GRUPP

123298, г. Москва,
ул. Народного Ополчения, д. 40
корп. 4, этаж 4, помещение 7

Тел/факс 8 (495) 455-05-
e-mail: inbox@v2grp.ru
v2grp.ru

АЛТАН

Автоматизированная Система Оперативного Управления Технологическими Процессами

Документация, содержащая сведения о технических требованиях и порядке установки ПО

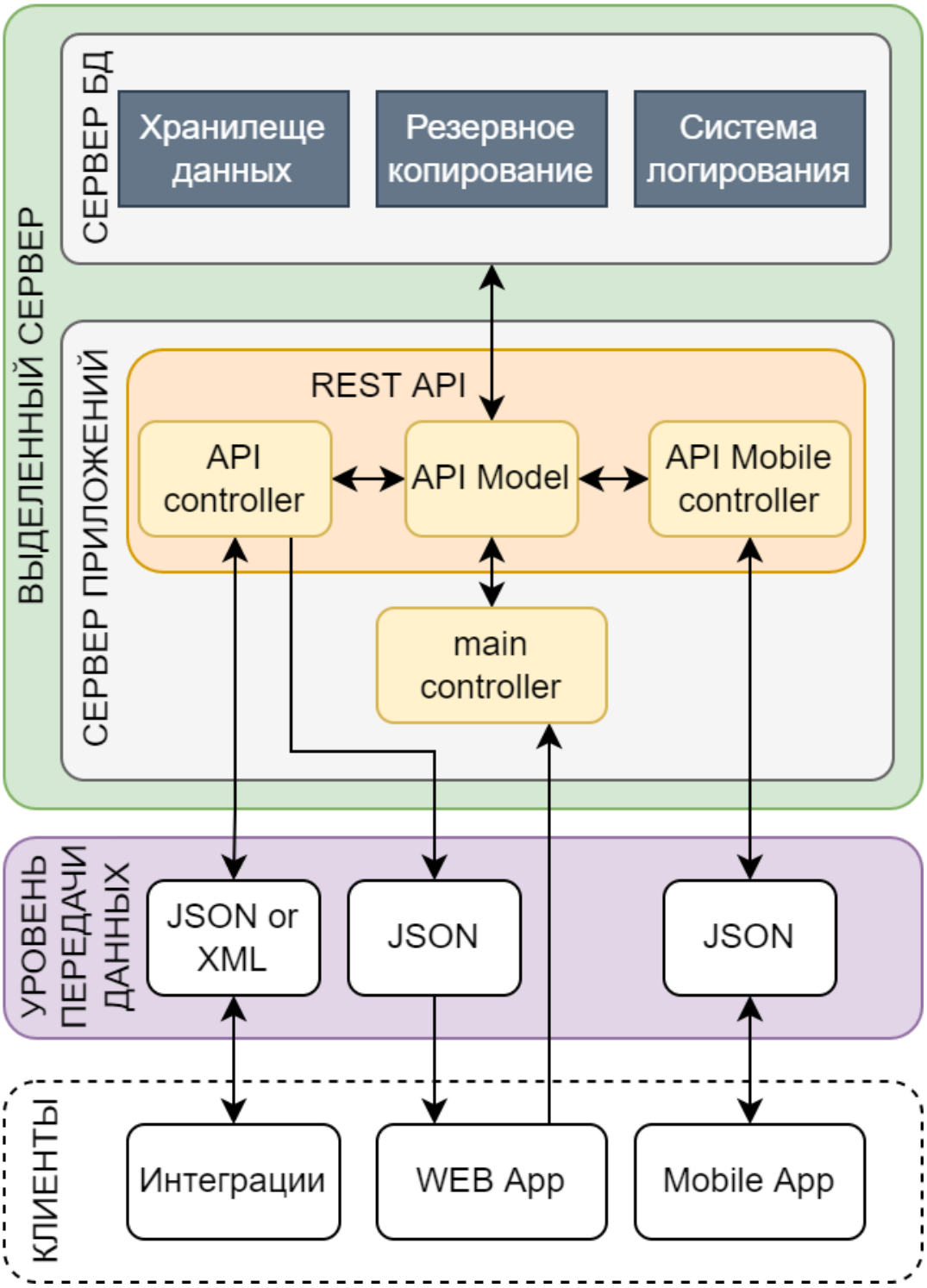
11.05.2024

123298, г. Москва,
ул. Народного Ополчения, д. 40
корп. 4, этаж 4, помещение 7

Тел/факс 8 (495) 455-05-
e-mail: inbox@v2grp.ru
v2grp.ru

Содержание:

1. Архитектура



2. Технологический стек

Технологический стек использует в себе инструменты, свободно распространяющиеся для коммерческого использования. Все технологии доказали свою применимость и надежность за время использования.

