БАЗИС

БАЗИС.ТЕХНОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ

РУКОВОДСТВО ПО УСТАНОВКЕ И ЭКСПЛУАТАЦИИ

Версия продукта	1.1.08
Версия документа	1.8
Дата	25.08.2026

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

Основные термины и сокращения, используемые в руководстве, приведены в таблице 1.

Таблица 1. Термины и сокращения

Термин / сокращение	Определение
DNS	Система доменных имен, обеспечивающая преобразование доменных имен в сетевые адреса
ESR	Extended Support Release – ветвь браузера с расширенным сроком поддержки
HTTPS	Защищенный протокол передачи данных между веб-браузером и сервером
RPO/RTO	Целевые показатели допустимой потери данных и времени восстановления соответственно
SaaS	Software as a Service – предоставление программного обеспечения как облачного сервиса
SBOM	Software Bill of Materials – формализованный перечень программных компонентов, входящих в состав продукта
SSD	Твердотельный накопитель
URL	Адрес информационного ресурса в сети
vCPU	Виртуальное процессорное ядро, выделенное виртуальной машине
x86_64	64-разрядная архитектура процессора семейства x86
ГБ	Гигабайт – единица измерения объема данных
ИБ	Информационная безопасность
Изолированный контур	Контур без прямого доступа в Интернет
ОС	Операционная система
ПО	Программное обеспечение
ТБ	Терабайт – единица измерения объема данных

1. НАЗНАЧЕНИЕ ДОКУМЕНТА

Настоящее руководство определяет целевые требования и порядок предоставления, установки, первичной настройки, приемки, эксплуатации, резервного копирования, обновления и удаления программного обеспечения (далее – ПО).

Руководство предназначено для администраторов информационных систем, специалистов по информационной безопасности, инженеров сопровождения и лиц, ответственных за приемку ПО.

Настоящее руководство применяется совместно с документами:

- «БАЗИС. Технологическое моделирование. Функциональные характеристики» для проверки заявленного функционального состава;
- «БАЗИС. Технологическое моделирование. Руководство администратора» для проверки заявленных административных функций;
- «БАЗИС. Технологическое моделирование. Руководство пользователя» для выполнения прикладных операций после ввода в эксплуатацию;
- «БАЗИС. Технологическое моделирование. Описание архитектуры и нефункциональных характеристик» для выбора схемы размещения и учета нефункциональных требований;
- «БАЗИС. Технологическое моделирование. Описание жизненного цикла, обновления и сопровождения» для соблюдения правил поставки, обновления, отката и технической поддержки.

2. ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ И РАЗВЕРТЫВАНИЯ

В таблице 2 представлены варианты предоставления и развертывания БАЗИС.

Таблица 2. Варианты предоставления и развертывания

Вариант	Размещение	Обновления	Целевое применение
Облачный сервис (SaaS)	Централизованный промышленный контур разработчика	Централизованно выполняются разработчиком по регламенту сервиса	Организации, требования ИБ которых допускают доступ через Интернет и размещение программного обеспечения и данных во внешнем защищенном контуре разработчика
Односерверное развертывание в инфраструктуре заказчика с доступом в Интернет	Один сервер заказчика; все компоненты программного комплекса размещаются на этом сервере	Администратор заказчика получает подписанный пакет обновления через защищенный канал и выполняет установку в соответствии с инструкцией	Пилотная эксплуатация и ограниченная производственная нагрузка без требований к высокой доступности
Распределенное развертывание в инфраструктуре заказчика с доступом в Интернет	Прикладные сервисы, расчетные процессы и данные размещаются на отдельных серверах или узлах		Производственная эксплуатация с повышенной нагрузкой, требованиями к масштабированию и возможностью построения отказоустойчивой конфигурации
Односерверное развертывание в инфраструктуре заказчика в изолированном контуре без доступа в Интернет	Один сервер в изолированном контуре заказчика; все компоненты программного комплекса размещаются на этом сервере	Подписанный пакет обновления переносится в изолированный контур в соответствии с регламентом информационной безопасности заказчика. Установку выполняет администратор заказчика	Автономная эксплуатация в изолированном контуре при ограниченной или умеренной нагрузке без требований к высокой доступности
Распределенное развертывание в инфраструктуре заказчика в изолированном	Прикладные сервисы, расчетные процессы и данные размещаются на отдельных серверах или узлах изолированного контура		Критически значимые корпоративные и технологические контуры с повышенными требованиями к

Вариант	Размещение	Обновления	Целевое применение
контуре без доступа в Интернет			производительности, доступности и отказоустойчивости

2.1. ОБЛАЧНЫЙ СЕРВИС

Размещение и доступ. Все прикладные и инфраструктурные компоненты БАЗИС размещаются в централизованном облачном контуре под управлением разработчика. Пользователи подключаются к сервису через Интернет по протоколу HTTPS и работают через веб-браузер. Доступ предоставляется с использованием учетных записей БАЗИС либо корпоративной системы единого входа.

Предоставление. Установка серверной части в инфраструктуре заказчика не выполняется. Разработчик предоставляет адрес сервиса, создает организацию и учетные записи либо настраивает корпоративный вход. Заказчик обеспечивает доступ к адресу сервиса, использование поддерживаемого браузера и доверие к сертификату HTTPS.

Обновление и откат. Обновления проверяются и устанавливаются централизованно разработчиком. Перед обновлением выполняются резервное копирование и контроль совместимости, а также определяется порядок отката. Администратор заказчика не получает и не устанавливает пакеты обновления.

Эксплуатация и ответственность. Разработчик отвечает за инфраструктуру, мониторинг, журналирование, резервное копирование и техническое обновление сервиса. Заказчик отвечает за своих пользователей, конечные устройства, сетевой доступ и допустимость обработки данных в облачном сервисе.

Применение и ограничения. Вариант предназначен для организаций, политика информационной безопасности которых допускает доступ через Интернет и размещение программного обеспечения и данных во внешнем защищенном контуре. Постоянное подключение к Интернету необходимо.

Схема предоставления БАЗИС как облачного сервиса приведена на рисунке 1.

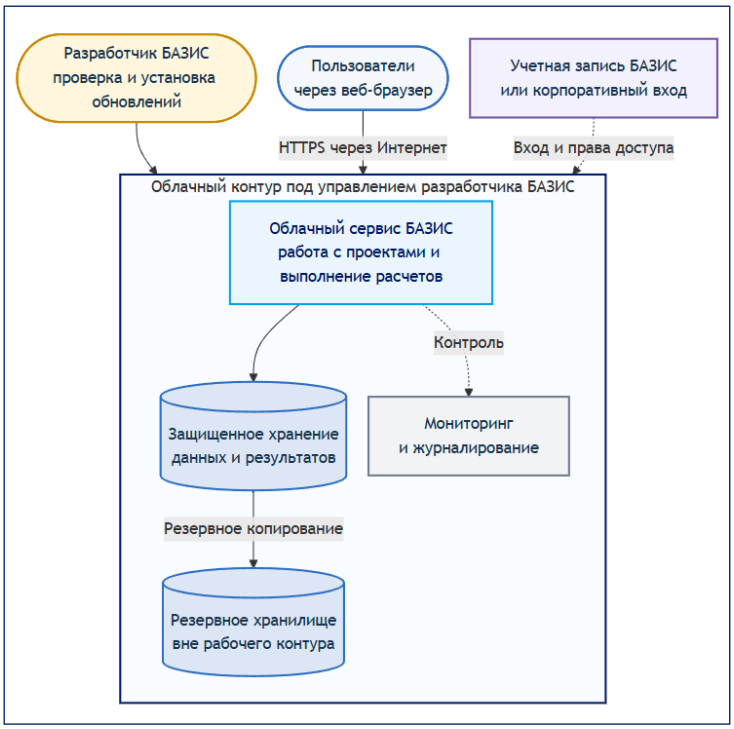

Рисунок 1. Облачный сервис

2.2. ОДНОСЕРВЕРНОЕ РАЗВЕРТЫВАНИЕ В ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА С ДОСТУПОМ В ИНТЕРНЕТ

Размещение и доступ. Все компоненты БАЗИС размещаются на одном физическом или виртуальном сервере заказчика под управлением Windows Server или Linux. Пользователи подключаются к серверу через корпоративную сеть по протоколу HTTPS.

Установка. Администратор заказчика получает подписанный поставочный комплект через защищенный канал, проверяет электронную подпись, контрольные суммы и совместимость, после чего устанавливает БАЗИС в соответствии с инструкцией. Исходные тексты, репозитории и средства сборки заказчику не передаются.

Обновление и откат. Администратор получает подписанный пакет обновления через Интернет, но решение о его установке принимает самостоятельно. Перед обновлением создается резервная копия, проверяется совместимость и определяется порядок отката. Автоматическая установка и прямой доступ разработчика к серверу по умолчанию не используются.

Эксплуатация и ответственность. Заказчик отвечает за сервер, операционную систему, сеть, сертификаты, мониторинг, резервное копирование и установку обновлений. Резервные копии должны храниться вне сервера БАЗИС. Разработчик предоставляет пакеты, документацию и техническую поддержку.

Применение и ограничения. Вариант подходит для пилотной эксплуатации и ограниченной производственной нагрузки без требований к высокой доступности. Все компоненты образуют единую точку отказа и не могут масштабироваться независимо.

Схема односерверного развертывания с доступом в Интернет приведена на рисунке 2.

