УДК 338

КИБЕРБЕЗОПАСНОСТЬ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: ВЫЗОВЫ И СТРАТЕГИИ ЗАЩИТЫ

Блохин Д.А.

Бакалавр

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Медведева О.С.

К.э.н., доцент,

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Аннотация: В статье рассматриваются актуальные проблемы кибербезопасности в государственном управлении, возникающие на фоне стремительной цифровизации государственной системы и роста числа кибератак. Обсуждаются основные угрозы, в том числе утечки данных, фишинг, DDoS-атаки и целенаправленные взломы, на примере статистики атак на госструктуры, финансовый сектор и транспортную отрасль. Значительное внимание уделяется нормативно-правовой базе Российской Федерации, направленной на защиту информации граждан и обеспечение безопасности государственных систем. Авторами сделан вывод о том, что только комплексное применение технических, законодательных и просветительских мер позволит значительно повысить уровень кибербезопасности и укрепить доверие граждан к электронным государственным услугам.

Ключевые слова: кибербезопасность, цифровизация государственных услуг, взаимодействие с гражданами, утечка данных, информационная безопасность.

CYBERSECURITY IN PUBLIC ADMINISTRATION: CHALLENGES AND PROTECTION STRATEGIES

Blokhin D.A.
undergraduate
Kaluga State University named after K.E. Tsiolkovsky
Kaluga, Russia
Medvedeva O.S.
Candidate of Economics, Associate Professor,
Kaluga State University named after K.E. Tsiolkovsky
Kaluga, Russia

Abstract: The article discusses current cybersecurity issues in public administration, which arise due to the rapid digitalization of the public system and the increasing number of cyberattacks. The main threats, including data breaches, phishing, DDoS attacks, and targeted hacking, are discussed using the example of statistics on attacks on government agencies, the financial sector, and the transportation industry. The article also focuses on the regulatory framework of the Russian Federation aimed at protecting citizens' information and ensuring the security of public systems. The authors conclude that only a comprehensive application of technical, legislative, and educational measures will significantly improve cybersecurity and strengthen citizens' trust in electronic public services.

Keywords: cybersecurity, digitalization of public services, interaction with citizens, data leakage, and information security.

В современном мире цифровые технологии все больше проникают во все сферы жизни, взаимодействие граждан с государственными структурами становится все более важным аспектом обеспечения эффективного государственного управления. В последние годы наблюдается активное внедрение инновационных решений, которые ориентированы на новые формы

коммуникаций, обеспечивают более прозрачное взаимодействие и способствуют повышению уровня вовлечённости граждан в процессы принятия решений [9]. Однако с ростом зависимости от цифровых платформ и услуг возникает серьезная проблема – утечка данных. Открытость и доступность информации, способствующие улучшению взаимодействия между государством и обществом, также создают риски для безопасности личных данных граждан. Эксперты BI.ZONE опубликовали отчет о трендах кибератак в России и СНГ за 2024 год. Наибольшее количество атак было зафиксировано в государственных организациях (15%), финансовом секторе (13%), а также в сфере транспорта и логистики (11%) [14]. В этой связи вопрос кибербезопасности становится особенно актуальным и одним из первостепенных вопросов.

Кибербезопасность включает в себя технологии, методы и навыки, предназначенные для защиты информационных технологий и инфраструктуры от несанкционированного доступа, уязвимостей и атак, которые могут быть использованы злоумышленниками в цифровом пространстве.

Термин «кибербезопасность» имеет различные трактовки, в зависимости от его отрасли. В таблице 1 представлены различные определения термина «кибербезопасность» в зависимости сферы его применения.

Таблица 1 – Термин «кибербезопасность» и его характеристика в различных отраслях

Сфера использования	Характеристика
Кибербезопасность в бизнесе [10]	«Это система мер и технологий, которая защищает цифровые ресурсы компании: серверы, сайты, CRM-системы, корпоративные чаты и облачные хранилища. Основная цель — предотвратить несанкционированный доступ, кражу или разрушение данных в цифровой среде, а также обеспечить бесперебойную работу бизнес-процессов»
Кибербезопасность в военной отрасли [6]	«Это защита оборонных сетей, систем и данных от киберугроз. Направлена на обеспечение конфиденциальности, целостности и доступности критически важной информации, а также на поддержание функциональности и эксплуатационной готовности военных систем»
Кибербезопасность в науке [12]	«Это совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. При этом основной упор делается на сохранение благоприятного состояния киберпространства, а не на число угроз»

Итак, можно сделать вывод, что кибербезопасность в государственном управлении это защита государственных информационных систем от киберугроз, включая утечки данных и вредоносные программы. Кибербезопасность в государственном управлении при взаимодействии с гражданами основывается на нескольких ключевых компонентах.

