realize_options_sec

Выпуск 0.0.29

июн. 17, 2026

Содержание

1 Общие положения

Раздел описывает встроенные механизмы безопасности системы Global ERP, а также возможности интеграции со сторонними средствами и сервисами безопасности для усиления защиты в процессе эксплуатации.

Встроенные механизмы безопасности системы реализованы в архитектуре и функциональности Global ERP. Они применяются для идентификации и аутентификации пользователей, управления доступом, аудита, журналирования, защиты каналов связи, управления секретами и безопасной обработки запросов.

Система Global ERP в типовой поставке не является готовой автоматизированной системой в защищенном исполнении (АСЗИ). Встроенные механизмы безопасности предоставляют базовый функционал, который конфигурируется и при необходимости дополняется внешними средствами защиты информации в рамках конкретного проекта внедрения. Полное соответствие требованиям ГОСТ Р 51583-2014 и статус АСЗИ достигаются после аттестации в реальных условиях эксплуатации заказчика.

1.1 Область применения

Раздел распространяется на компоненты Global ERP, включая платформу, серверные и клиентские модули, прикладные решения, эксплуатационную документацию и интерфейсы интеграции.

Материалы раздела применяются:

- подразделениями разработки при проектировании и реализации встроенных механизмов безопасности;
- подразделениями внедрения и сопровождения при консультировании заказчиков;
- подразделением информационной безопасности при оценке соответствия системы нормативным требованиям;
- заказчиками при проектировании защищенного контура эксплуатации системы.

1.2 Подходы к обеспечению безопасности

В Global ERP используются два взаимодополняющих подхода:

- **Security by design** — базовые меры информационной безопасности встроены в архитектуру и функциональность системы и обеспечиваются на уровне платформы.
- **Расширяемая модель безопасности** — система предусматривает интеграцию со сторонними средствами и сервисами безопасности, включая внешние системы аутентификации, мониторинга, контроля доступа и защиты инфраструктуры.

Архитектура системы Global ERP реализует следующие принципы безопасности:

- учет требований информационной безопасности на этапе проектирования;
- совместимость с внешними средствами защиты информации и предоставление интерфейсов для их интеграции;
- отсутствие конфликтов встроенных механизмов безопасности с бизнес-функциональностью системы;
- сохранение проектных показателей производительности при работе встроенных механизмов защиты.

1.3 Состав встроенных механизмов

Встроенные механизмы безопасности Global ERP описаны в отдельных страницах раздела:

- **Идентификация и аутентификация** — описывает способы установления пользователя, проверки учетных данных, локальную аутентификацию, парольную политику, защиту от подбора паролей, работу с LDAP, SSO, внешним прокси-сервером авторизации и техническими подключениями.
- **Управление доступом** — описывает категории учетных записей, ролевую модель доступа и контроль привилегий.

- **Безопасность выполнения и обработки запросов** — описывает меры безопасности при выполнении серверной логики, обработке пользовательского ввода и работе HTTP-интерфейсов.
- **Логирование, аудит и управление инцидентами** — описывает регистрацию событий безопасности, аудит действий пользователей, защиту журналов, обработку инцидентов и учет уязвимостей.
- **Инфраструктурная безопасность и сопровождение** — описывает меры безопасности, относящиеся к инфраструктуре, сетевому взаимодействию, защите каналов связи, управлению секретами, резервному копированию и обновлениям.

Страница «Рекомендации по информационной безопасности» содержит эксплуатационные рекомендации и не входит в описание встроенных механизмов безопасности системы.

1.4 Учет требований ГОСТ Р 51583-2014

Процесс создания системы Global ERP учитывает положения ГОСТ Р 51583-2014 в части обеспечения безопасности программного продукта следующими мерами:

- Разработка ведется в соответствии с техническим заданием, в котором на этапе проектирования архитектуры фиксируются требования к подсистеме безопасности.
- Архитектура системы обеспечивает совместимость с внешними средствами защиты информации и предоставляет интерфейсы для их интеграции.
- Встроенные механизмы безопасности не препятствуют нормальному функционированию системы и не снижают ее производительность ниже проектных показателей.
- В жизненный цикл разработки интегрированы обязательные процедуры верификации безопасности: статический анализ кода, автоматизированный анализ зависимостей (SCA), динамическое тестирование веб-интерфейсов и рецензирование изменений.
- Управление изменениями и выпуском релизов осуществляется в соответствии с Положением о безопасной разработке.
- Система сопровождается комплектом документации, обеспечивающим заказчику возможность проектирования подсистемы защиты, безопасной конфигурации и проведения приемочных испытаний.
- Обеспечивается регламентированный процесс обновления и технической поддержки.

1.5 Границы ответственности

В рамках обеспечения возможности построения АСЗИ на базе системы Global ERP ООО «Бизнес Технологии» обеспечивает:

- реализацию встроенных механизмов безопасности;
- соблюдение требований ГОСТ Р 51583-2014 в процессе разработки системы, а также требований внутренних нормативных документов по информационной безопасности;
- предоставление заказчику эксплуатационной документации, необходимой для проектирования, безопасной конфигурации и аттестации системы защиты информации;
- регламентированное сопровождение системы в части выпуска обновлений, устранения выявленных уязвимостей и технической поддержки.

Статус АСЗИ и соответствие требованиям ГОСТ Р 51583-2014 достигаются заказчиком в рамках проекта внедрения путем реализации комплекса организационных и технических мероприятий по защите информации, соответствующих модели угроз и условиям эксплуатации конкретного контура.

В рамках построения АСЗИ на базе Global ERP заказчик обеспечивает:

- разработку модели угроз и технического задания на систему защиты информации для конкретного контура эксплуатации;
- конфигурирование встроенных механизмов безопасности в соответствии с эксплуатационной документацией и моделью угроз;
- развертывание и интеграцию наложенных средств защиты информации, включая СЗИ от НСД, антивирусные средства и СКЗИ, в соответствии с проектной документацией;
- организацию аттестации системы на соответствие требованиям информационной безопасности.

Состав и содержание мероприятий определяются моделью угроз, техническим заданием на систему защиты информации и требованиями аттестационной документации для конкретного контура эксплуатации.

1.6 Нормативная база

Встроенные механизмы безопасности системы и порядок их разработки реализованы с учетом требований следующих нормативных и методических документов:

- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;
- Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- методические рекомендации OWASP;
- внутренние нормативные документы ООО «Бизнес Технологии» в области информационной безопасности;
- Положение о безопасной разработке;
- регламент управления уязвимостями;
- проектная документация на разработку системы.

1.7 Термины и сокращения

- ALDPro — служба каталогов, используемая в инфраструктуре заказчика в качестве источника учетных данных.
- АСЗИ — автоматизированная система в защищенном исполнении, в которой требования к защите информации реализуются на всех этапах жизненного цикла в соответствии с ГОСТ Р 51583-2014.
- CEF (Common Event Format) — стандартный формат представления событий безопасности.
- DRP (Disaster Recovery Plan) — план восстановления после сбоев и аварий.
- IDM (Identity Management) — система управления учетными записями, ролями и жизненным циклом идентичностей.
- MDM (Mobile Device Management) — класс систем для управления и контроля мобильных устройств.