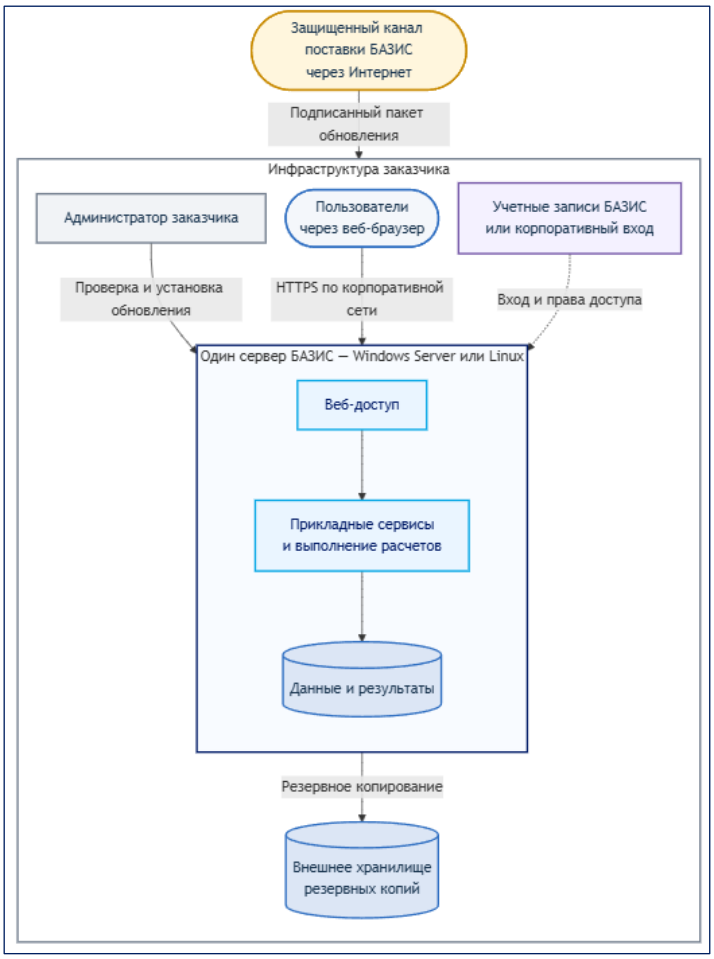

Рисунок 2. Односерверное развертывание в инфраструктуре заказчика с доступом в Интернет

2.3. РАСПРЕДЕЛЕННОЕ РАЗВЕРТЫВАНИЕ В ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА С ДОСТУПОМ В ИНТЕРНЕТ

Размещение и доступ. Прикладные сервисы, расчетные процессы и данные размещаются на отдельных серверах или узлах заказчика. Пользователи подключаются к единой точке доступа БАЗИС через корпоративную сеть по протоколу HTTPS.

Установка. Администратор получает подписанный поставочный комплект через защищенный канал, проверяет его целостность и устанавливает компоненты на узлы в соответствии с согласованной схемой размещения. Состав и количество узлов определяются нагрузкой и требованиями к доступности.

Обновление и откат. Пакет обновления получает администратор заказчика. Обновление выполняется в установленной последовательности: предварительная проверка, резервное копирование, остановка или переключение необходимых сервисов, обновление узлов, проверка работоспособности. Возможность обновления без полной остановки определяется конкретной конфигурацией и паспортом релиза.

Эксплуатация и ответственность. Заказчик обеспечивает работу всех узлов, балансировку нагрузки, мониторинг, резервирование и восстановление. Разработчик предоставляет требования к совместимости, порядок обновления и техническую поддержку.

Применение и ограничения. Вариант предназначен для производственной эксплуатации с повышенной нагрузкой и требованиями к масштабированию. Распределенное размещение создает

возможность построения отказоустойчивой конфигурации, но само по себе не обеспечивает отказоустойчивость.

Схема распределенного развертывания с доступом в Интернет приведена на рисунке 3.

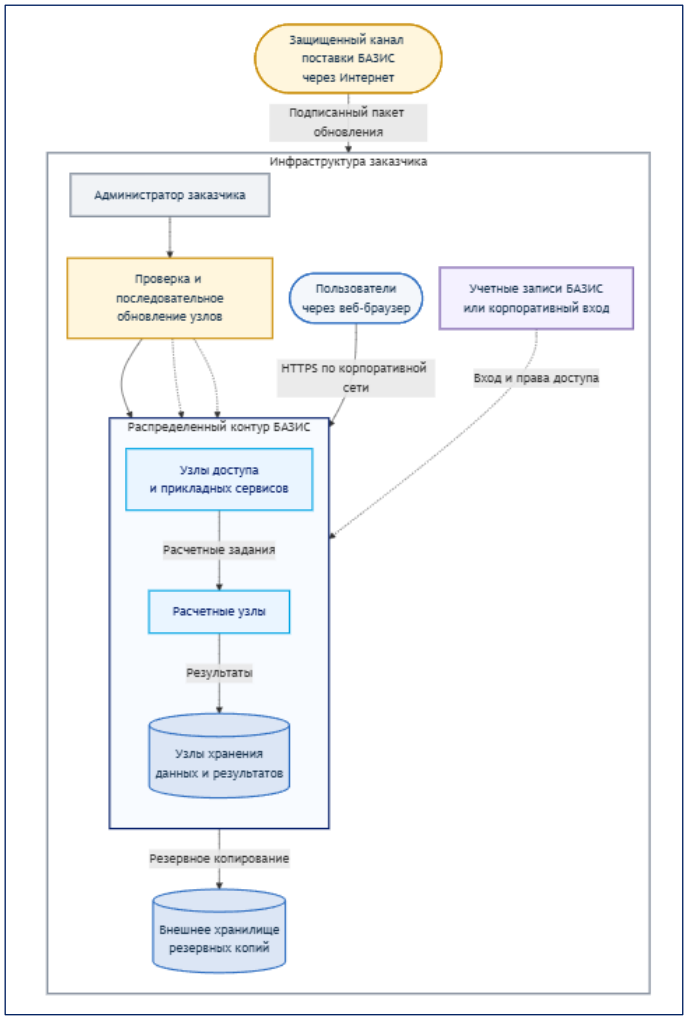

Рисунок 3. Распределенное развертывание в инфраструктуре заказчика с доступом в Интернет

2.4. ОДНОСЕРВЕРНОЕ РАЗВЕРТЫВАНИЕ В ИЗОЛИРОВАННОМ КОНТУРЕ БЕЗ ДОСТУПА В ИНТЕРНЕТ

Размещение и доступ. Все компоненты БАЗИС размещаются на одном сервере внутри изолированного контура заказчика. Для штатной работы, активации и обновления исходящие подключения к Интернету не требуются. Пользователи работают через внутреннюю сеть контура.

Установка. Подписанный поставочный комплект переносится через контролируемую границу на разрешенном носителе или через шлюз межконтурного обмена. До установки выполняются регистрация носителя, антивирусный контроль, проверка электронной подписи и сверка контрольных сумм.

Обновление и откат. Пакет обновления переносится в изолированный контур по регламенту информационной безопасности заказчика. Установку выполняет администратор после локальной проверки и создания резервной копии. Откат выполняется средствами поставочного комплекта либо путем восстановления согласованной резервной копии.

Эксплуатация и ответственность. Заказчик самостоятельно обеспечивает сервер, мониторинг, журналирование, резервное копирование и восстановление. Резервные копии

размещаются на отдельном устройстве внутри защищенного контура. Передача диагностических данных разработчику допускается только по решению заказчика.

Применение и ограничения. Вариант предназначен для автономной эксплуатации при ограниченной или умеренной нагрузке. Он не обеспечивает ни независимого масштабирования, ни высокой доступности.

Схема односерверного развертывания в изолированном контуре приведена на рисунке 4.

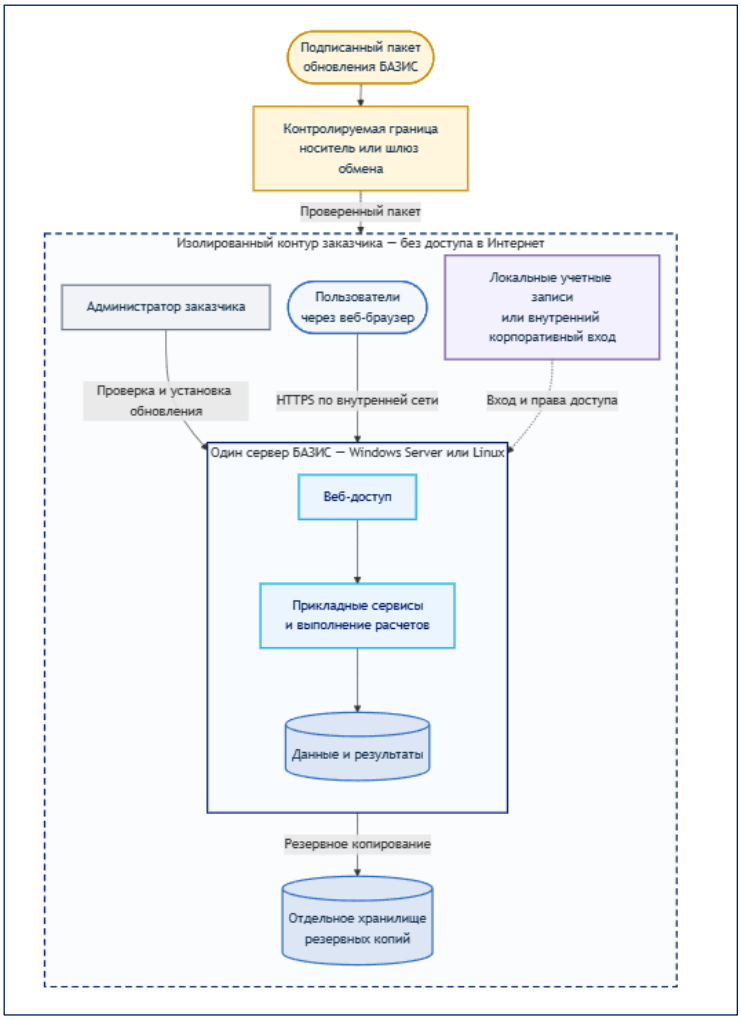

Рисунок 4. Односерверное развертывание в изолированном контуре без доступа в Интернет

2.5. РАСПРЕДЕЛЕННОЕ РАЗВЕРТЫВАНИЕ В ИЗОЛИРОВАННОМ КОНТУРЕ БЕЗ ДОСТУПА В ИНТЕРНЕТ

Размещение и доступ. Прикладные сервисы, расчетные процессы и данные размещаются на отдельных узлах изолированного контура. Все пользовательские и межкомпонентные соединения устанавливаются внутри сети заказчика. Доступ в Интернет для штатной эксплуатации не требуется.

