Научная статья
УДК 34.09
DOI: 10.18384/2949-513X-2026-2-65-75

ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: ИНФОРМАЦИОННО-ПРАВОВОЙ АСПЕКТ

Сапронов Д. Ю.
Московский государственный университет имени М. В. Ломоносова, г. Москва, Российская Федерация
e-mail: braingeek@mail.ru

Поступила в редакцию 13.04.2026
После доработки 26.04.2026
Принята к публикации 04.05.2026

Аннотация

Цель. Выявить тенденции и особенности, которые стали причиной серьёзной трансформации общественных отношений и появления новых вызовов в области информационной безопасности, и определить, какое воздействие это оказывает на сферу национальной безопасности и информационной безопасности государства.

Процедуры и методы. Использованы методыдз анализа и синтеза, системного анализа и др. В работе рассмотрен вопрос влияния цифровой обработки персональных данных на безопасность личности и государства, что особенно актуально в связи с обострением геополитической обстановки и ростом числа атак на информационную инфраструктуру нашей страны, в том числе и на информационные системы, которые обрабатывают персональные данные. Кроме этого, жертвы мошеннических действий под принуждением злоумышленников могут совершать различные противоправные действия, которые направлены в т. ч.и на государственные органы. Это требует совершенствования подходов государства к защите персональных данных физических лиц.

Результаты. Доказан вывод о том, что цифровизация обработки данных о физических лицах в значительной степени повлияла на общественные отношения и стала затрагивать не только права личности, но и национальную безопасность.

Теоретическая и/или практическая значимость. Актуализирована проблематика, связанная с необходимостью защиты интересов и безопасности государства в области охраны персональных данных, которая выходит на первый план по причине того, что постоянные утечки информации о физических лицах не только создают напряжение в обществе, отрицательно сказываясь на защищённости прав человека, но и оказывают отрицательное влияние на национальную безопасность. Обоснована необходимость актуализации документов стратегического планирования в области национальной и информационной безопасности с учётом появления новых угроз и вызовов.

Ключевые слова: персональные данные, защита личной жизни, защита персональных данных, информационное право, информационная безопасность, национальная безопасность, безопасность государства, совершенствование законодательства, цифровые сервисы, цифровой след, цифровое право, права человека

Для цитирования:
Сапронов Д. Ю. Правовая защита персональных данных и обеспечение национальной безопасности Российской Федерации: информационно-правовой аспект // Московский юридический журнал. 2026. № 2. С. 65–75. https://doi.org/10.18384/2949-513X-2026-2-65-75.

Original research article

LEGAL PROTECTION OF PERSONAL DATA AND ENSURING NATIONAL SECURITY OF THE RUSSIAN FEDERATION: INFORMATION AND LEGAL ASPECT

D. Sapronov
Lomonosov Moscow State University, Moscow, Russian Federation
e-mail: braingeek@mail.ru

Received by the editorial office 13.04.2026
Revised by the author 26.04.2026
Accepted for publication 04.05.2026

Abstract
Aim. To identify the trends and features that have caused a serious transformation of public relations and the emergence of new challenges in the field of information security, and what impact these changes have on the field of facial security.
Methodology. Various methods were used in the article. such as analysis and synthesis, system analysis and others. The paper considers the impact of digital processing of personal data on the security of individuals and the state, which is especially important due to the aggravation of the geopolitical situation and the increasing number of attacks on the information infrastructure of our country, including information systems that process personal data. In addition, victims of fraudulent actions under the coercion of intruders can commit various illegal actions, including those directed at government agencies. All this, in turn, requires improvement of the state's approaches to the protection of personal data of individuals.
Results. The conclusion is proved that the digitalization of data processing about individuals has significantly affected public relations and has begun to affect not only individual rights, but also national security.
Research implications lies in the fact that the problems related to the need to protect the interests and security of the state in the field of personal data protection have been actualized, which comes to the fore due to the fact that constant leaks of information about individuals not only create tension in society and negatively affect the business climate, but also affect the level of protection of human rights and national security. The necessity of tightening the legislation that regulates relations in the field of personal data protection is justified.
Keywords*:* personal data, protection of personal life, protection of personal data, information law, information security, national security, state security, improvement of legislation, digital services, digital footprint, digital law, human rights

For citation:
Sapronov, D. Yu. (2026). Legal Protection of Personal Data and Ensuring National Security of the Russian Federation: Information and Legal Aspect. In*: Moscow Juridical Journal*, 2, 66–76. https://doi.org/10.18384/2949-513X-2026-2-66-76.

