ХОРОШЕЕ УПРАВЛЕНИЕ

ИССЛЕДОВАТЕЛЬСКАЯ СТАТЬЯ

Кибербезопасность государства: внутренний контроль и управление рисками

Александр Сергеевич Юхно[a]

EDN: YDXAIT

[a] **Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации**

Аннотация: Цифровизация государственного управления сопровождается ростом киберугроз, однако существующие подходы к управлению рисками остаются фрагментарными и не обеспечивают системного контроля. Комплексный анализ российских и зарубежных исследований и аналитических обзоров в области кибербезопасности позволил систематизировать актуальные киберриски государства, выработать базовый алгоритм управления ими и разработать единую цифровую систему внутреннего контроля и управления рисками, которая может лечь в основу общегосударственной системы кибербезопасности. Такая система способна обеспечить мониторинг киберугроз в реальном времени, автоматизировать процесс принятия решения и повысить устойчивость системы государственного управления в целом. Результаты работы могут рассматриваться как теоретико-методологическая основа для дальнейших исследований адаптивных систем кибербезопасности и применяться в работе государственных органов, разрабатывающих программы кибербезопасности, и корпоративного сектора, нуждающегося в защите критической информационной инфраструктуры.

Ключевые слова: внутренний контроль, государственное управление, кибербезопасность, риски кибербезопасности, киберриски, риск-менеджмент, цифровая трансформация

Дата поступления статьи в редакцию: 9 сентября 2025 года.

National cybersecurity: internal control and risk management

Alexander S. Yukhno[a]

RESEARCH ARTICLE

[a] **Russian Presidential Academy of National Economy and Public Administration**

Abstract: The digitalization of public administration has resulted in an increase in cyber dangers; nevertheless, current approaches to risk management remain fragmented and do not allow for systematic supervision. A thorough examination of Russian and international studies and reviews in the field of cybersecurity has allowed us to organize the current cyber risks facing the state, develop a basic framework for managing them, and create a unified digital system for internal control and risk management, which can serve as the foundation for a nationwide cybersecurity system. This system can provide real-time cyber threat monitoring, automate decision-making, and enhance the overall resilience of government systems. Future research on adaptive cybersecurity systems can use the study's findings as a theoretical and methodological basis. The conclusions can also be used by businesses that need to safeguard vital information infrastructure and by government organizations developing cybersecurity initiatives.

Keywords: internal control, public administration, cybersecurity, cybersecurity risks, cyber risks, risk management, digital transformation

Received: September 9, 2025.

Введение

В июле 2025 года компания «Аэрофлот» подверглась одной из самых мощных кибератак в истории[1]. Подобные ситуации все чаще возникают в условиях цифровой трансформации: атаки затрагивают как частный, так и государственный сектор. В связи с этим жизненно важной задачей становится создание общегосударственной системы кибербезопасности, которая была бы способна оперативно адаптироваться к происходящим изменениям и своевременно реагировать на возникающие риски и угрозы.

Государственное управление в условиях цифровой трансформации требует комплексного анализа актуальных рисков. Настоящая работа призвана систематизировать актуальные риски кибербезопасности и разработать базовый алгоритм управления данными рисками. В статье будет предложен комплекс мер для формирования единой цифровой системы внутреннего контроля и управления рисками, позволяющей в режиме реального времени осуществлять мониторинг угроз, автоматизировать процессы принятия решений и повысить устойчивость системы государственного управления в целом.

Кибербезопасность как вызов системе государственного управления

Недостаточное внимание к кибербезопасности[2] со стороны государства чревато серьезными последствиями, включая финансовые потери, судебные иски, потерю конкурентоспособности, доверия граждан и т.д.; не исключен и физический ущерб, в том числе человеческие жертвы. Кибербезопасность можно рассматривать в различных аспектах: как комплекс технологических решений, связанных с обеспечением информационной и компьютерной безопасности; как сферу правового регулирования, предполагающую соблюдение требований законодательства; как элемент национальной и международной безопасности, подразумевающий высокую роль цифровых технологий в разведывательной деятельности и предотвращении конфликтов; наконец, как фактор экономического и социального развития, способствующий созданию материальных благ и инноваций через использование цифровых инструментов[3].

