«Цифровой Купол». Система централизованной аутентификации и управления доступом

DIGITAL DESIGN

О группе компаний Digital Design

Digital Design — один из 20 крупнейших разработчиков ПО в России

5 000+
успешных проектов

550+
специалистов

350+
клиентов в 30+ странах

30+
лет на рынке

РЖД Российские железные дороги · СБЕРБАНК · РусГидро · ГАЗПРОМ · МИНПРОМТОРГ РОССИИ

DIGITAL DESIGN

«Диджитал Дизайн»
Компания разрабатывает и внедряет системы автоматизации бизнес-процессов, электронного документооборота, информационной безопасности, а также портальные решения и мобильные приложения

docsvision

«ДоксВижн»
Компания стояла у истоков автоматизации документооборота и делопроизводства в нашей стране. Является одним из лидеров рынка СЭД/ECM/BPM. Платформа Docsvision используется более чем в 1 000 организаций России и стран ближнего зарубежья. Ее внедряют более 100 отечественных и зарубежных партнёров

Центр информационной безопасности

Соответствие требованиям регуляторов ИБ

Анализ и контроль защищенности ИС

Аудит ИБ и безопасность бизнес-процессов

Построение и внедрение процессов безопасной разработки ПО

Проектирование, внедрение подсистем защиты информации

Подготовка и аттестация на соответствие требованиям

Проектирование ЦОД в защищенном исполнении

Оглавление

Информация, обрабатываемая в ИС

Персональные данные работников и внешних субъектов

Служебная тайна, коммерческая тайна

Иная информация, охраняемая законодательством РФ

Типы информационных систем

Информационные системы АСУ ТП

- Приказ ФСТЭК России № 31

Информационные системы КИИ

- ФЗ № 187
- ПП РФ № 127
- Приказ ФСТЭК России № 239

Информационные системы персональных данных (ИСПДн)

- ФЗ № 152
- ПП РФ № 1119
- Приказ ФСТЭК России № 21
- Приказ ФСБ России №378

Государственные информационные системы (ГИС)

- ФЗ № 149
- ПП РФ № 676
- Приказ ФСТЭК России № 17
- Приказ ФСБ России № 524

Автоматизированные системы, обрабатывающие конфиденциальную информацию (АС/ИС)

- РД АС от НСД
- СТР-К (Спец треб-я и рекомендации)

Классы защищенности ИС

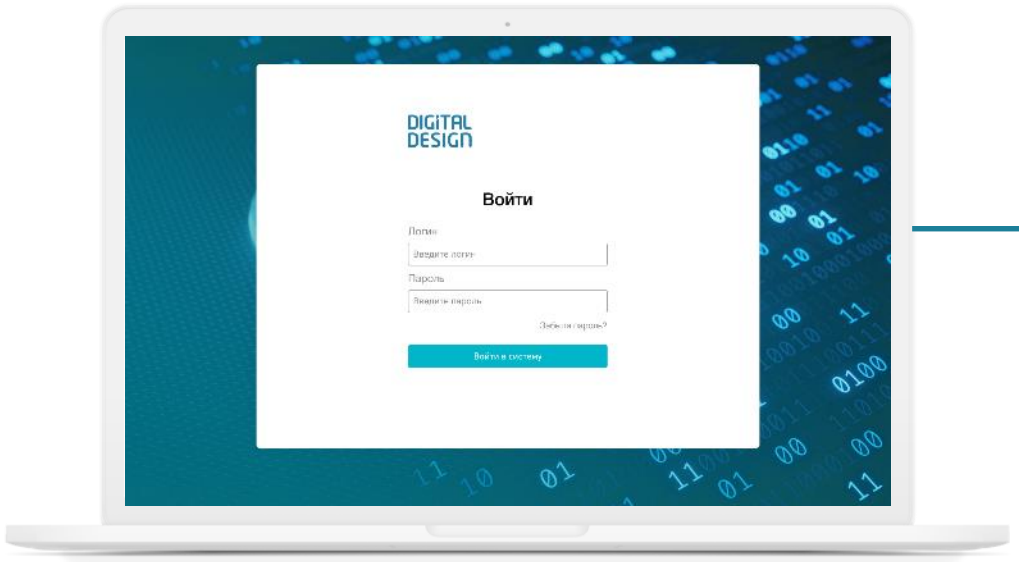
	АСУ ТП	КИИ	ИСПДн	АС/ИС	Сертификация СрЗИ
Классы защищенности ИС	К3	3	3-4 УЗ	1 Г	6 УД
	К2	2	2 УЗ		5 УД
	К1	1	1 УЗ		4 УД

Ключевая проблема

Разрозненная идентификация и аутентификация, регистрация событий безопасности усложняет аудит доступа сотрудников

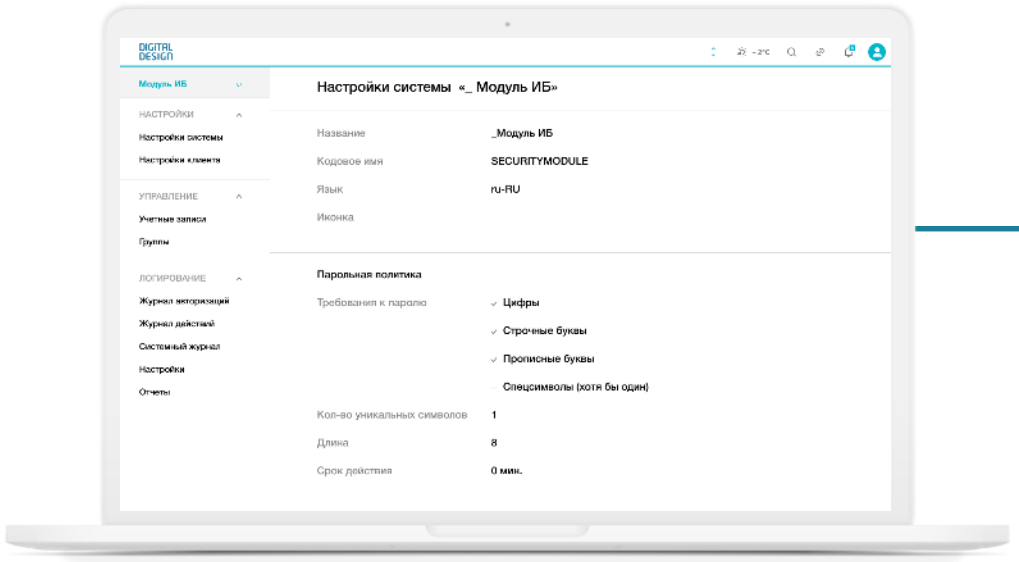
1. «Облачный» тренд и развитие технологии «тонкого» клиента
2. При удаленной работе повышается риск взлома учетных записей
3. Парольной аутентификации недостаточно для эффективной защиты многих приложений
4. Собственные механизмы входа приложений не всегда безопасны

