ISSN 2949-1150 (online)
2071-8284 (print)

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

CRIMINAL LAW SCIENCES

Научная статья
УДК 34.343

Организационно-правовые аспекты обращения с биометрическими персональными данными: криминологический взгляд

Алёна Сергеевна Артемьева, адъюнкт

Санкт-Петербургский университет МВД России
Санкт-Петербург (198206, ул. Летчика Пилютова, д. 1), Российская Федерация
alyonart95@mail.ru

Аннотация:
Введение. *Рост общественной значимости биометрических персональных данных в жизни общества и каждого гражданина в отдельности актуализирует необходимость всестороннего обеспечения безопасности новых социально-экономических реалий. В статье рассматриваются организационно-правовые меры, предпринимаемые государством в целях защиты биометрических персональных данных граждан от криминогенных угроз. Обозначаются причины возросших рисков бесконтрольного оборота биометрических персональных данных. Анализируется регулирование правоотношений, возникающих в сфере обращения с биометрическими персональными данными. В контексте обеспечения криминологической безопасности объясняются необходимость и значение административного и уголовного регулирования незаконного сбора, хранения, обработки и распространения биометрических персональных данных. Также автор приводит примеры использования биометрических персональных данных в установлении организационно-правовых режимов, направленных на обеспечение безопасности государственных границ, борьбы с незаконной миграцией, обеспечением общественного порядка и общественной безопасности, защиты личности, общества и государства от преступных посягательств.*
Методы. *Методологической базой исследования послужили такие общенаучные методы как анализ, систематизация, обобщение и абстрагирование, а также сравнительно-правовой и формально-юридический частноправовые методы.*
Результаты. *В ходе теоретического осмысления организационно-правовых вопросов, связанных с оборотом биометрических персональных данных и его регулированием, выявлены проблемы толкования, отсутствия нормативно-правового закрепления, несогласованности правовых режимов, а также фрагментарности принимаемых мер. Анализ введенной уголовно-правовой защиты биометрических*

Ключевые слова:
организационно-правовые меры, биометрические персональные данные, незаконный оборот, уголовно-правовая защита, организационно-правовой режим, криминологическая безопасность

Для цитирования:
Артемьева А. С. Организационно-правовые аспекты обращения с биометрическими персональными данными: криминологический взгляд // Вестник Санкт-Петербургского университета МВД России. 2026. № 1 (109). С. 80–91.

ISSN 2949-1150 (online)
2071-8284 (print)

персональных данных позволил обозначить ряд проблемных вопросов, требующих дополнительного внимания законодательной власти. Предлагаются решения, направленные на усовершенствование установленных государством правил обращения с биометрическими персональными данными в целях предотвращения их незаконного оборота, а также свободного от преступных посягательств развития биометрических технологий на благо личности, общества и государства в условиях криминологической безопасности.

Статья поступила в редакцию 31.03.2025; одобрена после рецензирования 24.02.2026; принята к публикации 20.03.2026.

Original article

Institutional and legal aspects of the biometric personal data handling: a criminological perspective

Alyona S. Artemyeva, Postgraduate

Saint Petersburg University of the MIA of Russia
1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation
alyonart95@mail.ru

Abstract:
Introduction. *The growing public importance of biometric personal data in the life of society and each citizen individually highlights the need for comprehensive security of new social and economic realities. The article discusses organisational and legal measures taken by the state in order to protect biometric personal data of citizens from criminal threats. The reasons of increased risks of uncontrolled biometric personal data traffic are identified. The legal relationships regulation arising in the field of biometric personal data handling is analysed. In the context of criminological safety, the need for and importance of administrative and criminal regulation of the illicit gathering, storage, processing and dissemination of biometric personal data is explained. The author also provides examples of the biometric personal data use in providing organisational and legal regimes aimed at the state borders security ensuring, combating illegal migration, maintaining public order and public safety, protection of the personality, society and state from criminal encroachments.*
Methods. *Such general scientific methods as analysis, systematisation, generalisation and abstraction, as well as comparative-legal and formal-legal private law methods served as the methodological basis of the study.*
Results. *In the course of theoretical comprehension of organisational and legal issues related to the biometric personal data processing and its regulation, problems of interpretation, lack of normative and legal consolidation, inconsistency of legal regimes, as well as fragmentation of taken measures have been identified. The analysis of the introduced criminal law protection of biometric personal data has identified a number of problematic issues that require additional attention by the legislative authority. Solutions aimed at improving the rules established by the state for biometric personal data handling in order to prevent their illegal trafficking, as well as free from criminal encroachments development of biometric technologies for the benefit of the individual, society and the state in conditions of criminological security are proposed.*

Keywords:
institutional legal measures, biometric personal data, illegal traffic, criminal legal protection, organisational legal regime, criminological security

For citation:
Artemyeva A. S. Institutional and legal aspects of the biometric personal data handling: a criminological perspective // Vestnik of Saint Petersburg University of the MIA of Russia. 2026. № 1 (109). P. 80–91.

The article was submitted March 31, 2025; approved after reviewing February 24, 2026; accepted for publication March 20, 2026.

Введение

Анализ действующих нормативных правовых актов, регулирующих правоотношения в сфере применения биометрических персональных данных, позволяет выявить ряд проблемных вопросов, начиная от терминологической несогласованности и заканчивая отсутствием правового регулирования в некоторых случаях возникновения правоотношений. Отнести это к упущению или недоработке органов законодательной власти было бы не вполне объективно. Во-первых, внедрение биометрических персональных данных в жизнь гражданина, общества и государства в ситуации стремительно меняющихся социально-экономических условий, сопровождаемых постоянно ускоряющимися темпами технологического прогресса, произошло практически стихийно. Во-вторых, распространение систем обработки биометрических персональных данных происходит снизу вверх, что естественно для рыночной экономики. Множество разнопрофильных фирм и организаций формируют запрос под свои коммерческие нужды. Другие, компетентные в удовлетворении этих нужд организации разрабатывают продукт, в нашем случае системы обработки биометрических персональных данных, и предлагают его на предварительно

изученный рынок, где биометрические системы успешным образом находят применение в самых разных сферах: от бытовых нужд отдельного потребителя до стратегических направлений промышленного развития целых отраслей. Эти процессы запускаются и проходят первые этапы развития в уже существующем правовом поле, которое не может охватывать явления, ранее не существовавшие. Тем временем в вопросе, касающемся оборота чувствительной категории персональных данных, промедление с правовой регламентацией может вызвать криминогенные риски и привести к общественно опасным последствиям, и правотворческая задача уполномоченных органов власти – своевременно осознавать возникающие в обществе потребности и формулировать отвечающие им нормы таким образом, чтобы не только устранить возникшие пробелы в правовом регулировании, но и предупредить существование внеправового поведения в данной конкретной сфере. Целью данной статьи видится анализ нормативных правовых актов и законодательных изменений последних лет в области применения биометрических персональных данных, выявление недостатков правового регулирования в контексте обеспечения криминологической безопасности и предложение актуальных, на наш взгляд, решений проблемы.

