Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Преодоление нелегальной трансграничной передачи персональных данных

Дмитрий Валерьевич Бахтеев ✉

Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Анна Михайловна Сосновикова

Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Евгений Владимирович Казенас

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

Ключевые слова

законодательство,
информационная безопасность,
информация,
инцидент,
компьютерная сеть,
персональные данные,
право,
связь,
трансграничная передача данных,
цифровые технологии

Аннотация

Цель: формирование комплексной междисциплинарной юридико-технологической модели управления рисками в сфере незаконной трансграничной передачи персональных данных посредством ликвидации законодательных лакун и создания системы автоматизированного контроля исходящих потоков информации, а также экспертного реагирования на выявленные инциденты.

Методы: в работе, помимо всеобщего диалектического и общенаучных, используются специально-юридические и кибернетические методы. Так, на основе сравнительно-правового анализа выявляются различия между национальным и международным регулированием трансграничных потоков персональных данных, а метод моделирования, положенный в основу второго раздела исследования, позволяет сформировать алгоритм выявления инцидентов информационной безопасности в сфере трансграничной передачи персональных данных и реагирования на них.

Результаты: сформулированы предложения по оптимизации законодательства в рассматриваемой сфере посредством введения специализированных охранительных норм за нарушение правил трансграничной передачи персональных данных, закрепления обязанности оператора уведомлять субъектов персональных данных о намерении осуществить передачу информации за рубеж. Во второй части работы описана концепция программного комплекса, предназначенного для детекции инцидентов информационной безопасности в рассматриваемой области, а также модель действия уполномоченного представителя оператора после получения сигнала от автоматизированной системы.

✉ Корреспондирующий автор

© Бахтеев Д. В., Сосновикова А. М., Казенас Е. В., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: для решения заявленной проблемы в работе объединяются знания и компетенции ученых-юристов и специалистов в сфере информационной безопасности, что позволяет предложить междисциплинарный подход. Одновременно с этим вопросы незаконной трансграничной передачи персональных данных на сегодняшний день не получили должного освещения в науке, поскольку российское законодательство в данной сфере изменилось не так давно. Авторы настоящей работы предлагают не столько усилить санкцию за нарушение законодательства в рассматриваемой сфере, сколько обеспечить наказание лиц, совершающих кибератаки, и вооружить операторов персональных данных действенным инструментом минимизации рисков утечки информации.

Практическая значимость: результаты исследования могут быть использованы для совершенствования законодательства в сфере трансграничной передачи персональных данных и организации деятельности уполномоченных сотрудников оператора персональных данных по управлению рисками в рассматриваемой сфере.

Для цитирования

Бахтеев, Д. В., Сосновикова, А. М., Казенас, Е. В. (2024). Преодоление нелегальной трансграничной передачи персональных данных. *Journal of Digital Technologies and Law*, *2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Содержание

Введение
1. Правовые аспекты трансграничной передачи персональных данных
   1.1. История формирования правоотношений, связанных с трансграничной передачей персональных данных
   1.2. Регулирование трансграничной передачи персональных данных законодательством Российской Федерации и международными нормами
2. Технико-технологические аспекты трансграничной передачи данных
   2.1. Основные технические каналы связи, по которым осуществляется трансграничная передача персональных данных
   2.2. Модель выявления фактов незаконной трансграничной передачи персональных данных посредством технических средств и реагирования на них
Заключение
Список литературы

Введение

Стремительное развитие технологий и общества в целом привело к стиранию границ между странами в виртуальном пространстве. Данное явление влечет за собой множество положительных последствий: возможность международного общения, доступность зарубежного образования, способность покупать товары из-за рубежа

и т. д. Однако оно не лишено и негативных проявлений, одним из которых является нелегальная трансграничная передача персональных данных.

Сегодня в России действуют достаточно строгие правила для осуществления такой передачи, в результате чего операторы персональных данных не всегда оказываются способны точно их соблюдать. Помимо этого, с каждым годом все чаще совершаются злоумышленные атаки, в результате которых персональные данные широкого круга лиц оказываются в открытом доступе и на зарубежных серверах, что нарушает конституционные права граждан, подрывает национальную безопасность государства и выливается в значительные штрафы для юридических лиц.

В этой связи перед нами стояла цель предложить оптимальную комплексную юридико-технологическую модель минимизации рисков незаконной трансграничной передачи персональных данных, соблюдя при этом баланс интересов всех заинтересованных лиц. Для достижения этой цели нами были решены следующие задачи: изучена история формирования отношений в данной сфере; проанализированы действующие нормативные положения, регламентирующие трансграничную передачу персональных данных как на национальном, так и на международном уровнях; сформулированы предложения по оптимизации этих норм; установлены основные каналы, по которым персональные данные могут быть переданы за рубеж, и установлены узлы, посредством воздействия на которые возможно предотвратить несанкционированные потоки; предложен алгоритм выявления инцидентов информационной безопасности в данной области и реагирования на них.

Считаем, что практическая реализация изложенных в настоящей работе предложений и акцентуация внимания на затронутых проблемах не только представят интерес для научного сообщества, но и позволят уменьшить нелегальные трансграничные потоки персональных данных.

1. Правовые аспекты трансграничной передачи персональных данных

1.1. История формирования правоотношений, связанных с трансграничной передачей персональных данных

Сегодня персональные данные априорно ассоциируются с «чувствительной» информацией (Ji et al., 2023), несанкционированное попадание которой третьим лицам является крайне нежелательным. Однако так было не всегда: долгое время в мире господствовал порядок, при котором, с одной стороны, права отдельного человека не имели значения, а с другой – отсутствовали глобализационные явления, порождающие активное международное взаимодействие на частном уровне. В этой связи феномен персональных данных не представлял интереса для его правовой регламентации, а трансграничной передачи такой информации в принципе не существовало – персональные данные человека могли попасть в другое государство только вместе с ним или непосредственно в связи с его скорым прибытием в это государство (например, при путешествии или в рамках направления дипломатических представителей из одной страны в другую). В то же время, если «личность» кого-то похищалась и противоправно использовалась за рубежом, данный факт никак не сказывался на жизни того, чьи данные оказались у злоумышленников.

Вместе с тем развитие общества постепенно привело к системным изменениям и в сфере персональных данных: так, уже во время Великой французской революции был поднят вопрос об уважении личности, ее свобод и в том числе права на личную тайну.

В Российской империи подобные права были легализованы по инициативе самого императора: Александр II принял Почтовый и Телеграфный уставы, в которых закрепил неприкосновенность частной жизни и тайну переписки. Также в Уголовном уложении были предусмотрены санкции за нарушение указанных норм (Балашкина, 2007). Подобная гарантия соблюдения личной тайны была исключена из правового поля после Великой Октябрьской революции, однако в Конституции СССР 1936 г. вновь появились положения, предусматривающие неприкосновенность личности, тайну переписки[1].

Однако в строгом понимании концепция персональных прав человека была еще очень далека от устоявшегося сегодня понимания персональных данных и режима их защиты. Первым профильным явлением, приближенно отвечающим современным реалиям, стала теория С. Уоррена и Л. Брендайса – американских юристов, которые в 1890 г. сформулировали понятие privacy как права «быть оставленным в покое» (Балашкина, 2007). Спустя примерно полвека было дано судебное толкование данной категории, из которого следует, что под privacy подразумевается неприкосновенность персональных данных и этот принцип вытекает из первых поправок к Конституции США.

Широкое же развитие концепция персональных данных получила только во второй половине XX в. и примерно в то же время на фоне зарождающейся цифровизации и интенсифицирующихся глобализационных явлений возник феномен трансграничной передачи такого рода информации.

