

ЭКОНОМИКА

ECONOMY

Менеджмент

Management

Научная статья

УДК 349.23+004.056+342.721

DOI: 10.55196/2411-3492-2026-3-53-163-171

**Защита и обработка персональных данных работника в эпоху
цифровизации: правовые и организационные аспекты****Ирина Леонидовна Кудзаева^{✉1}, Леонид Петрович Сужаев²**

Горский государственный аграрный университет, улица Кирова, 37, Владикавказ, Россия, 362040

^{✉1}kudzayeva.ira@mail.ru, <https://orcid.org/0009-0007-4300-8466>²irasuzhaeva73@gmail.com, <https://orcid.org/0009-0006-9893-2050>

Аннотация. Перевод кадрового делопроизводства в электронный формат, внедрение систем видеонаблюдения, биометрической идентификации, геолокации и удалённого мониторинга производительности резко расширили объём собираемых сведений о сотрудниках и создали новые каналы их утечки. Актуальность исследования определяется тем, что с 2022 г. ужесточилась ответственность за разглашение персональных данных сотрудников. Кроме того, с появлением новых технологий утечки персональных данных о работниках значительно возросли и увеличились в масштабе. Цель исследования состоит в систематизации правовых и организационных механизмов охраны персональных данных работников в условиях компьютеризации организационных процессов и определении настоящих рисков, которые при этом могут возникнуть у работодателей. В работе применён комплекс общенаучных и специально-юридических методов: формально-юридический анализ нормативных правовых актов; сравнительно-правовой метод (сопоставление российского и зарубежного регулирования); системный анализ судебной практики и правоприменительных актов Роскомнадзора; кейс-анализ реальных инцидентов утечки данных; статистический анализ данных о нарушениях в сфере персональных данных. В результате проведенных исследований установлено, что эффективная защита персональных данных работников требует построения многоуровневой системы, сочетающей правовые (локальные акты, договорная защита, работа с согласиями), организационные (разграничение доступа, обучение персонала) и технические (шифрование, DLP-системы, аудит) меры. Ни один из уровней не может быть заменён другим. Сформулированы практические рекомендации для работодателей: провести аудит существующей системы обработки персональных данных работников; актуализировать локальные акты с учётом реформ 2022–2023 гг.; выстроить процедуру уведомления Роскомнадзора об утечках; включить условия о защите персональных данных во все договоры с аутсорсерами и облачными провайдерами; обеспечить регулярное обучение сотрудников кадровых и ИТ-служб.

Ключевые слова: персональные данные, организация подходов к защите, охрана труда, управление системой, компьютеризация, биометрические данные, персональные данные, ответственность

Для цитирования. Кудзаева И. Л., Сужаев Л. П. Защита и обработка персональных данных работника в эпоху цифровизации: правовые и организационные аспекты // Известия Кабардино-Балкарского государственного аграрного университета им. В. М. Кокова. 2026. № 3(53). С. 163–171. DOI: 10.55196/2411-3492-2026-3-53-163-171

Original article

Protection and processing of employee personal data in the digital age: legal and organizational aspects

Irina L. Kudzaeva^{✉1}, Leonid P. Suzhaev²

Gorsky State Agrarian University, 37 Kirov Street, Vladikavkaz, Russia, 362040

^{✉1}kudzayeva.ira@mail.ru, <https://orcid.org/0009-0007-4300-8466>

²irasuzhaeva73@gmail.com, <https://orcid.org/0009-0006-9893-2050>

Abstract. The digitalization of personnel records management, the implementation of video surveillance systems, biometric identification, geolocation, and remote performance monitoring have dramatically expanded the volume of employee data collected and created new channels for data leakage. The relevance of this study is determined by the fact that, since 2022, penalties for the disclosure of employee personal data have become stricter. Moreover, with the advent of new technologies, leaks of employee personal data have significantly increased and expanded in scale. Therefore, the objective of the study is to systematize the legal and organizational mechanisms for protecting employee personal data in the context of the computerization of organizational processes and to identify the actual risks that employers may face. The study applies a combination of general scientific and specialized legal methods: formal legal analysis of regulatory legal acts; comparative legal method (comparison of Russian and foreign regulations); systems analysis of judicial practice and law enforcement acts of Roskomnadzor; case analysis of real data leakage incidents; statistical analysis of data on violations in the field of personal data. The conducted research revealed that effective protection of employees' personal data requires the development of a multi-layered system combining legal (regulatory laws, contractual protection, consent management), organizational (access control, staff training), and technical (encryption, DLP systems, audit) measures. No single layer can be replaced by another. Practical recommendations for employers have been formulated: conduct an audit of the existing system for processing employees' personal data; update local regulations in accordance with the 2022–2023 reforms; establish a procedure for notifying Roskomnadzor of leaks; include provisions for the protection of personal data in all contracts with outsourcers and cloud providers; and ensure regular training for HR and IT staff.