Методы

Использованы методы систематизации научных знаний, анализа и сравнения нормативных правовых актов, а также научных работ авторов, исследующих проблемы в сфере обращения с биометрическими персональными данными, обобщения изученного материала. В результате выявлены несовершенства в действующем нормативном правовом регулировании данной сферы в контексте обеспечения криминологической безопасности.

Результаты

Несколькими годами ранее регулирование правоотношений в сфере использования биометрических персональных данных сводилось к 152-ФЗ «О персональных данных»[1]. Вскоре практика показала, что этого не вполне достаточно с точки зрения правил и порядка обращения со столь специфической категорией данных, механизмов защиты, определения круга уполномоченных субъектов и случаев наступления ответственности. Примером организационно-правовой «погони» за сформировавшейся практикой может служить принятие Федерального закона № 572-ФЗ о единой биометрической системе[2], когда началу действия установленных штрафных санкций предшествовал организованный правительством переходный период с тем, чтобы дать возможность организациям, ранее осуществлявшим сбор, хранение и обработку биометрических персональных данных бесконтрольно, получить аккредитацию в соответствии со вступившим в силу законом или прекратить сбор биометрических персональных данных, направив все ранее собранные сведения данной категории в государственную информационную систему – единую биометрическую систему (далее – ГИС ЕБС). Создание такой системы по государственному заказу в рамках разработки инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме[3], преследует полезные, необходимые, социально обусловленные цели, а именно:

– перевод биометрии граждан из цифровых хранилищ частных компаний на государственную единую информационную платформу;

– обеспечение удобства в получении большого количества услуг бесконтактного сервиса;

– обеспечение безопасности персональных данных граждан за счет криптографической защиты и технологий хранения в обезличенном виде.

Рассмотрение вопросов хранения, сбора и обработки биометрических персональных данных неизбежно сопряжено с проблемами безопасности. В первую очередь специалисты разных

[1] О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 08.08.2024) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2006. № 31 (ч. 1). Ст. 3451.

[2] Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федеральный закон от 29 декабря 2022 г. № 572-ФЗ (ред. от 28.12.2024) // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

[3] Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме : постановление Правительства Российской Федерации от 8 июня 2011 г. № 451 (ред. от 01.11.2025) // СЗ РФ. 2011. № 24. Ст. 3503.

ISSN 2949-1150 (online)
2071-8284 (print)

областей, ученые и практики озабочены риском утечки биометрических персональных данных или злоупотреблением со стороны уполномоченных лиц. Специалисты в области права Уральского государственного экономического университета пишут: «На практике может произойти утечка машиночитаемых баз данных, создаваемых для обеспечения обработки биометрических персональных, обеспечив доступ к биометрии кому угодно. С технической точки зрения представляется маловероятным обеспечение абсолютной защиты данных» [1, с. 278]. Наталья Касперская, председатель ассоциации «Отечественный софт», сооснователь «Лаборатории Касперского» и президент компании InfoWatch, поддерживая биометрические технологии в целом, выражает недоверие Единой биометрической системе ввиду универсальности направлений использования собираемых биометрических персональных данных[4]. В качестве положительного примера приводится практика сбора МВД России биометрии для оформления биометрического загранпаспорта и Сбербанком для предоставления клиентам своих конкретных услуг – т. е. изолированные системы. Трудно не согласиться со специалистом в области информационной безопасности относительно уровня защиты баз данных таких крупных субъектов государственного и банковского сектора. Однако, как мы отмечали выше, субъектами обработки биометрических персональных данных становятся частные компании разного уровня, а учитывая значительные послабления от государства в контроле малого бизнеса с целью его поддержки, есть риск, что ниша может быть заполнена недобросовестными предпринимателями или организациями, не способными обеспечить достаточный уровень защиты. Тем временем постоянный рост интернета вещей и совершенствование удаленного формата взаимодействия человека с миром – процесс необратимый. С. С. Кузнецова, А. Н. Мочалов, М С. Саликов относят российскую модель законодательного регулирования оборота биометрической информации к «Азиатской» концепции, где за счет максимально широкого внедрения технологий биометрической идентификации в онлайн-среду и приоритета на применение «сквозных» технологий, стирается граница между виртуальным и физическим мирами [2, с. 265]. Поэтому переход на централизованное управление оборотом биометрических персональных данных видится важным и необходимым шагом государства на пути к защите населения от несанкционированного доступа к уникальной персонифицирующей информации граждан и рисков злоупотребления ею, что представляет угрозу криминологической безопасности. Более того, централизованный подход открывает возможности для эффективного применения биометрического аудита, о котором говорится в работе В. И. Волчихина, А. И. Иванова, И. Г. Назарова и др. о нейросетевой защите персональных биометрических данных [3, с. 135].

