BimarSystem

Оглавление

О программном обеспечении

BIMAR — это инновационная кросс-отраслевая цифровая платформа нового поколения, которая формирует совершенно иное качество данных в строительной, промышленной и других смежных отраслях.

Основное отличие BIMAR — получение информации непосредственно в момент совершения действия сотрудниками и рабочих на объекте. Это «живая» и актуальная картина происходящего, доступная в режиме реального времени, а не постфактум.

Модульная структура платформы дает возможность использовать её как целиком, так и по отдельным функциям: - Контроль проектирования - Производство - Склад - Логистика - Монтаж - Эксплуатация

Внутренний язык разработки отсуствует

Серверная часть разработана на языке Python

Web-интерфейс разработан на TypeScripts

Android приложение разработано на Kotlin

Операционная система для серверного решения Ubuntu 22.04 или RedOS 5

Веб-сервер Nginx

Для функционирования необходимы следующие протоколы

Для взаимодействия с пользовательким интерфейсом и API система использует: - 443/HTTPS

Для взаимодействия между компонентами система использует: - 80/HTTP - 636/TCP - 5432/TCP - 6379/TCP - 8000/TCP - 8888/TCP

BimarSystem

Описание обновлений

Описание обновлений (Release Notes)

Здесь представлена история изменений проекта. Начиная с версии **2.5.1**, ведётся автоматизированный учёт изменений.

Версия 2.5.2

🔒 Информационная безопасность

- Расширено логирование событий ИБ
- Добавлена авторизация по клиентскому сертификату
- Реализована двухфакторная аутентификация по email
- Расширена интеграция с LDAP — поддержка групп для управления ролями, сквозная доменная аутентификация (Kerberos/SSO)
- Добавлены настройки парольной политики: история паролей, срок действия, обязательная смена при первом входе
- Реализована автоматическая блокировка сессии при неактивности
- Чувствительные данные в конфигурации теперь шифруются (Fernet/AES128-CBC)
- Убрано отображение аутентификационных данных из журналов событий
- Добавлено управление ротацией журналов событий ИБ (предупреждение при заполнении, автоматическая очистка)
- Все события управления компонентами ИС (установка, изменение, удаление, конфигурационные файлы) теперь журналируются
- Подключён статический анализатор кода Bandit

🚀 Новые возможности

- Добавлена двухфакторная аутентификация

- Добавлена авторизация по клиентскому сертификату
- Расширены настройки парольной политики
- Добавлены мультипроектные ячейки
- Добавлены уведомления и подписки на изменение статусов

🛠 Исправления

- Улучшена очистка старых записей журнала событий
- Оптимизировано хранение конфиденциальных данных в конфигурации

📚 Документация

- Дополнено описание сетевых параметров и портов
- Добавлены инструкции по проверке контрольных сумм образов
- Обновлено описание механизмов резервного копирования

Версия 2.5.1

🚀 Новые возможности

- Добавлено логирование событий ИБ
- Добавлена возможность редактирования состава сборочного элемента
- Добавлена интеграция с LDAP
- Добавлено ограничение кол-ва попыток входа
- Добавлены настройки необходимой сложности пароля

🛠 Исправления

- Исправлена загрузка логотипа проекта

⚡ Оптимизации

- Оптимизированна выгрузка отчетов по секторам

Установка и обновление

Установка

Системные требования

- Наличие в системе docker с compose плагином
- Системные требования к аппаратной части:

Требования	**100user + 200.000 elements**	**500user + 1.000.000 elements**	**3000user + 4.000.000 elements**	**30000user + 100.000.000 elements**
RAM	10GB	16GB	30GB	128GB
CPU	4 cores 2.2GHz+	8 cores 2.2GHz+	30 cores 2.2Ghz+	60 cores 2.2Ghz+
disk space with 3D	500GB	1000GB	4TB	100TB
disk space without 3D	50GB	100GB	400GB	10TB
Network (communication channel)	50MB/s	150MB/s	1TB/s	25TB/s

Установка при наличии доступа к registry

- Перенести содержимое архива `bimar.rar` в одну директорию
- Заполнить сторки подключения к БД в .env файле
- Создать сеть

```
sudo docker network create bimar-network
```

• Авторизоваться в registry (доступы можно запросить у технической поддержки)

```
sudo docker login bimar.gitlab.yandexcloud.net:5050
```

• Загрузить образы

```
sudo docker compose pull
```

• Запустить контейнеры

```
sudo docker compose up -d
```

Установка из архива с docker образами

• Перенести содержимое архива `artifacts.rar` на сервер

• Загрузить образы

```
sudo docker load -i main.tar
sudo docker load -i nginx_image.tar
sudo docker load -i postgis_image.tar
sudo docker load -i redis_image.tar
```

• Заполнить сторки подключения к БД в .env файле

• Создать сеть

```
sudo docker network create bimar-network
```

• Запустить контейнеры

```
sudo docker compose up -d
```

Создание учетной записи администратора

```
sudo docker exec -it bimar-web-1 /bin/sh
python manage.py createsuperuser
```

