Государственное и муниципальное управление. Ученые записки. 2025. № 4. С. 54–62
State and Municipal Management. Scholar Notes. 2025;(4):54–62

Обзорная статья
УДК 351+352+004
EDN MVIYRG

Современные риски информационной безопасности в условиях цифровой трансформации государственного и муниципального управления: пути преодоления

Марина Викторовна Перова[1], Наталья Дмитриевна Никоненко[2], Максим Владимирович Прокопенко[3]

[1, 2, 3]Российская академия народного хозяйства и государственной службы при Президенте РФ, Южно-Российский институт управления, Ростов-на-Дону, Россия

[1]perova-mv@ranepa.ru, https://orcid.org/0000-0001-6989-8160
[2]nikonenko-nd@ranepa.ru, https://orcid.org/0009-0002-8664-6680
[3]prokopenko-mv@ranepa.ru, https://orcid.org/0000-0002-6803-7921

Аннотация

Введение. Статья посвящена актуальным вопросам обеспечения информационной безопасности в госсекторе. Проводится анализ киберугроз, которые могут быть реализованы в госсекторе. Анализируется защита персональных данных в целом.

Цель. Проанализировать ключевые риски в контексте цифровой трансформации госуправления в области информационной безопасности, опираясь на статистические данные и эмпирические показатели, а также определить пути преодоления.

Материалы и методы. Методологическую основу исследования составляют метод научной абстракции, анализ нормативных документов и стандартов, системный анализ, сравнительный анализ статистических данных, метод трендового анализа, а также метод экспертных заключений.

Результаты. В ходе исследования была проанализирована нормативно-правовая база обеспечения информационной безопасности в целом. Особое внимание уделено системам электронного документооборота как инструменту стратегического направления цифровой трансформации государственного управления. Определено, что данные системы являются одновременно государственными информационными системами и информационными системами персональных данных. Приводится краткий алгоритм обеспечения информационной безопасности в данном случае в контексте выполнения мер приказов Федеральной службы по техническому и экспортному контролю для государственных информационных систем и информационных систем персональных данных. Приводится статистика кибератак на органы государственной власти России за последние годы. Анализируются основные тренды деятельности злоумышленников и методы борьбы с ними.

Выводы. Государственные учреждения остаются приоритетной мишенью для злоумышленников, несмотря на развитие защитных механизмов. Важно выделить необходимые меры по укреплению информационной безопасности: комплексная реализация требований регуляторов (Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности), внедрение современных технических средств защиты информации, повышение квалификации государственных служащих в области информационной безопасности, постоянный мониторинг и актуализация систем защиты, развитие отечественных технологий кибербезопасности. Перспективные направления развития включают: интеграция искусственного интеллекта в системы защиты, развитие технологий предиктивной аналитики угроз, совершенствование механизмов раннего обнаружения атак, укрепление нормативно-правовой базы в сфере информационной безопасности. Таким образом, несмотря на достигнутые успехи в цифровизации государственного управления, требуется продолжение системной работы по укреплению информационной безопасности. Особое внимание следует уделить развитию отечественных технологических решений и повышению компетентности персонала в области защиты информации.

Ключевые слова: цифровая трансформация, государственные информационные системы, информационные системы персональных данных, системы электронного документооборота, кибератаки, киберугрозы, уязвимости, информационная безопасность

Для цитирования: Перова М. В., Никоненко Н. Д., Прокопенко М. В. Современные риски информационной безопасности в условиях цифровой трансформации государственного и муниципального управления: пути преодоления // Государственное и муниципальное управление. Ученые записки. 2025. № 4. С. 54–62. EDN MVIYRG

Review article

Modern information security risks in the context of digital transformation of public and municipal administration: ways to overcome

Marina V. Perova[1], Natalia D. Nikonenko[2], Maksim V. Prokopenko[3]

[1, 2,3]Russian Presidential Academy of National Economy and Public Administration,
South-Russian Institute of Management, Rostov-on-Don, Russia

[1]perova-mv@ranepa.ru, https://orcid.org/0000-0001-6989-8160
[2]nikonenko-nd@ranepa.ru, https://orcid.org/0009-0002-8664-6680
[3]prokopenko-mv@ranepa.ru, https://orcid.org/0000-0002-6803-7921

Abstract

Introduction. The article is devoted to topical issues of information security in the public sector. An analysis of cyber threats that can be implemented in the public sector is being conducted. The protection of personal data in general is analyzed.

