда и вытекает такой вид общественной опасности рассматриваемого преступления, как кумулятивная общественная опасность. Она характеризуется высоким негативным потенциалом. Этот потенциал направлен на другие общественные отношения, помимо тех, которые были затронуты совершенным преступлением. То есть преступное посягательство на один объект уголовно-правовой охраны потенциально влечет посягательство на другой объект: например, незаконное копирование информации может повлечь нарушение неприкосновенности частной жизни, нарушение авторских и прав, мошенничество или вымогательство.

Если в данном случае взаимосвязь общественной опасности преступления, предусмотренного ч. 1 ст. 272 УК РФ, с указанными деяниями очевидна, то ее взаимосвязь с преступлениями против общественной безопасности представить гораздо сложнее. Однако такая ситуация вполне возможна. Например, преступник вполне может «взломать» чужой аккаунт в соцсети или электронную почту для того, чтобы совершить заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ).

Таким образом, общественная опасность преступления, предусмотренного ч. 1 ст. 272 УК РФ, состоит в способности причинять вред общественным отношениям и в угрозе совершения иных преступлений. Поэтому мы относим его к преступлениям кумулятивной опасности, общественная опасность которых усиливается за счет кумулятивного эффекта – потенциальной вероятности причинения вреда иным объектам уголовно-правовой охраны. При этом рассмотренные преступления будут обладать общественной опасностью в случае причинения существенного вреда об-

щественным отношениям, который, собственно, и обусловливает дальнейшее ее развитие.

В таких обстоятельствах возникают разумные сомнения относительно того, насколько оправдана криминализация деяния, предусмотренного ч. 1 ст. 272 УК РФ, как самостоятельного преступления. При этом если обратиться к Кодексу Российской Федерации об административных правонарушениях, то в нем можно найти такие противоправные деяния, общественная опасность которых более очевидна. К таким можно отнести, допустим, нарушение санитарно-эпидемиологических требований к питьевой воде, а также к питьевому и хозяйственно-бытовому водоснабжению (ст. 6.5), сокрытие лицом, больным ВИЧ-инфекцией, венерическим заболеванием, источника заражения (ст. 6.1), невыполнение требований норм и правил по предупреждению и ликвидации чрезвычайных ситуаций (ст. 20.6).

Список источников

1. ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru/bigs/portal.html (с применением фильтров поиска: «дела федеральных судов общей юрисдикции», «уголовные дела», «дата поступления», «статья УК», «результат»).

2. Уголовное право. Общая часть : учеб. пособие / под общ. ред. В.А. Уткина, А.В. Шеслера. Томск : Издательский Дом Томского государственного университета, 2016.

3. Филимонов В.Д. Охранительная функция уголовного права. СПб. : Юрид. центр Пресс, 2003.

4. Фефелов П.А. Принципы советского уголовного права – основа уголовно-правового охранительного механизма : автореф. дис. ... д-ра юрид. наук. М., 1978.

5. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). URL: http://genproc.gov.ru/documents/nauka/execution/document-104550/

6. Приговор Сарапульского городского суда Удмуртской Республики по уголовному делу № 1-261/2015 от 09.09.2015 // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru/bigs/portal.html

7. Приговор Волжского городского суда Волгоградской области по уголовному делу № 1-1105/2016 от 17.11.2016 // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru/bigs/portal.html

8. Приговор Октябрьского районного суда г. Архангельска по делу 1-22/2017 от 13.02.2017 // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru/bigs/portal.html

References

1. *The State Automated System of the Russian Federation "Pravosudie"*. [Online] Available from: https://bsr.sudrf.ru/bigs/portal.html.

2. Utkin, V.A. & Shesler, A.V. (eds) (2016) *Ugolovnoe pravo. Obshchaya chast'* [Criminal Law. General Part]. Tomsk: Tomsk State University.

3. Filimonov, V.D. (2003) *Okhranitel'naya funktsiya ugolovnogo prava* [Protective Function of Criminal Law]. St. Petersburg: Yurid. tsentr Press.

4. Fefelov, P.A. (1978) *Printsipy sovetskogo ugolovnogo prava – osnova ugolovno-pravovogo okhranitel'nogo mekhanizma* [Principles of Soviet criminal law – the basis of the criminal law protective mechanism]. Abstract of Law Dr. Diss. Moscow.

5. Prosecutor General's Office of Russia. (n.d.) *Metodicheskie rekomendatsii po osushchestvleniyu prokurorskogo nadzora za ispolneniem zakonov pri rassledovanii*

prestupleniy v sfere komp'yuternoy informatsii (utv. Genprokuraturoy Rossii) [Guidelines for the implementation of prosecutorial supervision over the execution of laws in the investigation of crimes in the field of computer information (approved by the Prosecutor General's Office of Russia)]. [Online] Available from: http://genproc.gov.ru/documents/nauka/execution/document-104550/

6. The Udmurt Republic. (2015) *Prigovor Sarapul'skogo gorodskogo suda Udmurtskoy Respubliki po ugolovnomu delu № 1-261/2015 ot 09.09.2015* [The verdict of the Sarapul city court of the Udmurt Republic in Criminal Case No. 1-261/2015 of September 9, 2015]. [Online] Available from: https://bsr.sudrf.ru/ bigs/portal.html

7. The Volgograd Region. (2016) *Prigovor Volzhskogo gorodskogo suda Volgogradskoy oblasti po ugolovnomu delu № 1-1105/2016 ot 17.11.2016* [The verdict of the Volzhsky City Court of Volgograd Region in Criminal Case No. 1-1105/2016 dated November 17, 2016]. [Online] Available from: https://bsr.sudrf.ru/ bigs/portal.html

8. Arkhangelsk. (2017) *Prigovor Oktyabr'skogo rayonnogo suda g. Arkhangel'ska po delu 1-22/2017 ot 13.02.2017* [Sentence of the Oktyabrsky District Court of Arkhangelsk in Case 1-22/2017 dated February 13, 2017]. [Online] Available from: https://bsr.sudrf.ru/ bigs/portal.html

Информация об авторах:

Антонов А.Г. – доктор юридических наук, доцент, профессор кафедры уголовного права и процесса Ленинградского государственного университета им. А.С. Пушкина (Санкт-Петербург, Россия). E-mail: antonovanton1@mail.ru

Зорина Е.А. – кандидат юридических наук, доцент, начальник кафедры трудового права Санкт-Петербургского университета государственной противопожарной службы (Санкт-Петербург, Россия). E-mail: zorina_lena@mail.ru

Крюков Д.В. – аспирант кафедры уголовного права и процесса Ленинградского государственного университета им. А.С. Пушкина (Санкт-Петербург, Россия). E-mail: kryukov48@mail.ru

Авторы заявляют об отсутствии конфликта интересов.

Information about the authors:

A.G. Antonov, Leningrad State University named after A.S. Pushkin (St. Petersburg, Russian Federation). E-mail: antonovanton1@mail.ru

E.A. Zorina, Saint Petersburg University of the State Fire Service (St. Petersburg, Russian Federation). E-mail: zorina_lena@mail.ru

D.V. Kryukov, Leningrad State University named after A.S. Pushkin (St. Petersburg, Russian Federation). E-mail: kryukov48@mail.ru

The authors declare no conflicts of interests.

Статья поступила в редакцию 23.09.2021;
одобрена после рецензирования 15.01.2022; принята к публикации 17.05.2022.

The article was submitted 23.09.2021;
approved after reviewing 15.01.2022; accepted for publication 17.05.2022.