EDN: ZAOGYR

BY-SA

Дата поступления статьи: 19.01.2025
Дата поступления последней рецензии: 12.02.2025
Дата принятия статьи к публикации: 21.04.2025

Персональные данные как вид конфиденциальной информации в условиях формирования электронного государства

Демкин В. О.
Национальный исследовательский университет «Высшая школа экономики» (Москва, Российская Федерация)
E-mail: vodemkin@hse.ru

Аннотация

Введение: актуальность статьи обусловлена развитием систем электронного государства во многих странах мира. Электронное государство работает с большими объемами персональных данных, включая специальные их категории, биометрические. Цель исследования — проанализировать особенности обработки персональных данных в рамках государственных и муниципальных информационных систем, а также в разработке предложений по совершенствованию правового регулирования этой сферы, минимизации рисков информационной безопасности.

Методология и материалы: методологической основой исследования является системный анализ российского и международного законодательства, нормативно-правовых актов.

Результаты исследования и их обсуждение: основные результаты исследования свидетельствуют о том, что персональные данные обладают двойственной правовой природой, совмещая признаки конфиденциальной информации и тайны, условия обеспечения которой установлены не обладателем (владельцем, первоисточником) сведений, а законом императивно. Выявлена двойственная природа персональных данных: с одной стороны, они представляют собой конфиденциальную информацию, доступ к которой возможен с согласия ее владельца, а с другой — могут использоваться и без такого согласия, что делает их схожими с информацией, подпадающей под режим секретности. Установлено, что наибольшие риски для информационной безопасности и обработки данных в рамках электронного государства возникают на этапе создания и интеграции государственных и муниципальных информационных систем. Проанализированы правовые, организационные и технические меры по обеспечению информационной безопасности, подчеркнута важность их комплексного применения для снижения угроз.

Выводы: отмечено, что развитие цифрового государства требует формирования сбалансированной законодательной базы, которая бы одновременно обеспечивала защиту персональных данных и учитывала интересы государства, общества и граждан. Также сделан акцент на необходимости международной унификации норм обработки персональных данных, особенно в контексте Евразийского экономического союза, а также гармонизации соответствующих национальных законодательств.

Ключевые слова: электронное государство, персональные данные, информационная безопасность, конфиденциальная информация, обработка данных, информационные системы, право Евразийского экономического союза.

Для цитирования: *Демкин В. О.* Персональные данные как вид конфиденциальной информации в условиях формирования электронного государства // Теоретическая и прикладная юриспруденция. 2026. № 1 (27). С. 126–138. EDN: ZAOGYR

© Демкин В. О., 2026
© Demkin V. O., 2026

The article was submitted: 19.01.2025
Last review received: 12.02.2025
The article accepted for publication: 21.04.2025

Personal Data as a Type of Confidential Information in the Context of Developing an Electronic State

Vladislav O. Demkin
National Research University Higher School of Economics (HSE University) (Moscow, Russian Federation)
E-mail: vodemkin@hse.ru

Abstract

Introduction: The development of electronic state systems in many countries worldwide determines the relevance of the article. An electronic state processes large volumes of personal data, including special categories, biometric ones. The purpose of the study is to analyze the peculiarities of personal data processing within state and municipal information systems and to develop proposals for improving legal regulation in this area while minimizing information security risks.

Materials and methods: The methodological basis of the study includes a systematic analysis of Russian and international legislation, as well as normative legal acts. The main results indicate that personal data have a dual legal nature, combining features of confidential information and professional secrecy. The study is based on materials from Russian and foreign legislation, as well as legal literature.

The results of the study and their discussion: The dual nature of personal data has been identified: on the one hand, it constitutes confidential information that can be accessed with the owner's consent, while on the other hand, it can be used without such consent, making it similar to information under secrecy regimes. It has been established that the greatest risks to information security and data processing within the framework of an electronic state arise during the creation and integration of state and municipal information systems. Legal, organizational, and technical measures to ensure information security have been analyzed, with an emphasis on the importance of their comprehensive application to mitigate threats.

Conclusions: It has been noted that the development of a digital state requires the formation of a balanced legislative framework that simultaneously ensures the protection of personal data and takes into account the interests of the state, society, and individuals. Additionally, the necessity of international unification of personal data processing rules, particularly within the context of the Eurasian Economic Union, as well as the harmonization of relevant national legislations, has been highlighted.

Keywords: electronic state, personal data, information security, confidential information, data processing, information systems, law of the Eurasian Economic Union.

For citation: Demkin, V. O. (2026) Personal Data as a type of Confidential Information in the Context of Developing an Electronic State. *Theoretical and Applied Law*. No. 1 (27). Pp. 126–138. (In Russ.)

Введение

Сегодня активно развиваются институты электронного государства. Под ним можно понимать такой механизм организации институтов власти, при котором преимущественно в цифровой форме могут оказываться государственные и муниципальные услуги, так же как и исполняться обязанности физическими и юридическими лицами. Такая модернизация государственного управления требует создания реестров чувствительных данных, систем электронной идентификации субъектов права, инфраструктур межведомственного взаимодействия, способов обеспечения безопасности информации. При решении каждой из таких задач могут возникать правовые риски. Например, массовая обработка персональных

данных государственными органами лишь на основании закона, но без согласия субъекта нарушает баланс интересов в правоотношениях, особенно учитывая неоднозначное качество нормативных актов. Сбои в обработке данных вместе с ложной идентификацией личности могут привести к неблагоприятным и несправедливым правовым последствиям для человека, задачей которого станет доказать наличие ошибки в действиях органов власти. Эта проблема осложняется также вопросом «черного ящика», при котором никому, кроме владельца технологии, неизвестны причины и основания принятия определенного решения, если оно принималось автоматизированным образом[1].

