

КОНКУРЕНЦИЯ НОРМ ОБ ОХРАНЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: РАЗГРАНИЧЕНИЕ СТАТЬИ 272.1 УК РФ И СТАТЬИ 13.11 КоАП РФ

Дмитрий Сергеевич Корешников

Уральский государственный юридический университет им. В. Ф. Яковлева,
г. Екатеринбург, Российская Федерация
d.koreshnikov@loys.law

 <https://orcid.org/0009-0007-7643-8796>

Аннотация. Статья посвящена вопросам, вызванным изменением законодательства в области обработки персональных данных и введением соответствующей уголовной ответственности. Так, Федеральным законом от 30.11.2024 № 421-ФЗ в Уголовный кодекс Российской Федерации добавлена новая статья: «Статья 272.1. Незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения».

Появление новой уголовной статьи вызвало ряд вопросов, в том числе, как отграничить преступление, предусмотренное ст. 272.1 Уголовного кодекса Российской Федерации, от административного правонарушения, предусмотренного ст. 13.11. Кодекса Российской Федерации об административных правонарушениях.

В настоящей статье автором предпринята попытка ответить на этот вопрос и разграничить противоправные деяния, предусмотренные ст. 272.1 УК РФ и ст. 13.11 КоАП РФ. Проведено сравнение по объективной и субъективной стороне, по предмету преступного посягательства. Указано на необоснованность ряда подходов, предложенных для разграничения этих видов правонарушений. Сформулирован подход, при котором проводить различие необходимо прежде всего по тому, осведомлено ли лицо, обрабатывающее информацию с персональными данными, о незаконном источнике ее получения.

Ключевые слова: персональные данные, компьютерная информация, статья 272.1 УК РФ, статья 13.11 КоАП РФ, новая криминализация, конкуренция норм административного и уголовного закона


Для цитирования: Корешников Д. С. Конкуренция норм об охране персональных данных: разграничение статьи 272.1 УК РФ и статьи 13.11 КоАП РФ // Правопорядок: история, теория, практика. 2025. № 3(46). С. 49–54. DOI: 10.47475/2311-696X-2025-46-3-49-54

Research article

COMPETITION OF PERSONAL DATA PROTECTION STANDARDS: DIFFERENTIATION OF ARTICLE 272.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION AND ARTICLE 13.11 OF THE ADMINISTRATIVE CODE OF THE RUSSIAN FEDERATION

Dmitry S. Koreshnikov

Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russian Federation
d.koreshnikov@loys.law

 <https://orcid.org/0009-0007-7643-8796>

Abstract. The article is devoted to the issues caused by the change in legislation in the field of personal data processing and the introduction of corresponding criminal liability. Thus, Federal Law No. 421-FZ of November 30, 2024 added a new article to the Criminal Code of the Russian Federation: “Article 272.1. Illegal use and (or) transfer, collection and (or) storage of computer information containing personal data, as well as the creation and (or) ensuring the functioning of information resources intended for its illegal storage and (or) distribution.”

The emergence of a new criminal article gave rise to a number of questions, one of which was the question of distinguishing the elements of a crime provided for in Art. 272.1 of the Criminal Code of the Russian Federation from the elements of an administrative offense provided for in Art. 13.11. of the Code of the Russian Federation on Administrative Offenses.

In this article, the author attempts to answer this question and differentiate the illegal acts provided for in Article 272.1 of the Criminal Code of the Russian Federation and Article 13.11 of the Code of Administrative Offenses of the Russian Federation. A comparison is made on the objective and subjective side, on the subject of the criminal offense. The groundlessness of a number of approaches proposed for distinguishing these types of offenses is indicated. An approach is formulated in which the distinction must be made based on awareness of the source of origin of computer information containing personal data.

