- НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ -

Дата поступления рукописи в редакцию: 25.12.2025 г.
Дата принятия рукописи в печать: 16.02.2026 г.
DOI: 10.24412/2782-3830-2026-1-58-62

ШЕРАШЕНКОВА Екатерина Алексеевна,
К.п.н., доцент кафедры юриспруденции Смоленского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, e-mail smol@ranepa.ru

ФЕДОСКИН Николай Николаевич,
К.п.н., доцент кафедры юриспруденции Смоленского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, e-mail: nnfedoskin@yandex.ru

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ НА ПРИМЕРЕ СМОЛЕНСКОЙ ОБЛАСТИ

Аннотация. *В статье анализируются актуальные вопросы информационной безопасности исполнительных органов власти. Современные закономерности и тенденции широкомасштабного ускоряющегося процесса развития и при этом совершенствования информационных систем и технологий наглядно демонстрируют возрастание актуальности проблемы поиска высокого уровня технических, юридических, организационных и иных мероприятий обеспечения информационной безопасности. Активное внедрение информационных технологий в исполнительных органах власти Смоленской области способствует повышению открытости, прозрачности, подотчетности деятельности органов муниципальной власти, вовлеченности граждан в процессы муниципального управления. Вместе с тем, процесс порождает определённые проблемы, связанные с информационной безопасностью, так как загрузка большого количества данных граждан неизбежно ведет к повышению шанса утечек, различных нарушений, потерей конфиденциальных данных представляющих интерес для криминальных структур.*

Авторы отмечают, что общественные отношения, связанные с государственным регулированием в сфере информации и информационных технологий невозможны без теоретического исследования основных вопросов безопасности и их содержательного смысла.

Ключевые слова: *информационные технологии, правовое регулирование, цифровой суверенитет, исполнительные органы власти, информационная безопасность.*

SHERASHENKOVA Ekaterina Alekseevna,
PhD., Associate Professor of the Department of Legal Disciplines of the Smolensk Branch of the Russian Presidential Academy of National Economy and Public Administration

FEDOSKIN Nikolay Nikolaevich
PhD., Associate Professor of the Department of Legal Disciplines of the Smolensk Branch of the Russian Presidential Academy of National Economy and Public Administration

LEGAL ASPECTS OF INFORMATION SECURITY IN EXECUTIVE AUTHORITIES ON THE EXAMPLE OF THE SMOLENSK REGION

Annotation. *The article analyzes current issues of information security of executive authorities. Modern patterns and trends of a large-scale accelerating process of development and at the same time improvement of information systems and technologies clearly demonstrate the increasing urgency of the problem of finding a high level of technical, legal, organizational and other information security measures. The active introduction of information technologies in the executive authorities of the Smolensk region contributes to increasing openness, transparency, accountability of the activities of municipal authorities, and the involvement of citizens in the processes of municipal government. At the same time, the process creates certain problems related to information security, since downloading a large amount of citizens' data inevitably leads to an increased chance of leaks, various violations, and the loss of confidential data of interest to criminal structures. The authors note that public relations related to state regulation in the field of information and information technology are impossible without a theoretical study of the basic security issues and their meaningful meaning.*

Key words: *information technologies, legal regulation, digital sovereignty, executive authorities, information security.*

Информационная безопасность органов государственной власти Российской Федерации и населения является приоритетным направлением, одним из важнейших компонентов национальной безопасности. От эффективности системы защиты и обеспечения правовыми и техническими средствами, от взаимодействия органов исполнительной власти в данной сфере, зависит степень сохранности критически важных данных власти и граждан. Предпринимаемые решения должны полноценно противостоять информационным угрозам, которые требуют постоянного внимания и выстраивания алгоритмов противодействия. Главной целью является «защита прав граждан и организаций, формирование условий, нацеленных на реализацию прав и свобод человека и гражданина, закреплённых в законодательстве» [1, с.67].

Главным нормативно-правовым актом выступает Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ [2]. Информационная безопасность является критически важной сферой для деятельности органов исполнительной власти Смоленской области, требующей строгого соблюдения нормативных актов и правовых регуляций. Анализ правового регулирования в данной области выявляет несколько ключевых аспектов. В соответствии с законодательством Российской Федерации и нормативными актами Правительства Смоленской области, в области информационной безопасности устанавливаются основные принципы и требования [3]. Основу правового поля составляют федеральные законы, включая Указ Президента РФ от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации» [4] и Указ Президента РФ от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [5].