Основные функции «Цифрового Купола» (1)



- Управление сессиями пользователей во всех системах (поддерживающих OpenID Connect, OAuth) и отслеживание фактов и факторов идентификации и аутентификации пользователей
- Управление доступом пользователей к объектам доступа (ролевая модель)
- Генерация и выдача идентификационной информации
- Подходит для разных пользователей: сотрудников, клиентов, контрагентов

Основные функции «Цифрового Купола» (2)



- Управление идентификаторами
- Многофакторная аутентификация пользователей с применением Email, SMS, Push, TOTP
- Регистрация событий безопасности
- Обеспечение целостности
- Возможность выгрузки событий безопасности во внешнюю систему анализа защищенности (SIEM)


Внешние ИС
Управление сессиями пользователей в ИС
Отслеживание фактов и факторов идентификация и аутентификация
Email-сервер, SMS-шлюз, сервисы push-уведомлений,
Хранилище учетных записей и паролей
Управление доступом пользователей
Управление идентификаторами
Многофакторная аутентификация
Регистрация событий безопасности
Обеспечение целостности
Провайдеры идентификации
Сервисы инфраструктурной безопасности (SIEM, IDM, NGFW, PKI)

Типовая схема развертывания «Цифрового Купола»

Преимущества

Централизованное решение

Единый каталог пользователей для аутентификации

Ролевая модель

Передача функции безопасности по ролевой модели

Многофакторная аутентификация пользователей в корпоративных и облачных сервисах

Унифицированные политики аутентификации

Контроль целостности как внешних ИС, так и собственных

Протоколирование событий безопасности и подотчетность действий пользователей

Встроенная поддержка множества методов аутентификации
и подтверждения входа

Конфигурируемый пользовательский интерфейс страниц входа, регистрации, восстановления доступа, управления учетной записью

Roadmap 2024

Q2 2024

МОДИФИКАЦИЯ

Доработка функций безопасности

- 2FA с использованием аппаратных токенов (FIDO2)
- Контроль сессий пользователей
- Вход через госуслуги (ЕСИА)
- Доработка SSO через SAML

Q3 2024

МОДИФИКАЦИЯ

Доработка функций безопасности

- Вход по квалифицированной электронной подписи (УКЭП)
- Возможность беспарольной аутентификации
- Доработка возможности выбора проверки/снятия и фиксации КС по ГОСТ 34.11
- Возможность блокировки входа в ИС по группам/IP/подсетям

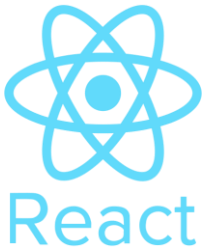
Q4 2024

СЕРТИФИКАЦИЯ И ДОРАБОТКА

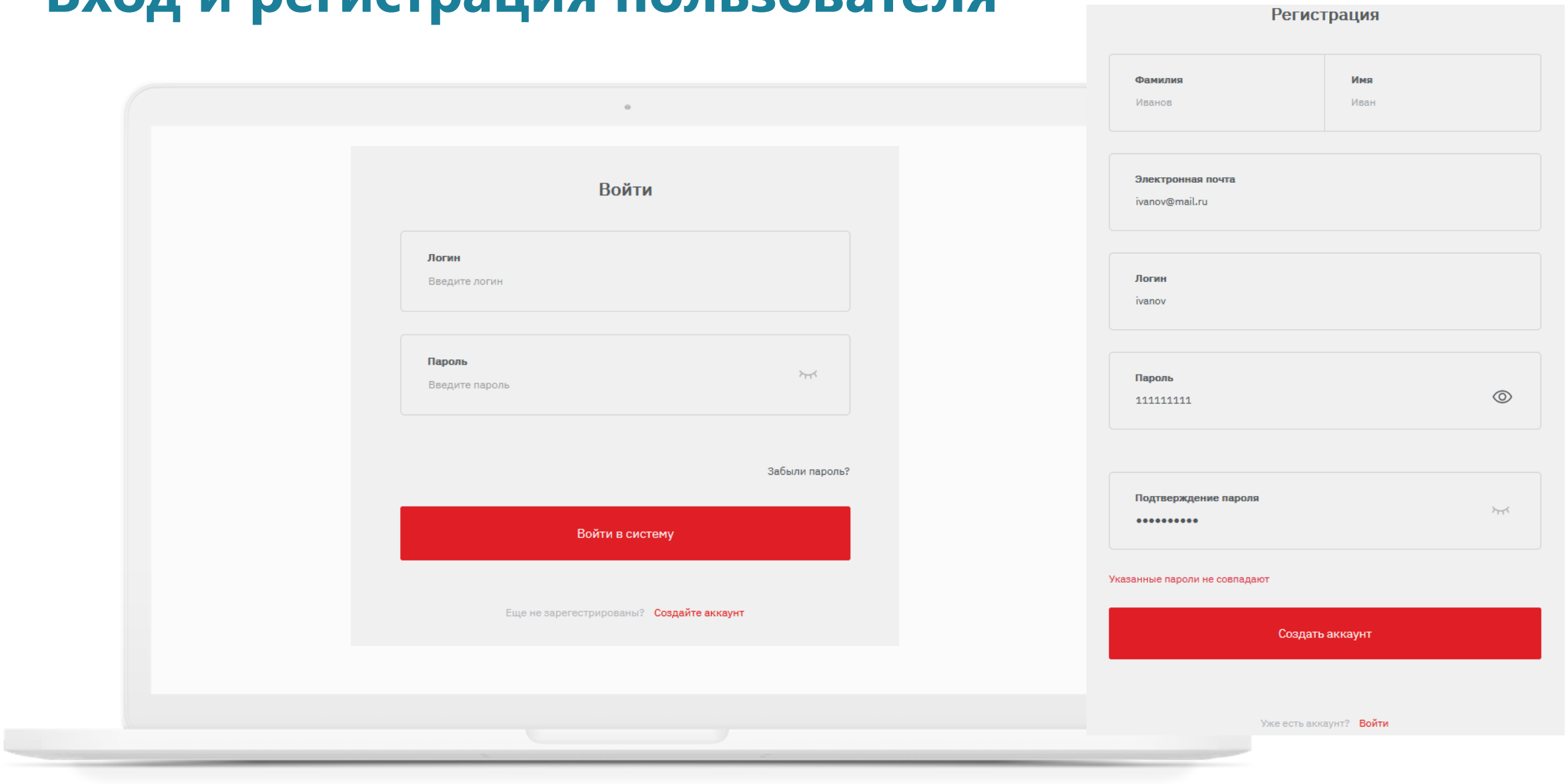
- Конфигурирование «Цифрового Купола» через веб-интерфейс (первичная настройка)
- Возможность установки «Цифрового Купола» в k8s
- Сертификация «Цифрового Купола» в ФСТЭК России по УД 4

