Утверждено

Директор Департамента цифровой трансформации и проектного менеджмента Министерства культуры и информации Республики Казахстан

_____ Токтагулов Е. Д.

«____»_____ 2026 г.

Утверждено

Директор

ТОО «Cuttle systems»

_____ Жайлыбаев Н.

«____»_____ 2026 г.

ОТЧЕТ ТЕХНИЧЕСКОГО АУДИТА

Информационной системы

«Единый электронный архив документов» (ИС ЕЭАД)

ЛИСТ УТВЕРЖДЕНИЯ

Договор №161040017107/260116/00 от 21.05.2026

Согласовано

Заместитель директора Департамента цифровой трансформации и проектного менеджмента Министерства культуры и информации Республики Казахстан

_____ Сыздыгалин Н.Н.

«____»_____ 2026 г.

Разработано

Директор по развитию

ТОО «Cuttle systems»

_____ Цой А.Е.

«____»_____ 2026 г.

г. Астана 2026 г.

Исполнители аудита

ФИО	Должность	Роль в проекте	Подпись
Цой Андрей Евгеньевич	Директор по развитию	Руководитель проекта	
Лукьянченко Андрей Григорьевич	Главный архитектор	Системный архитектор	
Нигиманова Айгерим Жуматаевна	Ведущий специалист по информационной безопасности	Аудит ИБ / системный аудитор	
Зейнолла Уәлихан Бағланұлы	Инженер инфраструктуры	Аудит инфраструктуры	
Асылбекұлы Бек	Системный аналитик	Технический аудит ИС	

АННОТАЦИЯ

Отчет — 98 с., 2 рис., 32 табл., 10 источников, 9 приложений.

КЛЮЧЕВЫЕ СЛОВА: технический аудит, информационная система, электронный архив, информационная безопасность, персональные данные, микросервисная архитектура, elasticsearch, электронная цифровая подпись, eol, гост 7.32-2017.

Объект исследования — информационная система «Единый электронный архив документов» (ИС ЕЭАД).

Цель работы — технический аудит системы по исходному коду, эксплуатационным журналам, предоставленным инфраструктурным данным и результатам нагрузочного тестирования с выявлением дефектов и рисков и подготовкой рекомендаций по их устранению.

Методы — ручной статический анализ исходного кода по десяти направлениям Технической спецификации; сверка сроков поддержки компонентов (EOL) с авторитетными источниками; перекрестная проверка автоматическим SAST-сканером; автоматизированный анализ журналов эксплуатации; анализ предоставленных инфраструктурных данных; нагрузочное тестирование на выделенном стенде.

Результаты — выявлено 116 находок (25 критических, 53 высоких, 27 средних, 11 низких); сформированы реестр рисков, матрица уязвимостей, таблица рекомендаций с ожидаемым эффектом и приоритизированный план мероприятий.

Область применения — приемка результатов аудита Заказчиком, планирование доработки и поэтапной модернизации системы.

СОДЕРЖАНИЕ

Исполнители аудита 2
АННОТАЦИЯ 3
ВВЕДЕНИЕ 9
Методология и охват аудита 10
1 Краткое резюме 13
1.1 Общая оценка состояния системы 13
1.2 Сильные стороны системы 13
1.3 Ключевые выводы 15
1.4 Топ-5 приоритетных действий 16
1.5 Последствия непринятия мер 17
2 Технический раздел 19
2.1 Общее заключение о состоянии системы 19
2.1.1 Работоспособность и архитектура 19
2.1.2 Соответствие нормативам 19
2.1.3 Уровень зрелости решений 20
2.2 Аппаратная часть 20
2.2.1 Инвентаризационная ведомость инфраструктуры 20
2.2.2 Соответствие мощностей фактической нагрузке 21
2.2.3 Уязвимости и узкие места 22
2.3 Программная часть 23
2.3.1 Анализ архитектуры ПО 23
2.3.2 Оценка производительности 24
2.3.3 Соответствие реализованного функционала ТЗ 24
2.4 Схемы архитектуры 25
2.5 Количественные и измеримые показатели 25
2.5.1 Анализ времени отклика 25
2.5.2 Оценка отказоустойчивости 25
2.5.3 Оценка резервного копирования (RPO/RTO) 26
2.5.4 Анализ нагрузочной устойчивости 27

3 Перечень выявленных проблем и рисков 28
3.1 Ключевые проблемные зоны и точки отказа 28
3.2 Реестр выявленных рисков 29
3.3 Матрица уязвимостей 30
4 Таблица рекомендаций с ожидаемым эффектом 31
5 Предложения по поэтапной оптимизации системы 41
5.1 Краткосрочные меры (до 1 месяца) 41
5.2 Среднесрочные меры (1–6 месяцев) 41
5.3 Долгосрочные меры (6+ месяцев) 41
5.4 Приоритизированный план мероприятий 42
5.5 Финансово-техническая оценка 42
ЗАКЛЮЧЕНИЕ 46
Приложения 48
Приложение А. Инвентаризационная ведомость инфраструктуры 49
А.1 Серверные мощности ЦОД АП 49
А.2 Ресурсы региональных узлов ЕЭАД 49
А.3 Сетевое оборудование (сегменты ЕТС ГО и Интернет) 50
Приложение Б. Схемы архитектуры 52
Приложение В. Исходные технические показатели 54
В.1 Объемы выделенных ресурсов ЕЭАД 54
В.2 Загруженность файловых систем региональных хранилищ 54
В.3 Прочие показатели 55
Приложение Г. Реестр выявленных рисков 56
Приложение Д. Матрица уязвимостей (Вероятность × Воздействие) 76
Приложение Е. Приоритизированный план мероприятий 78
Приложение Ж. Версии компонентов и сроки поддержки (EOL) 85
Приложение И. Анализ журналов эксплуатации 87
И.1 Сводные показатели 87
И.2 Категоризация ошибок (по классам дефектов) 88
И.3 Топ-проблемы — конкретные шаблоны сообщений 89
И.4 Рейтинг сервисов по ошибкам 90

И.5 Показатели по регионам (ЦОД) 91
И.6 Утечки ИИН по сервисам и тренд 92
И.7 Инвентарь брошенных .tmp (топ по размеру) 92
Приложение К. Результаты нагрузочного тестирования 95
Лист согласования 98

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчете применяются следующие обозначения и сокращения:

Сокращение	Расшифровка
ИС ЕЭАД	информационная система «Единый электронный архив документов» (предмет аудита; обозначение по Договору)
ЦОД АП	центр обработки данных Архива Президента
ИС	информационная система
ЦОД	центр обработки данных
АО «НИТ»	АО «Национальные информационные технологии» (оператор инфраструктуры)
МКИ	Министерство культуры и информации Республики Казахстан (Заказчик)
БИН	бизнес-идентификационный номер
ЕСЭДО	единая система электронного документооборота государственных органов
ШЭП	шлюз «электронного правительства»
ГБД ФЛ	государственная база данных «Физические лица»
ЕТС ГО	единая транспортная среда государственных органов
ИИН	индивидуальный идентификационный номер
ПД	персональные данные (Закон РК от 21.05.2013 № 94-V «О персональных данных и их защите»)
ЭЦП	электронная цифровая подпись
PKI	инфраструктура открытых ключей (Public Key Infrastructure)
ESB	интеграционная (сервисная) шина (Enterprise Service Bus)
NGFW	межсетевой экран нового поколения (Next-Generation Firewall)
IDS / IPS	система обнаружения / предотвращения вторжений
EOL	завершение жизненного цикла, прекращение поддержки программного обеспечения (End of Life)
OCR	оптическое распознавание символов
БПМ / BPM	управление бизнес-процессами (Business Process Management)
RPO / RTO	целевая точка / целевое время восстановления
RBAC	ролевое управление доступом (Role-Based Access Control)
JWT	веб-токен JSON (JSON Web Token)

Сокращение	Расшифровка
SAST	статический анализ защищенности кода (Static Application Security Testing)
CVE	общеизвестные уязвимости (Common Vulnerabilities and Exposures)

ВВЕДЕНИЕ

Технический аудит выполнен на основании Договора №161040017107/260116/00 от 21.05.2026 между ГУ «Министерство культуры и информации Республики Казахстан» (Заказчик) и ТОО «Cuttle systems» (Исполнитель). Объект аудита — государственная информационная система «Единый электронный архив документов» (ИС ЕЭАД), обеспечивающая хранение и предоставление доступа к официальным электронным документам Республики Казахстан.

Система построена по микросервисной архитектуре, интегрирована с государственными системами (ЕСЭДО, ОДО, ШЭП/СЭП, ГБД ФЛ) и использует национальную инфраструктуру электронной цифровой подписи. Эксплуатация системы с реальными персональными данными граждан предъявляет повышенные требования к информационной безопасности, надежности и соответствию законодательству Республики Казахстан, что определяет актуальность независимой технической оценки.

Цель аудита — оценить техническое состояние системы по исходному коду, эксплуатационным журналам и предоставленным инфраструктурным данным, выявить дефекты и риски и подготовить рекомендации по их устранению и поэтапной модернизации. Отчет включает краткое резюме для Заказчика, технический раздел, перечень выявленных рисков, рекомендации, предложения по оптимизации и обязательные приложения. Методология и охват аудита изложены в следующем разделе.

Методология и охват аудита

Предмет аудита: информационная система «Единый электронный архив документов» (ИС ЕЭАД). Аудит проведён комплексно: статический анализ исходного кода (без сборки и развёртывания), автоматизированный анализ эксплуатационных журналов, изучение предоставленных инфраструктурных данных, а также нагрузочное тестирование на выделенном стенде, идентичном промышленной среде.

Объем кодовой базы: 34 модуля Maven в каталоге sead/ (≈16 прикладных микросервисов + инфраструктурные сервисы Spring Cloud + общие библиотеки + frontend на Vue), интеграционная шина (sead-esb/esb, Apache Karaf/Camel/CXF), устаревший портал (sead-portal, WildFly; EJB+WAR+EAR, ~320 Java-классов). Дополнительно проанализированы журналы эксплуатации (966 млн строк) и инфраструктурные данные региональных ЦОД.

Дополнительно в охвате:

– эксплуатационные журналы по репрезентативной выборке региональных ЦОД за период март–июнь 2026 — фактическое подтверждение находок (Приложение И, находки LOG-001…LOG-008); поскольку во всех ЦОД развернута единая кодовая база (обособленные региональные системы на одинаковом ПО), выводы по проанализированным журналам репрезентативны для всех региональных инсталляций;

– инфраструктурные данные, полученные от АО «НИТ» (оператора инфраструктуры), по всем 16 ЦОД (серверные мощности, объемы ресурсов, загруженность файловых систем, IP-адресация, сетевые схемы) — Приложения А и В.

За рамками настоящего аудита (организационно-инфраструктурные вопросы оператора и заказчика):

– параметры электропитания;

– RPO/RTO и тестирование резервного копирования;

– аттестация и сертификация.

Применены следующие методы:

– ручной статический анализ исходного кода по десяти направлениям Технической спецификации (архитектура, версии/EOL, безопасность, интеграции, база данных, BPM, лицензирование, качество кода, клиентская часть, соответствие нормативным требованиям РК);

– сверка сроков поддержки (EOL) с авторитетными источниками (endoflife.date и официальные сайты производителей);

– перекрестная проверка результатов автоматическим SAST-сканером в качестве вспомогательного источника;

– автоматизированный анализ эксплуатационных журналов региональных ЦОД (ошибки, сбои интеграций, передача персональных данных в журналы);

– анализ предоставленных инфраструктурных данных (серверные мощности, загруженность хранилищ, сеть) и их сопоставление с результатами по коду и журналам;

– нагрузочное тестирование на выделенном стенде, идентичном промышленной среде (Apache JMeter; профили P0/P1/P2 по конфигурациям ЦОД; результаты — Приложение К).

Итоговые выводы и реестр рисков являются результатом аудита; программные средства использованы как вспомогательные.

Классификация рисков:

– критический (К) — потеря данных, недоступность системы, уязвимость безопасности, EOL без поддержки;

– высокий (B) — деградация производительности, частичная потеря данных, EOL-компонент, отсутствие обработки ошибок;

– средний (C) — проблемы качества кода, устаревшие, но поддерживаемые версии, отсутствие тестов;

– низкий (H) — стилевые проблемы, технический долг, пробелы в документации.

Ограничения:

– parent POM вне репозитория — часть версий не финализируема из кода;

– метрики времени выполнения (runtime) недоступны;

– лицензионное соответствие ABBYY FineReader и крипто-компонентов РК не верифицируемо из исходного кода.

1 Краткое резюме

1.1 Общая оценка состояния системы

Общая оценка: критическое состояние, требуется первоочередная доработка. ИС ЕЭАД функциональна и реализует требуемый объем задач государственного электронного архива, однако аудит исходного кода выявил серьезные дефекты безопасности, влияющие на защиту персональных данных граждан и юридическую значимость электронной подписи, а также массовое использование устаревших (EOL) компонентов без поддержки. Без устранения критических рисков система не может считаться безопасной для эксплуатации с реальными персональными данными.

Дополнительно проанализированы эксплуатационные журналы региональных ЦОД (966 млн строк) — они подтверждают выявленные дефекты на практике: зафиксировано более 220 млн ошибок (доминируют ошибки базы данных от единичного неисправного планового задания), а также утечка реальных персональных данных граждан (свыше 160 тыс. ИИН) в журналы — преимущественно в сервисе аудита. Часть проблем накапливается годами без устранения.

Всего выявлено находок: **116**. Распределение по критичности: **критические — 25, высокие — 53, средние — 27, низкие — 11**.

1.2 Сильные стороны системы

Наряду с выявленными дефектами, аудит подтверждает ряд объективных достоинств системы, которые служат прочной основой для доработки (а не замены):

– современная архитектура: микросервисный подход (≈16 сервисов) на Spring Boot + Spring Cloud (Eureka, Zuul, Config Server) с событийным

взаимодействием через Kafka — обеспечивает модульность, масштабируемость и независимое развертывание; выбор паттернов адекватен задачам государственного архива;

– функциональная полнота: реализован полный профиль электронного архива — управление документами, ЭЦП, апостиль, экспертиза ценности, читальный зал, отчетность; реализованный функционал соответствует Технической спецификации;

– глубокая интеграция с государственной экосистемой: ЕСЭДО, ОДО, ШЭП/СЭП, ГБД ФЛ, E-Otinish — система встроена в инфраструктуру электронного правительства РК;

– соответствие национальным криптотребованиям: для электронной подписи используется казахстанская PKI (Kalkan/GAMMA, KNCA), что отвечает требованиям РК к юридической значимости подписи;

– реализованы механизмы безопасности: аутентификация OAuth2/JWT, ролевая модель доступа, прикладная валидация входных данных на интеграциях (дефекты носят характер настройки и полноты, а не отсутствия механизмов);

– отказоустойчивая инфраструктура и изоляция регионов: обособленные региональные инсталляции (отказ в одном регионе не затрагивает остальные), БД в конфигурации «мастер + 2 ведомых узла», распределенное сетевое хранилище (чанк-ноды + металогер), межсетевые экраны NGFW в режиме High Availability, эшелонированная сетевая защита (Palo Alto/FortiGate/Cisco, IDS/IPS);

– асинхронная обработка нагрузки: значительная часть взаимодействий вынесена в Apache Kafka (20 топиков) — корректный подход к развязке сервисов и пропускной способности;

– стандартный, поддерживаемый стек технологий: PostgreSQL, Elasticsearch, Kafka, Camunda, Vue — массовые, хорошо документированные решения (проблема — устаревшие версии, а не сам выбор технологий), что упрощает сопровождение и подбор специалистов.

Совокупно это означает, что выявленные критические и высокие риски устранимы доработкой существующей системы; полная замена не требуется.

1.3 Ключевые выводы

– инфраструктура: по данным АО «НИТ» отражены серверные мощности, объемы ресурсов, загруженность файловых систем и сетевая архитектура (Приложения А, В); топология — обособленные региональные системы на единой кодовой базе при единой общей интеграционной шине;

– программное обеспечение: массовое использование устаревших компонентов без поддержки — Elasticsearch 6.4, Java 8, Spring Boot 2.x, Apache Camel 2.23, Camunda 7.11, Vue 2.7, WildFly 16; повышенный риск нерешаемых уязвимостей;

– безопасность: выявлены критические дефекты — приватные ключи ЭЦП и пароли в исходном коде/репозитории, отключение проверки TLS, XXE и SQL-инъекции, открытые без аутентификации сервисы, отсутствие ролевого контроля на уровне сервисов;

– соответствие нормативам: персональные данные (ИИН, ФИО) обрабатываются с существенными пробелами защиты (в журналах, в конфигурации, в поисковом индексе без шифрования) — риск несоответствия Закону РК «О персональных данных и их защите»;

– эксплуатация (по репрезентативной выборке журналов региональных ЦОД): одно неисправное плановое задание в сервисе хранения файлов порождает около 80% всех ошибок системы (свыше 99 млн отказов с каскадным

срывом транзакций БД); сервис хранения файлов — источник 99% ошибок; утечка реальных ИИН в журналы (свыше 160 тыс., из них 99% — в сервисе аудита) подтверждена фактически; дефекты не устранялись годами; журналы не ротируются и накапливают мусор (свыше 7 ГБ брошенных файлов);

– емкость хранилищ (данные по 16 ЦОД): файловые хранилища критически заполнены — 8 из 16 ЦОД на 90% и более, несколько на 100%; при полном заполнении возникает угроза невыполнения операций записи (прием документов, создание учетных записей, выдача архивных справок) и снижения производительности; требуется срочное увеличение емкости (INFRA-001);

– резервное копирование (данные АО «НИТ»): выполняется раз в месяц cron-скриптами, фактический RPO до 30 дней; загружаемые файлы пользователей на втором сервере приложений не резервируются (прямая связь с переполнением хранилищ) — критический риск потери юридически значимых документов; целевые RPO/RTO не определены (INFRA-002).

1.4 Топ-5 приоритетных действий

Соответствующие данные представлены в таблице 1.