Оговоримся, что под трансграничной передачей данных мы понимаем перемещение из государства, в котором субъект добровольно предоставил определенные сведения, позволяющие идентифицировать (однозначно установить) его личность, конкретному лицу (оператору), в иное государство с предоставлением третьим лицам последнего, совершенное оператором, в том числе без уведомления субъекта. Таким образом, равно как и законодательные нормы, о которых будет сказано далее, мы не рассматриваем ситуацию самостоятельного сообщения субъектом сведений о себе представителям иного государства, например, в случае путешествия за границу, когда при заселении в отель человек предоставляет свой паспорт и его данные вносятся в базу данных зарубежной гостиницы.

Интерес международного сообщества к описанному явлению оформился только после начала «компьютерной эпохи» (Romansky & Noninska, 2020; Zheng, 2021), поскольку в это время стали очевидны многие риски, связанные с отсутствием единых стандартов межгосударственного оборота персональных данных и их защиты в процессе такого оборота.

С одной стороны, получение различных прав и привилегий, реализация естественных интересов людей в эпоху широкого распространения Интернета почти невозможны без трансграничных потоков различных персональных данных (Fuentes, 2020). Это связано с развитием международного бизнеса, когда учредитель расположен в одном государстве, а его филиалы и представительства

[1] Глушкова, С. И. (2002). Права человека в России: теория, история, практика: учеб. пособие. Екатеринбург.

функционируют во множестве стран; дистанционным оформлением зарубежных командировок внутренней кадровой службой; направлением тяжелобольного человека на лечение в другое государство и множеством иных, нередко самых бытовых ситуаций (Артемова, 2023). Отдельно следует описать практику, широко распространенную в России до 2015 г. и связанную с использованием зарубежных баз данных, расположенных вне пределов Российской Федерации, для хранения персональных данных, полученных отечественными компаниями. Подобное использование сторонних ресурсов было связано с их дешевизной и существованием как таковых (Смоленский, Левшин, 2016), поскольку ранее в России отсутствовал запрос на разработку собственных надежных и доступных бизнесу различного размера баз данных, способных обрабатывать значительные объемы информации и выдерживать злоумышленные атаки. На аналогичные проблемы указывается и в зарубежных публикациях (Abdulrauf et al., 2023).

С другой стороны, персональные данные – очень ценный ресурс в условиях современного мира. Их легальная обработка позволяет коммерческим компаниям производить более адаптированные под интересы целевой аудитории товары, создавать таргетированную рекламу, привлекая новых клиентов и увеличивая прибыль. Для государств персональные данные необходимы в целях борьбы с преступностью и различного рода правонарушениями (в части использования камер с автоматическим распознаванием лиц, проведения геномной и дактилоскопической идентификаций и пр.), агрегирования статистических данных о населении (состояние здоровья, уровень жизни и т. п.), прогнозировании политических решений, которые получат поддержку населения, и др. Одновременно с этим персональные данные интересны и для злоумышленников, поскольку предоставляют им возможность реализовать различного рода хищения, дискредитировать конкретную личность в медиапространстве, шифровать собственную личность при реализации противоправных действий и т. д.

Таким образом, формируется многосторонний конфликт интересов даже в рамках одного государства, где граждане ратуют за неприкосновенность и сохранение в тайне собственных персональных данных (Абрамова, 2020), коммерческие организации стремятся увеличить прибыльность собственного бизнеса за счет использования информации о клиентах, злоумышленники стараются похитить персональные данные, чтобы облегчить или обеспечить возможность совершения тех или иных преступных действий, а государство стремится к единоличному контролю за максимальным числом сведений о собственных гражданах.

Ситуация усугубляется, если добавить фактор трансграничности, поскольку у субъектов персональных данных значительно снижается контроль за сведениями о себе; в коммерческом секторе повышается конкуренция, а значит, возрастает и спрос на большие объемы персональных данных потенциальных потребителей; злоумышленникам становится легче остаться безнаказанными и неустановленными за счет распределения различных стадий преступной деятельности по разным странам с различными правовыми режимами, условиями защиты персональных данных и правилами по выдаче преступников; государства же теряют часть контроля за персональными данными собственных граждан и одновременно с этим приобретают потенциальную возможность получения соответствующих сведений о жителях других стран, что может становиться инструментом в международном противодействии и политическом давлении.

Законодательные и международные нормы призваны найти баланс между частными интересами свободы физических лиц, коммерческим интересом компаний и стремлением государств к обеспечению безопасности. Представляется, что современные нормы права вполне обеспечивают некий компромисс в этих отношениях, однако они основываются на презумпции добросовестности всех сторон взаимодействия, что приводит к упущению преступного элемента. Вместе с тем наибольшую угрозу и для естественных прав граждан, и для коммерческого интереса организаций, и для национальной безопасности государств несет злоумышленное похищение персональных данных или нарушение режима их секретности, в результате которого сведения о людях попадают в открытую сеть.

Так, только за 2023 г. было выявлено 168 утечек персональных данных, наиболее крупными из которых стали:

– из программы лояльности «Спасибо» от Сбербанка – 52,5 млн записей;
– из сети по продаже одежды для спорта «Спортмастер» – 46 млн записей;
– из онлайн-аптеки zdravcity.ru – 8,9 млн записей;
– из сервиса «Кассы.ру» – 4,5 млн записей;
– из магазина ювелирных изделий Zoloto585 – 9,9 млн записей;
– от страховщика «Согаз» – 8,3 млн записей.

Отдельно заслуживает внимания ситуация получения неправомерного доступа к персональным данным 1 000 000 пользователей МТС Банка. Всего было неправомерно обнародовано три файла с персональной информацией клиентов. Первый включал миллион строк с именами, номерами телефонов, полом, ИНН и гражданством. Во втором было три миллиона записей с типами, частью 16-значных номеров карт и датами их выпуска. Третий файл включал 1,8 млн телефонов, 50 000 e-mail и пользовательские идентификаторы[2].

Один из наиболее масштабных инцидентов произошел летом 2024 г., когда в открытый доступ попали сведения, обрабатываемые Департаментом информационных технологий Москвы, по состоянию на сентябрь 2023 г. В обнародованном файле содержится 13 462 446 строк со следующей информацией о москвичах и гостях столицы, которые использовали цифровые сервисы:

– фамилия, имя, отчество;
– номер телефона (7,2 млн уникальных номеров);
– адрес электронной почты (4,8 млн уникальных адресов, более 16 тыс. из которых находятся на домене @mos.ru);
– адрес регистрации и фактического места проживания;
– дата рождения;
– серия, номер паспорта или свидетельства о рождении;
– место рождения;
– номер социальной карты москвича;
– номер полиса обязательного медицинского страхования[3].

---

2 Талаш, А. Утечка персональных данных: громкие скандалы, кого оштрафовали в прошлом году и как будут наказывать в 2024? Rosco. https://clck.ru/3EmK8s

3 Нефедова, М. В ДИТ Москвы заявили, что опубликованные хакерами данные – это компиляция. Хакер. https://clck.ru/3EmK9J

Укажем, что на момент написания работы правительство Москвы не подтверждает факт произошедшей утечки, сообщая о компиляции данных, свободно находящихся в сети по вине самих граждан либо в результате нарушения безопасности иных операторов.

Во всех описанных ситуациях персональные данные россиян попадали также на информационные ресурсы зарубежных государств, т. е. осуществлялась явная незаконная трансграничная передача данных по принципу прорвавшейся плотины. Однако неменьшую опасность представляет более скрытая трансляция такого рода сведений за рубеж[4].