Программный комплекс может быть развернут на серверах под управлением операционных систем:

- Linux;
- Windows Server;
- Unix-подобные.

Технологии хранения поддерживают следующие базы данных:

- PostgreSQL;
- Oracle Database 18c Express Edition.

Серверная часть написана на языке программирования PHP и может быть развернута на следующих Web-серверах:

- Apache;
- Nginx.

Web-интерфейс использует в своей работе формы, написанные на:

- PHP;
- JS.

Мобильное приложение работает на операционной системе Android (API 21-30). Язык программирования Java SDK API Level 30.

3. Технические требования

3.1. Оборудование и требования к нему

Система размещается и функционирует на физических или виртуальных серверах предприятия.

Рекомендуемые основные характеристики сервера:

Тестовый контур	
Архитектура	x86
Процессор	Intel® Xeon® серии E3-1200 v5 (Skylake, 4 ядра, 8MB Smart cache, 8.0GT/s DMI) и выше или аналог
Оперативная память	Не менее 16 ГБ
Дисковая подсистема	500ГБ, RAID контроллер

Сеть	2 интегрированных сетевых адаптера 1 Гбит/с
Питание	Сервер должен быть обеспечен бесперебойным питанием со временем резервирования достаточным для нормального завершения работы физического сервера после выключения электропитания

Продуктивный контур	
Архитектура	x86
Процессор	Intel® Xeon® серии E3-1200 v5 (Skylake, 4 ядра, 8MB Smart cache, 8.0GT/s DMI) и выше или аналог
Оперативная память	Не менее 16 ГБ
Дисковая подсистема	500ГБ, RAID контроллер
Сеть	2 интегрированных сетевых адаптера 1 Гбит/с
Питание	Сервер должен быть обеспечен бесперебойным питанием со временем резервирования достаточным для нормального завершения работы физического сервера после выключения электропитания

Каждый пользователь Системы должен быть обеспечен АРМ для оперативного доступа к Системе.

Для установки, настройки, обновления ПО, установленного на сервера на время внедрения и технического обслуживания Системы, необходим постоянный удаленный доступ, посредством программных средств «Удаленный рабочий стол» или аналогов. Доступ в сеть предприятия предоставляется посредством технологии VPN.

Для работы необходимо:

- Две учетные записи пользователей для одновременного удаленного подключения к серверам;
- Доступ пользователей к тестовому и продуктовому серверу;
- При работе через «Удаленный рабочий стол» должна быть возможность передачи файлов со своего рабочего места на удаленный компьютер.

Точное количество пользователей, которых необходимо обеспечить персональными компьютерами, необходимо уточнить на этапе Обследования системы.

Требования к персональным компьютерам пользователей:

Архитектура	x86
Процессор	4х ядерный процессор с частотой 3100 МГц и выше
Оперативная память	не менее 4 Гб
Дисковая подсистема	не менее 100 Гб
Сеть	100/1000 Мбит/с (необходим стабильный канал связи к серверу базы данных, с постоянной пропускной способностью

	не менее 10 Мбит/с)
Монитор	диагональ не менее 19”+
Мышь, клавиатура	стандартные

АРМ должны быть обеспечены подключение к ЛВС предприятия со скоростью передачи данных не менее 10МБ/сек.

Окончательные требования формируются на этапе разработки технического проекта на внедрение.

Требования к мобильным устройствам должны быть не ниже:

Оперативная память	3 Гб
Встроенная Flash-память	16Гб
Камеры	Тыловая камера 5Мп Фронтальная камера 3Мп
Сеть	100/1000 Мбит/с (необходим стабильный канал связи к серверу базы данных, с постоянной пропускной способностью не менее 10 Мбит/с)
Питание	Съемный аккумулятор, не менее 3000мАч
Монитор	Не менее 4”
Мышь, клавиатура	Сенсорный экран
Операционная система	Android 5.0, API level 21

3.2. Дополнительное оборудование

Считыватель NFC ACR1252U

Интерфейс подключения	
Питание	Через USB
Скорость	12 Мб/с
Напряжение питания	5В
Потребляемое напряжение	До 200 мА
Бесконтактный интерфейс	

