Flown

Установка и начало работы

Получите доступ к Flown в облаке разработчика или подготовьте к работе готовый продукт в инфраструктуре своей организации.

Редакция документации от 15 ноября 2026 года

Облачное использование и размещение у заказчика

ООО «Система поток» — ИНН 7447322882

Открыть этот раздел на сайте Flown

Выберите подходящий вариант размещения

Flown предоставляется в двух вариантах — использование в облаке разработчика и готовая виртуальная машина для размещения у заказчика.

В облаке сотрудник открывает выданный адрес организации и входит в свою учётную запись, эксплуатацию серверного окружения выполняет ответственная сторона по условиям сопровождения.

При размещении у заказчика передаётся готовая виртуальная машина, её ввод в работу и дальнейшее обслуживание выполняет команда поставщика либо специалисты заказчика, распределение работ закрепляется договором.

До начала работы согласуйте состав функций, подключаемые системы, ожидаемую нагрузку и ответственных за доступ сотрудников, эти сведения определяют параметры размещения и порядок приёмки.

Правообладатель Flown — ООО «Система поток», ИНН 7447322882, информацию о продукте и контакты разработчика можно найти на сайте Flown.

– Определите, кто администрирует пользователей внутри Flown.
– Определите, кто отвечает за серверное окружение, резервные копии и обновления.
– Зафиксируйте рабочий адрес и способ обращения за помощью.

Разделите обязанности администраторов

Администратор Flown управляет учётными записями, ролями и доступными ему настройками приложения, сотрудникам с этой ролью могут быть доступны пользователи, подключения, параметры процессов и обновлений.

Администратор серверной установки отвечает за запуск служб, сетевую доступность, хранение данных, резервное копирование и восстановление, назначение роли в интерфейсе само по себе не выдаёт доступ к серверу.

В небольшой организации эти обязанности может выполнять один специалист, в облачном варианте технические операции выполняет сторона, ответственная за облачное сопровождение.

Сотрудник передаёт администратору описание проблемы в интерфейсе, если причина относится к инфраструктуре, администратор Flown передаёт сведения техническому специалисту.

1. Назначьте контакт для вопросов входа и прав сотрудников.
2. Назначьте контакт для недоступности сервиса и технических работ.
3. Согласуйте, кто предупреждает пользователей о перерывах.
4. Проверьте, что контакты доступны сотрудникам до начала эксплуатации.

Подготовьте рабочее место для веб-доступа

Для работы через веб-интерфейс откройте выданный адрес Flown в браузере, установка программы на компьютер сотрудника для этого способа доступа не требуется.

Проверьте рабочий адрес по защищённому соединению HTTPS с той сети, из которой сотрудник будет работать, если по правилам организации требуется корпоративная сеть или защищённый удалённый доступ, сначала подключитесь к ним.

Браузер должен разрешать выполнение сценариев и хранение данных для рабочего сайта, Flown сохраняет в браузере сведения о сеансе, очистка данных сайта может потребовать повторного входа.

Если в организации используется сетевой фильтр или прокси, проверьте на рабочем адресе доступ к приложению и защищённые соединения WebSocket, они используются, в частности, для обмена сообщениями в чате с ассистентом.

Для диктовки и голосового диалога нужен доступ к исправному микрофону, разрешите запись для рабочего сайта и при необходимости проверьте разрешения операционной системы, текстовый чат можно использовать без микрофона.

1. Откройте рабочий адрес из сети сотрудника и убедитесь, что браузер не сообщает об ошибке сертификата.
2. Войдите в Flown, обновите страницу и проверьте, что сеанс сохраняется.
3. Отправьте безобидный текстовый запрос и дождитесь ответа ассистента.
4. Проверьте загрузку и скачивание небольшого файла без рабочих данных.
5. Если для работы нужен голос, включите запись на рабочем сайте и проверьте, что браузер получает звук с выбранного микрофона.

Установите приложение, если оно нужно

Flown можно использовать в браузере, а для работы через отдельное приложение выберите вариант для компьютера или мобильного устройства.

Откройте «Настройки» → «Скачать приложения» или страницу загрузки Flown по адресу https://flownai.ru/download/, там показаны варианты, доступные на момент установки.