Установка. Поставочный комплект переносится через контролируемую границу и проходит предусмотренные регламентом проверки. Компоненты устанавливаются на узлы в соответствии с утвержденной схемой размещения. Подключение к публичным репозиториям при установке не требуется.

Обновление и откат. Подписанный пакет переносится в изолированный контур, проверяется и предварительно испытывается в доступной тестовой среде. Администратор последовательно

обновляет узлы, проверяет совместимость компонентов и выполняет контрольные операции. Порядок возврата предыдущей версии определяется паспортом релиза и планом восстановления.

Эксплуатация и ответственность. Заказчик обеспечивает локальные средства мониторинга, журналирования, резервного копирования и восстановления. Постоянный удаленный доступ разработчика не предусматривается. Диагностические данные передаются за пределы контура только после проверки и разрешения владельца данных.

Применение и ограничения. Вариант предназначен для критически значимых корпоративных и технологических контуров с повышенными требованиями к производительности, доступности и автономности. Он требует наиболее развитых компетенций администрирования и собственной эксплуатационной инфраструктуры.

Схема распределенного развертывания в изолированном контуре приведена на рисунке 5.

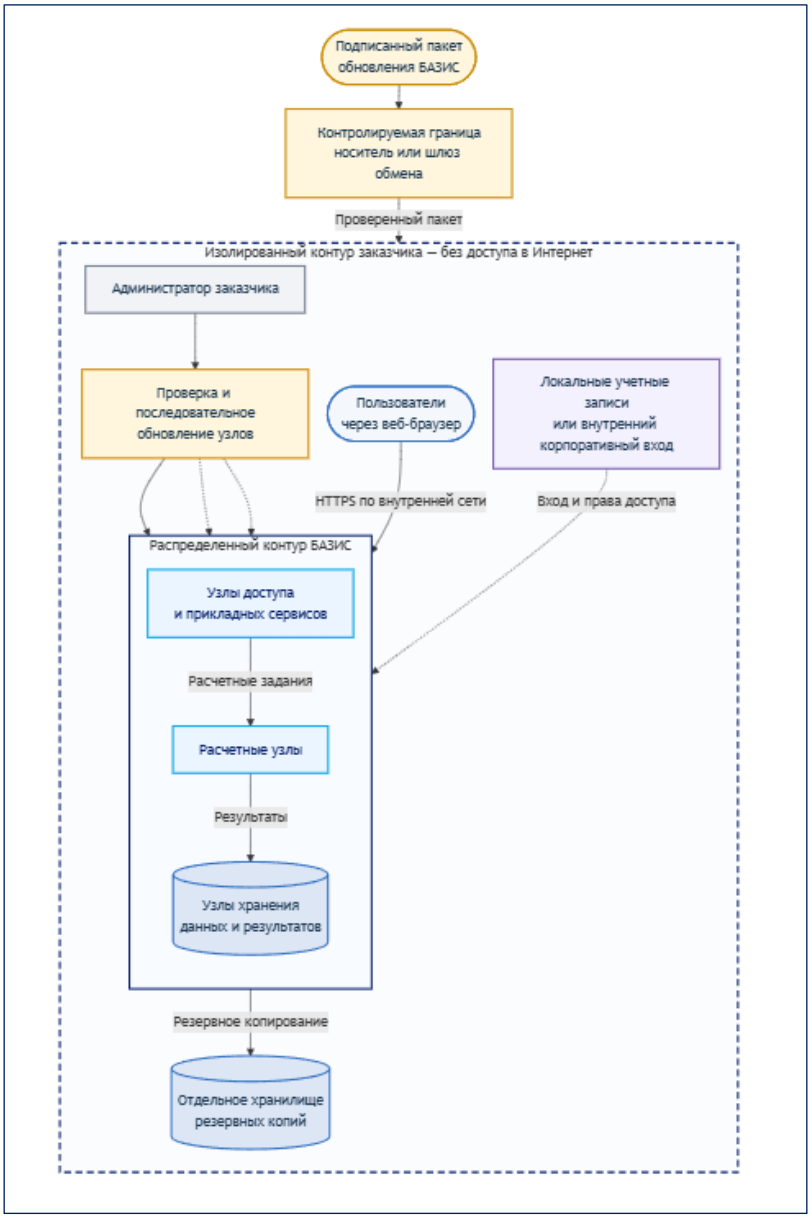

Рисунок 5. Распределенное развертывание в изолированном контуре без доступа в Интернет

2.6. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

Распределение ответственности при различных моделях предоставления представлено в таблице 3.

Таблица 3. Распределение ответственности

Область ответственности	Облачный сервис	Развертывание в инфраструктуре заказчика
Вычислительная инфраструктура	Разработчик	Заказчик
Серверная операционная система и инфраструктурные компоненты	Разработчик	Заказчик; разработчик устанавливает требования совместимости
Корпоративная сеть и доступ в Интернет	Заказчик обеспечивает доступ пользователей; облачный контур обслуживает разработчик	Заказчик
Сертификаты HTTPS	Разработчик для адреса облачного сервиса	Заказчик
Установка серверной части	Разработчик	Администратор заказчика по документации разработчика
Подготовка обновлений	Разработчик	Разработчик формирует подписанный пакет, документацию и порядок отката
Установка обновлений	Разработчик	Администратор заказчика
Мониторинг и журналирование	Разработчик по регламенту сервиса	Заказчик
Резервное копирование и восстановление	Разработчик по регламенту сервиса	Заказчик по настоящему руководству
Создание организации и первоначальная настройка доступа	Разработчик совместно с заказчиком	Администратор заказчика
Управление пользователями и ролями	Заказчик; разработчик обеспечивает предусмотренные сервисом средства управления	Заказчик

Область ответственности	Облачный сервис	Развертывание в инфраструктуре заказчика
Корпоративная система единого входа	Настраивается совместно при необходимости	Настраивается заказчиком при необходимости
Безопасность конечных устройств пользователей	Заказчик	Заказчик
Допустимость передачи и обработки данных	Заказчик в соответствии со своей политикой ИБ	Заказчик
Передача диагностических данных разработчику	В соответствии с регламентом облачного сервиса	Только по решению заказчика и в соответствии с его регламентом ИБ
Масштабирование и обеспечение доступности	Разработчик в пределах параметров облачного сервиса	Заказчик с учетом рекомендаций разработчика

3. СОСТАВ ПОСТАВКИ

Основной принцип поставки: для подключенного и изолированного контуров используется функционально идентичный поставочный комплект для выбранной операционной системы. Различаются способ доставки и, при необходимости, механизм активации, но не доступные функции БАЗИС.

3.1. ЛОГИЧЕСКАЯ СТРУКТУРА

В настоящем разделе приведены функциональные области БАЗИС, имеющие значение для установки, эксплуатации, защиты, мониторинга и восстановления системы. Такое представление не задает обязательный перечень исполняемых сервисов и не фиксирует количество процессов, служб, контейнеров, виртуальных машин или серверных узлов.

В односерверной конфигурации несколько функциональных областей могут быть объединены в одном развертываемом компоненте. В распределенной конфигурации одна функциональная область может быть реализована несколькими экземплярами. Точный состав, наименования и схема размещения развертываемых компонентов определяются поставочным комплектом, манифестом и профилем установки конкретного релиза.

Функциональные области программного комплекса представлены в таблице 4.

