

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРАВ ГРАЖДАН В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСЛЕ КОНСТИТУЦИОННО-ПРАВОВОЙ РЕФОРМЫ 2020 ГОДА

MECHANISMS FOR ENSURING THE PROTECTION OF CITIZENS' RIGHTS IN THE CONTEXT OF INFORMATION SECURITY AFTER THE 2020 CONSTITUTIONAL AND LEGAL REFORM

V. Melnichuk

Summary. This article examines the changes in the protection of citizens' rights in the field of information security caused by the constitutional and legal reform of 2020.

The author examines the impact of the amendments to the Constitution on the legal regulation of relations in the digital environment, in particular, on the protection of personal data, information security and digital rights of citizens. The work covers the main areas of updating legislation in this area and analyzes the strengthening of state responsibility for ensuring security in the information sphere.

The author focuses on key provisions of the reform, such as securing the right to protect personal information and strengthening cybersecurity measures.

Mechanisms for the implementation of these rights are also being considered, which include judicial practice, the activities of government agencies and new tools for digital regulation.

The author emphasizes the importance of maintaining a balance between the interests of the state and the rights of citizens in the context of digital transformation. In conclusion, the article offers recommendations for improving legislation and strengthening legal guarantees in the field of information security.

Keywords: Constitution of the Russian Federation, national security, information security, cybersecurity, reform, citizens' rights, digitalization, Constitutional Court.

Мельничук Виктор Алексеевич

К.в.н., доцент,

Санкт-Петербургский университет МВД России

melvic70@mail.ru

Аннотация. В данной статье рассматриваются изменения в сфере защиты прав граждан в области информационной безопасности, вызванные конституционно-правовой реформой 2020 года.

Автор исследует влияние внесенных поправок в Конституцию на правовое регулирование отношений в цифровой среде, в частности, на защиту персональных данных, информационную безопасность и цифровые права граждан. Работа охватывает основные направления обновления законодательства в этой области и анализирует усиление ответственности государства за обеспечение безопасности в информационной сфере.

В центре внимания автора лежат ключевые положения реформы, такие как закрепление права на защиту личной информации и усиление мер по обеспечению кибербезопасности.

Рассматриваются также механизмы реализации этих прав, которые включают судебную практику, деятельность государственных органов и новые инструменты цифрового регулирования.

Автор подчеркивает важность соблюдения баланса между интересами государства и правами граждан в условиях цифровой трансформации. В заключение статьи предлагаются рекомендации по совершенствованию законодательства и усилению правовых гарантий в сфере информационной безопасности.

Ключевые слова: Конституция РФ, национальная безопасность, информационная безопасность, кибербезопасность, реформа, права граждан, цифровизация, Конституционный Суд.

Информационная безопасность и защита прав граждан в цифровом пространстве становятся одними из ключевых вопросов современного общества. Стремительное развитие технологий, повсеместная цифровизация и широкое распространение интернета порождают новые вызовы, связанные с защитой личных данных, противодействием киберугрозам и обеспечением информационной прозрачности. На этом фоне актуальность юридических инструментов и государственных механизмов защиты прав граждан возрастает.

Конституционно-правовая реформа 2020 года стала важным этапом в развитии правовой системы России,

в том числе в контексте регулирования информационной безопасности. Внесенные изменения в Основной закон страны укрепили правовые гарантии защиты личности и открыли новые перспективы для развития нормативного регулирования в цифровой среде. Особую значимость приобрело закрепление в Конституции положений, направленных на защиту прав граждан в условиях глобальных информационных угроз.

Настоящая статья посвящена изучению влияния конституционно-правовой реформы на защиту прав граждан в сфере информационной безопасности. Основная цель работы — проанализировать новые правовые ме-

ханизмы, возникшие в результате реформы, оценить их эффективность и выявить возможные направления совершенствования законодательства в данной области.

В ходе исследования автор уделяет внимание не только изменениям в нормативно-правовой базе, но и их практическому применению, рассматривая примеры судебной практики, деятельность государственных органов. Особое внимание уделяется балансу интересов государства, общества и личности в обеспечении прав и свобод граждан в условиях цифровой трансформации.

Таким образом, статья направлена на углубленный анализ современного состояния защиты прав граждан в информационной сфере и разработку рекомендаций для дальнейшего совершенствования правового регулирования в данной области.

Конституция РФ¹ является основополагающим документом [1]. Она определяет права и обязанности граждан, государственное и территориальное устройство, очерчивает деятельность государственной власти, а также устанавливает правопорядок, законность и основные принципы жизнедеятельности государства. Конституция наделена высшей юридической силой. Новые нормативно-правовые акты создаются с опорой на Конституцию и не должны противоречить ей. Не вызывает сомнения, что в Конституции РФ следует искать основополагающие положения обеспечения осуществления прав граждан в сфере информационной безопасности.

