

CF Med

«Медданные Муковисцидоз»

Инструкция по установке и доступу к проверочному экземпляру

Правообладатель: Благотворительный фонд «Острова»

Техническое сопровождение: ООО «Оккервиль Лаб»

Версия документа: 1.5 | 1 октября 2026 г.

Документ подготовлен во исполнение подпункта «д» пункта 11 Правил, утверждённых постановлением Правительства РФ от 16.11.2015 № 1236.

Санкт-Петербург • 2026

1 Назначение документа

Настоящая инструкция содержит сведения, необходимые для доступа к проверочному экземпляру CF Med «Медданные Муковисцидоз», его технического осмотра, запуска и проверки. Она описывает зафиксированный UAT-экземпляр, регистрацию эксперта, пользовательские роли, размещение компонентов, миграции и состав данных, доступных для проверки.

Проверочный экземпляр уже развёрнут в отдельной UAT-среде Yandex Cloud и доступен через веб-приложение. Пользовательские функции проверяются после самостоятельной регистрации эксперта. Изолированная схема VPN/SSH подготовлена для проверки серверной части, контейнера CFMed.Api и тестовой базы данных; персональные реквизиты выдаются назначенному эксперту после письменного запроса проверяющей стороны.

VPN-профили, закрытые SSH-ключи, пароли и иные индивидуальные инфраструктурные реквизиты в документ не включаются. После назначения эксперта для него создаются отдельные временные реквизиты с ограниченным сроком и областью действия. Доступ к веб-консоли и IAM подаккаунта Yandex Cloud не требуется. Производственная среда и рабочая медицинская база в проверку не входят.

CF Med является централизованно развёрнутым веб-приложением. Для работы с пользовательскими функциями установка клиентских компонентов на рабочее место не требуется: используется веб-браузер. Серверная инфраструктура и база данных UAT уже развёрнуты; эксперт получает удалённый доступ по процедуре раздела 5.

2 Сведения и материалы для проверки

Материал	Содержание	Порядок передачи
Настоящая инструкция	Описание UAT-экземпляра, входа в приложение, компонентов, выпуска и проверки	В составе технических документов
Приложение по инфраструктурному доступу	Адреса, порты, индивидуальный VPN-профиль, SSH-имя, fingerprints, полномочия и срок действия доступа	Схема и шаги приведены в разделе 5; индивидуальные реквизиты передаются назначенному эксперту непублично после запроса
Регистрация в приложении	Эксперт регистрирует собственный адрес электронной почты; заявка одобряется действующим заведующим	Порядок описан в разделе 5
Паспорт контрольной сборки	Номер версии, дата фиксации, Docker tag, frontend commit и имена файлов клиентской сборки	Сведения приведены в разделе 3 и приложении А
Документ 04 «Руководство пользователя»	Перечень заявленных пользовательских функций CF Med	В составе регистрационного комплекта

3 Паспорт проверочного экземпляра

Параметр	Сведения
Наименование	CF Med «Медданные Муковисцидоз»
Правообладатель	Благотворительный фонд «Острова»
Техническое сопровождение	ООО «Оккервиль Лаб»
Форма предоставления	Удалённый доступ к предварительно развёрнутому UAT-экземпляру
Облачная платформа	Yandex Cloud, Российская Федерация
UAT folder ID	b1g5kjujc7dde4be5b13
Зона размещения вычислительных ресурсов	ru-central1-d
Номер проверочной версии	1.024
Дата фиксации экземпляра	11 сентября 2026 г.
Адрес веб-приложения	https://cf-med-app.website.yandexcloud.net/
Период доступности	Без заранее установленной даты окончания

3.1 Идентификация программной сборки

Номер 1.024 относится к проверочному экземпляру в целом. Серверная и клиентская части дополнительно идентифицируются собственными техническими признаками. Для CFMed.Api это тег контейнерного образа, а для CF-Med-App — commit исходного кода и имена хэшированных файлов статической сборки.

Компонент	Исходный код	Развёрнутый результат	Статус
CFMed.Api	SourceCraft: for-subaccount-fond-ostrova/cfmed-backend; ветка master	cr.yandex/crpfj42mbghnrlpqphjev/cf-med-api:1.087-uat	Развёрнутый образ UAT
CF-Med-App	SourceCraft: for-subaccount-fond-ostrova/cfmed-app; ветка main; commit 3ac64facd7739d24041f689ecb750c9f4f90a68e	Бакет cf-med-app; index.html и хэшированные JS/CSS bundles	Зафиксировано 11.09.2026

Компонент	Исходный код	Развёрнутый результат	Статус
Схема БД	Миграции Entity Framework Core в backend-репозитории	PostgreSQL на cf-med-test-db-vm; история в __EFMigrationsHistory	Тестовая база UAT

Отдельный build ID для текущей статической сборки CF-Med-App не генерируется. Её идентификатором служит совокупность commit 3ac64facd7739d24041f689ecb750c9f4f90a68e, даты фиксации и хэшированных имён файлов main-2D3VG247.js, polyfills-25SJB14S.js, scripts-PPDPQHDA.js и styles-F7TRY3BU.css. При следующей сборке хэши файлов изменятся.