Таблица 4. Логическая структура программного комплекса

Функциональная область	Назначение	Эксплуатационное значение
Пользовательский доступ и веб-интерфейс	Предоставление пользователям доступа к функциям БАЗИС через веб-браузер	Пользовательский доступ предоставляется по HTTPS. DNS-имя и сертификат определяются владельцем эксплуатационного контура
Аутентификация и управление доступом	Проверка учетных записей, назначение ролей и интеграция с корпоративной системой единого входа	Пользователям предоставляются минимально необходимые права; параметры интеграции определяются конфигурацией конкретного контура
Прикладные функции	Управление проектами, исходными данными, настройками и расчетными заданиями	Внутренние служебные интерфейсы не предоставляются для прямого пользовательского доступа
Выполнение расчетов	Выполнение расчетных операций и формирование результатов	Требования к ресурсам, количеству экземпляров и масштабированию определяются профилем установки конкретного релиза
Управление фоновыми и расчетными заданиями	Передача, планирование и контроль выполнения заданий	Внутренние механизмы обработки заданий доступны только серверным компонентам

Функциональная область	Назначение	Эксплуатационное значение
Хранение структурированных данных	Хранение метаданных проектов, настроек и иных согласованно изменяемых данных	Требуются контроль целостности, резервное копирование и согласованное восстановление
Хранение файлов и результатов	Хранение файлов проектов, расчетных результатов и других создаваемых системой материалов	Требуются контроль емкости и резервное копирование, согласованное с резервированием структурированных данных
Мониторинг и журналирование	Контроль работоспособности, ресурсов, событий, предупреждений и ошибок	Сроки хранения, состав и порядок передачи журналов определяются регламентом владельца эксплуатационного контура

3.2. СОСТАВ ПРЕДОСТАВЛЕНИЯ ОБЛАЧНОГО СЕРВИСА

При использовании облачного сервиса установка серверной части в инфраструктуре заказчика не выполняется. Для начала эксплуатации разработчик предоставляет заказчику следующие сведения и возможности:

- адрес промышленного облачного сервиса;
- учетные записи пользователей либо параметры настройки корпоративного входа;
- пользовательскую и применимую эксплуатационную документацию;
- регламент обслуживания и обновления сервиса;
- порядок обращения в техническую поддержку;
- сведения о поддерживаемых средствах доступа и известных ограничениях.

ПРИМЕЧАНИЕ. Серверные пакеты, программные образы, исходные тексты, средства сборки и административный доступ к инфраструктуре облачного сервиса заказчику не предоставляются.

3.3. ПОСТАВОЧНЫЙ КОМПЛЕКТ ДЛЯ ИНФРАСТРУКТУРЫ ЗАКАЗЧИКА

Состав и формат поставочного комплекта могут уточняться по мере развития продукта. Форма развертываемых компонентов — исполняемые пакеты, установочные комплекты, программные образы либо их сочетание — определяется паспортом конкретного релиза. Поставочный комплект не содержит исходных текстов, репозиториев и внутренних средств сборки.

Состав поставочного комплекта приведен в таблице 5.

Таблица 5. Состав поставочного комплекта

Элемент	Содержание
Манифест релиза	Версия, состав поставки, совместимость, контрольные суммы и сведения об электронной подписи

Элемент	Содержание
Поставочный комплект для Windows Server	Подписанные исполняемые пакеты, образы и средства установки, предусмотренные для поддерживаемых редакций Windows Server
Поставочный комплект для Linux	Подписанные исполняемые пакеты, образы и средства установки, предусмотренные для поддерживаемых дистрибутивов Linux
Шаблоны конфигурации	Примеры и шаблоны эксплуатационных параметров без паролей, ключей и иных секретов
Средства предварительной проверки	Проверка операционной системы, ресурсов, сетевых параметров, прав доступа и других обязательных условий установки
Средства обновления и миграции	Управляемая установка обновления, преобразование данных и предусмотренные релизом средства отката
Эксплуатационная документация	Руководство по установке и эксплуатации, паспорт релиза, матрица совместимости, известные ограничения и порядок обращения в поддержку
Лицензия	Подписанный лицензионный файл или иной предусмотренный договором механизм активации
Сведения о программных компонентах	SBOM или иной перечень сторонних компонентов, если его предоставление предусмотрено договором или требованиями заказчика

4. ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ

Настоящий раздел устанавливает требования к инфраструктуре заказчика, в которой развертывается программный комплекс. Для облачного сервиса вычислительная инфраструктура предоставляется и эксплуатируется разработчиком; требования к рабочим местам пользователей применяются в полном объеме.

Приведенные значения предназначены для предварительного планирования. Обязательные требования к конкретной версии, поддерживаемые сочетания операционных систем и инфраструктурных компонентов, а также состав сетевых взаимодействий фиксируются в паспорте релиза и матрице совместимости. Перед промышленным вводом параметры уточняются с учетом ожидаемой нагрузки, объема данных, требований к доступности и результатов нагрузочных испытаний.

4.1. ОБЩИЕ ТРЕБОВАНИЯ

Серверная часть может размещаться на физических серверах или виртуальных машинах. Односерверная конфигурация объединяет функции программного комплекса на одном узле; распределенная конфигурация размещает отдельные функции на нескольких узлах и допускает их независимое масштабирование.

- 64-разрядная серверная платформа архитектуры x86_64;
- выделение гарантированных ресурсов процессора и оперативной памяти; длительная переподписка ресурсов, способная влиять на время расчетов, не допускается;
- дисковая подсистема с производительностью, достаточной для одновременной работы с проектами, результатами и журналами; для рабочих данных рекомендуется SSD;
- работоспособные службы DNS и синхронизации времени для всех узлов контура;
- мониторинг доступности, загрузки процессора, использования памяти, дискового пространства и состояния прикладных функций;
- размещение резервных копий вне рабочего сервера или узла данных.

4.2. МИНИМАЛЬНЫЕ И РЕКОМЕНДУЕМЫЕ КОНФИГУРАЦИИ

Для предварительного определения состава оборудования применяются конфигурации, приведенные в таблице 6. Каждая строка описывает самостоятельный вариант развертывания.

Показатель vCPU соответствует количеству виртуальных процессорных ядер, выделяемых программному комплексу. При установке на физический сервер эквивалентный процессорный ресурс определяется с учетом характеристик процессора и правил платформы виртуализации. Для расчетных узлов должны выделяться гарантированные ресурсы без длительного превышения фактической вычислительной мощности сервера.

Таблица 6. Сводные конфигурации для планирования серверных ресурсов

Вариант развертывания	Состав	vCPU	Оперативная память	Выделяемая дисковая емкость с резервом свободного места
Минимальная конфигурация для пилотной эксплуатации	Один сервер	8	32 ГБ	От 300 ГБ SSD
Рекомендуемая односерверная производственная конфигурация	Один сервер	16	64 ГБ	От 1,5 ТБ SSD
Базовая распределенная конфигурация без дублирования узлов	Пять функциональных узлов	32–40	112 ГБ	От 1,6 ТБ
Распределенная отказоустойчивая конфигурация	Дублированные узлы и/или кластеры по проектной схеме	По проекту	По проекту	По проекту

Дисковая емкость в таблице включает рекомендуемый резерв не менее 30 процентов свободного пространства. Расчетный рабочий объем составляет 200 ГБ для пилотной конфигурации, 1 ТБ для односерверной производственной конфигурации и не менее 1,1 ТБ для базовой распределенной конфигурации. Значения емкости округлены вверх.

В приведенные значения не включены пространство для резервных копий, дополнительный запас для роста объема данных, резервные серверы, а также лицензии на операционные системы, платформу виртуализации и внешние инфраструктурные продукты. Эти затраты рассчитываются отдельно в соответствии с требованиями заказчика.

Наличие доступа в Интернет не влияет на базовую потребность в вычислительных ресурсах. Для подключенного и изолированного контуров различаются порядок доставки обновлений и сетевые правила, но не состав расчетной нагрузки.

В таблице 7 представлен расчет ресурсов базовой распределенной конфигурации.

Таблица 7. Ресурсы узлов базовой распределенной конфигурации

Узел	vCPU	Оперативная память	Рабочее дисковое пространство без резерва
Узел прикладных функций	8	16 ГБ	100 ГБ SSD
Узел выполнения расчетов	8–16	32 ГБ	100 ГБ SSD
Узел структурированных данных	8	32 ГБ	300 ГБ SSD
Узел мониторинга и журналирования	4	16 ГБ	100 ГБ SSD

Узел	vCPU	Оперативная память	Рабочее дисковое пространство без резерва
Узел хранения файлов и результатов	4	16 ГБ	500 ГБ
Итого для базовой распределенной конфигурации	32–40	112 ГБ	От 1,1 ТБ

Итоговая строка рассчитана для одного экземпляра каждого узла и не предусматривает отказоустойчивого дублирования. При увеличении количества экземпляров суммарные ресурсы соответствующей роли рассчитываются пропорционально количеству экземпляров и прибавляются к общему итогу. Например, второй расчетный узел дополнительно требует 8–16 vCPU, 32 ГБ оперативной памяти и 100 ГБ рабочего дискового пространства.

При использовании совместимых корпоративных средств хранения или мониторинга отдельные узлы могут быть исключены из поставочной схемы после согласования с разработчиком. При этом заказчик обеспечивает ресурсы и емкость не ниже значений, предусмотренных соответствующим профилем.

Приведенные характеристики применяются для предварительного расчета. Обязательные минимальные и рекомендуемые значения для конкретной версии устанавливаются паспортом релиза с учетом расчетной нагрузки, объема данных и требований к доступности.

4.3. ПОДДЕРЖИВАЕМОЕ СЕРВЕРНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Серверная часть поддерживает 64-разрядные операционные системы следующих семейств:

- Microsoft Windows Server 2022 и Windows Server 2025;
- Astra Linux Special Edition 1.7 и 1.8;
- РЕД ОС 8;
- Debian 12 и 13.

Точные редакции, уровни обновлений операционной системы, версии ядра и поддерживаемые сочетания компонентов указываются в матрице совместимости релиза. Наличие более новой версии операционной системы или инфраструктурного компонента само по себе не означает подтвержденную совместимость.