Система электронного государства всё чаще используется для коммуникации между органами власти и физическими и юридическими лицами. Публичными органами обрабатывается множество чувствительных данных, принимаются автоматизированные решения (либо с минимальным участием человека). В исследованиях ключевыми факторами доверия к органам власти в таких условиях называются способность органов власти обеспечивать безопасность данных; прозрачность их обработки и контроль населения за этим; степень чувствительности обрабатываемых данных; в целом опыт взаимодействия с интернет-сервисами[2]. Отмечается, что надлежащая и соответствующая ожиданиям субъектов защита персональных данных является ключевым фактором повышения доверия населения к электронному государству и имеет решающее значение для его эффективности[3].

В статье рассмотрены отдельные аспекты признания персональных данных в качестве одного из видов конфиденциальной информации, а также их обработки в рамках формирования электронного государства.

Методология и материалы

Методологической основой исследования является системный анализ российского и международного законодательства, нормативно-правовых актов. В качестве главного метода исследования используется анализ российской и зарубежной литературы и нормативно-правовой практики, в том числе исследование терминов и их определений, категоризация явлений. Основное внимание в работе уделяется российской правовой системе.

Результаты исследования и их обсуждение

1. Персональные данные как один из видов конфиденциальной информации

Конфиденциальность — правовой режим информации, который выражает ограниченность доступа к ней. Он является специальным и направлен на охрану сведений, свободное распространение которых нарушает права и законные интересы общества, государства, личности[4]. В этом режиме особое место занимает обладатель информации — субъект, который определяет режим доступа к ней и средства обеспечения ее конфиденциальности, перечень имеющих доступ к информации лиц. Принятые им решения обязательны для исполнения лицами, которым предоставляется такая информация.

Это утверждение относится в первую очередь к информации о ее обладателе, относящейся к нему. Однако некоторые виды тайн, которые включаются в область режима конфиденциальности, этому условию не соответствуют: сведения, составляющие профессиональную, служебную, государственную тайну,

---

[1] См.: *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд. М.: Статут, 2021. 468 с.; *Pasquale F.* (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. *Harvard University Press*. 304 p.

[2] *Beldad A., Jong M. de, Steehouder M.* (2011) I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. Computers in Human Behavior, vol. 27, no. 6, pp. 2233–2242. https://doi.org/10.1016/j.chb.2011.07.002

[3] *Beldad A., Geest T. van der, Jong M. de, Steehouder M.* A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online // Government Information Quarterly, 2012. Vol. 29, no. 1, pp. 41–49. DOI: https://doi.org/10.1016/j.giq.2011.05.003

[4] *Терещенко Л. К.* Правовой режим информации: дис. … д-ра. юрид. наук. М.: ИЗиСП, 2011. 415 с.

охраняются на основании закона, а не решений ее обладателя. Законом же определяются пределы использования, раскрытия такой информации.

Персональные данные являются одним из видов конфиденциальной информации, относящихся к их (первоначальному) обладателю, то есть к личности. В российском праве они определяются как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[5]. Такое понимание принято и в правовых актах Европейского союза[6].

Существует множество оснований для законной обработки персональных данных, в том числе их сбора. В частности, Федеральный закон «О персональных данных» упоминает в качестве таковых как исходящие от самого субъекта (его согласие или его участие в частно-правовых отношениях по заключению и исполнению договора), так и «навязываемые» ему извне (в частности, обработка по причине «необходимости» для достижения целей закона или международного договора, для обеспечения деятельности органов публичной власти, для достижения общественно значимых целей). При обработке персональных данных по основаниям, не связанным с волеизъявлением (непосредственным или подразумеваемым) субъекта, он утрачивает над ними контроль. Более того, он и не начинает обладать таковым: у субъекта нет права дозволять кому-либо обработку данных о нем, устраняя остальных от этого, устанавливать условия обработки. Таким образом, персональные данные как целостная категория обладает признаками как информации, субъект которых определяет пределы ее использования (и границы сохранения их конфиденциальности), так и тайны, условия обеспечения которой установлены законом императивно.

Такие их особенности проявляются наиболее ярко при обработке органами публичной власти в рамках систем электронного государства. Большинство сведений предоставляются органам публичной власти постольку, поскольку такое предоставление является обязательным для владельцев данных. Это может быть необходимо для целей получения различных льгот, субсидий, привилегий — таких, которые могут быть предоставлены только органами власти, поскольку не существует некоего «рынка льгот», других «поставщиков субсидий». В иностранной литературе также высказываются опасения о том, что судебные органы как представители власти могут чаще занимать сторону органов власти исполнительной в их спорах с физическими лицами. Так, например, это может выражаться в определении ответственности, которую административные органы и должностные лица понесут за инциденты с персональными данными; при определении самого факта наличия инцидента; при установлении размера ущерба, который понесли субъекты, и, соответственно, финансовой ответственности оператора в лице представителей власти[7].