3.2 Подтверждение полноты функций

Проверочный экземпляр версии 1.024, зафиксированный 11 сентября 2026 г., предназначен для проверки функций CF Med «Медданные Муковисцидоз», описанных в документе 04 «Руководство пользователя». Пользовательские сценарии доступны через веб-приложение, а техническая проверка серверных компонентов проводится через VPN и SSH с полными административными правами внутри изолированного UAT.

4 Архитектура и размещение компонентов

UAT-экземпляр состоит из статического клиентского приложения, серверного Web API, базы данных PostgreSQL и почтового сервиса. Пользовательский браузер получает клиентские файлы из Object Storage, после чего приложение обращается к CFMed.Api. Серверная часть работает с тестовой базой данных и отправляет служебные сообщения через Yandex Cloud Postbox. Адрес CFMed.Api, используемый проверочной клиентской сборкой: <https://cf-med-app.okkervil-lab-projects.ru/api>.

Компонент	Назначение	Фактическое размещение UAT	Доступ
CF-Med-App	Веб-интерфейс Angular	Yandex Object Storage, бакет cf-med-app; статические файлы	По адресу UAT через HTTPS
CFMed.Api	Серверная бизнес-логика и Web API на Kestrel	VM cf-med-test-vm2, 192.168.0.16; Docker-контейнер cf-med-api-server; порт 8080	Из UAT-сети; временный инфраструктурный доступ после запроса
PostgreSQL	Тестовая база данных приложения	VM cf-med-test-db-vm, 192.168.0.13; внутренний FQDN cf-med-test-db-vm.ru-central1.internal	Только через частную UAT-сеть; реквизиты после отдельного запроса
Container Registry	Хранение Docker-образов API	Registry cf-med-registry, ID crpj42mbghnrpqqhjev; автоматическое сканирование включено	Служебная учётная запись выпуска; экспертам не передаётся

Компонент	Назначение	Фактическое размещение UAT	Доступ
Postbox	Письма об одобрении и одноразовые коды	Yandex Cloud Postbox; верифицированный домен cf-med.ru	Через приложение
Исходный код	Проверка состава и происхождения сборки	Закрытые Git-репозитории Yandex SourceCraft	По отдельному согласованию без выдачи доступа к облачному аккаунту
VPN-шлюз	Защищённый вход во внутреннюю UAT-сеть	VM cf-med-test-vpn-vm; публичный адрес 130.193.56.188; внутренний адрес 192.168.0.14	OpenVPN; индивидуальная учётная запись и профиль передаются назначенному эксперту

Базовая ОС виртуальной машины CFMed.Api — Ubuntu 22.04 LTS. Серверная часть CFMed.Api использует Kestrel внутри Docker-контейнера. PostgreSQL имеет версию 16.

4.1 Ресурсы UAT

Ресурс	Состояние	Параметры	Назначение
cf-med-test-vm2	Running	2 vCPU, 2 ГБ RAM, 20 ГБ; 192.168.0.16	CFMed.Api
cf-med-test-vpn-vm	Running	2 vCPU, 2 ГБ RAM, 20 ГБ; публичный 130.193.56.188; внутренний 192.168.0.14	OpenVPN-шлюз изолированного UAT; индивидуальные реквизиты после запроса
cf-med-test-db-vm	Running	2 vCPU, 2 ГБ RAM, 20 ГБ; 192.168.0.13	PostgreSQL и тестовая база UAT
cf-med-app	Доступен	Object Storage; 11 объектов; 3,27 МБ	Статические файлы CF-Med-App
cf-med-registry	Active	ID crpj42mbghnrlpqphjev; 3,92 ГБ	Образы CFMed.Api

VM cf-med-test-db-vm предназначена для размещения тестовой базы данных UAT. Она не имеет публичного адреса; параметры подключения и отдельная временная учётная запись PostgreSQL сообщаются только при согласовании прямой проверки базы данных.

4.2 Размещение клиентских файлов

На дату подготовки документа в бакете cf-med-app присутствует UAT-снимок клиентской части. Объекты, позволяющие идентифицировать сборку, приведены ниже.

Путь или объект	Размер	Назначение
index.html	27,82 КБ	Точка входа веб-приложения
main-2D3VG247.js	2,88 МБ	Основной bundle приложения
polyfills-25SJB14S.js	33,74 КБ	Совместимость среды браузера
scripts-PPDPQHDA.js	78,78 КБ	Дополнительные скрипты
styles-F7TRY3BU.css	235,02 КБ	Стили приложения
favicon.ico	948 Б	Значок приложения
assets/images/charity-logo.jpeg	11,82 КБ	Логотип правообладателя
assets/ru-cities.json	9,45 КБ	Справочные данные городов

Публичный доступ к бакету относится только к статическим клиентским файлам. Пароли, строки подключения к БД, токены и медицинские данные не должны включаться в клиентскую сборку или объекты бакета.