Введение

Анализ генезиса понятия «национальная безопасность» в юридической науке требует первоочерёдного обращения к концепции общественного договора Т. Гоббса, сформировавшейся в эпоху Нового времени. Одной из ключевых причин заключения общественного договора выступает необходимость обеспечения безопасности государства: «Государство есть единое лицо, ответственным за действия которого сделало себя путём взаимного договора между собой и огромным множеством людей с тем, чтобы это лицо могло использовать силу и средства всех их так, как сочтёт необходимым для мира и общей защиты»

[1, с. 260]. Сама суть концепции Гоббса заключается в обеспечении безопасности индивидуумов, осуществивших заключение общественного договора.

В дальнейшем с развитием права идеи концепции общественного договора стали тем фундаментом, на котором базируется конституционализм. Становление государства и принятие Конституции – писанного акта, который принимается всеобщим голосованием и является воплощением идеи Т. Гоббса об общественном договоре. Конституция закрепляет среди приоритетов и безопасность личности, общества и государства[1]. Именно они стали ключевыми для большинства Конституций развитых стран. Государство силой своего принуждения обеспечивает состояние защищённости интересов личности, государства и общества, а также баланс между ними.

Исторически понятие «национальная безопасность» берёт своё начало в 1904 г. с его фиксации в послании президента США Т. Рузвельта Конгрессу. В дальнейшем произошла институционализация термина, в рамках которой его содержание оформилось как системное обеспечение безопасности 3 взаимосвязанных уровней: граждан, общества и государства: «"традиционная концепция национальной безопасности фокусируется на выживании государства": аспекты физической безопасности государства от внешних угроз (преимущественно военного реагирования), включают национальную оборону, национальную целостность и национальный суверенитет» [2, с. 15].

Правовое обеспечение национальной безопасности в Российской Федерации

В российской правовой системе понятие «национальная безопасность» получило нормативное закрепление в середине 1990-х гг. – спустя чуть более четверти века после распада советской системы. Его появление ознаменовало смену концептуальной парадигмы: на смену доминировавшему в советской правовой науке и законодательстве термину «государственная безопасность» пришла более комплексная категория, отражающая новые политико-правовые реалии. Впервые это понятия было закреплено в Федеральном законе № 24-ФЗ «Об информации, информатизации и защите информации»[2], в дальнейшем понятию «национальная безопасность» было дано следующее определение: «это состояние защищённости национальных интересов от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства»[3].

С течением времени отечественная теория национальной безопасности развивалась и совершенствовалась, с момента появления в правовом поле этого понятия были приняты следующие нормативные акты: Закон РФ № 2446-1[4], позднее на смену которому был принят Федеральный закон № 390-ФЗ «О безопасности»[5]. Кроме этого, принимались различные стратегические документы: первым таким актом стала «Концепция национальной безопасности Российской Федерации»[6], принятая в 1997 г., затем её заменила «Стратегия национальной безопасности Российской Федерации до 2020»[7], которой позднее пришла на смену «Стратегия национальной безопасности Российской

[1] Ст. 79.1 Конституция Российской Федерации (1993). Новая редакция: с комментариями Конституционного суда РФ. М.: Проспект, 2022. 116 с.

[2] Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» // Российская газета. 1995. № 39.

[3] Послание Президента Российской Федерации Федеральному Собранию «О национальной безопасности» от 13 июля 1996 г. // Российская газета. 1996. № 17.

[4] Закон РФ от 05.03.1992 № 2446-1 // Ведомости СНД и ВС РФ. 1992. № 15. Ст. 769.

[5] Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // Парламентская газета. 2011. № 1-2.