- MFA (Multi-Factor Authentication) — многофакторная аутентификация, использующая 2 и более независимых фактора подтверждения личности.
- NTP (Network Time Protocol) — протокол синхронизации времени в сетях.
- ORM (Object-Relational Mapping) — технология сопоставления объектов приложения с записями в базе данных.
- Security by design — подход к разработке, при котором требования безопасности учитываются на всех этапах жизненного цикла программного обеспечения.
- SIEM (Security Information and Event Management) — система сбора, корреляции и анализа событий информационной безопасности.
- SOAP (Simple Object Access Protocol) — протокол обмена структурированными сообщениями между приложениями.
- SQL Injection — уязвимость, связанная с внедрением SQL-кода через пользовательский ввод.
- SSO (Single Sign-On) — единая аутентификация пользователя для доступа к нескольким системам без повторного ввода учетных данных.
- SSRF (Server-Side Request Forgery) — уязвимость, позволяющая инициировать запросы от имени сервера к внутренним или внешним ресурсам.
- SYSLOG — протокол передачи сообщений журналирования.
- XSS (Cross-Site Scripting) — уязвимость, связанная с выполнением внедренного сценарного кода в интерфейсе пользователя.
- XXE (XML External Entity) — уязвимость, связанная с обработкой внешних XML-сущностей.
- Встроенные механизмы безопасности — реализованные в коде и архитектуре системы функции защиты информации, доступные для конфигурирования и применения без установки дополнительного программного обеспечения.
- Заказчик — юридическое лицо, осуществляющее внедрение, конфигурирование и эксплуатацию системы Global ERP в своем контуре.
- Информационная безопасность (ИБ) — состояние защищенности информации и информационных систем от несанкционированного доступа, искажения, утраты и иных угроз.
- Контроль целостности — проверка неизменности компонентов системы и данных.
- Наложенные средства защиты информации (СЗИ) — внешние по отношению к системе программные и аппаратные средства, обеспечивающие дополнительные меры защиты информации в конкретном контуре эксплуатации.
- Расширяемая модель безопасности — модель, предусматривающая интеграцию системы со сторонними средствами и сервисами безопасности.
- Ролевая модель доступа — модель разграничения доступа на основе ролей, назначаемых пользователям.
- Сетевая безопасность — совокупность мер по защите сетевых взаимодействий и ограничению сетевого доступа.

2 Описание встроенных механизмов безопасности системы Global ERP

2.1 Описание встроенных механизмов безопасности системы Global ERP

Общие положения

Настоящий документ «Описание встроенных механизмов безопасности системы Global ERP» (далее — Описание) определяет состав, назначение и принципы реализации встроенных механизмов защиты информации в системе Global ERP, а также устанавливает границы ответственности ООО «Бизнес Технологии» (далее — Общество) и заказчика при создании автоматизированных систем в защищенном исполнении (АСЗИ) всоответствии с ГОСТ Р 51583-2014.

Целями Описания являются:

- предоставление внутренним подразделениям и заказчикам достоверной информации о составе и назначении встроенных механизмов безопасности системы;
- обоснование соответствия архитектуры системы требованиям ГОСТ Р 51583-2014 в части обеспечения безопасности программного продукта;
- разграничение зон ответственности Общества как разработчика и заказчика как эксплуатирующей организации при построении и аттестации АСЗИ.

В Обществе применяется принцип обеспечения безопасности на этапе проектирования (*security by design*), предусматривающий встраивание механизмов защиты в архитектуру системы на всех этапах ее жизненного цикла.

Система Global ERP в типовой поставке не является готовой АСЗИ. Встроенные механизмы безопасности предоставляют базовый функционал, который конфигурируется и при необходимости дополняется внешними средствами защиты информации (СЗИ) в рамках конкретного проекта внедрения. Полное соответствие требованиям ГОСТ Р 51583-2014 и статус АСЗИ достигаются после проведения аттестации в реальных условиях эксплуатации заказчика.

Термины и определения

В настоящем Описании используются следующие термины и определения:

- **автоматизированная система в защищенном исполнении (АСЗИ)** — автоматизированная система, в которой требования к защите информации реализуются на всех этапах жизненного цикла в соответствии с ГОСТ Р 51583-2014;
- **встроенные механизмы безопасности** — реализованные в коде и архитектуре системы функции защиты информации, доступные для конфигурирования и применения без установки дополнительного программного обеспечения;
- **наложенные средства защиты информации (СЗИ)** — внешние по отношению к системе программные и аппаратные средства, обеспечивающие дополнительные меры защиты информации в конкретном контуре эксплуатации;
- **заказчик** — юридическое лицо, осуществляющее внедрение, конфигурирование и эксплуатацию системы Global ERP в своем контуре;
- ***security by design*** — подход к разработке, при котором требования безопасности учитываются на всех этапах жизненного цикла программного обеспечения, начиная с формирования требований и проектирования архитектуры.

Область применения

Настоящее Описание распространяется на все версии системы Global ERP и связанную с ними эксплуатационную документацию.

Требования Описания обязательны для применения:

- подразделениями разработки при проектировании и реализации встроенных механизмов безопасности;
- подразделениями внедрения и сопровождения при консультировании заказчиков;
- подразделением информационной безопасности при оценке соответствия системы нормативным требованиям.

Описание применяется совместно со следующими внутренними нормативными документами Общества:

- Положение о безопасной разработке;
- регламент управления уязвимостями;
- проектная документация на разработку системы.

Нормативная база

Встроенные механизмы безопасности системы и порядок их разработки реализованы с учетом требований следующих нормативных и методических документов:

- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;
- Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- методические рекомендации OWASP;
- внутренние нормативные документы Общества по информационной безопасности и безопасной разработке.

Архитектурные принципы безопасности

Архитектура системы Global ERP реализует следующие принципы безопасности:

- учет требований информационной безопасности на этапе проектирования (*security by design*);
- совместимость с внешними средствами защиты информации и предоставление интерфейсов для их интеграции;
- отсутствие конфликтов встроенных механизмов безопасности с бизнес-функциональностью системы;
- сохранение проектных показателей производительности при работе встроенных механизмов защиты.

Встроенные механизмы безопасности охватывают следующие функциональные подсистемы:

- идентификация и аутентификация;

- управление доступом;
- аудит и журналирование;
- защита каналов связи;
- управление секретами;
- безопасность выполнения и обработки запросов.