• По умолчанию сервис доступен на порту 8083 (настраивается в .env)

В случае развертывания БД не через предоставленный compose файл

Для работы требуется PostgreSQL версии 14 или выше. Для работы требуется БД PostgresSQL и установленным плагинами PostGIS и hstore

```
CREATE EXTENSION IF NOT EXISTS postgis;
CREATE EXTENSION IF NOT EXISTS hstore;
```

Обновление

Обновление при наличии доступа к registry

- Перенести содержимое архива `bimar.rar` в одну директорию
- Загрузить образы

```
sudo docker compose pull
```

- Запустить контейнеры

```
sudo docker compose up -d
```

Обновление из архива с docker образами

- Перенести содержимое архива `artifacts.rar` на сервер
- Загрузить образы

```
sudo docker load -i main.tar
sudo docker load -i nginx_image.tar
sudo docker load -i postgis_image.tar
sudo docker load -i redis_image.tar
```

- Запустить контейнеры

```
sudo docker compose up -d
```

BimarSystem

События ИБ

Подсистема регистрации и учета событий ИБ

Архитектура подсистемы

Подсистема регистрации и учета событий ИБ реализована в виде микросервиса **orchestrator** (оркестратор), который выполняет следующие функции:

- **Управление конфигурациями**: хранение, версионирование и отслеживание изменений файлов конфигураций сервисов
- **Сбор событий безопасности**: централизованный сбор и маршрутизация логов инфраструктуры и событий ИБ
- **Управление компонентами**: регистрация и учет компонентов системы

Классификатор типов событий по функциональному назначению

Класс события	Описание
AUTH	События идентификации и аутентификации
USER	Действия пользователей в системе
ADMIN	Административные действия
CFG	Изменение конфигурации и параметров системы
NET	Сетевые события и взаимодействие
DATA	Операции с данными и информационными ресурсами
SYS	Функционирование системы и средств защиты
LOG	Регистрация и обработка журналов

Уровни важности событий

Для оценки значимости событий информационной безопасности используется единая шкала уровней важности. Уровень важности определяется для каждого события и используется при анализе, корреляции и реагировании.

Применяются следующие уровни важности: **низкий**, **средний**, **высокий**, **критический**.

Атрибутный состав событий ИБ

Каждое зарегистрированное событие ИБ должно содержать обязательный набор атрибутов.

№	Атрибут	Описание
1	Дата и время события	Дата и время возникновения события
2	Идентификатор типа события (EventCode)	Уникальный код типа события в системе
3	Тип события	Тип события в соответствии с классификацией
4	Уровень важности	Оценка значимости событий ИБ
5	Результат операции	Успешно / неуспешно
6	Субъект события	Имя пользователя
7	Сетевой адрес субъекта	IP-адрес хоста субъекта
8	Объект события	Ресурс, функция или данные, по отношению к которым осуществлялась операция
9	Информация об объекте	Наименование объекта операции
10	Параметры изменения	Описание измененных параметров (если применимо)

Классы и типы событий ИБ

Общая таблица событий

Класс	Тип события	EventCode	Наименование события	Уровень важности
AUTH	AUTH_LOGIN	**AUTH_LOGIN_SUCCESS**	Успешная аутентификация пользователя	Низкий
AUTH	AUTH_LOGIN	**AUTH_LOGIN_FAIL**	Неуспешная попытка аутентификации пользователя	Средний
AUTH	AUTH_LOGOUT	**AUTH_LOGOUT**	Завершение сессии пользователя	Низкий
AUTH	AUTH_ACCOUNT	**AUTH_ACCOUNT_BLOCK**	Блокирование учётной записи пользователя	Высокий
AUTH	AUTH_DEVICE	**AUTH_DEVICE_SUCCESS**	Успешная аутентификация устройства	Низкий
AUTH	AUTH_DEVICE	**AUTH_DEVICE_FAIL**	Неуспешная попытка аутентификации устройства	Средний
USER	USER_ACCOUNT	**USER_CREATE**	Создание учётной записи	Средний
USER	USER_ACCOUNT	**USER_MODIFY**	Изменение учётной записи	Средний
USER	USER_ACCOUNT	**USER_BLOCK**	Деактивация учётной записи	Средний
ADMIN	ADMIN_GROUP	**GROUP_CREATE**	Создание группы	Низкий
ADMIN	ADMIN_GROUP	**GROUP_DELETE**	Удаление группы	Низкий
ADMIN	ADMIN_GROUP	**GROUP_MODIFY**		Средний