В современной международной практике отсутствует единый подход к формированию стратегий в сфере кибербезопасности. Одни государства сосредоточены на обеспечении защиты данных и документации, другие – на противодействии мошенничеству или снижении репутационных рисков. Представляется, что проблематику кибербезопасности в первую очередь необходимо рассматривать с точки зрения анализа рисков и управления ими. На практике способность государств выявлять, оценивать и управлять рисками существенно различается. Отдельные страны, обладающие более высоким уровнем технологического и методологического развития в данной сфере, как правило, формируют условия для безопасного взаимодействия всех участников цифровой среды, включая разработку и внедрение передовых практик, необходимых мер безопасности, предоставление соответствующей информационной поддержки и помощи гражданам с учетом динамично изменяющихся рисков.

Современные вызовы кибербезопасности носят системный характер. Активная вовлеченность государств в эту сферу обусловлена совокупностью ключевых факторов, включая наличие в их распоряжении большого объема данных, в т.ч. конфиденциальных, регулярные взломы баз данных, усложнение характера современных кибератак и государственной цифровой инфраструктуры, а также необходимость соблюдения требований законодательства, защиты персональных данных пользователей, коммерческой тайны, интеллектуальной собственности, денежных средств, информационных систем[4]. Кибербезопасность затрагивает все уровни государственного управления и предполагает взаимодействие широкого круга заинтересованных сторон в решении возникающих вопросов. Это делает необходимым создание целостной экосистемы защиты, объединяющей усилия различных органов власти, а также привлечения экспертного сообщества и частного сектора. Особую актуальность приобретают вопросы распределения полномочий, стандартизации подходов и обеспечения непрерывной защиты в условиях цифровой трансформации. Такой подход способствует усилению межведомственной координации в этой области. Учитывая, что цифровая среда является динамичной областью, приходится констатировать, что выработанные решения быстро устаревают и требуют постоянной актуализации[5].

Для оценки таких рисков требуется точная оценка как потенциального ущерба, так и вероятности [Edwards, Hofmeyer, Forrest, 2016. P. 3]. В исследовании Организации экономического сотрудничества и развития (далее – ОЭСР) «Оценка практики управления

1 «Аэрофлот» столкнулся с мощнейшей хакерской атакой из-за рубежа. https://www.vedomosti.ru/business/articles/2025/07/29/1127599-aeroflot-stolknulsya-s-moschneishei-hakerskoi-atakoi

2 На практике вопросы кибербезопасности часто обозначаются различными терминами: «цифровая безопасность», «информационная безопасность» и др. В настоящей работе термины используются как взаимозаменяемые.

3 Digital security risk management for economic and social prosperity: OECD recommendation and companion document (2015). P. 19–24. https://doi.org/10.1787/9789264245471-en (далее – OECD 2015)

4 Cyber security breaches survey 2019: statistical release. P. 13–14. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf (далее – Cyber security breaches survey 2019)

5 How your board can better oversee cyber risk. P. 3–4. https://www.pwc.com/us/en/governance-insights-center/publications/assets/pwc-how-your-board-can-better-oversee-cyber-risk.pdf

рисками цифровой безопасности в компаниях» отмечается, что эффективное управление рисками кибербезопасности позволит минимизировать частоту и негативное влияние инцидентов в этой области[6]. По этой причине важным практическим вопросом становится возможность эффективной оценки результатов управления рисками цифровой безопасности.

Принимая во внимание тот факт, что не существует официальной статистики, источников данных или широко признанных методологий для измерения реальной стоимости инцидентов в области кибербезопасности, их количество в данной области сложно измерить. Более того, государства, как правило, не готовы раскрывать информацию о своих уязвимостях, произошедших инцидентах и их влиянии на свое функционирование, что обусловлено необходимостью минимизации репутационных рисков, предотвращения потенциальной эскалации киберугроз и сохранения стратегических преимуществ в цифровой сфере[7]. При этом потребность в таких данных только продолжит возрастать.