Purpose. Analyze the key risks in the context of the digital transformation of public administration in the field of information security, based on statistical data and empirical indicators, and identify ways to overcome them.

Materials and methods. The methodological basis of the research consists of the method of scientific abstraction, the analysis of normative documents and standards, system analysis, comparative analysis of statistical data, the method of trend analysis, as well as the method of expert opinions.

Results. The study analyzed the regulatory framework for information security in general. Special attention is paid to electronic document management systems as a tool for the strategic direction of digital transformation of public administration. It is determined that these systems are both state information systems and personal data information systems. A brief algorithm for ensuring information security in this case is given in the context of the implementation of measures ordered by the Federal Service for Technical and Export Control for government information systems and personal data information systems. The statistics of cyber attacks on Russian government authorities in recent years are given. The main trends in the activities of intruders and methods of combating them are analyzed.

Conclusions. Government institutions remain a high-priority target for intruders, despite the development of protective mechanisms. It is important to highlight the necessary measures to strengthen information security: comprehensive implementation of regulatory requirements (Federal Service for Technical and Export Control, Federal Security Service), introduction of modern technical means of information protection, advanced training of government officials in the field of information security, constant monitoring and updating of protection systems, development of domestic cybersecurity technologies. Promising areas of development include: the integration of artificial intelligence into security systems, the development of predictive threat analytics technologies, the improvement of attack early detection mechanisms, and the strengthening of the regulatory framework in the field of information security. Thus, despite the successes achieved in the digitalization of public administration, continued systematic work is required to strengthen information security. Special attention should be paid to the development of domestic technological solutions and improving the competence of personnel in the field of information security.

Keywords: digital transformation, government information systems, personal data information systems, electronic document management systems, cyber attacks, cyber threats, vulnerabilities, information security

For citation: Perova M. V., Nikonenko N. D., Prokopenko M. V. Modern information security risks in the context of digital transformation of public and municipal administration: ways to overcome. *State and Municipal Management. Scholar Notes.* 2025;(4):54–62. (In Russ.). EDN MVIYRG

Введение

Современный этап социально-экономического развития характеризуется масштабной цифровизацией всех сфер общественной жизни. Согласно данным Международного союза электросвязи (ITU), к 2024 г. более 68 % населения мира имеют доступ к интернету, что создаёт объективные предпосылки для трансформации механизмов государственного управления[1]. В России, согласно данным, представленным в ежегодном аналитическом отчет «Белая книга цифровой экономики-2024» на портале «Госуслуги» зарегистрированы 129,9 млн граждан (что в 1,7 раз больше, чем в 2019 г.). В контексте цифровой трансформации формируется концепция электронного государства (e-government) – модели управления, где цифровые технологии выступают основным инструментом при реализации властных полномочий; обеспечении эффективной коммуникации с гражданами; обработки, хранения и передачи данных. Данный процесс представляет собой комплексное явление, соединяющее правовые, организационные и технологические основы государственной деятельности. Цифровая трансформация государственного управления влияет на все процессы государства, поэтому требует глубокого научного обоснования и анализа, например, в [1] рассматриваются вопросы трансформации в области документооборота. Однако, чем больше цифровых решений, тем больше внимания необходимо уделять обеспечению информационной безопасности и защите информации в целом.

Заметим, что при опубликовании научных статей по цифровым решениям (их разработке и алгоритмам) требуется получать заключение экспортного контроля о том, что там нет критически важной информации. Вопросам защиты информации посвящены работы [2, 3], в которых рассматриваются вопросы технической защиты информации, а также данные, которые являются наиболее желаемыми для злоумышленников. При реализации национального проекта «Экономика данных и цифровая трансформация государства» одной из базовых технологий является технология больших данных и возникают особенности при обеспечении безопасности данных. Особенности обеспечения информационной безопасности при работе с большими данными рассмотрены в исследовании [4]. Заметим, что базовыми цифровыми решениями в госсекторе являются государственные информационные системы, которые согласно нормативно-правовым актам разрабатываются на платформе ГосТех, компоненты аттестованы Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности (подробнее о платформе ГосТех [5, 6]), уже представлена дорожная карта ГосТех 2.0. В государственном секторе особое внимание уделяется и защите персональных данных, поскольку государственные информационные системы в большинстве случаев являются информационными системами персональных данных. И здесь возникают особенности по организации защиты. Кроме того, отдельно регулируются персональные данные государственных гражданских служащих и муниципальных служащих, а ведение их личных дел регулируется одним нормативно-правовым документом.