Схема работы «Цифрового Купола»

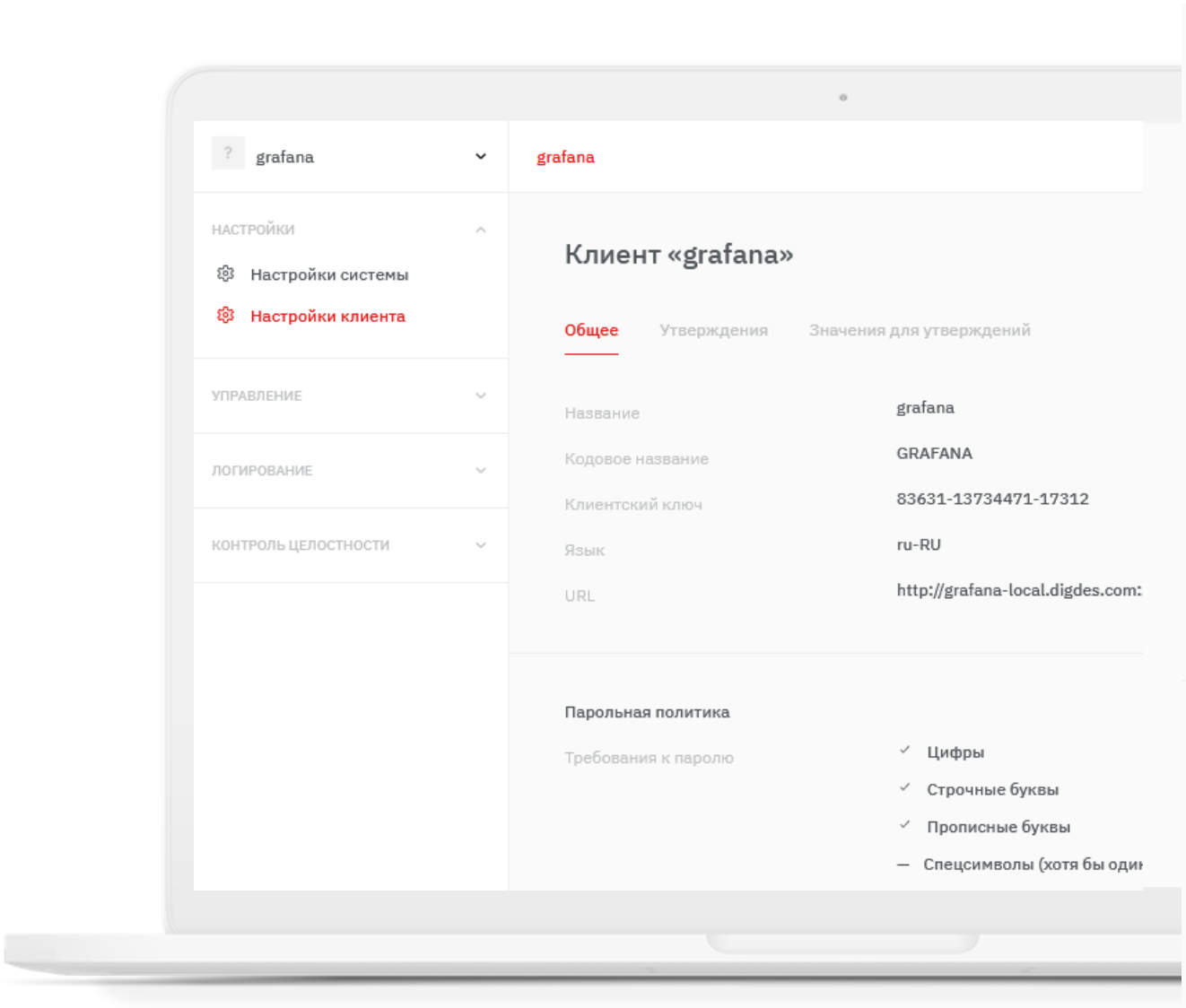
Компоненты «Цифрового Купола»