4.3 Отделение от продуктивной среды

Признак	UAT для проверки	PROD
Cloud folder	b1g5kjujc7dde4be5b13	b1gvu2mf5sav0t9164i0
API VM	cf-med-test-vm2	cf-med-api-vm
Registry ID	crpj42mbghnrlpqphjev	crp8dk19umjch9vmide5
Клиентская часть	Object Storage cf-med-app	VM cf-med-app-vm-2b; отдельный production-контур
База данных	CFCard, частный UAT endpoint	Кластер cf-med-postgresql; БД cf-med-db
Учётные данные БД	Отдельные UAT-реквизиты	Отдельные PROD-реквизиты
Доступ эксперта	Только UAT	Не предоставляется

Проверка не требует и не предусматривает подключение к продуктивной медицинской базе. Маршруты, учётные записи и секреты UAT не используются для доступа к PROD.

В продуктивной среде CF-Med-App размещается в Docker-контейнере с Nginx на VM под Ubuntu 22.04 LTS, а входящие HTTP/HTTPS-запросы маршрутизируются через Yandex Application Load Balancer. Эти сведения описывают PROD и не заменяют схему UAT: клиентские файлы проверочного экземпляра выдаются напрямую из Object Storage по адресу, указанному в разделе 3.

5 Регистрация эксперта и предоставление доступа

Проверочная учётная запись заранее не создаётся и не привязывается к почтовому ящику, недоступному эксперту. Эксперт самостоятельно регистрируется в UAT на адрес электронной почты, к которому имеет доступ. Это позволяет ему получить письмо о подтверждении и OTP без участия технического специалиста.

5.1 Регистрация и назначение ролей

Этап	Что происходит
Регистрация	Эксперт открывает https://cf-med-app.website.yandexcloud.net/ , регистрирует нового врача на собственный адрес электронной почты и выбирает одну из тестовых организаций: «СПБ ГБУЗ ГМПБ №2» или «СПБ ГБУЗ ДГБ Святой Ольги».
Уведомление	Система направляет уведомление действующему пользователю с ролью заведующего о новой заявке врача.
Одобрение	Нестерук Александр Александрович получает заявку, входит в «Панель заведующего», открывает «Врачи и пациенты» и одобряет регистрацию эксперта.
Роль врача	После одобрения эксперт получает доступ к пользовательским функциям врача.
Роль заведующего	После проверки роли врача той же учётной записи предоставляются права заведующего. Для отдельной проверки операции принятия заявки эксперт может зарегистрировать вторую учётную запись на другой доступный ему адрес электронной почты.

5.2 Подтверждение входа и OTP

После одобрения регистрации эксперт получает письмо со ссылкой для входа. При входе приложение направляет одноразовый код на тот же адрес электронной почты через Yandex Cloud Postbox. Код вводится на экране подтверждения. Флажок доверенного устройства позволяет не запрашивать повторный OTP на этом устройстве в течение семи дней. Если письмо задерживается, доступна повторная отправка; также проверяются папки «Спам» и «Рассылки».

Пароль эксперт задаёт при регистрации и не передаёт правообладателю. OTP также остаётся в распоряжении эксперта. Такой порядок исключает необходимость передавать заранее созданную учётную запись или доступ к чужому почтовому ящику.

5.3 Запрос доступа к VPN SSH и базе данных

Веб-регистрация не открывает инфраструктурный доступ. Схема защищённого входа в UAT через OpenVPN и SSH подготовлена отдельно от пользовательской регистрации. Письменный запрос проверяющей стороны определяет конкретного эксперта и срок доступа; после него создаются индивидуальные учётные данные. Назначенному эксперту предоставляются полные административные права к серверной части проверочного экземпляра в изолированном UAT.

VPN-шлюз cf-med-test-vpn-vm доступен по публичному адресу 130.193.56.188; сервер CFMed.Api и сервер тестовой PostgreSQL имеют только внутренние адреса 192.168.0.16 и

192.168.0.13. Для назначенного эксперта создаётся отдельная учётная запись OpenVPN. Индивидуальный профиль, пароль, имя SSH-пользователя и fingerprints серверов передаются адресно вне публичной документации.

Основной способ SSH-доступа — локальная учётная запись ОС и открытый ключ эксперта. Закрытый ключ остаётся у эксперта. Полные административные права root на серверных VM проверочного экземпляра предоставляются назначенному эксперту через sudo внутри изолированного UAT; прямой вход под именем root не используется. Доступ к веб-консоли Yandex Cloud, IAM-политикам и облачному подаккаунту не предоставляется. До выдачи доступа на стенде проверяется отсутствие рабочих ключей, production-конфигураций, исходных дампов и резервных копий производственной базы.

