

Дата поступления рукописи в редакцию: 03.07.2026 г.

DOI: 10.24412/2076-1503-2026-8-827-833

Дата принятия рукописи в печать: 24.07.2026 г.

СОСНОВСКИЙ Евгений Сергеевич,
преподаватель кафедры публичного права
Санкт-Петербургского государственного университета
аэрокосмического приборостроения,
e-mail: jacksos730@gmail.com

КИРИЛЛОВА Татьяна Константиновна,
доктор юридических наук, профессор кафедры гражданского
права Санкт-Петербургского государственного
университета аэрокосмического приборостроения,
e-mail: tania.kirillova.gmail.com@yandex.ru

КОНФИДЕНЦИАЛЬНОСТЬ СБОРА ДАННЫХ И ИХ ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫМИ ПОМОЩНИКАМИ НА ПРИМЕРЕ АЛИСЫ И САЛЮТА: ЮРИДИЧЕСКИЕ АСПЕКТЫ

Аннотация. В статье проводится комплексное исследование юридических аспектов сбора, обработки и использования персональных данных пользователей голосовыми виртуальными ассистентами на примере отечественных программных продуктов «Алиса» (ПАО «Яндекс») и «Салют» (ПАО «Сбербанк»). Анализируется соответствие практики обработки голосовых и биометрических данных требованиям Федерального закона «О персональных данных», исследуются проблемы информированного согласия, трансграничной передачи данных, локализации баз данных, а также защиты прав субъектов персональных данных, включая третьих лиц. Особое внимание уделяется квалификации голоса как биометрических персональных данных, вопросам ответственности операторов, а также сравнительно-правовому анализу с зарубежными подходами (GDPR). Авторы приходят к выводу о необходимости совершенствования правового регулирования обработки голосовых данных как особой категории персональной информации, внедрения принципов *privacy by design* (приватность на этапе проектирования) и *privacy by default* (приватность по умолчанию), а также усиления гарантий прав субъектов данных.

Ключевые слова: персональные данные, конфиденциальность, виртуальный помощник, голосовой ассистент, биометрические данные, информированное согласие, цифровые права, искусственный интеллект, локализация данных.

SOSNOVSKY Evgeny Sergeevich,
Lecturer at the St. Petersburg State University of Aerospace
Instrumentation

KIRILLOVA Tatiana Konstantinovna,
Doctor of Law, Professor of the Department of Public Law, St.
Petersburg State University of Aerospace Instrumentation

DATA COLLECTION PRIVACY AND ITS USE BY VIRTUAL ASSISTANTS ON THE EXAMPLE OF ALICE AND SALUT: LEGAL ASPECTS

Annotation. The article provides a comprehensive study of the legal aspects of the collection, processing and use of users' personal data by voice virtual assistants on the example of Russian software products "Alice" (Yandex) and "Salut" (Sberbank). The author analyzes the compliance of voice and biometric data processing practices with the requirements of the Federal Law "On Personal Data", explores the problems of informed consent, cross-border data transfer, database localization, as well as the protection of the rights of personal data subjects, including third parties. Particular attention is paid to the qualification of voice as biometric personal data, issues of operators' liability, and comparative legal analysis with foreign approaches (GDPR). The authors conclude that it is

necessary to improve the legal regulation of voice data processing as a special category of personal information, to introduce the principles of privacy by design and privacy by default, and to strengthen the guarantees of the rights of data subjects.

Key words: *personal data, privacy, virtual assistant, voice assistant, biometric data, informed consent, digital rights, artificial intelligence, data localization.*

Стремительное развитие технологий искусственного интеллекта и машинного обучения привело к массовому распространению голосовых виртуальных помощников, интегрированных в смартфоны, «умные» колонки, автомобили, телевизоры и разнообразную бытовую технику. Голосовой интерфейс постепенно становится одним из доминирующих способов взаимодействия человека с цифровой средой, что обусловлено его естественностью и удобством. В Российской Федерации лидирующие позиции на данном рынке занимают ассистент «Алиса» компании ПАО «Яндекс», интегрированный в устройства линейки «Яндекс.Станция», и семейство виртуальных ассистентов «Салют» (Сбер, Афина, Джой) ПАО «Сбербанк», реализованное в устройствах SberBoom, SberBox, SberPortal и мобильных приложениях экосистемы.