Говоря о современных практических механизмах защиты информации, Закон вводит понятие коммерческой биометрической системы (далее – КБС) – система, прошедшая процедуру аккредитации и имеющая право на обработку биометрических персональных данных. Раньше сбор, хранение и обработка биометрии пользователя, его верификация, проходили внутри IT-инфраструктуры оператора предоставления услуг. Теперь у организации есть два пути решения: 1) получить аккредитацию и самостоятельно через транзакционную модель осуществлять прямое взаимодействие с ЕБС (при этом допускается использование исключительно российских алгоритмов, прошедших тщательное тестирование специалистами Центра биометрических технологий) или 2) пользоваться посредничеством других КБС. Второй вариант предполагает следующий алгоритм: терминал считывает биометрические данные пользователя и в зашифрованном виде направляет их в аккредитованную КБС, которая сопоставляет полученные данные со своей базой эталонных биометрических векторов, полученных из ЕБС, устанавливает личность и отправляет ответ обратно в систему. Такой порядок, уверяют специалисты, исключает попадание биометрических данных граждан за пределы защищенной государственной системы ЕБС и связанных с ней КБС, что обеспечивает соблюдение усиленных требований информационной безопасности, разработанных на самом высоком уровне. В то же время исследователями приводятся аргументы не в пользу нового порядка работы с биометрическими персональными данными. Д. А. Петрова и В. А. Папкова пишут об ущемлении установленными требованиями прав малого и среднего бизнеса [4, с. 334]. В свою очередь, считаем требования о минимальном размере уставного капитала, а также о техническом соответствии оборудования, используемого для обработки биометрических персональных данных, объективно обусловленными. Данные требования выступают гарантиями технической и материальной способности организации обеспечить качественную и безопасную обработку биометрических персональных данных, а также,

[4] Копелевич И. Наталья Касперская: «Не торопитесь использовать свою биометрию!» // Бизнес Online : [электронное издание]. URL: https://m.business-gazeta.ru/article/527101 (дата обращения: 20.05.2025).

в случае обнаружения угрозы, возможность следовать прописанным для известного оборудования централизованным алгоритмам действий по ее устранению, что с точки зрения обеспечения криминологической безопасности минимизирует риски незаконного оборота рассматриваемой категории персональных данных, создавая условия защиты и охраны прав граждан. Еще на подступах к реализации Единой государственной системы обработки биометрических персональных данных в ряде научных публикаций в области криминологии говорилось о необходимости ограничить доступ к данной деятельности со стороны коммерческих участников[5].

Что касается работы над рисками, по согласованию с Федеральной службой безопасности Российской Федерации Министерством цифрового развития Российской Федерации утверждены перечни угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой информационной системе персональных данных[6]. Центральным банком Российской Федерации (далее – Банк России) сформулированы и нормативно закреплены перечни угроз безопасности, актуальные при обработке биометрических персональных данных как в собственных информационных системах организаций, так и при взаимодействии с ГИС ЕБС – указания Банка России от 25 сентября 2023 г. № 6540-У[7] и № 6541-У[8], среди них: угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации), нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных) применительно к каждому этапу обработки. Утвержденные перечни актуальны к использованию и в некредитных организациях, осуществляющих взаимодействие с ЕБС.

Однако Закон о единой биометрической системе[9] регулирует сбор, хранение и обработку только двух биометрических параметров (изображение лица и запись голоса), в то время как другие биометрические персональные данные, обладая не меньшим идентификационным потенциалом, остаются за пределами централизованного контроля их обработки. Речь идет прежде всего об отпечатках пальцев и ладоней рук, сетчатки и радужной оболочки глаза, геометрии кисти руки, рисунка вен, которые продолжают использоваться частными фирмами для осуществления пропускного режима на объекты и в жилище, разблокировки устройств и приложений, минуя выполнение обязательств к соблюдению единых государственных требований к условиям сбора, хранения и обработки биометрических персональных данных, т. к. действие рассматриваемого Закона на все виды биометрических персональных данных не распространяется.

В то же время сложно представить, чтобы Федеральный закон № 572-ФЗ, а значит, и Единая биометрическая система, охватили весь перечень биометрических персональных данных, прежде всего потому, что он не является исчерпывающим. Однако представляется целесообразным расширение количества отбираемых к обработке биометрических характеристик из числа наиболее активно используемых для идентификации и аутентификации. Так, на конференции

---

[5] Таранков О. И., Порошкина Т. С. Проблема безопасности при использовании биометрических данных граждан // Союз криминалистов и криминологов. 2020. № 4. С. 163. http://doi.org/10.31085/2310-8681-2020-4-208-159-164.

[6] Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных : приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25 мая 2021 г. № 494 (зарег. в Минюсте России 15.09.2021, № 65009) // Официальный интернет-портал правовой информации (http://pravo.gov.ru). URL: http://publication.pravo.gov.ru/document/0001202109160019 (дата обращения: 22.05.2025). Утратил силу.

[7] О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой : указание Банка России от 25 сентября 2023 г. № 6540-У (зарег. в Минюсте России 26.10.2023, № 75742) // Вестник Банка России. 2023. № 71.

[8] О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами : указание Банка России от 25 сентября 2023 г. № 6541-У (зарег. в Минюсте России 26.10.2023, № 75743) // Там же.

[9] СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

ISSN 2949-1150 (online)
2071-8284 (print)

«Технологии и доверие: защита подлинности и идентификация» АО «Гознак» анонсировал расширение функций автоматизации пользования услугами общественного транспорта на основе биометрической идентификации и электронного документа за счет подтверждения личности по радужной оболочке глаза и рисунку вен ладоней[10].

В целях обеспечения обороны страны и безопасности государства, охраны правопорядка, транспортной безопасности и противодействия терроризму постановлением Правительства Российской Федерации от 28 декабря 2018 г. № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы»[11] с изменениями и дополнениями от 7 марта 2023 г. утверждены Правила, в соответствии с которыми предоставление сведений осуществляется оператором ЕБС по мотивированному запросу МВД России или ФСБ Росси и их территориальных органов, направленному в соответствии с законодательством Российской Федерации посредством использования единой системы межведомственного электронного взаимодействия в течение одного дня с момента получения запроса. Остается неясным, какие именно сведения обязательны к предоставлению, т. к. в подп. «ж» п. 10 главы 2 Положения «О единой биометрической системе»[12] говорится о сведениях, содержащихся в единой биометрической системе в целом, тогда как п. 5 вышеупомянутых Правил предполагает только выдачу данных изображения лица человека, полученных с помощью фотовидеоустройств. В настоящее время Единой биометрической системой обрабатываются следующие биометрические персональные данные:

– изображение лица человека, полученное с помощью фотовидеоустройств;

– запись голоса человека, полученная с помощью звукозаписывающих устройств[13].

