#### УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ

Статья / Article

УДК / UDC 343.3.7 DOI 10.35231/18136230\_2021\_2\_168

## К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего ее блокирование

## А. Г. Антонов, Д. В. Крюков

Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация

В статье исследуется общественная опасность неправомерного доступа к компьютерной информации, повлекшего ее блокирование. В исследовании рассмотрена категория общественной опасности преступления в целом и применительно к так называемым киберпреступлениям, к которым относится неправомерный доступ к компьютерной информации, повлекший ее блокирование.

Авторами обосновывается тезис, что такое последствие неправомерного доступа к компьютерной информации, как блокирование само по себе, не всегда является общественно опасным, поскольку оно не отражает полной реализации общественной опасности данного деяния. Вместе с тем проявление общественной опасности такого деяния более очевидно в случае наступления последствий, отражённых в квалифицирующих признаках, установленных ч. 2–4 ст. 272 УК РФ. Приводится анализ судебной практики по уголовным делам о преступлениях, предусмотренных гл. 28 УК РФ, а также результаты социологического опроса, проведённого авторами в рамках исследования.

По результатам исследования сделан вывод, что общественная опасность рассматриваемого преступления проявляется, как правило, не в причинении вреда как таковом, а в «кумулятивном эффекте» — способности повлечь за собой причинение вреда другим общественным отношениям, охраняемым уголовным законом. При этом степень общественной опасности неправомерного доступа к компьютерной информации, не повлекшего каких-либо иных опасных последствий, кроме блокирования такой информации, достаточно низка для того, чтобы данное деяние было криминализировано.

**Ключевые слова**: общественная опасность, неправомерный доступ, компьютерная информация, кумулятивная опасность, блокирование компьютерной информации.

168

\_

<sup>©</sup> Антонов А. Г., Крюков Д. В., 2021

Для цитирования: Антонов А.Г., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего ее блокирование // Ленинградский юридический журнал. 2021. № 2(64). С. 168–179. DOI 10.35231/18136230\_2021\_2\_168

## To the question about the public danger of illegal access to computer information which entailed its blocking

## Anton G. Antonov, Dmitriy V. Kryukov

Pushkin Leningrad State University, Saint Petersburg, Russian Federation

The article examines the social danger of illegal access to computer information, which entailed its blocking. The study examines the category of social danger of crime in general and in relation to the so-called cybercrimes, which include illegal access to computer information which entailed its blocking.

The authors substantiate the thesis that such a consequence of unlawful access to computer information as blocking in itself is not always socially dangerous, since it does not reflect the full realization of the social danger of this act. At the same time, the manifestation of the public danger of such an act is more obvious in the event of the occurrence of the consequences reflected in the qualifying signs established by parts 2-4 of Article 272 of the Criminal Code of the Russian Federation. The authors provide an analysis of judicial practice in criminal cases on charges of crimes provided for by Chapter 28 of the Criminal Code of the Russian Federation, as well as the results of a sociological survey conducted by the authors as part of the study.

According to the results of the study, the authors concluded that the social danger of the crime in question manifests itself, as a rule, not in causing harm as such, but in the "cumulative effect" – the ability to entail harm to other social relations protected by criminal law. At the same time, the degree of public danger of unlawful access to computer information, which did not entail any other dangerous consequences, except for blocking such information, is low enough for this act to be criminalized.

**Key words**: public danger, illegal access, computer information, cumulative danger, blocking computer information.

**For citation**: Antonov, A.G., Kryukov, D.V. (2021) K voprosu ob obshchestvennoj opasnosti nepravomernogo dostupa k komp'yuternoj informacii, povlekshego ee blokirovanie [To the question about the public danger of illegal access to computer information which entailed its blocking]. *Leningradskii yuridicheskii zhurnal – Leningrad Legal Journal*. No 2 (64). pp. 168–179. DOI 10.35231/18136230\_2021\_2\_168 (In Russian).

## Введение

Компьютерная информация как объект законодательного регулирования в отечественное правовое поле попала относительно недавно. В 1992 г. появился Закон Российской Федерации «О правовой охране программ для электронно-вычислительных машин и баз данных»<sup>1</sup>, а составы преступлений в сфере компьютерной информации были сформулированы в первоначальной редакции Уголовного кодекса Российской Федерации 1996 г.<sup>2</sup>

При этом проблема защиты компьютерной информации в мире появилась, конечно, значительно раньше. Например, ещё в конце 80-х гг. ХХ в. знаменитому хакеру (а ныне — эксперту по компьютерной безопасности) Кевину Митнику удалось вторгнуться в компьютерную сеть Министерства обороны США, а в 1990 г. трое работников из Кремниевой долины были арестованы за проникновение в компьютеры правительства и телефонных компаний [1, с. 21].