Указанные технологии, обеспечивая пользователю комфорт взаимодействия с цифровыми сервисами, одновременно осуществляют непрерывный сбор колоссальных объемов персональных данных, включая аудиозаписи голоса, историю запросов, сведения о геолокации, данные об используемых устройствах, а также информацию о поведенческих паттернах пользователя. Более того, современные ассистенты способны формировать детальные профили пользователей, объединяя данные из различных сервисов единой цифровой экосистемы, что многократно усиливает потенциальные риски для приватности.

Актуальность темы обусловлена тем обстоятельством, что голосовые данные обладают особой чувствительностью: они позволяют не только идентифицировать личность говорящего, но и определить его эмоциональное состояние, пол, приблизительный возраст, акцент и региональную принадлежность, а в ряде случаев – сделать выводы о состоянии здоровья (например, о наличии заболеваний дыхательных путей или неврологических расстройств) [1]. Постоянная активность микрофона устройств с функцией активации по ключевому слову создает существенные риски несанкционированного вторжения в частную жизнь, гарантированную статьями 23 и 24 Конституции Российской Федерации, согласно которым каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а сбор, хранение, использование и распространение информации о частной жизни лица без его согласия

не допускаются.

Проблема приобретает особую остроту в условиях, когда правовое регулирование объективно отстает от темпов технологического развития. Законодатель вынужден реагировать на уже сложившиеся общественные отношения, что порождает многочисленные правовые пробелы и коллизии. В связи с этим исследование юридических аспектов функционирования виртуальных ассистентов представляется своевременным и практически значимым.

Степень научной разработанности темы остается недостаточной. Отдельные аспекты правового регулирования обработки персональных данных в цифровой среде рассматривались в работах Архипова В.В. [1], А.И. Савельева [2], Л.К. Терещенко [3], Т.А. Поляковой [4], Э.В. Талапиной [5], В.Б. Наумова [6]. Вместе с тем специфика правового статуса голосовых данных, собираемых виртуальными ассистентами, а также комплексный анализ их обработки на примере конкретных отечественных продуктов до настоящего времени не становились предметом самостоятельного монографического или статейного исследования, что определяет научную новизну настоящей работы.

Целью настоящей статьи является выявление и системный анализ юридических проблем, возникающих при сборе, обработке и использовании персональных данных виртуальными помощниками «Алиса» и «Салют», а также формулирование научно обоснованных предложений по совершенствованию действующего законодательства Российской Федерации в данной сфере.

Для достижения указанной цели поставлены следующие задачи: во-первых, определить правовую природу голосовых данных и решить вопрос об их квалификации в качестве биометрических персональных данных; во-вторых, проанализировать соответствие политики конфиденциальности и пользовательских соглашений рассматриваемых сервисов требованиям законодательства о персональных данных; в-третьих, выявить проблемы реализации института информированного согласия применительно к голосовым интерфейсам; в-четвертых, исследовать вопросы трансграничной передачи данных и локализации баз данных; в-пятых, рассмотреть механизмы защиты прав субъектов персональных данных, включая третьих лиц; в-шестых, провести сравнитель-

но-правовой анализ с зарубежными подходами; в-седьмых, предложить направления совершенствования правового регулирования.

Методологическую основу исследования составили общенаучные методы познания (анализ, синтез, индукция, дедукция, системный и структурно-функциональный подходы) и частнонаучные юридические методы: формально-юридический (для толкования норм законодательства о персональных данных), сравнительно-правовой (для сопоставления российского и зарубежного регулирования), а также метод юридического моделирования.