Таблица 1 — Топ-5 приоритетных действий

#	Действие	Приоритет	Срок
1	Увеличить емкость файловых хранилищ: 8 из 16 ЦОД заполнены на 90%+, несколько — на 100%. При 100% возникает угроза невыполнения операций записи (прием документов, создание учетных записей, формирование и выдача архивных справок) и деградации производительности. Немедленно расширить хранилища переполненных ЦОД, восстановить автоочистку и обеспечить резервное копирование файлов пользователей, не покрытых текущим ежемесячным бэкапом (INFRA-001, INFRA-002, LOG-002)	Критический	Немедленно
2	Отозвать и перевыпустить все приватные ключи ЭЦП и секреты, обнаруженные в коде/конфигах/репозитории	Критический	Немедленно

#	Действие	Приоритет	Срок
	(SEC-001, SEC-005, SEC-025, PORTAL-001); перенести в защищенное хранилище		
3	Закрыть критические уязвимости доступа и каналов: открытые без аутентификации сервисы, анонимная смена пароля, отключенный TLS, XXE, SQL-инъекции (SEC-002/003/004/011/018, PORTAL-002/003/004)	Критический	2–4 недели
4	Привести обработку персональных данных в соответствие Закону РК: убрать ИИН/ПД из журналов (в первую очередь audit-service) и конфигов, защитить поисковый индекс и шифрование (SEC-008/009, LOG-001, DB-011/012/015, COMP-001)	Высокий	1–2 месяца
5	Устранить корневые дефекты эксплуатации: исправить неисправное плановое задание autoDeleteExpiredDeletedFiles и сбои OCR-обработки (дает ~80% ошибок), восстановить ротацию и очистку журналов (LOG-002/003/004/005)	Высокий	1–2 месяца

1.5 Последствия непринятия мер

Непринятие мер по устранению выявленных критических рисков влечет для Министерства как государственного органа следующие последствия:

– регуляторная ответственность — обработка персональных данных граждан (ИИН, ФИО) с пробелами защиты и их попадание в журналы не соответствуют Закону Республики Казахстан «О персональных данных и их защите», что влечет риск предписаний уполномоченного органа, приостановки обработки персональных данных и юридических претензий; компрометация ключей электронной подписи снижает юридическую значимость хранимых документов;

– нарушение непрерывности эксплуатации — переполнение файловых хранилищ (8 из 16 ЦОД заполнены на 90% и более) при резервном копировании один раз в месяц создает риск приостановки приема документов, выдачи архивных справок и потери данных;

– репутационные риски — раскрытие персональных данных граждан и компрометация национальной электронной подписи снижают доверие к государственному электронному архиву.

Ориентировочная оценка затрат на устранение выявленных рисков приведена в разделе 5.5 «Финансово-техническая оценка».

2 Технический раздел

2.1 Общее заключение о состоянии системы

2.1.1 Работоспособность и архитектура

Система реализована в виде микросервисной архитектуры (≈16 прикладных микросервисов Spring Boot + инфраструктурные сервисы Spring Cloud) с интеграционной шиной (ESB на Apache Karaf/Camel) и устаревшим порталом на WildFly. Маршрутизация внешнего трафика — через API-шлюз Zuul (gateway-service); реестр сервисов — Eureka (discovery-service); централизованная конфигурация — Config Server (config-service) с хранением в каталоге properties-yaml. Асинхронное взаимодействие — через Apache Kafka (20 топиков). Интеграции: ЕСЭДО, E-Otinish, ГБДФЛ, ШЭП/СЭП (через ESB, протоколы CXF/SOAP и Kafka). Топология развертывания — обособленные региональные системы на единой кодовой базе: в каждом ЦОД области/города работает автономный экземпляр ИС ЕЭАД (собственные данные, БД и хранилище); региональные системы между собой не взаимодействуют, обмен данными ведется только с внешними системами через единую общую интеграционную шину ESB. Работоспособность системы подтверждается полнотой реализации; архитектурные дефекты — нарушение принципа «база данных на сервис» (11 сервисов делят БД sead-docs) и циклические зависимости между сервисами.

2.1.2 Соответствие нормативам

Соответствующие данные представлены в таблице 2.

Таблица 2 — Соответствие нормативам

Норматив / требование	Статус	Комментарий
Техническое задание (Annex 2)	Частично	Функционал реализован; выявлены отступления по безопасности и качеству
Закон РК «О персональных данных»	Не соответствует	ИИН/ПД в журналах, конфигах, незащищенном индексе (COMP-001)
Госстандарты РК (СТ РК)	[не верифицировано из кода]	Подтверждается аттестатом соответствия; вне предмета аудита по коду
ISO 27001 (ИБ)	[не верифицировано из кода]	Критические дефекты ИБ указывают на несоответствие практик
ИКТ-регламенты МЦиАП/NITEC	[не верифицировано из кода]	Сертификация не подтверждается из исходного кода
Резидентность данных (РК)	Подтверждается	Данные размещены в ЦОД АО «НИТ» на территории РК (16 региональных ЦОД, включая ЦОД АП; госсеть ЕТС ГО) — см. Приложения А, В

2.1.3 Уровень зрелости решений

Зрелость архитектурных решений — средняя: применены современные на момент разработки паттерны (микросервисы, event-driven, централизованная конфигурация), однако технологический стек устарел и в значительной части вышел из поддержки (см. раздел 2.3.1 и Приложение Ж). Практики безопасной разработки (управление секретами, защита парсинга, ролевой контроль, тестовое покрытие) реализованы неудовлетворительно.

2.2 Аппаратная часть

Инфраструктурные данные настоящего раздела (серверные мощности, объемы ресурсов, загруженность файловых систем, IP-адресация, сетевые схемы) получены от оператора инфраструктуры — АО «Национальные информационные технологии» (АО «НИТ») — и сведены в Приложениях А и В.

2.2.1 Инвентаризационная ведомость инфраструктуры

По инвентаризационным данным, полученным от АО «НИТ», ЦОД АП (Архива Президента) включает 14 серверов — приложения (2 ноды), БД (мастер + 2 слейва), распределенное сетевое хранилище (3 чанк-ноды + металогер), поиск Elasticsearch (3 ноды), сервер распознавания (OCR), сервер БПМ (Camunda) и сервер интеграционной шины ESB. Суммарно ЦОД АП: 98 ядер CPU, 288 ГБ RAM, 14.9 ТБ диск. Топология развертывания — обособленные региональные системы на единой кодовой базе: в каждом из 16+ ЦОД областей/городов РК работает автономный экземпляр ИС ЕЭАД (собственный стек микросервисов, БД и хранилище), при этом региональные системы между собой не взаимодействуют; интеграционная шина ESB — единая общая для всех региональных систем. Полная ведомость — Приложение А, объемы ресурсов — Приложение В.

2.2.2 Соответствие мощностей фактической нагрузке

Соответствующие данные представлены в таблице 3.

Таблица 3 — Соответствие мощностей фактической нагрузке

Компонент	**Установлено**	**Факт. нагрузка / утилизация**	**Оценка**
CPU	ЦОД АП 98 ядер; регионы 826 ядер	В пределах выделенных ресурсов под текущей нагрузкой	Норма; рекомендуется мониторинг утилизации
RAM	ЦОД АП 288 ГБ; регионы 7 342 ГБ	В пределах выделенных ресурсов под текущей нагрузкой	Норма; рекомендуется мониторинг утилизации
Диски (хранилища)	Региональные хранилища 3–32 ТБ на ЦОД (Прил. В)	8 из 16 ЦОД ≥90% заполнения (несколько на 100%)	Критично — переполнение, связь с LOG-002
Сеть	NGFW Palo Alto/FortiGate/Cisco; канал ЕТС ГО 12 288 кбит/с	Загрузка канала 53.7% (узел Нацархива)	В норме

2.2.3 Уязвимости и узкие места

Главное узкое место — дисковое: 8 из 16 региональных хранилищ заполнены на 90% и более, несколько — на 100% (Восточно-Казахстанская область, г.Алматы, Костанайская область, Атырауская область, г.Шымкент, Западно-Казахстанская область и др.). Это напрямую связано с находкой LOG-002: неисправное плановое задание autoDeleteExpiredDeletedFiles не удаляет просроченные файлы, и хранилища переполняются. Поскольку во всех ЦОД работает единая кодовая база (обособленные региональные системы), данное задание выполняется и отказывает в каждой региональной инсталляции независимо — отсюда переполнение хранилищ во многих ЦОД одновременно. Требуется немедленное увеличение емкости файловых хранилищ переполненных ЦОД (находка INFRA-001). При 100% заполнении возникает угроза невыполнения операций, требующих записи: сохранение документов, создание учетных записей пользователей, формирование и выдача архивных справок. Технически это проявляется как каскад ошибок PostgreSQL «current transaction is aborted» (вторая по частоте ошибка в журналах — свыше 60 млн записей): после первой неуспешной записи транзакция переходит в состояние отмены и последующие операции в ней не выполняются. Дополнительный риск — деградация производительности (нехватка свободного места под временные данные и журналы СУБД). Расширение емкости хранилищ и восстановление автоочистки просроченных файлов (LOG-002) — взаимодополняющие, одинаково обязательные меры. Сетевое резервирование: межсетевые экраны NGFW работают в режиме горячего резерва/High availability.

Резервное копирование реализовано через cron-скрипты с периодичностью один раз в месяц. На каждом регионе выделен отдельный диск, монтируемый в /backups по NFS на остальные серверы; резервируются приложения, логи, базы данных и данные Elasticsearch. Фактический RPO составляет до 30 дней, что

создает высокий риск потери данных и не отвечает требованиям к государственной информационной системе, обрабатывающей юридически значимые документы и персональные данные граждан. Загружаемые файлы пользователей на втором сервере приложений не резервируются из-за нехватки дискового пространства (прямая связь с INFRA-001) — только синхронизируются на резервный стенд без гарантий полного восстановления. Отсутствует централизованная система управления резервным копированием с мониторингом выполнения заданий и алертингом при сбоях; резервные копии персональных данных формируются вне централизованного контроля доступа, что усиливает регуляторный риск (INFRA-002, COMP-001).

2.3 Программная часть

2.3.1 Анализ архитектуры ПО

Соответствующие данные представлены в таблице 4.

Таблица 4 — Анализ архитектуры программного обеспечения

Компонент	**Версия / технология**	**Статус лицензии**	**Оценка состояния**
Ядро (микросервисы)	Java 8, Spring Boot 2.x, Spring Cloud	Open source (Apache 2.0)	Устаревшее (EOL), требует обновления
База данных	PostgreSQL + Hibernate 5.4 + Liquibase 3.8	Open source	Устаревшее; дефекты схемы/индексов
Поиск	Elasticsearch 6.4.2 (Transport Client)	Open source	Критически устаревшее (EOL)
Интеграции (ESB)	Karaf 4.2 + Camel 2.23 + CXF 3.x + Kafka	Open source	Устаревшее (EOL)
BPM	Camunda 7.11 Community	Community (EOL 10.2025)	Устаревшее
OCR / отчеты	ABBYY FineReader Engine 12; JasperReports 6.7	ABBYY — коммерческая; Jasper — LGPL	ABBYY устар./не верифиц.; Jasper OK

Компонент	Версия / технология	Статус лицензии	Оценка состояния
Криптография	Kalkan PKI, GAMMA, KNCA (РК)	Проприетарная (РК)	Требует подтверждения договоров
Веб-интерфейс	Vue 2.7 + Vuex + Element UI	Open source (MIT)	Устаревшее (EOL 12.2023)
Устаревший портал	WildFly 16 + Spring 5.1 + CXF 3.2	Open source	Устаревшее (EOL), критич. дефекты ИБ

2.3.2 Оценка производительности

Производительность оценена нагрузочным тестированием на выделенном стенде (Apache JMeter; профили P0/P1/P2 по конфигурациям ЦОД) — полные результаты приведены в Приложении К. Тестирование эмпирически подтвердило риски, выявленные по коду: выборка документов дела деградирует сверхлинейно из-за коррелированного подзапроса по иерархии документов без индекса (DB-008, DB-009) со сложностью, близкой к квадратичной; узкое место — база данных (CPU 90–100%, пул соединений исчерпан) и пул потоков шлюза (QA-004). Авторизация узким местом не является.

Соответствующие данные представлены в таблице 5.

Таблица 5 — Производительность ключевых операций (по нагрузочному тестированию)

Операция	Показатель (по тесту)	Целевой ориентир	Оценка
Авторизация (oauth2)	0,4–0,6 с	≤ 1 с	В норме
Выборка дела (1 000 док.)	7,5–11 с (медиана)	≤ 2 с	Деградация
Выборка дела (≥ 20 000 док.)	отказ (504)	—	Отказ
Выборка дела (50 польз., 1 000 док.)	p95 = таймаут; ошибок 6–45%	—	Критично

Порог отказа (504) задан таймаутом шлюза (~60 с) и носит алгоритмический характер — от тира оборудования не зависит (см. Приложение К).

2.3.3 Соответствие реализованного функционала ТЗ

Реализованный функционал (управление документами, ЭЦП, апостиль, экспертиза, читальный зал, отчетность, интеграции с госсистемами) в целом соответствует профилю государственного электронного архива и требованиям ТЗ. Отступления носят характер качества и безопасности реализации, а не отсутствия функций.

2.4 Схемы архитектуры

Логическая и физическая схемы архитектуры приведены в Приложении Б (рисунок 1 и рисунок 2).

2.5 Количественные и измеримые показатели

2.5.1 Анализ времени отклика

По результатам нагрузочного тестирования (Приложение К): авторизация выполняется за 0,4–0,6 с (в норме); выборка документов дела занимает 7,5–11 с уже на деле в 1 000 документов (деградация), а при ≥ 20 000 документов завершается отказом (504) по таймауту шлюза (~60 с). Под конкурентной нагрузкой (50 одновременных пользователей) 95-й перцентиль выборки достигает таймаута. Детальные показатели по профилям ЦОД приведены в Приложении К.

2.5.2 Оценка отказоустойчивости

По данным, полученным от АО «НИТ», на уровне отказоустойчивости (горячее резервирование и репликация) предусмотрено:

– база данных — мастер и 2 ведомых узла (репликация);

– хранилище — распределенное (3 чанк-ноды и металогер);

– сеть — межсетевые экраны NGFW в режиме High availability / горячего резерва;

– резерв ЕЭАД — Астана и регионы (Приложение В).

Резервное копирование (создание резервных копий данных) — отдельный механизм, рассмотренный в разделе 2.5.3; не следует смешивать его с отказоустойчивостью и репликацией выше. Вместе с тем реальный риск отказа создает переполнение хранилищ: 8 из 16 ЦОД заполнены на 90%+ (связь с LOG-002). Из кода: Eureka self-preservation отключен; retry/redelivery в ESB через БД.

2.5.3 Оценка резервного копирования (RPO/RTO)

По данным оператора инфраструктуры, резервное копирование выполняется cron-скриптами по расписанию раз в месяц. На каждом регионе выделен отдельный диск, монтируемый в /backups по NFS; резервируются приложения, логи приложений, базы данных, логи БД и данные Elasticsearch. Загружаемые файлы пользователей на втором сервере приложений не резервируются — только синхронизируются на резервный стенд. Целевые значения RPO и RTO операционными регламентами не определены; фактический RPO, исходя из периодичности резервного копирования, составляет до 30 дней (находка INFRA-002).

Соответствующие данные представлены в таблице 6.

Таблица 6 — Оценка резервного копирования (RPO/RTO)

Параметр	Текущее значение	Целевой ориентир	Оценка
RPO (целевая точка восстановления)	до 30 дней (расчетный, по периодичности копирования)	≤ 24 часа	Не соответствует
RTO (целевое время восстановления)	не определен регламентами	≤ 4 часа	Требует определения
Частота резервного копирования	1 раз в месяц (cron по расписанию)	Ежедневно + непрерывное журналирование транзакций БД	Не соответствует
Покрытие резервного копирования	приложения, логи, БД, логи БД, Elasticsearch;	Полное покрытие всех компонентов	Не соответствует

Параметр	Текущее значение	Целевой ориентир	Оценка
	файлы пользователей — частично (только синхронизация)		
Метод резервного копирования	cron-скрипты, монтирование /backups по NFS	Централизованная система с мониторингом и алертингом	Не соответствует
Тестирование восстановления	регламент не зафиксирован	Не реже 1 раза в квартал	Требует подтверждения

Рекомендации по приведению резервного копирования к целевым ориентирам — меры ОР.1–ОР.3 (Приложение Е); находка INFRA-002.

2.5.4 Анализ нагрузочной устойчивости

Проведено нагрузочное тестирование на выделенном стенде, идентичном промышленной среде (Apache JMeter), по профилям P0/P1/P2, соответствующим конфигурациям ЦОД; полные результаты — Приложение К. Ключевые выводы: при 50 одновременных пользователях на делах по 1 000 документов система насыщается — доля ошибок 504 составляет около 6% на усиленной конфигурации (P2), около 15% на ЦОД АП (P0) и около 45% на базовой группе (P1, фактически неработоспособна). Узкое место — база данных (CPU 90–100%, пул соединений 100/100 исчерпан) и пул потоков шлюза. Первопричина алгоритмическая (коррелированный подзапрос по иерархии документов без индекса, квадратичная сложность) — увеличение тира оборудования ее не устраняет (DB-008, DB-009, QA-004). На ЦОД со 100% заполнением файловых хранилищ нагрузочное тестирование невозможно из-за отсутствия места под тестовые данные (INFRA-001). Дизайн асинхронной обработки прослеживается по конфигурации Kafka (20 топиков, идемпотентность части продюсеров).

3 Перечень выявленных проблем и рисков

3.1 Ключевые проблемные зоны и точки отказа

Ниже выявленные проблемы сгруппированы по направлениям Технической спецификации (п. 3.4) со ссылками на находки реестра (Приложение Г).

Точки возможного отказа:

– общая база данных sead-docs, используемая 11 сервисами, — единая точка отказа на уровне данных (ARCH-001);

– единая общая интеграционная шина ESB на все региональные системы;

– отключен режим самосохранения Eureka;

– синхронные цепочки вызовов Feign без предохранителей — риск каскадных отказов (QA-004);

– переполнение файловых хранилищ и каскад прерванных транзакций БД (INFRA-001, LOG-002);

– пропускная способность канала ЕТС ГО;

– резервное копирование и параметры восстановления (RPO/RTO) требуют формализации и регламента; рекомендуемые ориентиры и меры — Приложение Е (OP.1–OP.3).

Устаревшее или неподдерживаемое программное обеспечение. Массовое использование компонентов, снятых с поддержки (EOL): Java 8, Spring Boot 2.x, Elasticsearch 6.4, Apache Camel 2.23, Camunda 7.11, Vue 2.7, WildFly 16 (находки VER-001…VER-008, перечень сроков поддержки — Приложение Ж). Повышенный риск нерешаемых уязвимостей и проблем совместимости.

Потенциальные риски потери данных:

– отказ операций записи при 100% заполнении файловых хранилищ (INFRA-001);

– каскадные сбои транзакций PostgreSQL (LOG-002);

– журнал аудита не иммутабелен, фиксируются нарушения ограничений БД при записи аудита — риск пропуска событий (SEC-015, LOG-007);

– захардкоженный ключ шифрования ИИН/ФИО — риск утраты доступа к данным при компрометации или потере ключа (DB-015);

– использование SHA-1 для контроля целостности файлов (SEC-020);

– резервное копирование раз в месяц (фактический RPO до 30 дней) с неполным покрытием — файлы пользователей на втором сервере приложений не резервируются (INFRA-002).