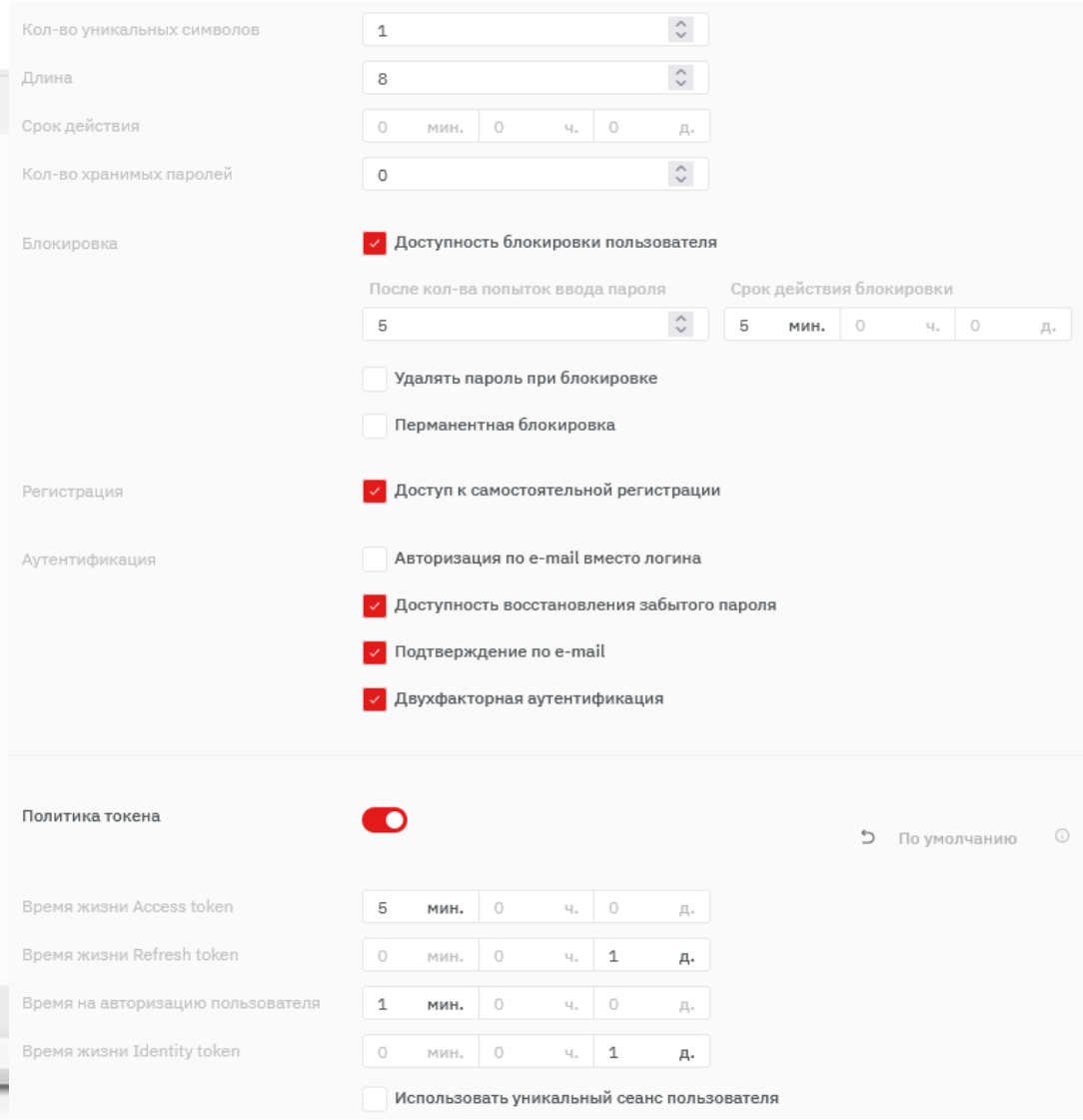


Вход и регистрация пользователя