Keywords: personal data, computer information, Article 272.1 of the Criminal Code of the Russian Federation, Article 13.11 of the Code of Administrative Offenses of the Russian Federation, new criminalization, competition of administrative and criminal law norms

For citation: Koreshnikov DS. Competition of Personal Data Protection Standards: Differentiation of Article 272.1 of the Criminal Code of the Russian Federation and Article 13.11 of the Administrative Code of the Russian Federation. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(3):49-54. (In Russ.) DOI: 10.47475/2311-696X-2025-46-3-49-54

Введение

04.12.2023 в Государственную Думу Российской Федерации внесен законопроект, предусматривающий дополнение Уголовного кодекса Российской Федерации статьей 272.1 УК РФ. В данной статье содержится описание состава преступления, связанного с незаконной обработкой компьютерной информации, содержащей персональные данные. В пояснительной записке в подтверждение необходимости такого нововведения указывалось, что «с января по август 2022 года в России произошли утечки 197 млн записей персональных данных и платежной информации. Черный рынок персональных данных постоянно растет, а основными источниками утечек являются сторонние злоумышленники или сами сотрудники компаний, которые продают или отдают бесплатно конфиденциальные данные своих клиентов. По отдельным оценкам в 2020 году общий ущерб от утечек личных данных превысил 3 млрд рублей, а в 2022 году указанный ущерб уже превысил 8 млрд. рублей. Так, на декабрь 2021 года в теневом сегменте сети «Интернет» («даркнет») циркулирует более 2000 баз данных общим объемом более 10 Тб, содержащие персональные данные о 80 % населения России. Общий объем официально выявленных утечек персональных данных за 2022 г. (о которых официально сообщалось в СМИ) — более 1130 млн записей, содержащие сведения о персональных данных граждан Российской Федерации»¹.

Признавая очевидную значимость указанной законодательной инициативы, у рецензентов законопроекта с самого начала возник вопрос о разграничении статьи 272.1 УК РФ и статьи 13.11. КоАП РФ. Так, в официальном отзыве на проект, данном заместителем Председателя Верховного Суда Российской Федерации Давыдовым В. А., указывалось на то, что «в диспозиции части 1 проектной статьи 272.1 УК РФ отсутствуют

криминообразующие признаки, позволяющие отграничить соответствующее преступление от противоправных действий, предусмотренных статьей 13.11. КоАП РФ, что может привести к конкуренции данного уголовно-правового запрета со статьей 13.11. КоАП РФ и существенно усложнить применение проектной нормы на практике»².

Законодатель постарался учесть высказанные замечания, однако практика правоприменения данной статьи демонстрирует факт отсутствия на сегодня однозначного подхода к разграничению преступления и правонарушения в области обработки персональных данных. В связи с чем имеется необходимость теоретического осмысления уже принятой и действующей нормы уголовного закона.

Материал и методы

При подготовке публикации использованы нормативно-правовые акты, регламентирующие вопросы обработки персональных данных и ответственности за нарушение законодательства о персональных данных. Ввиду исключительно короткого периода действия статьи 272.1 УК РФ в настоящий момент отсутствует судебная практика по этому составу преступления, нет должной научной разработанности исследуемого в статье вопроса. В связи с этим в настоящем исследовании прежде всего сделан акцент на анализе текста вновь принятого закона, который изучен с помощью формально-логического и сравнительно-правового метода. Предмет исследования, учитывая допустимый объем работы, сведен к сравнительному анализу ч. 1 ст. 272.1 УК РФ и ч. 1 и ч. 2 ст. 13.11 КоАП РФ. При этом проведено сравнение указанных составов по объективной и субъективной стороне, по предмету посягательства.

¹ Законопроект № 502113-8 // СОЗД ГАС «Законотворчество». URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 02.06.2025).

² Там же.

Описание исследования

Часть 1 статья 13.11 КоАП РФ предусматривает ответственность за обработку персональных данных в случаях или в целях, не предусмотренных законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния.

Часть 2 данной статьи говорит об ответственности за обработку персональных данных без согласия субъекта персональных данных.

Административная ответственность по обоим частям возникает только в случаях, если эти действия не содержат уголовно наказуемого деяния, на что прямо указано в ст. 13.11 КоАП РФ. Таким образом, законодатель ориентирует правоприменителя на приоритет уголовного закона, и только, если проверяемое деяние не подпадает по какому-либо признаку под состав преступления, возникает необходимость оценивать наличие в деянии признаков административного правонарушения.

Разграничение по предмету посягательства

Статья 13.11 КоАП РФ говорит о персональных данных, тогда как уголовная статья сужает предмет преступления до «компьютерной информации, содержащей персональные данные». Из этого можно было бы сделать вывод, что любая незаконная обработка персональных данных в виде компьютерной информации — это 272.1 УК РФ, а предметом ст. 13.11 КоАП РФ являются персональные данные в любом другом виде (форме), кроме компьютерной (например, на бумажных носителях). Такой вывод является неверным.