Первая глава Конституции РФ (об основах конституционного строя) не содержит в себе статей, посвященных собственно информационной безопасности, но показывает основы обеспечения любых прав граждан (особенно ст.ст. 2, 4, 5, 13, 15, 16).

Правовые гарантии обеспечения информационной безопасности дают федеральные органы власти РФ. В ведении Федерального центра находится «регулирование и защита прав и свобод человека и гражданина»; «информация, информационные технологии [2] и связь»; «обеспечение безопасности личности, общества и государства при применении информационных технологий» (п.п. «в», «и», «м» ст. 71 Конституции РФ).

Государство гарантирует (глава 2 Конституции РФ) права и защиту следующих прав граждан в области информационной безопасности: защиту прав на персональные данные, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений,

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=ls1t9bsxwd602547004 (дата обращения: 13.02.2024).

информации о частной жизни лица; право на распространение информации законным способом при соблюдении законодательства о государственной тайне, персональных данных, частной жизни, запретах на возбуждение ненависти и вражды; право на информацию от госорганов о событиях, создающих угрозу для жизни и здоровья людей, информацию об окружающей среде — ст.ст. 23, 24, 29, 41, 42, и общее право на защиту любых нарушенных прав — ст.ст. 45–54.

Разъяснения Конституционного Суда РФ о конституционности норм в связи с правами граждан на информационную безопасность дополняют правовую базу обеспечения данных прав граждан. Есть Постановление Суда, в котором Суд еще раз указал, что интернет-сервис обязан обеспечивать тайну связи².

Также, в последние годы стала формироваться более жесткая повестка по отношению к границам деятельности иноагентов на территории РФ, когда в списки иноагентов вносят организации и отдельных лиц. Так, Конституционный суд РФ подтвердил³ мнение о применении Закона об иноагентах по отношению к научной деятельности, высказанное в 2014 году. В 2021 году автономная НКО «Институт права и публичной политики» (ИППП) была признана Минюстом иноагентом. В жалобе в Конституционный Суд Институт высказался о применении этого Закона по отношению к научной деятельности в области конституционного права, обратил внимание на то, что Закон не позволяет разграничить научную и политическую деятельность. Также, ИППП усмотрел в решении Минюста о признании ИППП иноагентом нарушение ст. 44 Конституции РФ о свободе научной деятельности, ст. 29 о праве на свободу слова и распространения информации, ч. 2 ст. 55. В «вину» институту Минюст записал публикации аналитических и экспертных докладов, проведение публичных дебатов, подписание петиций об экспертизе Венецианской комиссии о поправках к Конституции и разработку поправок к закону о реабилитации жертв политических репрессий. Заметим, что в п. 4 ст. 4 Закона об иноагентах говорится,

² Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова». URL: https://www.consultant.ru/document/cons_doc (дата обращения: 13.02.2024).

³ Определение Конституционного Суда РФ от 27.12.2023 № 3554-О «Об отказе в принятии к рассмотрению жалобы автономной некоммерческой организации «Институт права и публичной политики» на нарушение ее конституционных прав абзацами первым — одиннадцатым пункта 6 статьи 2, пунктом 10 статьи 13.1 и пунктом 7 статьи 32 Федерального закона «О некоммерческих организациях», а также частями 2–5 статьи 4 Федерального закона «О контроле за деятельностью лиц, находящихся под иностранным влиянием». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&bas> (дата обращения: 13.02.2024).

что к «политической деятельности не относится деятельность в области науки ... если соответствующая деятельность не противоречит национальным интересам РФ». Суд не усмотрел «произвольного применения» законодательства об иностранных агентах к ИППП, отказал в рассмотрении жалобы.

Согласно п. 57 Стратегии национальной безопасности (далее — Стратегия нацбезопасности) государство много в чем и как обязуется исполнять в сфере обеспечения информационной безопасности [3]. Содержание пункта 57 на первый взгляд можно поделить на общие обязательства и конкретные.

Например, к общим отнесем такие как: генерировать безопасную среду оборота информации, для чего развивать систему предупреждения угроз информационной безопасности, например, деструктивного воздействия на российские информационные ресурсы; предупреждать и пресекать преступления и нарушения, совершаемые с использованием ИКТ; укреплять взаимодействие власти, общества и граждан в данной области.