Материалы и методы

При проведении исследования применялись: метод научной абстракции, анализ нормативных документов и стандартов, системный анализ, сравнительный анализ статистических данных, метод трендового анализа, а также метод экспертных заключений. Данная работа основывается на систематизации, анализе и опирается на понятийный аппарат, таких категорий, как цифровая трансформация, государственное и муниципальное управление, информационная безопасность, безопасность государственных информационных систем и информационных систем персональных данных. В рамках исследования проведен анализ применения цифровых технологий в государственном и муниципальном управлении, исследования государственной политики в области информационной безопасности, а также обеспечения безопасности государственных информационных систем и информационных систем персональных данных.

Результаты

Согласно аналитическим материалам портала TAdviser (2024), электронное государство представляет собой интегрированную систему, объединяющую органы власти разных уровней в едином цифровом контуре[2]. Ключевой признак – обеспечение взаимодействия участников через доверенные сервисы с гарантированной юридической значимостью. В Российской Федерации данная

[1] Международный союз электросвязи (ITU). Измерение цифрового развития: факты и цифры 2024 [Электронный ресурс]. – URL: https://www.itu.int/hub/publication/d-ind-ict_mdd-2024-4/?utm_source=Securitylab.ru (дата обращения: 17.10.2025).

[2] TAdviser. Цифровизация госсектора 2024: обзор [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Цифровизация_госсектора_2024 (дата обращения: 17.10.2025).

концепция реализуется в рамках национальных проектов «Экономика данных и цифровая трансформация государства» (далее – «Экономика данных»), «Цифровое государственное управление». По данным Минцифры РФ (2024)[1], показатели цифровизации госуслуг демонстрируют устойчивый рост: 95 % – доля граждан, имеющих доступ к порталу «Госуслуги»; 87 % – процент услуг, доступных в электронном формате; 78 % – уровень удовлетворённости пользователей цифровыми сервисами.

Одним из центральных инфраструктурных проектов цифровизации государственного управления является система межведомственного электронного взаимодействия (СМЭВ)[2]. В настоящее время она эволюционировала в полноценную экосистему, объединяющую разнообразные проекты и программные решения. Современная СМЭВ4 выходит за рамки простого информационного обмена: она предоставляет участникам взаимодействия инструменты самообслуживания и даёт возможность эффективно управлять процессами межведомственного взаимодействия на основе технологии витрин данных, а также реализовывать НСУД, что позволяет обеспечивать не только качество государственных данных, но и их безопасность.

Ростовская область занимает лидирующее положение среди субъектов Российской Федерации, использующих отечественные системы СЭД в крупных масштабах. Регион активно реализует одно из ключевых стратегических направлений – обеспечение технологической независимости в области цифровизации документооборота органов власти и местного самоуправления. Межведомственная система электронного документооборота и делопроизводства Ростовской области реализована на базе отечественного комплексного решения – СЭД «Дело» компании ЭОС. Первые автоматизированные рабочие места (АРМ) пользователей системы появились в регионе в 2006 году, а сегодня СЭД охватывает все региональные органы власти, муниципальные администрации и подведомственные им структуры, в том числе детские сады, школы, медицинские учреждения[3].

Основу оптимизации цифрового взаимодействия составляют современные системы электронного документооборота (ЭДО), обеспечивающие юридически значимую регистрацию документов; контролируемое движение данных; долговременное хранение информации.

В рамках реализации стратегических направлений в области цифровой трансформации государственного управления, обозначенных в Распоряжении Правительства РФ от 16 марта 2024 г. №637-р переход на электронный документооборот органов местного самоуправления, государственных и муниципальных учреждений должен составлять до 100 процентов к 2030 году; также должно быть обеспечено формирование единого информационного пространства в области внутриведомственного и межведомственного электронного взаимодействия органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации[4]. В 2022 году был запущен проект ГосЭДО (государственный электронный документооборот) – инициатива по созданию единого информационного пространства для электронного документооборота в госсекторе. В январе 2024 года объявлено о масштабном расширении системы: все российские правительственные ведомства будут интегрированы в ГосЭДО. Цель – обеспечить «прозрачную и доверенную коммуникацию» в государственном документообороте.

