УДК 004.3:681.518
DOI 10.17513/snt.40530

# РЕГЛАМЕНТАЦИЯ ПРОЦЕССОВ ОБСЛУЖИВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ИНСТРУМЕНТ СНИЖЕНИЯ ЭКСПЛУАТАЦИОННЫХ РИСКОВ В РЕГИОНАЛЬНОМ ГОСУДАРСТВЕННОМ УЧРЕЖДЕНИИ

**Салкин Д.А., Тявокина К.С., Палагин С.В., Звягинцев Н.А., Тюгашкин Д.А.**

*ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва», Россия, Саранск, e-mail: salkin_da@mail.ru*

В статье исследуется роль регламентации процессов обслуживания информационных систем в снижении эксплуатационных рисков региональных госучреждений. Цель настоящего исследования заключалась в разработке научно обоснованной модели регламента обслуживания информационной системы для региональных государственных учреждений, обеспечивающей системное снижение эксплуатационных рисков, повышение отказоустойчивости информационной системы, формализацию процедур управления инцидентами и обеспечение соответствия требованиям федерального законодательства Российской Федерации и нормативных документов. Для проведения исследования применялись методы анализа рисков Failure Mode and Effects Analysis, экспертной оценки, сравнительного анализа ключевых показателей эффективности до и после внедрения. В качестве материальной базы данного исследования выступают нормативные акты Российской Федерации, а также данные аудита информационной системы регионального учреждения из сферы социальной защиты. На основе системного анализа была разработана модель регламента, интегрирующая управление инцидентами, информационную безопасность и мониторинг. Показано, что регламентация процессов в организации существенно повышает качество обслуживания информационной системы в целом. Результаты исследования показали снижение времени простоя информационной системы, повышение доступности, сокращение инцидентов информационной безопасности. Доказано, что стандартизация процессов минимизирует человеческий фактор, обеспечивает соответствие федеральному законодательству Российской Федерации и нормативным документам, а также повышает удовлетворенность пользователей. Регламентация процессов обслуживания ИС продемонстрировала эффективность как комплексный механизм управления эксплуатационными рисками. Результаты работы могут выступать методологической базой для разработки типовых регламентов обслуживания информационных систем в госучреждениях, учитывающих специфику нагрузок и требования к работе с персональными данными.

**Ключевые слова: информационная система, эксплуатационные риски, регламент обслуживания, региональное госучреждение, стандартизация процессов**

# REGULATION OF INFORMATION SYSTEMS MAINTENANCE PROCESSES AS A TOOL FOR REDUCING OPERATIONAL RISKS IN A REGIONAL STATE INSTITUTION

**Salkin D.A., Tyavokina K.S., Palagin S.V., Zvyagintsev N.A., Tyugashkin D.A.**

*National Research Ogarev Mordovia State University, Russia, Saransk, e-mail: salkin_da@mail.ru*

The article examines the role of regulating information system maintenance processes in reducing operational risks in regional government agencies. The objective of this study was to develop a scientifically based model of information system maintenance regulations for regional government agencies that would systematically reduce operational risks, increase the fault tolerance of the information system, formalize incident management procedures, and ensure compliance with the requirements of federal legislation of the Russian Federation and regulatory documents. The study was conducted using the following methods: Failure Mode and Effects Analysis, expert assessment, and comparative analysis of key performance indicators before and after implementation. The material basis for this study is regulatory acts of the Russian Federation, as well as audit data of the information system of a regional institution in the field of social protection. Based on the systems analysis, a regulatory model was developed that integrates incident management, information security, and monitoring. It is shown that regulating processes in an organization significantly improves the quality of maintenance of the information system as a whole. The results of the study showed a decrease in the downtime of the information system, increased availability, and a reduction in information security incidents. It has been proven that process standardization minimizes human error, ensures compliance with Russian federal legislation and regulations, and improves user satisfaction. Regulating information system maintenance processes has demonstrated its effectiveness as a comprehensive mechanism for managing operational risks. The results of this work can serve as a methodological basis for developing standard regulations for information system maintenance in government agencies, taking into account the specific workloads and requirements for handling personal data.