Для macOS доступен установочный образ, для Windows — карточка в Microsoft Store, для iPhone — карточка в App Store. Совместимость с устройством и версией ОС сверяйте по карточке приложения перед установкой.

Если вместо рабочей ссылки указан статус «Скоро будет доступно», используйте веб-доступ, пока на странице не появится способ установки.

Перед установкой проверьте требования выбранного выпуска на странице загрузки или в магазине, при корпоративных ограничениях согласуйте установку с администратором.

1. Выберите устройство на официальной странице загрузки или в настройках Flown.
2. Откройте установочный файл или карточку магазина и выполните указания системы.
3. Для macOS и Windows откройте рабочий экземпляр в браузере, выберите «Настройки» → «Все настройки» → «Устройства» и в группе «Подключить компьютер» скопируйте «Ссылку для подключения Flown».
4. В настольном приложении вставьте эту ссылку в поле «Ссылка на приложение» и нажмите «Подключиться».
5. Для телефона используйте порядок подключения в разделе «Устройства» руководства «Настройки и администрирование Flown».
6. Выполните указанный приложением вход и проверьте, что открылся ваш рабочий экземпляр и профиль.

Окружение и требования к поставке

Для подготовки размещения используйте требования к сети и доступам и расчётные серверные профили в конце этого руководства. Конфигурация готовой виртуальной машины согласуется для конкретной поставки.

Расчётные ресурсы помогают выбрать начальную конфигурацию, но не устанавливают подтверждённый нагрузочными испытаниями минимум. Число одновременно работающих пользователей, объём материалов, версии окружения и ограничения браузеров проверяются при приёмке поставки.

Для сотрудника предусмотрены веб-доступ с настольного или мобильного устройства и отдельные клиентские приложения, наличие установщика и требования конкретного клиента проверяются в действующем разделе загрузок.

Часть окружения	Что подготовить	Что уточняется для поставки
Рабочее место	Браузер с выполнением сценариев, хранением данных сайта, загрузкой и скачиванием файлов	Поддерживаемые версии браузеров и ограничения корпоративных политик
Серверное окружение	Среду запуска согласованного комплекта, постоянные хранилища и доступ технического администратора	ОС, архитектура процессора, версии компонентов, ресурсы и ожидаемая нагрузка
Сеть	Рабочий адрес с HTTPS и доступ к нему из сети сотрудников	Доменные имена, сертификаты, прокси и разрешённые маршруты
Источники и обработка	Разрешённые подключения к моделям, корпоративным данным и службам обработки	Конкретные сервисы, учётные записи, полномочия и допустимый маршрут данных

Часть окружения	Что подготовить	Что уточняется для поставки
Сопровождение	Ответственных за пользователей, серверы, копии и обновления	Порядок работ, хранение копий, порядок восстановления и каналы обращения, согласованные для конкретной поставки

Подготовьте окружение заказчика

В исследованном облачном окружении серверные службы работают в контейнерах под управлением Docker и Docker Compose на Linux, состав окружения передаваемой виртуальной машины и требования к её запуску определяются для конкретной поставки.

Ресурсы сервера, версии программного окружения и объём хранения согласуются под состав поставки, количество работающих пользователей и характер задач.

При оценке нагрузки учитывайте не только число учётных записей, но и одновременную обработку файлов, выполнение программ, поиск по материалам и обращения к внешним системам.

Заранее определите адрес доступа, защищённое соединение HTTPS, необходимые сетевые маршруты и место для рабочих данных и копий, параметры корпоративной сети согласуйте с её администратором.

1. Согласуйте окружение и ответственных за его подготовку.
2. Уточните способ публикации рабочего адреса для сотрудников.
3. Проверьте сетевой доступ к согласованным внешним сервисам.
4. Подготовьте хранение рабочих данных и резервных копий.
5. Определите время приёмки и набор проверочных действий.

Определите состав серверного окружения

Веб-интерфейс и серверное приложение обеспечивают вход, доступ к разделам и обмен данными между браузером и платформой, за ответы ассистента и вызовы подключённых средств отвечает отдельная служба.