Класс	Тип события	EventCode	Наименование события	Уровень важности
			Изменение параметров группы	
ADMIN	ADMIN_GROUP	**GROUP_USER_ADD**	Добавление пользователя в группу	Низкий
ADMIN	ADMIN_GROUP	**GROUP_USER_REMOVE**	Исключение пользователя из группы	Низкий
ADMIN	ADMIN_ACTION	**ADMIN_ACTION**	Административное действие	Средний
CFG	CFG_INIT	**CFG_INIT_START**	Инициализация компонентов системы	Средний
CFG	CFG_FILE	**CFG_FILE_CREATE**	Создание конфигурационного файла	Средний
CFG	CFG_FILE	**CFG_FILE_DELETE**	Удаление конфигурационного файла	Средний
CFG	CFG_FILE	**CFG_FILE_MODIFY**	Изменение конфигурационного файла	Средний
CFG	CFG_PARAM	**CFG_PARAM_CHANGE**	Изменение параметров журналирования	Высокий
CFG	CFG_SECURITY	**CFG_SECURITY_CHANGE**	Изменение параметров безопасности	Высокий
CFG	CFG_COMPONENT	**CFG_COMP_REMOVE**	Удаление компонента системы	Высокий
CFG	CFG_COMPONENT	**CFG_COMP_UPDATE**		Высокий

Класс	Тип события	EventCode	Наименование события	Уровень важности
			Изменение компонента системы	
CFG	CFG_PROCESS	**CFG_PROC_CHANGE**	Изменение состава процессов	Средний
NET	NET_CHANGE	**NET_CHANGE**	Изменение сетевых параметров	Высокий
NET	NET_DENY	**NET_DENY**	Блокирование сетевого соединения	Средний
NET	NET_CHANGE	**NET_CHANGE_ID**	Изменение идентификаторов и атрибутов ИС	Высокий
DATA	DATA_MODIFY	**DATA_MODIFY**	Изменение данных	Средний
DATA	DATA_DELETE	**DATA_DELETE**	Удаление данных	Высокий
DATA	DATA_EXPORT	**DATA_EXPORT**	Экспорт защищаемых данных	Высокий
SYS	SYS_COMPONENT	**SYS_COMP_FAIL**	Отказ компонента системы	Критически
SYS	SYS_COMPONENT	**SYS_COMP_STOP**	Остановка компонента системы	Высокий
SYS	SYS_SECURITY	**SYS_SEC_FAIL**	Отказ механизма защиты	Критически
SYS	SYS_SECURITY	**SYS_SEC_DISABLE**	Отключение механизма защиты	Высокий
LOG	LOG_MANAGE	**LOG_CLEAR**	Очистка журналов	Высокий
LOG	LOG_MANAGE	**LOG_OVERFLOW**	Переполнение журнала	Высокий

Матрица соответствия «тип инцидента → меры реагирования»

Настоящая матрица устанавливает соответствие между типами событий ИБ, возможными типами инцидентов ИБ и мерами реагирования, применяемыми в ИС BIMAR SYSTEM.

Класс события	**Тип инцидента ИБ**	**Меры реагирования**
AUTH	Попытка НСД	Анализ журнала; блокировка учетной записи при превышении порога; уведомление администратора ИБ
USER	Нарушение управления доступом	Проверка прав; откат изменений; уведомление администратора ИБ
ADMIN	Несанкционированное администрирование	Анализ действий; приостановка учетной записи; расследование
CFG	Несанкционированное изменение конфигурации	Восстановление конфигурации; ограничение доступа; анализ причин
NET	Нарушение сетевой конфигурации	Проверка настроек; восстановление параметров; уведомление
DATA	Утечка / несанкционированный экспорт данных	Блокировка экспорта; анализ объема данных; расследование инцидента

BimarSystem

Документация

Новая релизная версия продукта выходит примерно 2 раза в месяц.

Всю информацию об изменениях можно найти на странице: Описание обновлений

Информацию об известных уязвимостях будет публиковаться в чатах поддержки, а так же её можно найти на странице: Известные проблемы

Контакты технической поддержки: is@bimar.pro, dk@bimar.pro

📥 **Скачать документацию в PDF:** docs.pdf

Настройки сервера

Конфигурационный файл

Все настройки приложения хранятся в едином YAML-файле конфигурации.

Основная структура файла

Файл конфигурации разделен на несколько основных секций:

- **`config`** - Основные настройки приложения.
- **`database`** - Настройки подключения к базе данных.
- **`django`** - Специфичные настройки Django фреймворка.
- **`security`** - Политики безопасности и паролей.
- **`two_factor_auth`** - Настройки двухфакторной аутентификации.
- **`ldap`** - Настройки интеграции с LDAP/Active Directory.
- **`sso`** - Настройки единого входа (Single Sign-On).
- **`redis`** - Настройки подключения к Redis.
- **`rabbitmq`** - Настройки подключения к RabbitMQ (для Celery).

Секция `config` (Основные настройки)

`debug`

- **Тип**: Boolean
- **По умолчанию**: false
- **Описание**: Определяет режим работы приложения. Влияет на поведение логирования, кэширования и других компонентов.