В целях качественного взаимодействия между органами государственной власти, а также надлежащего выполнения правоохранительными органами, в частности, МВД России, возложенных на них задач по защите личности, общества и государства от преступных посягательств, видится необходимым уточнить порядок предоставления сведений, дополнив подп. «б» п. 3 и п. 5 Правил предоставления оператором единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе, указанием на выдачу данных записи голоса человека или, на случай расширения перечня обрабатываемых в ГИС ЕБС биометрических персональных данных, изложить его в виде формулировки без указания на конкретные сведения.

Отсутствие в законодательстве перечня биометрических персональных данных порождает активные научные дискуссии. Так, Р. Н. Данелян и В. А. Яковлев-Чернышев предлагают дополнить ст. 11 Федерального закона № 572-ФЗ частью 1.1 следующего содержания:

«1.1. Видами биометрических персональных данных являются:

1) изображение лица человека, полученное с помощью фото-, видеоустройств;

2) запись голоса человека, полученная с помощью звукозаписывающих устройств;

3) особенности строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющие установить его личность;

4) радужная оболочка глаз;

5) иные виды биометрических персональных данных» [5, с. 31].

---

[10] Гознак вскоре представит технологию верификации по радужной оболочке глаза // Информационное агентство ТАСС : [сайт]. URL: https://tass.ru/ekonomika/11156969 (дата обращения: 02.05.2025).

[11] О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы (вместе с «Правилами предоставления оператором единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе», «Правилами предоставления оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в региональном сегменте единой биометрической системы») : постановление Правительства Российской Федерации от 28 декабря 2018 г. № 1703 (ред. от 07.03.2023) // СЗ РФ. 2018. № 53 (ч. II). Ст. 8727.

[12] Об утверждении Положения о единой биометрической системе, в том числе о ее региональных сегментах, и о признании утратившим силу постановления Правительства Российской Федерации от 16 июня 2022 г. № 1089 : постановление Правительства Российской Федерации от 31 мая 2023 г. № 883 (ред. от 01.09.2023) // СЗ РФ. 2023. № 23 (ч. II). Ст. 4193.

[13] СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

Такая попытка устранить выявленный пробел в законодательстве представляется не вполне обоснованной, поскольку не достигает поставленной цели. Проблема отсутствия законодательно закрепленного перечня биометрических персональных данных не может быть решена добавлением к ранее закрепленным двум видам этих данных еще двух-трех видов, в то время как ученые описывают большее количество существующих и возможных для использования биометрических персональных данных, среди которых кроме особенностей папиллярных узоров рук, радужной оболочки и сетчатки глаза, формы лица, особенностей письменной речи, почерка и динамики подписи, голоса и особенностей речи выделяют клавиатурный почерк и стилометрию, движение губ, микровибрацию пальцев, геометрию сердца и сердцебиение, акустический отклик среднего уха, термограмму лица, характеристики ДНК, характеристики пота, речевую подпись, особенности нейронных связей, запах и состав выдыхаемого воздуха, особенности походки, форму ушной раковины, структуру кожи и эпителия на пальцах, уровень солености кожи, биоакустическую подпись и некоторые другие характеристики [6; 7, с. 168]. Как видим, перспективы использования биометрических персональных данных в системе обеспечения криминологической безопасности велики, однако государству необходимо принимать во внимание еще один важный организационный момент. Как замечает А. М. Зинин, реальное использование биометрических параметров для идентификации возможно тогда, когда создаются соответствующие банки данных, в которых единообразно накапливаются соответствующие образцы. «Это связано с наличием и функционированием систем регистрации человека» [8, с. 63]. В связи с этим можно выделить еще одну ключевую проблему – отсутствие общего правового режима функционирования гражданских биометрических систем и правоохранительных идентификационных баз по биометрии [9, с. 177].

Возвращаясь к проблеме правовой неопределенности относительно перечня биометрических персональных данных, мы могли бы предложить два пути ее решения:

1) перечисление всех видов биометрических персональных данных, известных на настоящий момент, с указанием на то, что данный перечень не является исчерпывающим;

2) закрепление научно обоснованного и внутрисогласованного определения биометрических персональных данных с перечислением критериев относимости тех или иных персональных данных к биометрическим.

Как в первом, так и во втором случае устраняется неопределенность в толковании, правоприменении и правосудии.

Необходимость определения критериев относимости обосновывает в одной из своих работ И. А. Терещенко, предлагая «закрепить исчерпывающие и ясные критерии, согласно которым данные могут быть признаны биометрическими в каждом определенном рассматриваемом случае» [10, с. 191].

Государством сегодня разработаны новые меры ответственности в отношении:

– субъектов, не желающих следовать новому порядку работы с биометрическими персональными данными;

– физических и юридических лиц, нарушающих требования в области обработки биометрических персональных данных;

– лиц, чьи действия с компьютерной информацией, в т. ч. содержащей биометрические персональные данные, противоправны и представляют общественную опасность.

Федеральный закон от 30 ноября 2024 г. № 420-ФЗ[14], вступивший в силу 30 мая 2025 г., ужесточает административную ответственность за нарушения в области обработки биометрических персональных данных, существенно увеличив штрафы:

– за утечку биометрических персональных данных;

– нарушение порядка обработки биометрических персональных данных;

– непринятие организационных и технических мер по обеспечению безопасности биометрических персональных данных при их обработке;

– обработку биометрических персональных данных без аккредитации, где максимальный размер ответственности для юридических лиц может достигать 20 млн рублей. Принятие этих норм и адаптивное их усовершенствование – важный шаг к обеспечению криминологической безопасности, поскольку в задачи законодательства об административных правонарушениях входят: защита личности, охрана прав и свобод человека и гражданина, защита общественной нравственности, охрана порядка осуществления государственной власти, общественного порядка и общественной безопасности. Решение этих задач в рамках административного регулирования

[14] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 ноября 2024 г. № 420-ФЗ (ред. от 23.05.2025) // СЗ РФ. 2024. № 49 (ч. IV). Ст. 7411.

ISSN 2949-1150 (online)
2071-8284 (print)

обработки биометрических персональных данных представляет собой профилактику и адресное предупреждение совершения преступлений в исследуемой нами области.