Необходимые среды выполнения и инфраструктурные зависимости входят в поставочный комплект либо перечисляются в инструкции и матрице совместимости. Для изолированного контура все требуемые пакеты передаются в составе офлайн-поставки; установка из общедоступных репозиториев не требуется. При использовании внешних систем хранения или иных инфраструктурных сервисов применяются только версии и конфигурации, подтвержденные для соответствующего релиза.

4.4. ТРЕБОВАНИЯ К РАБОЧЕМУ МЕСТУ ПОЛЬЗОВАТЕЛЯ

Рабочие места пользователей могут работать под управлением РЕД ОС, других поддерживаемых операционных систем Linux, а также Windows 10 или Windows 11. Операционная система рабочего места не зависит от операционной системы сервера. Доступ к программному комплексу осуществляется через поддерживаемый веб-браузер по протоколу HTTPS; установка отдельной клиентской программы не требуется.

Требования к рабочему месту пользователя приведены в таблице 8.

Таблица 8. Требования к рабочему месту пользователя

Параметр	Минимальное значение	Рекомендуемое значение
Процессор	2 ядра	4 ядра и более
Оперативная память	8 ГБ	16 ГБ и более
Экран	1920 × 1080	1920 × 1080 и выше
Операционная система	РЕД ОС, другая поддерживаемая ОС Linux, Windows 10 или Windows 11	Корпоративно стандартизованная версия РЕД ОС либо иной ОС из матрицы совместимости
Сетевой доступ	Доступ к адресу БАЗИС по HTTPS	Стабильное подключение к сети размещения БАЗИС

Поддерживаются браузеры на базе Chromium, включая Google Chrome, Chromium, Microsoft Edge и Яндекс Браузер, а также Mozilla Firefox и Firefox ESR. Конкретные сочетания операционной системы и версии браузера указываются в матрице совместимости релиза.

4.5. ТРЕБОВАНИЯ К СЕТИ, ВРЕМЕНИ И СЕРТИФИКАТАМ

Требования к сети, времени и сертификатам приведены в таблице 9.

Таблица 9. Требования к сети, времени и сертификатам

Область	Требование
Пользовательский доступ	Доступ к БАЗИС по протоколу HTTPS; по умолчанию используется TCP-порт 443
Публикация сервера	Для развертывания в инфраструктуре заказчика публикация сервера в Интернете не требуется. Пользователи подключаются по внутреннему адресу или через предусмотренный заказчиком защищенный канал
Внутренние взаимодействия	Разрешаются только между согласованными узлами развертывания. Перечень внутренних портов и направлений соединений приводится в профиле установки конкретного релиза
Разрешение имен и время	Для всех узлов должны быть доступны корпоративные DNS и доверенный источник синхронизации времени
Сертификат	Для имени сервиса устанавливается действующий сертификат, которому доверяют рабочие места пользователей. Закрытый ключ хранится средствами, принятыми у владельца контура
Контур с доступом в Интернет	Доступ в Интернет используется только для предусмотренного способа получения подписанных обновлений и не требует входящего административного доступа со стороны разработчика

Область	Требование
Изолированный контур	Исходящие соединения в Интернет отсутствуют. Обновления и сопроводительные материалы переносятся через контролируемую границу по регламенту заказчика

4.6. АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ДОСТУПОМ

В зависимости от конфигурации релиза БАЗИС использует локальные учетные записи либо интегрируется с корпоративным поставщиком удостоверений. Заказчик определяет состав пользователей, назначает роли и обеспечивает актуальность учетных записей.

Включение сервера и рабочих мест в домен Active Directory не является универсальным требованием. Оно выполняется только тогда, когда выбранная заказчиком схема аутентификации или его внутренние правила информационной безопасности требуют доменного членства. Параметры интеграции и доверия фиксируются в профиле установки.

4.7. ПЛАНИРОВАНИЕ ЕМКОСТИ, РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

Емкость хранения определяется с учетом количества проектов и их версий, объема исходных данных и расчетных результатов, сроков хранения журналов, частоты резервного копирования и глубины хранения резервных копий.

- рабочие данные и их резервные копии размещаются на независимых носителях или в независимых системах хранения;
- в односерверной конфигурации единственная резервная копия не должна находиться на том же сервере;
- при раздельном хранении структурированных данных, файлов и результатов резервное копирование выполняется согласованно, чтобы обеспечить целостное восстановление;
- периодичность копирования и срок хранения определяются целевыми показателями допустимой потери данных и времени восстановления заказчика;
- восстановление из резервной копии проверяется до промышленного ввода и затем периодически по эксплуатационному регламенту;
- для рабочих томов рекомендуется сохранять не менее 30 процентов свободного пространства и настроить предупреждения, например, при заполнении 70, 85 и 95 процентов.

5. ПОДГОТОВКА К РАЗВЕРТЫВАНИЮ В ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА

Раздел применяется к односерверному и распределенному развертыванию БАЗИС в подключенном либо изолированном контуре заказчика. Подготовку выполняет администратор заказчика с необходимыми полномочиями. Требования конкретной версии уточняются по паспорту релиза и матрице совместимости.

5.1. ИСХОДНЫЕ ДАННЫЕ

До начала развертывания необходимо определить и согласовать исходные данные, приведенные в таблице 10.

Таблица 10. Исходные данные для развертывания

Область	Требуется определить
Схема размещения	Односерверная или распределенная схема; подключенный или изолированный контур
Серверная платформа	Windows или Linux, редакция и версия ОС, архитектура процессора, ограничения виртуализации
Ресурсы	Количество узлов, процессорные ресурсы, оперативная память, рабочее и резервное дисковое пространство
Сетевое взаимодействие	DNS-имя сервиса, адреса узлов, порт HTTPS, маршруты и разрешенные межсетевые соединения
Аутентификация	Корпоративный поставщик удостоверений либо локальные учетные записи; группы, роли и первичный администратор
Внешние компоненты	Адреса, сертификаты и служебные учетные записи инфраструктурных компонентов, если они размещаются отдельно
Защита данных	Место хранения резервных копий, требуемые значения RPO/RTO, срок хранения и контур тестового восстановления
Организация работ	Окно установки, ответственные лица, порядок согласования изменений и допустимость передачи диагностических данных

5.2. ПРЕДВАРИТЕЛЬНАЯ ПРОВЕРКА

1. Сверить операционную систему и аппаратные ресурсы каждого узла с паспортом релиза, матрицей совместимости и выбранным профилем нагрузки.
2. Проверить разрешение DNS-имен, синхронизацию системного времени, доверие к сертификатам и доступность только тех сетевых маршрутов, которые требуются выбранной схеме.
3. Проверить готовность внешних инфраструктурных компонентов, если они не входят в поставку и размещаются на отдельных узлах.
4. Создать служебные учетные записи с минимально необходимыми правами и подготовить защищенное средство хранения секретов.

5. Подготовить рабочие каталоги и места для хранения журналов и резервных копий. Резервные копии не должны храниться только на том же узле, что и рабочие данные.
6. Убедиться, что релизный комплект получен и проверен в соответствии с разделом 6.
7. Зафиксировать исходное состояние системы, согласовать окно установки и порядок возврата к исходному состоянию.

ВАЖНО. Резервная копия перед началом работ. При первичной установке на новый узел резервное копирование данных БАЗИС не требуется. При обновлении, переустановке или изменении существующей конфигурации резервная копия и контрольная точка восстановления обязательны.

5.3. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В командах и примерах паспорта релиза значения в угловых скобках заменяются параметрами конкретной установки.

Условные обозначения, используемые в паспорте релиза, приведены в таблице 11.

Таблица 11. Условные обозначения

Обозначение	Содержание
<версия>	Версия устанавливаемого релиза БАЗИС
<каталог_поставки>	Защищенный каталог, в который помещен проверенный релизный комплект
<DNS-имя_сервиса>	Согласованное DNS-имя пользовательской точки входа
<профиль_развертывания>	Односерверный профиль либо роль узла в распределенной схеме
<имя_службы>	Имя системной службы, указанное в паспорте релиза
<каталог_журналов>	Каталог хранения эксплуатационных журналов

6. ПОЛУЧЕНИЕ И ПРОВЕРКА РЕЛИЗНОГО КОМПЛЕКТА

Релизный комплект является единственным штатным источником установки и обновления БАЗИС в инфраструктуре заказчика. Он содержит исполняемые программные компоненты и эксплуатационные материалы, но не включает исходный код и средства сборки и не предоставляет доступа к репозиториям разработки.

6.1. СОСТАВ РЕЛИЗНОГО КОМПЛЕКТА

Релизный комплект включает следующие элементы:

- исполняемые пакеты, образы или установочные файлы для поддерживаемой серверной платформы и выбранной схемы размещения;
- штатный установщик или сценарий развертывания;
- подписанный манифест состава и контрольные суммы;
- паспорт релиза с версиями, требованиями, известными ограничениями и поддерживаемыми маршрутами обновления;
- матрица совместимости и профиль установки;
- лицензионные данные и инструкция по их применению;
- инструкция по обновлению и откату, если комплект предназначен для обновления;
- перечень компонентов сторонних разработчиков или SBOM, если его предоставление предусмотрено договором или обязательными требованиями.

6.2. ПОДКЛЮЧЕННЫЙ КОНТУР

Комплект передается через предусмотренный договором защищенный канал. Доступ в Интернет может использоваться для уведомления о выпуске версии и получения пакета, но не означает автоматическую установку. Решение о начале установки или обновления принимает администратор заказчика.