Для уголовного преследования нужна не любая компьютерная информация, содержащая персональные данные, а только такая информация, которая получена путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем, на что прямо указал в статье законодатель. Незаконный путь получения информации становится определяющей характеристикой предмета преступного посягательства.

Но означает ли это, что обработке данных, предусмотренной ст. 272.1 УК РФ, должно предшествовать какое-то предикатное преступление или правонарушение¹? Наш ответ будет отрицательным, так как информация может попасть к преступнику различными путями.

Субъект преступления, предусмотренного ст. 272.1 УК РФ, может иметь изначально законный доступ к средствам обработки и хранения компьютерной информации. Однако, действуя вопреки целям, для дости-

жения которых ему предоставлен доступ, такое лицо может произвести незаконное копирование и распространение информации, содержащей персональные данные.

В качестве примера можно привести публикацию с сайта Следственного комитета Российской Федерации, согласно которой в феврале 2025 года начальник одного из отделов филиала публично-правовой компании в Республике Карелии по просьбе знакомых незаконно передавал им содержащиеся в едином реестре недвижимости персональные данные людей, а также сведения об их имуществе. По данному факту возбуждено уголовное дело по п. «г» ч. 3 ст. 272.1 УК РФ².

Второй вариант, когда лицо, не имея законных оснований, осуществляет неправомерный доступ к компьютерной информации, например, осуществляет хакерский взлом интернет-сайта. Ранее такие действия квалифицировались по ст. 272 УК РФ — неправомерный доступ к охраняемой законом компьютерной информации, если деяние повлекло копирование данной информации. Однако, Федеральный закон от 30.11.2024 № 421-ФЗ кроме того, что внес в Уголовный кодекс Российской Федерации новую статью 272.1, он также изменил и статью 272 УК РФ. Теперь данная статья предусматривает уголовную ответственность за неправомерный доступ к охраняемой компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, за исключением случаев, предусмотренных статьей 272.1 УК РФ. Таким образом, неправомерный доступ к компьютерной информации с персональными данными с последующей обработкой данной информации полностью охватывается ст. 272.1 УК РФ и не требует дополнительной квалификации по ст. 272 УК РФ.

Третий вариант, когда лицо, осуществляющее незаконную обработку компьютерной информации, получило ее от третьего лица. В этом случае он будет подлежать уголовной ответственности, только если знал о неправомерности получения данной информации, потому что преступление, предусмотренное ст. 272.1 УК РФ, может совершаться исключительно с прямым умыслом, который подразумевает осознание лицом того, что он работает изначально с незаконно полученной информацией.

Вместе с тем автор настоящей статьи на практике столкнулся с несколько иной трактовкой предмета и субъективной стороны данного преступления. Так, после вступления в силу статьи 272.1 УК РФ сотрудниками правоохранительного органа проведено оперативно-разыскное мероприятие — обследование помещений компании. В ходе обследования изъяты служебные компьютеры сотрудников, на которых обнаружены файлы, содержащие данные физических лиц.

² В Петрозаводске следователями СК возбуждено уголовное дело по факту незаконной передачи компьютерной информации. URL: <https://karelia.sledcom.ru/news/item/1986097> (дата обращения: 01.06.2025).

¹ Вопрос о необходимости наличия предикатного преступления и возбуждения по нему уголовного дела поставлен Городовой А. и Кабановым М. в статье «Правовое регулирование должно быть универсальным». Адвокатская газета. Выпуск № 6 (431) 16–31 марта 2025 года. URL: <https://www.advgazeta.ru/mneniya/pravovoe-regulirovanie-dolzno-byt-universalnym/> (Дата обращения: 02.06.2025).

Сотрудники правоохранительных органов опросили указанных физических лиц и получили от них пояснения о том, что они не давали согласия на обработку персональных данных сотрудникам данной компании. При таких обстоятельствах правоохранители посчитали, что имеются все необходимые признаки состава преступления, предусмотренного ст. 272.1 УК РФ: нет согласия на обработку, значит, совершается преступление, в связи с чем нет необходимости устанавливать источник происхождения компьютерной информации.