Более того, оценив ежегодный рост количества преступлений, совершаемых с помощью информационно-телекоммуникационных сетей, в т. ч. интернета или путем неправомерного доступа к компьютерной информации, а также уровень общественной опасности от незаконного завладения персональными данными, в т. ч. биометрическими, законодатель ввел уголовную ответственность[15]. С 11 декабря 2024 г. Уголовный кодекс Российской Федерации[16] дополнен новой ст. 272[1] (далее – УК РФ), предусматривающей в ч. 2 наказание в виде штрафа до 700 тыс. рублей, принудительных работ или лишения свободы на срок до 5 лет за незаконное использование, передачу, сбор и хранение компьютерной информации, содержащей биометрические персональные данные.

Необходимости уголовно-правовой защиты этой категории данных в последние годы было посвящено немало работ ученых и практиков [1, с. 277; 11; 12, с. 107]. Криминализация незаконного оборота биометрических персональных данных – важный шаг на пути к обеспечению криминологической безопасности. Однако неразрывная связь незаконного оборота персональных данных с неправомерным доступом к компьютерной информации, по нашему мнению, не позволяет охватить весь спектр возможных преступных посягательств в отношении биометрических персональных данных. Статья 272[1] УК РФ направлена в большей степени на уголовно-правовое регулирование преступлений, связанных с массовым характером незаконного сбора, хранения, обработки и распространения биометрических персональных данных, которые практически всегда связаны с использованием больших баз данных и, следовательно, компьютерных устройств. Существует, например, «следовая» биометрия – биометрические персональные данные, способные отображаться на поверхностях. Для таких данных существует риск копирования злоумышленниками в преступных целях. Общественная опасность в этом случае представляется не меньшей в виду чувствительности и уязвимости этой категории данных, однако под действие данной уголовной нормы она не подпадает.

Ограничивающим фактором в принятии решения о привлечении к уголовной ответственности по данному виду преступлений может впоследствии выступить и само определение компьютерной информации. Согласно разъяснениям Верховного Суда Российской Федерации, под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи[17]. Специалисты разъясняют, что информация может передаваться и посредством беспроводных каналов связи, где отсутствуют электрические сигналы и, соответственно, такая информация не подпадает под правовое определение компьютерной [13, с. 158].

Ответственность за предусмотренные ст. 272[1] УК РФ преступления наступает с 16 лет. Учитывая специфику преступлений в сфере компьютерной информации, степень общественной опасности незаконного сбора и распространения биометрических персональных данных и тенденцию к снижению возраста лиц, владеющих сегодня современными технологиями, электронными устройствами и активно коммуницирующих в интернете, представляется целесообразным рассмотреть возможность наступления ответственности за отдельные преступления в сфере компьютерной информации для лиц, достигших 14 лет. Например, в интересах граждан и безопасности страны Федеральным законом от 17 ноября 2025 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[18] перечень преступлений, представляющих особую общественную опасность, наступление уголовной ответственности за которые п. 2 ст. 20 УК РФ предусматривается с четырнадцатилетнего возраста, дополнен восемью составами преступлений диверсионно-террористической направленности, что обусловлено ежедневными сводками о происшествиях последних лет, свидетельствующими об участившемся совершении особо опасных преступлений несовершеннолетними[19]. Удельный вес преступлений, совершенных несовершеннолетними или при их участии, от общего числа расследованных преступлений

---

[15] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30 ноября 2024 г. № 421-ФЗ // СЗ РФ. 2024. № 49 (ч. IV). Ст. 7412.

[16] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.02.2025) // СЗ РФ. 1996. № 25. Ст. 2954.

[17] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет : постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Бюллетень Верховного Суда Российской Федерации. 2023. № 3.

[18] СЗ РФ. 2024. № 49 (ч. IV). Ст. 7411.

[19] За какие преступления возраст уголовной ответственности теперь наступает с 14 лет // Российская газета. 2025. 18 ноября. № 262 (9801).

с 2023 по 2025 год вырос с 2,7 % до 3,4 %[20]. При этом за последние три года отмечается значительный рост преступлений террористического характера: в 2023 году было зарегистрировано 2 382 преступления, в 2024 – 3 714, в 2025 – 5 920, и экстремистской направленности: в 2023 году – 1 340, в 2024 – 1 719, в 2025 – 2 241[21]. Бенефициары подготовки и организации деятельности, направленной на дискредитацию государственной власти, подрыв конституционного строя и дестабилизацию в обществе, а также нанесение значительного ущерба экономике (всплеск мошенничеств), находятся, как правило, за рубежом, откуда координируют действия через мессенджеры, игровые сайты и другие платформы посредством мобильных и компьютерных устройств, о чем свидетельствует статистика преступлений, предусмотренных ст. 205[2] УК РФ и ст. 280 УК РФ, совершенных с использованием информационно-телекоммуникационных технологий, где количество публичных призывов к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма с 2023 по 2025 год включительно увеличилось с 548 до 1 367 преступлений, а публичные призывы к осуществлению экстремистской деятельности – с 367 до 705 преступлений[22]. Принятые меры, безусловно, отразятся на статистике положительным образом. Однако, как сказал заместитель министра внутренних дел Российской Федерации генерал-полковник полиции А. И. Храпов, «с каждой мерой, которая вступала в действие, мы фиксировали резкий спад регистрируемых преступлений с последующим частичным ростом, что говорит о том, что к этим мерам преступники приспосабливаются и понимают, как им надо дальше действовать»[23]. Тенденция к вовлечению несовершеннолетних в совершение опасных преступлений с использованием информационно-коммуникационных технологий или в компьютерной сфере, на наш взгляд, продолжится, т. к. именно данная возрастная категория одновременно:

1) владеет необходимыми навыками обращения с компьютерами, приложениями, новыми информационно-телекоммуникационными ресурсами;

2) проводит наибольшее количество времени на интернет-сайтах, игровых платформах и в мессенджерах;

3) психологически наиболее уязвима и подвержена внешнему влиянию по индивидуальному ряду причин (желание быть замеченными, иллюзия избранности, быстрый заработок, отрицание ближайшего окружения и т. д.).