**Keywords: information system, operational risks, maintenance regulations, regional government agency, process standardization**

## Введение

Интенсивная цифровизация государственных услуг сопровождается возрастанием эксплуатационных рисков информационных систем (ИС) в региональных учреждениях. Под эксплуатационными рисками понимается совокупность угроз, возникающих в процессе функционирования ИС и влияющих на их работоспособность, доступность и соответствие нормативным требованиям. К ним относятся аппаратные сбои, сбои программного обеспечения, ошибки персонала, инциденты информационной безопасности, а также риски, связанные с нарушением требований законодательства о защите информации и персональных данных.

Нестабильная работа ИС непосредственно угрожает качеству и непрерывности предоставления социально значимых услуг населению, а также влечет существенные финансовые, репутационные и правовые последствия, включая риск нарушения требований Федерального закона № 152-ФЗ «О персональных данных» [1]. В государственном секторе в большинстве случаев отсутствуют формализованные и стандартизированные процедуры обслуживания ИС. Этот фактор является ключевым в возникновении инцидентов, простоев и уязвимостей в сфере безопасности. Особенно остро проблема проявляется на региональном уровне, где зачастую эксплуатируются устаревшие (legacy) системы, ощущается дефицит высококвалифицированных ИТ-кадров, а существующие отраслевые регламенты либо отсутствуют, либо носят декларативный характер, не учитывая специфику нагрузок и требований к обработке персональных данных (ПДн).

В нормативной базе представлены фундаментальные подходы к управлению ИТ-сервисами [2] и информационной безопасностью [3; 4]. Научная литература, посвященная цифровизации государственного управления, предлагает оптимизационные модели цифрового управления в организационных структурах [5, с. 12–23; 6], а также методики оценки эффективности системы предоставления социальных услуг [7, с. 79–87; 8]. Ряд исследований [9-11] посвящен вопросам управления ИТ-рисками в организациях. Ведутся исследования в области оценки критичности рисков организации с применением современных нейросетевых технологий [12]. В области информационной безопасности в работах анализируется степень воздействия различных факторов на обеспечение информационной безопасности [13, с. 114–138], предлагаются методические подходы оценки рисков в информационной безопасности [14; 15]. Также ведется поиск эффективных инструментов для анализа и оценки рисков информационной безопасности бизнес-процессов [16]. Российское законодательство в области защиты информации устанавливает соответствующие требования (№ 149-ФЗ [17], № 152-ФЗ [1]). Однако, несмотря на обилие публикаций, в литературе представлено недостаточно решений, адаптированных к условиям региональных государственных учреждений. Отсутствуют методики интегрирования управления нагрузками в процессы обслуживания, что особенно критично для систем социальной защиты, характеризующихся регулярными всплесками активности. Недостаточно исследованы конкретные механизмы включения требований № 152-ФЗ и ГОСТ Р ИСО/МЭК 27001-2021 в операционные регламенты обслуживания ИС, обрабатывающих ПДн, с акцентом на предупреждение инцидентов. Реагирование на инциденты зачастую носит реактивный характер. Таким образом, разработка и внедрение регламентированных процессов обслуживания ИС представляется актуальной научно-практической задачей.

Разрабатываемый регламент обслуживания ИС должен обеспечивать не только снижение эксплуатационных рисков, но и повышать отказоустойчивость ИС. Под отказоустойчивостью понимается способность ИС сохранять работоспособность и доступность при возникновении отдельных отказов компонентов ИС или внешних воздействий.

**Цель исследования –** разработка научно обоснованной модели регламента обслуживания ИС для региональных госучреждений, обеспечивающей системное снижение эксплуатационных рисков, повышение отказоустойчивости ИС, формализацию процедур управления инцидентами и обеспечение соответствия требованиям № 152-ФЗ и ГОСТ Р ИСО/МЭК 27001-2021.

## Материалы и методы исследования

В качестве материальной базы данного исследования выступают:

− нормативная база: № 149-ФЗ, № 152-ФЗ, ГОСТ Р ИСО/МЭК 20000-1-2021, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р 51583-2014;

− данные аудита ИС регионального учреждения сферы соцзащиты (г. Саранск);

− научные публикации по управлению ИТ-рисками [18-20].

Для проведения исследования в работе применялись методы: анализ рисков FMEA, экспертных оценок, сравнительный ана-

лиз ключевых показателей эффективности (KPI) до/после внедрения.