Однако такой подход представляется неверным. В данной ситуации можно говорить лишь о наличии признаков правонарушения, предусмотренного ч. 2 ст. 13.11 КоАП РФ (обработка персональных данных без согласия). Для применения же ст. 272.1 УК РФ необходимо установить источник происхождения компьютерной информации и факт осведомленности лица о неправомерности данного источника. Нет никакой презумпции незаконности происхождения информации с персональными данными, но есть презумпция невиновности.

Тем более, что компьютерная информация, содержащая персональные данные, может быть получена из открытых, общедоступных источников или от лиц, которые заявляли о правомерности нахождения у них данной информации и наличии у них права на ее передачу третьим лицам. При таких обстоятельствах не будет состава преступления у лица, полагавшего, что получило доступ к информации на законных основаниях.

Для примера таких законных общедоступных источников информации, содержащих персональные данные, можно привести многочисленные сайты государственных органов¹:

– сайт Федеральной службы судебных приставов (<https://fssp.gov.ru/>) содержит информацию об исполнительных производствах в отношении физических лиц, сведения о розыске, сведения из реестра должников по алиментам;

– сайт Федеральной налоговой службы России (<https://www.nalog.gov.ru/>) содержит сведения об индивидуальных предпринимателях (ФИО, их телефоны, почта (ранее были и адреса регистрации), сведения о лицензиях, сведения об уплаченных суммах налогов и сборов, о наложенных обеспечительных мерах. На сайте производится проверка статуса налогоплательщика, сведения о приостановленных счетах, сведения о физических лицах, являющихся учредителями (участниками) нескольких организаций. На сайте также можно проверить ИНН на действительность, получить сведения о дисквалификации конкретного физического лица (запрет на право занимать определенные должности);

– сайт «Прозрачный бизнес» (<https://pb.nalog.ru/>) также дает возможность получить сведения из ЕГРЮЛ, ЕГРИП, Реестра дисквалифицированных лиц, информацию о многократном участии физического лица в организациях, о руководителях, участниках юридических лиц и другую значимую информацию;

¹ Необходимо учесть, что содержание указанных ресурсов постоянно меняется.

– сайт «Федресурс» (<https://fedresurs.ru/>) содержит информацию из единого федерального реестра юридически значимых сведений о фактах деятельности юридических лиц, индивидуальных предпринимателей и иных субъектов экономической деятельности. На сайте можно получить информацию по физическим лицам, в том числе сведения о банкротстве физического лица, сведения о кредиторах физического лица, наличии обременений, лизинга и другое;

– сайты Федеральной нотариальной палаты (<https://notariat.ru/ru-ru> и www.reestr-zalogov.ru). На данных сайтах можно получить информацию о залогах движимого имущества: сведения о залогодателях и залогодержателях, сведения об имуществе, переданном в залог. Также можно получить сведения из реестра наследственных дел, в том числе дату смерти физического лица.

– сайт недобросовестных поставщиков (<https://zakupki.gov.ru/>), на котором можно найти информацию о физических лицах (индивидуальных предпринимателях);

– сайт Генеральной прокуратуры России (<https://epp.genproc.gov.ru/>) содержит сведения о контрольных (надзорных) профилактических мероприятиях, из которых можно получить сведения о физических лицах: ФИО, должность и место работы, статья и дата привлечения к ответственности;

– сайт публичных должностных лиц (<https://declarator.org/>). На данном сайте можно получить доступ к налоговым декларациям лиц, занимающих или занимавших в прошлом публичные должности, из которых можно узнать его дату рождения, доход за год, наличие недвижимости, автомобилей, семейное положение (наличие супруга, детей);

– сайт МВД России (<https://мвд.рф>) содержит различные сервисы проверки физических лиц: нахождение в розыске лица (в т. ч. место рождения, национальность); проверка действительности паспорта, разрешения на работу и патента на осуществление трудовой деятельности;

– сайт Федеральной службы исполнения наказания (<https://fsin.gov.ru/>) содержит сведения о разыскиваемых лицах;

– сайт, содержащий реестр лиц, уволенных со службы в связи с утратой доверия за совершение коррупционных правонарушений (<https://gosszluzhba.gov.ru/reestr/>);

– сайт Минюста России (<https://minjust.gov.ru/>), на котором находится реестр иностранных агентов и сведения о них.