Во-первых, важна защита личных данных, что подразумевает обеспечение их безопасности и конфиденциальности с использованием технологий шифрования и соблюдения законодательных норм.

Во-вторых, необходимо внедрение современных технологий, включая антивирусные программы и системы защиты информации, чтобы гарантировать безопасность онлайн-сервисов для граждан. Реализация надежных методов пользовательской аутентификации, таких как двухфакторная аутентификация, помогает предотвратить несанкционированный доступ к государственным порталам.

Кроме того, важно проводить образовательные программы для повышения осведомленности граждан о киберугрозах и методах защиты личной информации. Разработка четких правил и стандартов кибербезопасности регулирует защиту данных граждан и управление киберрисками в государственных системах. Регулярный аудит и оценка безопасности помогают выявлять уязвимости и укреплять защиту информации о гражданах. Все это позволит создать надежную систему кибербезопасности, обеспечивающую безопасное взаимодействие граждан с государственными органами, а также повысить имидж государственных органов. Однако, следует отметить, что, если не формировать имидж самостоятельно, он будет создаваться стихийно под влиянием позитивных или негативных комментариев потребителей, что в свою очередь может привести к серьезным последствиям и сложностям в управлении им [11].

Также в Российской Федерации существует нормативно-правовые акты, которые составляют базу кибербезопасности в государственном управлении при коммуникации с гражданами (таблица 2).

Таблица 2 – Нормативно-правовые акты Российской Федерации, связанных с кибербезопасностью в государственном управлении при коммуникации с гражданами

Нормативно-правовой акт	Характеристика
Конституция Российской Федерации [1]	Содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности и другие. Например, устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи
Федеральный закон от 28 декабря 2010 г. №390-ФЗ «О безопасности» [2]	Закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и её функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности
Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]	Фиксирует базовые нормы для всей системы информационного законодательства, в том числе правового обеспечения информационной безопасности
Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации [4]	Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях её устойчивого функционирования при проведении в отношении её компьютерных атак
Указ Президента РФ от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [5]	Устанавливает запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, к информационно-телекоммуникационным сетям международного информационного обмена

Несмотря на то, что в Российской Федерации имеются нормативно-правовые акты, закрепляющие основы кибербезопасности в государственном управлении при коммуникации с гражданами, эта система не способна полностью устранить угрозы и кибератаки. Самым ярким примером является взлом портала «Госуслуги». По данным Роскомнадзора, за первый квартал 2024 года было зафиксировано более 12 000 попыток взлома портала «Госуслуг». Это на 37 % больше, чем за аналогичный период прошлого года. 63 % атак – фишинг (поддельные сайты и письма), 22 % – DDoS-атаки, 15 % –

сложные целенаправленные взломы (APT-атаки) [7]. В 2024 году количество преступлений, связанных с неправомерным доступом к компьютерной информации, выросло почти втрое по сравнению с предыдущим годом. Примерно 90 % этих преступлений касаются взломов аккаунтов на портале «Госуслуги». По данным МВД, в 2023 году таких случаев было чуть больше 36 тысяч, а в 2024 – уже свыше 104 тысяч.

В ответ на вызовы, связанные с кибератаками, Россия активно борется с угрозами в государственном секторе и при взаимодействии с гражданами. Для этого разработана комплексная стратегия, которая включает технические, организационные, законодательные и просветительские меры. Эти усилия направлены на повышение уровня кибербезопасности и защиту информации, что должно укрепить доверие граждан к электронным государственным услугам. Среди мероприятий, направленных на защиту информации, можно выделить следующие:

– Федеральный проект «Инфраструктура кибербезопасности». В его рамках проводится независимый анализ защищенности государственных информационных систем. Созданы специализированные учреждения, такие как Отраслевой центр государственной системы обнаружения и противодействия компьютерным атакам, Национальный удостоверяющий центр и Центр кибербезопасности [8].