Отсутствие заранее созданных персональных учётных записей не означает неготовность схемы доступа: VPN-шлюз, маршруты, внутренние адреса VM и порядок назначения полномочий подготовлены. Индивидуальные реквизиты создаются только после получения официального запроса и сведений о назначенном эксперте.

5.4 Порядок подключения по VPN и SSH

Подключение к UAT через VPN, вход по SSH на обе серверные VM и получение полных административных прав через sudo уже фактически проверялись ООО «Оккервиль Лаб» при работе со стендом и функционируют. Проверка выполнялась с действующими учётными записями технических специалистов, а не с отдельной временной учётной записью эксперта. Для назначенного эксперта создаётся отдельная временная локальная учётная запись, его открытый SSH-ключ добавляется на обе VM, а пользователю предоставляются права через sudo. Перед передачей реквизитов выполняется краткая контрольная проверка входа.

1. Эксперт передаёт ответственному специалисту ФИО, рабочий адрес электронной почты, требуемый срок доступа и свой открытый SSH-ключ формата Ed25519 или RSA. Закрытый ключ не передаётся.
2. ООО «Оккервиль Лаб» создаёт отдельного пользователя OpenVPN и локальную учётную запись ОС на серверных VM UAT, устанавливает открытый ключ, предоставляет полные административные права через sudo и ограничивает срок действия доступа.
3. По раздельным каналам эксперту передаются адрес клиентского интерфейса <https://130.193.56.188/>, логин, временный пароль или индивидуальный профиль .ovrp, имя SSH-пользователя и fingerprints ключей серверов.
4. Эксперт импортирует профиль в OpenVPN Connect, устанавливает VPN-соединение и проверяет доступность внутренних адресов 192.168.0.16 и 192.168.0.13.
5. Для входа на сервер CFMed.Api используется команда: `ssh -i <путь_к_закрытому_ключу> <ssh_пользователь>@192.168.0.16`.
6. Для входа на сервер тестовой базы используется команда: `ssh -i <путь_к_закрытому_ключу> <ssh_пользователь>@192.168.0.13`.
7. При первом входе эксперт сверяет fingerprint со значением, переданным ответственным специалистом. Полные административные полномочия проверяются командой `sudo -l`. Для административной оболочки внутри UAT используется `sudo -i`.
8. По завершении проверки VPN-пользователь и локальные SSH-учётные записи блокируются или удаляются, а ключи отзываются.

Для OpenVPN Access Server применяются TCP 443, UDP 1194 и TCP 943 (Client Web UI/Admin Web UI); фактически открытый набор портов определяется конфигурацией шлюза. SSH-порт 22 серверных VM доступен только из VPN-сети и не публикуется в интернете.

5.5 Альтернативный доступ по сертификату OS Login

Yandex Cloud поддерживает короткоживущие SSH-сертификаты OS Login. Такой вариант требует включения эксперта в Yandex Identity Hub и назначения облачных ролей, поэтому для данной проверки он не является основным. Если проверяющая сторона отдельно выбирает OS Login, сертификат экспортируется командой ниже и действует один час; для административного входа требуются роли `compute.osAdminLogin` и `resource-manager.auditor`, а для подключения через Yandex Cloud CLI дополнительно требуется `compute.operator`.

```
yc compute ssh certificate export --login <os_login> --organization-id <organization_id> -  
-directory <локальный_каталог>
```

После подключения к VPN вход по экспортированному сертификату выполняется стандартным SSH-клиентом на внутренний адрес UAT. Выбор OS Login согласуется отдельно, поскольку он затрагивает учётные сущности Yandex Cloud; по умолчанию применяется локальная SSH-учётная запись без выдачи облачных IAM-прав.

Официальные источники Yandex Cloud:

- Соединение с облачной сетью при помощи OpenVPN — <https://yandex.cloud/ru/docs/tutorials/routing/openvpn>
- Подключение к виртуальной машине по OS Login — <https://yandex.cloud/ru/docs/compute/operations/vm-connect/os-login>
- Экспорт SSH-сертификата — <https://yandex.cloud/ru/docs/compute/operations/vm-connect/os-login-export-certificate>
- Подключение к Linux VM по SSH — <https://yandex.cloud/ru/docs/compute/operations/vm-connect/ssh>

6 Функции, доступные для проверки

Проверочный экземпляр предоставляет заявленные пользовательские функции. В таблице приведены основные сценарии. Подробное описание интерфейса и операций, включая панель заведующего и статистику учреждения со скриншотами, содержится в документе 04 «Руководство пользователя».