Учет требований ГОСТ Р 51583-2014 в процессе разработки

Процесс создания системы Global ERP учитывает положения ГОСТ Р 51583-2014 в части обеспечения безопасности программного продукта следующими мерами:

- разработка ведется в соответствии с техническим заданием, в котором на этапе проектирования архитектуры фиксируются требования к подсистеме безопасности;
- архитектура системы атформы обеспечивает совместимость с внешними средствами защиты информации и предоставляет интерфейсы для их интеграции;
- встроенные механизмы безопасности не препятствуют нормальному функционированию системы и не снижают ее производительность ниже проектных показателей;
- в жизненный цикл разработки интегрированы обязательные процедуры верификации безопасности: статический анализ кода, автоматизированный анализ зависимостей (SCA), динамическое тестирование веб-интерфейсов и рецензирование изменений, обеспечивающие соответствие компонентов требованиям безопасности перед включением в поставочный контур;
- управление изменениями и выпуском релизов осуществляется в соответствии с Положением о безопасной разработке: обязательные проверки кода и зависимостей, контроль уязвимостей перед выпуском;
- Система сопровождается комплектом документации, обеспечивающим заказчику возможность проектирования подсистемы защиты, безопасной конфигурации и проведения приемочных испытаний;
- обеспечивается регламентированный процесс обновления и технической поддержки.

Встроенные механизмы безопасности системы

Архитектура Global ERP предоставляет следующие встроенные механизмы, соответствующие требованиям ГОСТ Р 51583-2014 и применимые при построении АСЗИ.

Идентификация и аутентификация

- **Политика паролей.** Система поддерживает настройку требований к сложности паролей (использование символов различных типов, минимальная длина), а также контроль истории и срока действия паролей. Параметры настраиваются в соответствии с руководством по политике паролей.
- **Интеграция со службами каталогов.** Поддерживается аутентификация пользователей через LDAP-каталоги, включая Microsoft Active Directory и ALDPro. Настройка выполняется в соответствии с инструкциями по LDAP-синхронизации и подключению к Active Directory.
- **Единый вход (SSO).** Система поддерживает использование внешних провайдеров аутентификации по протоколу OpenID Connect. Настройка выполняется в соответствии с руководством по настройке SSO.

- **Двухфакторная аутентификация (2FA).** Поддерживается использование второго фактора аутентификации (подтверждение по e-mail) при использовании внешнего провайдера идентификации. Настройка выполняется на стороне провайдера в соответствии с документацией по настройке 2FA.

Управление доступом

- **Ролевая модель (RBAC).** Доступ к функциям, данным и операциям системы предоставляется на основе ролей. Роли включают права на выполнение операций (чтение, добавление, изменение, удаление, выполнение действий) и назначаются пользователям через механизмы управления доступом в соответствии с руководством по настройке ролей.
- **Дискретный доступ к объектам.** Система поддерживает ограничение доступа на уровне отдельных объектов с использованием механизма дискретного доступа. Настройка правил выполняется в соответствии с разделом документации.

Аудит и журналирование

- **Аудит пользовательской активности.** Регистрация изменений данных и действий пользователей в системе (создание, изменение, удаление объектов). Аудит настраивается на уровне классов с сохранением данных в таблицах аудита и доступен для просмотра через интерфейс системы.
- **Журналы информационной безопасности.** Регистрация событий безопасности (аутентификация, ошибки входа, управление правами, сессии и др.). События логируются через специализированный логгер в формате CEF. Поддерживается экспорт событий во внешние системы (SIEM) по протоколу Syslog. Настройка журналирования и параметров экспорта выполняется в соответствии с документацией по настройке логирования событий информационной безопасности.

Защита каналов связи

- Защита сетевого взаимодействия обеспечивается с использованием TLS/SSL на уровне балансировщика (HAProxy), включая настройку сертификатов и HTTPS-подключения. Конфигурация выполняется согласно инструкции по настройке HAProxy и TLS.

Управление секретами

- **Хэширование паролей.** Пароли пользователей хранятся в виде хэшей алгоритма Argon2id без возможности восстановления исходного значения. Используется контроль истории паролей в хэшированном виде.
- **Шифрование учетных данных.** Для исключения хранения учетных данных в открытом виде применяется механизм шифрования данных. Настройка и выполнение шифрования осуществляется в соответствии с документацией по шифрованию учетных данных.
- **Интеграция с Kubernetes Secrets.** Система поддерживает развертывание через Helm-чарт (начиная с версии 5.4.0) и может использоваться совместно с внешними решениями для автоматизации работы с секретами: helm-secrets, sops, Sealed Secrets, External Secrets.

Безопасность выполнения и обработки запросов

- Архитектура системы предусматривает меры безопасности, направленные на предотвращение внедрения SQL-кода (SQL Injection), сокрытие информации о веб-сервере и безопасное выполнение серверной логики. Детальное описание реализованных мер приведено в соотвествующем разделе.

Зона ответственности ООО «Бизнес Технологии»

В рамках обеспечения возможности построения АСЗИ на базе системы Global ERP Общество обеспечивает:

- реализацию встроенных механизмов безопасности в соответствии с разделом «Встроенные механизмы безопасности системы» настоящего Описания;
- соблюдение требований ГОСТ Р 51583-2014 в процессе разработки системы, а также требований внутренних нормативных документов по информационной безопасности;
- предоставление заказчику эксплуатационной документации, необходимой для проектирования, безопасной конфигурации и аттестации системы защиты информации;
- регламентированное сопровождение системы в части выпуска обновлений, устранения выявленных уязвимостей и технической поддержки.

Зона ответственности заказчика

Статус АСЗИ и соответствие требованиям ГОСТ Р 51583-2014 достигаются заказчиком в рамках проекта внедрения путем реализации комплекса организационных и технических мероприятий по защите информации, соответствующих модели угроз и условиям эксплуатации конкретного контура.

В рамках построения АСЗИ на базе системы Global ERP заказчик, в частности, обеспечивает:

- разработку модели угроз и технического задания на систему защиты информации для конкретного контура эксплуатации;
- конфигурирование встроенных механизмов безопасности в соответствии с эксплуатационной документацией и моделью угроз;
- развертывание и интеграцию наложенных средств защиты информации (СЗИ от НСД, антивирусных средств, СКЗИ и др.) в соответствии с проектной документацией;
- организацию аттестации системы на соответствие требованиям информационной безопасности.

Приведенный перечень не является исчерпывающим. Состав и содержание мероприятий определяются моделью угроз, техническим заданием на систему защиты информации и требованиями аттестационной документации для конкретного контура эксплуатации.

2.2 Идентификация и аутентификация

Общая модель идентификации и аутентификации

В системе допускается использование следующих способов аутентификации:

1. Локальная аутентификация средствами платформы.
2. Аутентификация через внешний контур единого входа по протоколу OpenID Connect.
3. Аутентификация доменных пользователей с проверкой пароля внешней службой каталогов.
4. Аутентификация через внешний прокси-сервер авторизации.
5. Аутентификация технических подключений к REST- и SOAP-сервисам по схемам `Basic` и `Bearer`, включая постоянные токены и JWT.

При локальной аутентификации проверка учетных данных выполняется средствами Global ERP с применением встроенной политики паролей.

При использовании единого входа проверка учетных данных осуществляется внешним поставщиком идентификационных данных. Global ERP использует результат успешной аутентификации и применяет собственную модель авторизации.