[6] Указ Президента РФ от 17.12.1997 № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» // Российские вести. 1997. № 239.

[7] Указ Президента РФ от 12.05.2009 № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года" // Собрание законодательства РФ. 2009. № 20. Ст. 2444.

Федерации»[1] принятая в 2015 г., к 2021 г. ситуация в мире и вокруг нашей страны вновь потребовала коренных изменений в доктринальных источниках, связанных с национальной безопасностью, что потребовало принятия новой «Стратегии национальной безопасности Российской Федерации»[2].

Постоянное совершенствование стратегических документов в области национальной безопасности обусловлено динамикой внешних и внутренних вызовов, изменением сущности и масштабов угроз.

Своевременная реакция государственных органов и нормативно-правовое закрепление новых приоритетов становятся необходимыми условиями эффективного противодействия рискам. Эволюция доктринальных источников в этой сфере свидетельствует о формировании целостной системы взглядов государства на ключевые аспекты обеспечения национальной безопасности: понятийный аппарат, типологию угроз, стратегические приоритеты и механизмы защиты национальных интересов.

Взаимосвязь информационной сферы и национальной безопасности

Обеспечение национальной безопасности в существенной степени зависит от эффективной защиты государственных интересов в информационной сфере, что обусловлено возрастающей ролью информации и цифровых технологий в современном мире. Отечественные специалисты по информационной безопасности отмечают, что «Информация – это та субстанция, которая сопровождает нас всю жизнь. Информация позволяет человеку познавать мир и ощущать себя его частью, общаться с другими людьми, воспитывать детей, решать бытовые проблемы, заниматься хозяйственной деятельностью, творческим трудом… Информационная сфера в настоящее время стала системообразующим фактором жизни общества, и чем активней эта сфера общественных отношений развивается, тем больше политическая, экономическая, оборонная и другие составляющие национальной безопасности любого государства будут зависеть от информационной безопасности, и в ходе развития технического прогресса эта зависимость будет всё более возрастать» [3, с. 5].

Отечественная «Доктрина информационной безопасности» впервые была принята в декабре 2000 г.[3], этот документ закреплял правовое определение понятия «информационная безопасность»: «Под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[4]. Среди национальных интересов Российской Федерации Доктрина особо подчёркивала необходимость соблюдения конституционных прав и свобод граждан в области доступа к информации как значимого элемента государственной политики в информационной сфере.

Дополнительно следует отметить, что угроза соблюдению конституционных прав и свобод человека и гражданина нормативно выделена в качестве первоочерёдной и занимает лидирующую позицию в перечне угроз. В результате в российском правовом поле впервые на доктринальном уровне оформилась концептуальная взаимосвязь между обеспечением информационной безопасности государства и защитой конституционных прав личности, что акцентировало значимость их охраны в информационной сфере. Кроме этого, в документе говорилось: «закреплённые в Конституции Российской Федерации права граждан на неприкосновенность част-

[1] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2019. № 1 (ч. II). Ст. 212.

[2] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»// Собрание законодательства РФ. 2021. № 27 (ч. II). Ст. 5351.

[3] Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. № 187.

[4] Там же. Ст. 8.

ной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения»[1]. В связи с этим возникла необходимость совершенствования правовых механизмов защиты конституционных прав, в т. ч. механизмов правовой защиты персональных данных. Позднее был принят федеральный закон, регулирующий данную сферу.

Доктрина заложила стратегическую основу для интеграции сферы информационной безопасности в систему национальной безопасности государства. Впервые на официальном уровне эти направления были юридически связаны в рамках единой непротиворечивой иерархической структуры, что позволило выстроить последовательную политику обеспечения безопасности с учётом современных вызовов и угроз: «Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищённость национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы её обеспечения являются общими для этих сфер»[2].

В документе был отмечен факт недостаточной защищённости персональных данных граждан: «неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных)»[3]. Таким образом, документ не только оговаривал актуальные на тот момент угрозы и вызовы для информационной безопасности, но и предугадал будущие изменения, обусловленные стремительным развитием информационно-коммуникационных технологий.