На уровне регионального законодательства Правительства Смоленской области принимает меры по адаптации и конкретизации требований федерального законодательства в контексте региональных особенностей. Важным аспектом является разработка и внедрение местных нормативных актов, учитывающих специфику информационной инфраструктуры и особенности управления данными на территории области.

Основные нормативно-правовые акты, регулирующие информационную безопасность в Смоленской области, включают положения о защите конфиденциальной информации, обязанности органов исполнительной власти по обеспечению безопасности информации. Кроме того, часто регламентируется также и ответственность за нарушения в области информационной безопасности [6].

Необходимо также отметить, что на региональном уровне уделено много внимания проведению эффективной политики в сфере правовой поддержки борьбы с потерей данных. Так, принята особая программа развития, а именно «Концепция защиты информации на территории Смоленской области на 2022 – 2030 годы». В ней обозначена трактовка понятий, которыми оперируют органы исполнительной власти в ведении своей деятельности в сфере обеспечения безопасности информации.

Кроме того, данная концепция приводит конкретные шаги по реализации федеральной Доктрины информационной безопасности Российской Федерации. Также в данной концепции описан алгоритм реализации федеральных программ на региональном уровне, а также решения по обеспечению данных программ.

Региональное законодательство устанавливает конкретные органы, ответственные за ведение деятельности в сфере информационной безопасности. Примером этому может послужить Распоряжение Администрации Смоленской области от 20.04.2018 № 409-р/адм. «О возложении на смоленское областное государственное автономное учреждение «Центр информационных технологий» функций органа криптографической

защиты информации органов исполнительной власти Смоленской области, удостоверяющего центра органов исполнительной власти Смоленской области и об утверждении Положения об органе криптографической защиты информации органов исполнительной власти Смоленской области».

Важно отметить, что в рамках правового регулирования важным является учет не только национальных стандартов, но и международных норм в области информационной безопасности, что способствует обеспечению соответствия международным стандартам и повышению уровня защиты данных. Это также находит отражение в НПА, которыми руководствуются органы исполнительной власти. Так, в упомянутой выше Концепции одним из важных факторов необходимости ведения эффективной деятельности в сфере защиты данных является размещение на территории Смоленской области дипломатических и консульских учреждений, международных организаций и их представительств.

Эффективное применение правовых инструментов в области информационной безопасности требует системного подхода и взаимодействия между различными уровнями власти, бизнес-сообществом и общественными организациями. Важно обеспечить не только соблюдение формальных требований законодательства, но и развитие культуры информационной безопасности, повышение осведомленности сотрудников и граждан об угрозах и методах защиты информации.

Необходимость постоянного обновления и совершенствования нормативной базы подчеркивает важность дальнейшего развития правовых механизмов, способствующих эффективной защите информации на региональном уровне. Важно также уделять внимание совершенствованию локальных правовых норм, которые призваны помогать лучше реагировать на те вызовы в сфере информационной безопасности, с которыми сталкивается именно Смоленская область. Обращает на себя внимание и совершенствование применяемых технологий, когда «защита информации становится одной из важнейших задач, требующей системного подхода и непрерывного совершенствования» [7].

При анализе текущего состояния систем защиты информации в региональных органах показывает, что несмотря на применение основных мер защиты включая антивирусные программы и межсетевые экраны, имеются существенные недостатки. «Они включают ограниченные ресурсы для обновления и модернизации, а также недостаточную адаптацию к современным киберугрозам» [8, с.236].

Первоочередной задачей модернизации является обновление технической инфраструктуры. Прежде всего, это переход к актуальным версиям программного обеспечения, прежде всего отечественного, внедрение современных средств защиты (таких как DLP и системы шифрования) и применение облачных технологий с высоким уровнем безопасности.

Необходимо обратить внимание на усиление организационных мер. Создание и внедрение строгих практик информационной безопасности, регулярное обучение персонала, переподготовка кадров в случае необходимости, формирование культуры безопасности персонала все эти направления будут способствовать повышению уровня защиты данных.