Несмотря на динамичное развитие компьютерных технологий и информационно-коммуникационных сетей, преступления в сфере компьюинформации не получили заметного терной распространения российской правоприменительной практике. В производстве районных судов в Российской Федерации за период с января 2016 г. по февраль 2021 г., по данным ГАС «Правосудие», находилось лишь 1968 уголовных дел о преступлениях, предусмотренных статьями гл. 28 УК РФ. При этом приговоры вынесены лишь по 942 делам. Если говорить о ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), то за указанный период в производстве судов находилось 1076 уголовных дел по обвинению в преступлении, предусмотренном данной статьей, и по таким делам было вынесено лишь 525 приговоров<sup>3</sup>. Однако приведенные показатели не свидетельствуют об отсутствии актуальности исследуемого вопроса.

<sup>&</sup>lt;sup>1</sup> О правовой охране программ для электронно-вычислительных машин и баз данных: закон Российской Федерации от 23.09.1992 № 3523-1 // Ведомости Съезда народных депутатов Российской Федерации и Верховного суда Российской Федерации. № 42. 1992.

<sup>&</sup>lt;sup>2</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (исх. ред.) [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102041891&rdk=0.

<sup>&</sup>lt;sup>3</sup> ГАС РФ «Правосудие» [Электронный ресурс]. URL: https://bsr.sudrf.ru/bigs/portal.html (с применением фильтров поиска: «дела федеральных судов общей юрисдикции», «уголовные дела», «дата поступления», «статья УК», «результат»); дата обращения: 22.02.2021.

Напротив, они побуждают нас обратить внимание на характерные черты общественной опасности преступлений в сфере компьютерной информации, в том числе и такого преступного деяния, как неправомерный доступ к компьютерной информации, повлекший ее блокирование.

## Понимание категории «общественная опасность преступления»

Чем руководствовался законодатель, признавая соответствующие деяния общественно опасными? Несомненно, в XXI в. значимость компьютерной информации сложно преуменьшить, и общественные отношения в сфере безопасности компьютерной информации, конечно же, нуждаются в уголовно-правовой охране. Однако формирование и формулирование уголовно-правовых запретов в данной области не может осуществляться без учёта характера и степени общественной опасности деяний. Как справедливо отмечает Е.Ю. Антонова, общественная опасность является базовым основанием криминализации деяний, выделения привилегирующих, квалифицирующих и особо квалифицирующих признаков состава преступления [4, с. 36].

Если говорить об опасности неправомерных деяний в так называемом киберпространтве в целом, то исследователи видят её, в частности:

- в нарушении нормального функционирования компьютерной системы, чем нарушаются законные интересы личности, общества и государства [5, с. 45];
- угрозе общественной, государственной безопасности, национальным интересам [9, с. 27];
- максимальной скрытности деяний, их трансграничности и перерастании в масштаб международных угроз [7, с. 111].

Вместе с тем, анализируя конкретные уголовно-правовые запреты, установленные в гл. 28 Уголовного кодекса РФ, необходимо рассматривать общественную опасность не как некую абстрактную категорию, а как основу для криминализации исследуемого преступного деяния.

Компьютерная информация, имеющая конфиденциальный характер, с одной стороны, обладает высокой стоимостью, а с другой — её использование лицами, не уполномоченными на это, способно не только причинить существенный вред правам и свободам человека, но и может способствовать совершению преступных посягательств [6, с. 76].

Как известно, общественная опасность преступления проявляется в двух формах: причинении существенного вреда общественным отношениям, охраняемым уголовным законом, или создании угрозы причинения такого вреда<sup>1</sup>. Преступление следует рассматривать «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» [10, с. 44].

Исходя из этого, можно выделить некоторые типичные проявления общественной опасности преступления. Она выражается в виде уже состоявшегося вреда, причиненного общественным отношениям преступлением, а также может проявляться в угрозе повторения совершенного преступления и угрозе совершения дополнительного (смежного) преступления.