Роль	Функциональная область	Доступный сценарий
Врач	Список пациентов и фильтры	Поиск пациента и переход в карточку
Врач	Карточка пациента	Просмотр общих и медицинских данных тестового пациента
Врач	Медицинские заметки	Создание, изменение и удаление тестовой заметки
Врач	Обследования и показатели	Ввод физического, лабораторного и микробиологического показателя
Врач	Лечение и терапия	Создание тестовой записи и просмотр сводки
Врач	Статистические графики	Просмотр графиков антропометрии, функции лёгких и терапии

Роль	Функциональная область	Доступный сценарий
Врач	Семья	Добавление тестового родственника и приоритетного контакта
Врач	Обеспечение	Просмотр оборудования, материалов и льготного обеспечения
Врач	Отчёты и документы	Формирование DOCX-отчёта и загрузка тестового документа
Врач	Новый пациент	Создание тестовой карточки и тестового согласия
Заведующий	Врачи и пациенты	Одобрение врача и переназначение тестового пациента
Заведующий	Отчёты учреждения	Формирование отчётов по тестовым данным
Заведующий	Справочники	Просмотр препаратов, антибиотиков, ферментов и микроорганизмов
Заведующий	Каталог оборудования	Просмотр и изменение тестовой позиции
Заведующий	Статистика учреждения	Просмотр агрегированных графиков и показателей
Обе роли	Сообщение о проблеме	Отправка тестового обращения без персональных данных

Расчёты и отчёты в CF Med имеют информационно-справочный и организационно-учётный характер. Программа не выполняет автономную постановку диагноза, назначение лечения или принятие клинических решений.

7 Файлы программного обеспечения и конфигурация

7.1 CFMed.Api

Объект	Расположение	Комментарий
Решение	CFMed.sln	Точка сборки backend
Web API	CFMed.Api/	Контроллеры, точка запуска и Dockerfile
Dockerfile	CFMed.Api/Dockerfile	Сборка контейнера CFMed.Api
Прикладная логика	CFMed.Application/	Сценарии и сервисы приложения
Доменная модель	CFMed.Card.Domain/	Сущности и предметная модель
Доступ к данным	CFMed.Card.Infrastructure/	Entity Framework Core и репозитории
Тесты	CFMed.Application.Tests/	Unit-тесты прикладной логики

Объект	Расположение	Комментарий
Развёрнутый контейнер	cf-med-api-server на cf-med-test-vm2	Порт 8080; restart policy always
Секретная конфигурация	/data/secrets.json → /yc-user/data/secrets.json	Содержимое не включается в документ

Исходный код не обязан присутствовать на UAT VM: исполняемые файлы находятся в слоях Docker-образа. После выдачи персональных реквизитов инфраструктурного доступа эксперт может проверить образ, работающий контейнер, журналы и файлы внутри контейнера с административными правами в UAT. Содержимое secrets.json, токены и иные секреты в отчёт не копируются.

7.2 CF-Med-App

Исходный код клиентской части хранится в закрытом репозитории SourceCraft cfmed-app. Развёрнутый UAT-результат представляет собой статические файлы Angular-приложения в бакете cf-med-app. На VM CFMed.Api клиентские файлы не размещаются.

7.3 Конфигурация контейнера UAT

```
services:
  cf-mad-api:
    container_name: cf-med-api-server
    image: cr.yandex/crpj42mbghnrlpqphjev/cf-med-api:1.087-uat
    restart: always
    ports:
      - 8080:8080
    environment:
      - PORT=8080
      - Logging__YandexCloudLogger__ResourceType=cf-med-api-3
    volumes:
      - /data/secrets.json:/yc-user/data/secrets.json
```

В зафиксированном UAT-экземпляре используется образ с тегом 1.087-uat. При необходимости digest образа можно получить из работающего контейнера во время инфраструктурной проверки.

8 Сборка и выпуск проверочного экземпляра

Исходный код CFMed.Api и CF-Med-App хранится в закрытых репозиториях Yandex SourceCraft. Автоматизированный выпуск ещё настраивается. До завершения его приёмки применяется ручной выпуск с фиксацией версии и исходного commit, сборкой, размещением результата в соответствующем контуре и проверкой работоспособности.

Для UAT серверный образ публикуется в cr.yandex/crpj42mbghnrlpqphjev/cf-med-api и применяется к VM cf-med-test-vm2. Статическая сборка CF-Med-App загружается в бакет cf-med-app. В проверочном экземпляре используется образ CFMed.Api с тегом 1.087-uat; клиентская сборка идентифицируется commit и перечнем файлов из разделов 3.1 и 4.2.

Сведения о репозиториях, средствах и командах сборки приведены в документе 02 «Хранение исходного кода и компиляция». Порядок выпуска, активации и распространения приведён в документе 03 «Активация выпуск и распространение». Проверка запуска компонентов описана в разделе 9 настоящей инструкции.