Keywords: personal data, organizational approaches to protection, occupational safety, system management, computerization, biometric data, personal data, liability

For citation. Kudzaeva IL, Suzhaev LP. Protection and processing of employee personal data in the digital age: legal and organizational aspects *Izvestiya of Kabardino-Balkarian State Agrarian University named after V.M. Kokov.* 2026;(3):163–171. (In Russ.). DOI: 10.55196/2411-3492-2026-3-53-163-171

Введение. В современных реалиях компьютеризации персональные данные сотрудников являются основным объектом правовой защиты. Перевод кадрового делопроизводства в электронный формат, внедрение систем видеонаблюдения, биометрической идентификации, геолокации и удалённого мониторинга производительности резко расширили объём собираемых сведений о сотрудниках и создали новые каналы их утечки [1–3].

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно идентифицированному физическому лицу (ст. 3 Федерального закона № 152-ФЗ). Применительно к трудовым отношениям это –

личные дела и анкеты, сведения о заработной плате и социальных выплатах, медицинская документация, биометрические данные, данные о местонахождении работника в рабочее время, записи систем контроля доступа, переписка в корпоративных мессенджерах [2–6].

Актуальность темы определяется несколькими факторами: во-первых, нарастающим давлением регулятора (с 2022 г. ужесточилась ответственность за разглашение персональных данных сотрудников); во-вторых, с появлением новых технологий утечки персональных данных о работниках значительно возросли и увеличились в масштабе (в 2023 г. в России было зафиксировано более 300 значи-

мых утечек персональных данных в корпоративном секторе, из которых около 40% приходилось на сведения о сотрудниках [7]); в-третьих, реформа законодательства 2022–2023 гг. принципиально изменила ряд базовых требований [5, 6].

Цель исследования – систематизировать правовые и организационные механизмы охраны персональных данных работников в условиях компьютеризации организационных процессов и определить настоящие риски, которые при этом могут возникнуть у работодателей.

Задачи исследования:

- 1) провести анализ актуальной на сегодняшний день нормативно-правовой базы РФ, затрагивающей защиту персональных данных работников с учётом принятых в 2022–2023 гг. реформ;
- 2) систематизировать внутриорганизационные механизмы защиты персональных данных;
- 3) рассмотреть специфику обработки отдельных категорий данных работников (биометрия, медицинские данные, данные мониторинга);
- 4) оценить меры юридической ответственности и правоприменительную практику;
- 5) определить перспективы регулирования в части применения ИИ-технологий в кадровом делопроизводстве.

Материалы, методы и объекты исследования. В работе применён комплекс общенаучных и специально-юридических методов: формально-юридический анализ нормативных правовых актов; сравнительно-правовой метод (сопоставление российского и зарубежного регулирования); системный анализ судебной практики и правоприменительных актов Роскомнадзора; кейс-анализ реальных инцидентов утечки данных; статистический анализ данных о нарушениях в сфере персональных данных.

Нормативную основу составляют: Конституция РФ (ст. 23, 24), Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» с изменениями 2022–2023 гг., Трудовой кодекс РФ (гл. 14), постановления Правительства РФ № 1119 и № 687, приказы Роскомнадзора, а также практика Верховного суда РФ и арбитражных судов по спорам о защите персональных данных.

Результаты исследования

1. Нормативно-правовая база: структура и реформы 2022–2023 гг. Российская система защиты персональных данных работников носит многоуровневый характер. Конституционную основу образуют статья 23 и статья 24 Конституции Российской Федерации, определяющие право на неприкосновенность личной жизни гражданина. Базовым законодательным актом является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», устанавливающий принципы обработки, права субъектов и обязанности операторов [1]. Трудовое измерение регулирования сосредоточено в гл. 14 ТК РФ (ст. 86–90), конкретизирующей цели, пределы и порядок обработки кадровых данных [2].