Несоответствие нормативам и законодательным требованиям:

– обработка персональных данных с существенными пробелами защиты — риск несоответствия Закону Республики Казахстан «О персональных данных и их защите»: ИИН и ПД в журналах, конфигурации и поисковом индексе (COMP-001, COMP-002);

– иммутабельность и полнота журналирования операций не гарантированы (COMP-003);

– сертификация и аттестация (ISO 27001, СТ РК, регламенты МЦиАП/NITEC) не подтверждаются из исходного кода и находятся вне предмета настоящего аудита (COMP-004).

3.2 Реестр выявленных рисков

По результатам аудита выявлено 116 находок: **критических — 25, высоких — 53, средних — 27, низких — 11.** Полный реестр с описанием,

компонентом, доказательством (файл:строка), вероятностью, критичностью и рекомендацией приведен в **Приложении Г** (альбомная ориентация).

3.3 Матрица уязвимостей

Матрица «Вероятность × Воздействие» с распределением идентификаторов рисков приведена в **Приложении Д** (альбомная ориентация).

4 Таблица рекомендаций с ожидаемым эффектом

Приведены рекомендации по критическим и высоким рискам (полный перечень рекомендаций — в реестре, Приложение Г).

Соответствующие данные представлены в таблице 7.

Таблица 7 — Рекомендации по критическим и высоким рискам с ожидаемым эффектом

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
1	ARCH-001. Разделить БД по доменам, ввести API-границы	11 сервисов / БД sead-docs	Отказ одного сервиса не блокирует работу остальных; независимое развертывание и масштабирование сервисов	Высокий
2	ARCH-002. Развязать через события Kafka/рефакторинг	service-client	Устранение циклических зависимостей; сервисы развертываются и обновляются независимо	Высокий
3	VER-001. Миграция на поддерживаемую ES/OpenSearch	Elasticsearch 6.4.2	Закрытие известных CVE Elasticsearch; восстановление официальной поддержки и обновлений безопасности	Критический
4	VER-003. План обновления Java 17 + Spring Boot 3	Java 8 / Spring Boot 2.x	Переход на LTS-платформу с долгосрочной поддержкой; снижение технического долга всей кодовой базы	Высокий
5	VER-004. Обновление ESB до поддерживаемых версий	Camel 2.23 / Karaf 4.2 / CXF 3.x	Устранение EOL-рисков интеграционной шины; совместимость с актуальными версиями госсистем	Высокий
6	VER-005. Миграция клиентской части (frontend) на Vue 3 с обновлением зависимостей	Vue 2.7 + экосистема	Закрытие клиентских CVE (XSS, прототип-загрязнение); поддержка актуальных браузеров	Высокий

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
7	VER-006. Поэтапное обновление	Hibernate 5.4 / Liquibase 3.8 / POI 3.17 / Camunda 7.11	Устранение EOL-рисков Hibernate, Camunda и вспомогательных библиотек; совместимость с обновленными платформами	Высокий
8	SEC-001. Отозвать/перевыпустить ключ; HSM/Vault	sign-service.yml	Устранение риска компрометации ключа ЭЦП; восстановление юридической значимости электронных подписей	Критический
9	SEC-002. disallow-doctype-decl, отключить внешние сущности	integration-service-common/XmlUtils.java	Устранение XXE-уязвимости в пяти XML-парсерах; предотвращение чтения произвольных файлов сервера	Критический
10	SEC-003. Убрать /**, требовать JWT	sead-socket-service	Закрытие анонимного доступа ко всем эндпоинтам; требование аутентификации для любого запроса	Критический
11	SEC-004. Закрыть аутентификацией/авторизацией	OAuth2ResourceServerAutoConfiguration	Устранение анонимной смены пароля и проверки ИИН без аутентификации	Критический
12	SEC-005. Вынести в Vault/env, ротация, RS256	application.yml	Устранение захардкоженного ключа подписи JWT; ротация и перевод на асимметричный алгоритм RS256	Высокий
13	SEC-006. Уникальные секреты, короткий TTL, отзыв токенов	oauth2-service.yml	Исключение перекрестного использования OAuth2-секретов; снижение TTL токенов с 416 дней до безопасного значения	Высокий
14	SEC-007. Секрет-хранилище, ротация	properties-yaml	Вынос всех учетных данных из конфигурационных файлов в защищенное хранилище	Высокий
15	SEC-008. Маскирование, убрать ПД из журналов	sign/reference/audit	Прекращение утечки 160 тыс. ИИН в журналы; соответствие Закону РК «О персональных данных и их защите»	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
16	SEC-009. Убрать ПД из конфига	application.yml	Удаление 37 реальных ИИН граждан из конфигурационного файла	Высокий
17	SEC-010. Обосновать для stateless API; включить где есть сессии	Spring Security	Устранение глобального отключения CSRF там где используются сессии	Высокий
18	SEC-011. @PreAuthorize во всех сервисах (defense-in-depth)	gateway + 9 сервисов	Проверка ролей на уровне каждого сервиса; устранение возможности обхода авторизации через прямой вызов API	Критический
19	SEC-012. Resource-server + роль аудитора	audit-service	Ограничение доступа к журналу аудита ролью аудитора; исключение несанкционированного чтения	Высокий
20	SEC-013. Перепроверка подписи при выдаче/экспорте	document-service	Проверка ЭЦП при каждой выдаче документа; исключение выдачи документов с поврежденной или отозванной подписью	Высокий
21	SEC-015. Append-only журнал, хэш-цепочка целостности	audit-service	Иммутабельный журнал аудита с контролем целостности; невозможность задним числом удалить или изменить записи	Высокий
22	SEC-017. SASL/TLS, закрыть Kafdrop, фиксировать тег	ESB docker-compose	Аутентификация брокера Kafka; закрытие панели Kafdrop от внешнего доступа	Высокий
23	SEC-018. Удалить turnOffSslChecking; truststore УЦ РК	sign-service/SignApplication.java	Устранение глобального доверия всем TLS-сертификатам; проверка сертификатов госшлюзов	Критический
24	SEC-019. Убрать defaultTyping; allow-list типов	service-common/KafkaJsonSerialization.java	Устранение риска удаленного выполнения кода (RCE) через небезопасную десериализацию JSON	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
25	SEC-020. Перейти на SHA-256	file-storage-core	Замена устаревшего SHA-1 на SHA-256 для контроля целостности архивных файлов	Высокий
26	SEC-022. Throttling/CAPTCHA на auth-эндпоинты	oauth2/gateway	Защита от перебора паролей и энумерации ИИН на auth-эндпоинтах	Высокий
27	SEC-023. Секрет-хранилище, разные учетные данные dev/prod	document-service/EsedoComponent.java	Вынос учетных данных ЕСЭДО из кода; разделение учетных данных dev/prod	Высокий
28	SEC-025. Сменить пароль, SSH/секреты, включить SSL	config-service/bootstrap.yml	Замена открытого пароля git Config Server; включение SSL для репозитория конфигураций	Критический
29	SEC-026. Закрыть Basic/OAuth2; доступ сервис-к-сервису	discovery-service/config-service	Закрытие Eureka и Config Server аутентификацией; доступ только для доверенных сервисов	Высокий
30	SEC-027. Добавить проверку роли и организации	report/reading-room/expertise	Проверка принадлежности объекта организации пользователя на всех чувствительных эндпоинтах	Высокий
31	INT-001. try/catch + ErrorHandler + DLQ	notification/reference listeners	Гарантированная обработка событий Kafka; сообщения не теряются при сбое консьюмера	Высокий
32	INT-003. Секрет-хранилище	EsedoComponent	Вынос учетных данных ЕСЭДО из кода; устранение дублирования SEC-023	Высокий
33	INT-004. onException + таймауты	ESB SHEP2	Таймаут и обработка ошибок синхронного вызова ШЭП; предотвращение зависания ESB-маршрута	Высокий

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
34	INT-006. Подтвердить TLS/mTLS; защитить XML; не логировать ИИН	integration-service	Подтверждение TLS на каналах с ГБД ФЛ; исключение ИИН из журналов интеграций	Высокий
35	INT-007. Перевести интеграцию с ОДО на асинхронное взаимодействие (очередь/событие, неблокирующий вызов с ретраями и DLQ); вынести внешний вызов из обработчика Kafka	document-service / InventoryDocumentComponent (интеграция с ОДО)	Асинхронная интеграция с ОДО; блокирующий Feign-вызов не останавливает Kafka-консьюмер	Высокий
36	DB-008. LAZY + EntityGraph + batch_size	document-service-domain	Устранение N+1 запросов; снижение нагрузки на БД при выборке документов дела	Высокий
37	DB-009. saveAll, предзагрузка коллекций	AcceptanceReportServiceImpl.java	Пакетная запись вместо одиночных INSERT; снижение нагрузки на пул соединений БД	Высокий
38	DB-011. Минимизация ПД в ES, ролевой доступ	document-service / ES	Минимизация персональных данных в поисковом индексе; ролевой доступ к Elasticsearch	Высокий
39	DB-012. Миграция, TLS + аутентификация	Elasticsearch 6.4.2	Шифрование соединения с Elasticsearch; аутентификация всех клиентов индекса	Критический
40	DB-013. Частичные индексы WHERE deleted=false	db-changelog	Ускорение фильтрации по ~1 140 soft-delete запросам за счет частичного индекса	Высокий
41	DB-015. Ключ в Vault/KMS, ротация, перешифрование	apostille-service/ApostilleRequest.java	Вынос ключа шифрования ИИН/ФИО в KMS; устранение риска утраты доступа к данным при компрометации ключа	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
42	DB-016. Переписать запрос (одним проходом либо рекурсивным CTE); добавить индексы на таблицу связей иерархии; пагинация выборки; circuit-breaker на шлюзе	document-service / GET /documents/deal/{id}	Снижение времени выборки дела с 7–11 с до менее 2 с; устранение отказов 504 при ≥ 20 000 документов	Высокий
43	BPM-001. План обновления/миграции Camunda	bpm-service	Переход Camunda на поддерживаемый релиз; устранение EOL-рисков платформы BPM	Высокий
44	BPM-002. XSD-валидация + авторизация деплоя	BpmProcessServiceImpl.java	Валидация BPMN-схем перед деплоем; невозможность задеплоить некорректный процесс без авторизации	Высокий
45	BPM-003. history.time.to.live + cleanup	bpm-service	Ограничение роста таблиц истории ACT_HI_*; предотвращение переполнения БД от накопленных записей процессов	Высокий
46	QA-001. Логирование исключений; запрет пустых catch	FoundationServiceImpl и др.	Проглоченные исключения становятся видимыми в журналах; сокращение времени диагностики инцидентов	Высокий
47	QA-002. Минимальное покрытие критичных сервисов, порог в CI	все сервисы	Базовое тестовое покрытие критичных сервисов; регрессии выявляются в CI до выхода в продуктив	Высокий
48	FE-001. План миграции на поддерживаемые версии	vue-frontend/package.json	Устранение CVE клиентского стека; переход на поддерживаемые версии Vue и библиотек	Высокий
49	FE-002. httpOnly secure cookies для токенов	vue-frontend	Токены недоступны из JavaScript; кража токенов через XSS становится невозможной	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
50	FE-003. Контроль истечения на сервере (JWT exp)	vue-frontend/api.axios.js	Срок сессии контролируется сервером; клиент не может продлить сессию подделкой локального состояния	Высокий
51	FE-004. Вынести адреса в env/gateway	vue-frontend	Устранение захардкоженного IP файлового сервера из активного кода frontend	Высокий
52	FE-005. Санитизация (DOMPurify), CSP	vue-frontend/Search.vue	Санитизация HTML-вывода; закрытие XSS через v-html и dangerouslyUseHTMLString	Высокий
53	COMP-001. Программа защиты ПД (шифрование, маскирование, доступ)	ПД в целом	Системное устранение пробелов защиты ПД: шифрование, маскирование, ролевой доступ; соответствие Закону РК «О персональных данных и их защите»	Критический
54	COMP-002. Ролевой доступ к ПД на всех сервисах	RBAC/ПД	Ролевое разграничение доступа к ПД на всех сервисах; исключение несанкционированного доступа к персональным данным	Высокий
55	PORTAL-001. Отозвать ключ, удалить .p12 из VCS, HSM	seadportal/SignService.java + .p12	Устранение скомпрометированного ключа ЭЦП портала; удаление .p12 из репозитория	Критический
56	PORTAL-002. security-constraint/login-config по ролям	seadportal/web.xml	Закрытие всех admin-сервлетов аутентификацией; устранение открытого доступа к административным функциям	Критический
57	PORTAL-003. Убрать trust-all, truststore шлюза	seadportal/ServicesBean.java	Устранение глобального trust-all при обмене с госшлюзом СЭП/ШЭП	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
58	PORTAL-004. Параметризовать запросы	seadportal/UsersBean.java	Устранение SQL/JPQL-инъекции в портале через параметризацию запросов	Критический
59	PORTAL-005. Запрет DOCTYPE/внешних сущностей	seadportal/XmlUtils.java	Закрытие XXE в XML-парсерах портала	Высокий
60	PORTAL-006. Доверять заголовкам только от прокси; enforce сессию	seadportal/IpAddressFilter.java	Устранение доверия подделываемым заголовкам IP; принудительная проверка сессии	Высокий
61	PORTAL-007. Валидация Origin против белого списка	seadportal/Configurator.java	Защита WebSocket от CSWSH; валидация Origin по белому списку	Высокий
62	PORTAL-008. Отказ от нативной сериализации/allow-list	seadportal/XmlUtils,FileUtil	Устранение небезопасной Java-десериализации; предотвращение RCE через readObject	Высокий
63	PORTAL-009. Вынести учетные данные; удалить недокументированную функцию обхода	seadportal/pom.xml,WSseadportal.java	Вынос учетных данных БД из кода; удаление закомментированного backdoor adminlogin	Высокий
64	PORTAL-010. Перевести на TLS с проверкой сертификата	seadportal/Constants.java	Перевод интеграции с госшлюзом на TLS; устранение передачи данных по незащищенному http	Высокий
65	PORTAL-011. Миграция на поддерживаемые версии	seadportal (платформа)	Переход на поддерживаемую платформу или вывод из эксплуатации; устранение EOL-стека WildFly 16	Высокий
66	SEC-028. Проверка владения/организации на каждый доступ по ID	контроллеры (reading-room и др.)	Устранение IDOR — невозможность получить доступ к чужим сущностям по прямому идентификатору	Критический

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
67	SEC-029. Вынести учетные данные в секрет-хранилище; запрет хардкода в CI	apostille/document/integration/reference + портал	Устранение захардкоженных паролей в 11+ файлах backend и портала; запрет хардкода в CI	Критический
68	SEC-030. PreparedStatement; ревизия raw-SQL в ESB	sead-esb/RedeliveryProcessor.java	Устранение SQL-инъекции в ESB через параметризацию запросов	Высокий
69	SEC-031. Случайный пароль + смена при первом входе	document-service/AdminUserImportServiceImpl.java	Исключение импорта пользователей с единым предсказуемым паролем Password1$	Высокий
70	SEC-032. Единая безопасная XML-фабрика на весь проект	ESB/document-xlsx/портал	Единая защита от XXE по всему проекту (ESB, документы, портал)	Критический
71	LOG-001. Маскирование ПД на уровне логгера (в первую очередь audit); запрет логирования тел ответов ГБД	audit-service	Прекращение записи 158 тыс. ИИН в журналы audit-service; маскирование ПД на уровне логгера	Критический
72	LOG-002. Исправить транзакционность job (транзакция на элемент, обработка FK); алертинг на отказ плановых задач	file-storage / ScheduledFileStorage	Устранение ~80% всех ошибок системы (99 млн сбоев job); восстановление автоочистки просроченных файлов	Критический
73	LOG-003. Диагностировать IOException (ABBYY/диск/формат), валидировать вход OCR, устранить NPE	file-storage / RecognizeServiceImpl (OCR)	Устранение 8,6 млн OCR-ошибок; диагностика и исправление сбоев распознавания файлов	Высокий
74	LOG-004. Устранить корневые дефекты; ротация и лимиты live-логов; мониторинг доли ERROR	Эксплуатация / ротация журналов	Ротация live-журналов; устранение накопления 720 млн строк стектрейсов за несколько лет	Высокий
75	LOG-005. Очистка .tmp/cleanHistoryOnStart; централизация журналов;	Инфраструктура логирования (logback)	Очистка 294 брошенных .tmp-файлов (7,16 ГБ); восстановление нормальной ротации журналов	Высокий

№	Рекомендация	Компонент	Ожидаемый эффект	Приоритет
	расследование незавершенных ротаций			
76	LOG-006. Circuit-breaker/timeout/backoff для Feign; DLQ для Kafka; алертинг на всплески	document/integration/gateway (интеграции)	Снижение 1,14 млн сбоев интеграций; предохранители и DLQ предотвращают каскадные отказы	Высокий
77	INFRA-001. Немедленно увеличить емкость файловых хранилищ в переполненных ЦОД (приоритет — заполненные на 100%); параллельно устранить LOG-002 (восстановить автоочистку просроченных файлов) и внедрить мониторинг/алертинг заполнения с пороговыми уведомлениями	Файловые хранилища региональных ЦОД (сетевое хранилище / file-storage)	Устранение 100% заполнения в 6 ЦОД; восстановление возможности приема документов и создания учетных записей	Критический
78	INFRA-002. Перейти на ежедневное резервное копирование с непрерывным журналированием транзакций БД; обеспечить полное покрытие загружаемых файлов пользователей; внедрить централизованную систему резервного копирования с мониторингом выполнения заданий и алертингом; определить и зафиксировать целевые RPO и RTO (меры OP.1–OP.3, Приложение E)	Инфраструктура резервного копирования (все региональные ЦОД)	Снижение RPO с 30 дней до ≤ 24 часов; полное покрытие резервного копирования включая файлы пользователей	Критический

5 Предложения по поэтапной оптимизации системы

5.1 Краткосрочные меры (до 1 месяца)

– отозвать/перевыпустить приватные ключи ЭЦП и все секреты из кода/репозитория; перенести в Vault/переменные окружения (SEC-001, SEC-005, SEC-006, SEC-007, SEC-023, SEC-025, DB-015, PORTAL-001, PORTAL-009);

– закрыть открытые без аутентификации сервисы и анонимные операции; убрать permitAll("/**"), защитить смену пароля и check-iin (SEC-003, SEC-004, PORTAL-002);

– исправить XXE, SQL-инъекции и небезопасную десериализацию; восстановить проверку TLS (SEC-002, SEC-018, SEC-019, PORTAL-003, PORTAL-004, PORTAL-005);

– прекратить вывод ИИН/ПД в журналы и убрать реальные ИИН из конфигурации (SEC-008, SEC-009, PORTAL-012).