В соответствии с пунктом 1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Голосовая запись пользователя, безусловно, подпадает под данное определение, поскольку в совокупности с иными данными позволяет прямо или косвенно идентифицировать конкретное физическое лицо.

Однако наиболее дискуссионным остается вопрос о квалификации голоса как биометрических персональных данных. Согласно статье 11 указанного закона, биометрическими являются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных. Таким образом, ключевым критерием отнесения данных к биометрическим выступает не только их физиологическая природа, но и цель их использования [2, с. 214].

Данный подход подтверждается разъяснениями Роскомнадзора «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки», согласно которым фотографическое изображение, аудиозапись голоса и иные аналогичные сведения становятся биометрическими персональными данными лишь тогда, когда оператор использует их именно для установления личности конкретного субъекта, а не для иных целей. Следовательно, если запись голоса используется исключительно для распознавания смысла команды (преобразования речи в текст) и последующего выполнения запроса, такие данные формально не относятся к биометрическим. Напротив, если оператор применяет голосовой слепок для идентификации или аутентификации пользователя – как это реализовано в функции голосовой биомет-

рии в экосистеме Сбербанка, позволяющей подтверждать личность клиента по голосу, – данные приобретают безусловный статус биометрических и требуют письменного согласия субъекта в силу части 1 статьи 11 Закона № 152-ФЗ.

Как справедливо отмечает А.И. Савельев, отсутствие четкого и однозначного критерия «использования для установления личности» порождает существенную правовую неопределенность, поскольку один и тот же массив данных в зависимости от целей обработки может как относиться, так и не относиться к биометрическим [2, с. 216]. Данная неопределенность создает благоприятную почву для злоупотреблений со стороны операторов, которые могут декларировать неидентификационные цели обработки, фактически формируя голосовые слепки пользователей.

Существенное значение для рассматриваемой проблематики имеет принятие Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных...», установившего специальный правовой режим обработки биометрии и закрепившего функционирование Единой биометрической системы (ЕБС) как государственной информационной системы [5]. Согласно данному закону, размещение и обработка биометрических персональных данных для целей идентификации и аутентификации осуществляются преимущественно в рамках ЕБС, что существенно повышает требования к коммерческим операторам, работающим с голосовыми слепками, и фактически ограничивает возможность самостоятельного формирования частных биометрических баз данных. Как отмечает Э.В. Талапина, введение централизованной модели обработки биометрии направлено на усиление государственного контроля и защиту субъектов, однако создает и определенные риски концентрации чувствительных данных [5, с. 895].

Анализ пользовательских соглашений, политик конфиденциальности и публичной информации о рассматриваемых сервисах позволяет выявить ряд характерных особенностей обработки персональных данных.

Оба оператора собирают широкий спектр сведений: аудиозаписи голосовых команд, их текстовые расшифровки, метаданные устройства (модель, версия операционной системы, идентификаторы), сведения о сетевом соединении и IP-адресе, данные о геолокации, историю взаимодействий с сервисом, а также информацию о сопряженных устройствах «умного дома». Записи голоса могут использоваться для обучения нейросетевых моделей распознавания и синтеза речи, улучшения качества работы ассистента, а в от-

дельных случаях – для таргетирования рекламы в рамках экосистемы.

Принципиальная техническая особенность голосовых ассистентов состоит в том, что активация устройства осуществляется по ключевому слову («Алиса», «Салют», «Сбер»), что предполагает постоянный анализ звукового потока встроенным микрофоном в режиме ожидания. Хотя операторы заявляют, что передача аудиоданных на удаленные серверы начинается только после произнесения активационной фразы, а предшествующая обработка осуществляется локально на устройстве, риск случайной («ложной») активации и, как следствие, записи фоновых разговоров, в том числе третьих лиц, не давших согласия на обработку своих данных, остается существенным [3, с. 45]. Это порождает самостоятельную и до конца не разрешенную в законодательстве проблему обработки персональных данных лиц, которые не являются пользователями сервиса, не заключали пользовательского соглашения и не выражали какого-либо согласия на сбор и обработку своих голосовых данных.

