Технологические учётные записи

Документ: ИБ-69 · **Версия:** 1.0 · **Дата:** 22.06.2026 · **Классификация:** Конфиденциально

Параметр	Значение
Информационная система	ЛКИ
Владелец документа	Команда разработки
Согласующий	Служба информационной безопасности
Статус	На согласовании

История изменений

Версия	Дата	Автор	Изменение
1.0	22.06.2026	Команда разработки	Первоначальная редакция (реестр + матрица доступа)

---

1. Общие сведения

1.1. Назначение

Документ описывает технологические (служебные) учётные записи, токены и секреты, необходимые для работы ИС ЛКИ: их назначение, права, порядок заведения, хранения и ротации, а также матрицу доступа.

1.2. Область применения

Положения обязательны для администраторов при развёртывании и эксплуатации системы на любом Linux-сервере.

1.3. Термины и сокращения

Сокращение	Расшифровка
`.env`	Файл переменных окружения каталога установки
vault	Централизованное хранилище секретов
HMAC	Код аутентификации сообщения на основе хеша

2. Классификация учётных записей и секретов

Класс	Состав	Раздел
Учётные записи инфраструктуры	СУБД, Redis, Qdrant, объектное хранилище	3.1
Прикладные секреты (криптография)	Подпись токенов, pepper, ключ лицензии	3.2
Учётная запись первичного администратора	Bootstrap-администратор	3.3
Межсервисные токены	Сервис медиа, LLM-прокси, метрики	3.4
Секреты входящих интеграций (вебхуков)	E-mail, транскрипция, OCR, Telegram	3.5
Внешние провайдерские ключи	API-ключи LLM/поиска, мониторинг	3.6

3. Реестр технологических учётных записей и секретов

3.1. Учётные записи инфраструктуры

Учётная запись	Переменные	Назначение	Права	Порядок заведения
PostgreSQL (владелец БД)	`POSTGRES_USER`, `POSTGRES_PASSWORD`, `POSTGRES_DB`	Подключение приложения к СУБД	Полные права на свою БД	Создаётся при первом запуске СУБД
Redis	`REDIS_PASSWORD`	Очереди и кэш	Доступ к инстансу	Задаётся при запуске Redis
Векторная БД (Qdrant)	`QDRANT_API_KEY` (опц.)	Векторное хранилище	Доступ к коллекциям	Опционально; по умолчанию loopback
Объектное хранилище (S3)	`S3_ACCESS_KEY`, `S3_SECRET_KEY`, `S3_ENDPOINT`	Документы и артефакты	Чтение/запись в bucket	Заводится в S3-совместимом хранилище

Учётная запись	Переменные	Назначение	Права	Порядок заведения
	, `S3_BUCKET`, `S3_REGION`			
Объектное хранилище — наблюдаемость	`S3_OBS_ACCESS_KEY`, `S3_OBS_SECRET_KEY` (опц.)	Артефакты трейсинга	Чтение/запись	Опционально

Ключи объектного хранилища (`S3_ACCESS_KEY`, `S3_SECRET_KEY`) обязательно задаются уникальными значениями; значения по умолчанию не допускаются.

3.2. Прикладные секреты (криптография)

Секрет	Переменная	Назначение	Требования
Подпись access-токенов	`JWT_ACCESS_SECRET`	Подпись токенов доступа	≥ 32 символа, уникальный
Подпись refresh-токенов	`JWT_REFRESH_SECRET`	Подпись токенов обновления	≥ 32 символа, отличается от access
«Перец» refresh-токенов	`TOKEN_HASH_PEPPER`	Хеширование refresh-токенов (SHA-256)	Уникальный, секретный
Публичный ключ лицензии	`LICENSE_PUBLIC_KEY`	Проверка подписи лицензии (RSA)	PEM-кодированный ключ

3.3. Учётная запись первичного администратора

Переменная	Назначение
`ADMIN_EMAIL`	E-mail первого супер-администратора
`ADMIN_PASSWORD`	Первичный пароль (≥ 8 символов)

Создаётся при первом запуске сервера приложения, если отсутствует. После первого входа пароль подлежит смене.