Всего же за 2023 г. в открытый доступ попало более 300 млн записей с персональными данными российских граждан, что обернулась для бизнеса штрафами на общую сумму свыше 4,6 млн рублей[5]. И это только статистика по Российской Федерации, тогда как проблема носит мировой характер (Jurcys et al., 2022). Однако представляется, что ужесточение ответственности юридических лиц за происходящие нарушения конфиденциальности персональных данных пользователей не является оптимальной мерой, поскольку направлено на разрешение симптомов, но не борьбу с первопричиной – злоумышленниками, осуществляющими кибератаки. Такая ситуация связана, на наш взгляд, со сложностью выявления утечек в процессе, когда конфиденциальность уже нарушена, но данные еще не стали широкодоступными, а также с фактом принадлежности преступников к другим государствам и использованию ими высокотехнологичных средств шифрования собственных личности и действий. В этой связи представляется необходимым, с одной стороны, развивать международное и национальное законодательство в части наказания действительно виновных в нарушении неприкосновенности персональных данных, а с другой – создавать и внедрять в практическую деятельность Роскомнадзора специальные технологические средства выявления и блокировки противоправной трансграничной передачи персональных данных. Именно анализу действующего законодательства в рассматриваемой сфере и описанию моделей подобных технологических решений будут посвящены следующие части настоящей работы.

1.2. Регулирование трансграничной передачи персональных данных законодательством Российской Федерации международными нормами

В Российской Федерации базовой нормой, определяющей порядок трансграничной передачи персональных данных, выступает ст. 12 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[6] (далее – 152-ФЗ), которая претерпела с 2006 г. четыре редакции. Если изначально в ней было только три части, то сегодня, с последними поправками от 14 июля 2022 г., она состоит из 15 частей. Указанное наглядно подтверждает тенденции, с одной стороны, к интенсификации

[4] Пояснительная записка к проекту Федерального закона «О внесении изменений в Федеральный закон “О персональных данных” и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных». СОЗД. https://clck.ru/3EmKC8

[5] Роскомнадзор зафиксировал 168 утечек данных в 2023 году. Право.ru. https://clck.ru/3EmKCx

[6] О персональных данных. № 152-ФЗ от 27.07.2006/ (2006, 31 июля). Собрание законодательства Российской Федерации, № 31 (ч. I), ст. 3451.

глобализационных процессов, а с другой – к увеличению случаев такой трансграничной передачи данных, которая, не будучи напрямую запрещенной законом, нарушает законные права и свободы граждан, интересы государства в целом. Мы не будем углубляться в историческое сопоставление, сосредоточив свое внимание на актуальном нормативном регулировании вопроса.

Так, современная редакция статьи детально регламентирует процедуру трансграничной передачи персональных данных, согласно которой:

1. Перечень государств, в которые могут передаваться персональные данные из России, условно ограничен теми странами, которые либо являются членами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, либо обеспечивают высокие стандарты защищенности персональных данных по национальному законодательству.

2. Данное правило не является абсолютным, так как в крайних случаях возможна передача персональных данных в иные государства.

3. Любой оператор персональных данных обязан направлять в уполномоченный орган – Роскомнадзор[7] – отдельное мотивированное уведомление о намерении передать персональные данные за границу, указывая цели передачи, страну и конкретных получателей этой информации.

4. Роскомнадзор может принять решение о запрете передачи персональных данных в определенное государство или в определенной ситуации.

5. Указанная возможность не является абсолютной, однако круг оснований очень широкий и включает в себя:

– защиту основ конституционного строя России, нравственности, здоровья, прав и законных интересов граждан;

– обеспечение обороны страны и безопасности государства;

– защиту экономических и финансовых интересов Российской Федерации;

– обеспечение дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене.

6. Если будет принято решение о недопустимости передачи персональных данных, когда такая передача уже состоялась, то переданные персональные данные должны быть уничтожены, за что отвечает первоначальный оператор.

Также необходимо отметить, что в тексте ст. 12 152-ФЗ предусмотрено, что трансграничная передача персональных данных осуществляется в соответствии с вышеназванным федеральным законом и международными договорами Российской Федерации, которые, учитывая положения Конституции Российской Федерации, не могут быть приняты, если их положения или толкование противоречит Основному закону. В этой связи при анализе международных актов считаем целесообразным остановиться только на документах, ратифицированных в Российской Федерации.

---

7 Постановление Правительства РФ № 228 от 16.03.2009. https://clck.ru/3EmKGN

Центральным международным договором, который применяется для решения вопросов трансграничной передачи данных, является Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[8] (далее – Конвенция). Данная конвенция была принята в 1981 г. и незначительно модернизирована в 2018-м (в нее включены нормы, регламентирующие использование систем на основе технологии искусственного интеллекта для автоматизированной обработки персональных данных). Изначально документ подписали 44 государства, на сегодняшний день ее членами наравне с Россией являются 55 государств: Австрия, Азербайджан, Албания, Андорра, Аргентина, Армения, Бельгия, Болгария, Босния и Герцеговина, Буркина-Фасо, Великобритания, Венгрия, Германия, Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кабо-Верде, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Маврикий, Мальта, Марокко, Мексика, Молдова, Монако, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сан-Марино, Северная Македония, Сенегал, Сербия, Словакия, Словения, Тунис, Турция, Украина Уругвай, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония.

Данный нормативный акт регулирует отношения, возникающие при хранении персональных данных, т. е. любой информации об определенном или поддающемся определению физическом лице: осуществлении логических и/или арифметических операций с этими данными, их изменении, уничтожении, поиске или распространении, если эти действия осуществляются полностью или частично с помощью автоматизированных средств. В общих чертах положения Конвенции аналогичны нормам и гарантиям, закрепленным в 152-ФЗ, поскольку именно на основе Конвенции был принят закон Российской Федерации, однако, что естественно для международных соглашений, она носит более диспозитивный характер, оставляя широкий простор для усмотрения договаривающихся сторон. Мы не будем останавливаться на обзоре данной Конвенции, осветим лишь ту норму, которая непосредственно касается темы настоящего исследования.

Так, ст. 12 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных регулирует особенности трансграничной передачи персональных данных, устанавливая в качестве общего правила, что Стороны не могут запрещать или ограничивать трансграничные потоки персональных данных между собой только по мотиву защиты частной жизни. Вместе с тем из данного правила существует два исключения – в следующих ситуациях Стороны могут свободно запрещать или ограничивать передачу:

1) законодательное регулирование обработки отдельной категории персональных данных в стороне исхода отличается от аналогичных норм в принимающем государстве;

2) с территории принимающего государства персональные данные будут переданы в страну, не являющуюся Стороной Конвенции.

Таким образом, несмотря на, казалось бы, жесткое правило, гарантирующее свободную передачу персональных данных между Сторонами Конвенции, из него существуют два достаточно широких исключения и, кроме того, оно само не является

[8] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 (Страсбург, 28 января 1981 г.). (2014, 3 февраля). Собрание законодательства Российской Федерации, 5, ст. 419.

настолько строгим, как может показаться при поверхностном анализе. Запрещая ограничения по мотиву защиты частной жизни, рассматриваемое положение не запрещает государствам использовать иные основания для подобных ограничений. Например, в России закреплено, что трансграничная передача данных может быть ограничена или запрещена в целях обеспечения национальной безопасности и по иным не менее уважительным и весомым причинам. Из этого можно сделать вывод, что положения ст. 152-ФЗ и ст. 12 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных не противоречат друг другу, национальное законодательство лишь более детально регламентирует вопросы, обеспечивая большую защищенность для персональных данных своих граждан.

Представляется, что подобный подход является правильным, поскольку, как это было показано выше и отмечается учеными, персональные данные являются чувствительной информацией, попадание которой к злоумышленникам может существенно навредить как одному конкретному гражданину, так и обществу в целом (Акулин и др., 2020). Однако действующее на сегодняшний день нормативное и организационное регулирование трансграничной передачи персональных данных далеко от совершенства. Существует позиция, что наиболее правильной является модель свободной передачи персональных данных между странами, а условное или запретительное регулирование негативно влияет на процессы международного взаимодействия (Ferracane & Van der Marel, 2024). Вместе с тем, на наш взгляд, указанная точка зрения сосредоточена исключительно на интересах бизнеса и игнорирует вопросы прав человека, обеспечения национальной безопасности и риски преступной деятельности в рассматриваемой сфере, в связи с чем необходимо разрабатывать более консенсуальную охранительную модель.