Отдельного внимания заслуживает практика привлечения к прослушиванию и разметке (аннотированию) фрагментов аудиозаписей ассессоров – специалистов, вручную обрабатывающих данные для обучения алгоритмов. Даже при заявленной обезличенности таких записей сохраняется вероятность реидентификации субъекта по содержанию разговора, что подтверждается зарубежным опытом соответствующих разбирательств в отношении крупных технологических компаний [6, с. 138].

Не менее важным является вопрос трансграничной передачи данных и локализации баз данных на территории Российской Федерации в силу части 5 статьи 18 Закона № 152-ФЗ, обязывающей операторов при сборе персональных данных граждан РФ обеспечивать их запись, систематизацию, накопление, хранение, уточнение и извлечение с использованием баз данных, находящихся на территории России. Обучение крупных языковых моделей и систем распознавания речи нередко предполагает использование распределенных вычислительных мощностей и облачной инфраструктуры, что создает потенциальные риски нарушения требования о первичной локализации [4, с. 78].

Институт согласия субъекта персональных данных выступает одной из ключевых правовых гарантий защиты приватности. Согласно статье 9 Закона № 152-ФЗ, согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и добровольным. Однако применительно к виртуаль-

ным ассистентам реализация каждого из этих требований оказывается существенно затрудненной.

Во-первых, пользователь при активации сервиса акцептует объемные пользовательские соглашения и политики конфиденциальности, содержание которых он, как правило, не изучает в силу их значительного объема, сложности юридической терминологии и отсутствия реальной альтернативы (отказ означает невозможность использования продукта). Формируется феномен «согласия по умолчанию» (или «клик-согласия»), при котором формально-юридическое согласие не отражает действительной осознанной воли субъекта [6, с. 132]. В научной литературе данное явление получило наименование «парадокса приватности»: пользователи декларируют высокую озабоченность защитой своих данных, но на практике легко соглашаются на их обработку ради получения удобного сервиса [7, с. 88].

Во-вторых, в случае с «умными» колонками и иными устройствами без экрана отсутствует традиционный визуальный интерфейс, что делает практически невозможным надлежащее предоставление субъекту всей необходимой информации об обработке непосредственно в момент голосового взаимодействия. Требование информированности вступает в объективное противоречие с самой природой безэкранный голосового интерфейса.

В-третьих, как уже отмечалось, невозможно получить согласие третьих лиц, чей голос случайно попал в запись при ложной активации либо во время многопользовательского общения в помещении, где установлено устройство. Действующее законодательство не содержит адекватного механизма легитимации обработки данных таких лиц.

Как справедливо отмечается в юридической литературе, необходим постепенный переход от модели формального (декларативного) согласия к концепциям *privacy by design* (приватность на этапе проектирования) и *privacy by default* (приватность по умолчанию), предполагающим встраивание механизмов защиты приватности непосредственно в архитектуру технологии на самых ранних стадиях ее разработки [7, с. 91]. Данные концепции, получившие нормативное закрепление в Общем регламенте ЕС по защите данных (GDPR), пока не имеют прямого аналога в российском законодательстве.

Обращение к зарубежному опыту правового регулирования обработки данных виртуальными ассистентами представляет значительный интерес для совершенствования отечественного законодательства.

В Европейском союзе основным нормативным актом выступает Общий регламент по защи-

те данных (General Data Protection Regulation, GDPR), вступивший в силу в 2018 году. GDPR относит биометрические данные, обрабатываемые для целей однозначной идентификации, к особой категории данных (ст. 9), обработка которых по общему правилу запрещена и допускается лишь при наличии явно выраженного согласия либо иных строго определенных оснований. Регламент закрепляет принципы минимизации данных (data minimisation), ограничения цели (purpose limitation), а также прямо предусматривает обязанность обеспечения защиты данных на этапе проектирования и по умолчанию (ст. 25). Существенное значение имеет закрепленное GDPR «право на забвение» (right to be forgotten) и право на переносимость данных (data portability) [8, с. 12].

