

«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

**DIGITAL
DESIGN**

«Диджитал Дизайн»

Компания разрабатывает и внедряет системы автоматизации бизнес-процессов, электронного документооборота, информационной безопасности, а также порталные решения и мобильные приложения

docsvision

«ДоксВижн»

Компания стояла у истоков автоматизации документооборота и делопроизводства в нашей стране. Является одним из лидеров рынка СЭД/ЕСМ/ВРМ. 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

1. Введение
2. Ключевые проблемы
3. Функциональные возможности СЗИ Купол
4. Типовой план внедрения системы
5. Основные преимущества
6. Дорожная карта развития системы
7. Архитектура и компоненты системы
8. Примеры экранных форм

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 защищенност и 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

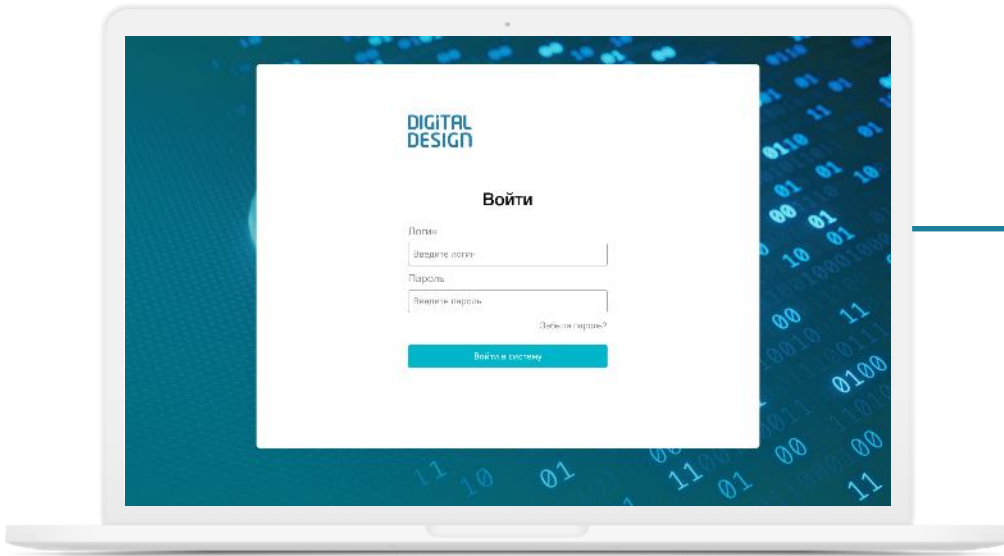
3

Парольной аутентификации недостаточно для эффективной защиты многих приложений

4

Собственные механизмы входа приложений не всегда безопасны

Основные функции «Цифрового Купола» (1)



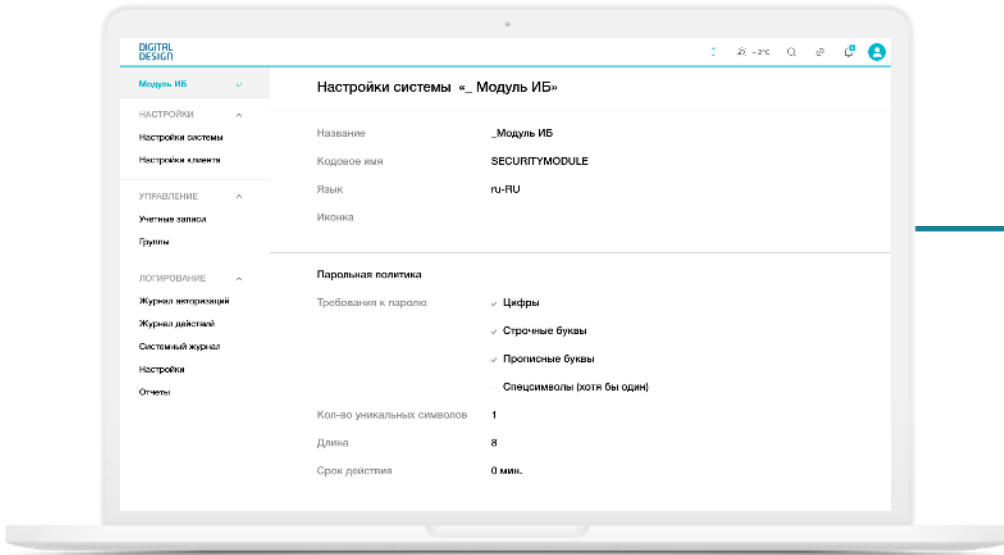
Управление сессиями пользователей во всех системах (поддерживающих OpenID Connect, OAuth) и отслеживание фактов и факторов идентификации и аутентификации пользователей