Современные исследования в области кибербезопасности демонстрируют необходимость анализа статистически значимых данных для выявления устойчивых тенденций и формирования прогностических моделей. Анализ динамики киберинцидентов за последнее десятилетие показывает, что, несмотря на относительную стабильность количества инцидентов, связанных с нарушением безопасности данных (как злонамеренных, связанных с целенаправленными атаками на конфиденциальную информацию, так и случайных, обусловленных человеческим фактором), их негативное воздействие на экономических агентов имеет выраженную тенденцию к усилению. Особую актуальность приобретает фактор растущей стоимости утечек персональных данных, что обусловлено расширением возможностей их монетизации и усложнением финансовых операций в цифровой среде. Данная закономерность указывает на качественное изменение характера киберугроз даже при сохранении прежней частоты их возникновения [Edwards, Hofmeyer, Forrest, 2016. P. 4].

Риски кибербезопасности

Согласно данным компании Positive Technologies, чаще всего жертвами кибератак становятся государственные учреждения: на госсектор приходится 15 % атак[8]. Подобные инциденты провоцируют системные сбои в работе государственного аппарата, что проявляется в снижении качества предоставления услуг, нарушении управленческих процессов и ухудшении координации между ведомствами.

В 2024 году Россия столкнулась с беспрецедентной эскалацией кибератак на критическую инфраструктуру и частный сектор. Одним из наиболее значимых инцидентов стал взлом государственной автоматизированной системы «Правосудие», приведший к масштабному сбою в работе судов. Одновременно наблюдались скоординированные атаки на федеральный удостоверяющий центр «Основание», телеканалы «Россия-1» и «Россия 24», официальный сайт МИД России и финансовый сектор. Параллельно произошли масштабные утечки данных в государственных учреждениях и частном секторе[9]. Эти инциденты демонстрируют системные уязвимости в защите данных и необходимость усиления мер кибербезопасности на государственном уровне. В этой связи Правительством Российской Федерации утвержден комплексный план мероприятий по реализации Концепции государственной системы противодействия преступлениям в сфере информационно-коммуникационных технологий, направленный на совершенствование законодательной базы, развитие технических средств противодействия киберугрозам и повышение цифровой грамотности населения[10].

В докладе ОЭСР «Управление рисками цифровой безопасности и конфиденциальности» отмечается, что в 2015 году ущерб от одного инцидента, связанного с цифровой безопасностью, для компаний среднего и малого бизнеса в Великобритании в среднем составлял составлял от 78 000 до 115 000 долларов США. На обеспечение кибербезопасности расходуется более 25 % бюджета таких предприятий. При этом не все структуры имеют кадровые и ресурсные возможности для управления рисками кибербезопасности, и далеко не все их сотрудники обладают необходимыми знаниями о них. По этой причине компании фокусируются в большей степени на вопросах операционной деятельности и поддержании финансовой стабильности, чем на управлении рисками кибербезопасности и развитии корпоративной культуры осведомленности о них[11]. С аналогичными сложностями сталкиваются и государственные учреждения. Таким образом, наблюдаемый устойчивый рост финансовых затрат и регуляторных мер в сфере кибербезопасности свидетельствует о ее переходе из технической плоскости в категорию стратегических приоритетов национальной безопасности.

6 Measuring digital security risk management practices in businesses. P. 5 https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/measuring-digital-security-risk-management-practices-in-businesses_d66dd6a6/7b93c1f1-en.pdf (далее – Measuring digital security)

7 Managing digital security and privacy risk. P. 14. https://www.oecd.org/content/dam/oecd/en/publications/reports/2016/06/managing-digital-security-and-privacy-risk_g17a2818/5jlwt49c-cklt-en.pdf (далее – Managing digital security)

8 Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть пятая. https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/

9 Обзор крупнейших киберинцидентов 2024 года. https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/

10 Утвержден распоряжением Правительства РФ от 14 августа 2025 года № 2207-р.

