SecurityGuide

Выпуск 0.0.2

Global System

февр. 03, 2026

Содержание

1 Реализованные меры обеспечения информационной безопасности

1.1 Общие положения

Назначение документа

Документ описывает реализованные в Global System меры обеспечения информационной безопасности, включая как встроенные в архитектуру и функциональность системы механизмы (security by design), так и возможности интеграции со сторонними средствами и сервисами безопасности для усиления защиты в процессе эксплуатации.

Область применения

Распространяется на все компоненты Global System, включая платформу, серверные и клиентские модули, прикладные решения и интерфейсы интеграции.

Подходы к обеспечению безопасности

В Global System 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 (например, внешние системы аутентификации, мониторинга, контроля доступа), позволяя усиливать защиту в зависимости от требований эксплуатации.

Термины и сокращения

- ALDPro — служба каталогов, используемая в инфраструктуре заказчика в качестве источника учетных данных.
- CEF (Common Event Format) — стандартный формат представления событий безопасности.
- DRP (Disaster Recovery Plan) — план восстановления после сбоев и аварий.
- IDM (Identity Management) — системы 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 два и более независимых факторов подтверждения личности.
- NTP (Network Time Protocol) — протокол синхронизации времени в сетях.
- ORM (Object-Relational Mapping) — технологии сопоставления объектов приложения с записями в базе данных.
- Security by design — подход к разработке, при котором меры информационной безопасности изначально закладываются в архитектуру и функциональность системы.
- SIEM (Security Information and Event Management) — системы 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.
- 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.
- 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.

1.2 Реализованные меры

Идентификация и аутентификация

В системе реализованы механизмы идентификации и аутентификации пользователей и устройств. Поддерживается:

- интеграция с системами единой аутентификации (*SSO*) во внутреннем контуре;
- многофакторная аутентификация (*MFA*), включая одноразовые пароли и приложения-аутентификаторы, во внешнем контуре;
- использование служб каталогов заказчика, включая Active Directory и *ALDPro* в качестве источников учетных данных.

Парольная политика

Реализована гибкая парольная политика, включающая:

- требования к минимальной длине пароля;
- требования к составу пароля (использование различных типов символов);
- контроль истории паролей и запрет повторного использования;
- проверку паролей по словарям;
- регламентированную периодичность смены паролей в соответствии с требованиями заказчика.

Подробнее см. в разделе Политика паролей.

Защита учетных записей

Поддерживается временная блокировка учетных записей при многократных неуспешных попытках входа.

Для устройств предусмотрены механизмы аутентификации с использованием сертификатов и дополнительных атрибутов, а также совместимость с системами класса *MDM*.

Ролевая модель

В Global System реализована ролевая модель доступа с разграничением полномочий на уровне платформы и прикладных компонентов. Поддерживается:

- запрет совмещения конфликтующих ролей;
- интеграция с внешними *IDM*-системами.

Доступ к функциям, данным и журналам событий осуществляется строго в соответствии с назначенными ролями.

Контроль привилегий

Проверка прав пользователя выполняется при обращении к системным и сервисным API, включая критичные REST-интерфейсы.

Безопасная работа с шаблонами

- 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.
- Разграничение прав на REST-сервис сессий внедрено.
- Разграничение прав на выполнение JEXL-скриптов через веб-сокеты реализовано.

Защита от изменения логики SQL-запросов (SQL Injection)

В системе реализован комплекс мер, направленных на предотвращение изменения логики SQL-запросов за счёт пользовательских данных. 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, что ограничивает выполнение операций, связанных с формированием SQL-запросов.

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

Пример 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 была нейтрализована за счёт экранирования пользовательского ввода и безопасного формирования SQL-запроса. Выполнение внедрённого SQL-кода не произошло.