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)



Типовая схема развертывания «Цифрового Купола»



Эксплуатация

Эксплуатация ИС с «Цифровым Куполом»

Масштабирование

Масштабирование на иные ИС

Интеграция

Интеграция ИС с «Цифровым Куполом»

Инсталляция

Установка отказоустойчивого исполнения «Цифрового Купола»

Обследование

Обследование ИС в части передачи ролевой модели в «Цифровом Куполе»



Преимущества



Централизованное решение

Единый каталог пользователей для аутентификации



Контроль целостности как внешних ИС, так и собственных



Ролевая модель

Передача функции безопасности по ролевой модели



Протоколирование событий безопасности и подотчетность действий пользователей



Многофакторная аутентификация пользователей в корпоративных и облачных сервисах



Встроенная поддержка множества методов аутентификации и подтверждения входа



Унифицированные политики аутентификации



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

Roadmap 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

Q2 2024



Q3 2024



Q4 2024



МОДИФИКАЦИЯ

Доработка функций безопасности

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

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

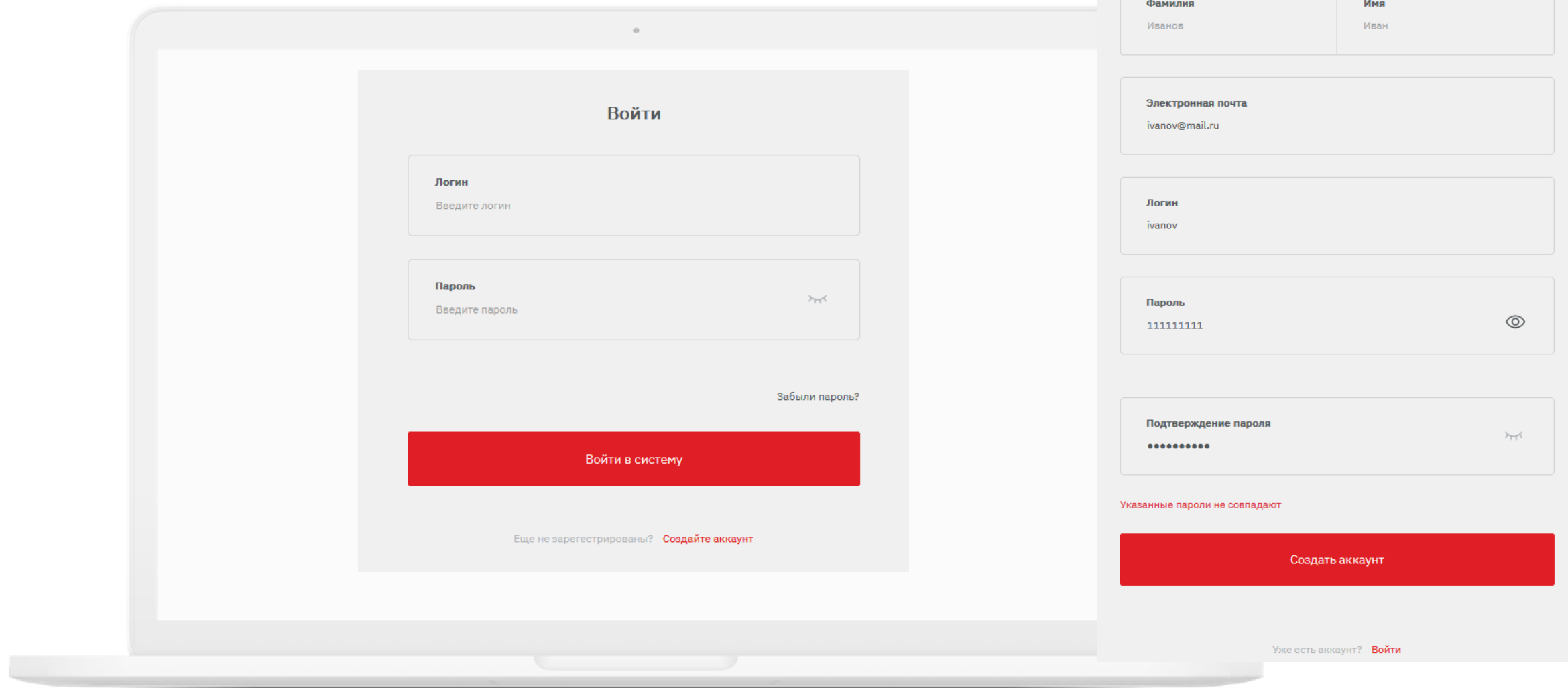
Схема работы «Цифрового Купола»