В исследованной облачной конфигурации PostgreSQL хранит рабочие записи, Redis используется для быстрого доступа к служебным данным, а Qdrant хранит поисковые коллекции для работы с материалами, для рабочих файлов выделяется постоянное хранилище.

В зависимости от согласованных функций проверяют службы обработки базы знаний, формирования документов и презентаций, выполнения кода, работы с браузером и поиска, для обмена инструментами с внешними приложениями может использоваться отдельная служба по протоколу Model Context Protocol.

Состав окружения и параметры размещения уточняются для конкретной поставки, доступность каждой выбранной функции проверяется на предоставленном экземпляре.

– Сетевой доступ сотрудников к рабочему адресу по HTTPS.

– Размещение базы данных, рабочих файлов, поиска по материалам и архивов.

– Маршруты к согласованным источникам данных, внешним моделям и другим службам.

– Доступы ответственных специалистов к серверной установке и к административным разделам Flown.

Разверните Flown из готовой виртуальной машины

При размещении в инфраструктуре заказчика Flown поставляется как готовая виртуальная машина с подготовленным серверным окружением, установка и последующее обслуживание выполняются сторонами, определёнными договором.

Формат виртуальной машины подбирается под систему виртуализации заказчика и согласуется при поставке, единый обязательный формат для всех заказчиков не установлен.

Это общий порядок ввода готовой виртуальной машины в работу, конкретные действия импорта и настройки зависят от формата переданного образа и системы виртуализации заказчика.

До развёртывания уточните формат полученного образа и совместимость с системой виртуализации организации, параметры ресурсов и версии окружения сверяются с утверждёнными требованиями к поставке.

До первого запуска подготовьте адрес и сетевые настройки, определите место для виртуальных дисков и копий, уточните способ получения доступа к виртуальной машине и к учётной записи администратора Flown.

При первом запуске проверьте доступ к консоли виртуальной машины и запуск серверных служб, затем подтвердите доступ с рабочего места сотрудника по выданному адресу HTTPS.

1. Получите виртуальную машину и сведения о версии Flown, сверяйте переданный образ по контрольной сумме, если она предоставлена.
2. Импортируйте образ средствами системы виртуализации заказчика или подключите переданные виртуальные диски, в зависимости от формата образа.
3. Назначьте согласованные ресурсы и сеть, проверьте доступность хранилища и настройте разрешение рабочего имени в сети сотрудников.
4. Запустите виртуальную машину, проверьте состояние серверных служб и настройте публикацию рабочего адреса по HTTPS, если она ещё не выполнена.
5. Выполните первый вход администратора и обычного пользователя, проверьте выбранные функции на контрольных данных.
6. Передайте рабочий адрес, порядок входа, контакты сопровождения и результаты проверки.

– Для ввода в эксплуатацию потребуются доступ к системе виртуализации и порядок получения административного доступа к экземпляру.

– Зафиксируйте расположение виртуальных дисков и отдельно подключённых хранилищ, если они используются.

– Для пробного запуска копии действующего экземпляра используйте изолированную сеть, чтобы копия не повторила рабочие задания и обращения к подключённым системам.

Получите доступ к облачному экземпляру

Ответственный за подключение организации сообщает рабочий адрес Flown и порядок первого входа, если у сотрудника ещё нет доступа, он обращается к администратору своей организации, который создаёт локальную учётную запись или проверяет доступ через настроенный каталог.

Веб-интерфейс открывается по адресу предоставленного экземпляра, доступность другого сайта Flown не подтверждает доступность рабочего адреса вашей организации.

Если страница не открывается, запишите адрес и текст сообщения браузера, при запросе авторизации используйте именно данные своей организации.

После успешного входа проверьте отображаемый профиль и доступные разделы, обнаруженное расхождение передайте администратору до загрузки рабочих материалов.

1. Откройте выданный рабочий адрес.
2. Дождитесь страницы входа, для входа с паролем используйте поля «Логин» и «Пароль».
3. Введите данные своей учётной записи и нажмите «Войти», для доменного входа используйте форму логина, которую сообщил администратор.
4. Откройте Профиль и проверьте сведения о своей учётной записи.
5. Убедитесь, что доступны разделы, необходимые для вашей работы.