Эволюция угроз в сфере информационной безопасности в течение 16-летнего периода привела к тому, что к 2016 г. возникла объективная потребность в обновлении концептуальных подходов государства к данной проблематике. В целях отражения новых вызовов и рисков была утверждена новая «Доктрина информационной безопасности Российской Федерации»[4], которая и действует по настоящее время. Документ выстраивает целостную систему правовых дефиниций в сфере информационной безопасности, закрепляя толкование взаимосвязанных понятий. К ним относятся: «национальные интересы Российской Федерации в информационной сфере», «угроза информационной безопасности Российской Федерации», «обеспечение информационной безопасности», «система обеспечения информационной безопасности». Также нормативно фиксируется содержание собственно базового понятия, обеспечивающего единство терминологического аппарата: «информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[5], в рамках доктринального подхода были институционализированы и нормативно закреплены основополагающие правовые понятия, составляющие понятийный аппарат сферы информационной безопасности. И на понятийном уровне закреплён приоритет защиты конституционных прав граждан

[1] Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. № 187. Ст. 4.

[2] Там же. Ст. 6.

[3] Там же. Ст. 4.

[4] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[5] Там же. Ст. 2.

как составного элемента информационной безопасности государства.

Кроме этого, рассматриваемый документ закрепляет глобальность и неотъемлемость информационных технологий как части всех сфер деятельности, относящихся к личности обществу и государству.

В перечне национальных интересов РФ в информационной сфере приоритетное место отведено защите конституционных прав и свобод граждан в части доступа к информации и её использования, обеспечению неприкосновенности частной жизни в условиях развития и становления информационного общества, а также информационной поддержке демократических институтов[1], Данный факт ещё раз демонстрирует значимость защиты прав и свобод личности в информационной сфере как неотъемлемого элемента национальной безопасности. Одновременно подчёркивается необходимость обеспечения устойчивой работы и развития информационной инфраструктуры, стимулирования отечественной отрасли информационных технологий, а также участия в построении системы международной информационной безопасности.

Среди угроз информационной безопасности в документа выделен ряд ключевых факторов: применение новых технологий в государственном управлении, которое, хотя и способствует развитию соответствующих институтов, одновременно порождает новые риски и вызовы; наращивание зарубежными странами возможностей по информационному воздействию на информационно-техническую инфраструктуру оппонентов и их стремление использовать достижения в области развития информационно-коммуникационных технологий для доминирования в информационном пространстве; использование современных информационных технологий террористическими и преступными организациями; увеличение числа скоординированных атак на объекты критической инфраструктуры нашей страны. Кроме того, в документе акцентируется внимание на низкой конкурентоспособности отечественных информационных технологий и электроники, а также на зависимости от зарубежной вычислительной техники и информационных технологий.

В качестве ещё одного элемента пространства угроз Доктрина определяет низкую осведомлённость граждан в вопросах, связанных с информационной безопасностью.

Рассматриваемый стратегический документ фиксирует угрозы конституционным правам граждан и подчёркивает опасность использования информационных технологий для несанкционированного доступа к персональным данным физических лиц.

Последующие годы продемонстрировали резкий рост числа преступлений в данной области, причём многие из них связаны с хищением финансовых средств у граждан с применением их персональных данных. Подобная угроза информационной безопасности приобрела значительные масштабы и представляет опасность не только для личной безопасности граждан, но и для национальной безопасности в целом. Более того, незаконно полученные финансовые ресурсы нередко используются для финансирования экстремистской и террористической деятельности, что усугубляет негативные последствия таких преступлений: «Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в т. ч. в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся всё изощрённее»[2]. В доктрине

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 8.

[2] Ст.17, Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074

была успешно спрогнозирована тенденция к усложнению и повышению убедительности преступлений, совершаемых с применением информационных технологий. В первую очередь, это относится к мошенническим схемам, нацеленным на изъятие финансовых средств у граждан.