– Проект «Багбаунти». Этот проект включает привлечение «белых» хакеров для проверки государственных систем на устойчивость, которые выявляют уязвимость за денежное вознаграждение [6].

– Система RT Protect EDR. Она предназначена для выявления кибератак на конечные устройства и оперативного автоматического противодействия. Защита осуществляется через анализ поведения объектов в почтовом и интернет-трафике, мониторинг сетевой активности и выявление аномалий с использованием искусственного интеллекта и машинного обучения [13].

Кроме того, до 1 марта 2026 года в России планируется введение платформы по борьбе с кибермошенничеством, которая будет обеспечивать взаимодействие государственных органов, банков и операторов связи. Основные функции антифрод-платформы будут включать сбор и обмен данными о кибермошеннических действиях, а также автоматический обмен сигналами о подозрительных событиях между участниками системы.

Таким образом, современная реалия характеризуется стремительным ростом кибератак, что ставит под угрозу работу госорганов и безопасность личных данных граждан. Несмотря на наличие разветвленной нормативно-правовой базы и активное внедрение передовых технологий защиты, таких как системы мониторинга, аутентификации и комплексные проекты по обеспечению кибербезопасности, динамика инцидентов указывает на необходимость постоянного совершенствования этих мер. Комплексный подход, объединяющий технические, законодательные и просветительские инициативы, является единственным эффективным способом противодействия эволюционирующим угрозам в цифровом пространстве и поддержания доверия граждан к государственным электронным сервисам.

Библиографический список

1. Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // КонсультантПлюс / [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 02.10.2025).

2. Федеральный закон от 28 декабря 2010 г. №390-ФЗ «О безопасности» // КонсультантПлюс / [Электронный ресурс] URL:

https://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 02.10.2025).

3. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» // КонсультантПлюс / [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.10.2025).

4. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации // КонсультантПлюс / [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 02.10.2025).

5. Указ Президента РФ от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // Президент России / [Электронный ресурс] URL: http://www.kremlin.ru/acts/bank/27040 (дата обращения: 02.10.2025).

6. Багбаунти Минцифры // минцифры_ / [Электронный ресурс] URL: https://digital.gov.ru/activity/kiberbezopasnost/bagbaunti-minczifry (дата обращения: 10.10.2025).

7. Военный рынок кибербезопасности – ведущие инновации и возникающие угрозы // Market Research Intellect / [Электронный ресурс] URL: https://www.marketresearchintellect.com/ru/blog/military-cybersecurity-market-leading-innovations-and-emerging-threats/ (дата обращения: 06.10.2025).

8. Госуслуги под прицелом: статистика 2024 года // dzen.ru / [Электронный ресурс] URL: https://dzen.ru/a/aJEZ5r7Ikyo3HRf2#kto_stoit_za_atakami_i_chto_im_nyjno (дата обращения: 06.10.2025).

9. Корнакова, К. М. Цифровые технологии для взаимодействия государства и общества / К. М. Корнакова, Т. Н. Субботина // Экономика и бизнес: теория и практика. – 2025. – № 5(123). – С. 179-183. – DOI 10.24412/2411-0450-2025-5-179-183. – EDN SBICHG.

10. Кибербезопасность в бизнесе // incrussia.ru / [Электронный ресурс] URL: https://incrussia.ru/understand/kiberbezopasnost-v-biznese-riski/ (дата обращения: 06.10.2025).

11. Надуваев, К. А. Использование PR-технологий в формировании позитивного имиджа организации / К. А. Надуваев, О. С. Медведева // Экономика и бизнес: теория и практика. – 2021. – № 6-2(76). – С. 104-111. – DOI 10.24412/2411-0450-2021-6-2-104-111. – EDN WEUNHM.

12. Проект «Концепция стратегии кибербезопасности Российской Федерации» // Правительство Российской Федерации / [Электронный ресурс] URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2014_Orig_Draft_41d4b3dfbdb25cea8a73.pdf (дата обращения: 06.10.2025).

13. Руководство пользователя RT Protect EDR // RT Protect EDR / [Электронный ресурс] URL: https://rt-ib.ru/docs/Руководство%20Пользователя%20RT%20Protect%20EDR.pdf (дата обращения: 10.10.2025).

14. BI.ZONE представила исследование российского ландшафта угроз за 2024 год // Хабр / [Электронный ресурс] URL: https://habr.com/ru/news/880130/ (дата обращения: 05.10.2025).

Оригинальность 80%