Задание по RBAC

Дурнов Алексей Николаевич

Московский физико-технический институт
Физтех-школа радиотехники и компьютерных технологий

Москва, 2025 г.

Состав персонала

1. Руководство и менеджмент (CEO, CTO, COO, PM)
2. Разработка (TechLead, Senior, Middle, Junior, QA, DevOps, UI/UX)
3. Поддержка и инфраструктура (Сис. админ, Support)
4. Отделы бизнеса и маркетинга (Product, Sales, Marketing Managers)
5. Финансовый и административный блок (CFO, HR, Office Manager)
6. Дополнительные роли (Data analyst, Legal Advisor)

Активы компании

Выберем основной набор активов обычной IT-компании:

- Офис
- Серверная
- Корпоративный мессенджер
- Корпоративная почта
- Корпоративный VPN
- Корпоративный портал поддержки
- Система мониторинга (Zabbix)
- База знаний (Confluence)
- Репозиторий (Microsoft Azure)
- CI/CD (Hive)
- Инструменты QA (Asgard)
- Сервис для моделирование макетов (Figma)
- Трекер задач и требований (Microsoft Azure)
- CRM-система (Customer Relationship Management)
- ERP-система (Enterprise Risk Management)

Разрешения (P)

Введём для выбранных активов основные разрешения в общем виде:

- Офис: доступ в офис в любое время, доступ к оборудованию (принтерам/сканерам).
- Серверная: доступ в серверную.
- Корпоративный мессенджер: аккаунт с доступом к общим чатам команд и возможность написать каждому сотруднику.
- Корпоративная почта: личный ящик (отправка/получение), доступ к общим папкам, регистрация в корпоративных сервисах.
- Корпоративный VPN: удаленный доступ к корпоративной сети.
- Корпоративный портал поддержки: создание тикетов, просмотр истории обращений.
- Система мониторинга: просмотр метрик, изменение метрик и настройка оповещений.
- База знаний: просмотр/редактирование страниц.
- Репозиторий: просмотр кода, отправление коммитов, создание веток и Pull Request'ов.

Разрешения (P)

- CI/CD: запуск сборок и изменение конфигурации pipeline.
- Инструменты QA: редактирование и запуск тестов, просмотр отчетов.
- Сервис для моделирование макетов (Figma): просмотр макетов, редактирование и создание компонентов.
- Трекер задач и требований: создание задач и требований, изменение статусов, назначение исполнителей.
- CRM-система: просмотр контактов клиентов, редактирование сделок, генерация отчетов.
- ERP-система: ввод данных, выполнение финансовых операций, просмотр аналитики.

Определим роли, исходя из классов эквивалентности по разрешениям. Но перед этим определим общие разрешения, которые будут у каждой роли (иерархия ролей: роль - сотрудник):

- Доступ в офис в любое время, доступ к оборудованию (принтерам/сканерам).
- Аккаунт в мессенджере с доступом к общим чатам команд и возможность написать каждому сотруднику.
- Личный ящик (отправка/получение), доступ к общим папкам, регистрация в корпоративных сервисах.
- Доступ к корпоративному VPN.
- Создание тикетов и просмотр истории обращений на внутреннем портале поддержки.

Роли (R, UA + PA)

- Officer (CEO, CTO, COO) - доступ к аналитике CRM/ERP, трекеру задач и требований, доступ к базе знаний.
- Project Manager (PM) - трекер задач и требований, доступ к базе знаний.
- TechLead - просмотр кода, создание задач и изменение статусов, доступ к базе знаний, изменение конфигурации pipeline'ов, настройка оповещений системы мониторинга.
- Developer (Senior, Middle, Junior) - просмотр кода, отправление коммитов, создание веток и Pull Request'ов, создание задач и изменение статусов, доступ к базе знаний, запуск pipeline'ов
- QA Engineer - доступ в серверную, редактирование и запуск тестов, просмотр кода, отправление коммитов, создание веток и Pull Request'ов, создание баг-задач, доступ к базе знаний.
- DevOps Engineer - доступ в серверную, изменение конфигурации pipeline'ов, настройка системы мониторинга, создание задач и изменение статусов.
- UI/UX Designer - просмотр макетов, редактирование и создание компонентов, создание задач и изменение статусов.

Роли (R, UA + PA)

- Сис. админ - доступ в серверную, настройка VPN и других корпоративных сервисов.
- Support - закрытие тикетов на портале поддержки.
- Business Manager (Product, Sales, Marketing Managers) - доступ к аналитике CRM/ERP, редактирование данных в CRM.
- CFO - доступ к аналитике CRM/ERP, редактирование данных в ERP.
- HR - доступ к базе знаний (HR-документов).
- Office Manager - управление оборудованием, ввод данных по закупкам в ERP.
- Data Analyst - доступ к аналитике CRM/ERP, просмотр метрик из системы мониторинга.
- Legal Advisor - доступ к базе знаний (юридические документы).

Ограничения

- Взаимное исключение ролей:
  - Сотрудник не может иметь одновременно две роли QA Engineer и Developer
  - Сотрудник не может иметь одновременно две роли CFO и Office Manager
  - Сотрудник не может иметь техническую роль и менеджерскую роль.
- Количественное ограничение ролей:
  - Не более 3 сотрудников в роли Officer.
  - Минимум 1 сотрудник в роли DevOps.
  - Сотрудников с ролью QA не меньше, чем в 5 раз, чем Developer'ов.

Административные роли (AP, AR, APA, AUA)

- Role Administrator (CEO) - назначать/отзывать роли пользователям.
  - can-assign:
    - Officer: сотрудник должен иметь стаж в компании 5 лет и подтверждение от совета директоров.
    - Project Manager: пользователь должен получить рекомендацию хотя бы от одного Officer.
    - TechLead: сотрудник должен иметь роль Developer 5 лет.
    - DevOps: пользователь должен пройти сертификацию по облачным технологиям.
    - Business Manager: пользователь должен быть утвержден текущим CFO.
    - Остальные роли: пользователь должен успешно пройти интервью (получить 2 рекомендации из 3).
  - can-revoke:
    - Officer: требуется согласие двух других Officer или совета директоров.
    - Остальные роли: уведомление от HR/выше стоящего менеджера и подтверждение причины отзыва роли.

Административные роли (AP, AR, APA, AUA)

- Policy Administrator (COO) - определять и настраивать статические и динамические ограничения для ролей RBAC.
  - не участвует в назначении ролей и разрешений.
- Service Administrator (Support) - предоставлять доступы к необходимым сервисам сотрудникам.
  - can-assign и can-revoke:
    - Все роли: при доставление доступа к указанным выше сервисам у соответствующей роли.
- Security Administrator (Support) - блокировка пользователей при подозрительной активности.
  - can-revoke:
    - Все роли: при подозрительной активности пользователя отзывается роль до окончательного вынесения решения.