Некоторым преступлениям присуща общественная опасность, заключающаяся исключительно в вероятности повторения аналогичных деяний [2, с. 126]. Так, например, при краже общественная опасность реализовывается окончательно и находит свое отражение в виде причинения имущественного ущерба и не развивается далее. Условно обозначим такую опасность простой. При этом общественная опасность других преступлений может обладать более высоким потенциалом причинения вреда обкоторый в себе щественным отношениям, заключает возможность повторения состоявшегося преступления, но и совершения нового, может быть, даже более тяжкого другого преступления, являющегося прямым следствием первого. Данный вид преступлений мы условно называет преступлениями кумулятивной опасности [1, с. 60].

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) общественная опасность данного деяния не исчерпывается его последствиями, и с одной стороны, опасность состоит в том, что окружающие видят, что можно совершать указанные деяния (например, повлекшие блокирование компьютерной информации), а с другой стороны, в том, что эти деяния могут причинить существенный вред другим общественным отношениям.

172

<sup>&</sup>lt;sup>1</sup> Уголовное право. Общая часть: учеб. пособие / под общ. ред. В.А. Уткина, А.В. Шеслера. Томск: ИД Томск. гос. ун-та, 2016. С. 107.

Из позиций такого понимания общественной опасности преступления мы будем исходить и при дальнейшем изложении вопроса относительно неправомерного доступа к охраняемой законом компьютерной информации, повлекшего ее блокирование.

# Характерные черты общественной опасности блокирования компьютерной информации

Как отмечает А.М. Николаев, основанием криминализации деяния являются происходящие в жизни общества процессы, развитие которых порождает объективную необходимость уголовно-правовой охраны определённых ценностей. К числу криминализационных оснований следует относить, в том числе, общественную опасность, распространенность деяний, осуждение их со стороны общественного мнения [8, с. 324].

Соответственно, для более полного анализа необходимо выяснить, признает ли население в целом преступления в сфере компьютерной информации общественно опасными. Какое положение общественная опасность этих преступлений занимает относительно других преступлений?

Для ответа на этот вопрос авторами данного исследования было предложено респондентам, являющимся представителями различных возрастных групп и не имеющим юридического образования, 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 опасными намеренное заражение ВИЧ-инфекцией или венерическим заболеванием.

Компьютерные преступления были признаны наименее опасными или совершенно не опасными для общества деяниями примерно пятой частью опрошенных. Большинство же признают такие деяния опасными для общества. Однако очевидно, что в сравнении с иными преступными деяниями компьютерные преступления зачастую представляются обычному человеку наименьшим из зол.

Часть 1 ст. 272 Уголовного кодекса РФ устанавливает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение,

блокирование, модификацию либо копирование компьютерной информации. Как видно, данный состав преступления включает в себя ряд альтернативных последствий. Одним из них является блокирование компьютерной информации, что и является предметом настоящего исследования.

Как отмечалось ранее, общественная опасность преступления проявляется в двух формах: реальном причинении вреда и возникновении реальной угрозы его причинения. С этих позиций неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее блокирование, исключением не является. Общественная опасность этого преступления заключается в реальном причинении вреда общественным отношениям и опасности его повторения (прецедентности).

Данное преступление можно признать оконченным только тогда, когда неправомерный доступ к определенной компьютерной информации повлек последствия в виде конкретного вреда общественным отношениям – блокирование 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 или наступлении тяжких последствий. При этом рассматриваемое преступление может порождать и другие преступления, например, блокирование информации может являться способом мошенничества или вымогательства.

Уголовный закон не раскрывает значения термина «блокирование» компьютерной информации. Однако, согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением закорасследовании преступлений сфере компьютерной HOB при информации» Генеральной прокуратуры Российской Федерации, блокирование информации – 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 её уничтожением<sup>1</sup>. 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 её использования. Иными словами, преступным последствием признаются некие временные неудобства, связанные с доступом к информации, и не более того.

Осуждённый в 2015 г. Сарапульским городским судом Удмуртской Республики гражданин Ш. на почве личных неприязненных отношений, с помощью заранее известных ему логина и пароля, зашёл в аккаунт своей подруги в социальной сети и выложил там её фото интимного содержания, после чего поменял пароль, заблокировав ей доступ к странице. Подсудимый был признан виновным в совершении неправомерного доступа к компьютерной информации, повлекшего модификацию и блокирование компьютерной информации (ч. 1 ст. 272 УК РФ), и ему было назначено наказание в виде штрафа в размере 20 тыс. рублей. При этом мера пресечения в виде подписки о невыезде была оставлена без изменения до вступления приговора суда в законную силу<sup>2</sup>.