При использовании внешнего прокси-сервера аутентификация пользователя осуществляется на стороне сервера авторизации. По результатам успешной аутентификации прокси-сервер формирует JWT-токен и передает его в Global ERP. Система валидирует токен и предоставляет доступ к функционалу в пределах назначенных прав доступа.

Для технических подключений к сервисам используются штатные HTTP-механизмы аутентификации. Для интеграционных сценариев поддерживаются логин и пароль, токены сервера приложений, долгоживущие пользовательские токены и JWT-токены, подписанные пользователем или прокси-пользователем.

Независимо от используемого механизма аутентификации, прикладная модель авторизации и проверка прав доступа реализуются в контуре Global ERP.

Идентификация пользователей

Идентификация пользователя в Global ERP осуществляется по уникальному идентификатору учетной записи. Указанный идентификатор используется в качестве логина и связывает учетную запись пользователя, механизмы аутентификации, назначенные роли и регистрируемые действия.

При локальной аутентификации идентификатор используется во внутреннем контуре Global ERP.

При аутентификации через внешние службы каталогов или внешний контур единого входа должно обеспечиваться однозначное сопоставление учетной записи пользователя в Global ERP с соответствующей внешней учетной записью. Для технических подключений идентификация осуществляется с использованием учетной записи пользователя, служебной учетной записи либо токена, связанного с учетной записью. Во всех случаях идентификатор должен однозначно определять субъект доступа.

Локальная аутентификация

При локальной аутентификации пользователь проходит встроенную процедуру аутентификации средствами платформы.

За включение централизованной настройки парольной политики отвечает флаг `bPasswordSettingsInOT` в классе `Btk_Setting`. При включенном флаге параметры задаются для типа объекта пользователя через `Btk_UserPasswordSetting`. При отключенном флаге применяются параметры из класса `Btk_User`.

Внутренняя реализация системы обеспечивает хранение паролей только в виде хэшей `Argon2id`. Исходное значение пароля не сохраняется и не может быть восстановлено по хэшу.

Для контроля повторного использования ранее применявшихся паролей используется сервис истории паролей. Значения предыдущих паролей сохраняются в журнале в хэшированном виде. Это позволяет проверять совпадение нового пароля с ранее использованными без раскрытия их исходных значений.

Проверка соответствия пароля установленным требованиям выполняется при его создании и смене. По истечении срока действия пароля система переводит пользователя в режим обязательной смены и при необходимости генерирует временный пароль.

Парольная политика

В Global ERP реализована комплексная политика паролей, направленная на обеспечение информационной безопасности. Политика охватывает:

- требования к минимальной длине и составу пароля;
- историю паролей и запрет повторного использования;
- проверку паролей по словарям и черным спискам;
- сроки действия постоянного и временного пароля;
- уведомления о необходимости смены пароля.

Для локальной аутентификации применяются следующие параметры политики паролей:

- обязательное использование специальных символов;
- обязательное сочетание букв и цифр;
- обязательное использование букв в разных регистрах;
- минимальная длина пароля;
- запрет на повторное использование определенного числа предыдущих паролей;
- минимальный срок действия пароля;
- срок действия постоянного пароля;
- срок действия временного пароля;
- период предварительного уведомления о необходимости смены пароля.

Параметры парольной политики настраиваются в соответствии с руководством по политике паролей.

Рекомендуемая базовая конфигурация предусматривает:

- минимальную длину пароля не менее 8 символов для обычных пользователей и не менее 12 символов для администраторов и привилегированных учетных записей;
- использование не менее 3 категорий символов;

- ограничение срока действия пароля;
- обязательную смену временного пароля при первом входе;
- ведение истории паролей.

Использование простых, предсказуемых и скомпрометированных паролей запрещено.

Автоматическая генерация паролей

При создании локальных учетных записей в системе может использоваться автоматическая генерация временного пароля в соответствии с действующей парольной политикой.

Сгенерированный пароль:

- соответствует установленным требованиям сложности;
- формируется с использованием криптографически стойкого генератора случайных значений;
- исключает использование предсказуемых последовательностей и словарных комбинаций;
- отображается администратору однократно в момент создания учетной записи.

После завершения операции создания пользователя повторное отображение исходного значения пароля средствами системы не выполняется.

Для учетных записей, созданных с автоматически сгенерированным временным паролем, рекомендуется обязательная смена пароля при первом входе пользователя в систему.

Защита от подбора паролей

Для предотвращения подбора паролей в локальном контуре аутентификации реализуется временная блокировка учетной записи пользователя при превышении допустимого количества последовательных неудачных попыток входа.

Параметр `jTempBlockingForUnsuccessfulLogin` определяет максимально допустимое количество неудачных попыток и продолжительность блокировки в минутах. При превышении установленного лимита система временно блокирует учетную запись.

В рекомендуемой конфигурации блокировка производится после 10 неудачных попыток входа сроком не менее 3 минут.

При использовании единого входа защита от подбора паролей дополнительно обеспечивается на стороне внешнего поставщика идентификационных данных. В сценариях OpenID Connect поддерживается настройка параметров механизма обнаружения перебора паролей: `Max login failures`, `Wait increment` и `Quick login check`.

Защита сеансов

Система обеспечивает автоматический разрыв сеанса при отсутствии активности пользователя.

Политики управления сеансами, включая обязательность разрыва и значения таймаутов, настраиваются на уровне конфигурации системы.

Управление сеансами распространяется на пользовательские подключения и применяется как элемент общего контура идентификации, аутентификации и защиты доступа.

Завершение сеанса

Сеанс работы пользователя может быть завершен по одному из следующих оснований:

- По инициативе пользователя — через штатную функцию выхода из системы.
- По таймауту бездействия — при отсутствии действий пользователя в течение интервала, заданного параметром `clientTimeout` в конфигурационном файле.
- По инициативе администратора — через функции администрирования активных сессий.
- По иным условиям, предусмотренным конфигурацией системы.

Повторная идентификация и аутентификация

После завершения сеанса доступ к функционалу системы возможен только после повторного прохождения идентификации и аутентификации штатными механизмами. При завершении сеанса интерфейс системы автоматически возвращается к окну аутентификации, предоставляя возможность начала нового сеанса.

Аутентификация через LDAP, Active Directory и ALDPro

Global ERP поддерживает аутентификацию пользователей через внешние службы каталогов, включая LDAP-каталоги, Active Directory и ALDPro. Для этого в конфигурации сервера приложений настраивается подключение к каталогу, а для базы данных активируется режим `authenticationType="ldap"`.

В указанном режиме проверка пароля пользователя не выполняется средствами платформы, а передается внешней службе каталогов для подтверждения подлинности.

Параметры парольной политики для доменных пользователей определяются корпоративной службой каталогов предприятия, включая групповые политики Active Directory или аналогичные политики LDAP/ALDPro. Смена пароля пользователя выполняется средствами операционной системы с пользовательского рабочего места, в том числе при очередном входе, если такая смена требуется политикой службы каталогов. Global ERP в этом сценарии не хранит доменный пароль и не управляет его сменой, а использует результат проверки учетных данных, выполненной службой каталогов.