Компоненты «Цифрового Купола»



Вход и регистрация пользователя



Войти

Логин

Введите логин

Пароль

Введите пароль



[Забыли пароль?](#)

Войти в систему

[Еще не зарегистрированы?](#) [Создайте аккаунт](#)

Регистрация

Фамилия

Иванов

Имя

Иван

Электронная почта

ivanov@mail.ru

Логин

ivanov

Пароль

111111111



Подтверждение пароля

.....

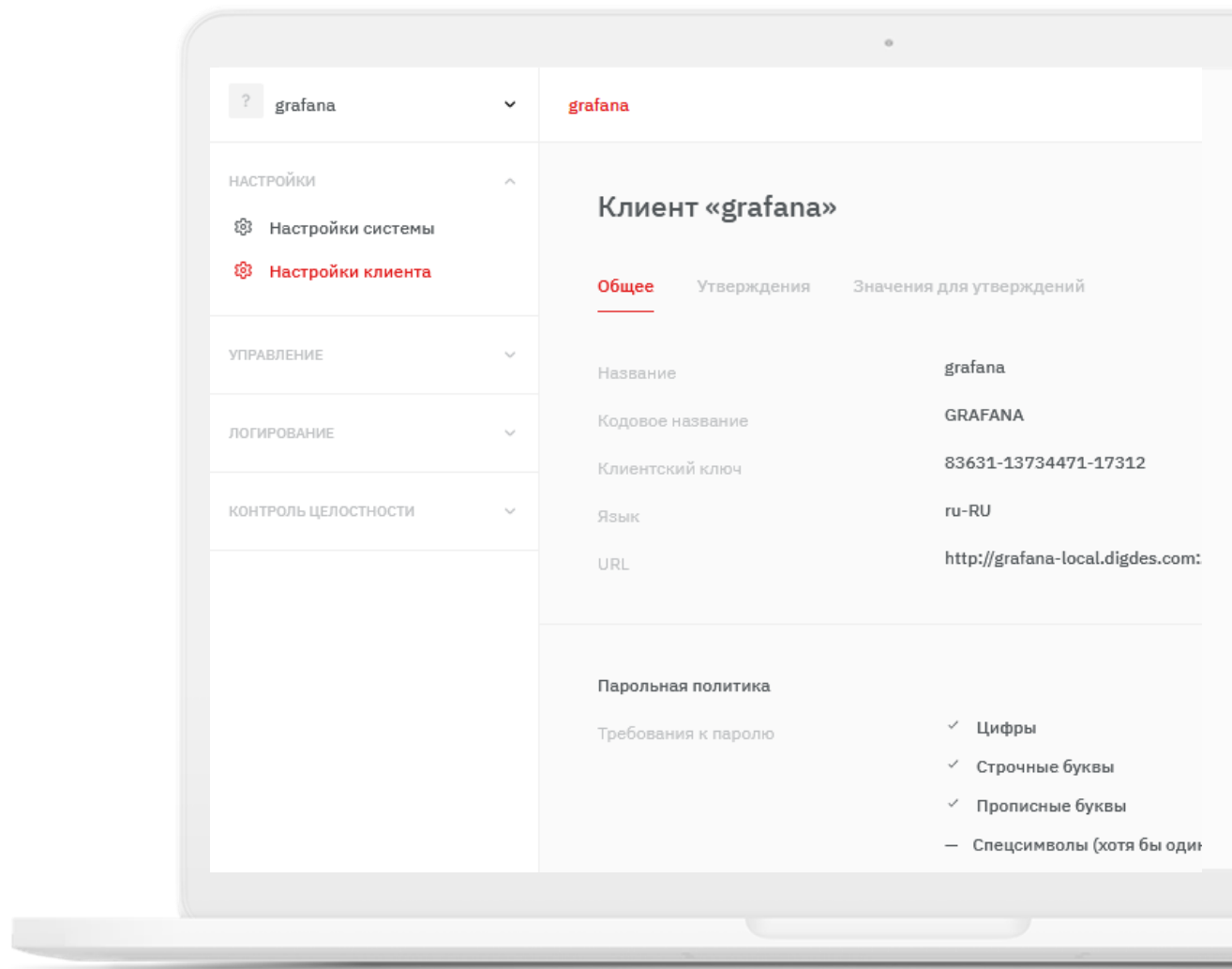


Указанные пароли не совпадают

Создать аккаунт

[Уже есть аккаунт?](#) [Войти](#)

Настройка системы (клиента)



Кол-во уникальных символов	<input type="text" value="1"/>
Длина	<input type="text" value="8"/>
Срок действия	<input type="text" value="0"/> мин. <input type="text" value="0"/> ч. <input type="text" value="0"/> д.
Кол-во хранимых паролей	<input type="text" value="0"/>
Блокировка	<input checked="" type="checkbox"/> Доступность блокировки пользователя После кол-ва попыток ввода пароля <input type="text" value="5"/> Срок действия блокировки <input type="text" value="5"/> мин. <input type="text" value="0"/> ч. <input type="text" value="0"/> д. <input type="checkbox"/> Удалять пароль при блокировке <input type="checkbox"/> Перманентная блокировка
Регистрация	<input checked="" type="checkbox"/> Доступ к самостоятельной регистрации
Аутентификация	<input type="checkbox"/> Авторизация по e-mail вместо логина <input checked="" type="checkbox"/> Доступность восстановления забытого пароля <input checked="" type="checkbox"/> Подтверждение по e-mail <input checked="" type="checkbox"/> Двухфакторная аутентификация
Политика токена	<input checked="" type="checkbox"/> По умолчанию
Время жизни Access token	<input type="text" value="5"/> мин. <input type="text" value="0"/> ч. <input type="text" value="0"/> д.
Время жизни Refresh token	<input type="text" value="0"/> мин. <input type="text" value="0"/> ч. <input type="text" value="1"/> д.
Время на авторизацию пользователя	<input type="text" value="1"/> мин. <input type="text" value="0"/> ч. <input type="text" value="0"/> д.
Время жизни Identity token	<input type="text" value="0"/> мин. <input type="text" value="0"/> ч. <input type="text" value="1"/> д.
	<input type="checkbox"/> Использовать уникальный сеанс пользователя