Российская судебная практика привлечения органов исполнительной власти и даже отдельных должностных лиц крайне немногочисленна, а размер налагаемых штрафов можно оценить как низкий. Так, в мае 2023 г. ФГУП «ГРЧЦ» (Главный радиочастотный центр) было привлечено к административной ответственности в виде административного штрафа в 30 000 руб. за необеспечение конфиденциальности персональных данных, из-за чего третьи лица получили неправомерный доступ к базе данных сотрудников ФГУП[8]. В другом деле фельдшер была привлечена к уголовной ответственности в виде судебного штрафа в размере 25 000 руб. за незаконное предоставление третьему лицу сведений пациентки, составляющих врачебную тайну[9]. В начале 2025 года был также опубликован большой массив данных,

---

[5] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31. Ст. 3451.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *EUR-Lex European Union Law*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 (дата обращения: 21.11.2024).

[7] См.: *Froomkin M. A.* (2009) Government Data Breaches. Berkeley Technology Law Journal, vol. 24, no. 3, pp. 1019–1059. URL: https://www.jstor.org/stable/24118272

[8] «Главный Радиочастотный центр» оштрафован за утечку базы данных сотрудников. URL: https://www.interfax-russia.ru/index.php/moscow/news/glavnyy-radiochastotnyy-centr-oshtrafovan-za-utechku-bazy-dannyh-sotrudnikov (дата обращения: 12.07.2025).

[9] Постановление Оренбургского районного суда Оренбургской области от 08.07.2024 по делу № 1-243/2024, УИД 56MS0070-01-2024-002134-41. Доступ из СПС «Консультант Плюс» (дата обращения: 12.02.2025).

предположительно, из единого государственного реестра недвижимости, однако Росреестр отрицает такую утечку и проводит проверку, результаты которой пока неизвестны[10].

В системе электронного государства персональные данные обрабатываются на основании закона и для целей исполнения функций органов публичной власти. Субъекты персональных данных уязвимы при обработке последних органами власти, не могут полноценным образом контролировать начало и процесс такой обработки. Вопросы обеспечения информационной безопасности, прозрачности обработки данных в условиях электронного государства поднимаются всё чаще в правовой, социологической и технической литературе.

2. Электронное государство. Обработка персональных данных органами власти

Термин «электронное государство» обладает комплексным политико-правовым значением, выражая происходящие в обществе процессы цифровизации властных отношений. Феномен электронного государства выражается в использовании современных цифровых технологий органами публичной власти для взаимодействия друг с другом, с населением и юридическими лицами. Таким взаимодействием может быть оказание дистанционных онлайн-услуг в автоматическом режиме (в том числе без участия человека), проведение онлайн-опросов (голосований), осуществление дистанционного правосудия, использование систем межведомственного взаимодействия (в том числе для оказания услуг в режиме «одного окна») и электронного документооборота.

Различаются широкий и узкий подходы к электронному государству. Узкий относится к выражению экономической выгоды от внедрения информационных технологий в деятельность органов публичной власти; широкий — к структурной социальной перестройке, способствующей эффективному общественному участию в демократических процессах[11].

Количество операций, осуществляемых с персональными данными, и категория рисков при их обработке в рамках электронного государства определяются степенью развития последнего. В литературе выделяют несколько стадий его развития, при этом на третьей и четвертой персональные данные обрабатываются наиболее активно и интерактивно. Третья стадия предполагает создание единого портала оказания государственных и муниципальных услуг, возможность лиц заполнять необходимые заявления и получать услуги в интерактивной форме, использование электронного документооборота, электронных подписей. На четвертой стадии выделяется возможность двустороннего влияния органов власти и физических и юридических лиц друг на друга с использованием цифровых технологий. Так, население способно участвовать в принятии решений органами публичной власти онлайн, направлять жалобы и подавать обращения[12].

При этом, согласно социологическим исследованиям, прозрачность при обработке данных и оказании государственных услуг с использованием информационных систем электронного государства повышает уровень доверия органам власти в целом[13].

Отличительной особенностью электронного государства третьей и четвертой стадий можно назвать накопление объемных массивов сведений о физических лицах, их сбор из различных источников (в том числе от частных субъектов), объединение в базы данных.

Россия на современном этапе развития стремится расширить использование технологий электронного государства. Указами Президента РФ в качестве целей развития страны до 2030 г. предусматри-

[10] В Росреестре опровергли утечку данных из ЕГРН. URL: https://www.rbc.ru/society/07/01/2025/677d7dd09a7947c25c825bf4 (дата обращения: 12.02.2025).

[11] См.: *Богдановская И. Ю.* Понятие «электронного государства»: правовые аспекты // В сб. «Информационное общество и социальное государство». М.: Юрист. 2011. С. 45–55; *Данилов Н. А.* Правовое регулирование электронного правительства в зарубежных странах: дис. ... канд. юрид. наук. М.: НИУ ВШЭ, 2013. 158 с. EDN: SUVYPB

[12] *Данилов Н. А.* Правовое регулирование электронного правительства в зарубежных странах: дис. ... канд. юрид. наук. М.: НИУ ВШЭ, 2013. 158 с. EDN: SUVYPB

[13] *Tolbert C. J., Mossberger K.* (2006) The Effects of E-Government on Trust and Confidence in Government // Public Administration Review, vol. 6, no. 3, pp. 354–369. URL: https://www.jstor.org/stable/3843917

ваются: развитие инфраструктуры электронного правительства для оказания государственных, коммерческих и некоммерческих услуг; поэтапный переход органов власти к использованию инфраструктуры электронного правительства[14]; формирование рынка данных[15].