`mode`

- **Тип**: String

- **Пример**: `local`, `stage`, `prod`
- **Описание**: Определяет режим работы приложения. Влияет на поведение логирования, кэширования и других компонентов.

`host`

- **Тип**: String
- **Пример**: `"localhost"`, `"0.0.0.0"`
- **Описание**: Хост, на котором будет запущен сервер приложения.

`port`

- **Тип**: Integer
- **Пример**: `80`, `8000`
- **Описание**: Порт для запуска сервера приложения.

`web_base_url`

- **Тип**: String (URL)
- **Пример**: `"https://web.stage.bimarkit.com"`
- **Описание**: Базовый URL фронтенд-приложения, используется для генерации ссылок.

Секция database (База данных)

`engine`

- **Тип**: String
- **Пример**: `"django.contrib.gis.db.backends.postgis"`
- **Описание**: Движок базы данных для Django (используется для пространственных данных).

`default`

- **Подсекция, содержащая параметры подключения**:
  - `host` (**Тип**: String) - Хост базы данных.
  - `port` (**Тип**: Integer) - Порт базы данных.
  - `name` (**Тип**: String) - Имя базы данных.
  - `user` (**Тип**: String) - Имя пользователя БД.
  - `password` (**Тип**: String) - Пароль пользователя БД.
  - `engine` (**Тип**: String) - Альтернативный движок для дополнительных возможностей (например, `psqlextra.backend`).

Секция `django` (Настройки Django)

`secret_key`

- **Тип**: String
- **Описание**: Секретный ключ Django для подписи сессий, токенов и т.д. **Должен быть уникальным и храниться в тайне!**

`allowed_hosts`

- **Тип**: String (разделенный запятыми список) или `"*"`
- **Описание**: Список доменных имен/хостов, с которых может обслуживаться это приложение. `"*"` разрешает все (не для продакшена).

`access_token_lifetime_min`

- **Тип**: Integer (минуты)
- **Описание**: Время жизни Access Token (JWT) для аутентификации.

`refresh_token_lifetime_min`

- **Тип**: Integer (минуты)
- **Описание**: Время жизни Refresh Token (JWT).

`cors_allowed_origins`

- **Тип**: String (URL)
- **Описание**: Origin, с которого фронтенд может делать запросы к API (для настройки CORS).

`session_age`

- **Тип**: Integer
- **По умолчанию**: 1209600 (14 дней)
- **Описание**: Время жизни сессии при неактивности пользователя (в секундах).

Секция `security` (Политики безопасности)

`log_rotation_days`

- **Тип**: Integer
- **По умолчанию**: 365
- **Описание**: Период ротации логов безопасности (в днях).

`storage_limit_mb`

- **Тип**: Integer
- **По умолчанию**: 1000
- **Описание**: Лимит хранилища логов ИБ в МВ

`memory_warning_percent`

- **Тип**: Integer
- **По умолчанию**: 70
- **Описание**: Порог после которого будут выдаваться предупреждения о заполнении хранилища логов ИБ

`login_attempts_limit`

- **Тип**: Integer
- **По умолчанию**: 3
- **Описание**: Лимит попыток входа.

`login_attempts_timeout`

- **Тип**: Integer
- **По умолчанию**: 300
- **Описание**: Время (в минутах) блокировки пользователя после превышения лимита попыток входа.

Политики сложности пароля:

`password_min_length` - Минимальная длина.

- **Тип**: Integer
- **По умолчанию**: 8
- **Описание**: Минимальная длина пароля.

`password_user_attributes_check` - Проверка на сходство с именем, почтой и т.д.

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли пароль на сходство с атрибутами пользователя.

`password_common_check` - Проверка по списку часто используемых паролей.

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли пароль на наличие в списке распространенных паролей.

`password_numeric_check` - Запрет паролей, состоящих только из цифр.

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль не состоит из цифр полностью.

`password_need_specials`

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль содержит специальные символы.

`password_need_uppercase`

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль содержит буквы в верхнем регистре.

`password_need_lowercase`

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль содержит буквы в нижнем регистре.

`password_need_number`

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль содержит цифры.

`password_need_three_letters`

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли что пароль содержит хотя бы три различных символа.

`password_weak_check` - Проверка на простые последовательности (`12345`, `qwerty`).

- **Тип**: Boolean
- **По умолчанию**: true
- **Описание**: Проверять ли пароль на содержание распространённых фраз и последовательностей.

`password_history` - Включение проверки истории паролей.

- **Тип**: Boolean

- **По умолчанию**: true
- **Описание**: Запрещать ли совпадение с паролем который уже был использован до этого.

`password_history_length` - Глубина истории (сколько последних паролей запоминать).

- **Тип**: Int
- **По умолчанию**: 3
- **Описание**: Глубина истории при проверке на совпадение со старыми паролями пользователя.

`password_expire_days` - Срок действия пароля (дней). `0` - пароль не истекает.