Параметры подключения к службе каталогов задаются в конфигурации `<ldap .../>` и включают, в частности, адрес LDAP-сервера и домен. Данный режим применяется для аутентификации доменных пользователей при сохранении прикладной модели ролей внутри Global ERP.

Система поддерживает синхронизацию пользователей из внешних служб каталогов. Для этого используется сервис LDAP-синхронизации, настраиваемый в модуле `Btk`. Сервис обеспечивает загрузку пользователей из указанных доменов, фильтрацию по группам и выбор режимов синхронизации в соответствии с выбранным сценарием. При необходимости к системному имени пользователя может быть добавлен домен в формате `User@Domain`.

Синхронизация учетных записей и аутентификация по доменному паролю являются самостоятельными процессами и могут применяться совместно. Пользовательские учетные записи могут предварительно загружаться в систему через сервис синхронизации, после чего аутентификация выполняется через домен или внешний контур единого входа.

Настройка выполняется в соответствии с инструкцией по LDAP-синхронизации и описанием параметров LDAP в конфигурации базы.

Процесс аутентификации с помощью единого входа

Поддержка единого входа реализована в компоненте Global Server через протокол OpenID Connect с использованием внешнего поставщика идентификационных данных. Настройка выполняется на стороне сервера приложений посредством блока `<openId>` в файле `global3.config.xml`.

Процесс аутентификации при использовании единого входа включает следующие этапы:

1. Пользователь инициирует вход в систему.
2. Аутентификация выполняется внешним провайдером идентификации.
3. На стороне внешнего провайдера могут использоваться федерация пользователей через LDAP, Active Directory или ALDPro, защита от подбора паролей и дополнительные факторы аутентификации.
4. После успешной аутентификации пользователю предоставляется доступ к функциям системы в рамках назначенных ролей и полномочий в Global ERP.

Во внешнем SSO-контуре могут использоваться корпоративные службы каталогов и механизмы многофакторной аутентификации, включая одноразовые пароли и приложения-аутентификаторы. Настройка второго фактора осуществляется на стороне поставщика идентификационных данных и может включать одноразовые коды, подтверждения по электронной почте, SMS, приложения-аутентификаторы и другие поддерживаемые провайдером методы.

Настройка выполняется в соответствии с руководством по настройке SSO. Настройка второго фактора описана в документации по настройке 2FA.

Аутентификация через внешний прокси-сервер авторизации

Global ERP поддерживает работу с внешним сервером авторизации `gs-authproxy` и совместимыми внешними сервисами авторизации. Данный режим применяется в сценариях, когда требуется вынести первичную аутентификацию пользователей во внешний контур, например для предоставления доступа пользователям внешних организаций к выделенному функционалу.

В схеме работы данного режима входящий запрос пользователя направляется на балансирующий или проксирующий узел, после чего поступает на внешний сервер авторизации или непосредственно в Global ERP. Внешний сервер авторизации проверяет учетные данные пользователя и при успешной аутентификации генерирует JWT-токен. Пользователь передается в Global ERP с полученным токеном, где система выполняет проверку токена, сопоставляет пользователя с внутренней учетной записью и применяет ролевую модель доступа.

В этом режиме внешний прокси обеспечивает первичную аутентификацию и выдачу токена, а Global ERP — проверку токена, сопоставление учетной записи и применение полномочий.

Подробнее см. в разделе Развертывание сервера приложений GS с сервером авторизации.

Аутентификация технических подключений и сервисов

Для технических подключений к REST- и SOAP-сервисам поддерживаются HTTP-схемы аутентификации `Basic` и `Bearer`.

При `Basic`-аутентификации клиент передает в запросе имя пользователя, пароль и имя базы. Имя пользователя и пароль кодируются в Base64 и передаются через заголовок `Authorization` в формате `Basic {Base64Cred}`, где `{Base64Cred}` — строка `user:password`. Имя базы может передаваться через сегмент URL, заголовок `Database` или HTTP-параметр `Database`. При отсутствии указания используется база по умолчанию, определяемая конфигурацией `global3.config.xml`.

При `Bearer`-аутентификации клиент передает токен аутентификации и имя базы. Для интеграционных сценариев могут использоваться токены сервера приложений, постоянные пользовательские токены и JWT-токены.

Поддерживаются следующие варианты JWT-аутентификации:

- `UserHash` — долгоживущий токен пользователя;
- `UserCrt` — JWT, подписанный пользователем;
- `ProxyCrt` — JWT, подписанный прокси-пользователем для выполнения действий от имени другого пользователя.

Долгоживущий токен формируется администратором и привязывается к учетной записи пользователя. Подписанные JWT используют RSA-ключи, сопоставленные с учетной записью пользователя или прокси-пользователя. Проверка действительности токена выполняется системой с использованием открытого ключа, хранящегося в базе данных решения.

Подробнее см. в разделе Аутентификация в REST/SOAP-сервисах.

Аутентификация устройств

Для устройств могут использоваться механизмы аутентификации с применением сертификатов и дополнительных атрибутов идентификации. В зависимости от архитектуры внедрения может использоваться интеграция с внешними системами управления устройствами класса `MDM`.

Использование таких механизмов допускается только в рамках штатного контура безопасности и не отменяет требований к сопоставлению устройства, учетной записи и назначенных прав доступа.

Источники учетных данных

В зависимости от архитектуры конкретного внедрения источником учетных данных могут выступать:

- локальная учетная запись Global ERP;
- внешняя служба каталогов LDAP, Active Directory или ALDPro;
- внешний провайдер идентификации в SSO-контуре;
- внешний прокси-сервер авторизации, выдающий JWT;
- учетные данные или токены, используемые для подключения к техническим сервисам.

Независимо от источника первичной аутентификации, учетные записи пользователей хранятся в базе данных Global ERP. Назначение ролей и проверка прав выполняются в контуре системы и описаны в разделе «Управление доступом».

Требования к расширениям и функциональному дизайну

Расширения и прикладные доработки обязаны использовать штатный контур идентификации и аутентификации Global ERP. Реализация изолированных механизмов входа, параллельных хранилищ паролей или обходных сценариев аутентификации не допускается. Аутентификация расширений должна выполняться одним из штатных способов, предусмотренных платформой.

2.3 Управление доступом

Классификация пользователей и учетных записей

Для целей управления доступом и разграничения полномочий учетные записи в системе Global ERP подразделяются на следующие категории:

1. **Внутренние пользователи** — сотрудники организации, имеющие постоянный доступ к системе для выполнения служебных обязанностей.
2. **Внешние пользователи** — клиенты, подрядчики и иные третьи лица, которым предоставляется ограниченный доступ к функционалу системы в рамках конкретных бизнес-процессов.
3. **Технические или сервисные учетные записи** — учетные записи, используемые для интеграций, автоматизированных процессов, сервисов и программных компонентов системы.
4. **Администраторы и привилегированные учетные записи** — пользователи с повышенными правами доступа к системным функциям, конфигурации, ролевым назначениям и критическим данным.