Анализируя отличие ГосЭДО от прежней системы электронного документооборота (СЭД), можно выделить следующие аспекты. Новая платформа включает два принципиальных усовершенствования: работа с машиночитаемыми документами, что даёт возможность отслеживать историю согласования, фиксировать исполнителей на каждом этапе, обеспечивать сквозную поддержку электронных подписей. Важно отметить, что механизм гарантирует подлинность и аутентичность

---

[1] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Цифровизация госуслуг – государство для граждан [Электронный ресурс]. – URL: https://digital.gov.ru/uploaded/files/0-chernyishenko_0zg5OE2.pdfИнфраструктура электронного правительства. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/infrastruktura-elektronnogo-pravitelstva (дата обращения: 17.10.2025).

[2] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Инфраструктура электронного правительства [Электронный ресурс]. – URL: https://www.cnews.ru/news/top/2024-08-22_v_rostove_k_rossijskoj_sisteme (дата обращения: 17.10.2025).

[3] CNews. В Ростове к российской СЭД «Дело» подключили более 4,7 тысяч организаций [Электронный ресурс]. – URL: https://www.cnews.ru/news/top/2024-08-22_v_rostove_k_rossijskoj_sisteme (дата обращения: 17.10.2025).

[4] Официальный интернет-портал правовой информации. О стратегическом направлении в области цифровой трансформации государственного управления : распоряжение Правительства РФ от 16 марта 2024 г. № 1305-р [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1305259154 (дата обращения: 17.10.2025).

пересылаемых документов. Второй аспект – ГосЭДО контролирует передачу и исполнение цифровых поручений, что повышает прозрачность процессов.

Полное подключение всех федеральных органов исполнительной власти, подчинённых правительству, к платформе ГосЭДО запланировано на 2025 год[1].

Важно отметить еще один ключевой аспект внедрении СЭД – обеспечение цифрового суверенитета как фактора информационной безопасности. Действительно использование отечественных СЭД-платформ; размещение данных в национальных центрах обработки (ЦОД); соблюдение требований законодательства о защите информации несомненно отражает тенденцию перехода к технологическому самоуправлению. Государственные структуры все чаще выбирают отечественные решения, что укрепляет защиту информационного пространства и формирует управленческую независимость. Электронный документооборот при этом выполняет двойную задачу: оптимизирует административные процессы и укрепляет способность государства к самостоятельному управлению цифровой инфраструктурой не только на федеральном, но и на региональном уровне.

Согласно отчёту ФСТЭК России (2024), внедрение российских СЭД позволило снизить риск внешнего вмешательства на 40 %; сократить зависимость от иностранных платформ до 8 % (против 35 % в 2020 г.); обеспечить соответствие 100 % документопотоков требованиям ФЗ № 152 «О персональных данных».

Рынок СЭД, ECM и CSP-систем стабильно растет последние несколько лет. В среднем динамика остается стабильной и составляет10-12% в год. В период с 2022 по 2024 год было реализовано свыше 1 300 проектов в сфере систем электронного документооборота (СЭД). Преобладающая доля из них создана на платформе Directum RX (620 реализованных проектов) от компании Directum. Помимо этого, в число наиболее востребованных решений вошли: ELMA365 ECM (152); Tessa (90); Docsvision (82); ТЕЗИС (48); 1С:Документооборот (38)[2]. В рейтинге участвовали 23 компании, включая вендоров и интеграторов. Совокупная выручка всех участников от реализации СЭД, ECM и CSP-проектов приблизилась к отметке 13 млрд рублей.

Анализируя факторы, которые влияют на данную динамику и развитие, можно выделить технологии искусственного интеллекта (ИИ) и развитие нейросетей, которые начинают активно выполнять роль помощника в анализе большого объема информации, в принятии решений, автоматизации рутинных операций, все большую популярность приобретают умные чат-боты и т.д. Активно добавляются модули по решению задач аналитической обработки информации на основе больших данных и облачных технологий, по обеспечению проектного и процессного управления.