Метод FMEA [21-23] выявляет скрытые риски до их реализации, позволяет увязать риски с требованиями № 152-ФЗ. Анализ рисков методом FMEA проводился в 5 этапов:

1) идентификация 17 функций ИС (авторизация, обработка ПДн, резервирование);

2) определение 23 потенциальных отказов;

3) определение показателей:

− Severity (S) – тяжесть последствий (1-10),

− Occurrence (O) – вероятность возникновения (1-10),

− Detection (D) – возможность обнаружения (1-10);

4) расчет приоритетного числа риска: $RPN = S \times O \times D$;

5) разработка корректирующих мер для рисков с $RPN > 100$.

Следует отметить, что каждый из показателей S, O и D принимает значения от 1 до 10. То есть максимальное значение приоритетного числа риска может достигать 1000 (10×10×10). Выбор порогового значения приоритетного числа риска (RPN) на уровне > 100 позволяет отфильтровать наиболее значимые риски, требующие первоочередного внимания. Порог $RPN > 100$ эквивалентен тому, что средняя оценка по каждому из параметров составляет примерно 4,7 балла. Это означает, что для превышения порога достаточно, чтобы риск обладал высокой тяжестью последствий ($S \geq 7$), или имел высокую вероятность возникновения ($O \geq 7$), или был трудно обнаруживаемым ($D \geq 7$), или имелась любая комбинация из достаточно высоких, но не экстремальных оценок. Таким образом, выбор порогового значения $RPN > 100$ на пятом этапе обусловлен необходимостью эффективно идентифицировать риски, представляющие наибольшую угрозу для отказоустойчивости и безопасности информационной системы, требующие разработки корректирующих мероприятий в первую очередь.

Экспертная оценка позволяет восполнить недостаток статистики и гарантирует работоспособность регламента в реалиях госсектора [24]. Она осуществлялась по следующей методике:

1. Формировалась выборка из 5 экспертов:

− 2 специалиста по информационной безопасности с опытом работы не менее 3 лет;

− 2 системных администратора с опытом работы не менее 5 лет;

− 1 руководитель ИТ-службы госучреждения.

2. Проводилось 3 этапа по методу Дельфи [25]:

− анонимная оценка регламента;

− анализ согласованности;

− выработка решений.

3. Производилась оценка по 10-балльной шкале:

− полнота разделов;

− соответствие № 152-ФЗ;

− практическая реализуемость.

Для сравнительного анализа KPI использовались такие метрики, как MTTR (Mean Time To Repair, среднее время простоя), доступность ИС (%), частота инцидентов ИБ (ед./квартал) и соблюдение SLA (%). Производился анализ по следующей методике. На первом этапе собирались данные за 6 месяцев до внедрения регламента, на втором – за 6 месяцев после внедрения регламента, затем рассчитывались относительные изменения по формуле

$$\Delta MTTR = (MTTR\_после – MTTR\_до) / MTTR\_до \times 100\%,$$

и проверялась статистическая значимость через t-критерий Стьюдента ($p<0.05$) [26].

В качестве количественных показателей отказоустойчивости ИС из вышеприведенных метрик KPI в данном исследовании использовались среднее время простоя (восстановления) (MTTR) и уровень доступности.

## Результаты исследования и их обсуждение

В рамках настоящего исследования для регионального государственного учреждения из сферы социальной защиты разработан типовой регламент обслуживания ИС. Разработка регламента для регионального уровня учитывала следующие ключевые аспекты.

1. Учет региональной специфики: уникальность инфраструктуры, используемых технологий и уровня квалификации персонала в каждом регионе.

2. Вовлечение заинтересованных сторон: необходимость участия в разработке ИТ-специалистов, специалистов по информационной безопасности (ИБ) и представителей пользовательских подразделений.

3. Соответствие нормативной базе: обязательное согласование с требованиями федерального законодательства, отраслевых стандартов и внутренних регламентов учреждения.

4. Обеспечение актуальности: регламентация периодического пересмотра документа в связи с изменениями законодательства, технологий и функциональных потребностей.

Разработка регламента включала следующие этапы:

− аудит текущего состояния ИС и процессов;

− идентификация рисков через FMEA;

− проектирование разделов регламента с механизмами снижения угроз;

− внедрение с интеграцией в системы мониторинга (Zabbix).

