Руководство администратора системы

Документ: ИБ-68 · **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 (структура по ГОСТ 19.503-79)

---

1. Общие сведения

1.1. Назначение документа

Документ определяет порядок администрирования информационной системы ЛКИ: предоставление прав пользователям, запрещённые комбинации ролей, критичные операции, выполняемые двумя лицами, управление учётными записями, аудит и реагирование на события безопасности.

1.2. Область применения

Положения обязательны для системных администраторов ИС ЛКИ независимо от площадки размещения.

1.3. Нормативные ссылки

- ГОСТ 19.503-79 (ЕСПД. Руководство системного программиста) — как методическая основа.
- ГОСТ Р ИСО/МЭК 27001 — в части управления доступом.
- Внутренний опросный лист требований ИБ (ИС: ЛКИ).

1.4. Термины и сокращения

Сокращение	Расшифровка
RBAC	Управление доступом на основе ролей
break-glass	Сессия экстренного доступа (раскрытия данных)
SIEM	Внешняя система сбора и корреляции событий

2. Общие сведения о системе

2.1. Назначение и функции АС

ЛКИ — веб-приложение; пользователи работают через браузер. Бизнес-объекты организованы по иерархии «компания → проект».

2.2. Архитектура и компоненты (кратко)

Сервер приложения (API) и фоновый обработчик, веб-интерфейс, СУБД PostgreSQL, Redis, векторная БД; единая точка входа — обратный прокси. Подробно — в документе «Настройки ОС и СУБД» (ИБ-67).

2.3. Состав модуля «Администрирование»

Административные функции вынесены в отдельный модуль с контроллерами под префиксом `/admin/*` (пользователи, компании, аудит, наблюдаемость, использование, задачи, работоспособность), доступными только ролям уровня `systemAdmin`.

3. Ролевая модель и управление доступом

Управление доступом трёхуровневое (система → компания → проект); проверки выполняются на прикладном уровне (guard-ы).

3.1. Системные роли

Роль	Назначение
`systemUser`	Обычный пользователь; доступ — по членству в компаниях/проектах
`systemAdmin`	Супер-администратор: управление компаниями и пользователями; по наблюдаемости — только чтение до открытия сессии экстренного доступа

Роль	Назначение
`systemAdminAuditor`	Доступ только на чтение к журналам администрирования; раскрытие «сырых» данных недоступно
`systemAdminBreakGlass`	Открытие сессии раскрытия для областей `this_trace` / `this_session_1h`
`systemAdminRoot`	Высший уровень: одобрение раскрытия области `this_company_24h`, изменение уровней доступа, ротация адреса выгрузки в SIEM

3.2. Роли уровня компании

Роль	Полномочия
`companyOwner`	Полный контроль над компанией
`companyAdmin`	Администрирование компании и её проектов
`companyMember`	Базовый участник компании

3.3. Роли уровня проекта

Роль	Полномочия
`owner`	Полный доступ к проекту, управление участниками
`editor`	Создание и редактирование содержимого
`viewer`	Доступ только на чтение

3.4. Иерархия и наследование

Тиры `systemAdmin*` проходят базовые проверки `systemAdmin`. Роли компании/проекта упорядочены по убыванию полномочий (owner > admin/editor > member/viewer).

3.5. Принцип минимальных привилегий

При создании пользователю назначается минимальная роль (`systemUser` / `companyMember`); повышенные полномочия назначаются явно и осознанно.

4. Управление учётными записями

4.1. Создание / приглашение

Учётная запись создаётся через модуль администрирования или процедуру приглашения. Доступ предоставляется только после принятия персонального приглашения (`/auth/accept-invite`).

4.2. Назначение и изменение ролей

Системная роль изменяется операцией `PATCH /admin/users/:id`; роли компании/участников — через контроллеры `/admin/companies/*`. Каждое изменение фиксируется в журнале аудита.

4.3. Блокировка и разблокировка

Блокировка — `PATCH /admin/users/:id` (`isActive=false`); разблокировка после превышения порога входа — `POST /admin/users/:id/unlock` (фиксируется в аудите).

4.4. «Удаление» как блокировка

Жёсткое удаление не предусмотрено; удаление реализовано как перевод в неактивное состояние — заблокированный пользователь не может входить и работать под своим именем.

4.5. Жизненный цикл и уведомления

E-mail-уведомления направляются при приглашении и сбросе пароля. (Уведомление при блокировке/деактивации и SMS-канал — при внедрении, требование п. 41.)

5. Порядок предоставления прав

5.1. Регламент выдачи прав

Права выдаются по обоснованной заявке, по принципу минимальных привилегий, с фиксацией в журнале аудита.

5.2. Запрещённые комбинации ролей

1. Учётная запись с системной ролью `systemAdmin*` **не должна** одновременно являться участником компании/проекта (контроль — организационный; кодовый инвариант — при внедрении, требование п. 32).
2. Под одной учётной записью не совмещаются административные и пользовательские полномочия.
3. Роль `systemAdminRoot` назначается ограниченному числу лиц.