Если ранее главным аргументом для вовлечения несовершеннолетних по ряду статей было отсутствие для них уголовного наказания, то теперь таким аргументом может стать возможность избежать ответственности за счет действий под чужими персональными данными, в частности, биометрическими, путем умелого использования компьютерных технологий, в чем современные подростки опережают иные возрастные категории граждан. О тонкой грани между правомерным использованием биометрических персональных данных и совершением с их помощью разного рода преступлений упоминается и в Сборнике практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом[24]. В документе говорится, что кража биометрических персональных данных может представлять собой несанкционированное получение фактических физических биометрических данных человека, например, создание копии отпечатков пальцев или маски его лица, или кражу биометрического шаблона, хранящегося в приложении или в базе данных в целях совершения преступных деяний, в частности, мошенничества, связанного с использованием похищенных данных для получения фиктивного займа, кредитной карты или приобретения дорогостоящих товаров; предлагается ряд мер для борьбы с этим явлением. В нашем уголовном законодательстве существует эффективная правовая мера борьбы

[20] Состояние преступности в России за январь – декабрь 2023 года // Министерство внутренних дел Российской Федерации : [официальный сайт]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 16.02.2026) ; Состояние преступности в России за январь – декабрь 2024 года // Там же. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 16.02.2026) ; Состояние преступности в России за январь – декабрь 2025 года // Там же. URL: https://xn--b1aew.xn--p1ai/reports/item/72174303/ (дата обращения: 16.02.2026).

[21] URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 16.02.2026) ; URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 16.02.2026) ; URL: https://xn--b1aew.xn--p1ai/reports/item/72174303/ (дата обращения: 16.02.2026).

[22] Там же.

[23] МВД сообщило о снижении числа киберпреступлений в РФ в 2025 году на 12 % // Интерфакс.ру : [сетевое издание]. URL: https://www.interfax.ru/digital/1073418 (дата обращения: 18.02.2026).

[24] Сборник практических рекомендаций и Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом : Окончательный проект // Организация Объединенных Наций : [официальный сайт]. URL: https://www.un.org/counterterrorism/sites/default/files/compendium-biometrics-20180618-ru.pdf (дата обращения: 18.02.2026).

ISSN 2949-1150 (online)
2071-8284 (print)

с неправомерным завладением персональными данными, в частности, биометрическими, в электронном виде, благодаря ст. 272[1] УК РФ, однако под действие ее санкции не подпадает вся «целевая группа» несовершеннолетних. Таким образом, актуализируется угроза роста совершения преступлений, предусмотренных п. 2 ст. 272[1] УК РФ, лицами, не достигшими возраста уголовной ответственности по данной статье, с целью сокрытия совершения ими других тяжких и особо тяжких преступлений, за которые уголовное наказание наступает с 14 лет. В связи с вышеизложенным считаем необходимым расширить содержание п. 2 ст. 20 УК РФ путем внесения в ее перечень состава преступления, предусмотренного п. 2 ст. 272[1] УК РФ.

Проблема неподподания под прямое действие уголовного законодательства случаев подделки и использования чужих биометрических персональных данных при совершении общественно опасных деяний заслуживает особого внимания. И. Н. Мосечкин предлагает установить уголовную ответственность за фальсификацию внешности, голоса, папиллярных узоров пальцев и других разновидностей биометрических данных с целью скрыть другое преступление или облегчить его совершение в отдельной статье УК РФ [14, с. 107]. Другие авторы, проводя параллель между подделкой документов, штампов, печатей и бланков и подделкой отображений биометрических характеристик человека, предлагают включить в ст. 327 УК РФ физические объекты, содержащие биометрические данные человека, в качестве предметов преступления [15, с. 42]. Учитывая рост общественной значимости биометрических персональных данных в жизни общества и каждого гражданина в отдельности, в рамках усовершенствования современного уголовного законодательства целесообразно рассмотреть возможность дополнить ряд статей УК РФ таким квалифицирующим признаком, как использование биометрических персональных данных.

Кроме мер, направленных на урегулирование уже сложившихся правоотношений, государство предпринимает шаги к установлению новых организационно-правовых режимов с использованием биометрических персональных данных в целях обеспечения национальной безопасности. Согласно постановлению Правительства Российской Федерации от 7 ноября 2024 г. № 1510 «О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства»[25], при прохождении иностранным гражданином и лицом без гражданства пограничного контроля при въезде в Российскую Федерацию или выезде из Российской Федерации в период проведения эксперимента (с 1 декабря 2024 г. по 30 июня 2026 г.) осуществляется сбор биометрических персональных данных (фотографического изображения лица и папиллярных узоров пальцев рук человека, а также на добровольной и безвозмездной основе геномной информации). Указанные биометрические персональные данные иностранного гражданина и лица без гражданства передаются в государственные информационные системы уполномоченных органов (ГИС ЕБС и базы данных органов внутренних дел) для идентификации или аутентификации иностранного гражданина или лица без гражданства. Въехавшие в Российскую Федерацию в период проведения эксперимента иностранные граждане и лица без гражданства в обязательном порядке получают электронную карту иностранного гражданина – материальный носитель, содержащий зафиксированную в графической и машиночитаемой формах информацию о держателе электронной карты иностранного гражданина, в т. ч. считываемую посредством идентификатора QR-кода, нанесенного на электронную карту иностранного гражданина.

Приказ Министерства внутренних дел Российской Федерации от 28 декабря 2021 г. № 1167 «Об утверждении порядков использования органами государственной власти документов в форме карты с электронным носителем информации, выданных иностранным гражданам или лицам без гражданства, для их идентификации с помощью биометрическом персональных данных»[26]

[25] О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства (вместе с «Правилами организации эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства», «Правилами оказания содействия подразделениям органов внутренних дел Российской Федерации в проведении добровольной государственной геномной регистрации посредством получения, хранения, уничтожения биологического материала, а также получения и передачи геномной информации») : постановление Правительства Российской Федерации от 7 ноября 2024 г. № 1510 (ред. от 07.11.2024) // СЗ РФ. 2024. № 47. Ст. 7114.