Разработанная модель регламента обслуживания ИС представляет собой нормативный документ, устанавливающий порядок выполнения работ по поддержанию работоспособности, развитию и модернизации информационных систем.

Типовая структура регламента обслуживания ИС для региональных государственных учреждений включает следующие основные разделы.

Общие положения: цель, область применения, используемые термины и определения, нормативные основания, основные принципы обслуживания, распределение зон ответственности, процедура актуализации документа.

Перечень обслуживаемых ИС: структурированный список информационных систем с указанием наименования, описания функциональности, версии, платформы, места размещения; ответственных лиц; перечня сопровождающей документации.

Организация обслуживания ИС: структура службы эксплуатации, функции и обязанности персонала, порядок взаимодействия; процедуры планового и внепланового обслуживания и технической поддержки; процессы управления инцидентами и проблемами; система контроля и отчетности; вопросы материально-технического обеспечения.

Управление информационной безопасностью: цели и задачи ИБ, нормативная база, организационные и технические меры обеспечения безопасности, процедуры управления доступом.

Мониторинг и отчетность: процедуры контроля состояния ИС, сбора метрик и формирования отчетности для анализа эффективности и принятия управленческих решений.

Апробация предложенного риск-ориентированного подхода к регламентации обслуживания ИС проведена в одном из региональных учреждений социальной защиты. Внедрение регламента способствует системному улучшению ключевых эксплуатационных характеристик ИС. Количественные результаты апробации, демонстрирующие значимую положительную динамику, представлены в таблице 1.

Из таблицы 1 можно заметить, что по всем ключевым показателям эффективности эксплуатации ИС наблюдается устойчивая положительная динамика. Среднее время простоя (MTTR) сократилось с 9,4 до 2,1 часа в месяц, что соответствует снижению на 78%. Следует отметить значимость данного результата, учитывая, что каждый час простоя системы обработки персональных данных влечет потенциальные штрафы в размере до 300 тыс. рублей в соответствии с требованиями № 152-ФЗ. Уровень доступности ИС повысился с 91% до 99,4%, что превысило первоначальный целевой показатель в 99,0%. Среднее время простоя (MTTR) и уровень доступности ИС позволяют количественно оценить эффективность предложенного регламента с точки зрения обеспечения бесперебойного предоставления государственных услуг населению.

Количество инцидентов информационной безопасности снизилось с 8 до 1 в квартал. Качественный анализ выявил, что 6 из 7 предотвращенных инцидентов были обусловлены человеческим фактором (ошибочные настройки прав доступа, несанкционированное использование съемных носителей). Соблюдение сроков технического обслуживания (ТО) увеличилось на 83%. В частности, эффективность процедур резервного копирования достигла 100% благодаря внедрению ежедневного копирования и еженедельного тестирования восстановления. Среднее время реакции на инциденты снизилось на 79% вследствие внедрения системы автоматизированного контроля соблюдения SLA.

**Таблица 1**

Количественная эффективность внедрения регламента

| Показатель | До внедрения | После внедрения | Отклонение (Δ,%) | Экономический эффект |
|---|---|---|---|---|
| Среднее время простоя ИС в месяц (MTTR) | 9,4 ч | 2,1 ч | -78% | 109500 руб./месяц |
| Уровень доступности ИС | 91% | 99,4% | +9,3% | |
| Количество инцидентов ИБ в квартал | 8 | 1 | -88% | 350000 руб./квартал |
| Соблюдение сроков ТО | 53% | 97% | +83% | |
| Среднее время реакции на инцидент (SLA) | 5,8 ч | 1,2 ч | -79% | |

Примечание: составлено авторами на основе полученных данных в ходе исследования.

Оценка экономического эффекта от сокращения времени простоя (методика расчета экономии от сокращения простоев: 7,3 ч × 50 пользователей × 300 руб./ч (средневзвешенная стоимость рабочего времени госслужащего)) показала прямую экономию в размере 109 500 руб./мес. Сумма предотвращенных убытков от ИБ-инцидентов составила 350 000 руб./квартал. Также снизились на 35% затраты на экстренный ремонт оборудования.

Таким образом, анализ количественных показателей обнаружил, что внедрение регламента привело к улучшению метрик отказоустойчивости (MTTR, уровень доступности), информационной безопасности (количество инцидентов), дисциплины эксплуатационных процессов (соблюдение сроков ТО) и эффективности службы поддержки (время реакции на инциденты).