9 Запуск перезапуск и проверка работоспособности

9.1 CFMed.Api

Команды ниже выполняет технический специалист либо эксперт после выдачи временного инфраструктурного доступа. До получения официального запроса SSH-реквизиты не создаются.

```
docker ps --filter name=cf-med-api-server
docker inspect cf-med-api-server
docker logs --tail 200 cf-med-api-server
docker restart cf-med-api-server
docker ps --filter name=cf-med-api-server
curl -I http://127.0.0.1:8080/
```

Ответ 404 на корневой путь API сам по себе не означает неработоспособность, если TCP-соединение установлено и маршруты приложения отвечают штатно. Специальный health endpoint в настоящем документе не предполагается, пока его адрес не подтверждён в контрольной сборке.

9.2 CF-Med-App

Клиентская часть является набором статических объектов и не имеет отдельного процесса на VM. При проверке браузер получает index.html и указанные в нём JS/CSS bundles. Отсутствие ошибок 404 и совпадение хэшированных имён файлов с перечнем в разделе 4.2 подтверждают загрузку зафиксированной клиентской сборки.

9.3 PostgreSQL и сквозная проверка

Область	Возможная проверка
PostgreSQL	Соединение с cf-med-test-db-vm из частной UAT-сети, запрос SELECT 1 и просмотр истории миграций
Вход	Регистрация эксперта, одобрение заявки, получение OTP и вход с назначенной ролью
Пользовательские функции	Открытие тестовой карточки, создание и удаление тестовой записи, формирование DOCX-отчёта
Администрирование	Панель заведующего, одобрение врача и назначение административной роли
Результат	Дата проверки, версия экземпляра, выявленные ограничения и технические замечания

10 Миграции базы данных

Эксперт не применяет миграции к уже развёрнутому проверочному экземпляру. Схема базы данных подготавливается ответственным техническим специалистом при выпуске CFMed.Api. История применённых миграций хранится в таблице __EFMigrationsHistory.

```
dotnet ef migrations list
dotnet ef database update
```

Эти команды относятся к техническому обслуживанию стенда и выполняются из backend-репозитория с конфигурацией UAT. Перед применением миграций технический специалист

сверяет целевую базу и наличие точки восстановления. Строка подключения production в операциях UAT не используется.

11 Обезличивание и синтезирование данных UAT

11.1 Источник и состав данных

В UAT используется изолированная копия структурированных клинических записей. После восстановления к ней применяется отдельный сценарий PostgreSQL, который заменяет прямые идентификаторы, контактные сведения и свободный текст синтетическими значениями, а вложенные документы удаляет. UAT не подключается к production-базе и не содержит её реквизитов доступа.

Для проверки расчётов, графиков, обследований и терапии сохраняются структурированные клинические значения: диагнозы, показатели и даты обследований, записи и даты терапии, препараты, дозировки, операции и связи между медицинскими сущностями. Эти значения не синтезируются. Поэтому UAT остаётся закрытым проверочным контуром, а доступ к нему ограничивается даже после замены идентифицирующих полей.

11.2 Преобразование данных пациента и родственников

Категория	Преобразование в UAT
ФИО пациента	Фамилия, имя и отчество полностью заменяются синтетическим ФИО с учётом значения пола. Исходные части ФИО не сохраняются в отображаемых полях UAT.
Даты рождения	Дата рождения пациента смещается на случайное число дней. Даты рождения и смерти родственников также смещаются. После преобразования проверяются хронологическая непротиворечивость и возрастные расчёты.
Идентификаторы и контакты	MID, номер записи, город, адрес, индекс, телефон, паспорт, СНИЛС, email, страховой полис, свидетельство о рождении, национальность и поликлиника заменяются синтетическими тестовыми значениями.
Технические ключи	UUID первичных и внешних ключей сохраняются для целостности связей. Отдельная таблица соответствия не создаётся; доступ к исходной базе для сопоставления не предоставляется.
Родственники	ФИО полностью заменяется синтетическим; телефон, email, национальность и генетические комментарии заменяются тестовыми значениями. Даты рождения и смерти смещаются. Тип родства, пол и признак приоритетного контакта сохраняются.
Комментарии	Свободный текст медицинской карты заменяется стандартизированными тестовыми формулировками.
Вложения	Ранее загруженные документы удаляются вместе с именами файлов, метаданными и содержимым файлов в базе данных.

После выполнения сценария проводится контрольная выборка по пациентам и родственникам: проверяется отсутствие исходных ФИО и контактных данных, корректность связей, дат и

возрастных групп. Перед выдачей серверного доступа дополнительно проверяется, что на UAT-ВМ и доступных эксперту путях отсутствуют исходные дампы и резервные копии производственной базы.

11.3 Медицинские комментарии и вложения

В сущности PatientMedicalData основное поле Notes для всех записей получает значение «Заметки врача». Остальные необязательные текстовые поля сохраняют NULL, если исходное значение отсутствовало; при наличии текста оно заменяется значением из таблицы ниже.