Таким образом, с течением времени взгляды государства на вызовы и угрозы в информационной сфере, стали видоизменяться и расширяться. В частности, действующая Доктрина информационной безопасности систематизирует и конкретизирует перечень угроз конституционным правам и свободам граждан, при этом акцентируя внимание на важности обеспечения надёжной защиты персональных данных как одного из ключевых элементов информационной безопасности. Помимо прочего, в структуре обеспечения информационной безопасности особое место занимает защита интересов личности – этот аспект выделен как одно из основополагающих направлений, которое определяет «обеспечение защищённости граждан от информационных угроз, в т. ч. за счёт формирования культуры личной информационной безопасности»[1], сложившаяся ситуация ставит перед государством комплексную задачу по созданию эффективной системы информирования населения.

Такая система призвана решать 2 взаимосвязанные задачи:

– доносить до граждан актуальные способы защиты их персональных данных;

– формировать у населения навыки безопасного поведения и цифровой грамотности в условиях динамичного становления информационного общества.

Важным аспектом является то, что Доктрина определяет данное направление как стратегически значимое – в числе основных приоритетов обеспечения информационной безопасности «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям»[2], такой подход устанавливает принцип выстраивания системы информационной безопасности, которая была бы ориентирована на предотвращение инцидентов, связанных с возникновением различных инцидентов безопасности. Благодаря этому становится возможным выстроить систему правовой защиты персональных данных, формирующую у операторов стимулы к целенаправленным инвестициям в обеспечение безопасности информации и профилактику утечек. Ст. 30 Доктрины закрепляет принцип иерархичности в вопросе соотношения понятий «система информационной безопасности» и «система национальной безопасности»: «Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации»[3], данный факт ещё раз демонстрирует причинно-следственную связь: эффективная защита национальных интересов в информационной сфере выступает неотъемлемым элементом обеспечения национальной безопасности государства.

Защита персональных данных как один из элементов информационной безопасности государства

С системной точки зрения технологический прогресс выступает одновременно и драйвером экономического развития, и фактором трансформации рисков в информационной сфере. Автоматизация процессов и внедрение механизмов удалённого совершения юридически значимых действий, стимулируя рост экономики и оптимизируя народное хозяйство, одновременно расширяют поверхность атак для киберпреступников. Следствием этого становится повышенный интерес злоумышленников к получению доступа к персональным данным физических лиц как ключевому ресурсу для реализации противоправных схем.

[1] Ст.17, Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 25.

[2] Там же. Ст. 7074

[3] Там же. Ст. 30.

Как зафиксировано в рассмотренных стратегических документах, информационно-коммуникационные технологии прочно интегрировались в различные сферы общественной жизни. Данный процесс выступил ключевым фактором становления информационного общества и развития цифровой экономики, одновременно спровоцировав трансформацию общественных отношений, в т. ч. в информационной сфере, где изменились модели взаимодействия субъектов, механизмы обмена данными и способы доступа к информации.

Развитие правового регулирования в этой сфере в нашей стране было непростым: оно началось с разрозненных правовых норм, которые не были связаны общей концепцией или структурой, и постепенно шло к формированию целостной системы, «до принятия базового Федерального закона «Об информации, информационных технологиях и о защите информации» и разработки концепции Информационного кодекса и Цифрового кодекса, а так же принятия "Доктрины информационной безопасности Российской Федерации"» [4, с. 59]. С системной точки зрения внедрение автоматизированных информационных систем в процессы обработки персональных данных инициировало трансформацию соответствующих общественных отношений. Переход от ручных методов к цифровым технологиям изменил масштаб и характер рисков: регулирование оборота данных перестало быть узкоотраслевой задачей и стало элементом системы национальной безопасности. В Доктрине данный аспект закреплён как один из приоритетов, подчёркивая взаимосвязь между защитой персональных данных и обеспечением суверенитета государства. В. А. Вайпан в своих работах подчёркивает важность регламентации защиты персональных данных: «Для права особое значение имеют регулирование сбора и оборота больших данных, формирование и обработка обезличенных данных, защита персональных данных и т. п.» [5, с. 12].