11 Managing digital security. P. 29.

Таблица. Основные риски кибербезопасности
Table. Key cybersecurity risks

Категория риска	Конкретные угрозы	Последствия	Меры защиты
Кибератаки на цифровую инфраструктуру	DDoS-атаки, целенаправленные кибератаки, программы-вымогатели и др.	Нарушение работы государственных органов и сервисов, ущерб экономике	Фаерволы, резервное копирование и др.
Утечка данных	Взломы баз данных, «фишинг», инсайдерские угрозы	Репутационные потери, угрозы безопасности жизни	Шифрование, двухфакторная аутентификация
Дезинформация	Недостоверная информация, боты и др.	Социальная дестабилизация, манипуляция общественным мнением	Мониторинг социальных сетей, проверка фактов, анализ информации с помощью цифровых технологий
Технологическая зависимость	Санкции на программное обеспечение (например, зарубежные операционные системы)	Сбои в работе государственных органов и организаций	Развитие отечественного ПО, импортозамещение
Кибершпионаж	Хакерские группы, государственный шпионаж	Угроза национальной безопасности, утрата конкурентных рыночных преимуществ	Криптография, сегментация сетей
Уязвимости устройств Интернета вещей	Взлом камер, датчиков и др.	Саботаж, слежка, аварии	Регулярные обновления, сетевой контроль
Нехватка кадров	Дефицит специалистов по кибербезопасности	Слабый ответ на угрозы	Программы профессиональной переподготовки кадров
Регуляторные риски	Нарушение законодательства о хранении данных, санкции и ограничения на технологии (экспортные ограничения, блокировка ПО), несоответствие отраслевым стандартам и др.	Штрафы за нарушения законодательства, судебные иски, блокировка сервисов, репутационные потери	Повышение уровня соблюдения законодательства, аудит данных, локализация технологий и данных, разработка собственных стандартов и т.д.

Источник: Составлено автором
Source: Compiled by the author

Управление рисками не может осуществляться изолированно и требует учета политического и социального контекстов. Кроме того, данный процесс должен обладать адаптивностью, позволяющей учитывать специфику конкретной ситуации [Renn, 2008. P. 353]. Эффективное управление рисками, вне зависимости от используемой методологии их оценки, должно обеспечивать решение следующих ключевых задач: идентификацию и систематизацию рисков, приемлемых для государства на стратегическом уровне; разработку комплексной матрицы, отражающей как актуальные, так и потенциальные угрозы; проведение вероятностного анализа и оценку потенциальных последствий реализованных рисков; построение аналитической модели для многофакторного исследования рисковых сценариев; а также классификацию рисков по критериям допустимости с определением оптимальных стратегий их минимизации. Данный подход позволяет сформировать системную основу для принятия обоснованных управленческих решений в области риск-менеджмента на государственном уровне[12].

В **таблице** представлены основные риски кибербезопасности, их последствия для государства и общества и возможные меры противодействия.

В настоящее время риски кибербезопасности постоянно увеличиваются, что обусловливает повышение требований к качеству государственного управления и используемым инструментам по управлению рисками в этой области. Предложенный список киберрисков является открытым и может быть дополнен в зависимости от сегмента экономики и специфики деятельности. Так, отдельные эксперты включают в него также риски прерывания обслуживания внутренних и внешних систем[13], риски кибермошенничества, риски в цепях поставок (поставщиков, подрядчиков и т.д.)[14], риски уязвимостей облачных продуктов, риски устаревшего программного обеспечения[15], риски социальной инженерии (см., например, [Ревенков, Бердюгин, 2017]), риски несовместимости цифровой инфраструктуры и программного обеспечения, риски цифровой инфраструктуры (устаревание оборудования или физическое воздействие).

Согласно докладу IBM Security и Института Ponemon за 2024 год, средний ущерб компании от утечки данных достиг 4,88 млн долларов США, что на 10 % превышает показатели предыдущего года. Исследование выявило, что организации, активно внедрявшие ис-

12 Risk taking: a corporate governance perspective. P. 28. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/895811468330941160

13 Cyber risk measurement and the holistic cybersecurity approach. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

14 How SOC reporting can help assess cybersecurity risk management in third-party relationships – and beyond. https://www.pwc.com/us/en/services/trust-solutions/digital-assurance-transparency/vendor-cybersecurity-risk.html

15 Today's top 10 cyber security threats. https://prowritersins.com/cyber-insurance-blog/top-10-common-cybersecurity-threats/

кусственный интеллект в системы защиты, смогли сократить потенциальные потери в среднем на 2,2 млн долларов. Более половины пострадавших организаций столкнулись с острой нехваткой специалистов по цифровой безопасности, что на 26,2 % больше, чем в 2023 году. Значительная часть инцидентов (35 %) была связана с использованием данных, находящихся за пределами защищенной системы управления данными, что подчеркивает трудности их контроля и защиты в условиях их распределенного хранения. Наиболее часто компрометировались персональные данные клиентов (46 % случаев). При этом привлечение правоохранительных органов в случае атак с использованием программ-вымогателей позволило сократить ущерб в среднем на 1 млн долларов; две трети организаций, воспользовавшихся такой помощью, избежали выплаты выкупа[16].