Реформа 2022–2023 гг. существенно изменила регуляторную среду. Федеральный закон от 14.07.2022 № 266-ФЗ ввёл обязательное уведомление Роскомнадзора об утечках данных в течение 24 часов (предварительное) и 72 часов (расширенное), распространил требования закона на иностранных операторов, обрабатывающих данные российских граждан, а также уточнил условия трансграничной передачи данных [5]. Федеральный закон от 12.12.2023 № 519-ФЗ ввёл оборотные штрафы за утечки персональных данных в размере от 0,1% до 3% годовой выручки оператора (но не менее 15 млн и не более 500 млн рублей) [6].

Принятие Закона № 519-ФЗ стало поворотным моментом: впервые в российской практике к работодателям как операторам данных может быть применена санкция, соразмерная их финансовым возможностям, что радикально меняет экономику комплаенса в сфере персональных данных.

2. Внутриорганизационные механизмы защиты персональных данных работников. Эффективная защита персональных данных работников требует выстраивания многоуровневой внутриорганизационной системы. Ниже рассматриваются её ключевые компоненты [8–10].

2.1. Локальная нормативная база. Обязательное содержание локальных актов предприятия: установленные согласно статье 18.1 Федерального закона «О персональных данных» № 152-ФЗ правила обработки персональных данных сотрудников; положение о защите персональных данных работников,

предусмотренное ст. 87 Трудового кодекса РФ; определение должностей работников, которым разрешён доступ к персональным данным; срок хранения персональных данных сотрудников. Работники, которым предоставлен доступ к персональным данным сотрудников, должны быть ознакомлены с вышеперечисленными документами под роспись [1, 2].

2.2. Персонализация ответственности и разграничение доступа. В обязанность работодателя входит назначение ответственного за порядок обработки персональных данных согласно статье 22.1 Федерального закона № 152-ФЗ. В организациях с большой численностью работников следует создавать отделы, обеспечивающие защиту персональных данных сотрудников согласно действующему законодательству РФ в этой сфере. Доступ к персональным данным сотрудников может предоставляться только специалистам указанного отдела и только в пределах производственной необходимости, по принципу минимизации данных. Обязательно ведение журналов доступа к информационным системам персональных данных (ИСПДн); все лица, допущенные к обработке данных, подписывают соглашение о неразглашении [3, 4, 11–13].

2.3. Работа с согласиями субъектов. Ключевым правовым основанием обработки персональных данных в трудовых отношениях является не согласие, а закон или трудовой договор: обработка данных, необходимых для исполнения трудовых обязанностей, не требует отдельного письменного согласия работника [1, 5]. Вместе с тем ряд операций требует явного согласия: обработка биометрических данных; публикация фотографий работника на сайте организации; передача данных третьим лицам, не являющимся государственными органами (банки зарплатных проектов, страховые компании, кадровые агентства); обработка специальных категорий данных (состояние здоровья, за исключением случаев, прямо предусмотренных законом) [1, 2].

Согласие должно соответствовать требованиям ст. 9 Закона № 152-ФЗ: быть конкретным, информированным, сознательным и выраженным в определённой форме. В трудовых отношениях существует риск признания согласия недействительным ввиду зависимого положения работника, поэтому Роскомнад-

зор рекомендует по возможности опираться на иные правовые основания [5].

2.4. Договорная защита при аутсорсинге обработки. При передаче обработки персональных данных работников сторонним организациям (аутсорсинг расчёта заработной платы, облачные HR-системы, кадровые агентства) необходимо заключение договора поручения обработки персональных данных (ст. 6 Закона № 152-ФЗ). Договор должен содержать: исчерпывающий перечень поручаемых действий; обязанность поверенного соблюдать конфиденциальность; требования к техническим мерам защиты; запрет на субпоручение без разрешения оператора; ответственность поверенного за нарушения. Оператор (работодатель) несёт солидарную ответственность перед субъектом данных за действия поверенного [1, 5].