Сюда же Указ Президента РФ⁴ отнес вопрос международного сотрудничества и просвещения. В настоящее время, в условиях обострения угроз национальной безопасности, многие граждане задают в соцсетях вопросы, почему наша страна (в лице заявлений официальных лиц, например, интервью В.В. Путина Такеру Карлсону, заявления С.Д. Лаврова, М.В. Захаровой и др.) постоянно «пытается» (по мнению граждан), что-либо доказать, заявить, возразить западной риторике, пересказывая исторические факты, объявляя в розыск иностранных официальных лиц, которые никуда физически не скрылись, запрашивает в ООН тематические заседания и т.п. На самом деле, это тоже работа по обеспечению информационной безопасности нашего государства [4] и всех граждан, которые в Стратегии [5] в разделе «Информационная безопасность» «звучат» более корректно: «доведение до российской и международной общественности достоверной информации о внутренней и внешней политике Российской Федерации» (подп. 15 п. 57). Таким образом, за отдельно выверенной в правовом смысле фразой может скрываться огромный пласт работы, которую ведет государство в области обеспечения информационной безопасности.

Есть в п. 57 Стратегии и более «жесткие» положения, не скрывающие за дипломатической риторикой обязательства государства противостоять угрозам, например, пресекать технические разведки иностранных служб, вычищать российский Интернет от иностранного

⁴ Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023) «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2

вмешательства, если его субъекты деструктивно информационно воздействуют на граждан и общество, особо укреплять защиту российских разработок военной спецтехники, развивать технологии искусственного интеллекта и квантовые вычисления как средства противодействия угрозам информационной безопасности.

Говорится в п. 57 Стратегии и об «обеспечении защиты конституционных прав и свобод человека и гражданина при обработке персональных данных [6], в том числе с использованием информационных технологий» (подп. 8).

Но в целом, Указ Президента РФ более сосредоточен на защите информационной безопасности граждан, общества и государства от внешних угроз.

Соответствующее федеральное законодательство РФ регулирует вопросы обработки и защиты персональных данных, передаваемых сообщений, ответственности за сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, обеспечения возмещения ущерба от действий должностных лиц, скрывающих какую-либо информацию, и т.д. — все это способствует обеспечению информационной безопасности граждан [7].

Деятельность государства в области обеспечения информационной безопасности следует разделить на правотворческую и правоприменительную.

Поскольку конституционные основы обеспечения информационной безопасности закладывались не только государством, т.к. Конституция, ее поправки принимаются с участием всех граждан РФ, то субъектами обеспечения являются граждане РФ, органы государства (законодательные, исполнительные, судебные), среди которых выделим роль Президента РФ (создание и продвижение Стратегии нацбезопасности) и Конституционного Суда РФ.

Между тем, имеется проблема в правовом толковании понятия информационная безопасность, информация.

Понятие информация даже в законе имеет неотчетливое определение, больше напоминающее перечисление синонимов: «сведения (сообщения, данные) независимо от формы их представления» (ст. 2 Закона об информации). Иная сущность выходит на первый план, когда категория информация выступает в связке с категорией безопасность. Однако прежнее легальное определение безопасности как «состояния защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз», сегодня в правовых источниках изъято и показано через деятельность обеспечения безопасности субъектами деятельности, озвучен

ную в статьях Закона о безопасности. Между тем, мы бы не назвали концептуально ясными вводные статьи этого закона (глава 1), изобилующие положениями общего характера. Прежнее легальное определение безопасности [8] как никогда верно раскрывало сущность этой актуальной в наше время категории. Присоединяя к ней прилагательные, несущие указание на области безопасности (информационная, экономическая, экологическая, общественная и т.д.), мы получали бы различные правовые природы безопасности в отдельно взятых сферах.

Например, перерабатывая процитированные выше определения, мы бы представили информационную безопасность [9] как «состояние информационной защищенности жизненно важных интересов личности, общества и государства, когда информационные сведения, инфраструктура защищены от внутренних и внешних угроз». Суть явления, думаем, раскрывается верно.

На уровне общества, например, организаций, информационная безопасность (защищенность) предоставляет собой сбалансированную защиту конфиденциальности, целостности и доступности данных о человеке или организации⁵.

На уровне государства информационная безопасность государства означает, согласно п.п. 48–57 Стратегии нацбезопасности и если собрать смыслы содержания данных пунктов, укрепление суверенитета России в информационном пространстве путем противодействия вмешательству иностранными государствами, их специальными службами, террористическими и экстремистскими организациями, транснациональными корпорациями, а также любыми преступными субъектами через информационно-коммуникационные технологии (ИКТ) во внутренние дела государства.

На уровне личности информационная безопасность [10] должна обозначать состояние защищенности разумной личности от информационных угроз. При совокупном применении самозащиты и защиты государства этого состояния можно достичь. Без самозащиты (фильтровать информацию, что полезно для своего психологического состояния, разумно дозировать информацию о себе в социальных сетях и т.п.) остается полагаться на деятельность государства, его обязательства в сфере обеспечения информационной безопасности. Именно этот вопрос далее следует рассмотреть подробно. Отметим мнение С.В. Барина, [11] предлагающего права граждан на информационную безопасность расклады-

вать на составляющие части как техническую, идеологическую, психологическую, правовую безопасности в области информации.