Для каждой категории учетных записей устанавливаются отдельные правила аутентификации, ограничения по доступу, а также требования к хранению и защите учетных данных.

В типовой поставке Global ERP не предусмотрены готовые профили доступа и роли для конкретных организационных моделей заказчика. Заказчик самостоятельно создает профили и роли, определяет состав привилегий и назначает их пользователям в соответствии со своими бизнес-процессами, организационной структурой и требованиями к разграничению доступа.

Ролевая модель доступа

В Global ERP применяется ролевая модель доступа с разграничением полномочий на уровне платформы и прикладных компонентов. Доступ к функциям, данным, журналам событий и API предоставляется на основании назначенных ролей.

Ролевая модель используется как основной механизм разграничения прав и поддерживает:

- разделение полномочий между различными категориями пользователей;
- ограничение доступа к критически важным операциям;
- контроль привилегий при обращении к системным и сервисным API;
- запрет совмещения конфликтующих ролей;
- интеграцию с внешними IDM-системами.

Роли включают права на выполнение операций: чтение, добавление, изменение, удаление и выполнение действий. Роли могут назначаться администратором системы вручную или через внешнюю систему управления идентификацией и доступом, интегрированную с Global ERP.

Независимо от источника первичной аутентификации, прикладные роли и полномочия назначаются и проверяются в контуре Global ERP.

Настройка ролей выполняется в соответствии с руководством по настройке ролей.

Контроль привилегий

Контроль привилегий в Global ERP осуществляется на основе ролевой модели и реализуется средствами платформы на серверной стороне.

Проверка прав доступа выполняется при каждом обращении к:

- прикладным операциям;
- объектам данных;
- системным и сервисным API;
- REST- и SOAP-сервисам;
- административным функциям и иным критичным интерфейсам.

Доступ к функциональности системы предоставляется при наличии соответствующих привилегий. При отсутствии необходимых прав выполнение операции запрещается.

Контроль доступа реализуется централизованно и не должен дублироваться или обходиться на уровне прикладного кода. Все проверки выполняются на стороне сервера, независимо от клиентского интерфейса или способа вызова.

Для ограничения доступа на уровне отдельных объектов используется механизм дискретного доступа. Настройка правил выполняется в соответствии с разделом документации по дискретному доступу.

2.4 Безопасность выполнения и обработки запросов

Безопасность выполнения серверной логики

Архитектура системы предусматривает ограничения, направленные на безопасное выполнение серверной логики, выполнение выражений и сценариев, а также предотвращение несанкционированных операций.

- ограничен доступ к SOAP-сервису, используемому для работы с шаблонами;
- шедуллер запускается под разными пользователями; настройка разграничения пользователей для шедуллера не применяется;
- вызов JEXL-выражений через SSH-консоль выполняется с использованием безопасного диалекта;
- реализовано разграничение прав на выполнение JEXL-скриптов через веб-сокеты.

Защита от изменения логики SQL-запросов

В системе реализован комплекс мер, направленных на предотвращение изменения логики SQL-запросов за счет пользовательских данных. Эти меры обеспечивают защиту от SQL-инъекций и исключают возможность выполнения несанкционированных операций с базой данных.

Реализованные меры	Описание реализации
Экранирование пользовательского ввода	Реализована функция `sqlEscape` для экранирования пользовательских данных. Использование функции обязательно при формировании SQL-запросов путём конкатенации строк и закреплено организационно в требованиях к разработке.
Безопасное построение динамических SQL-запросов	Реализован компонент `SqlBuilder` для формирования динамических SQL-запросов. Компонент автоматически выполняет экранирование пользовательских данных, если явно не указано иное.
Ограничение доступа к SQL-логике через JEXL	Реализован доступ к пакетам базы данных через JEXL с возможностью ограничения доступа ко всему пакету или к отдельным методам. Пакеты не отображаются в списке объектов администратора.
Разграничение доступа в REST-пакетах	Реализована возможность разграничения доступа в REST-пакетах на уровне URL входящих запросов.

Указанные меры применяются во всех компонентах системы, где пользовательские данные участвуют в формировании SQL-запросов, включая REST-интерфейсы и серверную логику.

Пример обработки запроса

```
GET /GLOBAL-QAS/gtk-ru.bitec.app.btk.utils.Btk_UrlObjectFinder%23UrlFinder/?ex;
↪sTableName_dz=btk_user;SELECT+version()::int%3d1;+--+-&ex;susername=UIB_SCAN2 HTTP/1.1
Host: global-qas.sgc.oil.gas
Cookie: access_token=<JWT>
```

В результате обработки запроса SQL-инъекция нейтрализуется за счет экранирования пользовательского ввода и безопасного формирования SQL-запроса. Выполнение внедрённого SQL-кода не происходит.

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=UTF-8

{
  "error": "Invalid request parameters"
}
```

Информация о версии базы данных и иных характеристиках СУБД в ответе отсутствует.

Сокрытие информации о веб-сервере

В целях снижения риска раскрытия технической информации HTTP-интерфейсы системы не передают сведения о типе и версии используемого веб-сервера.

Во всех HTTP-ответах исключена передача стандартных и расширенных заголовков, содержащих информацию о серверном программном обеспечении, включая `Server`, `X-Powered-By`, а также аналогичные заголовки сторонних компонентов и middleware.

Поведение единообразно для всех HTTP-эндпоинтов системы, включая REST-интерфейсы.

Пример