Для достижения этих задач формируются государственные информационные системы. В частности, уже создана и успешно действует Единая система идентификации и аутентификации (ЕСИА). Эта система позволяет физическим и юридическим лицам пройти процедуру регистрации и подтвердить сведения о них. После этого результаты идентификации в этой системе могут использоваться для аутентификации в других системах. ЕСИА также позволяет должностным лицам «связывать» сведения с конкретными лицами и обмениваться такими сведениями в рамках межведомственного взаимодействия.

Развитие обработки персональных данных в электронном государстве связано с созданием Единого регистра населения. В соответствии с принятым Федеральным законом «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» в единую информационную систему будут включены разнообразные сведения о гражданах России, об иностранцах, об апатридах, собранные из различных министерств, ведомств и организаций, для целей реализации государственных полномочий. Так, каждому человеку будет присвоен номер, который станет своего рода учетной карточкой, хранилищем персональных данных о нем, цифровым профилем. Достоверность таких данных будет презюмироваться, а иные лица могут (а некоторые — должны, например, нотариусы) обращаться к регистру для верификации представленных сведений.

Система также позволит более эффективно и даже проактивно оказывать государственные и муниципальные услуги. Уже сейчас в соответствии с Федеральным законом № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» на основании лишь наступления событий, являющихся основанием для предоставления услуги, соответствующий орган власти осуществляет подготовку результатов услуги и сообщает заявителю о возможности подать запрос о немедленном предоставлении результата услуги[16]. В таком порядке предлагается, например, присваивать номер СНИЛС автоматически, по факту регистрации рождения человека[17].

Ценность работы с персональными данными видна также и в принятии Федерального закона от 8 августа 2024 г. № 233-ФЗ о праве Министерства цифрового развития, связи и массовых коммуникаций РФ (Минцифры России) требовать предоставления обезличенных персональных данных у любого оператора. Такие данные будут храниться в специальной государственной информационной системе, и их обработка будет доступна любому желающему оператору (подпадающему под определенные критерии, в частности, о наличии только российского гражданства для физических лиц / месте регистрации в России для юридических лиц)[18].

Похожие тенденции наблюдаются не только в России. В частности, в Великобритании рассматривается законопроект под названием Data (Use and Access) Bill (Акт о данных (об их обработке и доступе к ним)). Так, в нем предполагается унификация данных о состоянии здоровья пациентов и обмен ими среди медицинских учреждений; создание инфраструктуры цифровой идентификации личности (и ве-

---

[14] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

[15] Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // СЗ РФ. 2024. № 20. Ст. 2584.

[16] Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. № 31. Ст. 4179.

[17] Проект Приказа Фонда пенсионного и социального страхования Российской Федерации «Об утверждении Административного регламента Фонда пенсионного и социального страхования Российской Федерации по предоставлению государственной услуги „Прием от граждан анкет в целях регистрации в системе индивидуального (персонифицированного) учета, в том числе прием от зарегистрированных лиц заявлений об изменении анкетных данных, содержащихся в индивидуальном лицевом счете, или о выдаче документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета“». URL: https://www.garant.ru/products/ipo/prime/doc/56873741/#review (дата обращения: 10.11.2024).

[18] Федеральный закон от 8 августа 2024 г. № 233-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“ и Федеральный закон „О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона „О персональных данных“» // СЗ РФ. 2024. № 33. Ст. 4929.

рификации сервисов с таким функционалом) и совершения ряда сделок с ее использованием, а также инфраструктуры электронной регистрации рождения и смерти[19].

Власти Европейского союза намерены создать «Единую цифровую идентичность»[20]. Так, в 2014 г. был принят Регламент «Об электронной идентификации и доверительных услугах для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/ЕС»[21]. Он обязывает государства-члены унифицировать и взаимно признавать национальные системы идентификации личностей и правила применения электронных подписей. Это позволит обеспечить доступ к цифровым услугам на всей территории Европейского союза любому человеку, имеющему европейское электронное удостоверение личности.

Таким образом, наиболее последовательное и урегулированное нормами права формирование цифровой личности происходит совместно с развитием электронного государства и сопровождающих это информационных систем. Создание Единого регистра населения, содержащего обширные данные о каждом гражданине, требует выработки четких стандартов их защиты. Презумпция достоверности данных усиливает ответственность государственных органов за поддержание их актуальности и полноты, но также увеличивает риски нарушения прав на неприкосновенность частной жизни в случае утечки данных или их использования не по назначению.

Развитие электронного государства также связано с развитием юридических фактов, под которыми понимаются конкретные жизненные обстоятельства, вызывающие в соответствии с нормами права наступление тех или иных правовых последствий — возникновение, изменение или прекращение правового отношения[22]. Например, среди таковых можно назвать регистрацию личности в системе для получения государственных услуг, присвоения идентификатора для получения пособий. Отличительной чертой таких юридических фактов является их автоматическая фиксация и использование в информационных системах, изменение правового статуса личности в автоматическом режиме, что является одной из основ проактивного оказания публичных услуг и что упрощает процесс управления и взаимодействия граждан с государством.