5.2 Среднесрочные меры (1–6 месяцев)

– внедрить ролевой контроль доступа (RBAC) на уровне всех сервисов; защитить Eureka/Config Server; обеспечить иммутабельность журнала аудита (SEC-011, SEC-012, SEC-015, SEC-026, SEC-027, COMP-002);

– защитить Elasticsearch (TLS+аутентификация), минимизировать ПД в индексе; устранить N+1 и добавить недостающие индексы (DB-008..014);

– повысить надежность интеграций: обработка ошибок Kafka-консьюмеров, DLQ/retry, таймауты (INT-001, INT-002, INT-004); TTL истории Camunda и валидация деплоя BPMN (BPM-002, BPM-003);

– улучшить качество: убрать пустые catch, ввести базовое тестовое покрытие, circuit-breaker, единую обработку ошибок; устранить риски frontend (httpOnly-cookies, CSP, санитизация) (QA-001/002/004, FE-002/003/005).

5.3 Долгосрочные меры (6+ месяцев)

– обновление EOL-стека: Elasticsearch/OpenSearch, Java 17 + Spring Boot 3, Apache Camel 3/4, Camunda, Vue 3, WildFly (или вывод портала) (VER-001..006, BPM-001, FE-001, PORTAL-011);

– рефакторинг архитектуры данных: разделение БД по доменам, развязка циклических зависимостей через события (ARCH-001, ARCH-002);

– решение по устаревшему порталу (WildFly): миграция на Spring Boot или вывод из эксплуатации (ARCH-003).

5.4 Приоритизированный план мероприятий

Приоритизированный план мероприятий приведен в **Приложении Е**.

5.5 Финансово-техническая оценка

Оценка ориентировочная. Работы выполняются командой специалистов (аналитик, архитектор, разработчики, инженеры по тестированию, DevOps-инженер, руководитель проекта); трудоемкость приведена в человеко-часах команды и включает полный цикл работ — анализ, разработку, тестирование, миграцию данных и приемку. Стоимость рассчитана в текущих ценах с учетом налогов и сопутствующих расходов (НДС 16%). Расширение емкости файловых хранилищ — отдельная инфраструктурная статья затрат (закупка и расширение СХД для переполненных ЦОД), определяется требуемым объемом дозакупки и в стоимость работ команды не входит; лицензии ABBYY FineReader и криптокомпонентов РК оцениваются отдельно по условиям правообладателей.

В соответствии с требованием Технической спецификации (п. 3.5) ниже приведен сравнительный анализ: доработка компонентов в сравнении с их заменой.

Соответствующие данные представлены в таблице 8.

Таблица 8 — Сравнительный анализ: доработка компонентов в сравнении с заменой

Компонент	Вариант А (доработка)	Вариант Б (замена / обновление)	Рекомендация
Elasticsearch 6.4 (EOL)	Настройка TLS и аутентификации поверх версии 6.4; компонент остается без поддержки	Миграция на OpenSearch / Elasticsearch 8, переход с Transport Client на REST API	Замена (EOL)
Платформа Java 8 / Spring Boot 2.x (EOL)	Платная продленная поддержка — внешние лицензионные затраты, временная мера	Обновление до Java 17 LTS и Spring Boot 3 по всем сервисам	Обновление (плановое)
ESB: Apache Camel 2.23 / Karaf 4.2 (EOL)	Сохранение текущих версий, риски накапливаются	Обновление до Camel 4 и актуального Karaf	Обновление
Camunda 7.11 Community (EOL)	Сохранение версии без обновлений	Обновление до поддерживаемого релиза	Обновление
Vue 2.7 и экосистема (EOL)	Точечные исправления, известные уязвимости сохраняются	Миграция на Vue 3 с обновлением библиотек	Замена / миграция
Портал на WildFly 16 (EOL, критические дефекты ИБ)	Исправление дефектов ИБ на текущей платформе (учтено в строке дефектов кода)	Миграция на современную платформу или вывод из эксплуатации	Вывод из эксплуатации с переносом функционала
Дефекты кода и конфигурации (ИБ, персональные данные, эксплуатация, БД, интеграции)	Устранение доработкой существующего кода	Замена не применима	Доработка

Вариант А по EOL-компонентам описывает сценарий сохранения текущей версии с минимальными доработками и является временной мерой; обновление до актуальной версии соответствует Варианту Б и включено в рекомендуемую программу модернизации. Стоимостные оценки приведены в таблице стоимости работ ниже.

Диапазон оценки обусловлен неопределенностью объема скрытых межкомпонентных зависимостей (11 сервисов используют общую базу данных sead-docs), степенью регрессий при обновлении EOL-компонентов и фактическим состоянием интеграций с внешними государственными системами, выявляемым в ходе выполнения работ.

Соответствующие данные представлены в таблице 9.

Таблица 9 — Ориентировочная стоимость работ по этапам

Направление работ	Горизонт	Трудоемкость, чел.-ч	Ориентировочная стоимость
Устранение критических дефектов ИБ: ключи ЭЦП, TLS, XXE, SQL-инъекции, открытые сервисы	Немедленно	400–800	9–18 млн ₸
Устранение утечки персональных данных: маскирование ИИН, вынос из журналов	Немедленно	400–600	9–14 млн ₸
Устранение дефектов эксплуатации: job autoDelete, OCR-сбои, ротация журналов	Немедленно	400–800	9–18 млн ₸
RBAC на уровне сервисов, иммутабельный аудит-лог	1–6 мес.	800–1 200	18–27 млн ₸
Надежность интеграций: DLQ, retry, таймауты Kafka/ESB	1–6 мес.	600–1 000	14–23 млн ₸
Производительность БД: индексы, коррелированный подзапрос, N+1	1–6 мес.	600–1 000	14–23 млн ₸
Camunda, frontend (cookies, CSP, санитизация)	1–6 мес.	800–1 400	18–32 млн ₸
Доработка дефектов (итого)	Немедленно — 6 мес.	4 000–6 800	91–155 млн ₸
Elasticsearch 6.4 → OpenSearch	6+ мес.	1 200–2 000	27–45 млн ₸
Java 8 + Spring Boot 2.x → Java 17 + Spring Boot 3.x	6+ мес.	1 600–2 400	36–54 млн ₸
Apache Camel 2.23 + Karaf 4.2 → Camel 4.x	6+ мес.	800–1 600	18–36 млн ₸
Camunda 7.11 → поддерживаемый релиз	6+ мес.	200–350	4–7 млн ₸
Vue 2.7 → Vue 3.x + Element Plus	6+ мес.	800–1 200	18–27 млн ₸
WildFly 16 / sead-portal → вывод из эксплуатации	6+ мес.	1 200–2 000	27–45 млн ₸
Рефакторинг архитектуры данных: разделение БД, развязка циклов	6+ мес.	1 600–2 800	36–63 млн ₸
Обновление EOL-стека и архитектуры (итого)	6+ мес.	7 400–12 350	166–277 млн ₸
Модернизация существующей системы (итого)	до 14 мес.	11 400–19 150	257–432 млн ₸
Полная замена системы (для сравнения)	≈ 14–30 мес.	22 700–37 800	510–850 млн ₸

Стратегический вывод: устранение критических и высоких рисков безопасности и эксплуатации достигается преимущественно доработкой существующего кода. Модернизация существующей системы (доработка

дефектов и поэтапное обновление EOL-компонентов) оценивается в 257–432 млн ₸ и приблизительно вдвое дешевле полной замены (510–850 млн ₸) при существенно меньших рисках и сроках. Расширение емкости файловых хранилищ является отдельной инфраструктурной статьей затрат.

ЗАКЛЮЧЕНИЕ

По результатам технического аудита информационной системы «Единый электронный архив документов» (ИС ЕЭАД) выявлено 116 находок (25 критических, 53 высоких, 27 средних, 11 низких). Система функциональна и в целом соответствует профилю государственного электронного архива, однако содержит критические дефекты информационной безопасности (приватные ключи и секреты в исходном коде, отключение проверки TLS, уязвимости XXE и SQL-инъекций, открытые без аутентификации сервисы) и массово использует компоненты, снятые с поддержки (EOL).

Анализ эксплуатационных журналов и инфраструктурных данных подтвердил выявленные дефекты на практике: переполнение файловых хранилищ ряда региональных ЦОД, массовые ошибки от единичного неисправного планового задания и попадание реальных персональных данных граждан в журналы. Нагрузочное тестирование подтвердило сверхлинейную деградацию выборки документов дела из-за отсутствия индекса по иерархии документов.

Выявленные критические и высокие риски устранимы доработкой существующей системы; полная замена не требуется. Первоочередные меры — ротация скомпрометированных ключей и секретов, закрытие уязвимостей доступа, приведение обработки персональных данных в соответствие Закону Республики Казахстан «О персональных данных и их защите», расширение емкости файловых хранилищ и устранение корневых дефектов эксплуатации. Детальные рекомендации, ожидаемый эффект и приоритизированный план мероприятий приведены в разделах 4–5 и Приложениях Г и Е.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ 7.32-2017. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.

2. ГОСТ 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления.

3. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V.

4. Техническая спецификация (Приложение 2 к Договору № 161040017107/260116/00 от 21.05.2026).

5. endoflife.date : сведения о сроках окончания поддержки программных компонентов [Электронный ресурс]. — URL: https://endoflife.date (дата обращения: 15.06.2026).

6. Camunda 7 Community Edition : официальная документация [Электронный ресурс]. — URL: https://docs.camunda.org (дата обращения: 15.06.2026).

7. Elastic (Elasticsearch) : официальная документация [Электронный ресурс]. — URL: https://www.elastic.co (дата обращения: 15.06.2026).

8. Spring Boot, Spring Cloud : официальная документация [Электронный ресурс]. — URL: https://spring.io (дата обращения: 15.06.2026).

9. OWASP Foundation. Application Security guidance (OWASP Top 10, ASVS) [Электронный ресурс]. — URL: https://owasp.org (дата обращения: 15.06.2026).

10. CWE/CVE. Common Weakness Enumeration / Common Vulnerabilities and Exposures [Электронный ресурс]. — URL: https://cve.mitre.org (дата обращения: 15.06.2026).

Приложения

Все приложения являются обязательной частью отчета (Техническая спецификация, раздел «обязательные приложения»). Состав приложений:

– приложение А — инвентаризационная ведомость инфраструктуры;

– приложение Б — схемы архитектуры;

– приложение В — исходные технические показатели;

– приложение Г — реестр выявленных рисков;

– приложение Д — матрица уязвимостей;

– приложение Е — приоритизированный план мероприятий;

– приложение Ж — версии компонентов и сроки поддержки (справочное);

– приложение И — анализ журналов эксплуатации (справочное);

– приложение К — результаты нагрузочного тестирования (справочное).

Приложение А. Инвентаризационная ведомость инфраструктуры

А.1 Серверные мощности ЦОД АП

Соответствующие данные представлены в таблице 10.

Таблица 10 — Серверные мощности ЦОД АП

№	Роль сервера	Диск, ГБ	RAM, ГБ	CPU, ядер
1	Сервер приложений, 1 нода	451,13	48	12
2	Сервер приложений, 2 нода	7 680	48	12
3	Сервер БД, мастер	537,16	32	6
4	Сервер БД, слейв	65,68	32	6
5	Сервер БД, слейв	67,78	32	6
6	Сетевое хранилище, мастер, 1-я чанк-нода	1 832,96	16	6
7	Сетевое хранилище, 2-я чанк-нода, Web-UI	1 792	16	6
8	Сетевое хранилище, 3-я чанк-нода, металогер	1 792	16	6
9	Поисковик (Elasticsearch), нода 1	392,71	8	6
10	Поисковик, нода 2	280,53	8	6
11	Поисковик, нода 3	329,33	8	6
12	Сервер распознавания (OCR)	13,74	8	6
13	Сервер БПМ (Camunda)	21,52	8	6
14	Сервер шины (ESB)	24,96	8	8
	ИТОГО	15 281,5	288	98

А.2 Ресурсы региональных узлов ЕЭАД

Соответствующие данные представлены в таблице 11.

Таблица 11 — Ресурсы региональных узлов ЕЭАД

№	Регион (ЦОД)	IP-адрес	CPU, ядер	RAM, ГБ	HDD, ГБ
1	Восточно-Казахстанская область	10.96.48.52	46	432	35 596
2	г.Алматы	10.17.48.44	46	432	33 300
3	Костанайская область	10.32.192.72	46	432	51 252
4	Атырауская область	10.80.48.53	136	862	55 224
5	г.Шымкент	10.247.48.52	92	864	60 880
6	Западно-Казахстанская область	10.128.48.57	46	432	31 500
7	Кызылординская область	10.176.48.55	46	432	44 524
8	Акмолинская область	10.32.48.63	46	432	66 346
9	Актюбинская область	10.64.48.78	46	432	41 596
10	Северо-Казахстанская область	10.88.48.58	92	864	63 000
11	Карагандинская область	10.144.48.94	46	432	31 500
12	Жамбылская область	10.112.48.49	46	432	35 524
13	Мангистауская область	10.32.192.241	46	432	34 500
14	Алматинская область	10.0.48.16	46	432	32 524

А.3 Сетевое оборудование (сегменты ЕТС ГО и Интернет)

Соответствующие данные представлены в таблице 12.

Таблица 12 — Сетевое оборудование (сегменты ЕТС ГО и Интернет)

Оборудование	Назначение	Кол-во	Технологии	Защита	Резервирование
Palo Alto	NGFW	2	BGP	IDS, IPS, FW	Горячее, ручное конфигурирование
FortiGate	NGFW	2	BGP	IDS, IPS, FW	Горячее, ручное конфигурирование
Cisco FPR 4120 (ETC) / 4110 (Интернет)	NGFW	1	ACL, OSPF, NAT	ACL Inspection, HTTPS	High availability

Приложение Б. Схемы архитектуры

Логическая схема архитектуры приведена на рисунке 1, физическая схема развертывания — на рисунке 2.

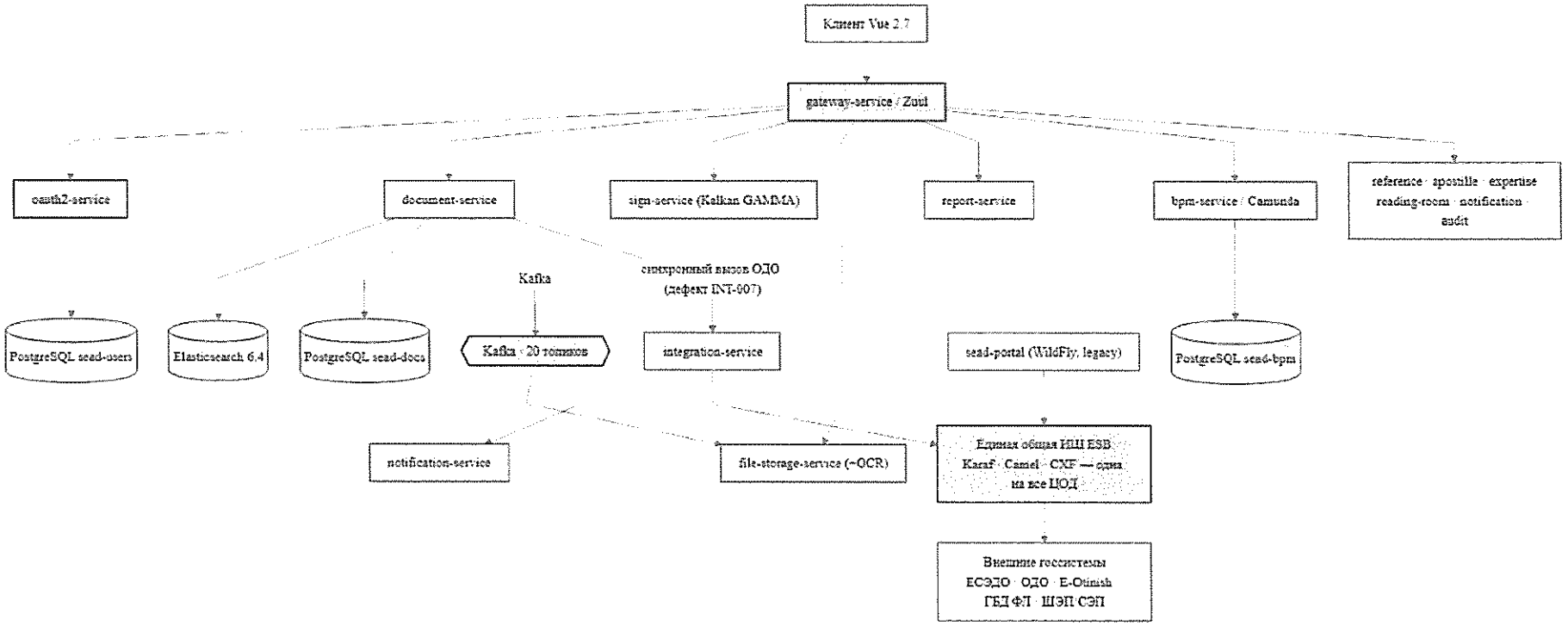

Рисунок 1 — Логическая схема (один региональный экземпляр; всего 16 обособленных систем на единой кодовой базе)

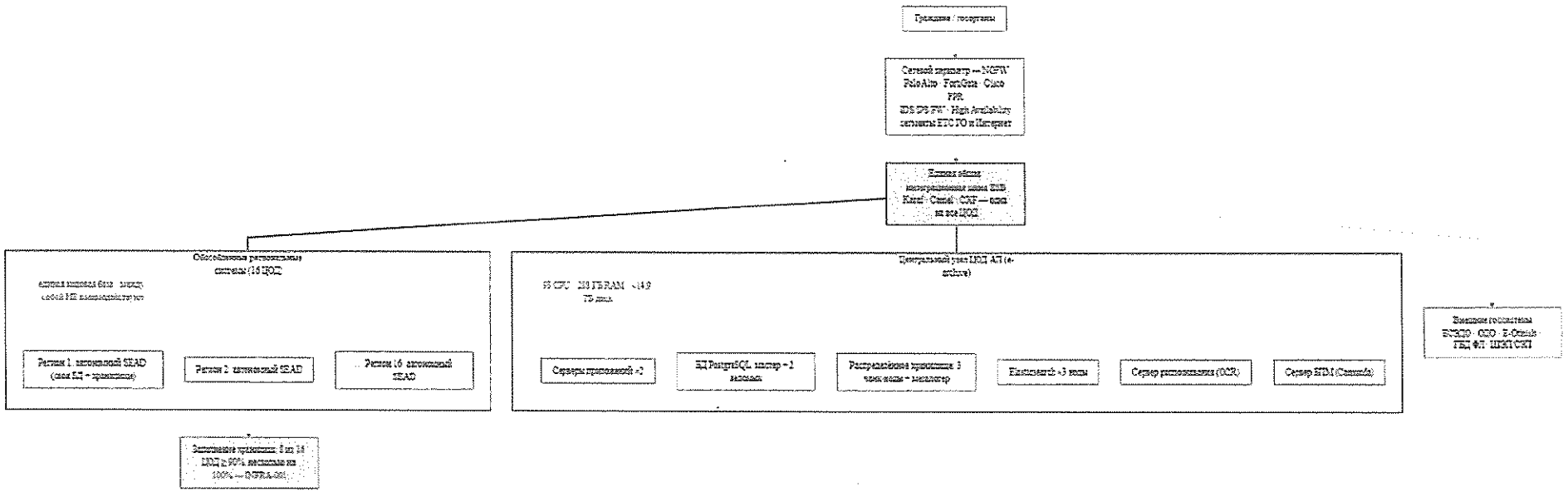

Рисунок 2 — Физическая схема развертывания (по данным инфраструктуры АО «НИТ»)

Приложение В. Исходные технические показатели

Показатели инфраструктуры настоящего приложения получены от АО «Национальные информационные технологии» (АО «НИТ»); показатели времени отклика — по результатам нагрузочного тестирования (Приложение К).