Пример ответа:

```
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. Реализованные меры исключают возможность изменения логики SQL-запросов и утечки технических сведений о базе данных.

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.

Безопасность интерфейса доступа

Для неавторизованных пользователей доступ ограничен минимальным набором функций, включая только страницы входа и восстановления пароля. Информация о внутренней структуре и компонентах системы не раскрывается.

Логирование событий безопасности

Реализованы механизмы сбора и накопления журналов доступа и событий безопасности.
Журналы могут передаваться во внешние системы мониторинга и *SIEM* в структурированном виде (JSON, *CEF*, *SYSLOG*).

Защита журналов

Доступ к журналам осуществляется на основе ролевой модели.
В журналах исключено хранение чувствительных данных либо применяется их шифрование.

В журналах исключено хранение чувствительных данных либо применяется их шифрование. Подготовлены и реализованы регламенты обработки и реагирования на события информационной безопасности.

Аудит пользовательской активности

Система обеспечивает аудит действий пользователей, включая:

- доступ к данным;
- вызовы сервисных интерфейсов;
- действия в рамках пользовательских сеансов.

Для всех транзакций, записанных в журнал аудита добавляются временные метки. Метка берётся либо по времени базы данных, либо по серверу приложения. Метки времени синхронизируются по протоколу NTP, что обеспечивает корректность аудита и расследования инцидентов.

Сетевая безопасность

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

Сокрытие информации о веб-сервере

В целях снижения риска раскрытия технической информации и усложнения первичного анализа (fingerprinting) инфраструктуры, HTTP-интерфейсы Global System 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 публичных и служебных HTTP-эндпоинтов системы, включая REST-интерфейсы.

Пример HTTP-запроса:

```
GET / HTTP/1.1 Host: global-qas.sgc.oil.gas
```

Пример HTTP-ответа:

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

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.

Безопасная разработка

В процессе разработки и сопровождения применяются средства статического и динамического анализа кода, а также контроль директивных и транзитивных зависимостей сторонних библиотек.

Учет и устранение уязвимостей

В Global System реализован процесс централизованного учета, анализа и устранения уязвимостей, выявляемых в ходе внутренних и внешних проверок безопасности, включая результаты специализированных работ по анализу защищенности.

В рамках данного процесса:

- все выявленные уязвимости классифицируются по уровню риска (высокий, средний, низкий, информационный);
- для каждой уязвимости фиксируются затронутые компоненты, сценарии эксплуатации и потенциальные угрозы;

- формируются и реализуются технические меры по устранению либо снижению риска;
- результаты устранения подлежат повторной проверке.

Примеры устраняемых уязвимостей приведены в таблице:

Класс уязвимости	Уровень риска	Выявленные сценарии	Реализованные меры
Внедрение SQL-кода (SQL Injection)	Высокий	Возможность влияния пользовательского ввода на формируемые SQL-запросы и получение данных из БД	Параметризация запросов, централизованная валидация и экранирование пользовательских данных, аудит ORM-механизмов
Недостаточная авторизация	Высокий	Выполнение пользователем действий, не соответствующих его привилегиям (доступ к служебным отчетам, договорам, идентификаторам)	Строгая серверная проверка прав доступа, централизованная ролевая модель, контроль доступа к REST- и SOAP-интерфейсам
Внедрение внешних сущностей XML (XXE)	Высокий / Средний	Обработка XML-данных с поддержкой внешних сущностей и DTD	Отключение обработки DTD и внешних сущностей, ограничение используемых форматов данных
Раскрытие информации в сообщениях об ошибках	Средний	Раскрытие установочных путей и внутренней структуры приложения	Централизованная обработка ошибок, вывод минимальной информации пользователю, регистрация подробностей только во внутренних журналах
Подделка запроса со стороны сервера (SSRF)	Средний	Возможность выполнения HTTP-запросов к внутренним сервисам	Ограничение допустимых схем и адресов, фильтрация целевых ресурсов, контроль сетевых взаимодействий
Использование ПО с известными уязвимостями	Средний	Использование уязвимых версий сторонних компонентов	Регулярный аудит зависимостей, контроль версий, регламент обновления программного обеспечения
Подбор учетных данных	Средний	Многократные попытки аутентификации через точки входа системы	Ограничение количества попыток входа, отказ от небезопасных схем аутентификации, применение защищенных механизмов входа
Межсайтовое выполнение сценариев (XSS)	Средний	Отображение неэкранированных пользовательских данных в интерфейсе	Обязательное экранирование пользовательского ввода перед отображением

Контроль выполнения мер

- Устранение уязвимостей выполняется совместно с разработчиками и ответственными за эксплуатацию.
- Критические уязвимости устраняются в приоритетном порядке.
- После внесения изменений проводится повторная проверка безопасности.
- Результаты проверок документируются и используются для совершенствования архитектуры security by design и интеграционных защитных механизмов.

Контроль целостности

Реализованы механизмы проверки подписей и контроля целостности компонентов системы. Процедуры описаны в эксплуатационной документации.

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 и восстановления из резервных копий.

Обновления и сопровождение

Реализован регламент выпуска, тестирования и установки обновлений, включая:

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

1.3 Управление инцидентами и развитие безопасности

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

Подготовлены эксплуатационные материалы, инструкции и базы знаний по развертыванию, эксплуатации и устранению нештатных ситуаций в составе документации на систему.

Учет и устранение выявленных уязвимостей

В Global System реализованы следующие 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 (высокий, средний, низкий);
- устранение уязвимостей, связанных с внедрением серверных шаблонов, путем запрета передачи и изменения шаблонов со стороны клиента;
- защита от внедрения SQL-кода за счет проверки, фильтрации и экранирования пользовательских данных;
- контроль и корректная проверка прав доступа при обращении к REST- и SOAP-сервисам;
- защита от межсайтового выполнения сценариев (XSS) путем обязательного экранирования пользовательского ввода;
- снижение риска подбора учетных данных за счет использования современных механизмов аутентификации и ограничения количества попыток входа;
- документирование реализованных мер и контроль их актуальности при обновлении системы.

2 Рекомендации по информационной безопасности