Обеспечение защиты прав и интересов субъектов персональных данных при развитии электронного государства заключается в том числе в создании платформы управления согласиями на обработку данных. Она подразумевает возможность физических лиц иметь доступ к своим данным, отозвать согласия, а также контролировать, каким образом их данные используются и передаются. Но, конечно, такой метод не поможет субъектам в контроле над обработкой данных в целях соблюдения требований закона, полномочий органов публичной власти; в отзыве согласия на такую обработку (поскольку оно и не требуется).

Рассмотрев персональные данные как один из видов конфиденциальной информации и основные элементы формирования электронного государства, перейдем к основным положениям и проблемам обработки персональных данных в государственных и муниципальных информационных системах.

3. Обработка персональных данных в государственных и муниципальных информационных системах

Г. Г. Камалова называет два вида субъективной (относительной) тайны, противопоставляя ее объективной (абсолютной) тайне. Первая характеризуется наличием введенного законом или правомерно установленного их обладателем правового ограничения возможности сбора, получения и обработки сведений; вторая охватывает сведения, полностью скрываемые человеком (не доверяемые даже узко-

[19] Data (Use and Access) Bill [HL]. Government Bill. URL: https://bills.parliament.uk/bills/3825 (дата обращения: 11.11.2024).

[20] Digital Identity for all Europeans. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (дата обращения: 16.12.2024).

[21] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (дата обращения: 16.12.2024).

[22] *Исаков В. Б.* Юридические факты в советском праве. М.: Юридическая литература, 1984. 124 с. EDN: YMWNKN

му кругу родных и близких)[23]. Представляется, что в современных электронных государствах сведений, составляющих объективную тайну, становится всё меньше: из нее исключаются персональные данные, обработка которых основана на требовании закона, например, подробности личной жизни людей, если они образуют состав преступлений и иных правонарушений.

Не любые сведения, идентифицирующие физическое лицо, подпадают под регулирование российского закона «О персональных данных». Так, согласно его ст. 1, им регулируется обработка персональных данных лишь с использованием средств автоматизации, а также без таких средств, но с «автоматизированным» характером (т.е. если имеется возможность осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в систематизированных собраниях персональных данных). Закон также не применяется, в частности, к отношениям по обработке персональных данных физическими лицами исключительно для личных и семейных нужд[24].

В современном электронном государстве множество сведений о личности выбывают из-под ее контроля и «доверяются» органам государственной власти. Они объединяются в общие базы данных, информационные системы, формируются реестры, используются инструменты для их связывания друг с другом. Особую роль играет обеспечение информационной безопасности систем электронного государства, поскольку «повышение открытости электронного правительства в условиях использования информационно-коммуникационных технологий сопровождается повышением уровня уязвимости государства: злоумышленники получают доступ к базам данных, содержащим персональные данные индивидов, а также получают возможность дестабилизировать работу обеспечивающих функционирование государства информационных систем»[25]. Информационную безопасность можно определить как состояние защищенности национальных интересов Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз[26].

Можно выделить множество угроз информационной безопасности в области обработки персональных данных в электронном государстве, например:

1. Угроза компрометации данных, так называемых «утечек» — ситуаций, при которых злоумышленник получает доступ к информационным системам, базам данных, содержащих персональные данные, в результате целенаправленного несанкционированного доступа и использует их для своих целей (как правило, распространяет среди неопределенного круга лиц или предоставляет определенным лицам).
2. Разглашение сведений о себе самим субъектом персональных данных в результате использования злоумышленником методов социальной инженерии.
3. Нарушение конфиденциальности из-за некорректной интеграции различных государственных информационных систем, при которой ведомства получают доступ к данным о физических лицах, которые не относятся к их компетенции.
4. Формирование неактуальных сведений на основе недостоверных данных.

Ряд угроз также влечет за собой ошибки в идентификации личности, то есть совершение действий «от имени» одного лица неуполномоченным лицом. Российским Федеральным законом «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…» идентификация определяется в качестве совокупности мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных

---

[23] См.: *Камалова Г. Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. … канд. юрид. наук. М.: ИГП РАН, 2020. 472 с. EDN: IHXJJF

[24] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31. Ст. 3451.

[25] *Данилов Н. А.* Правовое регулирование электронного правительства в зарубежных странах: дис. … канд. юрид. наук. М.: НИУ ВШЭ, 2013. 158 с.

[26] См.: *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … канд. юрид. наук. М.: Российская правовая академия Министерства Юстиции РФ, 2008. 438 с.

сведений с идентификатором — уникальным обозначением сведений о лице, необходимом для определения такого лица[27]. В результате компрометации учетных данных лица злоумышленником, пока не доказано иное, будет считаться, что действия совершаются от имени того лица, сведения для процесса идентификации которого были предоставлены

Противостояние угрозам информационной безопасности в электронном государстве осуществляется с помощью комплекса мер: правовых, организационных и технических.

Правовые меры защиты информации включают в себя развитие норм права персональных данных, которые определяют принципы обработки данных, основные права субъектов, ответственность за их нарушение, формируют отраслевые стандарты и нормативы.