Таким образом, Конституция РФ, решения Конституционного Суда РФ, Стратегия нацбезопасности и федеральные законы о безопасности, об информации заложили основополагающую базу обеспечения осуществления прав граждан в сфере информационной безопасности. Деятельность государства в указанной области следует является правотворческой и правоприменительной. Среди субъектов обеспечения выделим роль Президента РФ (создание и продвижение Стратегии нацбезопасности) и Конституционного Суда РФ.

Считаем, что для более качественного обеспечения осуществления прав граждан в сфере информационной безопасности следует дополнить нормы права в этой области, в частности вернуть определение понятия «безопасность» в Закон о безопасности, дополнить определение понятия «информация» в Законе об информации, далее, включать в каждый закон, где это подходит к логике его содержания, «свои» определения безопасности: информационной, экономической и др. Например, право на информационную безопасность граждан в свете национальной и повседневной безопасности [12] должно иметь составными частями конституционно-гражданскую (в связи с защитой), техническую, идеологическую, правовую безопасность.

Заключение

Проведенный анализ показал, что конституционно-правовая реформа 2020 года сыграла значимую роль в укреплении правовой основы для защиты прав граждан в области информационной безопасности. Внесенные изменения в Конституцию России обеспечили новые механизмы защиты личной информации, расширили ответственность государства за безопасность цифровой среды и закрепили права граждан в условиях стремительной цифровизации общества.

Тем не менее, несмотря на позитивные изменения, существуют определенные проблемы в реализации новых норм на практике. Среди них можно выделить недостаточную адаптацию подзаконных актов к обновленным конституционным положениям, слабую координацию между государственными органами и недостаточный уровень правовой грамотности граждан в вопросах информационной безопасности.

В условиях возрастающих информационных угроз особую значимость приобретает дальнейшая модернизация законодательства в этой сфере. Это включает усиление ответственности за утечки данных, разработку более эффективных механизмов противодействия

⁵ Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова». URL: https://www.consultant.ru/document/cons_doc (дата обращения: 13.02.2024).

киберугрозам [13] и создание условий для защиты прав граждан в условиях обработки больших объемов персональной информации.

Статья подчеркивает важность сохранения баланса между интересами государства, бизнеса и общества при регулировании информационной безопасности. Обеспечение этого баланса требует не только совершенствования законодательства, но и активного взаимодействия между всеми заинтересованными сторонами.

В заключение можно отметить, что успех реализации новых правовых механизмов, заложенных конституционно-правовой реформой 2020 года, зависит от комплексного подхода, включающего эффективное правоприменение, правовое просвещение граждан и активное использование современных технологий для повышения уровня безопасности в цифровом пространстве.

ЛИТЕРАТУРА

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=ls1t9bsxwd602547004 (дата обращения: 13.02.2025).
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3448.
3. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023) «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2
4. Федеральный закон от 14.07.2022 № 255-ФЗ (ред. от 24.07.2023) «О контроле за деятельностью лиц, находящихся под иностранным влиянием» // Собрание законодательства РФ. 2022. № 29 (часть II). Ст. 5222.
5. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности РФ» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.
6. Информационная безопасность // п. 3.35 в: Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения». СТО БР ИББС-1.0-2014 (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399). URL: <https://www.consultant.ru/document> (дата обращения: 13.02.2025).
7. Мельничук, В.А. информационная безопасность в России / В.А. Мельничук // 25 лет на службе Отечеству : Сборник научных трудов, посвященный деятельности научных школ Санкт-Петербургского университета МВД России и приуроченной к 25-летию со дня его образования / Сост.: О.И. Городовая, О.С. Кравченко, А.А. Жаворонкова. — Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. — С. 436–438. — EDN COGM0V.
8. Головистикова А.Н., Зильберт М.Н. Информационная безопасность в условиях цифровой трансформации: правовые аспекты // Государство и право. — 2021. — № 10. — С. 23–30.
9. Иванов П.В. Конституционные основы правового регулирования информационной безопасности в России // Право и государство. — 2020. — № 8. — С. 45–51.
10. Смирнов К.В. Баланс прав личности и интересов государства в цифровую эпоху // Вестник Московского университета. Серия 11: Право. — 2022. — № 2. — С. 67–74.
11. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. № 4(65). 97–104. 97.
12. Кобец Д.И. Перспективы развития законодательства в области защиты персональных данных после конституционных изменений // Юридическая наука и практика. — 2021. — № 5. — С. 34–41.
13. Губанов А.В. Киберугрозы и новые вызовы для законодательства России // Информационное право. — 2023. — № 6. — С. 18–24.

© Мельничук Виктор Алексеевич (melvic70@mail.ru)

Журнал «Современная наука: актуальные проблемы теории и практики»