Согласно данным IBM, с марта 2024 года по февраль 2025 года средняя глобальная стоимость утечки данных снизилась на 9 % до 4,44 миллиона долларов, что стало первым снижением за пять лет. Основными факторами сокращения ущерба стали ускоренное выявление и сдерживание нарушений, обеспеченное внедрением искусственного интеллекта и автоматизации в процессы безопасности. Средний срок локализации и устранения последствий инцидента сократился до 241 дня, что на 17 дней меньше по сравнению с предыдущим годом. Несмотря на снижение собственных затрат на 2,35 миллиона долларов, сфера здравоохранения сохранила статус наиболее уязвимой отрасли с средним ущербом в 7,42 миллиона долларов. Наиболее распространенной причиной утечек оставались фишинговые атаки (16 %), на втором месте – компрометация цепочек поставок (15 %), на третьем – инциденты, связанные с компрометацией учетных данных[17].

В этой связи государствам необходимо соблюдать баланс между обеспечением собственной цифровой безопасности и снижением убытков, с одной стороны, и повышением своей конкурентоспособности, с другой. В качестве примера эффективных инструментов предотвращения киберугроз можно привести такие меры, как обеспечение регулярного обновления программных приложений, ограничение возможности государственным и муниципальным служащим устанавливать программное обеспечение или изменять параметры конфигурации компьютера.

Следует признать, что в цифровой среде риски кибербезопасности невозможно устранить полностью, однако ими можно управлять, уменьшая до приемлемого уровня. Оценка риска должна быть направлена на прогнозирование потенциальных последствий данной угрозы в отношении государства и других заинтересованных сторон, и цифровой экосистемы в целом.

Базовый алгоритм управления киберрисками

Для настоящего исследования был разработан базовый алгоритм управления киберрисками, который можно описать как последовательность управленческих действий:

- определение целей и задач;
- выявление киберрисков и определение приемлемого уровня риска (риск-аппетита);
- анализ и систематизация киберрисков;
- оценка и приоритизация киберрисков;
- разработка дорожной карты управления киберрисками;
- мониторинг процесса управления киберрисками;
- внесение изменений или дополнений в процессы управления.

Государству не всегда удается оперативно реагировать на происходящие изменения. Более того, результаты опросов показывают, что все чаще на практике у сотрудников организаций отсутствуют необходимые знания в области кибербезопасности, что обусловливает непонимание потенциальных рисков и своих потребностей в этой области.

Несмотря на то, что предприятия все больше погружаются в проблематику цифровых рисков, как правило, они рассматривают их с технической точки зрения. Это подчеркивает важность интеграции управления рисками кибербезопасности в процессы принятия экономических и социальных решений, что позволит всем заинтересованным сторонам минимизировать угрозы и максимально реализовать потенциал цифровой среды[18]. Методы управления такими рисками необходимо интегрировать в общую структуру управления рисками и принятия управленческих решений в государстве. При этом система управления такими рисками должна включать как технологические подходы, так и методы риск-менеджмента[19].

Анализ практики говорит о том, что большинство участников цифрового взаимодействия внедряют определенные правила кибербезопасности или используют определенные средства защиты. Основным инструментом, как правило, выступает программное обеспечение, которое защищает их от таких рисков. К иным вариантам относятся брандмауэры с соответствующими конфигурациями, ограничение ИТ-администрирования и прав доступа для конкретных пользователей, разрешение доступа только через корпоративные устройства, контроль безопасности на используемых устройствах (например, ноутбуках), отдельная беспроводная сеть, мониторинг активности пользователей, соблюдения правил хранения и

16 Cost of a data breach 2024: financial industry. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry (далее – Cost of a data breach 2024)

17 Более подробно см.: Cost of a data breach 2024.

18 OECD 2015. P. 19.

19 Measuring digital security. P. 29.

перемещения личных данных, безопасное резервное копирование данных с помощью других средств или облачных сервисов[20].