2.1 Общие рекомендации

Требования к паролям

Для обеспечения безопасности учётных записей в Global ERP все сотрудники обязаны соблюдать следующие правила:

- **Длина и сложность**:
  → Пароль должен содержать не менее 12 символов, включая заглавные и строчные буквы, цифры и специальные знаки (например, `!`, `@`, `#`).
- **Запрещённые действия**:
  → Не допускается использование стандартных или простых паролей;
  → Запрещается записывать пароли на бумажных носителях, хранить в незащищённых файлах или передавать третьим лицам.
- **Рекомендация**:
  → Для создания и безопасного хранения паролей компания рекомендует использовать корпоративный менеджер паролей (например, Bitwarden, 1Password, Keeper).

Использование двухфакторной аутентификации (2FA)

Для доступа к критически важным функциям системы требуется дополнительный способ подтверждения личности:

- **Область применения**:
  → 2FA обязательна для всех администраторов системы и пользователей с расширенными правами доступа.
- **Способы подтверждения**:
  → В качестве предпочтительного метода используются мобильные приложения-аутентификаторы (например, Microsoft Authenticator, Google Authenticator) или аппаратные ключи безопасности (YubiKey, Google Titan).
- **Ограничение**:
  → Использование SMS для подтверждения не рекомендуется в целях безопасности.

Принцип предоставления минимальных прав доступа

Компания следует правилу, согласно которому пользователи получают ровно тот уровень доступа, который необходим для выполнения их рабочих задач:

- **Разделение обязанностей**:
  → Администраторы, управляющие функционалом Global ERP, не могут одновременно быть администраторами операционной системы или баз данных PostgreSQL.
- **Регулярная проверка**:
  → Не реже одного раза в квартал проводится аудит прав доступа.

Действия при возникновении инцидента информационной безопасности

При подозрении на взлом, утечку данных или компрометацию:

1. **Изолировать систему**: отключить сервер от корпоративной сети.
2. **Сохранить доказательства**: обеспечить сохранность всех логов (ОС, БД, приложение); не вносить изменения.
3. **Уведомить службу безопасности**: проинформировать службу информационной безопасности.
4. **Ожидать инструкций**: не восстанавливать систему до разрешения специалистов.

Политика резервного копирования данных

- **Регулярность**: ежедневное автоматическое резервное копирование.
- **Безопасное хранение**: копии хранятся на отдельном, изолированном сервере.
- **Шифрование**: все резервные копии шифруются алгоритмом AES-256.
- **Проверка работоспособности**: не реже раза в квартал проводится тестовое восстановление.

Запрет на использование неавторизованных сервисов

Категорически запрещено:

- Размещать данные из Global ERP в публичных облаках (Google Drive, Dropbox, Яндекс.Диск и т.п.);
- Передавать логины, пароли, логи или конфигурации через личную почту, мессенджеры (Telegram, WhatsApp, Viber) или соцсети;
- Копировать данные на личные USB-накопители.

  Все данные должны обрабатываться только в рамках корпоративной инфраструктуры.

Обучение в области информационной безопасности

- **Регулярность**: ежегодное обязательное обучение для всех пользователей Global ERP.
- **Ключевые темы**: противодействие фишингу, социальной инженерии, безопасная работа с данными.

Средства защиты информации на автоматизированных рабочих местах

Каждое рабочее место с доступом к Global ERP должно быть защищено:

- **Антивирусная защита**:
  → Установлена и активирована программа, одобренная ИТ-отделом;
  → Запрещено отключать защиту или менять настройки без согласования;
  → Базы обновляются автоматически.
- **Межсетевой экран (Firewall)**:
  → Активирован на всех станциях и серверах;
  → Правила ограничивают трафик только необходимыми сервисами.
- **Обновление ПО (Patch Management)**:
  → ОС и приложения (браузеры, Java, Adobe Reader, Office) обновляются в течение 72 часов для критических патчей;
  → Запрещено отключать автообновления.

2.2 Рекомендации по безопасности Global ERP

Security Baseline — базовый уровень безопасности

Сценарий A: Готовый baseline (рекомендуется)

- Файл: `security_baseline.conf` (`/etc/erp/`)
- Скрипт: `apply-security-baseline.sh`
- В UI: «Безопасность → Применить базовый профиль»

  После применения проверяется:

  - Учётные записи `admin`, `demo` — отключены;

- MFA для админов — включена через Microsoft Authenticator, Google Authenticator или YubiKey;
- TLS 1.2+ — активен, TLS 1.0/1.1 — отключены;
- Процесс запущен от отдельного пользователя ОС (не `root`).

Сценарий B: Ручная настройка

- Отключить все учётные записи по умолчанию;
- Настроить MFA через Microsoft Authenticator, Google Authenticator или YubiKey;
- Включить TLS 1.2 или выше, отключить TLS 1.0/1.1;
- Запускать процесс от отдельного пользователя ОС.

Управление ролями и полномочиями

- Использовать предопределённые роли (не назначать права вручную);