5.3. Критичные операции «в две руки»

Операция	Порядок
Раскрытие данных наблюдаемости «вся компания за 24 часа»	Принцип «двух лиц»: `systemAdminBreakGlass` подаёт запрос с обоснованием (≥ 20 символов), `systemAdminRoot` — одобряет
Изменение уровней доступа (`systemAdmin` / `systemAdminRoot`)	`systemAdminRoot` по согласованию со вторым лицом
Ротация адреса выгрузки в SIEM	`systemAdminRoot`
Выдача супер-административных прав новому лицу	Согласование двух лиц, фиксация в журнале

5.4. Согласование и фиксация

Все перечисленные операции фиксируются в журнале администрирования и выгружаются в SIEM.

6. Аутентификация и сессии

6.1. Вход и блокировка при подборе пароля

Вход — по уникальному идентификатору (e-mail) и паролю с выдачей JWT. После **5** неуспешных попыток учётная запись блокируется на **30 минут** (или до разблокировки администратором); каждая попытка фиксируется с IP.

6.2. Управление сессиями

Пользователь может самостоятельно завершить сеанс (`/auth/logout`, `/auth/sessions`). Принудительное завершение сеанса по неактивности (20 мин) и ограничение числа одновременных сессий — при внедрении (требования п. 22, 24).

6.3. Доменная аутентификация и 2FA

при внедрении (требования п. 37–39): интеграция с доменной аутентификацией и двухфакторная аутентификация на текущий момент не реализованы; вход — по email+пароль.

7. Администрирование подсистем

7.1. Управление компаниями

Создание, изменение, приостановка/активация компании, управление участниками и приглашениями — через `/admin/companies/*`.

7.2. Управление проектами и участниками

Управление проектами и их участниками выполняется в рамках компании с учётом ролей проекта.

7.3. Наблюдаемость и break-glass

Доступ к «сырым» данным наблюдаемости — только через сессию экстренного доступа с ограничением области, обязательным обоснованием и (для области 24 часа) одобрением второго лица. Все действия фиксируются.

7.4. Настройки системы

Изменения настроек компании и наблюдаемости фиксируются в журнале аудита (с новыми значениями; секреты маскируются).

8. Аудит и журналирование

8.1. Состав событий аудита

Журналируются: входы/выходы и неуспешные попытки (с IP), блокировка/разблокировка, управленческие действия (пользователи, компании, участники, приглашения), изменения ролей и настроек, отказы авторизации, нарушения целостности. Каждое событие содержит результат (успех/неуспех) и реквизиты (дата/время, исполнитель, объект, параметры).

8.2. Просмотр и выгрузка журнала

Журнал доступен через модуль администрирования (`/admin/audit`); выгрузка журнала наблюдаемости — в SIEM по защищённому каналу.

8.3. Неизменяемость журнала

Журнал на уровне приложения работает только в режиме добавления (методов изменения/удаления нет). Защита на уровне СУБД (триггеры/ограничение прав) — при внедрении (требование п. 53).

8.4. Реагирование на события безопасности

При срабатывании событий (множественные неуспешные входы, отказы авторизации, нарушения целостности) администратор анализирует источник (IP/UA) и принимает меры (блокировка, ротация секретов, эскалация).

9. Эксплуатация

9.1. Контроль работоспособности

Health-эндпоинты: `/health`, `/health/live`, `/health/ready`, `/health/obs`. Метрики — `/metrics` (по токену).

9.2. Типовые операции обслуживания

Перезапуск сервисов, ротация секретов, обновление образов — в окно технического обслуживания.

9.3. Резервное копирование

Порядок резервного копирования и восстановления — в документе «Настройки ОС и СУБД» (ИБ-67, разд. 12).

10. Сообщения администратору

В штатном режиме при ошибке пользователю возвращается обобщённое сообщение без раскрытия внутренних деталей (стек, SQL, пути ФС); полная информация об ошибке фиксируется на сервере и направляется в систему мониторинга. Администратор анализирует серверные журналы для диагностики.

11. Аварийные ситуации и реагирование на инциденты

- Недоступность сервиса — проверка health-эндпоинтов, журналов, состояния зависимостей (СУБД/Redis/Qdrant).
- Компрометация секрета — немедленная ротация (см. ИБ-69), отзыв сессий.
- Подозрение на НСД — анализ журнала аудита, блокировка учётных записей, эскалация в ИБ.

Приложение А. Матрица ролей и прав — см. разд. 3.

Приложение Б. Перечень критичных операций (разделение обязанностей) — см. разд. 5.3.

Приложение В. Перечень событий аудита — см. разд. 8.1.

Трассировка к требованиям ИБ: документ покрывает пункты опросного листа ИБ №№ 21, 27–35, 40–44, 46, 49, 68 (администрирование, выдача прав, разделение обязанностей, аудит действий).

Лист согласования

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