```
HTTP/1.1 303 See Other
location: https://global-qas.oil.gas/login/login.html?return-uri-Lw==
content-length: 0
```

2.5 Логирование, аудит и управление инцидентами

Логирование событий безопасности

В системе реализованы механизмы сбора и накопления журналов доступа и событий безопасности.

Система не выполняет функции SIEM. Журналы событий безопасности могут передаваться во внешние системы сбора и анализа в целях выявления инцидентов информационной безопасности. Передача осуществляется в независимое хранилище с использованием протокола `SYSLOG`, в том числе с поддержкой форматов `JSON` и `CEF`.

Журналы информационной безопасности фиксируют события аутентификации, ошибки входа, управление правами, сессии и другие события безопасности. События логируются через специализированный логгер в формате CEF. Настройка журналирования и параметров экспорта выполняется в соответствии с документацией по настройке логирования событий информационной безопасности.

Защита журналов

Доступ к журналам осуществляется в соответствии с ролевой моделью доступа и предоставляется только уполномоченным пользователям.

Журналы используются для мониторинга событий, расследования инцидентов и контроля корректности работы системы.

В журналах исключается хранение чувствительных данных: паролей, ключей доступа, токенов и реквизитов аутентификации. Если хранение чувствительной информации необходимо, применяются механизмы ограничения доступа и криптографической защиты.

В системе реализованы механизмы регистрации и обработки событий информационной безопасности, включая контроль действий пользователей и подключений к системе.

Журналы защищены от несанкционированного изменения и удаления в пределах реализованных механизмов разграничения доступа и администрирования системы.

Для журналов могут применяться регламентированные сроки хранения, архивирования и очистки в соответствии с внутренними процедурами эксплуатации и требованиями заказчика.

Аудит пользовательской активности

Система обеспечивает регистрацию и аудит действий пользователей, включая:

- доступ к данным;
- вызовы сервисных интерфейсов;
- действия, выполняемые в рамках пользовательских сеансов;
- события аутентификации и подключения к системе;
- создание, изменение и удаление объектов.

Для событий аудита фиксируются временные метки, идентификаторы пользователей и сведения о выполняемых операциях. Эти данные используются для мониторинга, расследования инцидентов и анализа действий в системе.

Аудит настраивается на уровне классов с сохранением данных в таблицах аудита и доступен для просмотра через интерфейс системы. Подробнее см. раздел Аудит пользовательской активности.

Синхронизация времени осуществляется с использованием протокола NTP. Это обеспечивает согласованность временных меток и корректность корреляции событий аудита.

Управление инцидентами

При выявлении инцидентов информационной безопасности проводится анализ причин, разрабатываются корректирующие меры и при необходимости выпускаются обновления системы.

Подготовлены эксплуатационные материалы и инструкции по развертыванию, эксплуатации и устранению нештатных ситуаций.

Учет и устранение выявленных уязвимостей

В системе реализованы меры по учету и устранению уязвимостей:

- выявление уязвимостей на этапах проектирования и разработки (`security by design`);
- учет результатов внутренних и внешних проверок безопасности;
- классификация уязвимостей по уровню риска;
- устранение выявленных уязвимостей;
- контроль актуальности реализованных мер при обновлении системы.

Дополнительно применяются следующие меры:

- защита от внедрения SQL-кода за счет проверки, фильтрации и экранирования пользовательских данных;
- защита от межсайтового выполнения сценариев (`XSS`) путем обязательного экранирования пользовательского ввода.

2.6 Инфраструктурная безопасность и сопровождение

Сетевая безопасность

Подготовлена схема взаимодействия компонентов системы, используемая для настройки правил сетевого доступа на стороне заказчика.

Защита каналов связи

Защита сетевого взаимодействия обеспечивается с использованием TLS/SSL на уровне балансировщика HAProxy, включая настройку сертификатов и HTTPS-подключения.

Конфигурация выполняется согласно инструкции по настройке HAProxy и TLS.

Управление секретами

К секретам относятся пользовательские пароли, учетные данные интеграций, токены, ключи доступа и иные данные, которые не должны храниться в открытом виде. Хранение пользовательских паролей описано в разделе «Идентификация и аутентификация»; в этом разделе рассматриваются механизмы защиты учетных данных и инфраструктурных секретов.

Для исключения хранения учетных данных в открытом виде применяется механизм шифрования данных. Настройка и выполнение шифрования осуществляется в соответствии с документацией по шифрованию учетных данных.

Система поддерживает развертывание через Helm-чарт, начиная с версии 5.4.0, и может использоваться совместно с внешними решениями для автоматизации работы с секретами: helm-secrets, sops, Sealed Secrets, External Secrets.

Совместимость с защищенной инфраструктурой

Система совместима с:

- решениями по защите виртуальных машин и контейнеров;
- антивирусными средствами заказчика, включая потоковый контроль загружаемых файлов;
- операционными системами российской разработки.

Контроль целостности

Реализованы механизмы проверки подписей и контроля целостности компонентов системы.

Защита данных

Для сред разработки и тестирования предусмотрены механизмы обезличивания и маскирования данных.

Резервное копирование и восстановление

Поддерживаются приложений-ориентированные резервные копии, ежедневное инкрементальное резервирование и восстановление инфраструктуры.

Разработаны:

- инструкции DRP;
- процедуры отката изменений;
- процедуры восстановления из резервных копий.

Обновления и сопровождение

Реализован регламент выпуска, тестирования и установки обновлений, включая:

- функциональное тестирование;
- нагрузочное тестирование;
- автотестирование;
- установку без простоев при кластеризации;
- автоматические и ручные сценарии обновления.

3 Рекомендации по информационной безопасности

3.1 Общие рекомендации

Требования к паролям

Для защиты учетных записей в `Global ERP` рекомендуется соблюдать следующие правила:

- пароль должен содержать не менее 12 символов;
- пароль должен включать буквы в разных регистрах, цифры и специальные символы;
- не следует использовать простые и типовые пароли;
- не следует записывать пароли на бумажных носителях, хранить их в незащищенных файлах и передавать другим лицам;
- для создания и хранения паролей рекомендуется использовать корпоративный менеджер паролей.

Использование двухфакторной аутентификации

Для доступа к критичным функциям системы рекомендуется использовать дополнительное подтверждение личности.

Рекомендуется:

- применять двухфакторную аутентификацию для администраторов системы и пользователей с расширенными правами;
- в качестве основного способа подтверждения использовать приложения-аутентификаторы или аппаратные ключи безопасности;
- не использовать `SMS` как основной способ второго фактора, если есть возможность применить более защищенные методы.

Принцип минимально необходимых прав

Пользователям рекомендуется предоставлять только тот уровень доступа, который необходим для выполнения их рабочих задач.

Рекомендуется:

- разделять административные полномочия;
- не совмещать в одной учетной записи избыточный набор прав;
- регулярно пересматривать выданные права доступа;
- проводить аудит прав доступа не реже одного раза в квартал.

Действия при инциденте информационной безопасности

При подозрении на компрометацию системы, утечку данных или несанкционированный доступ рекомендуется:

1. ограничить дальнейшее взаимодействие с затронутой системой в соответствии с внутренним регламентом;
2. обеспечить сохранность журналов и иных данных, необходимых для расследования;
3. уведомить ответственную службу информационной безопасности;
4. выполнять дальнейшие действия в соответствии с утвержденным порядком реагирования на инциденты.

Резервное копирование

Рекомендуется:

- выполнять регулярное резервное копирование данных;
- хранить резервные копии в изолированном контуре;
- использовать шифрование резервных копий;
- регулярно выполнять тестовое восстановление.

Периодичность резервного копирования, сроки хранения и порядок проверки рекомендуется определять внутренними регламентами организации.