[26] Об утверждении порядков использования органами государственной власти документов в форме карты с электронным носителем информации, выданных иностранным гражданам или лицам без гражданства, для их идентификации с помощью биометрических персональных данных (вместе с «Порядком использования органами государственной власти документа, подтверждающего прохождение иностранным гражданином или лицом без гражданства, прибывшим в Российскую Федерацию в целях, не связанных с осуществлением трудовой деятельности, на срок, превышающий девяносто календарных дней, либо в целях осуществления трудовой деятельности, обязательной государственной дактилоскопической регистрации и фотографирования, в форме карты с электронным носителем информации, для идентификации иностранного гражданина или лица без гражданства с помощью биометрических персональных данных», «Порядком использования органами государственной власти временного удостоверения

определяет порядок работы органов государственной власти в лице МВД России с указанными электронными картами в целях реализации задач в сфере миграционной политики, обеспечения общественного порядка и общественной безопасности.

Заключение

Законодательство Российской Федерации с 2020 года претерпевает значительные регулярные и последовательные изменения в вопросах регулирования оборота биометрических персональных данных. Среди основных организационных решений и правовых изменений, играющих, на наш взгляд, самую заметную роль в процессе обеспечения криминологической безопасности, можно выделить:

– создание государственной информационной системы – Единой биометрической системы;

– нормативно-правовое закрепление порядка предоставления сведений ГИС ЕБС правоохранительным органам;

– принятие пакета нормативно-правового регулирования функционирования ГИС ЕБС, в т. ч. установление запрета на оборот биометрических персональных данных вне ЕБС и КБС;

– запрет на передачу и распространение биометрических персональных данных граждан Российской Федерации за границу;

– ужесточение административно-правового регулирования незаконной обработки биометрических персональных данных;

– введение в Уголовный кодекс Российской Федерации ст. 272[1], в которой нашел отражение незаконный оборот биометрических персональных данных;

– внедрение биометрических персональных данных в организацию правового режима въезда в Российскую Федерацию и выезда из нее.

В результате проведенного исследования были выявлены некоторые недостатки в принимаемых организационно-правовых решениях, последствия которых могут оказать негативное влияние на практику правоприменения. Однако для их комплексной оценки необходимо изучить судебную практику и уголовную статистику за будущие два года.

Анализ действующих, принимаемых и проектируемых нормативных правовых актов в сфере регулирования сбора, хранения, обработки и передачи биометрических персональных данных показал, что решение проблемы возрастающих криминогенных рисков в данной области становится одной из первостепенных задач для уполномоченных органов государственной власти и подлежит контролю на самом высоком государственном уровне.

Список источников

1. *Бурлака С. Н., Бельдина О. Г.* Защита биометрических персональных данных: проблемы правового регулирования // Право и государство: теория и практика. 2023. № 10 (226). С. 277–279. http://doi.org/10.47643/1815-1337_2023_10_277

2. *Кузнецова С. С., Мочалов А. Н., Саликов М. С.* Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. С. 257–267. http://doi.org/10.17223/15617793/476/28

3. *Нейросетевая защита персональных биометрических данных* : монография / Волчихин В. И., Иванов А. И., Назаров И. Г. [и др.] ; под ред. Ю. К. Язова. Москва : Радиотехника, 2012. 157 с.

4. *Петрова Д. А., Папкова В. А.* Обработка биометрических персональных данных в свете изменения законодательства // Правовая политика и правовая жизнь. 2024. № 3. С. 329–336. http://doi.org/10.24412/1608-8794-2024-3-329-336

5. Данелян Р. Н., Яковлев-Чернышев В. А. Особенности правового регулирования биометрических персональных данных в Российской Федерации // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3 (57). С. 26–33. https://doi.org/10.37973/VESTNIKKUI-2024-57-3

6. *Ворона В. А.* Биометрическая идентификация личности : [монография]. Москва : Горячая линия – Телеком, 2022. 227 с.

7. *Фролова Е. Ю., Кошлыкова Ю. А.* Идентификация человека по биометрическим данным: обзор современных технологий // Северо-Кавказский юридический вестник. 2022. № 3. С. 167–174. https://doi.org/10.22394/2074-7306-2022-1-3-167-174

8. *Зинин А. М.* Идентификация человека по признакам внешности и методы биометрии // Вестник Университета имени О. Е. Кутафина. 2022. № 2 (90). С. 58–66. https://doi.org/10.17803/2311-5998.2022.90.2.058-066

личности лица без гражданства в Российской Федерации в форме карты с электронным носителем информации для идентификации лица без гражданства с помощью биометрических персональных данных», «Порядком использования органами государственной власти вида на жительство иностранного гражданина в форме карты с электронным носителем информации для идентификации иностранного гражданина с помощью биометрических персональных данных», «Порядком использования органами государственной власти патента, выдаваемого иностранному гражданину или лицу без гражданства, прибывшему в Российскую Федерацию в порядке, не требующем получения визы, в форме карты с электронным носителем информации, для идентификации иностранного гражданина или лица без гражданства с помощью биометрических персональных данных») : приказ Министерства внутренних дел Российской Федерации от 28 декабря 2021 г. № 1167 (зарег. в Минюсте России 29.12.2021, № 66666) // Официальный интернет-портал правовой информации (http://pravo.gov.ru). URL: http://publication.pravo.gov.ru/Document/View/0001202112290036 (дата обращения: 16.06.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

9. *Желудков М. А., Варыгин А. Н.* Безопасное использование биометрических персональных данных личности как средство борьбы с корыстной цифровой преступностью // Вестник Саратовской государственной юридической академии. 2024. № 4 (159). С. 170–178. https://doi.org/10.24412/2227-7315-2024-4-170-178

10. *Терещенко И. А.* Биометрические персональные данные: проблемы и перспективы определения понятия // Закон и право. 2024. № 2. С. 186–192. https://doi.org/10.24412/2073-3313-2024-2-186-192

11. *Вронская М. В., Виничук П. В.* Биометрические данные как объект правовой охраны и защиты: актуальные проблемы // Международный научно-исследовательский журнал. 2024. № 4 (142). https://doi.org/10.23670/IRJ.2024.142.109

12. *Чукреев В. А.* Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 3 (91). С. 107–116. https://doi.org/10.17803/2311-5998.2022.91.3.107-116

13. *Коврижных Л. А.* О подходах к определению понятия «компьютерная информация» / Неволинские чтения. Вопросы совершенствования высшего юридического образования на современном этапе : сборник материалов Международной научно-практической конференции, посвященной 210-летию со дня рождения К. А. Неволина, 85-летию Университета имени О. Е. Кутафина (МГЮА) и 45-летию Волго-Вятского института (филиала) Университета имени О. Е. Кутафина (МГЮА), г. Киров, 18 ноября 2016 г. Киров : Аверс, 2017. С. 158–163.