Выполните первый вход и настройте профиль

Для локальной учётной записи используется имя входа, заданное администратором, адрес электронной почты и имя входа могут различаться.

При использовании Active Directory порядок входа зависит от настройки корпоративного каталога, точную форму имени сообщает администратор организации.

В Профиле доступны личные данные, рабочие сведения и контакты, при локальной авторизации можно открыть отдельное окно смены пароля.

Для доменной учётной записи интерфейс показывает, что пароль и основные сведения управляются корпоративным каталогом, возможность смены локального пароля зависит от типа учётной записи.

1. Проверьте имя пользователя и раскладку клавиатуры перед входом.
2. После входа откройте Настройки и Профиль.
3. Проверьте отображаемое имя, рабочие сведения и контакты.
4. При доступной смене пароля введите текущий пароль, новый пароль и его повтор.
5. Сохраните данные и дождитесь сообщения об успешном выполнении.

Подготовьте сотрудников и рабочие права

Штатные роли называются Администратор и Пользователь, для сотрудников назначайте права в соответствии с выполняемой работой.

Для локального входа администратор открывает «Настройки» → «Пользователи», нажимает «Добавить», заполняет логин, пароль и подтверждение пароля, при необходимости указывает

отображаемое имя и почту, проверяет переключатель «Активен» и нажимает «Создать», рабочие права проверяет отдельно.

Доступ к разделам и доступ к конкретным материалам проверяйте отдельно, наличие пункта Проекты ещё не подтверждает участие во всех проектах организации.

Для приёмки используйте отдельную учётную запись обычного сотрудника, административная учётная запись показывает больше возможностей и не воспроизводит его рабочие условия.

1. Подготовьте список сотрудников и необходимых им функций.
2. Создайте учётные записи или настройте согласованный каталог.
3. Назначьте роли и участие в рабочих проектах.
4. Войдите как обычный сотрудник и проверьте согласованный набор действий.
5. Исправьте обнаруженные расхождения до начала массовой работы.

Проверьте зависимости выбранных функций

Обращения к внешней модели требуют настроенного провайдера, действующих учётных данных и сетевой доступности сервиса.

Поиск в интернете использует доступные поисковые службы, а работа с данными компании зависит от подключения соответствующего приложения и прав на стороне источника.

Размещение Flown у заказчика не определяет автоматически место выполнения всех операций, обработка зависит от выбранных моделей и подключённых сервисов.

Для приёмки выбирайте известные данные с понятным ожидаемым результатом, проверяйте отдельно чтение источника, обработку материала и разрешённое действие.

– Проверьте выбранное подключение, если у сервиса несколько аккаунтов.
– Сопоставьте результат чтения с исходной записью или документом.
– Для действия во внешней системе заранее согласуйте объект проверки.
– Убедитесь, что переданные материалы допустимы для выбранного провайдера.

Примите готовый экземпляр

Приёмка показывает, что предоставленный экземпляр выполняет согласованные рабочие действия в окружении организации.

Проверка главной страницы подтверждает доступность интерфейса, для приёмки функций дополнительно выполните вход и предметные действия.

Подготовьте небольшой документ, вопрос с известным ответом и пример работы с подключением, сохраните полученные файлы и откройте их в целевой программе.

Результат фиксируйте по каждому действию — что выполнено, под какой ролью, какой результат получен и какие вопросы требуют доработки.

1. Откройте рабочий адрес с устройства сотрудника.
2. Проверьте вход администратора и обычного пользователя.

3. Откройте согласованные разделы и один рабочий проект.
4. Отправьте проверочный запрос и проверьте ответ.
5. Проверьте загрузку, получение и открытие файла.
6. Выполните согласованный запрос к подключённой системе.
7. Передайте перечень расхождений ответственному за поставку.

Зафиксируйте сведения о передаваемом экземпляре

Перед началом эксплуатации сохраните сведения, по которым сотрудники и технические специалисты смогут определить свой экземпляр и обратиться за помощью.

В разделе «О программе» скопируйте сведения для поддержки, при технической передаче отдельно зафиксируйте состав серверного выпуска, дата редакции этой документации не заменяет версию установленного программного обеспечения.