3. Особенности обработки отдельных категорий данных работников.
3.1. Биометрические данные. Всё, что относится к биометрическим данным работников (отпечатки пальцев, рисунок вен, геометрия лица, образцы голоса), может использоваться работодателем только на основании письменного согласия работника, за исключением случаев, предусмотренных федеральными законами (ст. 11 Федерального закона № 152-ФЗ) [1]. Введение систем биометрической идентификации для контроля рабочего времени без согласия работника является грубым нарушением законодательства о персональных данных, что подтверждается практикой Роскомнадзора. Технические требования к защите биометрических ИСПДн – наивысшие (уровень защищённости УЗ-1 или УЗ-2 по Постановлению № 1119) [3].

3.2. Медицинские данные. Сведения о состоянии здоровья работника являются особыми персональными данными (статья 10 Федерального закона № 152-ФЗ), использование и обработка которых возможна только в определённых случаях: при наличии письменного согласия; если обработка необходима для защиты жизни работника; в связи с обязательными медицинскими осмотрами согласно ТК РФ [1, 2]. Передача медицинских данных работника страховым компаниям в рамках ДМС требует его явного согласия; работодатель не вправе раскрывать диагноз сотрудника даже непосредственному руководителю.

3.3. *Данные систем мониторинга и видеонаблюдения.* Видеонаблюдение на рабочих местах, мониторинг использования корпоративных устройств и сетей, геолокация служебных автомобилей – правомерны при условии: уведомления работников о факте наблюдения (в трудовом договоре или локальном акте); ограничения целей обработки контролем трудовой дисциплины и обеспечением безопасности; соразмерности меры поставленной цели [2, 4]. Тотальный мониторинг личной переписки работника (в том числе в корпоративных мессенджерах в нерабочее время) существенно нарушает права на неприкосновенность частной жизни. Согласно судебной практике РФ, признано недопустимым тотальное наблюдение без надлежащего уведомления [14–16].

3.4. *Трансграничная передача данных.* Реформа 2022 г. (изменения ФЗ от 14.07.2022 № 266-ФЗ) повысила требования к контролю по

передаче персональных данных на территорию иностранного государства, а именно: передача в страны, не обеспечивающие надлежащую защиту, допускается только при наличии разрешения органов Роскомнадзора, а также с письменного согласия субъекта [5]. Это особенно актуально для работодателей, использующих иностранные облачные HR-системы (SAP SuccessFactors, Workday, Oracle HCM): хранение данных российских работников на серверах за рубежом требует либо их локализации на территории РФ (ст. 22.1 Закона № 152-ФЗ в части первичного сбора), либо соблюдения специальных требований к передаче.

4. Правоприменительная практика: инциденты и ответственность. Анализ инцидентов и правоприменительной практики позволяет выделить наиболее типичные уязвимости и их правовые последствия (табл. 1).

Таблица 1. Типовые нарушения в сфере персональных данных работников и меры ответственности
Table 1. Typical violations in the field of personal data of employees and penalties

Тип нарушения	Правовое основание ответственности	Типичные санкции
Утечка персональных данных по вине работника (инсайдер)	Ст. 13.11 КоАП РФ; ст. 272, 183 УК РФ; ст. 1068 ГК РФ	Штраф до 500 млн руб. (Закон № 519-ФЗ); уголовное преследование; гражданский иск
Обработка биометрии без согласия	Ст. 11 Закона № 152-ФЗ; ст. 13.11 КоАП РФ	Предписание Роскомнадзора; штраф до 300 тыс. руб.
Непредоставление работнику доступа к его данным	Ст. 89 ТК РФ; ст. 14 Закона № 152-ФЗ	Предписание; штраф; иск о компенсации морального вреда
Утечка из облачной HR-системы иностранного провайдера	Ст. 6, 22.1 Закона № 152-ФЗ; Закон № 266-ФЗ	Оборотный штраф; предписание о локализации данных
Видеонаблюдение без уведомления работников	Ст. 86 ТК РФ; ст. 137 УК РФ	Признание доказательств недопустимыми; штраф; компенсация

Составлено авторами на основе [1, 2, 6, 7, 10].

Показательным примером является инцидент мая 2022 г., когда в публичный доступ попали персональные данные курьеров крупных сервисов доставки (Delivery Club, «Яндекс.Еда»): имена, телефоны, адреса доставок. Роскомнадзор привлёк операторов к ответственности по ст. 13.11 КоАП РФ. В итоге суды удовлетворяли иски пострадавших работников о компенсации морального вреда [8].