6.3. ИЗОЛИРОВАННЫЙ КОНТУР

Комплект переносится на согласованном носителе либо через контролируемый шлюз межконтурного обмена. До ввода в изолированный контур выполняются антивирусная проверка, регистрация носителя, сверка состава и контрольных сумм, а также проверка электронной подписи. Обратная передача журналов или диагностических материалов допускается только по решению владельца данных и через утвержденный канал.

ВАЖНО. Автономность поставки. Штатная установка в изолированном контуре не должна требовать загрузки пакетов из внешних репозиториев, обращения к публичным службам лицензирования или подключения к инфраструктуре разработчика.

6.4. ОБЯЗАТЕЛЬНЫЕ ПРОВЕРКИ

1. Сверить версию, назначение и состав комплекта с паспортом релиза.
2. Проверить электронную подпись манифеста и подписываемых объектов в объеме, установленном схемой поставки.
3. Сравнить контрольные суммы с подписанным манифестом.

4. Проверить, что лицензия выдана для требуемой организации, редакции и схемы развертывания.
5. Сохранить проверенный комплект в защищенном архиве релизов с ограниченным доступом.

ВНИМАНИЕ. Несоответствие комплекта. Пакет с неподтвержденной подписью, несовпадающей контрольной суммой, неполным составом или неподходящей лицензией не устанавливается. Такой пакет изолируется, а сведения о несоответствии передаются в техническую поддержку.

7. ПРЕДОСТАВЛЕНИЕ ДОСТУПА К ОБЛАЧНОМУ СЕРВИСУ

При использовании облачного сервиса (SaaS) установка серверной части заказчиком не выполняется. Организация получает адрес сервиса и согласованный способ аутентификации. Пользователи работают с сервисом в поддерживаемом веб-браузере. Рабочие места пользователей соответствуют требованиям раздела 4.

7.1. ИСХОДНЫЕ СВЕДЕНИЯ

Для предоставления доступа необходимы следующие исходные сведения:

- URL промышленного контура;
- согласованный способ аутентификации: учетные записи сервиса либо подключение корпоративного поставщика удостоверений;
- ответственный администратор организации;
- перечень пользователей, групп и требуемых ролей;
- ограничения на состав данных, которые разрешено передавать в облачный сервис.

7.2. ПРЕДОСТАВЛЕНИЕ И ПРОВЕРКА ДОСТУПА

1. Проверить доступность URL с рабочих мест пользователей и корректность защищенного HTTPS-соединения.
2. Создать администратора организации и пользователей либо настроить сопоставление корпоративных групп.
3. Назначить минимально необходимые роли и выполнить вход под учетной записью тестового пользователя.
4. Создать контрольный проект, выполнить разрешенную проверочную операцию и убедиться, что результат сохраняется.
5. Зафиксировать приемку доступа и перечень уполномоченных администраторов организации.

ПРИМЕЧАНИЕ. Ограничение доступа. Организации не передаются серверные пакеты облачного контура, исходный код или административный доступ к инфраструктуре разработчика. Экспорт пользовательских данных выполняется предусмотренными продуктом средствами.

8. УСТАНОВКА В ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА

БАЗИС устанавливается из подписанного релизного комплекта, предназначенного для целевой серверной платформы. Настоящий раздел устанавливает общий порядок. Точные имена файлов и образов, команды запуска, системные службы, каталоги, порты и ожидаемые результаты приводятся в паспорте соответствующего релиза.

8.1. ОБЩАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ

1. Получить и проверить релизный комплект в соответствии с разделом 6.
2. Заполнить карточку параметров установки и выбрать профиль размещения.
3. Запустить включенную в комплект предварительную проверку и устранить блокирующие замечания.
4. Установить исполняемые компоненты выбранного профиля штатным средством поставки.
5. Применить эксплуатационную конфигурацию, сертификат и лицензионные данные.
6. Зарегистрировать системные службы и настроить их запуск от выделенных служебных учетных записей.
7. Выполнить проверку готовности и оформить результат в соответствии с разделом 10.

Паспорт релиза должен содержать достаточные сведения для выполнения установки без обращения к исходному коду или среде разработки.

Сведения паспорта релиза и их назначение приведены в таблице 12.

Таблица 12. Сведения паспорта релиза

Сведения паспорта релиза	Назначение
Имена и версии пакетов, образов или установочных файлов	Однозначный выбор устанавливаемых объектов
Команда или способ запуска	Запуск штатного установщика либо сценария развертывания
Параметры установки	Заполнение профиля без изменения внутренних файлов приложения
Системные службы и команды управления	Проверка состояния, запуск, остановка и перезапуск
Сетевые порты и каталоги	Настройка межсетевого взаимодействия, журналов и резервного копирования
Команда определения версии	Подтверждение установленной версии и состава
Критерии успешного завершения	Проверка результата установки

8.2. УСТАНОВКА НА WINDOWS

Установка выполняется пользователем с полномочиями локального администратора на сервере под управлением поддерживаемой версии Windows либо с помощью средств централизованного управления, разрешенных политиками заказчика.

1. Поместить проверенный релизный комплект во временный каталог с доступом только для администратора установки.

2. Повторно проверить подпись и контрольные суммы непосредственно на целевом узле.
3. Запустить штатный установщик или сценарий Windows, указанный в паспорте релиза.
4. Выбрать односерверный профиль либо роль узла в распределенной схеме и передать только требуемые эксплуатационные параметры.
5. Подтвердить создание выделенных служебных учетных записей или указать заранее подготовленные учетные записи. Постоянная работа служб от имени локального администратора не допускается, если иное прямо не установлено паспортом релиза.
6. Применить только согласованные правила межсетевого экрана и права на каталоги. Секреты не должны передаваться в открытом виде через командную строку или сохраняться в журналах установки.
7. Проверить состояние созданных служб, установленную версию и журнал установки.
8. После приемки удалить временную копию комплекта либо переместить ее в защищенный архив релизов.

8.3. УСТАНОВКА НА LINUX

Установка выполняется на сервере под управлением поддерживаемой версии Linux из локального релизного комплекта или локального репозитория заказчика. Подключение к публичным репозиториям для штатной установки не требуется.

1. Поместить проверенный релизный комплект в каталог, доступный только администратору установки.
2. Повторно сверить контрольные суммы и подпись непосредственно на целевом узле.
3. Запустить штатный установочный сценарий, пакетный менеджер или средство развертывания, указанное в паспорте релиза.
4. Выбрать односерверный профиль либо роль узла и применить подготовленные эксплуатационные параметры.
5. Создать или подтвердить выделенные системные учетные записи без интерактивного входа. Ограничить права на исполняемые файлы, конфигурацию, секреты, журналы и рабочие каталоги.
6. Зарегистрировать службы в используемой системе управления службами и включить их автоматический запуск, если это предусмотрено профилем.
7. Применить согласованные правила межсетевого экрана и политики обязательного контроля доступа, если они используются заказчиком.
8. Проверить состояние служб, установленную версию и журнал установки, затем перенести комплект в защищенный архив релизов.

8.4. РАСПРЕДЕЛЕННОЕ РАЗВЕРТЫВАНИЕ

При распределенной схеме каждый узел устанавливается в соответствии с назначенной ролью и паспортом релиза. Последовательность развертывания определяется зависимостями конкретной версии. После установки каждого узла проверяются готовность узла, наличие защищенного соединения с разрешенными смежными узлами и отсутствие доступа к неиспользуемым сетевым ресурсам.

ПРИМЕЧАНИЕ. Единые критерии. Формат пользовательских данных, функциональные возможности и критерии приемки не зависят от выбранной серверной платформы.

Платформенные различия ограничиваются составом установочного комплекта, регистрацией служб, путями файловой системы и командами администрирования.

9. ПЕРВИЧНАЯ НАСТРОЙКА

9.1. ПАРАМЕТРЫ СРЕДЫ

Первичная настройка выполняется с помощью штатного установщика, конфигурационного шаблона или средства управления, входящих в релизный комплект. Ручное изменение внутренних файлов приложения допускается только тогда, когда это прямо предусмотрено паспортом релиза.

Основные группы параметров первичной настройки приведены в таблице 13.

Таблица 13. Параметры первичной настройки

Группа параметров	Содержание
Точка входа	DNS-имя сервиса, порт HTTPS, сертификат и цепочка доверия
Схема размещения	Идентификатор среды, роли узлов и разрешенные адреса взаимодействия
Хранение данных	Адреса, защищенные учетные данные и параметры компонентов хранения, если они размещены отдельно
Аутентификация	Локальные учетные записи либо параметры поддерживаемого корпоративного поставщика удостоверений, сопоставление групп и ролей
Лицензирование	Подписанные лицензионные данные и условия их применения в подключенном или изолированном контуре
Журналы и мониторинг	Каталоги, срок хранения, уровень журналирования и разрешенные средства сбора показателей
Резервное копирование	Место хранения, расписание, срок хранения и параметры контроля успешности
Региональные параметры	Часовой пояс, язык интерфейса и формат времени, если они настраиваются на уровне системы
ВНИМАНИЕ. Защита секретов. Пароли, токены, закрытые ключи и иные секреты хранятся только в средстве защищенного хранения, предусмотренном платформой и политикой заказчика. Они не включаются в открытые архивы, эксплуатационные журналы, протоколы и обращения в техническую поддержку.	