Поля	Синтетическое значение
PatientComplicationNotes, GeneticNotes, CorticosteroidsNotes, VitaminsNotes, DiureticsNotes, PulmozymeNotes, FoodAdditivesNotes, BaselineNote	Заметки врача
Genetics	Синтетические генетические сведения
MutationGenetics	Тестовая мутация CFTR
Disability	Тестовые сведения об инвалидности
MSE	Тестовые сведения МСЭ

Записи PatientDocument и связанные загруженные файлы удаляются из UAT. Вместе с содержимым удаляются имена файлов и доступные приложению метаданные. После каждого восстановления UAT из исходного набора сценарий преобразования выполняется повторно. Контрольная выборка подтверждает отсутствие исходных контактов, свободного текста и вложений.

12 Требования и зависимости

Категория	Требование
Рабочее место эксперта	Современный браузер, доступ к Интернету и электронной почте; для инфраструктурной проверки — OpenVPN Connect и SSH-клиент
Клиентская часть	Angular 19+; Node.js 20.19 и npm требуются только для повторной сборки
Серверная часть	Ubuntu 22.04 LTS; .NET 8; Kestrel; Docker Engine; Docker Compose либо механизм Yandex Cloud update-container
База данных	PostgreSQL 16; Npgsql; Entity Framework Core; endpoint и порт сообщаются в непубличном приложении после запроса
Исходный код	Git и отдельный доступ к закрытым репозиториям SourceCraft только при согласованной проверке
Облачные операции	Выполняются техническим специалистом; доступ эксперта к веб-консоли и IAM подаккаунта не требуется

Категория	Требование
Электронная почта	Один адрес, доступный эксперту; второй адрес требуется только при отдельной проверке ролей

13 Типовые проблемы подключения и работы

Симптом	Проверка	Действие
Адрес UAT не открывается	Сеть, DNS и HTTPS	Проверка доступности адреса и обращение к ответственному специалисту
Пустая страница или старая версия	Ошибки 404 для bundles и кэш браузера	Принудительное обновление страницы и сверка index.html с хэшированными файлами
API недоступен	Состояние контейнера, журналы и порт 8080	Перезапуск контейнера или повторное применение контейнерной спецификации техническим специалистом
Заявка врача не видна	Выбранная организация и раздел «Новые врачи»	Проверка заявки действующим пользователем с ролью заведующего
OTP не пришёл	Адрес, папки «Спам» и «Рассылки», таймер и журнал Postbox	Повторная отправка кода и проверка почтовых журналов
OTP снова запрашивается	Браузер, устройство и сохранение данных сайта	Повторный выбор доверенного устройства
Нет VPN или SSH	Статус индивидуальной учётной записи, срок доступа, импорт профиля, маршрут и SSH fingerprint	Обращение к ответственному специалисту; перевыпуск персонального профиля или ключа без изменения подготовленной схемы UAT
Ошибка подключения к БД	Маршрут VPN, частный endpoint, порт, SSL и временные реквизиты	Сверка параметров непубличного приложения и использование только UAT-реквизитов
Несоответствие схемы	__EFMigrationsHistory и версия API	Согласование недостающих миграций с техническим специалистом

14 Защита данных и границы доступа

- Схема инфраструктурного доступа заранее подготовлена и проверяется до подачи заявления; после официального запроса создаются индивидуальные реквизиты для назначенного эксперта, ограниченные сроком и необходимыми ресурсами UAT.
- Доступ к веб-консоли Yandex Cloud, IAM-политикам и подаккаунту не предоставляется.

- Полные административные права root предоставляются назначенному эксперту через sudo только внутри изолированного UAT-экземпляра.
- Production folder, production registry, production VM и рабочая медицинская база в область проверки не входят.
- У UAT и PROD разные учётные данные баз данных; пароли не публикуются и передаются отдельно.
- В документацию не включаются содержимое secrets.json, токены IAM/OAuth, закрытые SSH-ключи и OTP.
- Публичный бакет содержит только статические файлы CF-Med-App; секреты в клиентскую сборку не включаются.
- В UAT сохраняются структурированные клинические сведения, а прямые идентификаторы, контакты, свободный текст и вложения преобразуются или удаляются по правилам раздела 11.
- После завершения проверки временные учётные записи и инфраструктурный доступ блокируются либо удаляются, ключи отзываются.

15 Техническое сопровождение проверки

Техническое сопровождение осуществляет ООО «Оккervиль Лаб». Ответственный специалист поддерживает доступность UAT, помогает при первичном подключении, контролирует доставку OTP, предоставляет пояснения по контейнерам и БД и фиксирует инциденты.