– Наименование Flown и правообладатель ООО «Система поток», ИНН 7447322882.
– Рабочий адрес, способ входа и назначенный администратор организации.
– Версии интерфейса и сервера, состав предоставленных функций и результаты их приёмки.
– Подключённые внешние службы, ответственные за учётные записи и границы обработки данных.
– Для поставки заказчику — образ виртуальной машины, его формат, версия Flown, технические требования, способ получения административного доступа, расположение дисков и дополнительных хранилищ.
– Порядок резервного копирования, восстановления и обновления, ответственные по договору и внешний канал связи при недоступности приложения.
– Секреты и ключи передаются уполномоченным специалистам отдельно от общедоступной документации.

Разберите типовые затруднения при запуске

Если адрес не открывается, проверяйте написание, доступ к корпоративной сети и сообщение браузера, сведения об ошибке передайте ответственному за окружение.

Если вход отклонён, уточните имя пользователя, способ авторизации и активность учётной записи, при доменном входе дополнительно проверяется доступность каталога.

Если раздел отсутствует, администратор сопоставляет роль, настройки меню и состав функций экземпляра, повторная установка продукта для такой проверки не требуется.

Если чат открывается, но задача завершается ошибкой, запишите выбранную модель, подключение и момент сбоя, это помогает отделить доступность интерфейса от работы конкретной зависимости.

– В сообщении об ошибке укажите рабочий адрес без секретных параметров, время с часовым поясом, раздел, последовательность действий и точный текст ошибки. Добавьте доступные сведения о версии и отметьте, кого затронула проблема.
– Пароли и ключи доступа не включайте в переписку и снимки экрана.

– После исправления повторите именно действие, которое завершалось ошибкой.

Уточните причину ошибки на странице входа

Если форма сообщает о неверном логине или пароле, проверьте рабочий адрес, раскладку и форму логина, если ошибка повторяется, попросите администратора проверить учётную запись и её активность.

Если форма сообщает о слишком большом числе попыток, дождитесь указанного времени или попробуйте позже, частые повторы не помогают восстановить вход.

Если форма сообщает об отсутствии соединения или временной недоступности сервиса входа, запишите время и вид ошибки, проверка логина и пароля не заменяет проверку доступности сервиса.

Выберите расчётный серверный профиль

Для одного экземпляра Flown с внешними API языковых моделей и эмбеддингов используйте следующие ориентиры при планировании ресурсов. Это расчётные начальные конфигурации, а не результаты нагрузочного испытания и не гарантия обслуживания заданного числа пользователей.

Начальный профиль предназначен для запуска и приёмки одного экземпляра с ограниченным объёмом материалов. Расширенный профиль даёт больший запас для одновременной обработки файлов, выполнения программ и роста базы знаний. Конкретное число пользователей определяется проверкой согласованных сценариев.

Ориентиры учитывают наблюдаемую конфигурацию работающего экземпляра и запас для ОС, служб и временных файлов. Разовый замер потребления памяти не показывает пиковую нагрузку, а ресурсы общего сервера с несколькими экземплярами не являются ресурсами одной установки.

– Хранилище резервных копий рассчитывайте отдельно и размещайте вне единственной рабочей виртуальной машины.

– При локальном размещении моделей отдельно рассчитывайте ресурсы их исполнения, включая память и GPU при необходимости; приведённые профили их не включают.

– Перед эксплуатацией проверьте одновременно выбранные сценарии: разговор с ассистентом, обработку файлов, поиск по материалам, запуск программ и обращения к подключённым системам.

– Если растут время ответа, очередь заданий или потребление памяти и диска, увеличьте ресурсы либо ограничьте параллельную нагрузку по результатам измерений.

Параметр	Начальный профиль	Расширенный профиль
Процессор	8 vCPU, x86-64	16 vCPU, x86-64
Оперативная память	16 ГБ	32 ГБ
Диск для ОС, служб и рабочих данных	200 ГБ SSD с возможностью расширения	500 ГБ SSD/NVMe с возможностью расширения
GPU для внешних API моделей	Не требуется	Не требуется

Параметр	Начальный профиль	Расширенный профиль
Пропускная способность сети — ориентир	100 Мбит/с	1 Гбит/с

Рассчитайте хранение и запас для роста

Диск используется ОС, контейнерными образами, PostgreSQL, поисковыми коллекциями Qdrant, загруженными и созданными файлами, рабочими каталогами программ, кэшами и журналами. Соотношение этих данных зависит от сценариев, поэтому фиксированный объём векторной базы не назначается заранее.