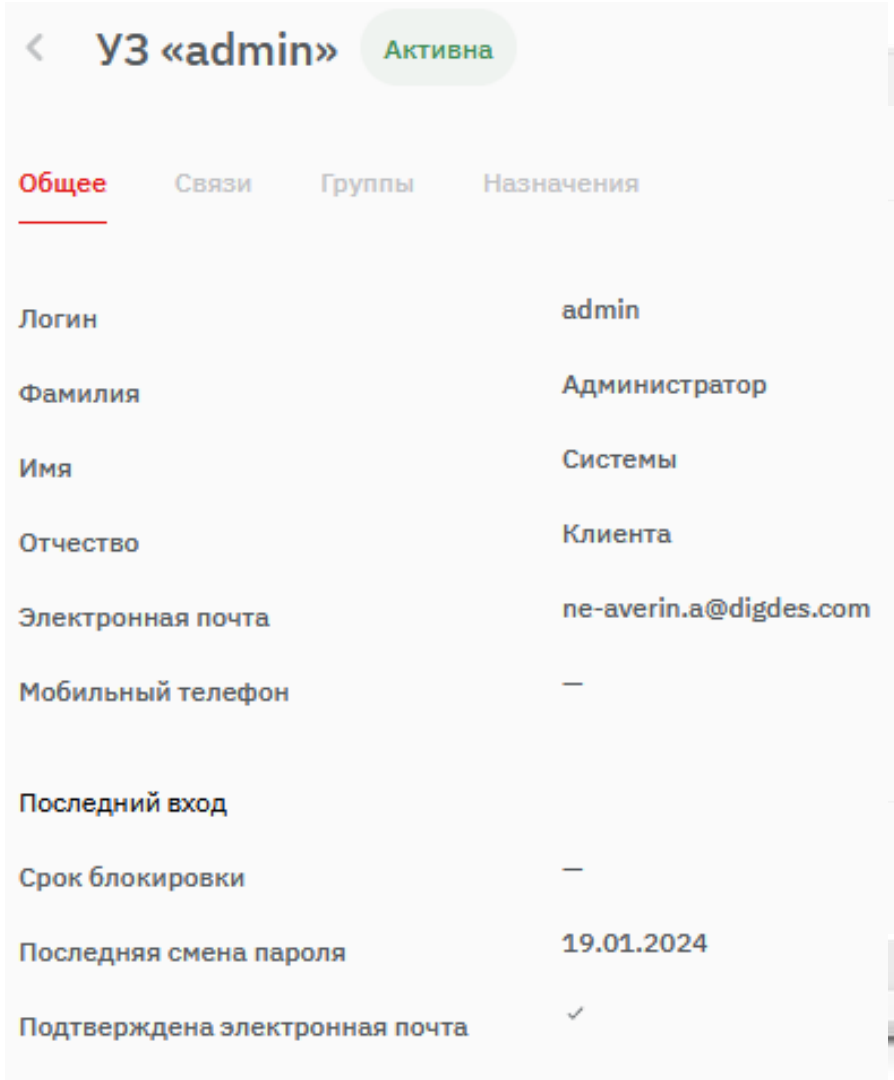


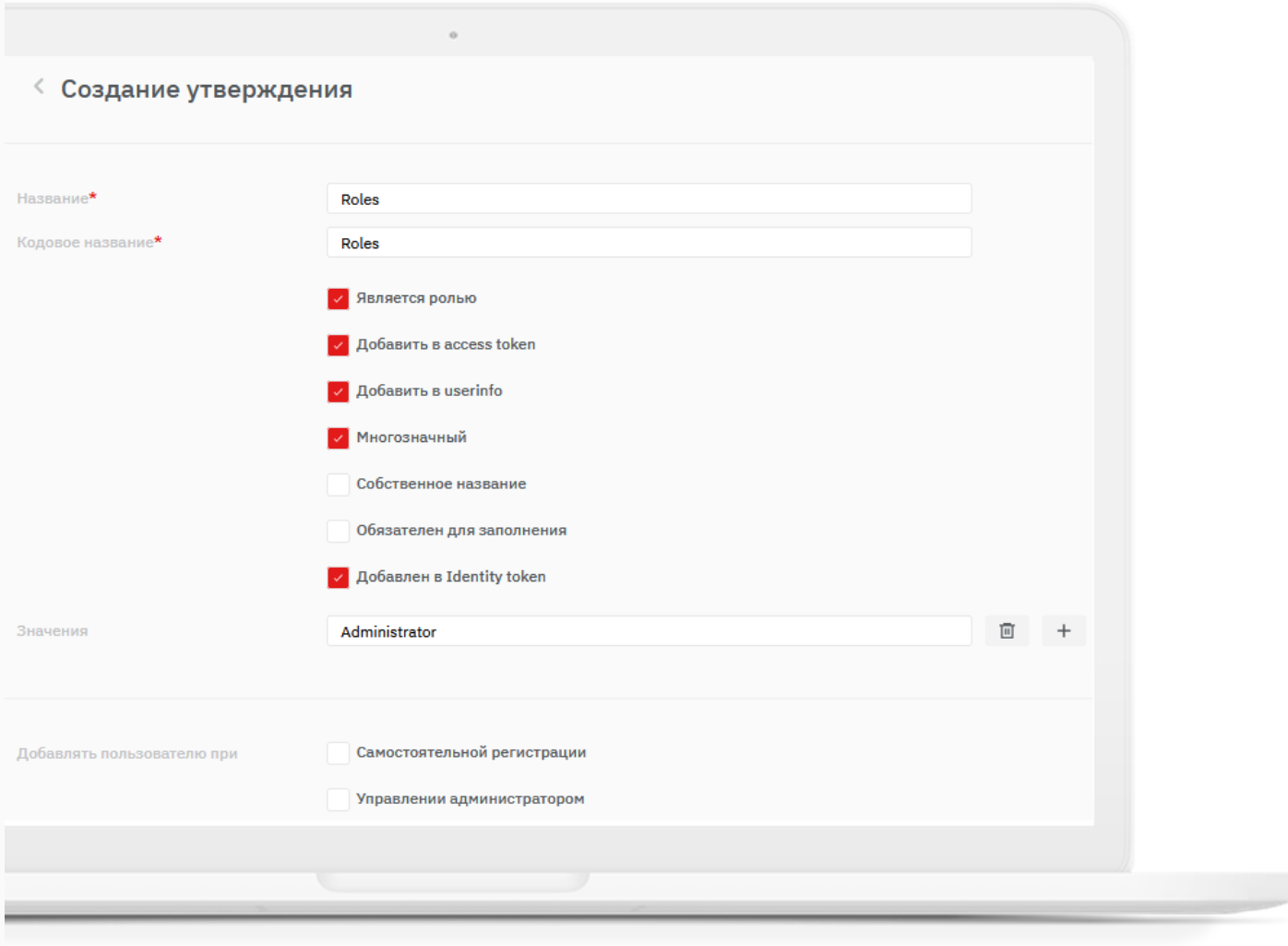
Настройка системы (клиента)