В банковском секторе фиксировались случаи инсайдерских утечек: сотрудник, злоупотребляя служебным доступом, копировал кадровые и клиентские базы. Подобные инциденты сопровождалась уголовными делами по ст. ст. 272 и 183 Уголовного кодекса Российской Федерации (незаконный доступ к компьютерной информации; противоправное получение и разглашение сведений, составляющих коммерческую тайну). Работодатель

был привлечен к гражданско-правовой ответственности за действия работника при исполнении трудовых обязанностей (ст. 1068 ГК РФ) [9, 10].

В госсекторе отмечались случаи раскрытия персональных данных государственных служащих из-за неверной конфигурации облачных хранилищ: списки сотрудников с должностями и контактами оказывались в открытом доступе. Роскомнадзор выносил предписания и обязывал операторов провести аудит и устранить нарушения.

5. Ответственность за нарушения: обновлённый санкционный режим. Система юридической ответственности за нарушения в сфере персональных данных работников является многоканальной. В 2022–2023 гг. она была существенно усилена [17, 18].

Административная ответственность предусмотрена ст. 13.11 КоАП РФ. С момента последних реформ базовые санкции для юридических лиц варьируются от 60 тыс. до 6 млн рублей, в зависимости от типа нарушения. Введённые Законом № 519-ФЗ оборотные штрафы (до 3% годовой выручки, но не более 500 млн рублей) применяются при крупных утечках, затрагивающих более 10000 субъектов [6].

Гражданско-правовая ответственность: работник имеет право на компенсацию морального вреда за незаконную обработку его личных данных (ст. 89 ТК РФ; ст. 151, 1099–1101 ГК РФ) [2]. Согласно разъяснениям Верховного суда РФ, моральный вред при нарушении прав субъекта персональных данных предполагается, размер которого определяется судом исходя из обстоятельств дела.

Уголовная ответственность наступает по ст. 137 УК РФ (нарушение неприкосновенности частной жизни) и ст. 272 УК РФ (неправомерный доступ к компьютерной информации) при умышленных деяниях, повлёкших существенный вред правам граждан.

Работодатель как оператор несёт риск ответственности за действия своих работников, допустивших утечку данных при исполнении трудовых обязанностей (ст. 1068 ГК РФ), – даже если сам работодатель формально соблюдал все требования законодательства.

6. ИИ-технологии в кадровом делопроизводстве: потенциал и правовые риски. Внедрение систем искусственного интеллекта в

HR-процессы (автоматизированный отбор резюме, оценка кандидатов, прогнозирование текучести кадров, анализ эффективности работников) создаёт новые вызовы для защиты персональных данных [11, 12, 19].

С правовой точки зрения ключевой проблемой является автоматизированное принятие решений, существенно затрагивающих права работника. Закон № 152-ФЗ (ст. 16) запрещает принятие решений, основанных исключительно на автоматизированной обработке данных, без согласия субъекта, если такие решения порождают юридические последствия [1]. Это означает, что автоматическое отклонение кандидата или принятие решения об увольнении исключительно на основании ИИ-системы является незаконным без соответствующего согласия и возможности оспорить такое решение.

Кроме того, ИИ-системы анализа поведения работников, эмоционального состояния (распознавание лица, анализ голоса) фактически обрабатывают биометрические данные, что требует письменного согласия и высокого уровня технической защиты [3, 11, 20]. Государственная Дума рассматривает законопроект об обязательной маркировке ИИ-систем в HR и раскрытии критериев алгоритмических решений, затрагивающих трудовые права.

Выводы

1. Российская модель защиты персональных данных работников прошла существенную трансформацию в 2022–2023 гг. Введение оборотных штрафов (Закон № 519-ФЗ), требований об уведомлении регулятора об утечках (Закон № 266-ФЗ) и ужесточение режима трансграничной передачи данных радикально повышают цену несоблюдения требований для работодателей.

2. Эффективная защита персональных данных работников требует построения многоуровневой системы, сочетающей правовые (локальные акты, договорная защита, работа с согласиями), организационные (разграничение доступа, обучение персонала) и технические (шифрование, DLP-системы, аудит) меры. Ни один из уровней не может быть заменён другим.