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 гражданскоправовой механизм, а именно: предъявление иска о защите чести и достоинства. Сама же процедура восстановления доступа к своей странице

<sup>&</sup>lt;sup>1</sup> Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. URL: http://genproc.gov.ru/documents/nauka/execution/document-104550/.

<sup>&</sup>lt;sup>2</sup> Приговор Сарапульского городского суда Удмуртской Республики по уголовному делу № 1-261/2015 от 09.09.2015. ГАС РФ «Правосудие» [Электронный ресурс]. URL: https://bsr.sudrf.ru/bigs/portal.html.

и удаления неприемлемого контента занимает не более пяти минут и не требует особых усилий от потерпевшего.

Таким образом, возникает вопрос о соразмерности правовых последствий для самого осуждённого и степени нанесённого им вреда. Осуждённому 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 осуждённого 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 личный 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.

Как отмечалось ранее, рассматриваемое преступление обладает кумулятивной общественной опасностью, которая характеризуется высоким негативным потенциалом. Этот потенциал направлен на другие общественные отношения, помимо тех, которые были затронуты совершённым преступлением. Иначе говоря, преступное посягательство на один объект уголовно-правовой охраны потенциально влечёт посягательство на другой объект: например, незаконное блокирование компьютерной информации может обусловить совершение мошенничества или вымогательства.

#### Заключение

Подводя итог, отметим, что общественная опасность неправомерного доступа к компьютерной информации, повлекшего её блокирование, состоит в способности причинять вред общественным отношениям и в угрозе совершения иных преступлений. Однако рассмотренное преступление будет обладать общественной опасностью в случае причинения существенного вреда общественным отношениям, который, собственно, и обусловливает дальнейшее ее развитие.

В таких обстоятельствах возникают разумные сомнения относительно того, насколько оправданна криминализация неправомерного доступа к компьютерной информации, повлекшего её блокирование, как самостоятельного преступления. Если обратиться к Кодексу Российской Федерации об административных правонарушениях, то в нём можно найти такие противоправные деяния, общественная опасность которых более очевидна. К ним 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 литературы

- 1. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М.: Мир, 1999. 351 с.
- 2. Антонов А.Г., Витовская Е.С. Об общественной опасности преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их аналогов // Человек: преступление и наказание. 2016. № 2 (93). С. 59–64.
- 3. Антонов А.Г. О соотношении категорий «общественная опасность преступления» и «личность преступника» // Государство и право. 2019. № 11. С. 125–129.
- 4. Антонова Е.Ю. Общественная опасность как основание криминализации деяний // Уголовная политика и правоприменительная практика: материалы VI междунар. науч-практ. конф. СПб.: Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия». 2018. С. 34–41.
- 5. Бражник С.Д., Соколова О.В. Преступления в сфере компьютерной информации как угроза экономической безопасности: криминологические и уголовно-правовые аспекты // Актуальные вопросы борьбы с преступлениями. 2017. № 3. С. 44–47.
- 6. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. 496 с.
- 7. Надточий Ю.В. Киберпреступность как угроза экологической безопасности // Азиатско-тихоокеанский регион: экономика, политика, право. 2018. Т. 20. № 3. С. 108–116.
- 8. Николаев А.М. Пределы криминализации деяний с учётом характера и степени их общественной опасности (истоки и перспективы формирования новой теории) // Пробелы в российском законодательстве. 2008. № 1. С. 322–324.
- 9. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25–29.
- 10. Филимонов В. Д. Охранительная функция уголовного права. СПб.: Юрид. центр Пресс., 2003. 196 с.