В первую очередь необходимо отметить, что, как известно, норма права должна состоять из трех элементов: гипотезы (описывающей общественные отношения, подлежащие регулированию), диспозиции (указывающей на требуемое или запрещенное поведение в данных общественных отношениях) и санкции (предусматривающей наказание за нарушение требований (запретов) к поведению). Если какой-либо из частей нет, то норма является «мертвой» и в действительности не будет применяться, лишится регулятивной силы. В этой связи, для того чтобы установленные ст. 12 152-ФЗ строгие правила трансграничной передачи персональных данных соблюдались, за их нарушение должна быть предусмотрена ответственность, с которой все не так однозначно. КоАП РФ в ст. 13.11, состоящей из девяти частей, предусматривает ответственность за различные нарушения законодательства о персональных данных, однако специальной нормы в части трансграничной передачи указанных сведений не существует, в связи с чем приходится обращаться к общему составу.

Так, ч. 1 ст. 13.11 КоАП РФ предусматривает, что «Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, влечет наложение административного штрафа на граждан в размере от 2 000 до 6 000 рублей; на должностных лиц – от 10 000 до 20 000 рублей; на юридических лиц – от 60 000 до 100 000 рублей»[9].

[9] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. (2002, 7 января). Собрание законодательства Российской Федерации, № 1 (ч. I), ст. 1.

Однако применение данной нормы видится затруднительным за счет очень размытой формулировки диспозиции. Так, с одной стороны, под случаи, не предусмотренные законодательством, или несовместимые цели может подпадать почти любое действие оператора, а с другой – несложно представить ситуацию, когда осуществляется формально легальная, но по факту противозаконная трансграничная передача персональных данных. Помимо этого, санкция данной нормы, если накладывать ее на ситуацию противозаконной трансграничной передачи персональных данных, оказывается очень незначительной, ведь прибыль от указанных противоправных действий может превышать суммы штрафов в десятки, а то и сотни раз.

Вместе с тем практика Роскомнадзора идет по иному пути: за рассматриваемые нарушения организации привлекаются по ч. 9 ст. 13.11, которая предусматривает, что «невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети “Интернет”, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, влечет наложение административного штрафа на граждан в размере от 30 000 до 50 000 рублей; на должностных лиц – от 100 000 до 200 000 рублей; на юридических лиц – от 1 000 000 до 6 000 000 рублей»[10].

Безусловно, санкция в данном случае намного существеннее, однако формально юридически приведенная норма вводит ответственность только за один частный случай противоправной трансграничной передачи персональных данных – неиспользование отечественных баз данных, что нарушает правило, введенное в 2015 г. В свою очередь, данное нормативное положение появилось только в 2019 г. Аналогичную ситуацию можно наблюдать и сегодня – введенная в 2022 г. усложненная процедура для трансграничной передачи персональных данных не обеспечена на сегодняшний день санкцией за нарушение ее правил, что негативно сказывается на регулятивном механизме. Считаем, что требуется в кратчайшие сроки разработать и принять специальную охранительную норму, направленную на предотвращение незаконной трансграничной передачи персональных данных. При этом считаем, что диспозиция такой нормы должна закреплять умышленную форму вины, чтобы операторы персональных данных не подлежали наказанию за кибератаку, совершенную на них. Это позволит уменьшить латентность подобных инцидентов, обеспечит сотрудничество операторов с правоохранительными органами и реализацию принципа справедливости санкции, так как она будет направлена против действительно виновных лиц. Одновременно с этим, особенно в условиях недружественной международной атмосферы, считаем необходимым ввести дополнительный квалифицирующий признак в ст. 272, 273, 274.1 Уголовного кодекса Российской Федерации (далее – УК РФ), предусмотрев в нем последствия в виде получения неправомерного доступа к охраняемой законом компьютерной информации лицами, находящимися за пределами Российской Федерации.

[10] Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30.12.2001 (ред. от 23.11.2024). (2024). СПС «КонсультантПлюс». https://clck.ru/3ExqcF

Следующая проблема связана с требованием самой ст. 12 152-ФЗ, согласно которому в случае принятия Роскомнадзором решения о запрете или ограничении трансграничной передачи персональных данных «оператор обязан обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им персональных данных»[11]. Представляется маловероятным, что правительство зарубежного, особенно недружественного, государства удалит полученные ранее из России персональные данные по указанию какой-либо коммерческой компании из нашего государства. Механизма, в соответствии с которым данное требование должно быть претворено в жизнь, не существует. Таким образом, учитывая уведомительный порядок трансграничной передачи персональных данных в государства, являющиеся Сторонами Конвенции Совета Европы или обеспечивающие адекватный уровень защиты персональных данных (еще 34 государства)[12], а также возможность в исключительных случаях осуществлять трансграничную передачу и в иные государства, создается весьма значительный риск утечек персональных данных россиян, их оставления на враждебной территории, после того как Роскомнадзор примет решение о том, что осуществленная передача не должна была произойти.

Если отойти от специальных норм, то можно выявить иную возможность защиты гражданами своих персональных данных от трансграничной передачи, предусмотренную п. 8 ч. 7 ст. 14 152-ФЗ, согласно которой субъект персональных данных вправе получать информацию об осуществленной или о предполагаемой трансграничной передаче его данных. В системном толковании с ч. 2 ст. 9 и ч. 1 ст. 14 152-ФЗ, предусматривающими, что субъект персональных данных может в любое время отозвать свое согласие на их обработку, а также может требовать от оператора удаления его персональных данных, в случае если человек не согласен с осуществлением трансграничной передачи его персональных данных, он может запретить осуществление таких действий оператором. Однако все описанные процессы должны быть инициированы самим субъектом, оператор не обязан сообщать о планируемой или осуществляемой трансграничной передаче персональных данных, пока от субъекта не поступит запрос на предоставление соответствующей информации. Вместе с тем большинство граждан, не обладая в должной мере развитой правовой культурой, могут не знать о данных особенностях, в связи с чем оказываются неспособными на практике защитить собственные интересы. К тому же, даже будучи осведомленным о приведенных правовых положениях, человек не способен отследить всех операторов, потенциально осуществляющих или планирующих осуществлять трансграничную передачу его персональных данных, поскольку таковых в отношении одного субъекта в современных условиях очень большое количество.

В этой связи считаем необходимым дополнить ст. 12 152-ФЗ правилом, предусматривающим обязательное уведомление субъекта персональных данных о намерении произвести трансграничную передачу информации о нем, а также предоставить

---

11 О персональных данных. № 152-ФЗ от 27.07.2006 (ред. от 08.08.2024). (2024). СПС «КонсультантПлюс». https://clck.ru/3Exr2K

12 Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 128 от 05.08.2022. https://clck.ru/3EmKNQ

ему возможность ограничить такую передачу в определенное государство или в конкретных ситуациях.

Несмотря на все сказанное выше, следует признать: в России предпринимаются комплексные меры для обеспечения максимальной защищенности персональных данных проживающих в государстве лиц. Так, нельзя не отметить Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21 июля 2014 г. № 242-ФЗ (так называемый Закон о локализации), внесший изменения в 152-ФЗ, согласно которым запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации должно осуществляться с использованием баз данных, находящихся на территории Российской Федерации[13].

Данное требование представляется весьма действенным для защиты персональных данных россиян, минимизации рисков утечек информации, обеспечения государственного контроля за сведениями о своих гражданах, а также исключения риска возникновения ситуаций, когда персональные данные российских граждан окажутся недоступными для отечественных компаний и государства по причине блокировки тех или иных зарубежных сервисов, отключения российских пользователей от зарубежных баз данных, будут использоваться для совершения преступлений. Однако данной позиции придерживаются не все – так, уже в 2015 г., когда описанная норма только вступала в силу, были разработаны сценарии ее обхода с целью минимизации убытков бизнеса (Веселицкий, 2015). В связи с чем на сегодняшний день можно ожидать широкое распространение серых схем, позволяющих в действительности хранить персональные данные российских граждан за рубежом.