Создание учетной записи и групп

< УЗ «admin» Активна

Общее Связи Группы Назначения

Логин	admin
Фамилия	Администратор
Имя	Системы
Отчество	Клиента
Электронная почта	ne-averin.a@digdes.com
Мобильный телефон	—
Последний вход	—
Срок блокировки	—
Последняя смена пароля	19.01.2024
Подтверждена электронная почта	✓

< Создание утверждения

Название* Roles

Кодовое название* Roles

- Является ролью
- Добавить в access token
- Добавить в userinfo
- Многочисленный
- Собственное название
- Обязателен для заполнения
- Добавлен в Identity token

Значения Administrator 🗑️ +

Добавлять пользователю при

- Самостоятельной регистрации
- Управлении администратором

Журнал действий

Журнал действий

по всем системам									
Действие	Система	Клиент	Объект	Информация об объекте	Дата и время	Логин	IP-адрес	Дата и время	Логин
Добавление		grafana	Политика токенов	Время жизни access token: 5 мин. Название клиента: grafana Время жизни identity token: 1 д. Использовать уникальный сеанс пользователя: Нет Время на авторизацию пользователя: 1 мин. Время жизни refresh token: 1 д.	12.02.2024, 12:31	admin	172.16.112.62		
Добавление		grafana	Контрольная сумма клиента	Тип контрольной суммы: Файлы Название клиента: grafana Пользователь: admin	23.01.2024, 11:51	admin	172.16.112.52	12.02.2024, 12:31	admin
Добавление		SecurityModule.AdministrationAPI	Контрольная сумма клиента	Тип контрольной суммы: Конфигурационные файлы Название клиента: SecurityModule.AdministrationAPI Пользователь: admin	23.01.2024, 11:46	admin	172.16.112.52	23.01.2024, 11:51	admin
Добавление		SecurityModule.AdministrationAPI	Контрольная сумма клиента	Тип контрольной суммы: Справочники Название клиента: SecurityModule.AdministrationAPI Пользователь: admin	23.01.2024, 11:46	admin	172.16.112.52	23.01.2024, 11:46	admin
Добавление			Значения группы	Id утверждения: 1 Название группы: Группа23 Значение: GlobalCatalogResetUsersPassword	23.01.2024, 11:46	admin	172.16.112.52	23.01.2024, 11:46	admin
Добавление			Значения группы	Id утверждения: 1 Название группы: Группа23 Значение: GlobalCatalogManageGroups	23.01.2024, 11:46	admin	172.16.112.52	23.01.2024, 11:46	admin
Добавление		SecurityModule.AdministrationAPI	Контрольная сумма клиента	Тип контрольной суммы: Справочники Название клиента: SecurityModule.AdministrationAPI Пользователь: admin	23.01.2024, 11:45	admin	172.16.112.52	23.01.2024, 11:46	admin
				Доступность блокировки пользователя: Да Доступность восстановления забытого пароля: Да Доступ к самостоятельной регистрации: Да Название клиента: grafana Перманентная блокировка: Нет Удалять пароль при блокировке: Нет Срок действия блокировки: 5 мин. Аутентификация по e-mail вместо логина: Нет				23.01.2024, 11:45	admin
				Перманентная блокировка: Нет Удалять пароль при блокировке: Нет Срок действия блокировки: 5 мин. Аутентификация по e-mail вместо логина: Нет					