Стандарты	• ISO/IEC 18092 NFC • ISO 14443 Type A & B • MIFARE • FeliCa
Протоколы	ISO 14443 T=CL для ISO14443-4 совместимых карт
Частота	13.56 MHz
Дальность считывания	До 50 мм в зависимости от метки
Скорость чтения/записи	• 106 Kbps, • 212 Kbps • 424 Kbps
Интерфейс SAM карты	
Стандарт	ISO 7816
Протокол	T=0 и T=1
Физические характеристики	
Размер	Д x Ш x В: 98.0 x 65.0 x 12.8 мм
Вес	81 г
Материал	ABS
Цвет	Черный
Размер антенны	50 x 40 мм
Длинна кабеля	1 м.
Периферия	
Светодиод	2х-цветный
Бипер	Монотонный
Условия эксплуатации	
Температура	0 °C – 50 °C
Влажность	До 90%
API	
PC/SC	CT-API через PC/SC
Сертификаты/Соответствия	• ISO 18092

	• ISO 14443 • ISO 7816 • NFC Forum • LASCOM • CE • FCC • VCCI • MIC • KC • PC/SC • CCID • RoHS 2 • Felica Performance Certification • USB Full Speed Microsoft® WHQL for Windows® 2000 • Windows® XP • Windows Vista® • Windows® 7 • Windows® 8 • Windows® 8.1 • Windows® Server 2003 • Windows® Server 2008 • Windows® Server 2008 R2 • Windows® Server 2012 • Windows® Server 2012 R2
Поддерживаемые операционные системы	• Windows® 2000 • Windows® XP • Windows Vista® • Windows® 7 • Windows® 8 • Windows® 8.1 • Windows® Server 2003 • Windows® Server 2003 R2 • Windows® Server 2008 • Windows® Server 2008 R2 • Windows® Server 2012 • Windows® Server 2012 R2 • Linux® • Mac OS® • Android™ 3.1 and above

Смарт-карта Рутокен ЭЦП 3.0 NFC

Основные характеристики	
Аппаратная часть	Защищенный микроконтроллер со встроенной энергозависимой памятью
EEPROM память	128 Кбайт
Габаритные размеры	85,6 x 53,98 x 0,76 мм
Масса	5,5 г
Поддерживаемые ОС	• Microsoft Windows 10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008 • GNU/Linux (в том числе отечественные) • Apple macOS 10.15/10.14/10.13/10.12/10.11/10.10/10.9 • Android 5 и новее • iOS 13 и новее • Аврора
Поддерживаемые интерфейсы и стандарты	
PKCS#11 версии 2.20, включая российский профиль (2.30 draft)	Да
Microsoft Crypto API	Да
PC/SC	Да
Microsoft Smartcard API	Да
USB CCID (работа без установки драйверов)	Да
ISO/IEC 7816	• ISO/IEC 7816-3, протокол T=0 и T=1 для контактной микросхемы, • ISO 14443 (NFC) для бесконтактной микросхемы.
Криптопровайдер	собственный Crypto Service Provider
Сертификаты X.509 версии 3 на уровне программного обеспечения	Да

Криптографические возможности	
Поддержка алгоритма ГОСТ 28147-89	Да, аппаратная реализация
Поддержка алгоритма ГОСТ Р 34.12-2015 (Магма)	Да, аппаратная реализация
Поддержка алгоритма ГОСТ Р 34.12-2015 (Кузнечик)	Да, аппаратная реализация
Режим шифрования	• простая замена, • гаммирование, • гаммирование с обратной связью
Режим выработки имитовставки	Да
Генерация ключей шифрования	Да
Импорт ключей шифрования	Нет
Запрет экспорта ключей шифрования	Да
Поддержка алгоритма ГОСТ Р 34.10-2012	Да, аппаратная реализация
Формирование и проверка ЭП	Да
Генерация ключевых пар	Да, с проверкой качества
Импорт ключевых пар	Да, с проверкой эмитента
Запрет экспорта ключевых пар	Да
Срок действия закрытых ключей	До 3 лет
Размер закрытого ключа	256 и 512 бит
Поддержка алгоритма ГОСТ 34.11-2012 (256 и	Аппаратная реализация