Из всего описанного выше можно сделать вывод, что нормативная регламентация рассматриваемого вопроса не способна в должной мере обеспечить защиту персональных данных россиян. Однако предупреждение случаев незаконной трансграничной их передачи – фундаментальная задача российского государства, от решения которой зависит безопасность населения страны и устойчивость государственной власти. В этой связи необходимо не только совершенствовать законодательство, но и разрабатывать технологические механизмы, которые позволили бы эффективно выявлять и блокировать подозрительные потоки персональных данных за пределы территории Российской Федерации до выяснения всех обстоятельств и принятия квалифицированного решения.

2. Технико-технологические аспекты трансграничной передачи данных

2.1. Основные технические каналы связи, по которым осуществляется трансграничная передача персональных данных

Для того чтобы перейти к непосредственному описанию технических средств предотвращения незаконной трансграничной передачи персональных данных, необходимо определить каналы потенциальной утечки информации. В настоящее время передача

[13] О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях. № 242-ФЗ от 21.07.2014. (2014). https://clck.ru/3EmKSW

персональных данных, которая может представлять угрозу, осуществляется посредством компьютерных сетей. Безусловно, многие компании, например, ведут бумажные личные дела сотрудников, однако ситуация, при которой идентифицирующие сведения из них будут получены в большом объеме, сохранены, переданы через границу и опубликованы так, чтобы быть доступными широкому кругу лиц, в том числе в целях их последующего преступного использования, полностью посредством аналоговых форм, представляется нереалистичной. Именно поэтому нами будут рассмотрены именно технические каналы связи, представленные компьютерными сетями.

Для прогнозирования уровня угрозы от противоправного доступа к информации, а также определения возможностей минимизации кибератак и утечек важно точно определить территорию, в рамках которой действует канал связи. Так, выделяются:

1. Глобальные сети. Самой известной из них является Интернет; они опоясывают весь мир. Кроме того, к глобальным будут относиться и внутринациональные сети, функционирующие в пределах конкретной страны или региона. Обеспечить полноценную защиту информации в таких сетях почти невозможно из-за принципа открытости и общедоступности, лежащего в основе их функционирования.

2. Городские сети. Из названия очевидно, что они существуют в пределах города. Однако чаще к этому уровню относят только сети, обслуживающие мегаполисы или городские агломерации. Именно на уровне городских сетей изначально было организовано специальное программное обеспечение «Паутина».

3. Корпоративные сети (организаций, предприятий). Сети данного уровня, с одной стороны у́же городских, поскольку направлены на обслуживание отдельных предприятий, но с другой – такие сети действуют трансгранично, т. е. позволяют связывать между собой филиалы и подразделения, расположенные в разных городах, регионах и странах.

Отметим, что корпоративные сети являются наиболее уязвимыми с точки зрения информационной безопасности, защищенности от кибератак, поскольку охватывают значительную территорию, но обслуживаются частным сектором, который бывает ограничен в ресурсах для постоянного обновления протоколов безопасности и не связан столь строгими правилами защиты информации, как государственные предприятия.

Вместе с тем к корпоративным сетям будут относиться и ведомственные каналы связи, степень защищенности которых наивысшая, поскольку по ним передается информация ограниченного доступа.

4. Локальные сети сосредоточены на небольшой территории (обычно в радиусе 1–2 км). Они функционируют на территории одного предприятия (завода, больницы, образовательного учреждения и т. п.). Обычно такие сети защищены достаточно хорошо, так как организованы в секторе, где оборот охраняемой законом информации осуществляется на ограниченной территории и посредством идентифицированного оконечного оборудования, при наличии достаточных ресурсов для настройки и поддержания систем безопасности.

5. Персональные сети предназначены для взаимодействия устройств, принадлежащих одному владельцу (членам семьи), на небольшом расстоянии (обычно до 10 м). Несмотря на низкую степень территориальной распределенности, отдельный человек может не уделять достаточного внимания соблюдению правил информационной безопасности и цифровой гигиены, что ставит его инфраструктуру под угрозу.

Как очевидно из приведенной классификации, трансграничная передача персональных данных может осуществляться исключительно по глобальным и корпоративным сетям. Вместе с тем в последнем случае подобного рода информация защищается и, если происходит инцидент, безопасность нарушается, то сведения передаются на глобальные сети, где и становятся доступными широкому кругу лиц, в том числе представителям иных государств. В этой связи можно сделать промежуточный вывод, что контроль за незаконной трансграничной передачей персональных данных будет наиболее эффективным на границе защищенного канала связи и глобальной сети. Такой подход позволит минимизировать риски ложноположительных ошибок, когда блокироваться будут легальные внутренние (между государственными органами, внутри подразделений юридического лица, между устройствами одного пользователя) потоки.

Для обоснования данного тезиса считаем необходимым остановиться подробнее на характеристике глобальных компьютерных сетей. Основная их характерная черта заключается в том, что они имеют децентрализованную архитектуру, распределены по континентам, странам, а физически могут быть расположены не только на земной поверхности, но и над ней, под водой – где угодно. Часть сегментов глобальных сетей могут быть продублированы в том числе с помощью спутниковых коммуникаций. Это в совокупности с указанным ранее основополагающим принципом открытого доступа позволяет создать систему, при которой любое устройство, имеющее выход в глобальную сеть, может взаимодействовать с любым иным подключенным оборудованием.

Чаще всего глобальные компьютерные сети опираются на выделенные линии, на одном конце которых маршрутизатор подключается к локальной сети, а на другом – коммутатор связывается с остальными частями глобальной. Более подробно об этих элементах будет сказано далее, так как они имеют определенное значение для выявления фактов несанкционированной передачи персональных данных.

Отметим, что современные компьютерные сети очень многое унаследовали от своих предшественников – линий телефонной связи. Главное технологическое новшество, которое привнесли с собой первые, состояло в отказе от принципа коммутации каналов, при котором для взаимодействия требуется физическое подключение двух устройств, выделение для их связи отдельного канала. На смену ему пришла технология многоуровневой коммутации пакетов, когда информация разделяется на маленькие блоки, передающиеся адресату по разным маршрутам.

В связи с таким устройством глобальных компьютерных систем невозможно контролировать потоки информации (в том числе персональных данных), когда они оказываются внутри системы (Иванова и др., 2010), поэтому все мероприятия по блокировке канала передачи данных должны быть осуществлены на местном уровне, поддающемся централизованному администрированию.

Помимо уровня сети, важным для вопроса предотвращения несанкционированных потоков персональных данных является определение среды, по которой передается информация. Это может быть:

– оптоволокно;
– медные провода;
– инфракрасный канал;
– радиоканал (Wi-Fi, LTE, Bluetooth и др.).

Проще всего осуществлять перехват, а значит, и блокирование информации, передающейся по материализованным средам – оптическим волокнам и медным проводам, так как в этом случае, что будет показано далее, техническое устройство, выявляющее несанкционированные потоки персональных данных, можно установить непосредственно на сам канал. Однако в этом случае весьма затруднительно определить тип передающихся данных – для этого необходимо осуществить их расшифровку, что требует дополнительных временных затрат и использования специального оборудования. Поэтому намного полезнее иметь доступ к так называемым узлам инфраструктуры – локальному сетевому оборудованию, которое может быть активным или пассивным.

Активное оборудование – это те устройства, которые непосредственно подключены к сетям и в связи с этим обеспечивают передачу и маршрутизацию данных. С помощью них возможно осуществлять полный цикл обработки данных: прием, систематизацию, хранение, управление, передачу – для этого такие устройства оборудованы собственным процессором и оперативной памятью.