В контексте управления рисками кибербезопасности инновационные решения для снижения риска могут принимать различные формы, которые могут и не иметь отношение к цифровым аспектам деятельности государства. ОЭСР в рекомендациях по вопросам управления рисками цифровой безопасности призывает к системному внедрению инновационных решений в процессы управления киберрисками. Инновации должны стать ключевым инструментом достижения приемлемого уровня безопасности, определяемого при оценке рисков, что предполагает их обязательный учет при принятии управленческих решений на всех уровнях. При этом внедрение инновационных решений для уменьшения возможного влияния неопределенности на деятельность государства само по себе может создавать неопределенности, связанные с другими аспектами деятельности. По этой причине управление рисками должно быть интегрировано в общий процесс принятия управленческих решений[21].

Предлагаемый комплекс мер может служить основой для разработки общегосударственной системы кибербезопасности. Данный подход направлен на формирование адаптивной системы защиты, сочетающей технологические, правовые и организационные механизмы. Он включает: формирование единой стратегии и нормативной базы путем разработки государственного стандарта управления киберрисками, согласованного с целями цифровой трансформации и национального развития; институциональное развитие через закрепление персональной ответственности должностных лиц, создание специализированных организационных структур и проведение межведомственных координационных мероприятий; интеграцию риск-ориентированных подходов в процессы принятия управленческих решений с обязательной количественной и качественной оценкой киберрисков; технологическую модернизацию за счет внедрения инструментов анализа больших данных и искусственного интеллекта; систему непрерывного обучения и аттестации специалистов; ресурсное сопровождение, предусматривающее бюджетное финансирование и развитие сотрудничества с бизнес-сообществом, научными организациями и международными партнерами для обмена передовыми практиками в области цифровой безопасности. Результаты исследования свидетельствуют о необходимости дальнейшей детализации предложенных мер с учетом динамичного развития киберсреды и эволюции цифровых угроз.

20 Cyber security breaches survey 2019. P. 29.

21 OECD 2015. P. 11, 54–55.

Единая цифровая система внутреннего контроля и управления рисками

Внедрение цифровых технологий в сферу государственного управления повышает его прозрачность и подотчетность системы в целом. В условиях перехода к датацентричной экономике, использования новых методов управления и увеличения количества возникающих рисков особое значение для заинтересованных сторон приобретают управленческие практики и развитие риск-менеджмента, нацеленные на повышение качества корпоративной культуры в системе государственного управления.

Сетевое и децентрализованное взаимодействие заинтересованных сторон усложняют выбор правовой юрисдикции и затрудняет правоприменение, создавая сложности в части надзора и соблюдения нормативных требований[22]. В этом контексте мы предлагаем рассматривать внедрение цифровых технологий в управленческую деятельность в качестве стимула для трансформации методов и форматов реализации внутреннего контроля и управления рисками.

Автоматизация позволяет согласовывать контроль и управление рисками с управленческими процессами, одновременно повышая их эффективность [Bamberger, 2010. P. 686]. Она помогает выявлять риски на раннем этапе и обеспечивает более эффективное соблюдение нормативных требований, снижая как затраты на их осуществление, так и риск штрафных санкций за потенциальные нарушения законодательства [Arner, Barberis, Buckley, 2016. P. 375–376].

Получение ценности в результате внедрения такого подхода возможно при соблюдении трех условий: отслеживании и снижении затрат на внедрение цифрового контроля и управления рисками, увеличении масштаба инициатив в этой области, цифровизации процессов. Создаваемые информационные системы контроля автоматизируют действия в части управления цифровыми системами, выявления рисков и соответствия нормативным требованиям по широкому кругу вопросов (финансы, аудит, доступ к данным), распространяясь на всю создаваемую цифровую экосистему [Dameri, 2009. P. 32–34]. Как следствие, все более важное значение приобретает контроль и управление рисками при работе с большими данными, в первую очередь касающимися их безопасности и конфиденциальности. Эта деятельность подразумевает разработку соответствующих внутренних политик, процедур, стандартов и находит отражение в организационных изменениях[23].

22 Why decentralised finance (DeFi) matters and the policy implications. P. 43 https://www.eurofi.net/wp-content/uploads/2022/06/oecd_why-decentralised-finance-defi-matters-and-the-policy-implications_january2022.pdf (далее – Why DeFi matters)

23 Benefits of data governance and compliance https://www.datasciencecentral.com/benefits-of-data-governance-and-compliance/; The importance of data governance and compliance https://www.itgovernance.co.uk/blog/the-importance-of-data-governance-and-compliance

В текущих условиях эффективный контроль возможен лишь при условии комплексного анализа данных, формирующих основу управленческих процессов[24]. В этой связи все больше государственных и частных структур приходят к осознанию актуальности внедрения цифрового контроля и управления рисками[25].