- **Тип**: Int
- **По умолчанию**: 0 - без ограничений
- **Описание**: Ограничение времени жизни пароля.

Секция `two_factor_auth` (2FA)

`enabled`

- **Тип**: Boolean
- **Описание**: Глобальное включение/выключение двухфакторной аутентификации.

`require_after_failed_attempts`

- **Тип**: Integer
- **Описание**: Требовать 2FA после указанного количества неудачных попыток входа. `0` - всегда требовать.

`code_length`

- **Тип**: Integer
- **Описание**: Длина одноразового кода для 2FA.

Секция `ldap` (Интеграция с LDAP/AD)

Настройки подключения по LDAP указаны в разделе Настройки LDAP

Секция `sso` (Единый вход)

Настройки SSO указаны в разделе Настройки SSO

Секции `redis` и `rabbitmq` (Внешние сервисы)

`redis.url`

- **Тип**: String (URL)
- **Пример**: `"redis://localhost:6379/0"`
- **Описание**: Полный URL для подключения к Redis (используется для кэша, Celery брокера результатов).

`rabbitmq.url`

- **Тип**: String (URL)
- **Пример**: `"amqp://guest:guest@localhost:5672/"`
- **Описание**: Полный URL для подключения к RabbitMQ (используется как брокер сообщений для Celery).

Общие рекомендации

`config.debug`

```
config:
  debug: false
```

Объяснение: Режим отладки должен быть выключен в продакшен-окружении, чтобы предотвратить утечку информации.

SECRET_KEY

```
SECRET_KEY = 'your_strong_secret_key_here'
```

Объяснение: Используйте сильный и уникальный секретный ключ. Не храните его в репозитории или публично доступных местах.

MODE

```
mode: "prod"
```

Объяснение: Установите режим работы приложения как `prod` (production) для активации соответствующих настроек безопасности.

DJANGO_ALLOWED_HOSTS

```
DJANGO_ALLOWED_HOSTS = 'example.com,www.example.com'
```

Объяснение: Ограничьте список разрешенных хостов, чтобы предотвратить атаки типа Host header injection.

ACCESS_TOKEN_LIFETIME_MIN

```
ACCESS_TOKEN_LIFETIME_MIN = 15
```

Объяснение: Уменьшите время жизни access token для минимизации ущерба при компрометации токена.

REFRESH_TOKEN_LIFETIME_MIN

```
REFRESH_TOKEN_LIFETIME_MIN = 60 * 24 * 7  # 7 дней
```

Объяснение: Установите разумное ограничение времени жизни refresh token, например, 7 дней.

SECURITY_LOG_ROTATION_DAYS

```
SECURITY_LOG_ROTATION_DAYS = 365
```

Объяснение: Храните логи безопасности не менее одного года для анализа и аудита.

SQL_PASSWORD

```
SQL_PASSWORD = 'your_strong_db_password'
```

Объяснение: Используйте сложный пароль для базы данных. Избегайте использования простых или стандартных паролей.

CELERY_TASK_ALWAYS_EAGER

```
CELERY_TASK_ALWAYS_EAGER = False
```

Объяснение: Отключите синхронное выполнение задач Celery в продакшене, чтобы избежать блокировки основного потока.

PASSWORD_MIN_LENGTH

```
PASSWORD_MIN_LENGTH = 12
```

Объяснение: Увеличьте минимальную длину пароля до 12 символов для повышения уровня безопасности.

PASSWORD_USER_ATTRIBUTES

```
PASSWORD_USER_ATTRIBUTES = True
```

Объяснение: Включите проверку пароля на сходство с атрибутами пользователя (например, имя, фамилия).

PASSWORD_COMMON_PASSWORD

```
PASSWORD_COMMON_PASSWORD = True
```

Объяснение: Проверьте пароль на наличие в списке распространенных паролей.

PASSWORD_NUMERIC_PASSWORD

```
PASSWORD_NUMERIC_PASSWORD = True
```

Объяснение: Проверьте, что пароль не состоит только из цифр.

LOGIN_ATTEMPTS_LIMIT

```
LOGIN_ATTEMPTS_LIMIT = 5
```

Объяснение: Установите лимит попыток входа (например, 5) для предотвращения брутфорс-атак.

LOGIN_ATTEMPTS_TIMEOUT

```
LOGIN_ATTEMPTS_TIMEOUT = 15  # в минутах
```

Объяснение: Сократите время блокировки после превышения лимита попыток входа, чтобы минимизировать влияние на пользователей.

BimarSystem

Настройки LDAP

Настройка LDAP аутентификации для Active Directory

Этот документ описывает параметры конфигурации для подключения к Active Directory через LDAP.