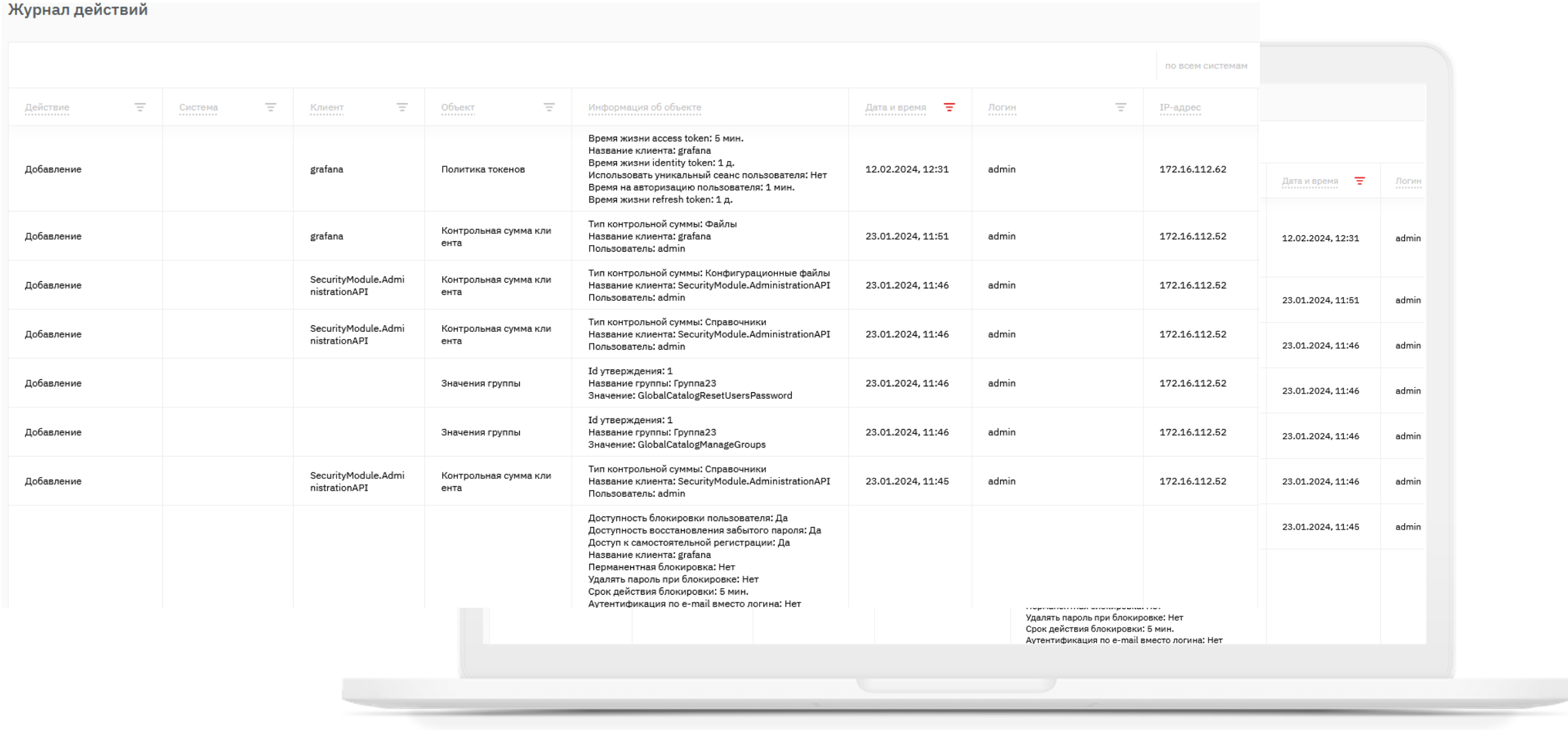


Создание учетной записи и групп

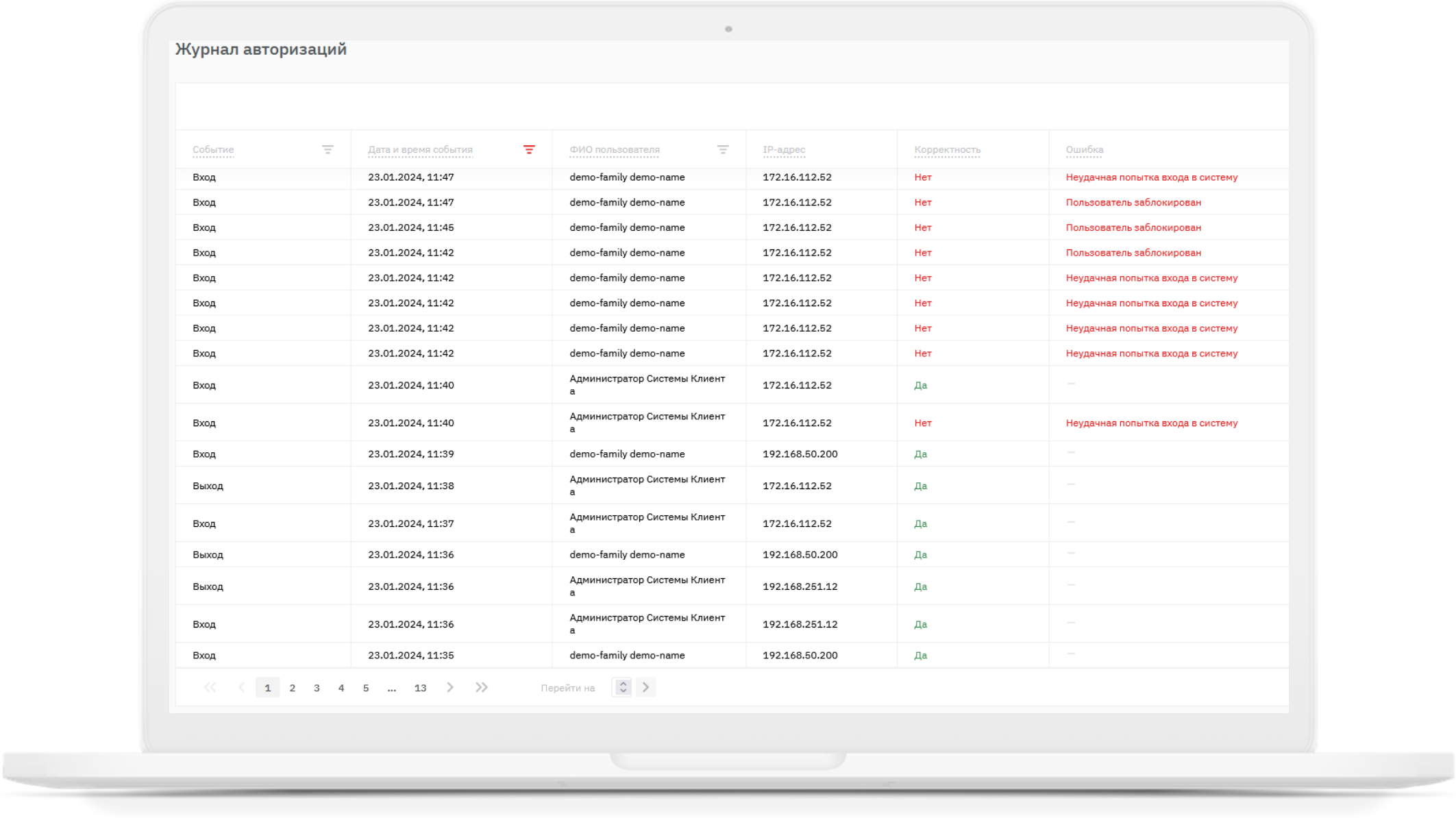




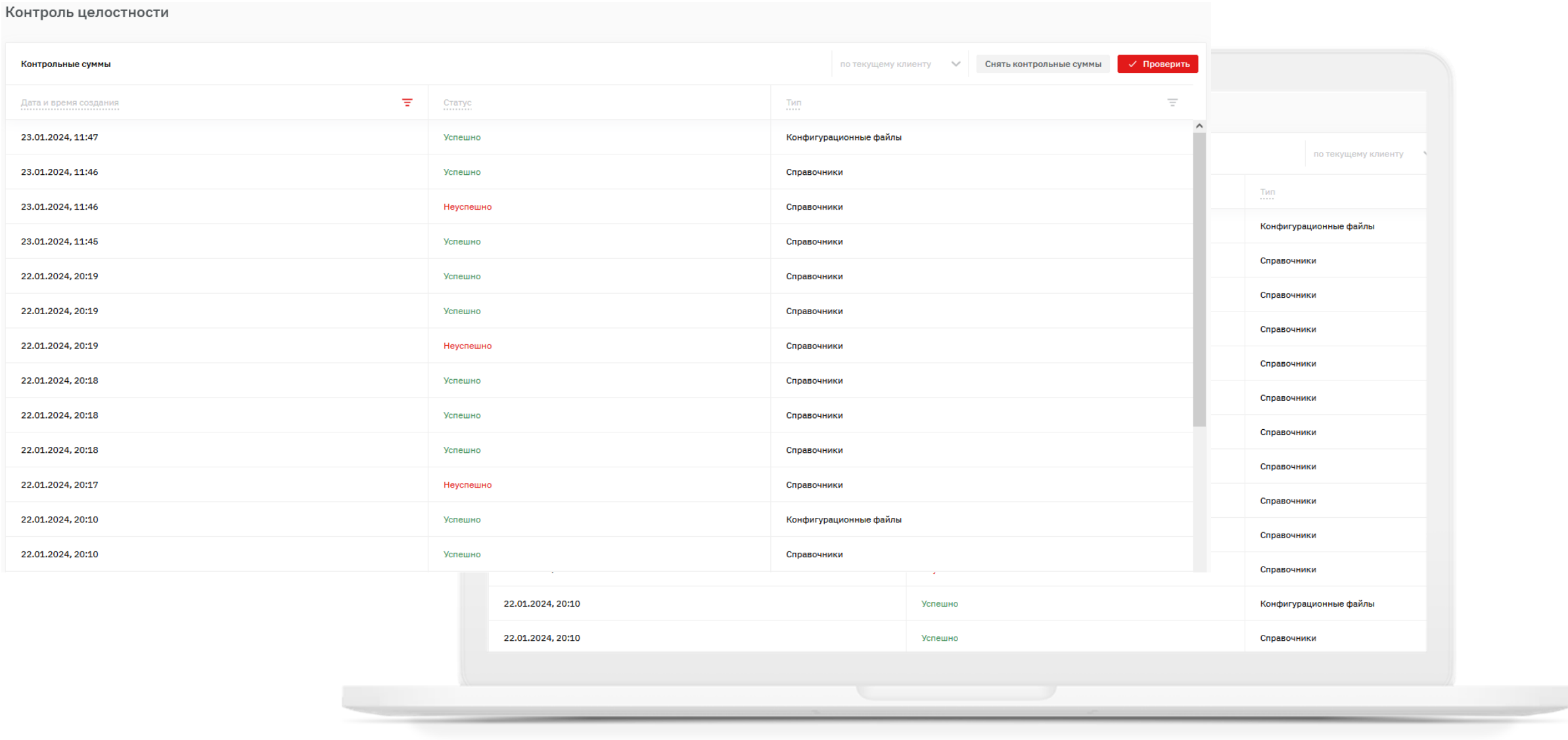
Журнал действий



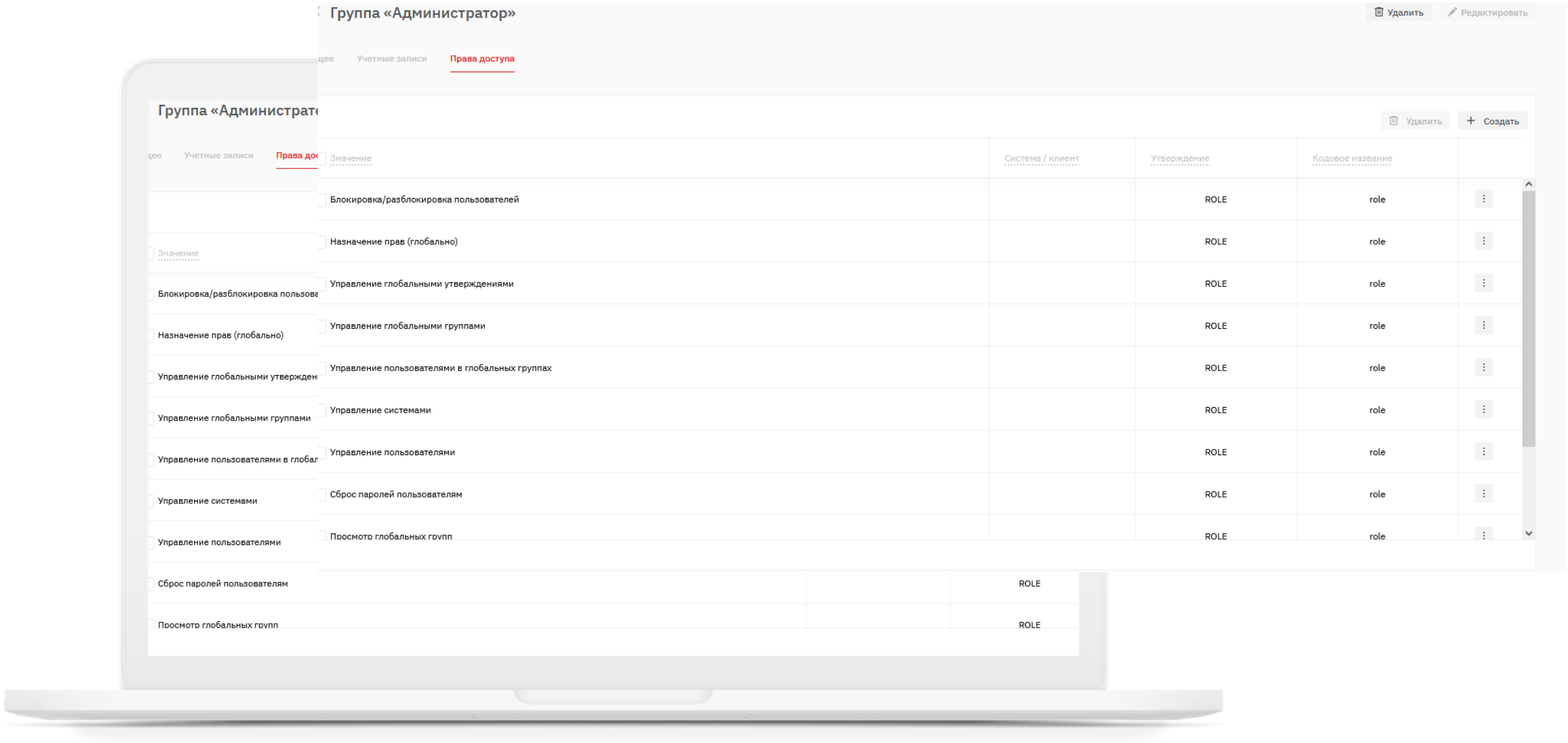