9.2. АУТЕНТИФИКАЦИЯ И РОЛИ

При настройке аутентификации и ролей следует соблюдать следующие требования:

- назначать роли по служебной необходимости и не предоставлять постоянные расширенные полномочия без обоснования;
- разделять администрирование платформы и работу с пользовательскими проектами, если это предусмотрено ролевой моделью релиза;
- использовать персональные учетные записи и не применять общие учетные записи нескольких работников;

- регулярно пересматривать активные учетные записи, роли и сопоставление корпоративных групп;
- защитить учетную запись первичного или аварийного администратора и использовать ее только по утвержденному регламенту.

При подключении корпоративного поставщика удостоверений точный протокол, обязательные атрибуты и допустимые варианты сопоставления определяются паспортом релиза и согласованной схемой интеграции.

9.3. ЗАВЕРШЕНИЕ НАСТРОЙКИ

1. Применить конфигурацию и выполнить требуемый перезапуск служб.
2. Проверить отсутствие ошибок запуска и предупреждений о недостающих параметрах.
3. Сформировать обезличенное описание конфигурации: версия, схема размещения, узлы, порты и внешние зависимости без секретов.
4. Сохранить конфигурационный шаблон и описание в защищенном эксплуатационном архиве.

10. ПРОВЕРКА И ВВОД В ЭКСПЛУАТАЦИЮ

После установки выполняется приемочная проверка. Проверка подтверждает не только запуск компонентов, но и возможность выполнения основного пользовательского сценария.

Критерии приемки программного комплекса приведены в таблице 14.

Таблица 14. Критерии приемки

Проверка	Критерий приемки
Версия и состав	Установленная версия, профиль и роли узлов соответствуют паспорту релиза
Готовность служб	Все обязательные службы находятся в состоянии готовности; циклические перезапуски и блокирующие ошибки отсутствуют
HTTPS	Пользовательский URL доступен, сертификат действителен, ему доверяют рабочие места и он соответствует DNS-имени; незащищенный доступ не используется
Аутентификация	Администратор и тестовый пользователь входят согласованным способом; роли и ограничения доступа различаются ожидаемым образом
Хранение данных	Выполняются разрешенные операции создания, чтения и сохранения данных; ошибки целостности отсутствуют
Контрольный расчет	Контрольный проект открывается, задание завершается, результат отображается и сохраняется
Журналы и мониторинг	События доступны уполномоченному администратору; секреты и закрытые ключи в журналах отсутствуют; основные показатели поступают в средство мониторинга
Резервное копирование	Создана первая согласованная резервная копия, проверены ее состав и читаемость; тестовое восстановление выполнено либо запланировано утвержденным регламентом
Перезапуск	После контролируемого перезапуска узла или служб система возвращается в состояние готовности без ручного исправления конфигурации

Результат оформляется протоколом ввода в эксплуатацию. В протоколе указываются версия, схема размещения, перечень узлов, дата, исполнитель, результаты проверок, известные ограничения, контрольная точка восстановления и согласованные отклонения.

11. ШТАТНАЯ ЭКСПЛУАТАЦИЯ

11.1. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ

Периодичность контроля устанавливается эксплуатационным регламентом заказчика с учетом критичности системы и режима ее использования. Контролируются:

- доступность пользовательского URL и готовность обязательных служб;
- количество ожидающих и выполняемых расчетных заданий, доля ошибок и длительность операций;
- загрузка процессора, оперативной памяти и дисков, а также свободная емкость хранилищ;
- ошибки приложения, инфраструктуры и аутентификации;
- успешность резервного копирования и результаты периодических тестов восстановления;
- срок действия сертификатов, лицензионных данных и служебных учетных записей;
- целостность журналирования и доступность средств мониторинга.

11.2. ЗАПУСК И ОСТАНОВКА

Запуск, остановка и перезапуск выполняются только штатными средствами релизного комплекта. Точные команды и последовательность для конкретной версии приводятся в паспорте релиза.

Перед плановой остановкой прекращается прием новых пользовательских и расчетных заданий, ожидается завершение допустимых операций и, если остановка связана с изменением системы, создается контрольная точка восстановления. После запуска проверяются состояние служб, пользовательский URL, аутентификация и выполнение контрольной операции.

11.3. УПРАВЛЕНИЕ ЕМКОСТЬЮ И ПРОИЗВОДИТЕЛЬНОСТЬЮ

При устойчивом увеличении времени выполнения расчетов сначала анализируются профиль нагрузки, используемые ресурсы, состояние хранилищ и число параллельных расчетов. Изменение ресурсов, числа расчетных процессов или схемы размещения выполняется после резервного копирования, фиксации исходной конфигурации и проверки совместимости. Для перехода от односерверной к распределенной схеме используется утвержденный профиль миграции.

11.4. РЕГЛАМЕНТНЫЕ РАБОТЫ

К регламентным работам относятся:

- продление и замена сертификатов до окончания срока их действия;
- актуализация лицензии в порядке, установленном договором;
- пересмотр ролей, служебных и пользовательских учетных записей;
- контроль ротации журналов и удаление временных данных только штатными средствами;
- проверка доступности резервных копий и выполнение тестового восстановления;
- проверка наличия поддерживаемых обновлений и уведомлений о существенных ограничениях.

12. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

12.1. ОБЪЕКТЫ РЕЗЕРВНОГО КОПИРОВАНИЯ

Объекты резервного копирования и требования к ним приведены в таблице 15.

Таблица 15. Объекты резервного копирования

Объект	Требование
Структурированные данные	Согласованная полная или инкрементальная копия с обеспечением целостности транзакций
Файлы проектов и результаты	Согласованная копия пользовательских файлов, расчетных результатов и иных сохраняемых объектов
Конфигурация	Профиль размещения, эксплуатационные параметры и перечень внешних зависимостей без открытых секретов
Секреты и сертификаты	Отдельная защищенная копия средствами заказчика; закрытые ключи не включаются в обычный архив данных
Лицензионные данные	Защищенная копия действующих подписанных данных и сведений об их применении
Журналы аудита	Копирование в соответствии со сроком хранения и требованиями расследования событий

12.2. СОЗДАНИЕ РЕЗЕРВНОЙ КОПИИ

1. Зафиксировать установленную версию БАЗИС, схему размещения и состав резервируемых объектов.
2. Перевести систему в согласованное состояние либо использовать поддерживаемый механизм согласованного копирования без остановки.
3. Создать согласованные копии структурированных данных и файловых объектов, соответствующие одной логической точке времени.
4. Сохранить конфигурацию, лицензионные данные и необходимые сведения о сертификатах отдельно от рабочих данных.
5. Проверить завершение процедуры, контрольные суммы, состав и читаемость копии.
6. Перенести копию за пределы зоны отказа рабочего узла и зарегистрировать ее в журнале резервного копирования.

12.3. ВОССТАНОВЛЕНИЕ

1. Подготовить поддерживаемую версию серверной платформы и БАЗИС, совместимую с восстанавливаемой копией.
2. Восстановить инфраструктурные компоненты, конфигурацию и защищенные секреты из доверенных источников.
3. Восстановить структурированные данные и файловые объекты из согласованной точки.
4. Запустить БАЗИС и выполнить проверки готовности, аутентификации и контрольного проекта.

5. Зафиксировать фактические значения RPO/RTO, состав восстановленных данных и выявленные отклонения.

ВАЖНО. Регулярная проверка. Наличие файла резервной копии не подтверждает возможность восстановления. Тестовое восстановление выполняется в отдельном контуре с периодичностью, установленной политикой заказчика.

13. МОНИТОРИНГ, ЖУРНАЛЫ И ДИАГНОСТИКА

13.1. РЕКОМЕНДУЕМЫЕ ПОКАЗАТЕЛИ

Рекомендуется контролировать следующие показатели:

- готовность прикладных и расчетных компонентов;
- число ожидающих, выполняющихся и завершившихся с ошибкой заданий, а также продолжительность расчетов;
- загрузка процессора и памяти, свободная дисковая емкость и задержки операций хранения;
- доступность компонентов хранения данных и внешних зависимостей;
- частота серверных ошибок, отказов аутентификации и повторных запусков служб;
- время последнего успешного резервного копирования и результат последнего тестового восстановления;
- срок действия сертификатов, лицензии и служебных учетных данных.

13.2. ЭКСПЛУАТАЦИОННЫЕ ЖУРНАЛЫ

Журналы должны содержать дату и время, идентификатор узла или компонента, уровень события, код и краткое описание. Системное время узлов синхронизируется. Доступ к журналам ограничивается уполномоченными администраторами, а срок хранения и правила ротации устанавливаются политикой заказчика. Пароли, токены, закрытые ключи и полное содержимое пользовательских проектов в журналы не записываются.

Для диагностики допускается временное повышение уровня журналирования в соответствии с паспортом релиза. После завершения анализа уровень возвращается к штатному, чтобы избежать избыточного объема данных и риска раскрытия конфиденциальных сведений.

13.3. ДИАГНОСТИЧЕСКИЙ ПАКЕТ

Диагностический пакет формирует администратор штатным средством релиза. Перед передачей администратор проверяет период, за который сформированы данные, состав и размер пакета, а также отсутствие секретов. Передача пакета из инфраструктуры заказчика выполняется только по решению заказчика.

Допустимый состав диагностического пакета приведен в таблице 16.