Практика применения GDPR к деятельности разработчиков голосовых ассистентов уже сформировала важные прецеденты, связанные с прозрачностью обработки данных, обязанностью уведомления пользователей о ручной обработке аудиозаписей и необходимостью получения отдельного согласия на использование данных для целей улучшения сервисов. Данный опыт демонстрирует ценность дифференцированного подхода к различным целям обработки одних и тех же данных.

Сопоставление российского и европейского регулирования показывает, что отечественное законодательство, несмотря на его совершенствование, пока не выработало специализированного режима для высокотехнологичных способов обработки данных, каковыми являются голосовые ассистенты. Действующее законодательство предоставляет субъекту персональных данных ряд прав: право на доступ к своим данным, их уточнение, блокирование и уничтожение (ст. 14 Закона № 152-ФЗ), право на отзыв согласия, а также право на обжалование действий оператора в Роскомнадзор или в судебном порядке. Однако на практике реализация этих прав применительно к голосовым ассистентам существенно осложнена.

Так, субъекту крайне затруднительно получить полный объем собранных о нем данных, поскольку они распределены между различными сервисами экосистемы и представлены в различных форматах. Особую сложность представляет реализация права на удаление данных: даже при удалении конкретных аудиозаписей из личного кабинета пользователя невозможно добиться их полного изъятия из обучающих выборок (датасетов) уже обученных нейросетевых моделей, поскольку с технической точки зрения «извлечение» данных из параметров модели практически неосуществимо. Это порождает фундаментальное противоречие между правом субъекта на удаление

данных и необратимостью процесса машинного обучения.

Существенным шагом в направлении усиления защиты прав субъектов стало ужесточение административной ответственности операторов. Федеральным законом от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» введена дифференцированная, в том числе оборотная, административная ответственность за нарушения в области обработки персональных данных, включая значительные штрафы за неправомерную передачу (утечку) персональных данных [8]. Введение оборотных штрафов, размер которых исчисляется в процентах от выручки организации, свидетельствует о существенном повышении внимания законодателя к проблеме защиты информации и призвано стимулировать операторов к добросовестному исполнению обязанностей по обеспечению безопасности данных.

Вместе с тем меры юридической ответственности носят преимущественно последующий (репрессивный) характер и не всегда способны предотвратить нарушение прав субъектов. В связи с этим представляется целесообразным сместить акцент правового регулирования в сторону превентивных механизмов, встроенных в саму технологию обработки данных.

На основании проведенного анализа представляется целесообразным сформулировать следующие направления совершенствования законодательства Российской Федерации в сфере обработки данных виртуальными ассистентами.

Во-первых, необходимо закрепить в законодательстве специальный правовой режим голосовых данных с учетом их потенциально биометрического характера. Целесообразно установить презумпцию повышенной защиты голосовых записей независимо от декларируемой оператором цели обработки, что устранил существующую правовую неопределенность в вопросе их квалификации.

Во-вторых, следует нормативно закрепить принцип минимизации сбора данных (data minimization), в силу которого оператор вправе собирать только те данные, которые объективно необходимы для достижения заявленной цели, с одновременным установлением обязательных технических требований к устройствам (например, обязательное локальное распознавание активационной фразы без передачи предшествующего аудиопотока).

В-третьих, необходимо разработать механизмы уведомления и защиты прав третьих лиц, чьи данные могут быть случайно собраны устройством при ложной активации, включая обязатель-

ное автоматическое удаление записей, полученных вне контекста намеренного обращения пользователя.

В-четвертых, представляется обоснованным нормативное закрепление принципов *privacy by design* (приватность на этапе проектирования) и *privacy by default* (приватность по умолчанию) по образцу зарубежного регулирования, обязывающих разработчиков встраивать средства защиты приватности в архитектуру продукта на стадии проектирования, а также устанавливать по умолчанию наиболее приватные настройки, требующие от пользователя осознанных действий для расширения объема собираемых данных.