Пассивное оборудование может быть названо вспомогательным: оно характеризуется отсутствием собственного источника питания и поэтому не может оказывать какого-либо воздействия на проходящие потоки данных. Здесь можно провести метафорическую аналогию с мостом через реку, когда по обеим сторонам от него установлены светофоры, знаки, регламентирующие порядок движения, но сам он – только участок дороги, на котором получить новую информацию и модернизировать под ее влиянием поведение нельзя. Так и пассивное оборудование лишь создает среду для передачи данных, не управляя трафиком и не производя обработку данных. К пассивному оборудованию относятся, в частности:

– кабели (например, витая пара или оптоволоконный кабель), применяющиеся для соединения устройств и передачи данных между ними;

– разъемы, патч-панели и кроссовые поля, применяющиеся для соединения кабелей и устройств;

– разветвители или сращивающие коробки, применяющиеся для разделения или объединения оптоволоконных линий связи.

Таким образом, роль пассивного сетевого оборудования сводится к обеспечению более эффективного и надежного функционирования сети, в связи с чем блокировать потоки персональных данных на нем затруднительно.

Активное сетевое оборудование очень разнообразно и выполняет разнообразные функции:

– распределение трафика между сетями;

– соединение локальных сетей на разных уровнях (от внутриорганизационного до мирового);

– обеспечение беспроводной связи между устройствами внутри локальной сети;

– определение целевого направления пакетов данных.

Последнее представляет особый интерес для настоящего исследования, поскольку таким образом возможно установить, что определенные чувствительные данные направляются за рубеж (на устройство, MAC-адрес которого зарегистрирован за рубежом).

Исходя из рассмотренных особенностей, следует, что для эффективного предотвращения несанкционированных трансграничных потоков чувствительной информации, минимизации рисков ложноположительных и ложноотрицательных ошибок при определении направления движения информации, необходимо с помощью специализированных технических устройств воздействовать именно на активное сетевое оборудование.

Вместе с тем существует множество различных типов сетевых устройств, каждое из которых обладает своими уникальными особенностями, характеристиками и предназначением, в связи с чем мы остановимся только на кратком описании тех из них, на которые целесообразно воздействовать для предотвращения несанкционированных трансграничных потоков персональных данных.

1. Коммутатор или свитч. Это устройство, имеющее временную (промежуточную) память, связывает конечное число устройств в единую сеть. Количество устройств, которые может связать коммутатор зависит от числа имеющихся у него портов.

Общий принцип его работы можно представить следующим образом: на первом этапе на коммутатор поступают данные, которые передаются на все порты, при этом MAC-адрес отправителя идентифицируется и закрепляется за одним конкретным портом. Далее, если поступают пакеты, предназначенные для устройства с идентифицированным MAC-адресом, то они передаются только на закрепленный за ним порт. В противном случае данные передаются на все порты. Со временем происходит идентификация всех взаимодействующих в сети устройств.

В аспекте рисков несанкционированной трансграничной передачи данный коммутатор может быть полезен для детекции источника их исхода (т. е. определения личности виновного сотрудника), а также выявления самого факта передачи персональных данных.

Аналогичные функции, но в ином, более широком масштабе выполняют концентраторы (хабы), которые отличаются от коммутаторов большей уязвимостью к угрозам информационной безопасности за счет меньшей «интеллектуальности».

2. Роутер или маршрутизатор предназначен для передачи пакетов данных между разными компьютерными сетями. Для этого он использует таблицу маршрутизации, в которой содержатся MAC-адреса оконечных устройств и пути связи с ними. Роутер сопоставляет MAC-адрес получателя, указанный в пакете данных, с указанной таблицей и передает сведения адресату. Одновременно с этим маршрутизатор – модерируемая система, функционирующая по правилам, заданным администратором, который может указать на необходимость фильтрации трафика, шифрования (дешифрования) определенных данных, осуществления иной их обработки.

Таким образом, осуществлять детектирование инцидентов несанкционированной трансграничной передачи данных оптимальнее всего именно на уровне маршрутизатора, автоматизировав этот процесс посредством введения нескольких дополнительных правил на этапе его установки и настройки. Однако маршрутизатор не предназначен специально для такого контроля, в отличие от следующего элемента сетевой инфраструктуры.

3. Межсетевой экран, или Firewall, – программный или программно-аппаратный комплекс, специально функционирующий для защиты компьютерной сети от несанкционированного доступа, злоумышленных атак, хищения данных и других угроз внешней среды. Основные задачи, решаемые межсетевым экраном, сводятся к следующим:

– фильтрация трафика;

– блокировка попытки входа в сеть из неизвестных или недоверенных источников;

– блокировка передачи (приема) определенных типов трафика (например, трафика с вредоносным содержимым или персональными данными), и пр.

Безусловно, любое из описанных устройств может быть использовано для детекции потоков персональных данных, предотвращения или как минимум выявления не только их свободной передачи за рубеж, но и злоумышленного похищения. Однако наибольший эффект такие мероприятия будут иметь при их воспроизведении на узлах маршрутизаторов и межсетевых экранов. Далее мы рассмотрим несколько обобщенный сценарий указанных защитных мероприятий.

2.2. Модель выявления фактов незаконной трансграничной передачи персональных данных посредством технических средств и реагирования на них

Прежде чем перейти к описанию заявленной модели, оговоримся, что настоящая часть исследования будет предметно ограничена действиями внутри юридического лица или государственного органа, являющихся операторами персональных данных. Также мы не будем рассматривать методы предотвращения атак, нацеленных на хищение персональных данных, так как они в общем виде сводятся к постоянному обновлению протоколов безопасности и оборудования, соблюдению всех требований технических регламентов и Роскомнадзора в данной сфере, использованию сертифицированного и лицензионного программного обеспечения. Однако и эти меры не гарантируют безуспешность любых злоумышленных атак, поэтому считаем важным создать механизм выявления нелегальных трансграничных потоков персональных данных вне зависимости от того, по какой причине они произошли: в результате внешнего прорыва контура безопасности или вследствие неправомерных (либо ошибочных) действий со стороны самого оператора. При этом, поскольку основная проблема на сегодняшний день сосредоточена вокруг крупных операторов персональных данных в лице корпораций и государственных органов, мы сосредоточимся именно на детекции потоков из локальных, городских и корпоративных сетей, которые далее для упрощения будут обобщенно называться локальными.

Укажем, что базовым мероприятием, в рамках которого может быть выявлена и предотвращена несанкционированная трансграничная передача персональных данных, является контроль. Представляется, что он не только должен быть предусмотрен в локальных актах и инструкциях как обязательный элемент управления сетью, но и состоять из совместных усилий технических, в том числе автоматизированных, устройств и человека.

Процесс контроля работы сети обычно делят на два этапа: мониторинг и анализ. Вместе с тем большое значение имеет предварительная подготовка, которая подразумевает разработку локальных актов организации, нормативное закрепление порядка выявления, обработки информации об инцидентах информационной безопасности и реагирования на них (Rowe, 2003).

На этапе мониторинга собираются первичные данные, необходимые в дальнейшем для осуществления анализа ситуации и принятия обоснованного решения (Pascual et al., 2024). Мониторинг, особенно у крупных операторов персональных данных, может (и, скорее, должен) осуществляться с помощью технических средств.

Причем считаем необходимым разработать программно-аппаратный модуль, который можно будет интегрировать в оборудование конкретной организации, государственного органа, адаптировать под специфику деятельности оператора и его технико-технологические ресурсы, обеспечивая эффективное накопление всей релевантной информации. Такое устройство должно работать по следующему алгоритму:

1. Фиксация факта, исходящего за пределы локальной сети потока данных (любых).

2. Фильтрация потоков персональных данных (их задержка).

3. Определение направления данных потоков.

3.1. Если поток направлен за границу – его блокирование.

3.2. Если поток носит внутренний характер – его пропуск.

4. Информирование уполномоченного лица оператора о выявленном потоке, передача такому сотруднику всей сопроводительной информации (время, источник, направление и т. д.).