Ограничение использования несанкционированных сервисов

Рекомендуется исключить обработку рабочих данных `Global ERP` вне корпоративной инфраструктуры.

Не рекомендуется:

- размещать рабочие данные в публичных облачных сервисах без согласования;
- передавать логины, пароли, журналы и конфигурационные файлы через неутвержденные каналы связи;
- копировать рабочие данные на личные носители без разрешения.

Обучение пользователей

Рекомендуется организовать регулярное обучение пользователей вопросам информационной безопасности.

В программу обучения рекомендуется включать:

- правила безопасной работы с учетными данными;
- противодействие фишингу и социальной инженерии;
- порядок работы с чувствительными данными;
- действия при выявлении инцидентов информационной безопасности.

Защита автоматизированных рабочих мест

Рабочие места с доступом к `Global ERP` рекомендуется защищать стандартными средствами информационной безопасности.

Рекомендуется:

- использовать антивирусное программное обеспечение, одобренное ИТ-подразделением;
- не отключать защитные механизмы без согласования;
- использовать межсетевой экран на рабочих станциях и серверах;
- своевременно устанавливать обновления операционной системы и прикладного программного обеспечения;
- контролировать актуальность сигнатур и обновлений защитных средств.

3.2 Рекомендации по безопасности Global ERP

Базовый уровень безопасности

Рекомендуется сформировать и применять базовый профиль безопасности для типового развертывания системы.

Базовый профиль может включать:

- отключение неиспользуемых учетных записей;
- включение многофакторной аутентификации для административных учетных записей;
- использование защищенных протоколов и актуальных версий `TLS`;
- запуск серверных процессов от отдельной учетной записи операционной системы.

Если готовый профиль безопасности не используется, рекомендуется выполнить аналогичные настройки вручную.

Управление ролями и полномочиями

Рекомендуется:

- использовать утвержденные роли доступа;
- по возможности избегать ручного назначения отдельных прав вне ролевой модели;
- анализировать конфликты полномочий;
- согласовывать изменения ролей и фиксировать их в журналах или заявках на изменение.

В оперативном режиме работы системы не следует использовать учетные записи суперпользователей, то есть учетные записи с расширенными или максимальными правами доступа.

Начальная административная учетная запись используется только на этапе первичной настройки: для создания ролей, профилей и назначения административных полномочий. После настройки ролевой модели с начальной административной учетной записи необходимо снять права суперпользователя. При необходимости учетную запись можно дополнительно заблокировать, отключить или удалить по регламенту заказчика.

Текущее администрирование должно выполняться через именные учетные записи администраторов. Для них назначаются отдельные административные роли и профили, ограниченные задачами управления и настройки системы. Такие учетные записи не должны использоваться для работы с основным прикладным функционалом, если это не требуется по рабочим задачам.

Мониторинг критичных операций

Рекомендуется контролировать:

- изменение мастер-данных;
- массовый экспорт данных;
- выполнение критичных действий в нерабочее время;
- попытки обхода контрольных процедур.

События безопасности рекомендуется передавать во внешние системы мониторинга и `SIEM`, если такие средства используются в инфраструктуре организации.

Требования к инфраструктуре

Рекомендуется:

- размещать сервер приложений и базу данных в изолированном сетевом сегменте;
- ограничивать доступ к системе из внешних сетей;
- публиковать веб-интерфейсы через доверенный обратный прокси с включенным `TLS`;
- ограничивать физический доступ к серверам;
- использовать поддерживаемые версии операционных систем, систем управления базами данных и сопутствующего ПО.

Настройка базы данных

Рекомендуется:

- не использовать системную учетную запись `postgres` или ее аналог для работы приложения;
- создать отдельную учетную запись базы данных для `Global ERP`;
- ограничить подключения к базе данных по сетевым адресам;
- использовать безопасные методы аутентификации;
- включить шифрование сетевого взаимодействия;
- настроить журналирование операций изменения данных в соответствии с требованиями эксплуатации и аудита.

Управление обновлениями

Рекомендуется:

- устанавливать обновления безопасности в регламентированные сроки;
- предварительно тестировать обновления в отдельной среде;
- использовать только доверенные источники обновлений;
- проверять подлинность пакетов и дистрибутивов.

Безопасность при кастомизации

При разработке и внедрении доработок рекомендуется:

- контролировать зависимости сторонних библиотек;
- использовать средства статического анализа кода;
- исключать небезопасные конструкции и отладочные механизмы в промышленной среде;
- проверять пользовательские доработки на соответствие внутренним требованиям безопасной разработки.

Контроль технического долга

Рекомендуется не оставлять в промышленной среде:

- временные учетные записи;
- временные правила сетевого доступа;
- устаревшие версии операционных систем, `СУБД` и библиотек без плана обновления.

Если такие исключения временно необходимы, рекомендуется ограничивать срок их действия и согласовывать их по внутреннему регламенту.

Интеграция с корпоративными средствами мониторинга

При наличии в инфраструктуре соответствующих средств рекомендуется интегрировать `Global ERP` с системами мониторинга и анализа событий.

Возможные направления интеграции:

- экспорт метрик состояния системы;
- передача журналов во внешние системы сбора и анализа;
- контроль доступности сервисов и ключевых точек входа;
- контроль параметров защищенного соединения и времени отклика.

3.3 Подход Security by Design

Архитектурные принципы

При проектировании и развитии решений на базе `Global ERP` рекомендуется учитывать следующие принципы:

- отсутствие неявного доверия к внутренней сети;
- анализ угроз для критичных компонентов;
- изоляция данных и компонентов в многоконтурных и многопользовательских сценариях;
- централизованный контроль доступа к данным и функциям системы.

Аутентификация

Рекомендуется:

- использовать современные протоколы аутентификации и единого входа;
- включать многофакторную аутентификацию для привилегированных пользователей;
- ограничивать число неуспешных попыток входа;
- контролировать повторное использование паролей в соответствии с принятой парольной политикой.

Авторизация

Рекомендуется:

- использовать ролевую модель доступа;
- при необходимости дополнять ее контекстными ограничениями;
- предотвращать совмещение конфликтующих полномочий;
- предоставлять права по принципу минимальной достаточности.

Защита данных

Рекомендуется обеспечивать защиту данных:

- при передаче — за счет использования защищенных протоколов связи;
- при хранении — за счет механизмов шифрования и разграничения доступа;
- при отображении и журналировании — за счет маскирования чувствительных данных.

Защита от типовых атак

При разработке и эксплуатации рекомендуется учитывать защиту от следующих угроз:

- внедрение `SQL`-кода;
- межсайтовое выполнение сценариев;
- подделка межсайтовых запросов;
- несанкционированный доступ к объектам по прямым идентификаторам;
- ошибки в проверке прав доступа.

Управление сеансами

Рекомендуется:

- задавать тайм-аут неактивности пользовательских сеансов;
- использовать централизованное завершение сеансов при необходимости;
- применять безопасные атрибуты cookie;
- настраивать параметры сеансов в соответствии с внутренними требованиями безопасности.

Аудит

Рекомендуется журналировать:

- вход и выход пользователей;
- изменение прав и ролей;
- экспорт данных;
- выполнение критичных административных действий.

Срок хранения журналов и порядок их защиты рекомендуется определять внутренними нормативными документами.

3.4 Соответствие требованиям

При эксплуатации `Global ERP` рекомендуется учитывать применимые для организации нормативные и отраслевые требования в области информационной безопасности и защиты данных.

В зависимости от среды эксплуатации это могут быть:

- требования к защите персональных данных;
- требования к журналированию и аудиту;
- требования к аутентификации и разграничению доступа;
- требования к управлению уязвимостями и обновлениями;
- требования внутренних стандартов организации и внешних регуляторов.