В-пятых, необходимо обеспечить реальную прозрачность алгоритмов обработки данных виртуальными ассистентами. Это предполагает закрепление обязанности оператора предоставлять субъекту в доступной и понятной форме сведения о том, какие категории данных собираются, для каких целей используются, передаются ли они третьим лицам и применяются ли для обучения моделей искусственного интеллекта. Особую значимость приобретает информирование пользователя о фактах ручной обработки (прослушивания) аудиозаписей ассессорами с предоставлением возможности отказаться от использования данных в этих целях без утраты доступа к основному функционалу сервиса.

В-шестых, требуется решение проблемы реализации права на удаление данных применительно к обученным нейросетевым моделям. Учитывая техническую невозможность «извлечения» конкретных данных из параметров модели, целесообразно на нормативном уровне закрепить альтернативные гарантии: обязательное предварительное обезличивание данных перед их включением в обучающие выборки, установление предельных сроков хранения исходных (необезличенных) записей, а также ведение операторами реестров использования данных в целях машинного обучения.

В-седьмых, представляется целесообразным разработать специальные правила обработки данных несовершеннолетних, поскольку голосовые ассистенты активно используются детьми (в том числе через специальные детские режимы). Учитывая повышенную уязвимость данной категории субъектов, необходимо установление усиленных требований к получению согласия законных представителей и ограничению профилирования несовершеннолетних пользователей.

Реализация предложенных мер позволит сформировать сбалансированную модель правового регулирования, обеспечивающую как условия для технологического развития отечественных

цифровых экосистем, так и надлежащую защиту конституционных прав граждан на неприкосновенность частной жизни.

Проведенное исследование позволяет сформулировать ряд выводов, имеющих как теоретическое, так и практическое значение.

Во-первых, установлено, что современное правовое регулирование обработки персональных данных не в полной мере учитывает специфику функционирования голосовых виртуальных помощников. Стремительное развитие технологий искусственного интеллекта существенно опережает темпы адаптации законодательства, что порождает многочисленные правовые пробелы и коллизии.

Во-вторых, обосновано, что голосовые данные занимают особое положение в системе персональной информации. Обладая признаками, приближающими их к биометрическим данным, голос при определенных условиях (использование для идентификации) приобретает статус биометрических персональных данных с соответствующим усиленным режимом защиты. Существующая привязка квалификации данных к цели их использования порождает правовую неопределенность и требует законодательного уточнения, вплоть до введения презумпции повышенной защиты голосовых записей.

В-третьих, анализ практики обработки данных ассистентами «Алиса» и «Салют» продемонстрировал типичные для данной технологии юридические проблемы: непрозрачность процессов обработки, преимущественно формальный характер информированного согласия («парадокс приватности»), риски несанкционированного сбора данных третьих лиц при ложной активации устройств, сложности с локализацией данных при использовании распределенной облачной инфраструктуры, а также техническую невозможность полной реализации права субъекта на удаление данных, вошедших в обучающие выборки нейросетевых моделей.

В-четвертых, сравнительно-правовой анализ показал, что зарубежные подходы, прежде всего закрепленные в Общем регламенте ЕС по защите данных (GDPR), выработали ряд эффективных механизмов (принципы минимизации данных, ограничения цели, *privacy by design* (приватность на этапе проектирования) и *privacy by default* (приватность по умолчанию), заимствование которых с учетом особенностей национальной правовой системы представляется обоснованным и целесообразным.

В-пятых, несмотря на существенное усиление административной ответственности операторов, включая введение оборотных штрафов за

утечки персональных данных, меры ответственности носят преимущественно репрессивный характер и не способны в полной мере предотвратить нарушение прав субъектов. В связи с этим приоритет должен быть отдан превентивным механизмам защиты, встроенным в саму технологию.