3. Обработка специальных категорий данных (биометрия, медицинские сведения) и применение систем мониторинга работников требуют особой правовой осторожности:

именно в этих сферах концентрируется наибольшее число нарушений и претензий регулятора.

4. Внедрение ИИ-технологий в HR создаёт новые правовые риски, связанные с автоматизированным принятием решений и скрытой обработкой биометрии. Российское законодательство в этой части пока отстаёт от темпов технологического развития, что порождает правовую неопределённость.

5. Практические рекомендации для работодателей: провести аудит существующей системы обработки персональных данных работников; актуализировать локальные акты с учётом реформ 2022–2023 гг.; выстроить процедуру уведомления Роскомнадзора об утечках; включить условия о защите персональных данных во все договоры с аутсорсерами и облачными провайдерами; обеспечить регулярное обучение сотрудников кадровых и ИТ-служб.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2023). Москва: Проспект, 2023. 52 с.
2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 22.04.2024). Москва: Проспект, 2024. 424 с.
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»». Москва: Официальное издание, 2022. 18 с.
6. Федеральный закон от 12.12.2023 № 519-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Москва: Официальное издание, 2023. 12 с.
7. Минбалеев А. В. Обеспечение кибербезопасности и международной информационной безопасности в системе обеспечения информационного суверенитета // Правовое обеспечение суверенитета России: проблемы и перспективы: сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции юридического факультета МГУ им. М. В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях. Москва, 2024. С. 134–137. EDN: AKYBIT
8. Гатиятуллина Э. М. Защита персональных данных в условиях цифровизации: эволюция и современное состояние // Закон и власть. 2023. № 3. С. 33–37. EDN: CMIVFT
9. Тишкович К. С. Влияние цифровизации на трансформацию признаков трудовых правоотношений // Правоприменение в публичном и частном праве: материалы Международной научной конференции. Омск, 2023. С. 389–393. EDN: WYUJZK
10. Бачило И. Л. О методах и методологии в информационном праве // Динамика институтов информационной безопасности. Правовые проблемы. Сборник научных трудов. Отв. ред. Т. А. Полякова, В. Б. Наумов, Э. В. Талапина. 2018. С. 20–28. EDN: YHNHEL
11. Харитонов Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 337–358. DOI: 10.21202/jdtl.2023.14. EDN: DXNWHV
12. Кутько В. В., Батова О. В., Городнова О. Н. Правовое государство как явление социально-правовой действительности // Вестник Российского университета кооперации. 2020. № 4(42). С. 128–131. EDN: UFCIVA
13. Minbaleev A.V., Evsikov K.S., Solovkin S.V. Development of legal and normative-technical regulation of quantum communications // Kutafin Law Review. 2025. Т. 12. № 4. С. 781–800. DOI: 10.17803/2713-0533.2025.4.34.781-800. EDN: RTOLKY
14. Полякова Т. А., Минбалеев А. В., Троян Н. А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131–144. DOI: 10.31857/S102694520025209-0. EDN: JUISEQ
15. Минбалеев А. В. Перспективные направления правового регулирования персональных данных // Юридический Вестник Дагестанского государственного университета. 2024. Т. 52. № 4. С. 152–156. DOI: 10.21779/2224-0241-2024-52-4-152-156. EDN: BJNVQZ

16. Лютов Н. Л. Запрет генетической дискриминации и защита генетических персональных данных: перспективы модификации норм трудового права // Журнал российского права. 2021. Т. 25. № 10. С. 72–84. DOI: 10.12737/jrl.2021.124. EDN: JN1JFZ

17. Тишкович К. С. Актуальные проблемы обработки персональных данных в трудовых правоотношениях // Вестник Омского университета. Серия: Право. 2023. Т. 20. № 1. С. 66–74. DOI: 10.24147/1990-5173. EDN: CDZLCY

18. Сердюк П. Л. Особенности уголовной ответственности за мошенничество с использованием электронных средств платежа и компьютерной информации // Уголовная политика в современной России: состояние и перспективы развития: сборник материалов Всероссийской научно-практической конференции. Уфа, 2020. С. 81–87. EDN: LANABS

19. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Основные тенденции и проблемы развития науки информационного права // Государство и право. 2022. № 9. С. 94–104. DOI: 10.31857/S102694520022203-4. EDN: WFOCEJ

20. Офман Е. М. Наблюдение и контроль в трудовых отношениях: баланс прав и интересов работников и работодателей // Журнал российского права. 2021. Т. 25. № 11. С. 73–87. DOI: 10.12737/jrl.2021.136. EDN: WMJJVS

References

1. *Federal'nyj zakon ot 27.07.2006 № 152-FZ «O personal'nykh dannykh» (red. ot 06.02.2023)* [Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" (as amended on February 6, 2023)]. Moscow: Prospekt, 2023. 52 p. (In Russ.)