Важно заметить совершенствование современных СЭД в направлении исполнения требований регуляторов, например, в соответствии с приказом Минцифры №542 от 19.06.2025 (Метод рекомендации по установлению требований к системам электронного документооборота), ГОСТ 56939-2024 (БРПО), Приказ ФСТЭК от 11.04.2025 N 117 Требования о защите информации, содержащейся в ИС госорганов, Требования ФСБ. Внедряется работа с цифровыми поручениями (ПП РФ 637-р от 16.03.2024 «Об утверждении стратегического направления в области цифровой трансформации государственного управления»). 31.12.2025 – ФОИФ и ОГВ субъектов Российской Федерации перешли на цифровой формат поручений.

Несмотря на прогресс в формировании единого цифрового пространства при реализации концепции цифровой трансформации госуправления данный процесс сопряжен с различными угрозами и рисками, особенно в области информационной безопасности, включая киберугрозы и киберпреступления.

Рассматривая аспекты обеспечения информационной безопасности в органах государственного и муниципального управления, необходимо отметить, что Российская Федерация выступает одним из антилидеров в области информационных атак и киберпреступлений. По данным компании Positive Technologies, в период с июля 2024 г. по сентябрь 2025 г. на Россию пришлось порядка 15% всех успешных кибератак в мире и 72% атак, зафиксированных в СНГ[3]. По данным компании RT-Solar,

[1] Коммерсантъ. Цифра прописалась в Белом доме [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/6465536 (дата обращения: 17.10.2025).
[2] TAdviser. Российский рынок СЭД, ECM и CSP-систем: итоги и перспективы [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/СЭД (дата обращения: 17.10.2025).
[3] Авезова Я., Резников Р., Беседина В. CODE RED 2026: Актуальные киберугрозы для российских организаций [Электронный источник]: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id2 (Дата обращения: 15.10.2025 г.)

с начала 2025 г. продолжает расти интенсивность атак на российские компании. Количество среднего числа срабатываний, свидетельствующих о возможном заражении вредоносным ПО, увеличилось во втором квартале 2025 г. на 20% по сравнению с предыдущим периодом[1].

Говоря о структуре кибератак, отметим, что органы государственной и муниципальной власти находятся на первом месте по количеству успешных кибератак. На доли госучреждений приходится 21% успешных атак. При этом количество атак имеет тенденцию к увеличению: в третьем квартале 2025 года среднее количество срабатываний в госорганизациях выросло на 23,6%.

Если говорить об объектах атак в госучреждениях, то наибольшей популярностью у злоумышленников пользуются компьютеры, серверы и сетевое оборудование: на них было направлено 80% успешных атак. На шпионаж приходится 68% атак, атаки, целью которых является финансовая выгода, составляют 20%, а на хактивизм приходится 8% атак.

Наибольшую популярность у преступников при осуществлении кибератак имеет вредоносное программное обеспечение. На него пришлось 56% успешных атак. На рис. 1 можно увидеть распределение срабатываний в 3 квартале 2025 года.

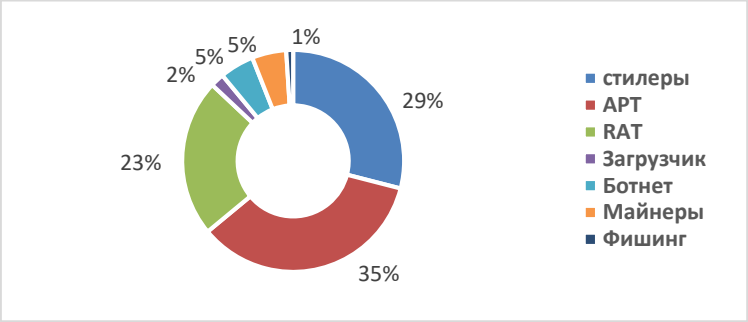

Рис. 1 Доля распределения срабатываний в 3 квартале 2025[2]
Fig. 1 Share of triggered events in the third quarter of 2025

Как видим из приведенных данных, 35% срабатываний приходится на APT – деятельность известных профессиональных хакерских группировок. Среди вредоносных программ первое место занимают программы-стилеры – программы, предназначенные для похищения конфиденциальной информации пользователя, такой как логины, пароли, данные банковских карт и других личных данных. На втором месте находятся Remote Access Trojan (RAT) – трояны удаленного администрирования, которые позволяют злоумышленнику удаленно управлять устройством, часто без ведома жертвы. Отметим, что в 2025 г. происходит снижение доли стилеров, которые все больше уступают по популярности RAT. Преимуществом RAT является более сложное обнаружение, а также то, что троян может быть использован не только для похищения данных, но и для продажи другим злоумышленникам возможности получить доступ во взломанную систему организации.