Перечень открытых источников можно продолжать еще долго, но главное — из него следует, что в сети «Интернет» для общего доступа размещено огромное число сведений о конкретных физических лицах. Использование данных сайтов и государственных сервисов для сбора данных не должно подпадать под действие статьи 272.1 УК РФ, так как отсутствует составообразующий признак — информация, полученная незаконным путем.

Не лишним будет отметить, что в пояснительной записке к законопроекту инициатор ведет диалог с вышеприведенным отзывом Верховного Суда Российской Федерации и указывает на доработку проекта в следующем ключе: «Таким образом, для целей уголовного законодательства конкретизирован объект преступного посягательства (компьютерная информация), которая содержит персональные данные, полученные незаконным путем. Это позволяет разграничить новый состав УК РФ от правонарушений, ответственность за которые предусмотрена Кодексом Российской Федерации об административных правонарушениях в статье 13.11 «Нарушение законодательства РФ в области персональных данных», а также иных составов преступлений»¹.

Разграничение по совершаемым действиям

Часть 1 ст. 272.1 УК РФ криминализирует следующие действия: незаконное использование, незаконную передачу (распространение, предоставление, доступ), незаконный сбор, незаконное хранение информации, содержащей персональные данные.

Статья 13.11 КоАП РФ говорит лишь о незаконной обработке персональных данных. При этом данная статья КоАП РФ является бланкетной и прямо отсылает к законодательству в области персональных данных.

Определение обработки персональных данных дано в Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ, согласно статье 3 которого обработка персональных данных — любое действие с персональными данными, включая **сбор**, запись, систематизацию, накопление, **хранение**, уточнение (обновление, изменение), извлечение, **использование**, **передачу (распространение, предоставление, доступ)**, обезличивание, блокирование, удаление, уничтожение персональных данных.

Исходя из буквального сопоставления указанных норм, можно было бы предположить, что ст. 272.1 УК РФ не охватывает такие виды обработки персональных данных, как запись, систематизацию, накопление, уточнение (обновление, изменение), извлечение, обезличивание, блокирование, удаление, уничтожение персональных данных. Таким образом, указанные действия должны подпадать под действие статьи 13.11. КоАП РФ. Вместе с тем вполне допускаем, что практика применения ст. 272.1 УК РФ такие действия как запись, систематизацию, накопление, уточнение, обезличивание и извлечение будет трактовать как хранение, использование или сбор персональных данных соответственно.

При такой трактовке для административной ответственности должно остаться только блокирование, удаление и уничтожение персональных данных, хранящихся в виде компьютерных файлов.

Но, как говорилось выше, в статью 272 УК РФ также внесено изменение. Теперь данная статья предусматривает уголовную ответственность за неправомер-

ный доступ к охраняемой компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, за исключением случаев, предусмотренных статьей 272.1 УК РФ. В связи с этим встает вопрос: «за исключением случаев, предусмотренных статьей 272.1 УК РФ» относится только к копированию компьютерной информации? Если нет и законодатель имел при этом ввиду и уничтожение, и блокирование, и модификацию, то в объективную сторону ст. 272.1 УК РФ будут входить и такие незаконные способы обработки компьютерной информации с персональными данными как блокирование, удаление и уничтожение.

Таким образом, практика применения статьи 272.1 УК РФ может пойти по пути как узкого, буквального, так и максимально широкого толкования, при котором уголовная ответственность будет наступать за любое действие, входящее в понятие «обработка персональных данных», предусмотренного Федеральным законом «О персональных данных».

На наш взгляд такой расширительный подход будет необоснованным, особенно в случаях, связанных с обезличиванием, уничтожением и удалением компьютерной информации, содержащей персональные данные, полученные неправомерным путем. Исходя из пояснительной записки² к проекту закона о введении ст. 272.1 УК РФ, цель новой статьи — борьба с незаконным оборотом персональных данных, которые используются для совершения преступлений в отношении граждан. Уничтожение или обезличивание неправомерно полученных данных, напротив, исключает возможность их дальнейшего использования в преступных целях и не представляет той общественной опасности, которая необходима для уголовной криминализации деяния.

Разграничение по цели обработки данных

В юридических изданиях [3; 4] встречается точка зрения, что возможным способом преодоления конкуренции ст. 272.1 УК РФ и ст. 13.11 КоАП РФ является установление цели обработки персональных данных: при административном правонарушении цель обработки персональных данных изначально является законной, а при преступлении — нет.