2. *Trudovoj kodeks Rossijskoj Federatsii ot 30.12.2001 № 197-FZ (red. ot 22.04.2024)* [Labor Code of the Russian Federation of 30.12.2001 No. 197-FZ (as amended on 22.04.2024)]. Moscow: Prospekt, 2024. 424 p. (In Russ.)

3. *Postanovlenie Pravitel'stva RF ot 01.11.2012 № 1119 «Ob utverzhdenii trebovanij k zashchite personal'nykh dannykh pri ikh obrabotke v informacionnykh sistemakh personal'nykh dannykh»* [Resolution of the Government of the Russian Federation of November 1, 2012 No. 1119 "On Approval of Requirements for the Protection of Personal Data When Processed in Personal Data Information Systems"]. (In Russ.)

4. *Postanovlenie Pravitel'stva RF ot 15.09.2008 № 687 «Ob utverzhdenii Polozheniya ob osobennostyakh obrabotki personal'nykh dannykh, osushchestvlyaeмой bez ispol'zovaniya sredstv avtomatizatsii»* [Resolution of the Government of the Russian Federation of September 15, 2008 No. 687 "On approval of the Regulation on the specifics of personal data processing carried out without the use of automation tools"]. (In Russ.)

5. *Federal'nyj zakon ot 14.07.2022 № 266-FZ «O vnesenii izmenenij v Federal'nyj zakon «O personal'nykh dannykh»* [Federal Law of July 14, 2022 No. 266-FZ "On Amendments to the Federal Law "On Personal Data". Moscow: Oficial'noe izdanie, 2022. 18 p. (In Russ.)

6. *Federal'nyj zakon ot 12.12.2023 № 519-FZ «O vnesenii izmenenij v Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyakh»* [Federal Law of 12.12.2023 No. 519-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses". Moscow: Oficial'noe izdanie, 2023. 12 p. (In Russ.)

7. Minbaleev AV. Ensuring Cybersecurity and International Information Security in the System of Ensuring Information Sovereignty. *Pravovoe obespechenie suvereniteta Rossii: problemy i perspektivy. Sbornik dokladov XXIV Mezhdunarodnoj nauchno-prakticheskoy konferentsii i XXIV Mezhdunarodnoj nauchno-prakticheskoy konferentsii Yuridicheskogo fakul'teta MGU im. M.V. Lomonosova v ramkakh XIII Moskovskoj yuridicheskoy nedeli. In the collection: Legal Support of Russia's Sovereignty: Problems and Prospects*. [Legal Support of Russia's Sovereignty: Problems and Prospects. Collection of reports from the XXIV International Scientific and Practical Conference and the XXIV International Scientific and Practical Conference of the Law Faculty of Moscow State University named after M.V. Lomonosov within the framework of the XIII Moscow Legal Week]. In 4 parts. Moscow, 2024. Pp. 134–137. (In Russ.). EDN: AKYBIT.

8. Gatiyatullina EM. Protection of personal data in the context of digitalization: evolution and current state. *Zakon i vlast'*. 2023;(3):33–37. (In Russ.). EDN: CMIVFT

9. Tishkovich KS. Influence of digitalization on transformation of features of labor legal relations. *Pravoprimenenie v publichnom i chastnom prave: materialy Mezhdunarodnoj nauchnoy konferentsii* [Law Enforcement in Public and Private Law: Proceedings of the International Scientific Conference]. Omsk, 2023. Pp. 389–393. (In Russ.). EDN: WYUJZK.