#### References

- 1. Aikov, D., Seiger, K., Fonstorkh, U. (1999). *Komp'yuternye prestupleniya. Rukovodstvo po bor'be s komp'yuternymi prestupleniyami* [Computer crimes. Guide to Combating Computer Crime]. Moscow: Mir. 351 p. (In Russian).
- 2. Antonov, A.G., Vitovskaya, E.S. (2016). Ob obshchestvennoi opasnosti prestuplenii v sfere nezakonnogo oborota narkoticheskikh sredstv, psikhotropnykh veshchestv i ikh analogov [On the public danger of crimes in the field of illicit trafficking in narcotic drugs, psychotropic substances and their analogues]. *Chelovek: prestuplenie i nakazanie Man: crime and punishment.* No 2 (93). pp. 59–64. (In Russian).
- 3. Antonov, A.G. (2019). O sootnoshenii kategorii «obshchestvennaya opasnost' prestupleniya» i «lichnost' prestupnika» [On the ratio of the categories "public danger of a crime" and "personality of the offender"]. *Gosudarstvo i pravo State and law.* No 11. pp. 125–129. (In Russian).
- 4. Antonova, E.Yu. (2018). *Obshchestvennaya opasnost' kak osnovanie kriminalizatsii deyanii* [Public danger as a basis for the criminalization of acts]. Ugolovnaya politika i pravoprimenitel'naya praktika [Criminal policy and law enforcement practice]. Materialy VI mezhdunar. nauch-prakt. konf. Saint-Petersburg: Severo-Zapadnyi filial FGBOUVO «Rossiiskii gosudarstvennyi universitet pravosudiya». pp. 34–41. (In Russian).
- 5. Brazhnik, S.D., Sokolova, O.V. (2017). Prestupleniya v sfere komp'yuternoi informatsii kak ugroza ekonomicheskoi bezopasnosti: kriminologicheskie i ugolovno-pravovye aspekty [Crimes in the field of computer information as a threat to economic security: criminological and criminal legal aspects]. *Aktual'nye voprosy bor'by s prestupleniyami Topical issues of combating crimes*. No 3. pp. 44–47. (In Russian).
- 6. Volevodz, A.G. (2001). *Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva* [Countering computer crimes: the legal basis for international cooperation]. Moscow: Yurlitinform. 496 p. (In Russian).
- 7. Nadtochii, Yu.V. (2018). Kiberprestupnost' kak ugroza ekologicheskoi bezopasnosti [Cybercrime as a threat to environmental security]. *Aziatsko-tikhookeanskii region: ekonomika, politika, pravo Asia-Pacific region: economics, politics, law.* T. 20. No 3. pp. 108–116. (In Russian).
- 8. Nikolaev, A.M. (2008). Predely kriminalizatsii deyanii s uchetom kharaktera i stepeni ikh obshchestvennoi opasnosti (istoki i perspektivy formirovaniya novoi teorii) [The limits of criminalization of acts, taking into account the nature and degree of their social danger (the origins and prospects for the formation of a new theory)]. *Probely v rossiiskom zakonodatel'stve Gaps in Russian legislation.* No 1. pp. 322–324. (In Russian).
- 9. Novichkov, V.E., Pykhtin, I.G. (2018). Sotsial'no-pravovoe obosnovanie vvedeniya ugolovnoi otvetstvennosti za nepravomernoe vozdeistvie na kriticheskuyu informatsionnuyu infrastrukturu Rossiiskoi Federatsii [Socio-legal justification for the introduction of criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation]. *Psikhopedagogika v pravookhranitel'nykh organakh Psychopedagology in law enforcement agencies*. No 2 (73). pp. 25–29. (In Russian).
- 10. Filimonov, V. D. (2003). Okhranitel'naya funktsiya ugolovnogo prava [The protection function of criminal law]. Saint-Petersburg: Yurid. tsentr Press. 196 p.

Уголовное право и криминология Criminal law and criminology

### Вклад соавторов

Соавторство неделимое.

## Co-authors' contribution

Co-authorship is indivisible.

## Об авторах

**Антонов Антон Геннадьевич,** доктор юридических наук, профессор, профессор кафедры уголовного права и процесса, Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация, ORCID ID: 0000-0003-2708-020X, e-mail: antonovanton1@mail.ru

**Крюков Дмитрий Витальевич,** аспирант кафедры уголовного права и процесса, Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация, ORCID ID: 0000-0000-0000, e-mail: kryukov48@mail.ru

#### About the authors

**Anton G. Antonov,** Dr. Sci. (Law), Associate Professor, Professor of the Department of of Criminal Law and Process, Pushkin Leningrad State University, Saint Petersburg, Russian Federation, ORCID ID: 0000-0003-2708-020X, e-mail: antonovanton1@mail.ru

**Dmitriy V. Kryukov,** postgraduate student of the Department of Criminal Law and Process, Pushkin Leningrad State University, Saint Petersburg, Russian Federation, ORCID ID: 0000-0000-0000, e-mail: kryukov48@mail.ru

Поступила в редакцию: 10.03.2021 Received: 10 March 2021

Принята к публикации: 27.05.2021 Accepted: 27 May 2021

Опубликована: 29.06.2021 Published: 29 June 2021