Использование организационных мер особенно важно для защиты информационных систем электронного государства: они включают в себя, среди прочего, разграничение доступа (принцип, согласно которому доступ к данным предоставляется только тем сотрудникам, которым он необходим для выполнения обязанностей, с учетом принципа минимальной достаточности), регламентирование процессов обработки данных, назначение ответственных за обработку персональных данных лиц, внедрение процедур внутреннего контроля и аудита.

Технические меры направлены на использование, собственно, технологий и инфраструктуры для обеспечения безопасности данных. Наиболее подробным образом меры защиты массивов данных были описаны в европейском Мнении 05/2014 по техникам анонимизации Рабочей группы статьи 29 (Opinion 05/2014 on Anonymization Techniques, Article 29 Data Protection Working Party), принятом еще до вступления в силу европейского Регламента по защите данных (General Data Protection Regulation, далее — GDPR). В этом документе выделяются: добавление шума (случайных числовых значений в данные, чтобы исказить точные значения и скрыть детали); генерализация (снижение точности данных путем объединения их в более крупные категории); псевдонимизация и маскирование (использование псевдонимов или иных переменных, заменяющих реальные значения, которые «открываются» с использованием ключа расшифровки); квантование (округление); перемешивание (изменение порядка записей в системе, изменение связей между субъектами и данными)[28].

Ярким примером интеграции юридических и технологических решений является организация защиты российских веб-ресурсов от несанкционированного использования с применением государственной системы идентификации личности. Поскольку государственные информационные системы содержат множество чувствительной информации, позволяют совершать юридически значимые действия онлайн, то к ним предъявляются особые требования. Так, например, Постановлением Правительства РФ от 19.10.2023 № 1739 установлено, что доступ к ЕСИА осуществляется только при условии использования усиленной квалифицированной электронной подписи либо прохождения двухфакторной идентификации с помощью логина и пароля (простая электронная подпись) совместно с идентификацией в ЕБС, вводом одноразового кода подтверждения, получаемого на другом авторизованном устройстве или по СМС[29]. Помимо этого, используется функция так называемого «тайм-аута» — прекращение сессии пользователя по прошествии определенного времени. Обязательность прохождения двухфакторной идентификации (и ее повторное прохождение в случае длительного отсутствия) серьезным образом нивелирует риски при использовании простой электронной подписи — логина и пароля, которые пользователь может использовать и на других порталах, с менее чувствительной информацией. В таких условиях злоумышленникам сложнее получить доступ к аккаунту пользователя: одних только логина и пароля будет недостаточно.

Сведения, содержащиеся в государственных информационных системах, могут быть неактуальными, но при этом влиять на права и обязанности населения. Российский Федеральный закон «О персо-

---

[27] Федеральный закон «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» от 29.12.2022 № 572-ФЗ // СЗ РФ. 2023. № 1. Ст. 19.

[28] Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (дата обращения: 15.11.2024).

[29] Постановление Правительства РФ от 19.10.2023 № 1739 «О внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2023. № 43. Ст. 7738.

нальных данных» (ст. 14) и GDPR (ст. 16) устанавливают право субъекта на уточнение персональных данных, которые являются неверными, неполными или неактуальными. Однако российское право и право стран Европейского союза не содержат норм о приоритете сведений, предоставленных самим субъектом при обращении за получением государственной услуги. Презюмируется, что корректными являются те сведения, что содержатся в государственных и муниципальных информационных системах. При их неактуальности требуется уточнить сначала их, а лишь затем обращаться за получением иных услуг, связанных с такими данными.

При этом в российской судебной практике можно обнаружить сразу несколько сходных дел, где истцы (граждане) выступали против органов власти с требованием исключить из базы данных МВД России сведения об их уголовном или административно-правовом преследовании, которое было прекращено по решению уполномоченных должностных лиц. Такие лица ссылались на необходимость предоставить при устройстве на работу справки об отсутствии судимости и уголовного преследования, однако такие сведения в базах сохранялись. Суды кассационной инстанции отказывают в требовании удалить или изменить (актуализировать) такие сведения, поскольку ведомственные и межведомственные положения органов власти не предусматривают такого основания для уничтожения данных, как прекращение уголовного и административно-правового преследования по нереабилитирующим основаниям[30]. Таким образом, в любом случае действует презумпция корректности данных, указанных в государственных и муниципальных информационных системах.

В рамках Евразийского экономического союза (далее также — ЕАЭС) тоже важно создание общего информационного пространства, обмен персональными данными населения между органами власти государств-членов, развитие инфраструктуры оказания государственных услуг на региональном уровне. Решениями Высшего Евразийского экономического совета обозначены направления и основные сферы цифровой трансформации государств-членов ЕАЭС[31]. В частности, предполагается сопряжение национальных информационных систем государств-членов (создание общей цифровой инфраструктуры и цифровых платформ), развитие их интероперабельности (технологической открытости), укрепление «аналоговых» основ цифровой трансформации[32].

Можно предположить, что указанные направления развития ЕАЭС подвергают обработку персональных данных в рамках электронных государств дополнительным существенным рискам. Евразийский экономический союз действует на основании договоров между государствами-участниками, которые входят в национальные правовые системы стран. Соответственно, обработка персональных данных основана на необходимости для достижения целей, предусмотренных международным договором Российской Федерации или законом. Кроме того, обработка по этому основанию освобождена от требования о «приземлении» обработки персональных данных граждан РФ в базах данных, находящихся на территории России (ч. 5 ст. 18 Федерального закона «О персональных данных»).