Важной частью обеспечения сохранности данных является создание и внедрение соответствующих систем мониторинга угроз и превентивного реагирования на них. Необходимо использовать специальные средства защиты, в дополнение к используемым антивирусным программам. Это очень актуальная тема в контексте появления угроз, которые несет в себе искусственный интеллект. Потенциально он может серьёзно облегчить проведение DDoS-атак на серверы органов власти, создать массовые фейковые рассылки и найти пути обхода защитных алгоритмов, используемые службами безопасности.

Вместе с тем, искусственный интеллект может помогать и предупреждать появление подобных угроз. Здесь следует обратить внимание на опыт коммерческих предприятий, которые проводят исследования в сфере возможностей ИИ для аудита систем безопасности [9]. ИИ может также использоваться как замена т.н. «белым хакерам», проводя испытания систем безопасности органов исполнительной власти на прочность.

Следует обратить внимание и на сотрудничество с ведущими региональными университетами, которые и готовят кадры для органов власти. Сотрудничество с университетами также может привнести большое количество позитивных изменений, связанных с исследованием самых актуальных технических вызовов, и стоит анализировать и внедрять этот опыт одновременно привлекая высококвалифицированные кадры в службы безопасности. Возможным путём совершенствования является создание особых совместных лабораторий, где учёные будут не только вести обособленное изучение технических вопросов, но и подготавливать решения для конкретного заказчика, которым может выступить государство или региональные власти.

Внедрение систем управления информационной безопасностью (СУИБ), также способно

существенно повысить устойчивость к киберугрозам. Необходимо внедрять отечественные СУИБ, которые могут быть использованы в разных организациях в зависимости от их потребностей и специфики и не уступающие западным аналогам. Например, ОС Astra Linux Special Edition — сертифицированная отечественная ОС со встроенными средствами защиты информации. Позволяет обрабатывать любую информацию ограниченного доступа — от персональных данных до государственной тайны «особой важности». Что очень важно в современных условиях, соответствует требованиям безопасности всех регуляторов к ПО для импортозамещения. «InfoWatch Traffic Monitor» - Российская DLP-система, представляющая собой инструмент предотвращения утечек, обнаружения и устранения угроз. Визитной карточкой российской DLP-системы компании InfoWatch являются технологии контентного анализа и обработки больших объемов информации с помощью искусственного интеллекта.

Выбор СУИБ зависит от потребностей и возможностей конкретной организации. Некоторые из этих продуктов могут быть интегрированы друг с другом для обеспечения более комплексной защиты информации [10].

В 2024 году РАНХиГС провел исследование, целью которого было определение уровня «цифровой зрелости» органов власти в России. По результатам анализа было выявлено, что, начиная с 2022 года падает активность внедрения технологий искусственного интеллекта в государственных органах, из 52 проанализированных ведомства только половина готова к внедрению искусственного интеллекта в свою деятельность.

Эффективная работа органов власти невозможна без решения ключевых проблем, препятствующих созданию эффективного регионального управления в России. Проблемными остаются вопросы «разрозненности методов перевода государственных и муниципальных услуг в цифровую среду; низкий уровень «цифрового образования» государственных и муниципальных служащих; технически сложное оформление государственных официальных сайтов; отсутствие единой правовой базы для регулирования вопросов деятельности государственных и муниципальных органов в цифровой среде» [11, с. 44].

Решение большей части указанных проблем видится в совершенствовании нормативно-правового регулирования. Необходимо законодательное закрепление порядка раскрытия информации цифровыми сервисами, а также порядка сбора и хранения данных. Законодательно закрепить установление запрета на ограничение информационного суверенитета человека. Отсутствие единых стандартов пользовательских соглашений и политики цифровых сервисов для отечественных цифровых сервисов также нуждается в дальнейшей правовой проработке. Актуальными проблемами правового регулирования остаются задачи минимизации состава обрабатываемых персональных данных, необходимых для решения различных вопросов, возлагаемых на государственные и иные органы исполнительной власти.

Список литературы:

[1] Зуев Е.Д., Минаев А.В. Понятие и признаки исполнительной власти в России // Международный журнал гуманитарных и естественных наук. 2024. №2-3 (89) С.63-71.

[2] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» // Российская газета. 29 июля 2006 г. N 165.

[3] «Концепция защиты информации на территории Смоленской области на 2022 – 2030 годы»// https://it-security.admin-smolensk.ru/obshaia-informac/

[4] Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Официальный интернет-портал правовой информации (pravo.gov.ru) 25 декабря 2023 г. № 0001202312250083.