512 бит)	
Вычисление значения хэш-функции	Да, в т. ч. с возможностью последующего формирования ЭП
Формирование и проверка ЭП	Да
Генерация ключевых пар	Да, с проверкой качества
Импорт ключевых пар	Да
Запрет экспорта ключевых пар	Да
Срок действия закрытых ключей	До 3 лет
Поддержка алгоритма ГОСТ 34.11-94	Аппаратная реализация
Выработка сессионных ключей (ключей парной связи)	**Да** • **по схеме VKO GOST R 34.10-2001 согласно RFC 4357** • **по схеме VKO GOST R 34.10-2012 согласно RFC 7836**
Расширение по схеме EC El-Gamal	Да
Поддержка алгоритма RSA	Аппаратная реализация расшифрования и подписи (RSA-1024, RSA-2048, **RSA-4096**)
Формирование электронной подписи	Да
Генерация ключевых пар	Да, с проверкой качества
Импорт ключевых пар	Да
Запрет экспорта ключевых пар	Да
Размер ключей	**до 4096 бит**
Поддержка алгоритма ECDSA	**Да, кривые secp256k1 и secp256r1**

Поддержка алгоритмов DES (3DES), AES, RC2, RC4, MD4, MD5, SHA-1, SHA-256	Хранение экспортируемых ключей в EF, SHA-1, SHA-256, MD5 в PKCS#11, RC4, MD4, MD5, SHA-1, SHA-256, 3DES, AES в minidriver
Формирование электронной подписи	Да
Генерация ключевых пар	Да, с проверкой качества
Импорт ключевых пар	Да
Работа с СКЗИ «КриптоПро 5.0» по протоколу защиты канала SESPAKE (ФКН2).	**Да**
Сведения о сертификате	
Наличие сертификата ФСТЭК	В процессе
Наличие сертификата ФСБ	В процессе
Файловая система	
Файловая структура	Встроенная, по стандарту ISO/IEC 7816-4
Тип размещения файловых объектов в памяти (архитектура файловой системы)	Использование File Allocation Table (FAT)
Количество папок и уровень их вложенности	Уровень ограничен объемом свободной памяти
Число файловых объектов внутри папки	до 255 включительно
Хранение ключевой информации	• использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов; • использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов

Запрет экспорта закрытых и симметричных ключей	Да
Шифрование файловой системы	Да, прозрачное, алгоритм ГОСТ 28147-89, уникальный ключ шифрования для каждого экземпляра устройства
Дополнительно	Использование Security Environment для удобной настройки параметров криптографических операций
Аутентификация и конфиденциальность	
Двухфакторная аутентификация	Да, предъявление токена + ввод PIN-кода
Уровни доступа	• Гость • Пользователь • Администратор
Разграничение доступа к файловым объектам в соответствии с уровнем доступа	Да
Ограничение числа попыток ввода PIN-кода	Да, настраиваемое
Поддержка PIN-кодов	• глобальные PIN-коды: Администратора и Пользователя, • локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов) • **Настраиваемые аппаратные политики качества PIN-кодов**
Ограничение минимального размера PIN-кода	Да, настраивается независимо для любого PIN-кода
Дополнительно	• поддержка комбинированной аутентификации: • аутентификация по глобальным PIN-кодам • аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам. • возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами. • индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные.

Возможность встраивания радиочастотной метки	Да
Поддерживаемые типы меток	Работа с системами контроля и управления доступом, поддерживающими протокол NFC
Встроенный контроль и индикация	
Контроль целостности прошивки	Да
Контроль целостности системных областей памяти	Да
Проверка целостности RSF-файлов перед использованием	Да
Типы счетчиков	• счетчик изменений файловой системы • счетчик изменений PIN-кодов • счетчики последовательных неудачных попыток ввода PIN-кодов
Проверка правильности функционирования криптографических алгоритмов	Да
Режимы работы светодиодного индикатора	• готовность к работе • выполнение операции • нарушение в системной области памяти

4. Порядок установки

С целью упрощения установки решения АЛТАН на серверах заказчика рекомендуется использовать Docker Engine (специализированное программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации данных).