Таким образом, совершенствование законодательства должно идти по пути закрепления специального правового режима голосовых данных, нормативного внедрения принципов минимизации данных и приватности на этапе проектирования, разработки механизмов защиты прав третьих лиц и несовершеннолетних, обеспечения прозрачности алгоритмов обработки, а также решения проблемы реализации права на удаление данных в контексте машинного обучения. Реализация указанных мер позволит достичь необходимого баланса между технологическим прогрессом, интересами развития отечественной цифровой индустрии и конституционным правом граждан на неприкосновенность частной жизни, личную и семейную тайну.

Список литературы:

- [1] Архипов В.В. Информационное право и информационная безопасность в условиях цифровой трансформации // Информационное право. — 2021. — № 2. — С. 4–9.
- [2] Савельев А.И. Научно-практический комментарий к Федеральному закону «О персональных данных». — 2-е изд. — М.: Статут, 2021. — 512 с.
- [3] Терещенко Л.К. Правовое регулирование обработки персональных данных в цифровую эпоху // Журнал российского права. — 2021. — № 5. — С. 42–54.
- [4] Полякова Т.А. Правовые проблемы обеспечения информационной безопасности при обработке больших данных // Государство и право. — 2020. — № 8. — С. 74–83.
- [5] Талапина Э.В. Правовое регулирование использования биометрических персональных данных // Вестник Санкт-Петербургского университета. Право. — 2022. — Т. 13. — № 4. — С. 890–905.
- [6] Наумов В.Б. Проблемы правового регулирования оборота персональных данных в условиях цифровизации // Труды Института государства и права РАН. — 2021. — Т. 16. — № 3. — С. 125–145.
- [7] Незнамов А.В. Правовое регулирование технологий искусственного интеллекта: постановка проблемы // Закон. — 2020. — № 5. — С. 85–96.
- [8] Войниканис Е.А. Защита персональных данных: тенденции развития законодательства и

правоприменительной практики // Право. Журнал Высшей школы экономики. — 2022. — № 3. — С. 4–29.

[9] Амелин Р.В., Чаннов С.Е. Государственные и муниципальные информационные системы в системе правовых отношений // Информационное право. — 2021. — № 3. — С. 18–23.

[10] Зорькин В.Д. Право в цифровом мире // Журнал конституционного правосудия. — 2020. — № 4. — С. 1–8.

[11] Рожкова М.А. Что понимается под персональными данными в цифровую эпоху // Хозяйство и право. — 2021. — № 7. — С. 3–16.

References:

- [1] Arkhipov V.V. Information law and information security in the context of digital transformation // Information law. — 2021. — № 2. — S. 4-9.
- [2] Savelyev A.I. Scientific and practical commentary on the Federal Law "On Personal Data." - 2nd ed. - M.: Statute, 2021. - 512 s.
- [3] Tereshchenko L.K. Legal regulation of personal data processing in the digital age // Journal of Russian Law. — 2021. — № 5. - S. 42-54.
- [4] Polyakova T.A. Legal problems of ensuring information security in the processing of big data // State and law. — 2020. — № 8. - S. 74-83.
- [5] E.V. Talapina. Legal regulation of the use of biometric personal data // Bulletin of St. Petersburg University. Right. — 2022. - T. 13. — № 4. - S. 890-905.
- [6] Naumov V.B. Problems of legal regulation of the circulation of personal data in the context of digitalization // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. — 2021. - T. 16. — № 3. - S. 125-145.
- [7] Neznamov A.V. Legal regulation of artificial intelligence technologies: posing a problem // Law. — 2020. — № 5. - S. 85-96.
- [8] Voynikanis E.A. Protection of personal data: trends in the development of legislation and law enforcement practice // Law. Journal of the Higher School of Economics. — 2022. — № 3. - S. 4-29.
- [9] Amelin R.V., Channov S.E. State and municipal information systems in the system of legal relations // Information law. — 2021. — № 3. - S. 18-23.
- [10] Zorkin V.D. Law in the Digital World // Journal of Constitutional Justice. — 2020. — № 4. - S. 1-8.
- [11] Rozhkova M.A. What is meant by personal data in the digital age // Economy and law. — 2021. — № 7. - S. 3-16.