Параметр	Сведения
Ответственный специалист	Нестерук Александр Александрович, технический специалист ООО «Оккervиль Лаб»
Электронная почта	alexander@okkervil-lab.ru
Телефон или мессенджер	+7 931 224-42-98
Период поддержки	Без заранее установленной даты окончания, на период работы UAT; рабочие дни, московское время (UTC+3)
Срок реакции	Не позднее одного рабочего дня для критического и обычного обращения
Резервный контакт правообладателя	+7 921 871-94-95

Приложение А Идентификация проверочного экземпляра

Поле	Значение
Номер проверочной версии	1.024
Дата фиксации	11 сентября 2026 г.
UAT URL	https://cf-med-app.website.yandexcloud.net/
CFMed.Api image	cr.yandex/crpj42mbghnrlpqphjev/cf-med-api:1.087-uat
Backend	SourceCraft for-subaccount-fond-ostrova/cfmed-backend; ветка master
Frontend commit	3ac64facd7739d24041f689ecb750c9f4f90a68e
Frontend bundles	main-2D3VG247.js; polyfills-25SJB14S.js; scripts-PPDPQHDA.js; styles-F7TRY3BU.css
База данных	PostgreSQL на cf-med-test-db-vm, 192.168.0.13
Период доступности	Без заранее установленной даты окончания

Приложение Б Описание готовности экземпляра

Экземпляр, указанный в приложении А, предназначен для проверки заявленных функций CF Med «Медданные Муковисцидоз». Он использует изолированную UAT-копию структурированных клинических данных и не предоставляет доступ к рабочей базе. Прямые идентификаторы, контакты, свободный текст и вложенные документы преобразованы либо удалены в порядке, описанном в разделе 11.

Фактическая готовность проверочного экземпляра на 29 сентября 2026 г.

Сценарий PostgreSQL для обезличивания выполнен на предъявляемом UAT. Полные ФИО пациентов и родственников заменены синтетическими значениями; контакты и иные прямые идентификаторы заменены тестовыми значениями; свободный текст стандартизирован; записи PatientDocument и связанные вложения удалены; даты рождения смещены. После обработки проверены работа приложения, отображение возрастных групп и показатели раздела «Статистика учреждения».

Исходные дампы и резервные копии рабочей базы на доступных эксперту серверных ВМ UAT не размещались. Производственные реквизиты и конфигурации, позволяющие подключиться к PROD, в проверочный экземпляр не включены. Непосредственно перед выдачей доступа выполняется повторная контрольная проверка доступных каталогов как штатная мера безопасности.

Технические UUID сохраняются исключительно для целостности связей внутри UAT; таблица соответствия с рабочей базой не создаётся, доступ к рабочей базе не предоставляется. Структурированные клинические сведения и клинические даты сохранены для функциональной проверки, поэтому инфраструктурный доступ предоставляется адресно, временно и только к изолированному UAT.

Подключение к UAT через VPN, вход по SSH на обе серверные ВМ и получение полных административных прав через sudo уже фактически проверялись ООО «Оксервилл Лаб» при работе со стендом и функционируют. Проверка выполнялась с действующими учётными записями технических специалистов, а не с отдельной временной учётной записью эксперта. Для назначенного эксперта создаётся отдельная временная локальная учётная запись, его открытый SSH-ключ добавляется на обе ВМ, а пользователю предоставляются права через sudo. Перед передачей реквизитов выполняется краткая контрольная проверка входа.

VPN-шлюз, маршруты и внутренние адреса UAT подготовлены. После получения официального письма с данными назначенного эксперта для него создаётся отдельный пользователь OpenVPN и направляется ссылка на Client Web UI для получения персонального VPN-профиля. Эксперт передаёт свой открытый SSH-ключ; на обеих серверных ВМ UAT создаётся временная локальная учётная запись, ключ размещается в authorized_keys, а пользователю предоставляются полные административные права через sudo. Закрытый SSH-ключ не передаётся правообладателю.

В ответном письме сообщаются адрес VPN-портала, логин и временный пароль, SSH-имя пользователя, внутренние адреса ВМ, fingerprints и срок действия доступа. Доступ к веб-консоли и IAM подаккаунта Yandex Cloud не предоставляется. После завершения проверки временные учётные записи, VPN-профиль и SSH-ключ отзываются либо удаляются.

Приложение В Порядок передачи индивидуальных реквизитов

- Пошаговая схема VPN/SSH, публичный адрес шлюза и внутренние адреса UAT приведены в разделе 5; после запроса адресно передаются только индивидуальный VPN-профиль, логин, временный пароль, SSH-имя, fingerprints и срок действия.
- Реквизиты отдельной временной учётной записи PostgreSQL передаются непублично, если прямое подключение к тестовой базе входит в объём проверки.
- Read-only доступ к SourceCraft может быть предоставлен по отдельному согласованию. IAM-доступ к облачному подкаккаунту при этом не передаётся.
- Учётная запись веб-приложения в этот комплект не входит: эксперт создаёт её самостоятельно по процедуре раздела 5.