В.1 Объемы выделенных ресурсов ЕЭАД

Соответствующие данные представлены в таблице 13.

Таблица 13 — Объемы выделенных ресурсов ЕЭАД

Назначение	CPU (ядра)	RAM, ГБ	HDD, ГБ	SSD, ГБ
ЦОД АП	114	778	53 143	34 692
ЕЭАД резерв (Астана)	94	738	78 000	—
ЕЭАД резерв (регионы)	734	6 816	502 430	—
ЕЭАД регионы (Приложение А)	826	7 342	617 266	—

В.2 Загруженность файловых систем региональных хранилищ

Соответствующие данные представлены в таблице 14.

Таблица 14 — Загруженность файловых систем региональных хранилищ

Регион (ЦОД)	Емкость, ТБ	Занято, %	Статус
Восточно-Казахстанская область	13	100%	Критично
г.Алматы	11	100%	Критично
Костанайская область	32	100%	Критично
Атырауская область	9,6	100%	Критично
г.Шымкент	12	100%	Критично
Западно-Казахстанская область	8,6	100%	Критично
Кызылординская область	21	99%	Критично
область Жетісу	15	90%	Критично
Акмолинская область	13	85%	Внимание
Актюбинская область	19	85%	Внимание
Северо-Казахстанская область	8,6	80%	Внимание
Туркестанская область	8,3	76%	Внимание
Карагандинская область	8,6	66%	Норма
Жамбылская область	8,9	66%	Норма
Павлодарская область	8,6	15%	Норма
Мангистауская область	3	9%	Норма

Регион (ЦОД)	Емкость, ТБ	Занято, %	Статус
ИТОГО (с данными по ФС)	≈ 200.2 ТБ	≈ 87% (≈ 174.0 ТБ)	8 критич.

Переполнение региональных хранилищ напрямую связано с находкой LOG-002 (неисправная очистка просроченных файлов). Источник: «Состояние хранилища по регионам» (АО «НИТ»).

В.3 Прочие показатели

Соответствующие данные представлены в таблице 15.

Таблица 15 — Прочие технические показатели

Показатель	Зафиксированное значение	Источник / метод
Суммарная емкость региональных хранилищ	≈ 200.2 ТБ	Состояние хранилища (НИТ)
Дисковая емкость сервера БД (мастер)	537 ГБ	Серверные мощности ЦОД АП (АО «НИТ»)
Загрузка канала связи (узел Нацархива)	53.7% (пик 6 600 кбит/с)	Мониторинг каналов (НИТ)
Время отклика (авторизация / выборка дела)	0,4–0,6 с / 7,5–11 с	Нагрузочное тестирование (Приложение К)

Приложение Г. Реестр выявленных рисков

Классификация критичности: К — критический, В — высокий, С — средний, Н — низкий. Доказательство — путь к файлу и строка в исходном коде.

Соответствующие данные представлены в таблице 16.

Таблица 16 — Реестр выявленных рисков

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
1	**ARCH-001**	Нарушение database-per-service: 11 микросервисов делят одну БД sead-docs	11 сервисов / БД sead-docs	properties-yaml/application.yml:44; per-service *.yml (→/sead-docs)	Высокая	Высокий	Разделить БД по доменам, ввести API-границы
2	**ARCH-002**	Циклические Feign-зависимости между document/sign/report/apostille/integration	service-client	service-client/.../client/* (встречные @FeignClient)	Средняя	Высокий	Развязать через события Kafka/рефакторинг
3	**ARCH-003**	Гибридная архитектура: устаревший портал (WildFly) сосуществует с микросервисами и ESB	sead-portal (WildFly)	sead-portal/.../META-INF/persistence.xml:4; seadportal-war/pom.xml:75-81	Средняя	Средний	Зафиксировать роль портала, план миграции/вывода
4	**ARCH-004**	Рассинхрон версий: брокер Kafka 3.7 vs клиенты 2.x	ESB / Kafka	sead-esb/esb/docker-compose/docker-compose.yml	Средняя	Средний	Сверить и зафиксировать совместимые версии
5	**VER-001**	EOL (линейка 6.x — 10.02.2022) + Transport Client (удален в ES7)	Elasticsearch 6.4.2	document-service/pom.xml:138	Высокая	Критический	Миграция на поддерживаемую ES/OpenSearch

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
6	**VER-002**	Устаревшая коммерческая версия ABBYY FineReader 12 (вне актуальной линейки поддержки)	ABBYY FineReader 12	ocr-finereader-engine/pom.xml:16-24	Высокая	Средний	Перейти на поддерживаемую версию ABBYY FineReader или рассмотреть переход на альтернативный OCR-движок
7	**VER-003**	Устаревшая платформа: Java 8 (бесплатная поддержка Oracle завершена), Spring Boot 2.7 OSS EOL 30.06.2023	Java 8 / Spring Boot 2.x	sead-esb/esb/sead-osgi/pom.xml:67-69; service-common/pom.xml:70	Высокая	Высокий	План обновления Java 17 + Spring Boot 3
8	**VER-004**	EOL ESB-стек (Camel 2.x EOL 31.01.2022)	Camel 2.23 / Karaf 4.2 / CXF 3.x	sead-esb/esb/pom.xml:39,45; CXF 3.x	Высокая	Высокий	Обновление ESB до поддерживаемых версий
9	**VER-005**	EOL frontend-стек (Vue 2 EOL 31.12.2023): Element UI, CKEditor 12, BPMN.js 4, ECharts RC, Webpack 4, Axios 0.18	Vue 2.7 + экосистема	vue-frontend/package.json:51,18,23,29,101	Высокая	Высокий	Миграция клиентской части (frontend) на Vue 3 с обновлением зависимостей
10	**VER-006**	Устаревшие компоненты (Hibernate 5.4 EOL 10.01.2022, Camunda 7 CE EOL 10.2025)	Hibernate 5.4 / Liquibase 3.8 / POI 3.17 / Camunda 7.11	bpm-service/pom.xml:50; seadportal-ejb/pom.xml:131,74	Высокая	Высокий	Поэтапное обновление
11	**VER-007**	Невоспроизводимая сборка: lodash:latest,	frontend / sign-service	vue-frontend/package.json:40; sign-service/pom.xml:96-100	Средняя	Средний	Зафиксировать версии, перенести

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		system-scope JAR (GAMMA)					JAR в приватный репозиторий
12	**VER-008**	Parent POM kz.inessoft.sead вне репозитория — часть версий не финализируема из кода	Сборка (parent POM)	parent kz.inessoft.sead:sead — отсутствует в репозитории	Средняя	Средний	Предоставить parent POM для полной верификации версий
13	**SEC-001**	Приватный ключ ЭЦП (PKCS#12) + пароль Aa123456 в открытом конфиге	sign-service.yml	properties-yaml/sign-service.yml:57-58,62	Высокая	Критический	Отозвать/перевыпустить ключ; HSM/Vault
14	**SEC-002**	XXE: 5 XML-фабрик без защиты от внешних сущностей	integration-service-common/XmlUtils.java	integration-service-common/.../XmlUtils.java:49,117,127,157,175	Высокая	Критический	disallow-doctype-decl, отключить внешние сущности
15	**SEC-003**	permitAll("/**") — доступ ко всем эндпоинтам без аутентификации	sead-socket-service	sead-socket-service/.../OAuth2ResourceServerConfig.java:30,40,43-44	Высокая	Критический	Убрать /**, требовать JWT
16	**SEC-004**	Анонимная смена пароля и проверка ИИН (check-iin)	OAuth2ResourceServerAutoConfiguration	service-common/.../OAuth2ResourceServerAutoConfiguration.java:46-48	Высокая	Критический	Закрыть аутентификацией/авторизацией
17	**SEC-005**	Захардкоженный ключ подписи JWT	application.yml	properties-yaml/application.yml:119	Высокая	Высокий	Вынести в Vault/env, ротация, RS256
18	**SEC-006**	Общий секрет "password" для всех OAuth2-клиентов; токены 100ч/416дней	oauth2-service.yml	properties-yaml/oauth2-service.yml:59,62,63	Высокая	Высокий	Уникальные секреты, короткий TTL, отзыв токенов

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
19	**SEC-007**	Хардкод DB/email/gateway/интеграционных credentials	properties-yaml	application.yml:6-7,211; gateway-service.yml; integration-service.yml	Высокая	Высокий	Секрет-хранилище, ротация
20	**SEC-008**	Логирование ИИН и ПД (нарушение Закона РК)	sign/reference/audit	SignServiceImpl.java:226; ArchiveReferenceServiceImpl.java:1891; AuditServiceImpl.java:49	Высокая	Критический	Маскирование, убрать ПД из журналов
21	**SEC-009**	37 реальных ИИН граждан в конфиге (белый список ИИН, параметр white-list-iin)	application.yml	properties-yaml/application.yml:149	Высокая	Высокий	Убрать ПД из конфига
22	**SEC-010**	CSRF отключен глобально во всех конфигурациях	Spring Security	gateway ServiceConfig.java:75; OAuth2ResourceServerAutoConfiguration.java:59; socket OAuth2ResourceServerConfig.java:43	Средняя	Высокий	Обосновать для stateless API; включить где есть сессии
23	**SEC-011**	Нет method-level RBAC: авторизация только на Zuul, 9 сервисов без проверки ролей	gateway + 9 сервисов	gateway ServiceConfig.java:74; service-common OAuth2ResourceServerAutoConfiguration.java:57	Высокая	Критический	@PreAuthorize во всех сервисах (defense-in-depth)
24	**SEC-012**	Журнал аудита без защиты доступа (нет spring-security)	audit-service	audit-service AuditController.java:19-65; audit-service/pom.xml (нет spring-security)	Высокая	Высокий	Resource-server + роль аудитора
25	**SEC-013**	Подпись не перепроверяется при выдаче/чтении документа	document-service	document DocumentServiceImpl.java:186-188; SignedFilesServiceImpl.java:129-139	Средняя	Высокий	Перепроверка подписи при выдаче/экспорте
26	**SEC-014**	OCSP-проверка отзыва сертификата по флагу (может быть выключена)	sign-service	sign SignServiceImpl.java:135-136	Средняя	Средний	Сделать OCSP обязательной в проде

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
27	**SEC-015**	Журнал аудита не иммутабелен (наследует CRUD, нет append-only)	audit-service	audit AuditRepository.java:12; db-changelog/.../20180927-add-audit-table.sql; 20200807/20210203-update-table-audit.sql	Средняя	Высокий	Append-only журнал, хэш-цепочка целостности
28	**SEC-016**	/actuator/refresh доступен любому аутентифицированному (меняет конфиг)	Actuator	properties-yaml/*.yml (include health,info,refresh); OAuth2ResourceServerAutoConfiguration.java:54-57	Средняя	Средний	Ограничить ролью администратора
29	**SEC-017**	Kafka/Kafdrop без аутентификации, порты наружу, образ без тега	ESB docker-compose	sead-esb/esb/docker-compose/docker-compose.yml:10,13,29,32	Средняя	Высокий	SASL/TLS, закрыть Kafdrop, фиксировать тег
30	**SEC-018**	Глобальное отключение проверки TLS (trust-all) для всех HTTPS процесса	sign-service/SignApplication.java	sign-service/SignApplication.java:54,69-88	Высокая	Критический	Удалить turnOffSslChecking; truststore УЦ РК
31	**SEC-019**	Небезопасная десериализация (enableDefaultTyping) — потенциальный RCE	service-common/KafkaJsonSerialization.java	service-common/KafkaJsonSerialization.java:16,21	Средняя	Критический	Убрать defaultTyping; allow-list типов
32	**SEC-020**	SHA-1 для контроля целостности файлов архива	file-storage-core	file-storage-core/FileStorageServiceImpl.java:1614-1615	Средняя	Высокий	Перейти на SHA-256
33	**SEC-021**	Загрузка CRL по URL без ограничения схемы/хоста (в связке с trust-all)	sign-service/CRLInfo.java	sign-service/.../kalkan/CRLInfo.java:97	Низкая	Средний	Белый список УЦ-хостов, https, таймауты
34	**SEC-022**	Нет rate-limiting на auth/смену пароля/check-iin (перебор, энумерация ИИН)	oauth2/gateway	oauth2-service/.../CustomResourceOwnerPasswordTokenGranter.java:~140-154	Высокая	Высокий	Throttling/CAPTCHA на auth-эндпоинты

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
35	**SEC-023**	Захардкоженные учетные данные интеграции ЕСЭДО (isead)	document-service/EsedoComponent.java	document-service/.../component/EsedoComponent.java:120-121	Высокая	Высокий	Секрет-хранилище, разные учетные данные dev/prod
36	**SEC-024**	Утечка деталей ошибок наружу (e.getMessage, printStackTrace)	множество сервисов	file-storage DocumentFileStorageController.java:311,580,...; XmlUtils.java; ApostilleRequestServiceImpl.java:270,388	Средняя	Средний	Единый @ControllerAdvice; стек только в лог
37	**SEC-025**	Хардкод учетных данных git Config Server (team-ci/Qwerty98AA) + skip-ssl-validation	config-service/bootstrap.yml	config-service/src/main/resources/bootstrap.yml:10-13	Высокая	Критический	Сменить пароль, SSH/секреты, включить SSL
38	**SEC-026**	Eureka и Config Server без собственной аутентификации	discovery-service/config-service	discovery-service/bootstrap.yml; config-service (spring-security отсутствует)	Средняя	Высокий	Закрыть Basic/OAuth2; доступ сервис-к-сервису
39	**SEC-027**	Отсутствие @PreAuthorize на чувствительных эндпоинтах (часть SEC-011)	report/reading-room/expertise	report ReportController.java:69-150; reading-room AccessRequestController.java:36-57; expertise api/*	Высокая	Высокий	Добавить проверку роли и организации
40	**INT-001**	Kafka-консьюмеры без обработки ошибок и ack	notification/reference listeners	notification-service-common/NotificationEventListener.java:20; reference-service/.../kafka/ReferenceEventListener.java:20	Средняя	Высокий	try/catch + ErrorHandler + DLQ

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
41	**INT-002**	Отсутствие DLQ; retry реализован через PostgreSQL в ESB	Kafka consumers	sead-esb/.../camel-context.xml:381-438,355	Средняя	Средний	DLQ-топики Kafka, стандартный retry
42	**INT-003**	Хардкод учетных данных интеграции (=SEC-023)	EsedoComponent	document-service/.../component/EsedoComponent.java:120-121	Высокая	Высокий	Секрет-хранилище
43	**INT-004**	Нет обработчика ошибок/таймаута синхронного ответа SHEP2	ESB SHEP2	sead-esb/.../camel-context.xml:365-375,183	Средняя	Высокий	onException + таймауты
44	**INT-005**	XSD-валидация на интеграционной шине (ИШ) не применяется по проектному решению — валидация входящих сообщений выполняется в самой системе (на уровне приложения)	ESB CXF seadService	sead-esb/.../camel-context.xml:15-21 (XSD на ИШ не применяется по проектному решению; валидация — на уровне приложения)	Низкая	Низкий	Для защиты в глубину рассмотреть схема-валидацию на границе ИШ дополнительно к прикладной; обеспечить защиту XML-парсинга от XXE (SEC-002/SEC-032)
45	**INT-006**	ИИН во внешних каналах; TLS не подтвержден; XML через XXE-уязвимый util	integration-service	integration GbdServiceImpl.java; EOtinishServiceImpl.java:30-40	Средняя	Высокий	Подтвердить TLS/mTLS; защитить XML; не логировать ИИН
46	**INT-007**	Синхронная интеграция с ОДО в обработке описи (SeadInventoryDocument): внутри Kafka-листенера	document-service / InventoryDocumentComponent (интеграция с ОДО)	document InventoryDocumentComponent.java:1135 (integrationClient.sendEHedRequest в @KafkaListener	Высокая	Высокий	Перевести интеграцию с ОДО на асинхронное взаимодействие

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		выполняется блокирующий Feign-вызов к integration-service→ОДО, что блокирует консьюмер и снижает отказоустойчивость/пропускную способность		INVENTORY_DOCUMENT_HED_FILE:1115); IntegrationClient.java:24,40 (@FeignClient, синхронный sendEHedRequest); CreatedWith.BY_ODO:537			(очередь/событие, неблокирующий вызов с ретраями и DLQ); вынести внешний вызов из обработчика Kafka
47	**DB-001**	Монолитные миграции (splitStatements:false), затруднен частичный откат	db-changelog	db-changelog/.../sead-docs/liquibase-changelog.yml:1-30	Средняя	Средний	Атомарные changeSet, DML отдельно от DDL
48	**DB-002**	Дублирующиеся id changeSet	db-changelog	db-changelog/.../sead-docs/liquibase-changelog.yml:18-34	Низкая	Низкий	Сквозная уникальная нумерация
49	**DB-003**	serial/int4 PK на растущих таблицах (риск переполнения)	db-changelog sead-docs	sead-docs/20180914-document-tables.sql:1-20; 20180926-alter_ids_bigserial.sql	Низкая	Средний	Перевести растущие таблицы на bigint
50	**DB-004**	Информационно: схема в целом хорошо проиндексирована (388 индексов, FK)	db-changelog	sead-docs/20180914-document-tables.sql:110-128; 20180927-add-audit-table.sql:14-15	Низкая	Низкий	Поддерживать практику
51	**DB-005**	Конкатенация значений в нативный SQL (Long/formatter снижают риск)	document-service/DeadlineServiceImpl.java	document-service/.../DeadlineServiceImpl.java:34-40,67-76,99-100	Низкая	Средний	Параметризовать запросы