Внедрение регламента также обусловило значимые качественные изменения:

1) снизилось влияния человеческого фактора:

− ошибки конфигурации сократились с 17 до 2 случаев в квартал,

− нарушения процедур резервного копирования снизились со 100% до 8%,

− полностью исключены случаи наличия активных учетных записей уволенных сотрудников («забытые» учетные записи);

2) улучшились процессы взаимодействия: количество конфликтов, связанных с размытостью ответственности, сократилось на 87% после четкого определения ролей (ответственный, подотчетный, консультирующий, информируемый) для каждого участника процесса;

3) оптимизирована работа ИТ-персонала: произошло качественное изменение распределения рабочего времени. До внедрения регламента распределение времени работы персонала было следующим: реагирование на аварии – 65%, документирование – 20%, плановые работы – 15%. После внедрения доля плановых работ и оптимизации процессов возросла до 78%, тогда как время на реагирование на аварии сократилось до 22%. Данный сдвиг свидетельствует о переходе от реактивной к проактивной модели управления ИТ-инфраструктурой;

4) повысилась удовлетворенность пользователей с 42% до 89%;

5) произошла оптимизация некоторых процессов. Интеграция управления изменениями и ИБ-контроля сократила время согласования обновлений с 14 дней до 3 часов. Автоматизированная система напоминаний о плановом ТО снизила количество пропущенных мероприятий с 31 до 2 случаев в месяц.

В данной работе все возможные риски функционирования ИС были разбиты на 4 категории, предложены механизмы снижения риска по каждой категории и проанализирована эффективность механизмов снижения рисков (табл. 2).

Снижению рисков функционирования ИС в рамках предложенного регламента обслуживания способствуют следующие ключевые технологические решения:

− многоуровневая эскалация оповещений в интеллектуальной системе мониторинга,

− реализация динамического SLA с автоматической адаптацией к нагрузкам.

Результаты исследования позволяют предложить для типовых региональных государственных учреждений следующие практические рекомендации:

1. Реализовать процедуру приоритизации рисков на основе следующего алгоритма:

а) выполнить анализ видов и последствий отказов (FMEA) в отношении всех ИС;

б) сфокусироваться на рисках с числом приоритета риска (RPN), превышающим 120;

в) применить компенсирующие контрмеры для устаревших legacy-систем.

**Таблица 2**

Сравнительная эффективность механизмов снижения рисков

| Категория риска | Механизм снижения риска | Эффективность, % | Пример реализации механизма снижения риска |
|---|---|---|---|
| Аппаратные сбои | Прогнозная аналитика + плановое ТО | 92 | Предсказание 93% отказов HDD за 14 дней |
| Человеческий фактор | Стандартизация + симуляционное обучение | 88 | VR-тренажер для отработки инцидентов |
| Кибератаки | Сегментация сети + поведенческий анализ | 95 | Блокировка 100% попыток программ-вымогателей |
| Юридические риски | Автоматизированный контроль № 152-ФЗ | 100 | Ежедневная проверка 32 параметров |

Примечание: составлено авторами на основе полученных данных в ходе исследования.

2. Внедрять регламент обслуживания поэтапно: в первую очередь – на системах, не соответствующих требованиям № 152-ФЗ, во вторую очередь – на сервисах, критичных по показателю времени простоя.

Ключевыми условиями успешного внедрения регламента в организации являются:

− интеграция его требований в должностные инструкции сотрудников,

− организация автоматизированного контроля выполнения SLA,

− регулярный пересмотр документа (с рекомендуемой периодичностью, например, 6 месяцев).

## Заключение

Регламентация процессов обслуживания ИС продемонстрировала эффективность как комплексный механизм управления эксплуатационными рисками. Ее внедрение обеспечивает: системное снижение простоев, повышение отказоустойчивости ИС и соблюдение законодательных норм. Формализация процедур уменьшает роль человеческого фактора и ускоряет устранение инцидентов.

Результаты работы составляют методологическую базу для разработки типовых регламентов обслуживания ИС в госучреждениях, учитывающих специфику нагрузок и требования к работе с персональными данными.