Страны-участницы ЕАЭС предъявляют различные требования к обработке персональных данных. Национальные законы в этой сфере наделяют субъектов различными правами, а органы власти — разными обязанностями. Это создает риски при обработке персональных данных, ведь подавляющая часть населения даже не в состоянии оценить условия обработки данных в другой стране в рамках цифровой интеграции и оказания «межрегиональных» услуг. Конечно, повышается и риск инцидентов с данными.

---

[30] См., напр.: Кассационное определение Четвертого кассационного суда общей юрисдикции от 01.08.2024 № 88а-19209/2024 по делу № 2а-1486/2023. Доступ из СПС «Консультант Плюс» (дата обращения: 12.02.2025); Кассационное определение Восьмого кассационного суда общей юрисдикции от 23.10.2024 № 88А-21560/2024 по делу № 2а-2311/2024. Доступ из СПС «Консультант Плюс» (дата обращения: 12.02.2025); Кассационное определение Первого кассационного суда общей юрисдикции от 26.11.2024 № 88а-37666/2024 по делу № 2а-1032/2024. Доступ из СПС «Консультант Плюс» (дата обращения: 12.02.2025).

[31] См.: Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». URL: https://www.garant.ru/products/ipo/prime/doc/71708158/ (дата обращения: 16.11.2024); Общие подходы к формированию цифрового пространства Евразийского экономического союза в перспективе до 2030 года. Цифровая повестка ЕАЭС. URL: https://eec.eaeunion.org/comission/department/inftech/kk_wg/workgroup/materials/docs.php (дата обращения: 16.11.2024).

[32] Цифровая повестка ЕАЭС 2025: перспективы и рекомендации. Обзор совместного исследования Всемирного банка и Евразийской экономической комиссии. URL: https://eec.eaeunion.org/upload/medialibrary/833/Vsemirnyy-bank-Perspektivy-i-Rekomendatsii.pdf (дата обращения: 16.11.2024).

В свою очередь, обработка персональных данных на межрегиональном уровне уже несколько десятков лет успешно работает на территории Европейского союза: общие условия об обработке данных содержатся в директивах и регламентах этого объединения государств. Полагаем, что прежде чем создавать общую цифровую платформу обработки данных о населении в масштабе ЕАЭС, требуется принять международный договор об унификации правил такой деятельности, гармонизировать национальное законодательство в этой сфере. Помимо этого, не последнюю роль в гармонизации правил обработки персональных данных на территории Европейского союза играют специальные консультативные органы содружества — European Data Protection Board (Европейский совет по защите данных), а до принятия GDPR — Article 29 Data Protection Working Party (Рабочая группа по статье 29).

Схожего органа не существует в ЕАЭС. Его создание позволило бы унифицировать правила обработки персональных данных лиц, находящихся в странах содружества, определить правила обмена данными между органами государственной власти стран союза, в частности, таможенными, правоохранительными, налоговыми. В компетенцию такого органа могла бы входить разработка единых стандартов обработки персональных данных; обеспечение их соблюдения не только странами-участницами, но и физическими и юридическими лицами; рассмотрение жалоб и разрешение споров в сфере защиты данных; предоставление консультаций органам власти, а также частным и юридическим лицам по вопросам защиты информации, регулирования обработки данных и разработки политик конфиденциальности; участие представителей органа в качестве экспертов в судебных разбирательствах стран ЕАЭС, а также в структурах законодательной и исполнительной власти.

Выводы

Цифровизация публичных услуг улучшает их прозрачность, но требует адаптации законодательства в сфере персональных данных. Комплексный подход к защите персональных данных и их обработке должен учитывать не только национальные, но и международные стандарты, способствуя формированию доверия граждан к электронным системам. Гармонизация законодательства в странах ЕАЭС и внедрение передовых технологий безопасности представляют собой перспективное направление дальнейших исследований и практической реализации.

Современные информационно-коммуникационные технологии открывают широкие перспективы для улучшения уровня оказываемых государственных услуг в рамках цифрового государства. Персональные данные как вид конфиденциальной информации обладают некоторыми особенностями: их обработка возможна (в некоторых случаях, и особенно часто — в электронном государстве) без желания субъекта.

Электронное государство в процессе своего становления проходит несколько этапов, но главным из них является тот, при котором формируется множество связанных друг с другом информационных систем. Чем более открытым становится государство, тем больше рисков информационной безопасности несет обработка данных в таких условиях. При этом ее обеспечение осуществляется с использованием правовых, организационных и технических мер, а также их совокупности. Помимо этого, следует уделять особое внимание актуальности сведений о населении.

Стремление создать «электронное межгосударственное объединение» (по аналогии с «электронным государством») прослеживается также и в ЕАЭС. Представляется, что прежде чем создавать общую цифровую платформу обработки данных, требуется принять международный договор об унификации правил такой деятельности и гармонизировать национальное законодательство в этой сфере. Унификация подходов к обработке персональных данных позволит минимизировать риски такой обработки при трансграничном взаимодействии. В частности, возможна разработка единого стандарта защиты данных, принятие актов ЕАЭС наподобие специализированных мнений и разъяснений, которые издаются специальными органами в Европейском союзе.