14. *Мосечкин И. Н.* Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования. Вестник Санкт-Петербургского университета. Право, 2025. Т. 16, № 1. С. 95–110. https://doi.org/10.21638/spbu14.2025.107

15. *Чукин Д. С., Муфаздалов С. И.* Объекты с биометрическими данными как предмет преступления, предусмотренного статьей 327 Уголовного кодекса Российской Федерации // Право в Вооруженных Силах – Военно-правовое обозрение. 2020. № 4 (273). С. 37–42.

References

1. *Burlaka S. N., Bel'dina O. G.* Zashchita biometricheskih personal'nyh dannyh: problemy pravovogo regulirovaniya // Pravo i gosudarstvo: teoriya i praktika. 2023. № 10 (226). S. 277–279. http://doi.org/10.47643/1815-1337_2023_10_277

2. *Kuznecova S. S., Mochalov A. N., Salikov M. S.* Biometricheskaya identifikaciya v internete: tendencii pravovogo regulirovaniya v Rossii i za rubezhom // Vestnik Tomskogo gosudarstvennogo universiteta. 2022. № 476. S. 257–267. http://doi.org/10.17223/15617793/476/28

3. *Nejrosetevaya zashchita personal'nyh biometricheskih dannyh* : monografiya / Volchihin V. I., Ivanov A. I., Nazarov I. G. [i dr.] ; pod red. Yu. K. Yazova. Moskva : Radiotekhnika, 2012. 157 s.

4. *Petrova D. A., Papkova V. A.* Obrabotka biometricheskih personal'nyh dannyh v svete izmeneniya zakonodatel'stva // Pravovaya politika i pravovaya zhizn'. 2024. № 3. S. 329–336. http://doi.org/10.24412/1608-8794-2024-3-329-336

5. *Danelyan R. N., Yakovlev-Chernyshev V. A.* Osobennosti pravovogo regulirovaniya biometricheskih personal'nyh dannyh v Rossijskoj Federacii // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2024. T. 15, № 3 (57). S. 26–33. https://doi.org/10.37973/VESTNIKKUI-2024-57-3

6. *Vorona V. A.* Biometricheskaya identifikaciya lichnosti : [monografiya]. Moskva : Goryachaya liniya – Telekom, 2022. 227 s.

7. *Frolova E. Yu., Koshlykova Yu. A.* Identifikaciya cheloveka po biometricheskim dannym: obzor sovremennyh tekhnologij // Severo-Kavkazskij yuridicheskij vestnik. 2022. № 3. S. 167–174. https://doi.org/10.22394/2074-7306-2022-1-3-167-174

8. *Zinin A. M.* Identifikaciya cheloveka po priznakam vneshnosti i metody biometrii // Vestnik Universiteta imeni O. E. Kutafina. 2022. № 2 (90). S. 58–66. https://doi.org/10.17803/2311-5998.2022.90.2.058-066

9. *Zheludkov M. A., Varygin A. N.* Bezopasnoe ispol'zovanie biometricheskih personal'nyh dannyh lichnosti kak sredstvo bor'by s korystnoj cifrovoj prestupnost'yu // Vestnik Saratovskoj gosudarstvennoj yuridicheskoj akademii. 2024. № 4 (159). S. 170–178. https://doi.org/10.24412/2227-7315-2024-4-170-178

10. *Tereshchenko I. A.* Biometricheskie personal'nye dannye: problemy i perspektivy opredeleniya ponyatiya // Zakon i pravo. 2024. № 2. S. 186–192. – https://doi.org/10.24412/2073-3313-2024-2-186-192

11. *Vronskaya M. V., Vinichuk P. V.* Biometricheskie dannye kak ob"ekt pravovoj ohrany i zashchity: aktual'nye problemy // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2024. № 4 (142). https://doi.org/10.23670/IRJ.2024.142.109

12. *Chukreev V. A.* Personal'nye dannye, v tom chisle biometricheskie dannye, kak predmety ugolovno-pravovoj ohrany // Vestnik Universiteta imeni O. E. Kutafina (MGYUA). 2022. № 3 (91). S. 107–116. https://doi.org/10.17803/2311-5998.2022.91.3.107-116

13. *Kovrizhnyh L. A.* O podhodah k opredeleniyu ponyatiya «komp'yuternaya informaciya» / Nevolinskie chteniya. Voprosy sovershenstvovaniya vysshego yuridicheskogo obrazovaniya na sovremennom etape : sbornik materialov Mezhdunarodnoj nauchno-prakticheskoj konferencii, posvyashchennoj 210-letiyu so dnya rozhdeniya K. A. Nevolina, 85-letiyu Universiteta imeni O. E. Kutafina (MGYUA) i 45-letiyu Volgo-Vyatskogo instituta (filiala) Universiteta imeni O. E. Kutafina (MGYUA), g. Kirov, 18 noyabrya 2016 g. Kirov : Avers, 2017. S. 158–163.

14. *Mosechkin I. N.* Dipfejk-tekhnologii i biometricheskie dannye: napravleniya ugolovno-pravovogo regulirovaniya. Vestnik Sankt-Peterburgskogo universiteta. Pravo, 2025. T. 16, № 1. S. 95–110. https://doi.org/10.21638/spbu14.2025.107

15. *Chukin D. S., Mufazdalov S. I.* Ob"ekty s biometricheskimi dannymi kak predmet prestupleniya, predusmotrennogo stat'ej 327 Ugolovnogo kodeksa Rossijskoj Federacii // Pravo v Vooruzhennyh Silah – Voenno-pravovoe obozrenie. 2020. № 4 (273). S. 37–42.