Автоматизация процессов обработки персональных данных обусловила существенные изменения в характере общественных отношений, складывающихся в этой сфере [6, с. 29]. Развитие технологий привело к тому, что удалённый и практически мгновенный доступ к данным о физических лицах стал ключевой особенностью их оборота. С одной стороны, это открыло новые возможности: множество услуг и сервисов теперь доступны из любой точки мира. С другой – упростило злоумышленникам доступ к персональным данным, из-за чего количество случаев их несанкционированного получения заметно возросло.

Т. А. Полякова отмечает следующее: «Сегодня процесс формирования цифровой среды создаёт запрос на развитие системы организационных и правовых механизмов взаимодействия субъектов информационного и цифрового обмена, оборота цифровых данных в различных сферах нашей жизни» [7, с. 32]. В условиях активной цифровизации общественных отношений перед профессиональным юридическим сообществом встаёт принципиально важная задача – обеспечить адаптацию действующего законодательства к современным вызовам, связанным с развитием информационных технологий и изменением форматов взаимодействия субъектов права.

Повсеместная цифровизация актуализировала необходимость пересмотра существующих подходов к обеспечению информационной безопасности. Ключевым фактором, обуславливающим эту потребность, выступает устойчивый рост количества инцидентов, связанных с утечками персональных данных, что свидетельствует о недостаточности традиционных методов защиты в современных условиях[1]. Центральный банк отмечает тревожную динамику утечек персональных данных

[1] В Сбербанке крупнейшая утечка в истории российского банковского сектора // CNEWS: [сайт]. URL: https://www.cnews.ru/news/top/2019-10-03_sberbank_dopustil_krupnejshuyu (дата обращения: 15.10.2024).

в России. В I полугодии 2023 г. количество таких инцидентов достигло 76 — это в 4 раза больше, чем за первые 6 месяцев 2022 г. (19 утечек)[1].

Трансформация геополитической обстановки инициировала рост числа кибератак на государственные организации. Ключевой целью злоумышленников выступает получение доступа к персональным данным, что обусловлено их высокой ценностью в современных условиях[2], включая передачу сведений разведывательным организациям стран, отношения с которыми характеризуются как недружественные.

Процесс цифровизации хранения и обработки персональных данных, наряду с позитивными трансформациями во всех сферах общественной жизни, обусловил появление новых вызовов и угроз для национальной безопасности государства. Данный тезис находит отражение в научных работах российских исследователей, в частности А. В. Морозова: «В центре внимания всех мероприятий по обеспечению ИБ, прежде всего, должна находиться информационная среда системы органов государственной власти. Это объясняется тем, что их деятельность по управлению государством и обществом обеспечивает создание реальных гарантий свобод и прав человека, защиту интересов граждан страны и их социально значимых ассоциаций» [8, с. 25]. Персональные данные физических лиц, попавшие в руки злоумышленников, могут быть использованы для совершения противоправных действий.

Согласно официальным данным, в 2022 г. объём финансовых хищений у клиентов банков составил 14,1 млрд руб., что является максимальным показателем начиная с 2019 г. При этом годовой прирост объёма хищений составил 4,29%, что коррелирует с активным развитием дистанционных платёжных сервисов и увеличением объёма операций с использованием электронных средств платежа[3].

Использование злоумышленниками украденных персональных данных для совершения противоправных действий имеет многоуровневые последствия. Во-первых, это непосредственно угрожает безопасности физических лиц. Во-вторых, провоцирует социальную напряжённость в обществе, что негативно отражается на имидже государства и уровне защищённости его интересов в информационной сфере. В конечном счёте это подрывает национальную безопасность. Кроме того, финансовые средства, полученные в результате мошенничества, могут быть направлены на финансирование террористических и экстремистских группировок, а также использоваться иностранными спецслужбами в их деятельности. В последнее время участились случаи принуждения мошенниками своих жертв к совершению противоправных действий[4], в т. ч. и против государственных органов[5].

Доступ злоумышленников к персональным данным угрожает безопасности государства: они не только наносят финансовый ущерб гражданам, но и с помощью социальной инженерии принуждают жертв к противоправным действиям, вредящим национальной безопасности. Например, участились атаки на логистическую и железнодорожную инфраструктуру[6].