В Российской Федерации развитие цифровых технологий происходит в рамках национального проекта «Экономика данных». В данном проекте (федеральный проект «Кибербезопасность») особое внимание уделяется обеспечению безопасности персональных данных. Это является закономерным, так как персональные данные используются не только в государственном управлении, но и в различных областях экономики. К информационным системам персональных данных относятся системы электронного документооборота (в госсекторе СЭД является одновременно государственной информационной системой и информационной системой персональных данных), CRM-системы (данные системы начинают активно внедряться в госсекторе в контексте клиентоцентричности и реализации проекта «Государство для людей»), формы обратной связи на сайтах и тех систем, которые согласно определению Закона о персональных данных являются таковыми. Отметим, что из года в год персональные данные как видно из рис.2 являются одними из наиболее желаемыми данными для атак согласно данным https://www.ptsecurity.com с целью хищения данных. Как видно из рис. 2, число атак на государственные учреждения стабильно растёт. Проанализировав данные с учетом линейного тренда можно сделать вывод об активизации данного процесса.

[1] Ландшафт киберугроз: аналитика сенсоров во втором квартале 2025 года // Rt-Solar [Электронный источник]: https://rt-solar.ru/solar-4rays/blog/6067/(Дата обращения: 25.10.2025 г.)
[2] Куда сместились киберугрозы? Итоги 2 квартала 2025 года в России [Электронный источник]: https://rt-solar.ru/solar-4rays/blog/6067/ (Дата обращения: 25.10.2025 г.)

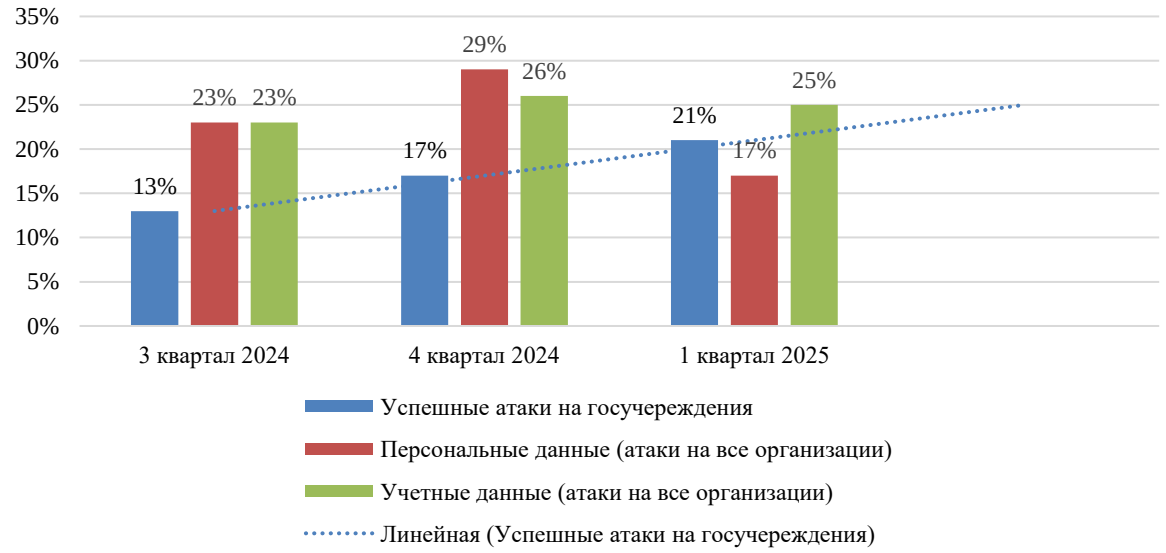

Рис. 2. Успешные атаки и утечки данных
Fig. 2. Successful attacks and data breaches

В рамках федерального проекта «Кибербезопасность» ужесточается наказание в области неправомерной обработки персональных данных. Заметим, что до недавнего времени самые большие штрафы, предусмотренные в КоАП были в области несоблюдения требований по локализации персональных данных. Подход к большим штрафам в области наказаний за нарушения при обработке персональных данных является общемировой практикой. Рассмотрим пример КНР и Европейского регламента (GDPR). Заметим, что обсуждения об ужесточении наказания за неправомерную обработку персональных данных велись давно и это была планомерная работа. Согласно GDPR, если не соблюдается его принципы, то штрафы могут быть существенными – максимально возможные штрафы до 20 миллионов евро или до 4% от общего мирового годового оборота.