## Список литературы

1. Федеральный закон № 152-ФЗ «О персональных данных» (с изменениями и дополнениями) [Электронный ресурс]. URL: https://internet.garant.ru/#/document/12148567 (дата обращения: 06.06.2025).

2. ГОСТ Р ИСО/МЭК 20000-1-2021 «Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов». М.: Стандартинформ, 2022, 32 с.

3. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2022, 28 с.

4. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». М.: Стандартинформ, 2018, 20 с.

5. Львович Я.Е., Львович И.Я., Чопоров О.Н., Горячко В.В., Каширина И.Л., Сорокин С.О., Тишуков Б.Н., Михель А.А., Чернышов Б.А., Швиндт А.Н., Преображенский А.П., Сапожников Г.П., Львович Э.М., Львович К.И., Преображенский Ю П. Оптимизация цифрового управления в организационных системах: монография. Воронеж: ВИВТ, 2021. 191 с. URL: https://e.lanbook.com/book/219467 (дата обращения: 17.06.2025). ISBN: 978-5-4446-1550-8.

6. Львович К.И. Управление эффективностью деятельности персонала в условиях цифровой трансформации организационных систем // Моделирование, оптимизация и информационные технологии. 2020. № 8(3). URL: https://moit.vivt.ru/wp-content/uploads/2020/08/LvovichKI_3_20_1.pdf. DOI: 10.26102/2310-6018/2020.30.3.039.

7. Шапошников В.А. Зубкова Т.И., Скороходова Л.А. Современные аспекты реализации механизма межведомственного взаимодействия при оказании социальных услуг: монография / Под ред. В. А. Шапошникова. Екатеринбург: РГППУ, 2021. 140 с. URL: https://e.lanbook.com/book/332846 (дата обращения: 17.06.2025). ISBN: 978-5-8050-0717-1.

8. Шимановская Я.В. Подходы к оценке качества социальных услуг // ЦИТИСЭ. 2021. № 4(30). С. 34-45. URL: https://ma123.ru/ru/2021/10/id-0138-ru/ (дата обращения: 15.09.2025). DOI: 10.15350/2409-7616.2021.4.04. EDN: UEUGAL.

9. Тимофеева Т. Б., Коркмазов Р. К. Анализ и систематизация рисков, возникающих при внедрении корпоративных информационных систем в компаниях // Вестник университета. Секция: Компьютерные и информационные науки. 2025. № 4. С. 72-83. URL: https://vestnik.guu.ru/jour/article/view/6142/3336 (дата обращения: 15.09.2025). DOI: 10.26425/1816-4277-2025-4-72-83. EDN: PVQQXM.

10. Дмитриева М. А., Шедько Ю. Н. Цифровые тренды в стратегическом управлении и существующие ИТ-риски // Управленческие науки. 2023. Т. 13. № 2. С. 6-15. URL: https://managementscience.fa.ru/jour/article/view/448/358 (дата обращения: 15.09.2025). DOI: 10.26794/2304-022X-2023-13-2-6-15. EDN: CUPQOU.

11. Дудкина Е. В. Управление ИТ-рисками инфраструктурной организации РФ // Инновации и инвестиции. 2023. № 11. С. 69-73. URL: https://www.innovazia.ru/archive/55107/ (дата обращения: 15.09.2025). EDN: VBMLJU.

12. Чумакова Е.В., Корнеев Д.Г., Гаспариан М.С., Махов И.С. Оценка уровня критичности операционного риска банка на основе нейросетевых технологий // Прикладная информатика. 2023. Т. 18. № 2 (104). С. 103-115. URL: http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=2933 (дата обращения: 15.09.2025). DOI: 10.37791/2687-0649-2023-18-2-103-115. EDN: DFXCLQ.

13. Кухарский А.Н. Информационная безопасность политического процесса в системе государственного и муниципального управления: монография. Чита: ЗабГУ, 2021. 260 с. URL: https://e.lanbook.com/book/271505 (дата обращения: 17.06.2025). ISBN: 978-5-9293-2742-1.

14. Козырь Н.С. Методические подходы риск-менеджмента информационной безопасности // Научные труды КубГТУ. 2023. № 4. С. 99-109. URL: https://ntk.kubstu.ru/data/mc/0100/4667.pdf (дата обращения: 15.09.2025). EDN: AKOYEP.