3.4. Межсервисные токены

Токен	Переменная	Направление вызова
Сервис обработки медиа	`FFMPEG_REST_AUTH_TOKEN`	Сервер приложения → сервис транскодирования
LLM-прокси (опц.)	`LLM_PROXY_AUTH_TOKEN`	Сервер приложения → промежуточный LLM-прокси
Метрики	`METRICS_TOKEN`	Система мониторинга → `GET /metrics` (Bearer; при отсутствии — закрыт)

3.5. Секреты входящих интеграций (вебхуков)

Источник	Переменные	Способ проверки
Уведомления о доставке e-mail	`RESEND_WEBHOOK_SECRET`	HMAC-подпись
Сервис транскрипции	`ASSEMBLYAI_WEBHOOK_AUTH_HEADER_NAME`, `ASSEMBLYAI_WEBHOOK_AUTH_HEADER_VALUE`	Проверка заголовка
Сервис распознавания (OCR)	`OCR_AUTH_TOKEN`, `OCR_WEBHOOK_SECRET`	Токен и HMAC с защитой от повторного воспроизведения
Telegram	`TELEGRAM_BOT_TOKEN`, `TELEGRAM_WEBHOOK_SECRET`	Секрет вебхука

3.6. Внешние провайдерские ключи

`OPENAI_API_KEY`, `ANTHROPIC_API_KEY`, `COHERE_API_KEY`, `TAVILY_API_KEY`, `XAI_API_KEY`, `MOONSHOT_API_KEY`, `DASHSCOPE_API_KEY`, `OPENROUTER_API_KEY`, `GIGA_AUTH_KEY`, `RESEND_API_KEY`, `ASSEMBLYAI_API_KEY`, `SENTRY_BACKEND_DSN`, ключи оповещений (`OBS_TELEGRAM_BOT_TOKEN_DEFAULT`, `OBS_PAGERDUTY_INTEGRATION_KEY_DEFAULT`).

4. Матрица доступа технологических учётных записей

Субъект (учётная запись/сервис) × объект (ресурс) × права (Ч — чтение, З — запись, А — административные).

Субъект \ Объект	PostgreSQL	Redis	Qdrant	S3	Внешние API
Сервер приложения (API)	Ч/З	Ч/З	Ч/З	Ч/З	Ч/З
Фоновый обработчик	Ч/З	Ч/З	Ч/З	Ч/З	Ч/З
Сервис обработки медиа	—	Ч/З	—	—	—
Система мониторинга	—	—	—	—	Ч (`/metrics`)
Системный администратор хоста	А	А	А	—	—

5. Порядок заведения и хранения

5.1. Генерация секретов

Сильные значения генерируются криптографически стойким способом (например, `openssl rand -hex 32`).

5.2. Хранение

Значения задаются в `.env` (права `600`, владелец — учётная запись развёртывания); реальные секреты в репозитории не хранятся. **Рекомендация:** применение централизованного хранилища секретов (vault).

5.3. Передача и доступ

Доступ к `.env` и секретам — только у ответственных лиц; передача — по защищённым каналам.

6. Управление жизненным циклом

6.1. Ротация

1. Сгенерировать новое значение.
2. Обновить переменную в `.env`.
3. Перезапустить затронутые сервисы.

4. Для внешних интеграций (вебхуки, метрики) синхронно обновить значение на стороне внешней системы.
5. Зафиксировать факт ротации в журнале администрирования.

6.2. Отзыв / блокировка

При компрометации — немедленная ротация затронутого секрета и отзыв активных сессий.

6.3. Аудит использования

Действия с учётными записями и факты ротации фиксируются в журнале администрирования.

7. Требования к стойкости секретов

- Токены/секреты — не менее 32 символов, криптографически стойкие.
- Пароль первичного администратора — не менее 8 символов; подлежит смене после первого входа.
- Уникальность значений между средами (dev/prod) и между разными секретами.

8. Внешние провайдерские ключи

Не являются учётными записями системы, однако хранятся в `.env` и подлежат защите наравне с прочими секретами (перечень — в разд. 3.6).

9. Рекомендации по усилению

9.1. Для подключения приложения к СУБД выделить отдельную роль с минимально необходимым набором привилегий вместо учётной записи-владельца (требования п. 25, 58).

9.2. Рассмотреть применение централизованного хранилища секретов (vault) вместо файла `.env` (требование п. 13).

Приложение А. Полный реестр переменных окружения — см. разд. 3.

Приложение Б. Матрица доступа — см. разд. 4.

Трассировка к требованиям ИБ: документ покрывает пункты опросного листа ИБ №№ 11, 13, 25, 58, 69 (технологические учётные записи, секреты, права, порядок заведения).

Лист согласования

Роль	ФИО	Подпись	Дата
Подготовил (разработка)			
Согласовал (ИБ)			
Утвердил			