Использование цифровых технологий позволяет значительно повысить эффективность государственного управления, охватить максимальное количество объектов проверки и контроля, интегрировать его с информационными системами управления, технологической архитектурой и цифровой инфраструктурой государства. Оно способствует усилению системы риск-менеджмента и оперативному реагированию на возникающие отклонения показателей в режиме реального времени, значительно повышая качество внутреннего контроля и управления рисками.

Внедрение цифровых технологий в данные процессы обеспечивает ряд преимуществ, включая повышение прозрачности и подотчетности управленческих процессов за счет автоматизированного мониторинга и контроля ключевых показателей; оптимизацию ресурсов через автоматизацию рутинных операций, что снижает количество ошибок ручного труда, сокращает долгосрочные затраты и высвобождает персонал для аналитической работы; качественное преобразование риск-менеджмента благодаря структурированному анализу данных, выявлению отклонений, формированию статистики в динамике и прогнозному моделированию; организационное развитие, проявляющееся в росте цифровых компетенций сотрудников и формировании цифровой корпоративной культуры. Данные преимущества создают синергетический эффект, обеспечивая не только операционную эффективность, но и совершенствование системы управления в стратегическом плане.

Представляется, что внедрение цифровых технологий в государственную деятельность в целях создания единой цифровой системы внутреннего контроля и управления рисками следует осуществлять поэтапно, последовательно достигая поставленных в дорожной карте целей и активно вовлекая в этот процесс различные структурные подразделения. Формирование единой цифровой системы внутреннего контроля и управления рисками в государственном управлении включает три последовательных этапа, обеспечивающих системную трансформацию управленческих процессов. На первом этапе создается централизованная система с унифицированными процессами, включающая декомпозицию контрольных задач, устранение дублирования функций, формализацию внутренних политик, разработку методологии оценки рисков, внедрение цифровых инструментов автоматизации и создание единого информационного пространства для аккумулирования результатов контроля. Второй этап предполагает разработку концепции интегрированной аналитической цифровой платформы, предусматривающую формирование межведомственной команды, согласование управленческих процессов, интеграцию с базами данных и системами риск-менеджмента, а также закрепление персональной ответственности за функциональными блоками платформы. На заключительном этапе создается единая цифровая система внутреннего контроля и управления рисками, включающая внедрение технологий искусственного интеллекта и машинного обучения, полную интеграцию с государственными информационными системами, обновление цифровых управленческих процессов и институционализацию ответственности структурных подразделений за конечные результаты. Ключевым системообразующим элементом на всех этапах выступает непрерывный сбор аналитических данных о качестве управленческих процессов, позволяющий выявлять ошибки, оптимизировать практику управления и актуализировать требования к развитию системы, что обеспечивает эволюционное совершенствование механизмов контроля и управления рисками в государственном секторе в режиме реального времени. Ключевая роль в создании такой единой цифровой системы управления принадлежит Правительству, которому необходимо не только разработать и утвердить принципы и подходы к ее организации, но и непосредственно принимать участие в реализации концепции на практике в целях управления киберрисками.

Развитие инструментов цифрового управления будет способствовать дальнейшей цифровой трансформации управленческих процессов в государствах и формированию ими собственных цифровых платформ и цифровых экосистем отраслевых платформ. В перспективе государства смогут разработать и использовать технологические инструменты контроля для внедрения в качестве узлов сети или на уровне смарт-контрактов. Так, например, логичным выглядит постепенное внедрение в деятельность государственных органов цифровых помощников по вопросу контроля и управления рисками. Кроме того, протокол в коде смарт-контрактов может непосредственно содержать требования по соблюдению нормативных требований. Децентрализованные механизмы управления позволяют создавать отчеты для соблюдения нормативных требований в режиме реального времени[26]. Данные

24 Integrating risks in business process models. https://core.ac.uk/download/pdf/301353094.pdf

25 Под «цифровым контролем и управлением рисками» автор понимает элемент системы управления в организации, направленный на согласование управленческих процессов для постоянного выявления и минимизации возникающих рисков с использованием цифровых технологий, включая искусственный интеллект, машинное обучение и аналитику данных в режиме реального времени.