Пример конфигурации

```
ldap:
  enabled: true
  auth_ldap_server_uri: "ldaps://host.customer.loc"
  auth_ldap_bind_dn: "CN=Searcher LDAP,OU=ServiceUsers,OU=Customer,DC=customer,DC=loc"
  auth_ldap_bind_password: "your_password_here"
  auth_ldap_user_search_base: "dc=customer,dc=loc"
  auth_ldap_user_search_filter: "(sAMAccountName=%(user)s)"
  auth_ldap_group_search_base: "DC=customer,DC=loc"
  auth_ldap_group_search_filter: "(objectClass=group)"
  auth_ldap_attr_firstname: "cn"
  auth_ldap_attr_lastname: "sn"
  auth_ldap_attr_email: "mail"
  groups:
    admin:
      dn: "cn=admin,ou=groups,dc=example,dc=com"
      is_superuser: true
      is_staff: true
    operator:
      dn: "cn=admin,ou=groups,dc=example,dc=com"
      is_superuser: false
      is_staff: true
    user:
      dn: "cn=admin,ou=groups,dc=example,dc=com"
      is_superuser: false
      is_staff: false
```

```
    it_g:
      dn: "cn=it_g,ou=it,ou=customer,dc=customer,dc=loc"
      is_superuser: true
      is_staff: true
```

Обязательные параметры

`ldap.enabled`

- **Тип**: boolean
- **По умолчанию**: `false`
- **Описание**: Включает/выключает LDAP аутентификацию
- **Пример**: `true`

`auth_ldap_server_uri`

- **Тип**: string
- **Формат**: `ldap://хост` или `ldaps://хост`
- **Описание**: URI LDAP сервера Active Directory
- **Примеры**:
  - `ldap://host.customer.loc` (незащищенное соединение)
  - `ldaps://host.customer.loc` (защищенное соединение TLS)
  - `ldap://192.168.1.10` (по IP адресу)

> ⚠️ **Важно**: При использовании `ldaps://` убедитесь, что сертификат CA добавлен в доверенные корневые центры сертификации.

`auth_ldap_bind_dn`

- **Тип**: string
- **Формат**: Distinguished Name (DN) сервисной учетной записи
- **Описание**: Учетная запись для подключения к AD и поиска пользователей
- **Примеры**:
  - `CN=Searcher LDAP,OU=ServiceUsers,OU=Customer,DC=customer,DC=loc`
  - `ldapsearcher@customer.loc` (UPN формат)
  - `customer\ldapsearcher` (DOMAIN\username формат)

`auth_ldap_bind_password`

- **Тип**: string

- **Описание**: Пароль сервисной учетной записи

Параметры поиска пользователей

`auth_ldap_user_search_base`

- **Тип**: string
- **Описание**: Базовый DN для поиска пользователей
- **Рекомендация**: Для AD обычно используется корень домена
- **Пример**: `dc=customer,dc=loc`

`auth_ldap_user_search_filter`

- **Тип**: string
- **Описание**: Фильтр для поиска пользователей
- **Для Active Directory**: `(sAMAccountName=%(user)s)`
- **Шаблон**: `%s` заменяется на имя пользователя, введенное при входе

> **Примечание**: В Active Directory используется `sAMAccountName`, а не `uid`

Параметры поиска групп

`auth_ldap_group_search_base`

- **Тип**: string
- **Описание**: Базовый DN для поиска групп
- **Пример**: `DC=customer,DC=loc` (по всему домену)

`auth_ldap_group_search_filter`

- **Тип**: string
- **Описание**: Фильтр для поиска групп
- **Для Active Directory**: `(objectClass=group)`

Маппинг атрибутов

`auth_ldap_attr_firstname`

- **Тип**: string
- **Описание**: Атрибут LDAP, содержащий имя пользователя

- **Для AD**: `cn`, `givenName`
- **Пример**: `cn`

auth_ldap_attr_lastname

- **Тип**: string
- **Описание**: Атрибут LDAP, содержащий фамилию пользователя
- **Для AD**: `sn`, `surname`
- **Пример**: `sn`

auth_ldap_attr_email

- **Тип**: string
- **Описание**: Атрибут LDAP, содержащий email
- **Для AD**: `mail`, `userPrincipalName`
- **Пример**: `mail`

Настройки групп

Структура групп

```
groups:
  <имя_группы_в_приложении>:
    dn: "DN_группы_в_AD"
    is_superuser: boolean
    is_staff: boolean
```

Примеры групп

```
groups:
  # Группа администраторов
  admin:
    dn: "CN=Domain Admins,CN=Users,DC=customer,DC=loc"
    is_superuser: true
    is_staff: true

  # Группа операторов
  operator:
    dn: "CN=Operators,OU=Groups,DC=customer,DC=loc"
    is_superuser: false
    is_staff: true

  # Группа обычных пользователей
```

```
  user:
    dn: "CN=Domain Users,CN=Users,DC=customer,DC=loc"
    is_superuser: false
    is_staff: false

  # IT группа
  it_g:
    dn: "CN=IT_Group,OU=IT,OU=Customer,DC=customer,DC=loc"
    is_superuser: true
    is_staff: true
```