Законодательство о персональных данных развивается в контексте развития цифровых технологий и национального проекта «Экономика данных». С 25 ноября 2025 г. вступает в силу Приказ Минцифры России от 02.06.2025 № 511 «Об установлении дополнительных требований, предъявляемых к официальному сайту российской организации, осуществляющей деятельность в области информационных технологий, в информационно-телекоммуникационной сети «Интернет», в котором указывается, что доступ к сайту осуществляется без передачи персональных данных. Кроме того, у операторов персональных данных станет больше обязанностей, планируется что с 1 марта 2028 г. операторы станут передавать в ЕСИА информацию об обработке личных сведений. Напомним, что согласно изменениям в Закон о персональных данных 2022 г. операторы обязаны быть подключены к ГосСОПКА. При обработке персональных данных особое внимание уделяется согласию на обработку персональных данным. Напомним, что с 1 сентября 2025 г. вступили в силу изменения в статью 9, которая регулирует работу с согласием на обработку персональных данных. Теперь согласие должно оформляться отдельно от иных документов, которое подписывает субъект персональных данных.

Если рассматривать государственные информационные системы, то большинство из них будет информационными системами персональных данных. Ярким примером является СЭД в госсекторе. В этом случае необходимо выполнять два Приказа ФСТЭК РФ и два Приказа ФСБ для государственных информационных систем, не содержащих информацию, относящуюся к государственной тайне, и информационным системам персональных данных. Отметим, что в данном случае рекомендуется сначала выполнять мероприятия Приказа ФСТЭК России от 11.02.2013 № 17 (после 1 марта 2026 г. Приказа ФСТЭК России от 11.04.2025 № 117), а затем Приказа ФСТЭК России от 18.02.2013 № 21. Заметим, что минимальный набор мер согласно приказам ФСТЭК для государственных информационных систем шире, чем минимальный набор мер для информационных систем персональных данных. Кроме того, отметим, что, например, для государственных информационных систем третьего класса защищенности меры защиты обеспечивают 3 и 4 уровни защищенности персональных данных.

Заметим, что отдельно регулируется обеспечение безопасности персональных данных государственных и муниципальных служащих. Ведение личных дел государственных гражданских и муниципальных служащих регулируется Указ Президента РФ от 30.05.2005 N 609 (ред. от 10.10.2024) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Заключение

По результатам проведенного анализа можно констатировать следующие ключевые выводы. Цифровая трансформация государственного сектора демонстрирует значительный прогресс, однако сопровождается ростом киберугроз. Государственные учреждения остаются приоритетной мишенью для злоумышленников, несмотря на развитие защитных механизмов. Основные угрозы безопасности концентрируются в следующих областях: СЭД, МЭДО, защита персональных данных в государственных информационных системах, риски отказа функционирования критически важных сервисов. Позитивные тенденции в сфере информационной безопасности включают: активное развитие отечественных решений для СЭД, внедрение единой платформы ГосТех, усиление требований к защите персональных данных, рост внимания к импортозамещению. Важно выделить необходимые меры по укреплению информационной безопасности: комплексная реализация требований регуляторов (ФСТЭК, ФСБ), внедрение современных технических средств защиты информации, повышение квалификации государственных служащих в области ИБ, постоянный мониторинг и актуализация систем защиты, развитие отечественных технологий кибербезопасности. Перспективные направления развития включают: интеграция искусственного интеллекта в системы защиты, развитие технологий предиктивной аналитики угроз, совершенствование механизмов раннего обнаружения атак, укрепление нормативно-правовой базы в сфере информационной безопасности

Таким образом, несмотря на достигнутые успехи в цифровизации государственного управления, требуется продолжение системной работы по укреплению информационной безопасности. Особое внимание следует уделить развитию отечественных технологических решений и повышению компетентности персонала в области защиты информации

Список источников

1. Ударова О. В. Некоторые вопросы организации документационного обеспечения деятельности федеральных органов исполнительной власти (по результатам мониторинга процесса документообразования и объемов документооборота в федеральных органах исполнительной власти за 2024 год) // Вестник ВНИИДАД. 2025. № 5. С. 31–41.