26 Why DeFi matters. P. 58.

меры будут способствовать усилению кибербезопасности государства, обеспечивая защиту его суверенитета в новых условиях.

Обобщая вышеуказанные подходы, следует выделить следующие особенности развития контроля и управления рисками в системе государственного управления в настоящее время. Во-первых, высокий темп цифровой трансформации экономики стимулирует внедрение новых механизмов управления и риск-менеджмента, которые дополняют или изменяют имеющиеся опыт и инструменты. Во-вторых, цифровизация управленческой деятельности отражает тренд на усложнение работы органов государственной власти в цифровой экономике. В-третьих, активное внедрение цифровых технологий, в частности технологий искусственного интеллекта и больших данных, способствуют повышению качества управленческой деятельности.

Заключение

Проведенное исследование позволяет сделать следующие выводы. Во-первых, цифровая трансформация государственного управления требует создания общегосударственной системы кибербезопасности, поскольку фрагментарные подходы к управлению рисками не обеспечивают необходимого уровня защиты от киберугроз. Во-вторых, разработанный базовый алгоритм управления киберрисками и предложенная единая цифровая система внутреннего контроля и управления рисками способны обеспечить мониторинг киберугроз в режиме реального времени, автоматизировать процесс принятия решения и повысить устойчивость системы государственного управления в целом. В-третьих, успешная реализация предложенных мер напрямую зависит от системного внедрения инновационных решений на всех уровнях управления, что обусловлено динамичным характером цифровой среды и необходимостью постоянной адаптации защитных механизмов к новым вызовам. Полученные результаты создают методологическую основу для дальнейших исследований в области адаптивных систем кибербезопасности и разработки механизмов международного взаимодействия в сфере кибербезопасности.

Литература

Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания. *Национальные интересы: приоритеты и безопасность*. 2017. № 9 (354). С. 1747–1760. https://doi.org/10.24891/ni.13.9.1747. EDN: WTCYWU

Arner D.W., Barberis J.N., Buckley R.P. FinTech, RegTech and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business.* 2017. Vol. 37. No. 3. P. 371–413. In English

Bamberger K.A. Technologies of compliance: risk and regulation in a Digital Age. *Texas Law Review.* 2010. Vol. 88. No. 4. P. 669–739. In English

Dameri R.P. Improving the benefits of IT compliance using enterprise management information systems. *Electronic Journal of Information Systems Evaluation.* 2009. Vol. 12 (1). P. 27–38. In English

Edwards B., Hofmeyr S., Forrest S. Hype and heavy tails: a closer look at data breaches. *Journal of Cybersecurity.* 2016. Vol. 2. Issue 1. P. 3–14. https://doi.org/10.1093/cybsec/tyw003. In English

Renn O. Risk governance. Coping with uncertainty in a complex world. London: Earthscan. 2008. In English

References

Revenkov P.V., Berdyugin A.A. Social engineering as a source of risks in online banking services. *National interests: priorities and security*. 2017. No. 9 (354). P. 1747–1760. https://doi.org/10.24891/ni.13.9.1747. EDN: WTCYWU. In Russian

ИНФОРМАЦИЯ ОБ АВТОРЕ:

Александр Сергеевич Юхно, кандидат юридических наук, доцент, заведующий кафедрой государствоведения Института государственной службы и управления
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119571, Москва, проспект Вернадского, 82). E-mail: yukhno-as@ranepa.ru
https://orcid.org/0000-0003-2999-2982

Для цитирования: *Юхно А.С.* Кибербезопасность государства: внутренний контроль и управление рисками. *Государственная служба*. 2026. № 2. С. 6–13.

INFORMATION ABOUT THE AUTHOR:

Alexander S. Yukhno, Candidate of Sci. (Law), Associate Professor, Head of the Department of State Studies, Institute of Public Administration and Civil Service
Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119571, Russian Federation). E-mail: yukhno-as@ranepa.ru
https://orcid.org/0000-0003-2999-2982

For citation: *Yukhno A.S.* National cybersecurity: internal control and risk management. *Public Administration*. 2026. No. 2. P. 6–13.