При этом может быть использована программная реализация, аналогичная той, которая уже положительно зарекомендовала себя при выявлении и обработке цифровых следов пользователя (Daniela & Amélie, 2022). Отметим также, что при необходимости такое устройство может быть настроено на блокировку любых потоков персональных данных или иного рода сведений до их предварительной проверки уполномоченным лицом.

Далее уполномоченным работником выполняется анализ – осмысление собранной на этапе мониторинга информации, сопоставление ее с профильными (целевыми) шаблонами и последующее принятие управленческого решения. На данном этапе человек должен оценить в части трансграничных потоков персональных данных:

1) передаются ли они в государство, являющееся Стороной Европейской конвенции или обеспечивающее надлежащую защиту персональных данных;

2) уполномочен ли оператор на осуществление трансграничной передачи персональных данных;

3) направлено ли уведомление о данной передаче в Роскомнадзор;

4) соответствует ли информация, указанная в уведомлении, обстоятельствам и содержанию передающихся персональных данных;

5) нет ли запрета или ограничения на передачу этих персональных данных в конкретное государство при существующих условиях;

6) не поступило ли возражение от субъекта персональных данных на передачу сведений о нем за границу;

7) не нарушают ли цели передачи персональных данных законодательства Российской Федерации;

8) кто является инициатором передачи персональных данных (сотрудники организации или внешний субъект, нарушивший безопасность локальной сети).

После ответа на все указанные вопросы уполномоченное лицо принимает решение, допустить трансграничную передачу персональных данных или сообщить руководителю (либо в правоохранительные органы) о выявленном и своевременно предотвращенном инциденте информационной безопасности. В общем виде описанная модель представлена на рис. 1.

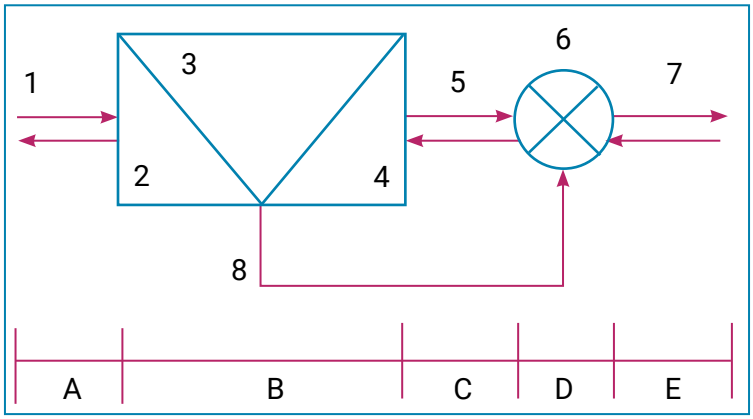

Рис. 1. Графическое представление модели выявления факта трансграничной передачи персональных данных и принятия управленческого решения

На участке «A» цифрой 1 показаны входящие и исходящие потоки данных физического, сетевого, канального, транспортного, сеансового, представительского, прикладного уровней. Получение для последующего анализа информации от всех семи уровней модели ISO/OSI в простых, иерархических, маршрутных, агрегатных и прочих формах необходимо в связи с тем, что поступающие данные, в том числе персональные, могут иметь не только текстовое представление.

На участке «B» в модуле 2 происходит определение получателя данной информации путем анализа его IP-адреса, доменного имени, иных подобных сведений и сопоставления с официальными данными о регистрации данных IP-адресов.

Сведения о принадлежности IP-адреса к географической (страновой) локации и юридическому или физическому лицу могут быть получены из официальных ресурсов регистраторов доменных имен[14]. Разумеется, в рассматриваемой модели наивысший приоритет доверия будет принадлежать регистраторам доменных имен, осуществляющим свою деятельность на территории России (в силу норм действующего законодательства и регуляторных норм Федеральной службы по техническому и экспертному контролю, Федеральной службы безопасности Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и пр.).

Если получатель находится в пределах Российской Федерации, то дальнейший анализ пакета не производится и он пропускается без изменений на участок «D» модуля 6. Если получатель находится за пределами Российской Федерации, то далее пакет обрабатывается модулем 3.

На участке «B» в модуле 3 происходят сбор и нормализация информации (данных), предназначенных для получателей за пределами страны. Именно здесь предполагается работа уполномоченного работника организации (государственного органа).

Процедура нормализации данных представляет из себя программно-математические преобразования (в том числе, но не ограничиваясь: TLS/SSL, HTTPS, HTTPX, E1/T1, ATM и другие) любых представлений данных в текстовую форму.

[14] Координационный центр доменных имен .RU/.РФ. https://clck.ru/3EmLBZ

На участке «B» в модуле 4 происходит анализ нормализованных данных на соответствие атрибутивно-содержательным признакам подпадающих под определение персональных данных.

Для этого в организации должен быть на уровне локального акта или инструкции определен список обрабатываемых персональных данных и разработаны соответствующие шаблоны (например, регулярные выражения), в соответствии с которыми осуществляется процедура детектирования целевой информации. Укажем, что в зависимости от конкретных задач оператора персональных данных модуль 4 может располагаться перед модулем 3, т. е. предшествовать человеческому анализу.

Если в проанализированном трафике выявлены совпадения с шаблонами информации, недопустимой для передачи, то на участок «D» модуля 6 посылается управляющее воздействие (элемент 8) об уничтожении (отбрасывании) конкретного пакета и журналировании данного события. Такая команда в рассмотренной модели может быть подана уполномоченным сотрудником, однако нельзя исключать и полностью автоматизированную работу предлагаемого программного модуля.

На участке «D» в модуле 6 находится корпоративный межсетевой экран, который, помимо своих основных функций, также при появлении управляющего воздействия (команды) с участка «B» принимает решение об уничтожении (отбрасывании) конкретного пакета и журналировании события защиты информации.

Элементы 5 и 7 являются стандартными потоками информации внутри локальной сети и модуля автоматизированной обработки потоков исходящих данных.

Подобные алгоритмы предлагаются и зарубежными коллективами ученых (Liu et al., 2024; Pascual et al., 2024; Guaman et al., 2021; Yan et al., 2023), в связи с чем считаем небесполезным также налаживать международное сотрудничество в указанной сфере, чтобы наиболее эффективно достигать целей защиты чувствительной информации.

Оговоримся, что рассмотренные нами мониторинг и анализ – лишь части более детального алгоритма, который включает в себя сопутствующие организационные мероприятия (создание локальных актов в сфере обеспечения информационной безопасности, сотрудничество с регулирующими государственными органами, осуществление общей и частной превенции и т. д.). Однако настоящее исследование не претендует на полноту и исчерпывающий характер, в связи с чем считаем достаточным осветить непосредственно те стадии управления, в рамках которых могут быть задействованы специализированные технические средства, как это было заявлено изначально.

Заключение

Подводя итог описанному выше, подчеркнем следующее.

1. Отношения по трансграничной передаче персональных данных смогли развиться только в цифровую эпоху, когда глобальные потоки информации вне границ какого-либо государства стали обыденностью, в связи с чем нормативное и политическое регулирование данной сферы только формируется.

2. Персональные данные являются ценным ресурсом: содержат в себе сведения о личной жизни человека, которые он желает сохранить в тайне; необходимы для развития бизнеса; требуются для эффективной борьбы с преступлениями и правонарушениями; выступают важным компонентом преступной и иной противоправной

деятельности; могут быть фактором в межгосударственной и межполитической борьбе.

3. Нелегальные трансграничные потоки персональных данных несут в себе серьезную угрозу для прав личности, национальной безопасности и финансового благополучия организаций, однако действующие национальные и международные нормы права не обеспечивают достаточный для их предотвращения механизм.

4. Для разрешения указанной проблемы требуется ввести специальный состав за нарушение установленного порядка трансграничной передачи персональных данных в КоАП РФ, дополнить квалифицирующие признаки в статьях УК РФ, посвященных нарушению безопасности компьютерной информации; обязать оператора персональных данных сообщать их субъекту о намерении осуществить трансграничную передачу такого рода информации.