[5] Указ Президента РФ от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (с изменениями и дополнениями от 13 июня 2024) // Собрание законодательства Российской Федерации от 2 мая 2022 г. N 18 ст. 3058

[6] Постановление Администрации Смоленской области от 19 января 2018 № 15 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений». [Электронный ресурс]. URL: https://it-security.admin-smolensk.ru/obshaia-informac

[7] Колесникова Д.С., Верещагина Е.А., Гуляев В.Е. Построение онтологической модели для предметной области «информационная безопасность» // ИВД. 2023. №7 (103). URL: https://cyberleninka.ru/article/n/postroenie-ontologicheskoy-modeli-dlya-predmetnoy-oblasti-informatsionnaya-bezopasnost (дата обращения: 21.12.2025).

[8] Бойченко, И. С. Модели правового регулирования нейросетей. / И. С. Бойченко // Образование и право. – 2019. – № 1. – С. 235-237.

[9] Титков Д.И., Резниченко С.А. Революция в аудите информационной безопасности: искусственный интеллект // Вестник науки. 2024. №4 (73). URL: https://cyberleninka.ru/article/n/

revolyutsiya-v-audite-informatsionnoy-bezopasnosti-iskusstvennyy-intellekt (дата обращения: 21.12.2025).

[10] Федоров А.В., Жихарев А.Г., Кальченко Д.М. Обеспечение информационной безопасности в органах исполнительной власти. Проблемы и решения // Научный результат. Информационные технологии. 2024. №1. - С. 135-137.

[11] Никифорова С.А. Электронное правительство - новая концепция государственного управления. // Вестник Санкт-Петербургского университета МВД России. – 2020. - № 6. – С. 40-47.

References:

[1] Zuev E.D., Minaev A.V. Concept and signs of executive power in Russia//International Journal of Humanities and Natural Sciences. 2024. No. 2-3 (89) S.63-71.

[2] Federal Law of 27.07.2006 N 149-FZ (as amended by 24.06.2025) " On Information, Information Technologies and Information Protection "// Rossiyskaya Gazeta. July 29, 2006 N 165.

[3] "Concept of information protection in the Smolensk region for 2022-2030 "// https://it-security.admin-smolensk.ru/obshaia-informac/

[4] The doctrine of information security of the Russian Federation: Decree of the President of the Russian Federation of 05.12.2016 No. 646//Official Internet portal of legal information (pravo.gov.ru) December 25, 2023 No. 0001202312250083.

[5] Decree of the President of the Russian Federation of May 1, 2022 N 250 "On additional measures to ensure the information security of the Russian Federation" (as amended and supplemented on June 13, 2024)//Collection of legislation of the Russian Federation of May 2, 2022 N 18 Art. 3058

[6] Resolution of the Administration of the Smolensk Region dated January 19, 2018 No. 15 "On the definition of threats to the security of personal data relevant to the processing of personal data in the information systems of personal data of the executive authorities of the Smolensk Region and their subordinate institutions." [Electronic resource]. URL: https://it-security.admin-smolensk.ru/obshaia-informac

[7] Kolesnikova D.S., Vereshchagina E.A., Gulyaev V.E. Building an ontological model for the subject area "information security "//IVD. 2023. №7 (103). URL: https://cyberleninka.ru/article/n/postroenie-ontologicheskoy-modeli-dlya-predmetnoy-oblasti-informatsionnaya-bezopasnost (дата обращения: 21.12.2025).

[8] Boychenko, I. S. Models of legal regulation of neural networks ./I. S. Boychenko//Education and law. – 2019. – № 1. - S. 235-237.

[9] Titkov DI, Reznichenko S.A. Revolution in information security audit: artificial intelligence//Bulletin of Science. 2024. №4 (73). URL: https://cyberleninka.ru/article/n/revolyutsiya-v-audite-informatsionnoy-bezopasnosti-iskusstvennyy-intellekt (дата обращения: 21.12.2025).

[10] Fedorov A.V., Zhikharev A.G., Kalchenko D.M. Ensuring information security in executive authorities. Problems and solutions//Scientific result. Information technology. 2024. №1. - S. 135-137.

[11] Nikiforova S.A. Electronic government is a new concept of public administration .//Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2020. - № 6. - S. 40-47.