---

1 Роскомнадзор сообщил о росте утечек данных в четыре раза в I полугодии // ТАСС: [сайт]. URL: https://tass.ru/obschestvo/18333157 (дата обращения: 15.10.2024).

2 Хакеры взломали сайт МосгорБТИ // Forbes: [сайт]. URL: https://www.forbes.ru/tekhnologii/494123-hakery-vzlomali-sajt-mosgorbti (дата обращения: 25.10.2024).

3 Россияне сдали мошенникам рекордные ₽14 млрд // РБК: [сайт]. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f (дата обращения: 25.10.2024).

4 Мошенники убедили жительницу Казани перевести им 750 тыс. рублей и устроить пожар в отеле // Московский Комсомолец: [сайт]. URL: https://kazan.mk.ru/incident/2023/11/02/moshenniki-ubedili-zhitelnicu-kazani-perevesti-im-750-tys-rubley-i-ustroit-pozhar-v-otele.html (дата обращения: 27.10.2024).

5 На Урале зафиксировали случаи принуждения жертв мошенников к поджогам военкоматов // ТАСС: [сайт]. URL: https://tass.ru/proisshestviya/17567183 (дата обращения: 27.10.2024).

6 По статье «Диверсия» // Гудок: [сайт]. URL: https://gudok.ru/zdr/173/?ID=1637772 (дата обращения: 27.10.2024).

Заключение

Проведённый анализ свидетельствует о многокомпонентном характере ущерба, наносимого утечками персональных данных. Подобные инциденты не ограничиваются нарушением безопасности отдельных лиц, но также создают риски для национальной безопасности государства. Это демонстрирует неразрывную связь между уровнем защищённости личной информации граждан и устойчивостью информационной инфраструктуры страны. В связи с этим возникает объективная необходимость разработки обновлённых подходов к регулированию оборота персональных данных, в т. ч. закрепления приоритета их защиты в рамках доктринальных документов.

На рассматриваемом уровне регулирования представляется необходимым институционально зафиксировать стратегическую роль персональных данных в системе национальной безопасности, а также подчеркнуть критическую важность их надёжной защиты как элемента обеспечения государственных интересов. «Информация о юридических и физических лицах, в т. ч. персональные данные, в современных условиях являются стратегически важным ресурсом, безопасность которого имеет критическое значение для национальной безопасности», данное положение могло бы быть зафиксировано в разделе «Информационная безопасность» «Стратегии национальной безопасности Российской Федерации», это позволило бы на доктринальном уровне подчеркнуть связь защищённости персональных данных и национальной безопасности, это акцентирует внимание на стратегической важности вопроса защиты персональных данных для безопасности государства.

Кроме этого, в «Доктрину национальной безопасности Российской Федерации», также следует внести ряд дополнений, связанных с защитой персональных данных. Например, в ст. 8, посвящённую национальным интересам в информационной сфере, следующее дополнение: «Обеспечение всесторонней защиты персональных данных физических лиц, особенно при обработке которых используются автоматизированные информационные технологии, кроме этого особое внимание должно быть уделено защите информационных систем в которых производится обработка персональных данных». В п. «ж» ст. 23 Доктрины следует после слов «иной информации ограниченного доступа и распространения» добавить фразу «…а также персональных данных», таким образом пункт целиком приобретёт следующий вид «обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, а также персональных данных, в т. ч. за счёт повышения защищённости соответствующих информационных технологий».

В ст. 25 целесообразно также акцентировать внимание на необходимости снижения числа мошенничеств в информационной сфере. Данные дополнения позволят на доктринальном уровне закрепить необходимость повышенного внимания к защите персональных данных, что будет способствовать повышению безопасности оборота и хранения персональных данных на системном уровне.

Обеспечение защиты персональных данных представляет собой комплексную многокомпонентную задачу, решение которой имеет принципиальное значение для двух взаимосвязанных уровней безопасности: индивидуальной защиты прав и свобод граждан, а также обеспечения национальной безопасности государства в целом.