Журнал авторизаций

Журнал авторизаций

Событие	Дата и время события	ФИО пользователя	IP-адрес	Корректность	Ошибка
Вход	23.01.2024, 11:47	demo-family demo-name	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:47	demo-family demo-name	172.16.112.52	Нет	Пользователь заблокирован
Вход	23.01.2024, 11:45	demo-family demo-name	172.16.112.52	Нет	Пользователь заблокирован
Вход	23.01.2024, 11:42	demo-family demo-name	172.16.112.52	Нет	Пользователь заблокирован
Вход	23.01.2024, 11:42	demo-family demo-name	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:42	demo-family demo-name	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:42	demo-family demo-name	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:42	demo-family demo-name	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:40	Администратор Системы Клиента	172.16.112.52	Да	—
Вход	23.01.2024, 11:40	Администратор Системы Клиента	172.16.112.52	Нет	Неудачная попытка входа в систему
Вход	23.01.2024, 11:39	demo-family demo-name	192.168.50.200	Да	—
Выход	23.01.2024, 11:38	Администратор Системы Клиента	172.16.112.52	Да	—
Вход	23.01.2024, 11:37	Администратор Системы Клиента	172.16.112.52	Да	—
Выход	23.01.2024, 11:36	demo-family demo-name	192.168.50.200	Да	—
Выход	23.01.2024, 11:36	Администратор Системы Клиента	192.168.251.12	Да	—
Вход	23.01.2024, 11:36	Администратор Системы Клиента	192.168.251.12	Да	—
Вход	23.01.2024, 11:35	demo-family demo-name	192.168.50.200	Да	—

<< < 1 2 3 4 5 ... 13 > >>

Перейти на >

Контроль целостности

Контроль целостности

Контрольные суммы			по текущему клиенту	Снять контрольные суммы	✓ Проверить
Дата и время создания	Статус	Тип			
23.01.2024, 11:47	Успешно	Конфигурационные файлы			
23.01.2024, 11:46	Успешно	Справочники			
23.01.2024, 11:46	Неуспешно	Справочники			
23.01.2024, 11:45	Успешно	Справочники			
22.01.2024, 20:19	Успешно	Справочники			
22.01.2024, 20:19	Успешно	Справочники			
22.01.2024, 20:19	Неуспешно	Справочники			
22.01.2024, 20:18	Успешно	Справочники			
22.01.2024, 20:18	Успешно	Справочники			
22.01.2024, 20:18	Успешно	Справочники			
22.01.2024, 20:17	Неуспешно	Справочники			
22.01.2024, 20:10	Успешно	Конфигурационные файлы			
22.01.2024, 20:10	Успешно	Справочники			

Контрольные суммы			по текущему клиенту	Снять контрольные суммы	✓ Проверить
Дата и время создания	Статус	Тип			
22.01.2024, 20:10	Успешно	Конфигурационные файлы			
22.01.2024, 20:10	Успешно	Справочники			

Примеры ролевой модели (1)

Группа «Администратор»

Удалить Редактировать

Учетные записи Права доступа

Группа «Администратор»

Удалить Создать

Значение	Система / клиент	Утверждение	Кодовое название	
Блокировка/разблокировка пользователей		ROLE	role	⋮
Назначение прав (глобально)		ROLE	role	⋮
Управление глобальными утверждениями		ROLE	role	⋮
Управление глобальными группами		ROLE	role	⋮
Управление пользователями в глобальных группах		ROLE	role	⋮
Управление системами		ROLE	role	⋮
Управление пользователями		ROLE	role	⋮
Сброс паролей пользователям		ROLE	role	⋮
Просмотр глобальных групп		ROLE	role	⋮
Сброс паролей пользователям		ROLE		
Просмотр глобальных групп		ROLE		

Примеры ролевой модели (2)

Группа «Пользователь системы» Удалить Редактировать

Общее Учетные записи **Права доступа**

Удалить Создать

<input type="checkbox"/> Значение	Система / клиент	Утверждение	Кодовое название	
<input type="checkbox"/> Просмотр клиента	SecurityModule, SecurityModule.AdministrationAPI	ROLE	role	⋮
<input type="checkbox"/> Просмотр глобальных групп		ROLE	role	⋮
<input type="checkbox"/> Просмотр системных журналов		ROLE	role	⋮
<input type="checkbox"/> Просмотр пользователей		ROLE	role	⋮
<input type="checkbox"/> Просмотр системы	SecurityModule	ROLE	role	⋮

Контакты



Дмитрий Щербаков

Scherbakov.D@digdes.com

Санкт-Петербург

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

www.digdes.ru

info@digdes.com

**DIGITAL
DESIGN**

Москва

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