Параметры группы

Параметр	Тип	Описание
`dn`	string	Distinguished Name группы в Active Directory
`is_superuser`	boolean	Дает права суперпользователя Django
`is_staff`	boolean	Разрешает доступ в административную панель Django

---

Проверка подключения

Команда для тестирования LDAP:

```
# Проверка аутентификации
ldapsearch -x -H ldap://host.customer.loc \
  -D "CN=Searcher LDAP,OU=ServiceUsers,OU=Customer,DC=customer,DC=loc" \
  -W \
  -b "dc=customer,dc=loc" \
  "(sAMAccountName=administrator)"

# Поиск всех групп
ldapsearch -x -H ldap://host.customer.loc \
  -D "CN=Searcher LDAP,OU=ServiceUsers,OU=Customer,DC=customer,DC=loc" \
  -W \
  -b "dc=customer,dc=loc" \
  "(objectClass=group)" cn
```

Решение частых проблем

1. Ошибка "Invalid credentials"

Причина: Неправильный DN или пароль **Решение**:

- Проверьте правильность `auth_ldap_bind_dn`
- Проверьте пароль в `auth_ldap_bind_password`
- Попробуйте UPN формат: `username@domain.loc`

2. Ошибка "Can't contact LDAP server"

Причина: Проблемы с сетью или сертификатами **Решение**:

- Проверьте доступность сервера: `ping host.customer.loc`
- Для `ldaps://` добавьте сертификат CA в доверенные
- Используйте `ldap://` для тестирования

Готовые примеры конфигураций

Для Active Directory:

```
ldap:
  enabled: true
  auth_ldap_server_uri: "ldap://dc.example.com"
  auth_ldap_bind_dn: "service_account@example.com"
  auth_ldap_bind_password: "secure_password"
  auth_ldap_user_search_base: "dc=example,dc=com"
  auth_ldap_user_search_filter: "(sAMAccountName=%(user)s)"
  auth_ldap_group_search_base: "dc=example,dc=com"
  auth_ldap_group_search_filter: "(objectClass=group)"
```

Для OpenLDAP:

```
ldap:
  enabled: true
  auth_ldap_server_uri: "ldap://openldap.example.com"
  auth_ldap_bind_dn: "cn=admin,dc=example,dc=com"
  auth_ldap_bind_password: "admin_password"
  auth_ldap_user_search_base: "ou=users,dc=example,dc=com"
  auth_ldap_user_search_filter: "(uid=%(user)s)"
  auth_ldap_group_search_base: "ou=groups,dc=example,dc=com"
  auth_ldap_group_search_filter: "(objectClass=groupOfNames)"
```

Настройки SSO

Настройка SSO аутентификации через Kerberos/SPNEGO

Этот документ описывает параметры конфигурации для единого входа (SSO) через Kerberos/SPNEGO в Active Directory окружении.

Пример конфигурации

```
sso:
  enabled: true
  keytab_spn: "HTTP/web.bimarkit.com@CUSTOMER.LOC"
  keytab_path: "/etc/krb5.keytab"
```

Обязательные параметры

`sso.enabled`

- **Тип**: boolean
- **По умолчанию**: `false`
- **Описание**: Включает/выключает SSO аутентификацию через Kerberos
- **Пример**: `true`

`keytab_spn`

- **Тип**: string
- **Формат**: `HTTP/hostname@REALM`
- **Описание**: Service Principal Name для вашего веб-приложения

- **Примеры**:
  - `HTTP/webapp.customer.loc@CUSTOMER.LOC`
  - `HTTP/web.bimarkit.com@CUSTOMER.LOC`

> ⚠️ **Важно**: SPN должен совпадать с DNS именем вашего приложения

keytab_path

- **Тип**: string
- **Формат**: Абсолютный путь к файлу keytab
- **Описание**: Путь к keytab файлу с ключами сервиса
- **Примеры**:
  - `/etc/krb5.keytab`

Проверка подключения

Тестирование keytab файла

```
# Проверить содержимое keytab
klist -ket /path/to/krb5.keytab

# Проверить аутентификацию
kinit -kt /path/to/krb5.keytab HTTP/webapp.customer.loc

# Проверить билет
klist
```

Решение частых проблем

1. Ошибка "Key table entry not found"

Причина: Неправильный SPN в keytab **Решение**: - Проверьте SPN: `setspn -L webapp-service` - Убедитесь, что `keytab_spn` совпадает с SPN в keytab - Пересоздайте keytab с правильным SPN

2. Ошибка "Cannot contact KDC"

Причина: Проблемы с DNS или KDC **Решение**: - Проверьте DNS: `nslookup dc.customer.loc` - Проверьте доступность KDC: `telnet dc.customer.loc 88` - Убедитесь, что `krb5.conf` настроен правильно

3. Ошибка "GSSAPI authentication failed"