5. Одновременно с оптимизацией законодательства требуется внедрять в системы обеспечения информационной безопасности организаций и государственных органов, выступающих операторами персональных данных специализированные технические средства детекции несанкционированных трансграничных потоков персональных данных.

6. Применение указанных средств должно производиться по следующему алгоритму: постоянный автоматизированный фоновый контроль всех исходящих потоков информации, определение их направления; выявление потоков, движущихся за границу государства; отнесение информации в данном потоке к персональным данным; блокировка потока, соответствующего двум указанным признакам; сообщение о выявленном потоке уполномоченному работнику организации (государственного органа); оценка человеком допустимости трансграничной передачи данных; принятие решение о пропуске или окончательной блокировке потока; сообщение в последнем случае о выявленном и предотвращенном инциденте информационной безопасности.

Представляется, что реализация описанного алгоритма, а также совершенствование нормативного регулирования в сфере трансграничной передачи персональных данных позволит снизить количество хищений и ненамеренных утечек данного рода чувствительной информации, тем самым защитить права граждан, обеспечить политическую устойчивость Российской Федерации, снизить число преступлений с использованием чужих персональных данных и добиться финансового благополучия у коммерческих организаций.

Список литературы

Абрамова, А. Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: Основополагающие принципы защиты персональных данных. *Регион и мир*, *11*(4), 21–25. https://www.elibrary.ru/eveayh

Акулин, И. М., Чеснокова, Е. А., Гурьянова, Н. Е., Пресняков, Р. А., Летова А. Д. (2020). Возможность трансграничной передачи связанных со здоровьем персональных данных в рамках ЕАЭС: реальность, перспективы. *Менеджер здравоохранения*, *7*, 65–73. https://doi.org/10.37690/1811-0185-2020-7-65-73

Артемова, А. Н. (2023). Правовое регулирование трансграничной передачи персональных данных. *Юридическая наука и практика*, *19*, 3, 9–16. EDN: https://www.elibrary.ru/cgfugw. DOI: https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Балашкина, И. В. (2007). Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации. *Право и политика*, *7*, 92–105. https://www.elibrary.ru/hzyhnn

Веселицкий, О. И. (2015). Вопросы трансграничной передачи персональных данных в соответствии с требованиями 242-ФЗ. *Сборники конференций НИЦ Социосфера*, *53*, 275–279. https://www.elibrary.ru/vbvgev

Иванова, О. В., Иванов, П. В., Смелов, М. Н. (2010). Проблемы и алгоритмы поиска информации в глобальных компьютерных сетях. *T-Comm: Телекоммуникации и транспорт*, *4*(3), 23–25. https://www.elibrary.ru/ophpnz

Смоленский, М. Б., Левшин, Н. С. (2016). Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России. *Наука и образование: хозяйство и экономика, предпринимательство, право и управление*, *2*(69), 111–114. https://elibrary.ru/item.asp?id=25423352

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Сведения об авторах

Бахтеев Дмитрий Валерьевич – доктор юридических наук, доцент, профессор кафедры криминалистики имени И. Ф. Герасимова, заведующий лабораторией цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Сосновикова Анна Михайловна – стажер-исследователь лаборатории цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Казенас Евгений Владимирович – студент, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Адрес: 620002, Россия, г. Екатеринбург, ул. Мира, 19
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77 / Уголовное право
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 28 июня 2024 г.
Дата одобрения после рецензирования – 12 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Overcoming Illegal Cross-border Transfer of Personal Data

Dmitry V. Bakhteev ✉
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Anna M. Sosnovikova
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Evgeniy V. Kazenas
Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia

Keywords

communications,
computer network,
cross-border data transfer,
digital technologies,
incident,
information security,
information,
law,
legislation,
personal data

Abstract

Objective: to form of a comprehensive interdisciplinary legal and technological risk management model in the field of illegal cross-border transfer of personal data by eliminating legislative gaps and creating a system for automated control of outgoing information flows, as well as expert response to identified incidents.

Methods: in addition to general dialectical and general scientific methods, special legal and cybernetic methods were used. For example, based on comparative legal analysis, the authors reveal differences between national and international regulation of cross-border flows of personal data. In the second section, the modeling method allows forming an algorithm for identifying information security incidents in the field of cross-border transfer of personal data and responding to them.

Results: the article formulates proposals to optimize legislation in the field under study by introducing specialized protective norms for violating the rules of cross-border transfer of personal data and stipulating the operator's obligation to notify personal data subjects of the intention to transfer the information abroad. The second section describes the concept of a software package designed to detect information security incidents in the field under consideration, as well as a model of action of an authorized representative of the operator after receiving a signal from the automated system.

✉ Corresponding author
© Bakhteev D. V., Sosnovikova A. M., Kazenas E. V., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: to solve the set problem, the work combines the knowledge and competencies of legal scientists and specialists in the field of information security, which allows an interdisciplinary approach. At the same time, it is stated that the issues of illegal cross-border transfer of personal data have not received proper coverage in science today, since Russian legislation in this area has changed recently. The authors propose not so much to strengthen the sanction for legislation violation in this area, as to ensure the punishment of persons who commit cyberattacks, and to equip personal data operators with an effective tool to minimize the risks of information leakage.

Practical significance: the research results can be used to improve legislation in the field of cross-border transfer of personal data and the organization of activities of authorized employees of the personal data operator for risk management in this area.

For citation

Bakhteev, D. V., Sosnovikova, A. M., Kazenas, E. V. (2024). Overcoming Illegal Cross-border Transfer of Personal Data. *Journal of Digital Technologies and Law, 2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

References

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Abramova, A. G. (2020). Contemporary issues of personal data protection in the network: fundamental principles of personal data protection. *Region i mir*, *11*(4), 21–25. (In Russ.).

Akulin, I. M., Chesnokova, E. A., Guryanova, N. E., Presnyakov, R. A., & Letova, A. D. (2020). Possibility of transboundary transfer of health-personal data within the EAEU: reality, prospects. *Menedzher Zdravookhranenia*, *7*, 65–73. (In Russ.). https://doi.org/10.37690/1811-0185-2020-7-65-73

Artemova, A. N. (2023). Legal regulation of cross-border personal data transfer. *Yuridicheskaya nauka i praktika*, *19*(3), 9–16. (In Russ.). https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Balashkina, I. V. (2007). Features of the constitutional regulation of the right to privacy in the Russian Federation. *Pravo i politika*, *7*, 92–105. (In Russ.).

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ivanova, O. V., Ivanov, P. V., & Smelov, M. N. (2010). Problems and algorithms of information retrieval in global computer networks. *T-Comm*, *4*(3), 23–2. (In Russ.).

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Smolenskij, M. B., & Levshin, N. S. (2016). Localization of personal data of Russian citizens as a component of Russia's economic and national security. *Nauka i obrazovanie: khozyajstvo i ekonomika, predprinimatelstvo, pravo i upravlenie*, *2*(69), 111–114. (In Russ.).

Veseliczky, O. I. (2015). Issues of cross-border transfer of personal data in accordance with the requirements of 242-FZ. *Collections of conferences of the Sotsiosfera SIC*, *53*, 275–279. (In Russ.).

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Authors information

Dmitriy V. Bakhteev – Dr. Sci. (Law), Professor, Department of Criminalistic named after I. F. Gerasimov, Head of Laboratory of Digital Technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Anna M. Sosnovikova – probation researcher of the Laboratory for digital technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Evgeniy V. Kazenas – student, Ural Federal University named after the first President of Russia B. N. Yeltsin
Address: 19 Mira Str., 620002, Yekaterinburg, Russia
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research was funded by the grant of the Russian Science Fund No. 23-78-10011, https://rscf.ru/project/23-78-10011/

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 28, 2024
Date of approval – July 12, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024