15. Колычев В.Д., Буданов Н.А. Комплексная методика оценки рисков информационной безопасности в коммерческом банке // Безопасность информационных технологий. 2021. Т. 28. № 2. С. 83-97. URL: https://bit.spels.ru/index.php/bit/article/view/1346/1231 (дата обращения: 15.09.2025). DOI: 10.26583/bit.2021.2.08. EDN: MHMRJK.

16. Болдыревский П.Б. Кистанова Л.А. Анализ и оценка рисков информационной безопасности бизнес-процессов // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Экономические науки. 2023. № 4 (72). С. 18-24. URL: http://www.unn.ru/pages/e-library/vestnik_soc/18115942_2023_-_4(72)_unicode/2.pdf (дата обращения: 15.09.2025) DOI: 10.52452/18115942_2023_4_18. EDN: BAVRWM.

17. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) [Электронный ресурс]. URL: https://internet.garant.ru/#/document/12148555 (дата обращения: 06.06.2025).

18. Титов А.И. Управление рисками ИТ-проектов на основе компонентной структуры разрабатываемого программного обеспечения // Интеллектуальные технологии на транспорте. 2017. №4. С. 12-17. URL: https://cyberleninka.ru/article/n/upravlenie-riskami-it-proektov-na-osnove-komponentnoy-struktury-razrabatyvaemogo-programmnogo-obespecheniya (дата обращения: 06.06.2025).

19. Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности // Вест-

ник НГУ. Серия: Информационные технологии. 2011. Т. 9. Вып. 2. С. 80-89. URL: https://cyberleninka.ru/article/n/klassifikatsiya-riskov-informatsionnoy-bezopasnosti (дата обращения: 17.06.2025).

20. Соколов Д.А., Савченко Н.А., Соловьев М.В., Схведиани А.Е. Методика оценки рисков ИТ-проектов // Естественно-гуманитарные исследования. 2024. № 4 (54). URL: https://cyberleninka.ru/article/n/metodika-otsenki-riskov-it-proektov (дата обращения: 17.06.2025). EDN: YNWLNS.

21. Филатов В.В., Путина А.М. FMEA-анализ как комплексный метод управления качеством // Прикладные экономические исследования. 2022. № 1. С. 45-51. URL: https://cyberleninka.ru/article/n/fmea-analiz-kak-kompleksnyy-metod-upravleniya-kachestvom (дата обращения: 17.06.2025). DOI: 10.47576/2313-2086_2022_1_45.

22. Inaam Nasrallah, Ibtissam Sabbah, Chadia Haddad, Lina Ismaiil, Jana Kotaich, Pascale Salameh, Assem EL. Kak, Rihab Nasr, Wafa Bawab. Evaluating the academic scientific laboratories' safety by applying failure mode and effect analysis (FMEA) at the public university in Lebanon. 2023. V 9. I 12. P. 45-51. URL: https://www.sciencedirect.com/science/article/pii/S2405844023083536 (дата обращения: 20.08.2025). DOI: 10.1016/j.heliyon.2023.e21145.

23. Клочков А.Е. Методология FMEA для анализа рисков в системе АИСМК // Стандарты и качество. 2024. № 10. С. 86-89. URL: https://ria-stk.ru/stq/adetail.php?ID=235180 (дата обращения: 15.09.2025). EDN: RBSYKX.

24. Зацаринный А.А., Ионенков Ю.С. О применении экспертных методов при оценке эффективности и качества информационных систем // Системы и средства информатики. 2022. Т. 32. № 2. С. 47-57. URL: https://www.elibrary.ru/download/elibrary_48649631_65083749.pdf. DOI: 10.14357/08696527220205. EDN: NJDPAY.

25. Калашник Г.А., Попов Г.А. Современные методы согласования экспертных оценок // Современные научные исследования и инновации. 2022. № 6. URL: https://web.snauka.ru/issues/2022/06/98492 (дата обращения: 05.06.2025).

26. Григорьева А.В. Система ключевых показателей эффективности как инструмент принятия бизнес-решений // Современная экономика: проблемы и решения. 2024. № 2. С. 67-85. URL: https://e.lanbook.com/journal/issue/358640 (дата обращения: 17.06.2025).

**Конфликт интересов:** Авторы заявляют об отсутствии конфликта интересов.

**Conflict of interest:** The authors declare that there is no conflict of interest.