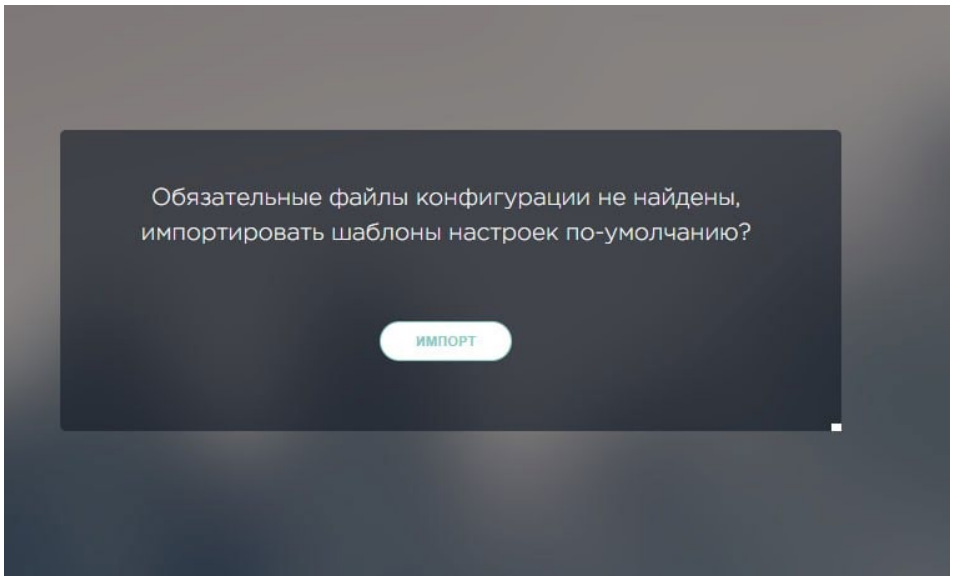
- Для того, чтобы установить Docker Engine, необходимо пройти по ссылке - https://docs.docker.com/engine/install/ ;
- Далее необходимо скачать установочный файл в одной из доступных на сайте конфигурации и произвести установку Docker Engine в операционную систему;
- После завершения установки Docker Engine нужно выбрать каталог в операционной системе и создать файл docker-compose.yml со следующим содержимым:

```
services:
    altan-web:
        image: altan-registry.v2grp.ru/altan:latest
        container name: altan-web
        ports:
            - 3000:80
        restart: always
```

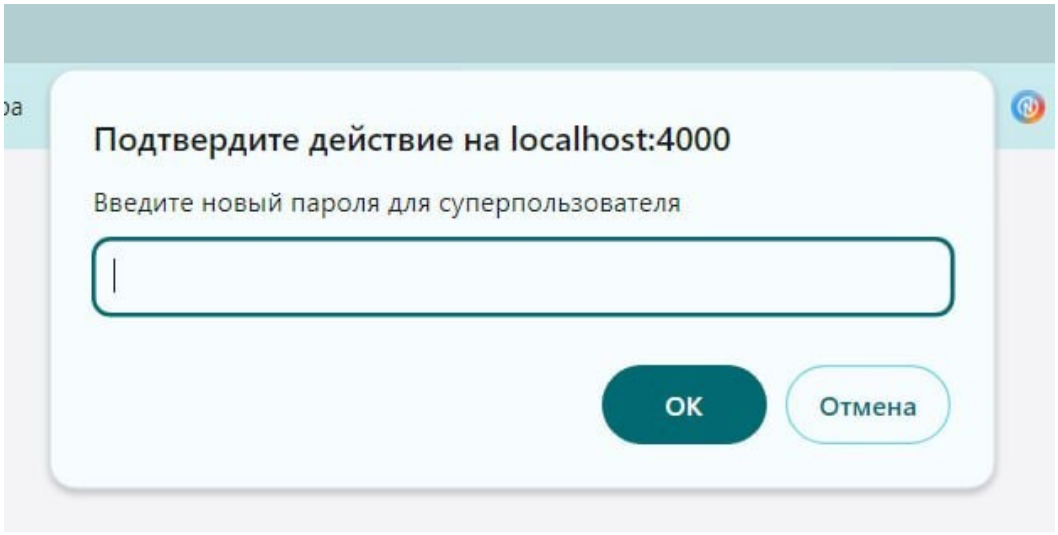
- В выбранном ранее каталоге выполняется команда: «docker login ***"(ссылка на репозиторий)"--*** username ***"(логин)"*** --password ***"(пароль)"*** && docker compose up» *
- После выполнения описанных выше шагов работа с решением АЛТАН будет доступна через web-браузер, заранее установленный в операционной системы (к примеру, Google Chrome);
- Далее выполняется первичная установка**:
  - импортируются шаблоны настроек конфигурации по умолчанию;

* Ссылка на docker-контейнер, а также все необходимые для запуска реквизиты предоставляются заказчику при заключении договора

**Настройка производится под запрос конкретного заказчика



- Устанавливается новый пароль суперпользователя;



- Для того, чтобы начать работу с решением АЛТАН необходимо ввести в адресную строку браузера ссылку http://localhost:3000 и нажать на кнопку перехода к web-ресурсу.