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
52	**DB-006**	Динамический SQL (значения параметризованы — инъекции нет)	document-service-common/ReportRepositoryImpl.java	document-service-common/.../ReportRepositoryImpl.java:515,575,636	Низкая	Низкий	Criteria API/QueryDSL (техдолг)
53	**DB-007**	Информационно: параметризация native-запросов соблюдена	репозитории @Query	репозитории с @Query(nativeQuery=true) (параметризованы)	Низкая	Низкий	Поддерживать практику
54	**DB-008**	EAGER-ассоциации, N+1 не смягчен (нет EntityGraph/batch)	document-service-domain	document-service-domain/.../PassportSpecification.java:54,58,65,69,91; application.yml:16-28	Высокая	Высокий	LAZY + EntityGraph + batch_size
55	**DB-009**	N+1 в циклах + save() по одной записи вместо saveAll	AcceptanceReportServiceImpl.java	document-service/.../AcceptanceReportServiceImpl.java:641,665-674,784,908	Высокая	Высокий	saveAll, предзагрузка коллекций
56	**DB-010**	Не заданы hibernate batch_size / default_batch_fetch_size	application.yml	properties-yaml/application.yml:16-28	Средняя	Средний	Включить JDBC-батчинг
57	**DB-011**	Содержимое документов и ПД в Elasticsearch без защиты	document-service / ES	document-service/src/main/resources/es_create_index_scheme.json:60,210,212	Высокая	Высокий	Минимизация ПД в ES, ролевой доступ
58	**DB-012**	ES 6.4 EOL + подключение без TLS и аутентификации	Elasticsearch 6.4.2	document-service/pom.xml:136-139; application.yml:110-111	Высокая	Критический	Миграция, TLS + аутентификация
59	**DB-013**	Нет индекса на soft-delete колонке deleted (~1140 фильтров)	db-changelog	sead-docs/20181113-add-deleted-to-document.sql (нет индекса на deleted)	Высокая	Высокий	Частичные индексы WHERE deleted=false
60	**DB-014**	Поздние/выборочные индексы на частых фильтр-колонках	db-changelog	sead-docs/20210125-create-indexes.sql:1-3	Средняя	Средний	Покрытие индексами по EXPLAIN

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
61	**DB-015**	Захардкоженный pgcrypto-ключ шифрования ИИН/ФИО	apostille-service/ApostilleRequest.java	apostille-service/.../domain/ApostilleRequest.java:46-47	Высокая	Критический	Ключ в Vault/KMS, ротация, перешифрование
62	**DB-016**	Деградация выборки документов дела: коррелированный подзапрос по иерархии документов без индекса (квадратичная сложность). Нагрузочный тест — отказ 504 при деле ≥ 20 000 док. и при 50 одновременных пользователях (доля ошибок до 45%); БД CPU 90–100%, пул соединений исчерпан. Эмпирическое подтверждение DB-008/DB-009/QA-004	document-service / GET /documents/deal/{id}	Нагрузочное тестирование (Приложение К): EXPLAIN ANALYZE — 1 000 док. ≈ 0,9 с, 10 000 ≈ 12–17 с, 40 000 ≈ 120–168 с; Seq Scan таблицы связей (~61 000 строк) без индекса, коррелированный подзапрос на каждую строку (loops)	Высокая	Высокий	Переписать запрос (одним проходом либо рекурсивным CTE); добавить индексы на таблицу связей иерархии; пагинация выборки; circuit-breaker на шлюзе
63	**BPM-001**	Camunda 7.11 Community — EOL (линейка 7 CE EOL 10.2025)	bpm-service	bpm-service/pom.xml:48-56	Высокая	Высокий	План обновления/миграции Camunda
64	**BPM-002**	Динамический деплой BPMN без XSD-валидации и (требует подтв.) проверки прав	BpmProcessServiceImpl.java	bpm-service/.../BpmProcessServiceImpl.java:199-214	Средняя	Высокий	XSD-валидация + авторизация деплоя
65	**BPM-003**	История ACT_HI_* без TTL — риск разрастания БД	bpm-service	sead-bpm/20190827-postgres_engine_7.11.0.sql:758-	Высокая	Высокий	history.time.to.live + cleanup

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
				1295,157 (TTL не задан в application.yml)			
66	**BPM-004**	Старые версии процессов накапливаются	bpm-service	sead-bpm/20190827-postgres_engine_7.11.0.sql:143-160	Низкая	Низкий	Периодическая очистка устаревших версий
67	**BPM-005**	Нет защит от зависших процессов/задач (deadline/эскалация)	bpm-service	bpm-service (dueDate/эскалация не найдены)	Средняя	Средний	dueDate/эскалация на UserTask, мониторинг
68	**LIC-001**	Коммерческая лицензия не верифицирована из исходного кода; компонент устарел (ABBYY FineReader Engine 12)	ABBYY FineReader 12	ocr-finereader-engine/pom.xml:16-24	Высокая	Средний	Верифицировать лицензионное соответствие и рассмотреть переход на актуальную версию или альтернативное решение
69	**LIC-002**	Community Edition (LGPL) — соответствие соблюдено	JasperReports 6.7	report-service/pom.xml:15-61	Низкая	Низкий	Зафиксировать редакцию в реестре
70	**LIC-003**	Apache 2.0 — без ограничений (compliant)	POI/PDFBox/Tika/xmlsec	report-service/pom.xml:95-103; file-storage-service/pom.xml:66-69	Низкая	Низкий	Отметить как соответствующие
71	**LIC-004**	Проприетарные крипто-компоненты РК (system-scope JAR)	Kalkan/GAMMA/KNCA	sign-service/pom.xml:39-101; src/main/resources/lib/crypto.gammaprov.jar	Средняя	Средний	Подтвердить договоры с НУЦ РК/GAMMA
72	**LIC-005**	Двойная лицензия LGPL/коммерческая —	Liquibase	db-changelog/pom.xml:16-19	Низкая	Низкий	Отметить как compliant

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		используется LGPL (compliant)					
73	**QA-001**	Множественные пустые/проглатывающие catch-блоки	FoundationServiceImpl и др.	FoundationServiceImpl.java:2751,2756, ...,4184; SeadJwtTokenStore.java:69	Высокая	Высокий	Логирование исключений; запрет пустых catch
74	**QA-002**	Критически низкое покрытие тестами	все сервисы	document-service/src/test (единичные); прочие сервисы — тестов нет	Высокая	Высокий	Минимальное покрытие критичных сервисов, порог в CI
75	**QA-003**	Хардкод хостов/URL/ПД вместо параметризации	properties-yaml	properties-yaml/application.yml:107,110-117,149	Средняя	Средний	Профили окружения/секрет-хранилище
76	**QA-004**	Синхронные Feign-цепочки без circuit-breaker/fallback	service-client	service-client/.../client/* (Feign без circuit-breaker)	Средняя	Средний	Circuit-breaker + fallback + таймауты
77	**QA-005**	Мертвый код; неиспользуемые Kafka-топики	FoundationServiceImpl	FoundationServiceImpl.java:2709-2746; application.yml:54,55,66	Низкая	Низкий	Удалить мертвый код/топики
78	**QA-006**	Отсутствие единой стратегии обработки ошибок (printStackTrace)	множество сервисов	XmlUtils.java; ApostilleRequestServiceImpl.java (printStackTrace)	Средняя	Средний	Единый @ControllerAdvice; логгер
79	**FE-001**	EOL/CVE-зависимости (Vue 2.7, Axios 0.18, ECharts RC, Webpack 4 и др.)	vue-frontend/package.json	vue-frontend/package.json:51,21,29,40,18,23,101	Высокая	Высокий	План миграции на поддерживаемые версии

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
80	**FE-002**	Токены доступа/refresh и ПД в localStorage (кража через XSS)	vue-frontend	api.axios.js:26-28; store.service.js:3-23,53; Login.vue:493-501	Высокая	Критический	httpOnly secure cookies для токенов
81	**FE-003**	Истечение сессии вычисляется на клиенте (подделываемо)	vue-frontend/api.axios.js	api.axios.js:34,38,44,47; store.service.js:13-14	Средняя	Высокий	Контроль истечения на сервере (JWT exp)
82	**FE-004**	Захардкоженный публичный IP файлового сервера в активном коде	vue-frontend	page/deals/DealDetails1.vue:144; App.vue:116; vue.config.js:26-31	Высокая	Высокий	Вынести адреса в env/gateway
83	**FE-005**	XSS: v-html с данными бэкенда + dangerouslyUseHTMLString, без DOMPurify	vue-frontend/Search.vue	page/.../search/Search.vue:234,257,281,298,324,351,379; api.axios.js:104	Средняя	Высокий	Санитизация (DOMPurify), CSP
84	**FE-006**	Неполная обработка ошибок API (тихие сбои)	vue-frontend	page/foundation/ListFoundation.vue:658-674; api.controllers.js	Средняя	Средний	Единая обработка ошибок с уведомлением
85	**COMP-001**	Системные пробелы защиты ПД (Закон РК «О персональных данных»)	ПД в целом	application.yml:149; SignServiceImpl.java:226; es_create_index_scheme.json; ApostilleRequest.java:46	Высокая	Критический	Программа защиты ПД (шифрование, маскирование, доступ)
86	**COMP-002**	Недостаточный контроль доступа к ПД (RBAC, анон. эндпоинты)	RBAC/ПД	см. SEC-011, SEC-012, SEC-004	Высокая	Высокий	Ролевой доступ к ПД на всех сервисах
87	**COMP-003**	Аудит: иммутабельность и полнота покрытия не гарантированы	audit-service	audit-service AuditController.java; AuditServiceImpl.java:49	Средняя	Средний	Иммутабельность журнала, подтвердить покрытие

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
88	**COMP-004**	Сертификация и аттестация (МЦиАП/NITEC, СТ РК, ISO 27001) не подтверждаются из исходного кода (вне предмета аудита). Резидентность данных подтверждается инфраструктурными данными (ЦОД АО «НИТ» на территории РК). Оценка безопасности выполнена статическим методом (анализ кода + SAST, находки SEC-*)	Организационно-инфраструктурное соответствие	[не верифицировано из кода] — данные НИТ/заказчика	—	Низкий	Аттестация и сертификация находятся вне предмета настоящего аудита по исходному коду; соответствие не верифицировано
89	**PORTAL-001**	Приватный ключ ЭЦП портала закоммичен в репозиторий + пароль 123456Gg	seadportal/SignService.java + .p12	seadportal-ejb/.../sign/service/SignService.java:38-39; resources/GOSTKNCA_*.p12	Высокая	Критический	Отозвать ключ, удалить .p12 из VCS, HSM
90	**PORTAL-002**	Нет контейнерной защиты — админ-сервлеты открыты	seadportal/web.xml	seadportal-war/.../WEB-INF/web.xml:1-264	Высокая	Критический	security-constraint/login-config по ролям
91	**PORTAL-003**	Trust-all SSL глобально (обмен с госшлюзом СЭП/ШЭП)	seadportal/ServicesBean.java	seadportal-ejb/.../bean/ServicesBean.java:1396-1420	Высокая	Критический	Убрать trust-all, truststore шлюза
92	**PORTAL-004**	SQL/JPQL-инъекция (конкатенация ввода в запрос)	seadportal/UsersBean.java	seadportal-ejb/.../bean/UsersBean.java:206,225; SystemBean.java:1352,1577,1595	Высокая	Критический	Параметризовать запросы

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
93	**PORTAL-005**	XXE в XML-парсерах портала	seadportal/XmlUtils.java	seadportal-ejb/.../util/XmlUtils.java:97-111,149,275; seadportal-war/.../socket/WSfunctions.java:115-118,138-141	Высокая	Высокий	Запрет DOCTYPE/внешних сущностей
94	**PORTAL-006**	Фильтр не выполняет аутентификацию; доверие подделываемым заголовкам	seadportal/IpAddressFilter.java	seadportal-war/.../servlet/filter/IpAddressFilter.java:58-65,106-111	Средняя	Высокий	Доверять заголовкам только от прокси; enforce сессию
95	**PORTAL-007**	Cross-Site WebSocket Hijacking (нет проверки Origin)	seadportal/Configurator.java	seadportal-war/.../socket/Configurator.java:21-30; WSseadportal.java:57-60,100-105	Средняя	Высокий	Валидация Origin против белого списка
96	**PORTAL-008**	Небезопасная Java-десериализация (readObject без фильтра)	seadportal/XmlUtils,FileUtil	seadportal-ejb/.../util/XmlUtils.java:301-306; FileUtil.java:100,259	Средняя	Высокий	Отказ от нативной сериализации/allow-list
97	**PORTAL-009**	Хардкод учетных данных БД + закомментированная недокументированная функция обхода аутентификации (backdoor adminlogin)	seadportal/pom.xml,WSseadportal.java	seadportal-war/pom.xml:81-83; WSseadportal.java:1300-1302	Высокая	Высокий	Вынести учетные данные; удалить недокументированную функцию обхода
98	**PORTAL-010**	Интеграция с госшлюзом по незащищенному http://	seadportal/Constants.java	seadportal-ejb/.../util/Constants.java:67-68,79	Средняя	Высокий	Перевести на TLS с проверкой сертификата
99	**PORTAL-011**	EOL-стек: WildFly 16, Spring 5.1, CXF 3.2, jQuery 3.3/3.4	seadportal (платформа)	seadportal/pom.xml:31,27-28,45,37; webapp/js/jquery-3.3.1/3.4.1	Высокая	Высокий	Миграция на поддерживаемые версии

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
100	**PORTAL-012**	Логирование ИИН/ПД и тел сообщений	seadportal	WSfunctions.java:215,229,275,329; WSseadportal.java:89-92; IpAddressFilter.java:112	Высокая	Средний	Маскирование/удаление ПД из журналов
101	**PORTAL-013**	Нет тестов; printStackTrace/System.out; проглоченные исключения	seadportal (качество)	seadportal/src/test (0 тестов); XmlUtils.java:56,67,90 (printStackTrace)	Средняя	Средний	Тесты критичных путей; логгер
102	**SEC-028**	IDOR: отсутствие object-level авторизации — доступ к чужим сущностям по прямому ID при наличии аутентификации	контроллеры (reading-room и др.)	reading-room AccessRequestController.java; DamagedActController.java; DocumentHandoutRequestController.java (@PathVariable id без проверки владения)	Высокая	Критический	Проверка владения/организации на каждый доступ по ID
103	**SEC-029**	Системный хардкод интеграционных паролей (isead/test/password) в 11+ backend-файлах и портале	apostille/document/integration/reference + портал	setPassword("isead") — 11 файлов (apostille/document/integration/reference); portal ServicesBean.java:913,991,1047,1282,1357,1455,1704,1771,1821	Высокая	Критический	Вынести учетные данные в секрет-хранилище; запрет хардкода в CI
104	**SEC-030**	Raw JDBC SQL-конкатенация в ESB (Statement.executeQuery)	sead-esb/RedeliveryProcessor.java	sead-esb/esb/sead-osgi/.../dead/RedeliveryProcessor.java:44-48	Средняя	Высокий	PreparedStatement; ревизия raw-SQL в ESB
105	**SEC-031**	Хардкоженный дефолт-пароль пользователя Password1$ при импорте	document-service/AdminUserImportServiceImpl.java	document-service/.../AdminUserImportServiceImpl.java:304	Высокая	Высокий	Случайный пароль + смена при первом входе
106	**SEC-032**	XXE расширенного охвата (ShepMessageHelper, SimpleXLSXWorkbook,	ESB/document-xlsx/портал	ESB ShepMessageHelper.java:183,215; document SimpleXLSXWorkbook.java:158; portal	Высокая	Критический	Единая безопасная XML-фабрика на весь проект

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		XMLDSigObject) — дополняет SEC-002		XMLDSigObject.java:246; WSfunctions.java:115,138,174,2850			
107	**LOG-001**	ПД в журналах: 160 318 ИИН в журналах, из них audit-service 158 667 (99%). Эксплуатационное подтверждение SEC-008/COMP-001	audit-service	logs_analytics.json: iinTotal=137512; iinBySvc audit-service=135861, document-service=1651; iinByRegion Алматинская=38117, Карагандинская=25045 — см. Приложение И	Высокая	Критический	Маскирование ПД на уровне логгера (в первую очередь audit); запрет логирования тел ответов ГБД
108	**LOG-002**	Сломанный плановый job autoDeleteExpiredDeletedFiles падает ~99 млн раз → каскад PostgreSQL «transaction aborted» (свыше 100 млн). БД — 81% всех ошибок; file-storage — 99%	file-storage / ScheduledFileStorage	logs_aggregate.json fingerprints: ScheduledFileStorage|autoDeleteExpiredDeletedFiles ERROR JpaSystemException=39.78M; SqlExceptionHelper|current transaction is aborted=40.68M; категория БД 85.1M (74.1%) — см. Приложение И	Высокая	Критический	Исправить транзакционность job (транзакция на элемент, обработка FK); алертинг на отказ плановых задач
109	**LOG-003**	Массовый сбой OCR-разбивки файлов: SPLIT FILE ERROR IOException (8.6 млн) + NPE + SeadServiceException. Категория файлы/OCR — 22% ошибок	file-storage / RecognizeServiceImpl (OCR)	fingerprints: RecognizeServiceImpl|SPLIT FILE ERROR IOException=8.61M (7.39M+1.22M); IOException=25.64M; OCR START ERROR NullPointerException=149465 — см. Приложение И	Высокая	Высокий	Диагностировать IOException (ABBYY/диск/формат), валидировать вход OCR, устранить NPE
110	**LOG-004**	Многолетние неустраненные циклические аварийные завершения (crash-loop) (ошибки с 2020, пики ~1.5 млн/день в 2026); live-	Эксплуатация / ротация журналов	logs_analytics.json trend: диапазон 2020-08…2026-07, 468 дней с ошибками; топ-дни 2026-06-06=1496661; stacktrace=720696500 — см. Приложение И	Высокая	Высокий	Устранить корневые дефекты; ротация и лимиты live-логов; мониторинг доли ERROR