Причина: Неправильное время или версия протокола **Решение**: - Синхронизируйте время: `ntpdate dc.customer.loc` - Проверьте версию протокола в keytab - Используйте современные алгоритмы (AES256)

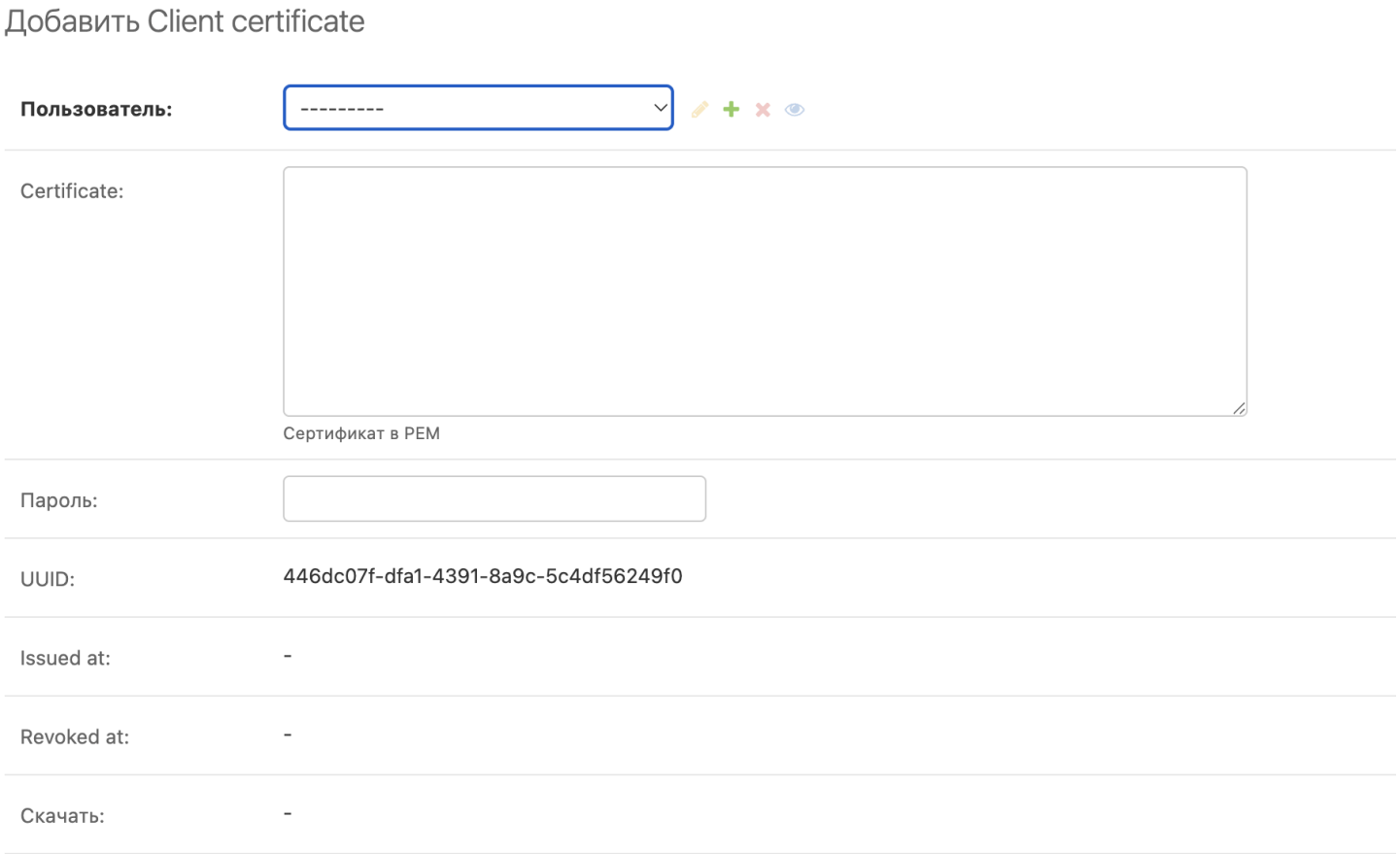
4. Браузер не предлагает SSO

Причина: Сайт не в зоне доверия **Решение**: - Добавьте сайт в "Local Intranet" зону - Убедитесь, что URL использует FQDN - Проверьте настройки IE/Chrome для Integrated Windows Authentication

BimarSystem

Авторизация по сертификату

Добавление сертификата пользователя:



Настройки сертификата и ключа которыми будут подписаны пользовательские сертификаты: CA_CRT_PATH = config_loader.get("django.ca_crt_path", str(BASE_DIR.parent / "infrastructure" / "ssl" / "ca.crt")) CA_KEY_PATH = config_loader.get("django.ca_key_path", str(BASE_DIR.parent / "infrastructure" / "ssl" / "ca.key")) CA_KEY_PASSWORD = config_loader.get("django.ca_key_password", None)