С таким подходом вряд ли можно согласиться. Статья 5 Федерального закона «О персональных данных» прямо предусматривает, что одним из принципов обработки персональных данных является соблюдение законной цели такой обработки. Как указано в части 2 данной статьи, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Часть 1 статьи 13.11. КоАП РФ в качестве одного из альтернативных действий, образующих правона-

¹ Законопроект № 502113-8 // СОЗД ГАС «Законотворчество». URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 02.06.2025).

² Законопроект № 502113-8 // СОЗД ГАС «Законотворчество». URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 02.06.2025).

рушение, предусматривает обработку персональных данных, несовместимую с целями сбора персональных данных.

При таких обстоятельствах ч. 1 ст. 13.11 КоАП РФ указывает на незаконную цель обработки как основание привлечения именно к административной ответственности.

В то же время часть 1 статьи 272.1 УК РФ вообще не предусматривает какую-либо цель в качестве необходимого признака состава преступления.

Таким образом, предложенный способ разрешения коллизии не основан на нормах законов.

Заключение и вывод

На сегодняшний день можно выделить один основной критерий, по которому необходимо разграничивать ч. 1 ст. 272.1 УК РФ и ч. 1 и 2 ст. 13.11. КоАП РФ. Таким критерием является осведомленность лица, осуществляющего незаконную обработку компьютерной информации с персональными данными, об источнике происхождения данной информации. Если он знает, что данная информация получена незаконным путем, то можно вести речь о наличии в его действиях признаков состава преступления, если нет — то только об административном правонарушении.

Список источников

1. Городова А., Кабанов М. Правовое регулирование должно быть универсальным // Адвокатская газета. Выпуск № 6 (431) 16–31 марта 2025 года. URL: <https://www.advgazeta.ru/mneniya/pravovoe-regulirovanie-dolzno-byt-universalnym/> (дата обращения: 02.06.2025)
2. Кисин В. Р., Попугаев Ю. И. О коллизии (конкуренции) норм, предусматривающих административную и уголовную ответственность, и способы ее разрешения // Научный портал МВД России. 2013. № 2 (22). С. 79–88.
3. Мунтян А. Фокус правоприменителя на субъективную сторону состава правонарушения. О конкуренции составов новой ст. 272.1 УК РФ и ст. 13.11. КоАП РФ // Адвокатская газета. Выпуск № 24 (425) 16–31 декабря 2024 года. URL: <https://www.advgazeta.ru/mneniya/fokus-pravoprimenitelya-na-subektivnuyu-storonu-sostava-pravonarusheniya/> (дата обращения: 02.06.2025).
4. Панина Н. Н. Совершенствование правовых механизмов привлечения к уголовной ответственности за незаконный оборот персональных данных // Уголовно-правовое обеспечение правоохранительной деятельности: взгляд молодежи. Материалы научно-практической конференции, проведенной в рамках I Съезда Молодежной секции Международного союза криминалистов. Москва, 2024. С. 211–215.
5. Петровец К. Разграничение уголовного и административного составов за действия, повлекшие утечку персональных данных // Адвокатская газета. Выпуск № 24 (425) 16–31 декабря 2024 года URL: <https://www.advgazeta.ru/mneniya/razgranichenie-ugolovno-i-administrativnogo-sostavov-za-deystviya-povlekshie-utechku-personalnykh-dannikh/> (дата обращения: 02.06.2025).

СВЕДЕНИЯ ОБ АВТОРЕ

Корешников Дмитрий Сергеевич

Ассистент кафедры уголовного права им. М. И. Ковалева, Уральский государственный юридический университет имени В. Ф. Яковлева
Россия, 620066, г. Екатеринбург, ул. Комсомольская, д. 21
E-mail: d.koreshnikov@loys.law
ORCID: 0009-0007-7643-8796

INFORMATION ABOUT THE AUTHOR

Dmitry S. Koreshnikov

Assistant of Department of Criminal Law named after M. I. Kovalev, Ural State Law University named after V. F. Yakovlev
21 Komsomolskaya str., Yekaterinburg 620066, Russia
E-mail: d.koreshnikov@loys.law
ORCID: 0009-0007-7643-8796

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 20.06.2025.

Дата рецензирования статьи / Revised: 17.07.2025.

Дата принятия статьи к публикации / Accepted: 15.08.2025.