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		логи не ротируются → 720 млн строк стектрейсов					
111	**LOG-005**	Брошенные .tmp незавершенной ротации: 294 файла = 7.16 ГБ (Атырауская 2.7 ГБ, Костанайская 1.65 ГБ) со стектрейсами циклических аварийных завершений	Инфраструктура логирования (logback)	logs_summary.txt: .tmp=294 файла / 7165 МБ; tmpInventory: Атырауская 2707 МБ, Костанайская 1654 МБ, Шымкент 677 МБ — см. Приложение И	Высокая	Высокий	Очистка .tmp/cleanHistoryOnStart; централизация журналов; расследование незавершенных ротаций
112	**LOG-006**	Сбои интеграций в журналах: 1.14 млн (document 751к, integration 126к). Feign/NoRouteToHost/UnknownHost/Timeout. Подтверждает QA-004/INT-*	document/integration/gateway (интеграции)	logs_analytics.json services: document-service intFail=751398, integration=126432, notification=94478, gateway=41084; FeignException=579110, NoRouteToHost=154728 — см. Приложение И	Высокая	Высокий	Circuit-breaker/timeout/backoff для Feign; DLQ для Kafka; алертинг на всплески
113	**LOG-007**	Нарушения ограничений БД при записи (Constraint 1.1 млн / DataIntegrity 1.0 млн) — риск пропуска записей аудита; усиливает SEC-015	audit-service (целостность)	grandTotalCurrent.exc: ConstraintViolationException=1102647, DataIntegrityViolationException=1007520 — см. Приложение И	Средняя	Средний	Идемпотентная запись аудита; мониторинг отказов; сбой не теряет событие
114	**LOG-008**	Секреты в журналах (135: пароли/токены/Authorization); избыточный служебный INFO	Политика логирования / секреты	logs_summary.txt: секретов=135; INFO-шум (Resolving eureka endpoints/5мин, +++++ start timer	Средняя	Средний	Маскировать секреты в журналах; пересмотр уровней

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		раздувает объем и прячет ошибки; NPE в эксплуатации 217 505		+++++); NullPointerException=217505 — см. Приложение И			(служебное→DEBUG); устранить NPE
115	**INFRA-001**	Критическое исчерпание емкости файловых хранилищ: 8 из 16 ЦОД заполнены ≥90%, несколько (ВКО, Алматы, Костанай, Атырау, Шымкент, ЗКО) — на 100%. При 100% заполнении возникает угроза невыполнения операций записи — не только сохранения файлов, но и записей в БД (создание учетных записей, формирование/выдача архивных справок): переполнение вызывает каскад ошибок PostgreSQL «current transaction is aborted» (2-я по частоте в журналах — свыше 60 млн). Сопутствующий риск — деградация производительности. Усугубляется	Файловые хранилища региональных ЦОД (сетевое хранилище / file-storage)	infra/«Состояние хранилища по регионам» + work/infra_data.json (8 ЦОД ≥90%: ВКО/Алматы/Костанай/Атырау/Шымкент/ЗКО — 100%, Кызылорда 99%, Жетісу 90%); Приложение В.2; связь с LOG-002	Высокая	Критический	Немедленно увеличить емкость файловых хранилищ в переполненных ЦОД (приоритет — заполненные на 100%); параллельно устранить LOG-002 (восстановить автоочистку просроченных файлов) и внедрить мониторинг/алертинг заполнения с пороговыми уведомлениями

№	ID	Описание риска	Компонент	Доказательство (файл:строка)	Вер-ть	Крит.	Рекомендация
		неработающей автоочисткой (LOG-002)					
116	**INFRA-002**	Критически низкая частота резервного копирования (cron-скрипты раз в месяц, фактический RPO до 30 дней) и неполное покрытие: загружаемые файлы пользователей на втором сервере приложений не резервируются (нехватка места, связь с INFRA-001) — только синхронизация на резервный стенд без гарантий восстановления; RTO операционными регламентами не определен; отсутствует централизованная система управления резервным копированием с мониторингом и алертингом	Инфраструктура резервного копирования (все региональные ЦОД)	Документация АО «НИТ», раздел 12 «Резервное копирование»: cron-скрипты раз в месяц, диск /backups по NFS; резервируются приложения, логи, БД, логи БД, данные Elasticsearch; загружаемые файлы пользователей на 2-м сервере приложений не резервируются (связь с INFRA-001, LOG-002)	Высокая	Критический	Перейти на ежедневное резервное копирование с непрерывным журналированием транзакций БД; обеспечить полное покрытие загружаемых файлов пользователей; внедрить централизованную систему резервного копирования с мониторингом выполнения заданий и алертингом; определить и зафиксировать целевые RPO и RTO (меры OP.1–OP.3, Приложение E)

Приложение Д. Матрица уязвимостей (Вероятность × Воздействие)

Соответствующие данные представлены в таблице 17.

Таблица 17 — Матрица уязвимостей (Вероятность x Воздействие)

Вероятность \ Воздействие	Критическое	Высокое	Среднее	Низкое
Высокая	VER-001, SEC-001, SEC-002, SEC-003, SEC-004, SEC-008, SEC-011, SEC-018, SEC-025, DB-012, DB-015, FE-002, COMP-001, PORTAL-001, PORTAL-002, PORTAL-003, PORTAL-004, SEC-028, SEC-029, SEC-032, LOG-001, LOG-002, INFRA-001, INFRA-002	ARCH-001, VER-003, VER-004, VER-005, VER-006, SEC-005, SEC-006, SEC-007, SEC-009, SEC-012, SEC-022, SEC-023, SEC-027, INT-003, INT-007, DB-008, DB-009, DB-011, DB-013, DB-016, BPM-001, BPM-003, QA-001, QA-002, FE-001, FE-004, COMP-002, PORTAL-005, PORTAL-009, PORTAL-011, SEC-031, LOG-003, LOG-004, LOG-005, LOG-006	VER-002, LIC-001, PORTAL-012	—
Средняя	SEC-019	ARCH-002, SEC-010, SEC-013, SEC-015, SEC-017, SEC-020, SEC-026, INT-001, INT-004, INT-006, BPM-002, FE-003, FE-005, PORTAL-006, PORTAL-007, PORTAL-008, PORTAL-010, SEC-030	ARCH-003, ARCH-004, VER-007, VER-008, SEC-014, SEC-016, SEC-024, INT-002, DB-001, DB-010, DB-014, BPM-005, LIC-004, QA-003, QA-004, QA-006, FE-006, COMP-003, PORTAL-013, LOG-007, LOG-008	—

Вероятность \ Воздействие	Критическое	Высокое	Среднее	Низкое
Низкая	—	—	SEC-021, DB-003, DB-005	INT-005, DB-002, DB-004, DB-006, DB-007, BPM-004, LIC-002, LIC-003, LIC-005, QA-005

Находки с критичностью «не применимо» (COMP-004) отнесены в столбец «Низкое».

Приложение Е. Приоритизированный план мероприятий

План приоритизирован по волнам реализации — от аварийных мер к долгосрочной модернизации — и закрывает требования Технической спецификации: roadmap с кратко- и долгосрочными мерами и план по обеспечению отказоустойчивости и резервированию (п. 3.5), а также измеримые показатели результата (п. 3.6). Каждое мероприятие связано с идентификаторами находок реестра (Приложение Г); оценка трудоемкости согласована с финансово-технической оценкой (раздел 5.5). Рекомендации носят консультативный характер и могут быть реализованы Заказчиком самостоятельно либо с привлечением подрядчика.

Соответствующие данные представлены в таблице 18.

Таблица 18 — Приоритизированный план мероприятий

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
B0.1	Расширить емкость переполненных файловых хранилищ (ЦОД с заполнением 90–100%)	INFRA-001, LOG-002	Волна 0 (0–72 ч)	Средняя	Свободная емкость восстановлена (заполнение < 85%); операции записи (прием документов, создание учетных записей, выдача архивных справок) выполняются без сбоев
B0.2	Отозвать и перевыпустить скомпрометированные ключи ЭЦП и секреты, удалить их из репозитория	SEC-001, PORTAL-001, DB-015, SEC-025, SEC-029, SEC-031	Волна 0 (0–72 ч)	Низкая	Все ключи и секреты отозваны и перевыпущены; удалены из системы контроля версий; перенесены в защищенное хранилище (Vault/HSM)
B0.3	Отключить глобальное доверие TLS (trust-all) в системе и портале	SEC-018, PORTAL-003	Волна 0 (0–72 ч)	Низкая	trust-all удален; настроен truststore УЦ РК; внешние соединения проверяют сертификаты

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
B0.4	Закрыть открытые без аутентификации сервисы и анонимные операции	SEC-003, SEC-004, PORTAL-002	Волна 0 (0–72 ч)	Низкая	Все эндпоинты требуют аутентификации; анонимная смена пароля и проверка ИИН (check-iin) закрыты
B1.1	Устранить инъекционные уязвимости (XXE, SQL/JPQL) и небезопасную десериализацию	SEC-002, SEC-019, SEC-030, SEC-032, PORTAL-004, PORTAL-005, PORTAL-008	Волна 1 (до 1 мес)	Средняя	XML-парсинг защищен от внешних сущностей единой фабрикой; SQL параметризован; небезопасная десериализация устранена
B1.2	Прекратить вывод ИИН, персональных данных и секретов в журналы (в первую очередь audit-service)	SEC-008, LOG-001, LOG-008, PORTAL-012	Волна 1 (до 1 мес)	Средняя	Маскирование на уровне логгера; количество ИИН и секретов в журналах сведено к нулю
B1.3	Исправить плановое задание автоочистки просроченных файлов и восстановить ротацию журналов	LOG-002, LOG-004, LOG-005	Волна 1 (до 1 мес)	Средняя	Задание выполняется без сбоев; журналы ротируются с лимитами по объему; брошенные .tmp-файлы очищены
B1.4	Внедрить мониторинг и алертинг (заполнение хранилищ, отказ плановых задач, доля ошибок ERROR)	INFRA-001, LOG-002, LOG-004	Волна 1 (до 1 мес)	Низкая	Настроены пороговые уведомления; инциденты выявляются проактивно, до отказа
B1.5	Ввести ограничение частоты запросов на аутентификацию, смену пароля и проверку ИИН	SEC-022	Волна 1 (до 1 мес)	Низкая	Перебор паролей и энумерация ИИН заблокированы (throttling/CAPTCHA)
B1.6	Убрать реальные ИИН и захардкоженные сетевые адреса из конфигурации и активного кода	SEC-009, FE-004, QA-003	Волна 1 (до 1 мес)	Низкая	Конфигурация не содержит персональных данных; сетевые адреса вынесены в окружение/шлюз

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
B2.1	Внедрить ролевой контроль доступа (RBAC) на уровне сервисов и авторизацию на уровне объектов (защита от IDOR)	SEC-011, SEC-027, SEC-028, COMP-002	Волна 2 (1–6 мес)	Средняя	Каждый сервис проверяет роль и принадлежность объекта; доступ к чужим сущностям по прямому идентификатору невозможен
B2.2	Обеспечить иммутабельность и защиту доступа журнала аудита	SEC-012, SEC-015, COMP-003, LOG-007	Волна 2 (1–6 мес)	Средняя	Журнал ведется в режиме append-only с контролем целостности; доступ по роли аудитора; события не теряются при сбоях
B2.3	Защитить поисковый индекс Elasticsearch (TLS и аутентификация) и минимизировать в нем персональные данные	DB-011, DB-012	Волна 2 (1–6 мес)	Средняя	Доступ к индексу аутентифицирован и шифрован; объем персональных данных в индексе минимизирован
B2.4	Оптимизировать работу с данными: устранить N+1, добавить недостающие индексы, переписать запрос выборки дела	DB-008, DB-009, DB-010, DB-013, DB-014, DB-016	Волна 2 (1–6 мес)	Средняя	p95 выборки дела (1000 документов) < 2 с; отказы 504 устранены; включен пакетный режим JDBC
B2.5	Повысить надежность интеграций: обработка ошибок Kafka-консьюмеров, очереди недоставленных сообщений (DLQ), предохранители, асинхронность интеграции с ОДО	INT-001, INT-002, INT-004, INT-007, QA-004, LOG-006	Волна 2 (1–6 мес)	Средняя	Консьюмеры обрабатывают ошибки и подтверждают обработку; настроены DLQ и повторные попытки; внешние вызовы не блокируют обработчики
B2.6	Настроить управление бизнес-процессами Camunda: TTL истории, валидация и	BPM-002, BPM-003, BPM-004, BPM-005	Волна 2 (1–6 мес)	Средняя	История ACT_HI_* ограничена TTL с очисткой; деплой процессов валидируется и авторизуется; зависшие задачи отслеживаются

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
	авторизация деплоя BPMN, эскалации задач				
B2.7	Усилить безопасность клиентской части: токены в httpOnly-cookies, серверный контроль срока сессии, политика CSP и санитизация вывода	FE-002, FE-003, FE-005	Волна 2 (1–6 мес)	Средняя	Токены недоступны из JavaScript; XSS-векторы закрыты; срок сессии контролируется сервером
B2.8	Повысить качество кода: устранить пустые блоки catch, ввести единую обработку ошибок и базовое тестовое покрытие	QA-001, QA-002, QA-006, SEC-024, FE-006, PORTAL-013	Волна 2 (1–6 мес)	Высокая	Исключения не проглатываются; действует единый обработчик ошибок; критичные сервисы покрыты тестами с порогом в CI
B2.9	Закрыть служебные интерфейсы: actuator, Eureka, Config Server, Kafka и панель Kafdrop	SEC-016, SEC-017, SEC-026	Волна 2 (1–6 мес)	Низкая	Служебные эндпоинты под аутентификацией и ролью; брокер и панель недоступны извне
B2.10	Привести криптографические практики к стандарту: SHA-256 для контроля целостности, обязательная проверка отзыва сертификатов (OCSP), корректная настройка CSRF	SEC-010, SEC-014, SEC-020, SEC-021	Волна 2 (1–6 мес)	Низкая	SHA-1 заменен на SHA-256; отзыв сертификатов проверяется в промышленной среде; CSRF включен где применимо
OP.1	Внедрить регламент резервного копирования по схеме 3-2-1 с целевыми RPO ≤ 24 ч (при непрерывном журналировании транзакций — до ≤ 1 ч) и RTO ≤ 4 ч; перейти с ежемесячного копирования на ежедневное,	INFRA-002	Отказоустойчивость (1–6 мес)	Средняя	Ежедневное полное копирование и непрерывное журналирование транзакций; файлы пользователей резервируются; копии хранятся не менее чем в двух средах, одна — вне основной площадки

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
	обеспечить полное покрытие файлов пользователей				
OP.2	Обеспечить регулярное тестирование восстановления из резервных копий	INFRA-002	Отказоустойчивость (1–6 мес)	Средняя	Восстановление проверяется не реже одного раза в квартал; фактические RPO/RTO подтверждены и задокументированы
OP.3	Сформировать и поддерживать план аварийного восстановления (DR) и централизованную систему резервного копирования с мониторингом и алертингом	INFRA-002	Отказоустойчивость (1–6 мес)	Средняя	Регламентированы процедуры переключения и восстановления; состояние копий и реплик отслеживается мониторингом, сбои заданий фиксируются алертингом
B3.1	Обновить компоненты, снятые с поддержки (EOL): Elasticsearch/OpenSearch, Java 17 и Spring Boot 3, Apache Camel, Camunda, Vue 3, клиентские библиотеки	VER-001, VER-003, VER-004, VER-005, VER-006, BPM-001, FE-001, PORTAL-011	Волна 3 (6–18 мес)	Высокая	Все компоненты переведены на поддерживаемые версии; известные уязвимости (CVE) закрыты
B3.2	Рефакторинг архитектуры данных: разделение общей БД по доменам, развязка циклических зависимостей через события	ARCH-001, ARCH-002, ARCH-004	Волна 3 (6–18 мес)	Высокая	Сервисы не делят одну базу данных; циклические Feign-зависимости устранены
B3.3	Принять решение по устаревшему порталу: миграция на современную платформу или вывод из эксплуатации	ARCH-003, PORTAL-006, PORTAL-007, PORTAL-009, PORTAL-010	Волна 3 (6–18 мес)	Высокая	Роль портала определена; критичные дефекты ИБ устранены либо портал выведен из эксплуатации

№	Мероприятие	Находки	Волна / срок	Трудоемкость	Критерий завершения
B3.4	Верификация версий и лицензий: предоставить parent POM для полной верификации версий; подтвердить лицензии крипто-компонентов РК	VER-008, LIC-004	Волна 3 (6–18 мес)	Средняя	Версии полностью верифицируемы; лицензии крипто-компонентов РК подтверждены
B3.5	Закрепить практику безопасной разработки: запрет хардкода секретов в CI, контроль зависимостей, периодический аудит	SEC-005, SEC-006, SEC-007, QA-005	Волна 3 (6–18 мес)	Средняя	Секреты не попадают в код (проверка в конвейере CI); зависимости отслеживаются; мертвый код удален

Измеримые показатели успеха — целевые значения для контроля реализации плана (Техническая спецификация, п. 3.6):

Соответствующие данные представлены в таблице 19.

Таблица 19 — Целевые измеримые показатели (KPI) реализации плана

Показатель	Целевое значение	Контролирует мероприятия
Заполнение файловых хранилищ во всех ЦОД	< 80%	B0.1, B1.4
Количество ИИН и секретов в журналах	0	B1.2
Доля записей уровня ERROR в журналах	< 0,1% от объема	B1.3, B2.5
Время выборки документов дела (1000 док.), p95	< 2 с; отказов 504 нет	B2.4
Время авторизации, p95	< 1 с	B0.4, B1.5
Доля эндпоинтов с проверкой роли (method-level)	100%	B2.1
Покрытие тестами критичных сервисов	≥ 60% (ориентир)	B2.8

Показатель	Целевое значение	Контролирует мероприятия
Резервное копирование	RPO ≤ 24 ч (≤ 1 ч при непрерывном журналировании), RTO ≤ 4 ч; тест восстановления ежеквартально	ОР.1–ОР.3
Компоненты вне поддержки (EOL) в эксплуатации	0	В3.1

Приложение Ж. Версии компонентов и сроки поддержки (EOL)

Сроки окончания поддержки (EOL) сверены с авторитетными источниками (endoflife.date и официальные сайты вендоров) на 15.06.2026.

Соответствующие данные представлены в таблице 20.

Таблица 20 — Версии компонентов и сроки поддержки (EOL)

Компонент	**Версия**	**Проверенный статус поддержки (EOL)**
Java	8	Oracle Premier до 31.03.2022; Extended до 31.12.2030; патчится LTS-вендорами (Temurin/Corretto/Azul). Устаревшая LTS.
Spring Boot	2.x (2.7)	OSS-поддержка завершена 30.06.2023; коммерческая до 30.06.2029
Spring Cloud / Security OAuth	2.0.x / 2.2.1	Соответствует Spring Boot 2.x — вне поддержки
Elasticsearch	6.4.2	Линейка 6.x — EOL 10.02.2022; Transport Client удален в ES7. Критично.
Apache Camel	2.23.2	Последняя 2.x (2.25) — EOL 31.01.2022
Apache Karaf	4.2.4	Устаревшая (2020), вне активной поддержки
Apache CXF	3.2.7 / 3.3.2	Линейка 3.x устаревшая; актуальна 4.x
Camunda BPM (Community)	7.11.0	Camunda 7 CE — EOL: последний релиз 7.24 (14.10.2025), далее без патчей
Hibernate ORM	5.4.17	EOL 10.01.2022
Liquibase	3.8.6	Устаревшая (2019); LGPL — compliant
Apache POI	3.17 / 5.2.3	3.17 (2016) критически устаревшая; рассинхрон версий
Apache PDFBox	2.0.15/16	Линейка 2.0.x устаревшая; актуальна 3.0
JasperReports	6.7.0	Community (LGPL); устаревшая, но соответствие соблюдено
ABBYY FineReader Engine	12.0	Коммерческая, устаревшая; лицензионное соответствие не верифицировано из исходного кода

Компонент	Версия	Проверенный статус поддержки (EOL)
Vue.js	2.7.14	Vue 2 — EOL 31.12.2023
Frontend (Element UI / CKEditor / BPMN.js / ECharts / Webpack / Axios)	2.13 / 5 v12.4 / 4.0 / 4.2-rc / 4 / 0.18	Все устаревшие/без активной поддержки; ряд — известные CVE
WildFly (портал)	16.0.0.Final	Релиз 2019; community поддерживает только актуальный релиз (ныне 30+)

Источники: endoflife.date (java, spring-boot, elasticsearch, apache-camel, hibernate, vue), camunda.com (Camunda 7 CE EOL), wildfly.org. Часть версий backend управляется отсутствующим parent POM и не финализируема из кода (VER-008).