Журнал авторизаций



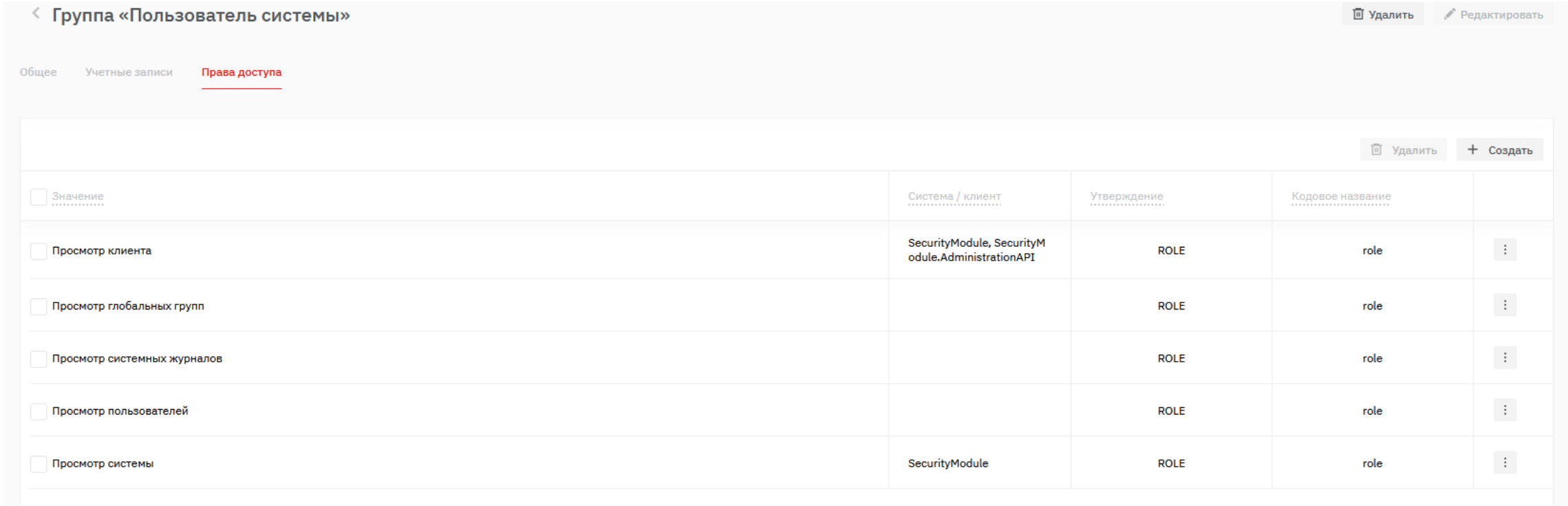
Контроль целостности



Примеры ролевой модели (1)



Примеры ролевой модели (2)



Контакты

Дмитрий Щербаков

Scherbakov.D@digdes.com

Санкт-Петербург

наб. реки Смоленки, д. 33
телефон: +7 812 346 58 33

Москва

Одесская ул., дом 2, корпус С., БЦ "Лотос", 10 этаж
телефон: +7 499 788 74 94

www.digdes.ru

info@digdes.com

DIGITAL DESIGN