Анализ современных правовых аспектов обработки персональных данных в процессе становления электронного государства акцентирует внимание на обеспечении соблюдения баланса интересов участ-

ников такого процесса, в особенности в случае такой обработки, которая не требует согласия или иного волеизъявления субъекта.

Список источников

1. *Богдановская И. Ю.* Понятие «электронного государства»: правовые аспекты // В сб. «Информационное общество и социальное государство». М.: Юрист. 2011. С. 45–55.
2. *Данилов Н. А.* Правовое регулирование электронного правительства в зарубежных странах: дис. … канд. юрид. наук. М.: НИУ ВШЭ, 2013. 158 с. EDN: SUVYPB
3. *Исаков В. Б.* Юридические факты в советском праве. М.: Юридическая литература, 1984. 124 с. EDN: YMWNKN
4. *Камалова Г. Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. … канд. юрид. наук. М.: ИГП РАН, 2020. 472 с. EDN: IHXJJF
5. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд. М.: Статут, 2021. 468 с.
6. *Терещенко Л. К.* Правовой режим информации: дис. … д-ра юрид. наук. М.: ИЗиСП, 2011. 415 с.
7. *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … канд. юрид. наук. М.: Российская правовая академия Министерства Юстиции РФ, 2008. 438 с.
8. Beldad A., Geest T. van der, Jong M. de, Steehouder M. (2012) A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly*, vol. 29, no. 1, pp. 41–49. DOI: https://doi.org/10.1016/j.giq.2011.05.003
9. Beldad A., Jong M. de, Steehouder M. (2011) I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, vol. 27, no. 6, pp. 2233–2242. https://doi.org/10.1016/j.chb.2011.07.002
10. Froomkin M. A. (2009) Government Data Breaches. *Berkeley Technology Law Journal*. Vol. 24, no. 3, pp. 1019–1059. URL: https://www.jstor.org/stable/24118272
11. Tolbert C. J., Mossberger K. (2006) The Effects of E-Government on Trust and Confidence in Government. *Public Administration Review*, vol. 6, no. 3, pp. 354–369. URL: https://www.jstor.org/stable/3843917
12. Pasquale F. (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. *Harvard University Press*. 304 p.

Об авторе:

Демкин Владислав Олегович, аспирант Аспирантской школы по праву, Национальный исследовательский университет «Высшая школа экономики», Москва, Российская Федерация; ORCID: 0000-0002-1079-425X, e-mail: vodemkin@hse.ru

References

1. Bogdanovskaya, I. Yu. (2011) The concept of 'e-State': legal aspects. In: Informatsionnoe obshchestvo i sotsial'noe gosudarstvo. *Lawyer*, pp. 45–56. (In Russ.)
2. Danilov, N. A. (2013) Legal regulation of e-government in foreign countries: Candidate of Legal Sciences dissertation. *HSE University*, 158 p. (In Russ.)
3. Isakov, V. B. (1984) Legal facts in Soviet law. *Legal literature Publ*. 124 p. (In Russ.)
4. Kamalova, G. G. (2020) Legal Support for Information Confidentiality in the Context of Information Society Development: Candidate of Legal Sciences dissertation. *Institute of State and Law of the Russian Academy of Sciences*, 472 p. (In Russ.)

5. Savelyev, A. I. (2021) Scientific-practical article-by-article commentary to the Federal Law “On Personal Data”. 2-nd ed. *Statut*, 468 p. (In Russ.)
6. Tereshchenko, L. K. (2011) Legal regime of information: Doctor of Legal Sciences dissertation. *Institute of Legislation and Comparative Law*, 415 p. (In Russ.)
7. Polyakova, T. A. (2008) Legal support of information security in building an information society in Russia: Candidate of Legal Sciences dissertation. *Russian Legal Academy of the Ministry of Justice of the Russian Federation*, 438 p. (In Russ.)
8. Beldad, A., Geest, T. van der, Jong, M. de, Steehouder, M. (2012) A cue or two and I’ll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens’ personal information disclosed online. *Government Information Quarterly*, vol. 29, no. 1, pp. 41–49. DOI: https://doi.org/10.1016/j.giq.2011.05.003
9. Beldad, A., Jong, M. de, Steehouder, M. (2011) I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, vol. 27, no. 6, pp. 2233–2242. https://doi.org/10.1016/j.chb.2011.07.002
10. Froomkin, M. A. (2009) Government Data Breaches. *Berkeley Technology Law Journal*, vol. 24, no. 3, pp. 1019–1059. URL: https://www.jstor.org/stable/24118272
11. Tolbert, C. J., Mossberger, K. (2006) The Effects of E-Government on Trust and Confidence in Government. *Public Administration Review*, vol. 6, no. 3, pp. 354–369. URL: https://www.jstor.org/stable/3843917
12. Pasquale, F. (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. *Harvard University Press*. 304 p.

About the author:

Vladislav O. Demkin, postgraduate student of the Postgraduate School of Law, National Research University Higher School of Economics (HSE University), Moscow, Russian Federation; ORCID: 0000-0002-1079-425X, e-mail: vodemkin@hse.ru

Автор заявляет об отсутствии конфликта интересов.
The author declares that there is no conflict of interest.