ЛИТЕРАТУРА

1. Гоббс Т. Левиафан, или материя, форма и власть государства церковного и гражданского. М.: Соцэкгиз, 1991. 503 с.
2. Khan E. M. Comprehensive national security: contemporary discourse // Margalla Papers. 2022. Iss. I. P. 1–17. DOI: 10.54690/margallapapers.26.i.94
3. Шерстюк В. П., Информационная безопасность в системе обеспечения национальной безопас-

ности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. 1999. № 5. С. 3–5
4. Минбалеев А. В., Защита прав субъектов генетической информации в правовом государстве в условиях развития информационного общества // Правовое государство: теория и практика. 2020. № 2. С. 57–68. DOI: 10.33184/pravgos-2020.2.6
5. Вайпан В. А. Цифровое право: истоки, понятие и место в правовой системе // Право и экономика. 2024. № 1. С. 5–27.
6. Тедеев А. А. К вопросу о трансформации системы права в условиях развития информационно-коммуникационных технологий: постановка проблемы // Информационное пространство: обеспечение информационной безопасности и право: сб. науч. трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. М.: ИГП РАН, 2018. С. 25–39.
7. Полякова Т. А., Бойченко И. С., Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации // Правовая политика и правовая жизнь. 2023. № 3. С. 26–34. DOI: 10.24412/1608-8794-2023-3-26-34
8. Малюк А. А., Морозов А. В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 21–36. DOI: 10.26583/bit.2019.4.02

REFERENCES

1. Hobbes, T. (1991). *Leviathan, or Matter, the Form and Power of the State of Church and Civil*. Moscow: Sotsekgiz publ. (in Russ.).
2. Khan, E. M. (2022). Comprehensive National Security: Contemporary Discourse. In: *Margalla Papers,* I, 1–17. DOI: 10.54690/Margallapapers.26.I.94
3. Sherstyuk, V. P. (1999). Information Security in the National Security System of Russia, Federal and Regional Aspects of Information Security. In: *Information Society*, 5, 3–5 (in Russ.).
4. Minbaleev, A. V. (2020). Protection of the Rights of Subjects of Genetic Information in a Legal State in the Context of the Development of an Information Society. In: *Legal State: Theory And Practice*, 2, 57–68. Doi: 10.33184/Pravgos-2020.2.6 (in Russ.).
5. Vaipan, V. A. (2024). Digital Law: Origins, Concept and Place in the Legal System. In: *Law and Economics*, 1, 5–27 (in Russ.).
6. Tedeev, A. A. (2018). On the Transformation of the Legal System in the Context of the Development of Information and Communication Technologies: Posing a Problem. In: Polyakova, T. A., Naumova, V. B. & Minbaleeva, A. V., Eds. *Information Space: Ensuring Information Security And Law*. Moscow: Igp Ras, 25–39 (in Russ.).
7. Polyakova, T. A. & Boychenko, I. S. (2023). Features of Interaction and Legal Support of Information Security in a Single Biometric System in the Russian Federation. In: *Legal Policy and Legal Life*, 3, 26–34. DOI: 10.24412/1608-8794-2023-3-26-34 (in Russ.).
8. Malyuk, A. A. & Morozov, A. V. (2019). The Formation of a Digital Economy and the Problems of Improving Regulatory Regulation in the Field of Information Security. In: *Information Technology Security*, 26 (4), 21–36. DOI: 10.26583/Bit.2019.4.02 (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Сапронов Дмитрий Юрьевич (г. Москва) – научный сотрудник Центра стратегических исследований Института математических исследований сложных систем (ЦСИ ИМИСС) Московского государственного университета имени М. В. Ломоносова, ведущий инженер отдела МТО Высшей школы государственного аудита МГУ,
ORCID:0000-0002-4465-1978; e-mail: braingeek@mail.ru

INFORMATION ABOUT THE AUTHOR

Dmitry Yu. Sapronov (Moscow) – Scientific Researcher, Center for Strategic Studies, Institute for Mathematical Research of Complex Systems; Senior Engineer, Tech Department, Higher School of State Audit, Lomonosov Moscow State University;
ORCID:0000-0002-4465-1978; e-mail: braingeek@mail.ru