10. Bachilo IL. On Methods and Methodology in Information Law. *Dinamika institutov informacionnoj bezopasnosti. Pravovye problemy. Sbornik nauchnykh trudov*. [Dynamics of Information Security Institutions. Legal Problems. Collection of Scientific Papers. Ed. TA Polyakova, VB Naumov, EV Talapina]. 2018. Pp. 20–28. (In Russ.). EDN: YHNHEL

11. Haritonova YuS. Legal means of providing the principle of transparency of the artificial intelligence. *Journal of Digital Technologies and Law*. 2023;1(2):337–358. (In Russ.). DOI: 10.21202/jdtl.2023.14. EDN: DXNWHV
12. Kutko VV, Batova OV, Gorodnova ON. The legal state as a phenomenon of social and legal activity. *Vestnik of the Russian university of cooperation*. 2020;(4):128–131. (In Russ.). EDN: UFCIVA
13. Minbaleev AV, Evsikov KS, Solovkin SV. Development of legal and normative-technical regulation of quantum communications. *Kutafin Law Review*. 2025;12(4):781–800. DOI: 10.17803/2713-0533.2025.4.34.781-800. EDN: RTOLKY
14. Polyakova TA, Minbaleev AV, Troyan NA. Formation of a culture of information security of citizens of the Russian Federation in the face of new challenges: public law problems. *State and Law*. 2023;(5):131–144. (In Russ.). DOI: 10.31857/S102694520025209-0. EDN: JUISEQ
15. Minbaleev AV. Promising areas of legal regulation of personal data. *Law herald of Dagestan state university*. 2024;52(4):152–156. (In Russ.). DOI: 10.21779/2224-0241-2024-52-4-152-156. EDN: BJNVQZ
16. Lyutov NL. Prohibition of genetic discrimination and protection of genetic personal data: prospects for modification of labor law norms. *Journal of russian law*. 2021;25(10):72–84. (In Russ.). DOI: 10.12737/jrl.2021.124. EDN: JNIFZ
17. Tishkovich KS. Actual problems of processing personal data in labour law relations. *Herald of Omsk university. Series "Law"*. 2023;20(1):66–74. (In Russ.). DOI: 10.24147/1990-5173. EDN: CDZLCY
18. Serdyuk PL. Features of criminal liability for fraud using electronic means of payment and computer information. *Ugolovnaya politika v sovremennoj Rossii: sostoyanie i perspektivy razvitiya: sbornik materialov Vserossijskoj nauchno-prakticheskoy konferentsii* [Criminal policy in modern Russia: state and development prospects: collection of materials from the All-Russian scientific and practical conference]. Ufa, 2020. Pp. 81–87. (In Russ.). EDN: LAHABS
19. Polyakova TA, Minbaleev AV, Krotkova NV. Main trends and problems of development of the science of information law. *State and Law*. 2022;(9):94–104. (In Russ.). DOI: 10.31857/S102694520022203-4. EDN: WFOCEJ
20. Ofman EM. Monitoring and control in labor relations: balancing the rights and interests of employees and employers. *Journal of Russian law*. 2021;25(11):73–87. (In Russ.). DOI: 10.12737/jrl.2021.136. EDN: WMJJVS

Сведения об авторах

Кудзаева Ирина Леонидовна – кандидат экономических наук, доцент, доцент кафедры технических систем в агробизнесе, Федеральное государственное бюджетное образовательное учреждение высшего образования «Горский государственный аграрный университет»

Сужаев Леонид Петрович – кандидат технических наук, доцент кафедры технических систем в агробизнесе, Федеральное государственное бюджетное образовательное учреждение высшего образования «Горский государственный аграрный университет», SPIN-код: 3389-9964

Information about the authors

Irina L. Kudzaeva – Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Technical Systems in Agribusiness, Gorsky State Agrarian University

Leonid P. Suzhaev – Candidate of Technical Sciences, Associate Professor of the Department of Technical Systems in Agribusiness, Gorsky State Agrarian University, SPIN-code: 3389-9964

Авторский вклад. Все авторы принимали непосредственное участие в планировании, выполнении и анализе данного исследования. Все авторы ознакомились и одобрили окончательный вариант статьи.

Author's contribution. All authors have directly participated in the planning, execution and analysis of this study. All authors have read and approved the final version of this article.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest. The authors declare no conflict of interest.

Статья поступила в редакцию 03.06.2026;
одобрена после рецензирования 25.06.2026;
принята к публикации 02.07.2026.

The article was submitted 03.06.2026;
approved after reviewing 25.06.2026;
accepted for publication 02.07.2026.