Для начального размещения не требуется автоматически резервировать 1 ТБ только под платформу. Ориентир 200 ГБ относится к небольшому стартовому объёму данных; если материалы и архивы уже занимают значительное место, добавьте их фактический объём и запас до импорта.

Используйте SSD/NVMe для рабочих данных. Планируйте расширение тома и свободное место для обновления контейнеров, временной обработки файлов и восстановления копий. Срок хранения журналов и резервных копий задаётся для конкретного экземпляра.

1. Оцените текущий объём исходных файлов и ожидаемое ежемесячное пополнение.
2. Уточните объём баз данных, поисковых коллекций, создаваемых документов и рабочих каталогов.
3. Определите период хранения копий и необходимое отдельное хранилище.
4. Проверьте свободное место до обновления, массовой загрузки и восстановления.
5. Настройте наблюдение за заполнением диска и порядок его расширения.

Подготовьте ОС и административный доступ

Серверный профиль рассчитан на Linux x86-64 и контейнерное окружение Docker с Docker Compose. В проверенном работающем окружении используется Ubuntu Server 24.04 LTS. Версии ОС и контейнерного окружения внутри передаваемой виртуальной машины фиксируются в составе выпуска.

Для Ubuntu Server 22.04 LTS, Debian 12 и других вариантов окружения совместимость проверяется для конкретного образа и выпуска. Само наличие совместимого гипервизора не подтверждает работу любого образа без проверки.

При поставке готовой виртуальной машины получатель импортирует подготовленное окружение, повторная установка всех компонентов вручную не предполагается. Обновление ОС и контейнерного окружения выполняет ответственная сторона по договору с проверкой совместимости.

Техническому администратору нужен согласованный доступ к консоли виртуальной машины и, если используется удалённое сопровождение, SSH с необходимыми полномочиями. Доступ организуется через разрешённую сеть, VPN или промежуточный сервер; общедоступный SSH не является обязательным.

Для SSH используйте согласованные ключи и ограничение источников подключения. Установите синхронизацию времени и согласуйте часовой пояс, особенно для расписаний и сопоставления журналов.

– Зафиксируйте версию ОС, Docker и Docker Compose при передаче экземпляра.

– Проверьте, кто имеет административный доступ и кто отвечает за его отзыв.

– Не включайте закрытые ключи, пароли и токены в общедоступную документацию.

– Проверьте доступ ответственного специалиста до начала обслуживания.

Настройте сетевые маршруты и защищённый доступ

Для сотрудников подготовьте рабочее доменное имя и HTTPS на порту 443 с доверенным сертификатом. Порт 80 нужен только при выбранной схеме перенаправления или обслуживания сертификата. Внутренний адрес и корпоративный удостоверяющий центр допустимы, если устройства сотрудников доверяют сертификату.

Прокси и межсетевой экран должны пропускать необходимые HTTPS-запросы и защищённые WebSocket-соединения рабочего экземпляра. Отдельно проверьте загрузку и скачивание файлов и длительные ответы; ограничения размера и времени ожидания согласуются с администратором сети.

Для внешних моделей и эмбеддингов требуется исходящий HTTPS, обычно на порт 443. Отдельно разрешите согласованные источники обновлений, поисковые службы и внешние API, используемые выбранными сценариями. Перечень адресов зависит от фактически настроенных провайдеров и подключений и фиксируется при поставке.

Серверу нужен доступ к подключаемым внутренним системам: опубликованному HTTP-сервису 1С, порталу Битрикс24, базам данных, почте и другим выбранным источникам. Порты, адреса и полномочия берутся из настройки каждой системы. Доступ по ping не заменяет проверку прикладного соединения.

Для удалённого администрирования разрешите SSH на порту 22 либо другом согласованном порту только из разрешённой сети. Внутренние порты баз данных и служебных контейнеров не требуется открывать сотрудникам или всему интернету.