Таблица 16. Состав диагностического пакета

Может быть включено после проверки администратором	Только по отдельному разрешению владельца данных	Не передается
Версия и номер сборки; обезличенная схема размещения; состояния служб; коды ошибок; показатели ресурсов; фрагменты журналов без секретов и проектных данных	Файлы проектов; персональные данные; полные журналы, содержащие технологические сведения; выгрузки структурированных данных; конфигурация, содержащая чувствительные адреса	Пароли; токены; закрытые ключи; исходный код; средства доступа к внутренней инфраструктуре разработки

13.4. ПЕРЕДАЧА ДИАГНОСТИЧЕСКИХ ДАННЫХ

В подключенном контуре используется предусмотренный договором защищенный канал. В изолированном контуре пакет переносится через контролируемый шлюз или зарегистрированный носитель. Автоматическая отправка телеметрии из инфраструктуры заказчика по умолчанию не выполняется; иной режим допускается только при его явном включении заказчиком и документированном составе передаваемых данных.

14. ОБНОВЛЕНИЕ И ОТКАТ

Настоящий раздел определяет технический порядок обновления. Периодичность выпуска версий, сроки поддержки и обозначение ветвей устанавливаются отдельной утвержденной релизной политикой, паспортом релиза и договором сопровождения.

14.1. ПОРЯДОК ПРИМЕНЕНИЯ ОБНОВЛЕНИЙ

Порядок применения обновлений для различных моделей предоставления приведен в таблице 17.

Таблица 17. Порядок применения обновлений

Модель предоставления	Порядок
Облачный сервис	Обновление выполняет разработчик после внутренних проверок и подготовки к возможному возврату. Пользователям заранее сообщаются существенные изменения в порядке, установленном регламентом сервиса
Инфраструктура заказчика с доступом в Интернет	Администратор получает уведомление и подписанный комплект через защищенный канал. Установку инициирует администратор заказчика. Автоматическая установка по умолчанию не выполняется
Изолированный контур	Подписанный комплект переносится через контролируемую границу, проверяется локально и устанавливается администратором в согласованное окно

14.2. ПОДГОТОВКА К ОБНОВЛЕНИЮ

1. Изучить паспорт релиза, матрицу совместимости, известные ограничения и обязательный маршрут перехода между версиями.
2. Проверить подпись, контрольные суммы и полноту комплекта.
3. Проверить обновление в тестовом контуре или на согласованной копии данных, если этого требует критичность системы.
4. Создать и проверить резервную копию данных, конфигурации и лицензионных сведений.
5. Согласовать окно работ, ответственных лиц, критерии успеха и условия отката.
6. Зафиксировать текущую версию, схему размещения и состояние мониторинга.

14.3. ВЫПОЛНЕНИЕ ОБНОВЛЕНИЯ

1. Прекратить прием новых заданий и дождаться завершения допустимых операций.
2. Остановить службы в порядке, указанном в паспорте релиза.
3. Установить подписанный пакет и выполнить включенные в него преобразования данных и конфигурации.
4. Запустить службы и выполнить сокращенную проверку готовности.
5. Проверить аутентификацию, контрольный проект, журналы, мониторинг и взаимодействие узлов.
6. Зафиксировать новую версию, результаты и выявленные ограничения в протоколе обновления.

14.4. ОТКАТ

Откат выполняется при невыполнении критериев приемки, невозможности устранить блокирующую ошибку в согласованное окно или возникновении риска нарушения целостности данных. Использование предыдущего исполняемого пакета допустимо только при совместимости формата данных. Если обновление изменило структуру или содержание данных несовместимым образом, выполняется документированный обратный переход либо восстановление согласованной резервной копии.

ВАЖНО. Целостность версий. Не допускается длительная эксплуатация несогласованной комбинации компонентов разных версий, если такая комбинация прямо не разрешена паспортом релиза. После отката повторно выполняются проверки раздела 10.

15. УДАЛЕНИЕ

1. Запретить новые подключения и прием новых заданий, уведомить пользователей и завершить активные операции.
2. При необходимости создать финальную резервную копию и выполнить предусмотренный продуктом экспорт пользовательских данных.
3. Остановить и отключить системные службы штатным средством релизного комплекта.
4. Удалить исполняемые компоненты, пакеты или образы штатным средством поставки.
5. Отозвать служебные учетные записи, сертификаты, секреты, лицензии и правила сетевого доступа, которые больше не используются.
6. Сохранить, передать или уничтожить данные, журналы и резервные копии только по утвержденному решению владельца данных.
7. Зафиксировать версию удаленного программного комплекса, перечень сохраненных данных, места их хранения и ответственных лиц.

ВАЖНО. Разделение программных компонентов и данных. Удаление БАЗИС по умолчанию не должно уничтожать данные заказчика. Безвозвратное удаление данных выполняется только по отдельному утвержденному регламенту и подтвержденному перечню объектов.

16. ТИПОВЫЕ НЕИСПРАВНОСТИ

Типовые неисправности и рекомендуемые действия приведены в таблице 18.

Таблица 18. Типовые неисправности и рекомендуемые действия

Симптом	Что проверить	Действие
Пользовательский URL недоступен	DNS, сертификат, сетевой маршрут, входной узел и состояние служб	Устранить сетевую или служебную причину; не отключать HTTPS как постоянное решение
Не выполняется вход	Системное время, поставщик удостоверений, срок сертификата, учетная запись, группы и роли	Восстановить штатный способ аутентификации; аварийную учетную запись применять только по регламенту
Службы не переходят в состояние готовности	Ресурсы, конфигурацию, внешние зависимости и сообщения журналов запуска	Собрать диагностический пакет, устранить причину; не выполнять повторную установку без сохранения журналов
Расчетные задания не запускаются	Лицензию, готовность расчетных узлов, доступность данных, свободные ресурсы и ограничения очередности выполнения	Восстановить недоступный компонент или ресурс; после исправления повторно выполнить контрольное задание
Увеличилось время расчета	Текущую нагрузку, параллельные задания, процессор, память, диски и задержки хранения	Определить узкое место; изменять ресурсы и масштабировать только после анализа и фиксации конфигурации

Симптом	Что проверить	Действие
Недостаточно свободного дискового пространства	Рабочие данные, журналы, временные файлы, локальные резервные копии и незавершенные операции	Расширить емкость и применить согласованную политику хранения; не удалять рабочие данные вручную
Не создается резервная копия	Права, свободное место, доступность места назначения, согласованность данных и журнал процедуры	Устранить причину, повторить копирование и проверить восстановимость; не начинать обновление без подтвержденной копии
Обновление не прошло приемку	Маршрут перехода, совместимость, подпись пакета, преобразования данных, готовность служб и контрольный проект	Прекратить внедрение версии и выполнить документированный откат
Истекает срок сертификата или лицензии	Дату окончания, процедуру продления, цепочку доверия и возможность применения в изолированном контуре	Заранее получить и проверить новые данные, установить их в согласованное окно и повторить проверку готовности

17. ОБРАЩЕНИЕ В ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ

17.1. СВЕДЕНИЯ ДЛЯ ОБРАЩЕНИЯ

При обращении в техническую поддержку следует указать:

- версия и номер сборки БАЗИС, серверная ОС и схема размещения;
- дата и время возникновения, наблюдаемый результат и ожидаемое поведение;
- масштаб влияния, частота повторения и наличие обходного решения;
- последние изменения и уже выполненные безопасные проверки;
- идентификатор операции или задания без раскрытия содержимого проекта;
- проверенный администратором диагностический пакет либо разрешенная его часть.

17.2. ПЕРЕДАЧА МАТЕРИАЛОВ

Канал обращения, режим работы и сроки реакции определяются договором сопровождения или паспортом технической поддержки. В подключенном контуре используется защищенный канал. В изолированном контуре материалы передаются через тот же контролируемый механизм, который применяется для релизных комплектов.

Перед передачей владелец данных определяет допустимый состав материалов. Пароли, токены, закрытые ключи и неразрешенные пользовательские данные в обращение не включаются.

17.3. ПРИМЕНЕНИЕ РЕКОМЕНДАЦИЙ И ИСПРАВЛЕНИЙ

Техническая поддержка анализирует предоставленные сведения и направляет рекомендации либо подписанный комплект исправления. Решение о применении исправления в инфраструктуре заказчика принимает администратор заказчика. Исправление устанавливается по процедуре раздела 14 с обязательной проверкой результата и возможностью отката.

ПРИЛОЖЕНИЕ А. КОНТРОЛЬНЫЙ ЛИСТ ГОТОВНОСТИ

Контрольный лист готовности приведен в таблице 19.

Таблица 19. Контрольный лист готовности

№	Контрольный пункт	Отметка / комментарий
1	Выбраны схема размещения, тип контура, серверные ОС и профиль релиза	
2	Ресурсы каждого узла сверены с разделом 4, паспортом релиза и профилем нагрузки	
3	Подготовлены DNS, системное время, сертификаты, сетевые маршруты и правила межсетевого экранирования	
4	Созданы служебные учетные записи и защищенное хранилище секретов	
5	Подготовлены внешние инфраструктурные компоненты, если они размещаются отдельно	
6	Получены и проверены подпись, контрольные суммы, лицензия и состав релизного комплекта	
7	Определены место резервного копирования, RPO/RTO и порядок тестового восстановления	
8	Согласованы способ аутентификации, первичный администратор, группы и роли	
9	Выполнена установка и зафиксированы версии, службы и роли узлов	
10	Выполнены проверки URL, HTTPS, аутентификации, хранения данных и контрольного расчета	
11	Настроены мониторинг, оповещения, ротация журналов и контроль резервного копирования	
12	Оформлен протокол ввода в эксплуатацию и назначены ответственные лица	