- Проводить анализ SoD (например: «создать поставщика» + «оплатить счёт» — запрещено одному пользователю);
- Запретить использование ролей типа `SAP_ALL` или `ERP_SUPER_ADMIN` в повседневной работе;
- Все изменения в ролях — утверждать и логировать.

Мониторинг критических операций

Отслеживать через Splunk, IBM QRadar, Elastic SIEM или Microsoft Sentinel:

- Изменение мастер-данных (контрагенты, банки, цены);
- Массовый экспорт данных (>1000 записей);
- Действия в нерабочее время (22:00–6:00);
- Попытки обхода контрольных процедур.

  Логи хранить не менее 180 дней.

Требования к инфраструктуре

- **Поддерживаемые ОС**:
  → Linux: RHEL 8+, Ubuntu 20.04 LTS+;
  → Windows: Windows Server 2016+.
- **Версия PostgreSQL**: 12, 13, 14 или 15.
- Сервер Global ERP и БД — в изолированной VLAN, без доступа из интернета;
- Доступ к веб-интерфейсу — только через reverse proxy (nginx, Apache) с TLS 1.2+;
- **Физический доступ** к серверам — ограничен (только авторизованный персонал).

Настройка PostgreSQL

- **Запрещено** использовать учётную запись `postgres` для работы приложения.
- Создать отдельного пользователя БД (например, `erp_app`).
- В файле `pg_hba.conf` разрешить подключения только с IP-адреса сервера приложения, используя метод аутентификации `scram-sha-256`.
- В файле `postgresql.conf` установить параметры:
  → `ssl = on` — для шифрования трафика;
  → `log_statement = 'mod'` — для логирования всех операций изменения данных (DDL и DML).

Управление обновлениями

- **Сроки установки**:
  → Все security-патчи должны быть установлены в течение 30 календарных дней.
- **Тестирование**:
  → Перед установкой — обязательное тестирование в staging-среде.
- **Источники**:
  → Только официальный портал поддержки или подписанные репозитории (APT/YUM с проверкой GPG-подписи).

Безопасность при кастомизации

- **Анализ зависимостей**:
  → Использовать Snyk или OWASP Dependency-Check для сканирования библиотек.
- **Запрещённые компоненты**:
  → Log4j 1.x, jQuery < 3.5, Spring Framework $< 5.3.0$.
- **Анализ кода**:
  → Прогонять код через SonarQube или Semgrep (SAST).
- **Запрещено в продакшене**:
  → `eval()`,
  → динамический SQL без параметризации,
  → отладочные консоли.

Устранение технического долга

- **Запрещено оставлять**:
  → Временные учётные записи;
  → Правила firewall «разрешить всё»;
  → Устаревшие ОС/PostgreSQL без плана обновления.
- **Исключения**:
  → Должны иметь обоснование, утверждение ИБ-службы и срок действия (30 дней).

Интеграция с корпоративными системами мониторинга и SIEM

- **Метрики**:
  → Эндпоинт `/metrics` (Prometheus) → визуализация в Grafana.
- **Логи**:
  → Экспорт через Syslog (TCP) или вебхуки (JSON over HTTPS) → Splunk / QRadar / Elastic SIEM.
- **Доступность**:
  → Проверки в Zabbix на `/health`, валидность TLS, задержку транзакций.

2.3 Security by Design: как безопасность встроена в Global ERP

Архитектура

- **Zero Trust**: нет доверия к внутренней сети.
- **Threat Modeling**: по методологии STRIDE для каждого компонента.
- **Изоляция данных**: при мульти-тенантности — логическая или физическая.

Аутентификация

- **Стандарты**: SAML 2.0, OpenID Connect, OAuth 2.0.
- **MFA**: TOTP (Google Authenticator, Microsoft Authenticator), FIDO2 (YubiKey).
- **Блокировка**: после 5 неудачных попыток.
- **История паролей**: 24 последних пароля не могут быть повторно использованы.

Авторизация

- **RBAC/ABAC**: встроенные механизмы.
- **SoD**: предотвращение конфликтов («создать + оплатить»).
- **Минимальные привилегии**: по умолчанию — только чтение.

Защита данных

- **In transit**: TLS 1.2+ (SSL 3.0, TLS 1.0/1.1 — отключены).
- **At rest**:
  → ОС: BitLocker (Windows), LUKS (Linux);
  → Приложение: AES-256-GCM для ПДн (ИНН, СНИЛС).
- **Маскировка**: ПДн автоматически скрываются в логах и UI.

Защита от атак

- **SQLi**: только параметризованные запросы.
- **XSS**: автоматическое экранирование + CSP.
- **CSRF**: anti-CSRF токены.
- **IDOR**: проверка прав на каждый запрос к объекту.

Сессии

- **Тайм-аут**: 15 минут бездействия.
- **Управление**: централизованное разлогирование.
- **Cookies**: флаги `HttpOnly`, `Secure`, `SameSite=Strict`.

Аудит

- **Логируются**: вход/выход, экспорт данных, изменение ролей.
- **Форматы**: Syslog, CEF, JSON для SIEM.
- **Хранение**: 180+ дней, защита от модификации.

Инфраструктура, секреты, DevSecOps, обновления, документация

(Содержание остаётся технически точным и детальным, как в предыдущей версии — все инструменты и стандарты уже указаны.)

2.4 Соответствие требованиям (Compliance)

- **GDPR**: шифрование ПД (AES-256-GCM), право на удаление, аудит.
- **ФЗ-152**: защита ПД, SoD, логирование.
- **PCI DSS**: MFA (Authenticator/YubiKey), пароли (12+ символов), логи.
- **ISO 27001:2022**:
  - A.8.9 — управление доступом (раздел 2.2),
  - A.8.16 — мониторинг (раздел 2.3),
  - A.8.23 — обработка данных (раздел 3.4).