2. Зацаринный А. А., Гаврилов В. Е. Некоторые подходы к развитию технического регулирования в области информационной безопасности систем с искусственным интеллектом // ИТ-Стандарт. 2025. № 3(44). С. 11–18.

3. Моросанова А. А. Большие, персональные, обезличенные данные: проблемы отраслевого регулирования // Вестник Московского университета. Серия 6: Экономика. 2025. Т. 60. № 3. С. 172-193. https://doi.org/10.55959/MSU0130-0105-6-60-3-8.

4. Полтавцева М. А., Зегжда Д. П. Моделирование информационных процессов систем управления большими данными для решения задач кибербезопасности // Программные продукты и системы. 2024. № 1. С. 54–61. https://doi.org/10.15827/0236-235X.145.054-061

5. Еремин С. Г. Применение цифровых технологий в сфере государственного управления на федеральном уровне и направления их совершенствования // Экономика. Налоги. Право. 2024. Т. 17. № 1. С. 98-105. https://doi.org/10.26794/1999-849X-2024-17-1-98-105

6. Цифровая трансформация государственного управления: современные реалии / Н. Д. Никоненко, А. А. Краснухина, Е. А. Егорова [и др.] // Наука, инновации, общество в современных условиях : монография. Пенза : Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 5–15.

References

1. Udarova O.V. Some Issues of Document Management Organization in Federal Executive Bodies Based on the Results of Monitoring Document Creation Process and Volume of Document Flows in Federal Executive Bodies for 2024 Year. *Herald of VNIIDAD.* 2025;(5):31–41. (In Russ.)

2. Zatsarinny A.A., Gavrilov V.E., Some Approaches to Development of Technical Regulation in Information Security Systems with Artificial Intelligence. *IT-Standard*. 2025;3(44):11–18. (In Russ.)

3. Morosanova A.A. Big Data, Personalized Data, Deidentified Data: Problems of Sectoral Regulation. *Moscow University Bulletin. Series 6. Economics*. 2025;60(3):172–193. (In Russ.). https://doi.org/10.55959/MSU0130-0105-6-60-3-8

4. Poltavtseva M.A., Zegzda D.P. Modeling Information Processes of Big Data Management Systems for Cybersecurity Tasks Solution. *Software Products & Systems*. 2024;(1):54–61. https://doi.org/10.15827/0236-235X.145.054-061 (In Russ.).

5. Eremin S.G., Application of Digital Technologies at the Federal Level of Public Administration and Directions for Their Improvement. *Economy. Taxation. Law*. 2024;17(1):98–105. https://doi.org/10.26794/1999-849X-2024-17-1-98-105 (In Russ.).

6. Nikonenko N.D., Krasnukhina A.A., Egorova E.A., et al. Digital Transformation of Public Administration. In: *Modern Realities, Science, Innovation, Society under Current Conditions:* Monograph. Penza: Nauka i Prosveschenie Publ., 2022. P. 5–15. (In Russ.).

Информация об авторах

М. В. Перова – кандидат педагогических наук, доцент, зав. кафедрой информационных технологий, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Южно-Российский институт управления.

Н. Д. Никоненко – кандидат физико-математических наук, доцент, доцент кафедры информационных технологий, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Южно-Российский институт управления.

М. В. Прокопенко – кандидат экономических наук, доцент кафедры информационных технологий, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Южно-Российский институт управления.

Information about the authors

M. V. Perova – Head of the Department of information technology, Cand. Sci. (Pedagogy), Associate Professor, Russian Presidential Academy of National Economy and Public Administration, South-Russia Institute of Management.

N. D. Nikonenko – Cand. Sci. (Phys.-Math.), Associate Professor of the Department of Information Technology, Russian Presidential Academy of National Economy and Public Administration, South-Russia Institute of Management.

M. V. Prokopenko – Cand. Sci. (Econ.), Associate Professor of the Department of Information Technology, Russian Presidential Academy of National Economy and Public Administration, South-Russia Institute of Management.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts.

Статья поступила в редакцию 21.10.2025; одобрена после рецензирования 27.11.2025; принята к публикации 28.11.2025.
The article was submitted 21.10.2025; approved after reviewing 27.11.2025; accepted for publication 28.11.2025.