Приложение И. Анализ журналов эксплуатации

Источник: выгрузка журналов по репрезентативной выборке региональных ЦОД (области/города РК). Период: 2020-08-28…2026-07-04. Проанализировано строк (живые .log + суточные .zip): 1 645 470 286. Метод: потоковый автоматизированный скан без распаковки на диск с категоризацией ошибок и фингерпринтингом сообщений. Поскольку во всех ЦОД развернута единая кодовая база (одинаковое ПО, обособленные региональные системы), результаты репрезентативны для всех региональных инсталляций. Персональные данные не разглашаются: ИИН маскированы, шаблоны сообщений обезличены.

Логи — эксплуатационные данные. Раздел дает фактическое подтверждение и дополнение находок аудита кода (см. LOG-001…LOG-008 в реестре, Приложение Г). Исторические незавершенные файлы ротации (.tmp) учтены отдельно от текущего состояния. Примечание: сырье ERROR (свыше 220 млн) — это десятки повторяющихся дефектов, размноженных циклами отказов; реальную картину дают категоризация и топ-проблемы ниже.

И.1 Сводные показатели

Соответствующие данные представлены в таблице 21.

Таблица 21 — Сводные показатели журналов эксплуатации

Показатель	Текущее состояние (live+zip)	Исторические .tmp
Записей уровня ERROR	221 992 497	4 028 888
Исключений всего (вкл. цепочки)	254 407 077	—
Сбои интеграций (Connect/Feign/timeout)	1 183 544	3 684 966

Показатель	Текущее состояние (live+zip)	Исторические .tmp
Строк стектрейсов	1 154 450 355	58 126 876
ИИН в журналах (по ключу iin/declarantIIN)	160 318	268
Секретов (пароли/токены) в журналах	156	—
Брошенных .tmp-файлов / объем	—	302 шт / 7 316 МБ

И.2 Категоризация ошибок (по классам дефектов)

Соответствующие данные представлены в таблице 22.

Таблица 22 — Категоризация ошибок по классам дефектов

Категория	Доля	Кол-во	Топ-исключения
База данных / персистентность	81.2%	206 537 467	GenericJDBCException: 100 832 861; JpaSystemException: 100 832 855; ConstraintViolationException: 1 671 346; DataIntegrityViolationException: 1 335 906
Обработка файлов / OCR (I/O)	16.9%	42 922 914	IOException: 42 866 492; IOFileUploadException: 55 412; EOFException: 514; ZipException: 332
Доменные (бизнес) ошибки	0.5%	1 374 414	expertiseException: 754 419; SeadServiceException: 619 993; ExpertiseException: 2
Интеграции / сеть (RPC)	0.5%	1 339 422	FeignException: 604 569; NoRouteToHostException: 154 755; ClientException: 152 680; UnknownHostException: 110 443
Прочее / неклассифицированное	0.4%	1 018 651	onError: 452 650; UnsatisfiedLinkError: 130 487; RuntimeException: 101 678; TikaException: 69 080
Дефекты кода	0.3%	808 373	IllegalStateException: 516 739; NullPointerException: 253 545; ClassCastException: 26 873; ArrayIndexOutOfBoundsException: 6 039
Очереди / Kafka	0.1%	254 872	ListenerExecutionFailedException: 254 872
Почтовые уведомления (SMTP)	0%	110 387	MessagingException: 110 387

Категория	Доля	Кол-во	Топ-исключения
Данные / парсинг / XML	0%	17 418	NumberFormatException: 16 693; DateTimeParseException: 705; JsonMappingException: 14; SAXParseException: 3
ЭЦП / криптография	0%	12 162	CertificateException: 10 860; SignatureException: 1 300; CMSException: 2
Сбои запуска / контекста	0%	8 852	BeanCreationNotAllowedException: 5 627; BeanCreationException: 2 030; WebServerException: 717; ApplicationContextException: 478
Безопасность / доступ	0%	2 145	BadCredentialsException: 1 320; SessionAuthenticationException: 783; InsufficientAuthenticationException: 42

И.3 Топ-проблемы — конкретные шаблоны сообщений

Соответствующие данные представлены в таблице 23.

Таблица 23 — Топ-проблемы — шаблоны сообщений

Кол-во	Категория	Шаблон сообщения (обезличено)
99 314 946	База данных / персистентность	k.i.s.f.s.ScheduledFileStorage|-----+++++----->>> autoDeleteExpiredDeletedFiles ERROR: org.springframework.orm.jpa.JpaSy
66 309 991	База данных / персистентность	o.h.e.jdbc.spi.SqlExceptionHelper|ОШИБКА: текущая транзакция прервана, команды до конца блока транзакции игнорируются
34 464 435	База данных / персистентность	o.h.e.jdbc.spi.SqlExceptionHelper|ERROR: current transaction is aborted, commands ignored until end of transaction block
7 391 335	Обработка файлов / OCR (I/O)	k.i.s.f.s.impl.RecognizeServiceImpl|SPLIT FILE ERROR: java.io.IOException: Недопустимый аргумент
5 734 364	Обработка файлов / OCR (I/O)	k.i.s.f.s.impl.RecognizeServiceImpl|SPLIT FILE ERROR: java.io.IOException: Invalid argument
1 218 700	Обработка файлов / OCR (I/O)	k.i.s.f.s.impl.RecognizeServiceImpl|SPLIT FILE ERROR: java.io.IOException: Input/output error

Кол-во	Категория	Шаблон сообщения (обезличено)
999 414	База данных / персистентность	o.s.s.s.TaskUtils$LoggingErrorHandler|Unexpected error occurred in scheduled task. org.springframework.transaction.Unexp
988 074	База данных / персистентность	k.i.s.f.s.impl.RecognizeServiceImpl|Find all fileRecognizes error: org.springframework.dao.DataIntegrityViolationExcepti
899 351	База данных / персистентность	o.h.e.jdbc.spi.SqlExceptionHelper|ОШИБКА: UPDATE или DELETE в таблице "?" нарушает ограничение внешнего ключа "?" таблиц
729 743	База данных / персистентность	k.i.s.f.s.i.FileStorageServiceImpl|Find all fileRecognizes error: org.springframework.orm.jpa.JpaSystemException: could
729 743	База данных / персистентность	k.i.s.f.s.impl.RecognizeServiceImpl|Find all fileRecognizes error: org.springframework.orm.jpa.JpaSystemException: could
495 658	База данных / персистентность	k.i.s.f.s.ScheduledFileStorage|-----+++++->>> autoDeleteExpiredDeletedFiles ERROR: org.springframework.dao.InvalidDa
184 507	Обработка файлов / OCR (I/O)	k.i.s.f.s.impl.RecognizeServiceImpl|OCR ERROR...
183 416	Обработка файлов / OCR (I/O)	k.i.s.f.s.impl.RecognizeServiceImpl|OCR START ERROR... java.lang.NullPointerException: null
167 637	Очереди / Kafka	o.s.k.listener.LoggingErrorHandler org.springframework.kafka.listener.ListenerExecutionFailedException: Listener method

И.4 Рейтинг сервисов по ошибкам

Соответствующие данные представлены в таблице 24.

Таблица 24 — Рейтинг сервисов по ошибкам

Сервис	ERROR	Сбои интеграций	ИИН в журналах
file-storage-service	220 825 368	4 549	0
document-service	503 506	751 738	1 651

Сервис	ERROR	Сбои интеграций	ИИН в журналах
audit-service	339 615	1 878	158 667
notification-service	188 394	110 707	0
reference-service	77 763	125 488	0
integration-service	42 439	139 240	0
oauth2-service	8 339	3 043	0
gateway-service	2 696	43 421	0
sign-service	1 938	536	0
report-service	757	494	0
socket-service	480	721	0
apostille-service	366	361	0

И.5 Показатели по регионам (ЦОД)

Соответствующие данные представлены в таблице 25.

Таблица 25 — Показатели по регионам (ЦОД)

Регион (ЦОД)	ERROR	Сбои интегр.	ИИН	.tmp (шт/МБ)
ЗКО	126 301 461	22 317	2 376	5/101
Карагандинская область	69 632 229	31 436	25 045	19/548
Алматы	13 610 467	49 518	2 223	48/399
ВКО	3 888 856	100 373	15 337	33/355
Атырауская область	1 783 877	309 680	1 868	65/2707
Кызылординская область	953 985	60 325	3 846	1/1
Павлодар	947 003	14 624	17 339	3/5

Регион (ЦОД)	ERROR	Сбои интегр.	ИИН	.tmp (шт/МБ)
Шымкент	944 848	125 347	320	39/677
Туркестанская область	943 340	60 324	8 755	14/179
СКО	928 223	10 385	9 530	10/175
Актюбинская область	676 969	8 554	8 647	23/464
Костанайская область	661 261	340 445	6 485	39/1654
Жамбылская область	382 746	14 126	13 898	2/42
Алматинская область	197 892	25 149	38 117	0/0
Мангыстауская область	139 340	10 941	6 532	1/9

И.6 Утечки ИИН по сервисам и тренд

Соответствующие данные представлены в таблице 26.

Таблица 26 — Утечки ИИН по сервисам

Сервис	ИИН в журналах
audit-service	158 667
document-service	1 651

Тренд ошибок: 480 дней с ошибками, диапазон 2019-07-23…2026-06-18 (нератируемые live-логи накапливаются с развертывания — дефекты не устранялись годами). Пиковые дни: 2026-03-20 (2 931 037), 2026-03-21 (2 912 041), 2026-03-25 (2 905 873), 2026-03-24 (2 904 442), 2026-03-23 (2 902 755).

И.7 Инвентарь брошенных .tmp (топ по размеру)

Соответствующие данные представлены в таблице 27.

Таблица 27 — Инвентарь брошенных временных файлов ротации

Регион	Файл	МБ	Дата	Топ-исключения
Алматы	expertise-service.2025-05-18.0.log3001231105760373 8.tmp	78.7	2025-05-17	HttpServerErrorException:84363, handleError:84363
Алматы	report-service.2025-05-18.0.log3001231316321983 5.tmp	78.3	2025-05-17	HttpServerErrorException:84315, handleError:84315
Атырауская область	integration-service.2020-08-16.0.log103977275485162.tmp	58.0		ConnectException:29354, IllegalStateException:14677
Атырауская область	integration-service.2020-08-17.0.log190378553968085.tmp	57.9		ConnectException:29290, IllegalStateException:14645
Атырауская область	integration-service.2020-08-18.0.log276777702566981.tmp	57.8		ConnectException:29244, IllegalStateException:14622
Атырауская область	sign-service.2020-08-16.0.log103976629543506.tmp	56.5		ConnectException:28724, IllegalStateException:14362
Атырауская область	sign-service.2020-08-18.0.log276779096503960.tmp	56.2		ConnectException:28620, IllegalStateException:14310
Атырауская область	report-service.2020-08-16.0.log103982355020055.tmp	54.8		ConnectException:27754, IllegalStateException:13877
Атырауская область	report-service.2020-08-17.0.log190381057628825.tmp	54.7		ConnectException:27690, IllegalStateException:13845
Атырауская область	gateway-service.2020-08-17.0.log185610797879040.tmp	52.2	2020-08-17	ConnectException:26684, IllegalStateException:13342
Атырауская область	gateway-service.2020-08-18.0.log271078564587137.tmp	51.5	2020-08-18	ConnectException:26336, IllegalStateException:13168
Атырауская область	sign-service.2020-08-17.0.log182679205822821.tmp	51.4		ConnectException:26138, IllegalStateException:13069

Регион	Файл	МБ	Дата	Топ-исключения
Атырауская область	report-service.2020-08-18.0.log271153335286449.tmp	51.1		ConnectException:25866, IllegalStateException:12933
Атырауская область	gateway-service.2020-08-16.0.log97025453720058.tmp	50.9	2020-08-16	ConnectException:26028, IllegalStateException:13014
Карагандинская область	file-storage-service.2026-02-04.6.log2615523046388525.tmp	50.2	2026-02-04	JpaSystemException:93347, GenericJDBCException:93347
Карагандинская область	file-storage-service.2026-02-26.6.log4516321711316529.tmp	50.1	2026-02-26	JpaSystemException:92915, GenericJDBCException:92915

Сводные результаты анализа эксплуатационных журналов представлены в таблицах настоящего приложения. Полные агрегированные данные передаются Заказчику в электронном виде на машинном носителе.

Приложение К. Результаты нагрузочного тестирования

Нагрузочное тестирование проведено на выделенном стенде, идентичном промышленной среде (инструмент — Apache JMeter), по трем профилям, соответствующим конфигурациям ЦОД. Целевые операции — авторизация (POST /oauth/token) и выборка документов дела (GET /documents/deal/{id}). Топология запроса: шлюз (Zuul) → oauth2-service → document-service → PostgreSQL. Порог отказа — таймаут шлюза (~60 с): время отклика свыше 60 с фиксируется как ошибка 504.

Шкала оценки времени отклика:

– менее 1 с — в норме;

– 1–10 с — деградация;

– 10–60 с — критично;

– свыше 60 с — отказ.

Проведены два вида прогонов: тест А — объемный (1 пользователь, наращивание объема дела); тест В — конкурентный (50 одновременных пользователей, дело 1 000 документов, пиковый сценарий).

Соответствующие данные представлены в таблице 28.

Таблица 28 — Профили нагрузочного тестирования и сопоставление с ЦОД

Профиль	**Конфигурация**	**ЦОД**
P0 — ЦОД АП	98 ядер / 288 ГБ RAM / ~15,3 ТБ	ЦОД АП (Архива Президента)

Профиль	Конфигурация	ЦОД
P1 — базовая группа	46 ядер / 432 ГБ RAM	13 региональных ЦОД (Акмолинская, Актюбинская, Алматинская, ВКО, Жамбылская, ЗКО, Карагандинская, Костанайская, Кызылординская, Мангистауская, г. Алматы, Павлодарская, Туркестанская)
P2 — усиленная группа	92–136 ядер / 862–864 ГБ RAM	г. Шымкент, Северо-Казахстанская, Атырауская

Соответствующие данные представлены в таблице 29.

Таблица 29 — Тест А (объемный, 1 пользователь): медиана времени выборки документов дела по объему

Операция / объем дела	P0	P1	P2	Оценка
Авторизация (oauth2)	0,44 с	0,55 с	0,47 с	В норме
Выборка дела, 1 000 док.	7,5 с	11 с	8,1 с	Деградация
Выборка дела, 5 000 док.	51 с	57 с	54 с	Критично
Выборка дела, 10 000 док.	26 с	38 с	28 с	Критично
Выборка дела, ≥ 20 000 док.	отказ 504	отказ 504	отказ 504	Отказ

Соответствующие данные представлены в таблице 30.

Таблица 30 — Тест В (50 одновременных пользователей, дело 1 000 док.): время отклика выборки и доля ошибок

Профиль	avg	p50	p90	p95	p99	Доля 504
P0 — ЦОД АП	33 с	28 с	57 с	504	504	~15%
P1 — базовая группа	48 с	52 с	504	504	504	~45%
P2 — усиленная группа	22 с	18 с	41 с	56 с	504	~6%

Соответствующие данные представлены в таблице 31.

Таблица 31 — Утилизация ресурсов под конкурентной нагрузкой (тест В, установившийся участок)

Профиль	CPU приложения	CPU БД	Пул соединений БД	Узкое место
P0 — ЦОД АП	~65%	~98%	100/100 (исчерпан)	БД (CPU/диск) + пул потоков шлюза
P1 — базовая группа	~75%	~100% (насыщение)	100/100 (исчерпан)	БД (насыщение) + пул потоков шлюза
P2 — усиленная группа	~55%	~90%	90/100	БД близка к насыщению

Соответствующие данные представлены в таблице 32.

Таблица 32 — Первопричина: чистое время запроса в БД по объему дела (EXPLAIN ANALYZE)

Объем дела	P0	P1	P2
1 000 документов	0,89 с	1,25 с	0,95 с
10 000 документов	12,2 с	17,5 с	13,1 с
40 000 документов	119,7 с	168 с	127 с

Выводы. Авторизация узким местом не является. Выборка документов дела деградирует сверхлинейно (сложность близка к квадратичной) из-за коррелированного подзапроса по иерархии документов с полным сканированием таблицы связей (~61 000 строк) без индекса. Отказ (504) наступает при объеме дела ≥ 20 000 документов, а под конкурентной нагрузкой — при насыщении базы данных. Узкое место — база данных (CPU, дисковый ввод-вывод) и пул потоков шлюза; различие профилей — лишь в запасе по параллелизму (тем меньше, чем меньше ядер). Увеличение тира оборудования первопричину не устраняет — требуется исправление запроса и индексация (находки DB-016, DB-008, DB-009, QA-004). На ЦОД со 100% заполнением файловых хранилищ нагрузочное тестирование невозможно из-за отсутствия свободного места под тестовые данные (INFRA-001).

Лист согласования

Министерство культуры и информации Республики Казахстан

Ф.И.О.	Должность/Подразделение	Подпись
Биенова Ж.Б.	Рук. упр ДУТПМ	
Сыздыгалин И.Н.	Зам. дир ДУТПМ	

ТОО «Cuttle systems»

Ф.И.О.	Должность/Подразделение	Подпись
Цой Андрей Евгеньевич	Директор по развитию, ТОО «Cuttle systems»	
Лукьянченко Андрей Григорьевич	Главный архитектор	
Нигиманова Айгерим Жуматаевна	Ведущий специалист по информационной безопасности, ТОО «Cuttle systems»	
Зейнолла Уәлихан Бағланұлы	Инженер инфраструктуры, ТОО «Cuttle systems»	
Асылбекұлы Бек	Системный аналитик	