Использование внешних моделей требует доступного маршрута к ним. Размещение Flown у заказчика само по себе не означает автономную работу без внешних сервисов и не исключает передачу выбранных данных настроенным обработчикам.

1. Согласуйте имя экземпляра, сертификат и сети сотрудников.
2. Проверьте вход по HTTPS и работу чата с рабочего места.
3. Проверьте доступ сервера к выбранной модели и источникам данных.
4. Проверьте получение обновлений по согласованному маршруту.
5. Зафиксируйте разрешённые назначения, порты и ответственных за изменения сети.

Подготовьте облачный экземпляр к проверке

Для облачного использования на рабочем месте проверяющего достаточно веб-доступа к предоставленному экземпляру. Импорт виртуальной машины и установка серверных компонентов на его компьютер не требуются.

Перед передачей доступа ответственный за экземпляр проверяет доступность необходимых моделей и служб обработки, подготавливает контрольные материалы и назначает права. Пользователь проверяет результат в видимом интерфейсе; настройка скрытых серверных компонентов относится к

техническому сопровождению.

Проверяющему передают рабочий адрес, порядок входа, перечень проверяемых функций и контакт сопровождения. Учётные данные передают отдельно по согласованному каналу, не размещают в общедоступном руководстве или PDF.

В разделе «Функциональные характеристики» приведены условия проверки разных функций и контрольный пример ответа по документу. Полные пользовательские инструкции доступны в соответствующих разделах документации.

1. Откройте выданный адрес из сети проверяющего и убедитесь, что вход по HTTPS доступен без ошибки сертификата.
2. Подготовьте отдельную учётную запись обычного пользователя. Если проверяется администрирование, подготовьте отдельный доступ с необходимыми полномочиями.
3. Откройте «Настройки» → «Все настройки», в группе «Поддержка» выберите «О программе» и зафиксируйте доступные сведения о версиях. Дата документации не заменяет версию экземпляра.
4. Проверьте доступность модели запросом с известным ответом. Если селектор модели показан, используйте доступный вариант; отсутствие селектора не означает, что модель можно настроить через скрытый раздел.
5. Выполните контрольный пример с файлом. Для остальных функций используйте отдельные сценарии из таблицы функциональных характеристик.
6. Если требуется внешнее приложение, подготовьте его тестовое подключение и известный объект для чтения. Доступ к каталогу приложений не подтверждает, что подключение уже настроено.
7. Передайте результаты проверки и перечень ограничений вместе с порядком обращения за помощью.

Подключите источник для контрольного сценария

Выполняйте эти действия, если проверяется работа с внешним приложением. Для первого запроса по приложенному файлу подключение корпоративной системы не требуется.

Подключение содержит параметры конкретного сервиса. Доступ к карточке приложения и создание подключения не доказывают наличие прав на все его объекты: итог проверяется под учётной записью назначенного сотрудника.

Названия полей и действия проверки зависят от приложения. Для 1С предусмотрена «Проверить доступность», однако такое же действие не обещается для каждой карточки каталога. Подробные поля описаны в руководстве «Приложения и подключения».

1. Откройте «Приложения», выберите карточку нужного сервиса и нажмите «Подключить» либо «Добавить подключение». Если подключение уже есть, в карточке может отображаться «Подключить ещё одну учётную запись».
2. Выберите «Личное — только моё» для своего подключения. Для общего подключения администратор выбирает «Общее — для организации».
3. Заполните параметры, которые запрашивает форма выбранного приложения, или пройдите предложенную авторизацию в тестовом источнике. Выполните предусмотренную этой формой проверку и сохранение.

4. Для общего подключения проверьте настройки доступа сотрудников и режим входа. Если доступ выдаётся выбранным сотрудникам, добавьте нужного участника и при необходимости настройте его вход.
5. Войдите назначенным сотрудником, выберите нужное подключение в рабочем контексте чата и попросите прочитать заранее известную тестовую запись без изменения данных.
6. Сравните ответ с записью в исходной системе. При ошибке сохраните название подключения, время и текст сообщения; пароль и ключ в протокол проверки не включайте.