КОМПЛЕКСНЫЕ ИНФОСИСТЕМЫ · ГРУППА КОМПАНИЙ ТЕХНОИНЖИНИРИНГ

РУКОВОДСТВО ПО ПЛАНИРОВАНИЮ · ДЛЯ ИТ- И ИБ-СЛУЖБ

Платформа ГАУС: ИТ-инфраструктура и информационная безопасность

Что нужно знать ИТ-службе и службе информационной безопасности заказчика при планировании внедрения: размещение компонентов, сетевые взаимодействия, сегментация, функции ИБ, соответствие требованиям регуляторов, защищённая настройка.

KIS-IT-2026-001	0.2	25.08.2026	2.0.x
Обозначение документа	Версия документа	Дата ревизии	Версия платформы

Содержание

1. О документе

2. Компоненты и их размещение

3. Сетевые взаимодействия

4. Сегментация сети

5. Требования к окружению

6. Каталог функций информационной безопасности

7. Контур ГАУС.Copilot с точки зрения ИБ

8. Соответствие мерам приказов ФСТЭК №31 и №239

9. Чек-лист защищённой настройки

10. Обновления, резервное копирование, жизненный цикл

11. Контакты

1. О документе

Документ адресован ИТ-службе и службе информационной безопасности заказчика. Он отвечает на вопросы, которые обычно задают на этапе согласования внедрения: «что и где будет установлено», «какие соединения открыть на межсетевых экранах», «как платформа вписывается в нашу модель угроз и требования регуляторов», «как настроить систему защищённо».

1.1. Связанные документы

Обозначение	Документ
KIS-TO-PLT-2026-001	Техническое описание платформы — архитектура, характеристики, сайзинг
KIS-AG-2026-001	Архитектурный гайд: типовые архитектуры А1–А6
KIS-DS-PLT-2026-001	Датшит «Платформа ГАУС»
KIS-REG-2026-001	Регуляторная справка: реестр ПО, сертификаты, совместимости
KIS-OL-BMS-2026-001	Опросный лист — сбор исходных данных, включая раздел ИТ и ИБ

1.2. Термины

Компонент платформы — служба или приложение из состава поставки. **Полевой уровень** — контроллеры, приборы и датчики объекта. **Наложенные средства защиты (СЗИ)** — внешние средства защиты информации, применяемые заказчиком. **КИИ** — критическая информационная инфраструктура (187-ФЗ).

2. Компоненты и их размещение

Состав развёртывания зависит от выбранной архитектуры (A1–A6, см. KIS-AG-2026-001). Полный перечень возможных компонентов:

Компонент	Где размещается	Примечание для ИТ-службы
Центральный сервер (микросервисы)	серверный сегмент АСУ; физический сервер или ВМ	ядро системы; при резервировании — пара узлов (основной + горячий резерв)
Служба архива	совместно с сервером или выделенный узел / пара узлов	наибольшие требования к дисковой подсистеме; зеркалирование на два узла
Драйверы протоколов	сервер или отдельные хосты ввода-вывода	хосту ввода-вывода нужен сетевой доступ к своему полевому сегменту
Видеосервис	сервер или выделенный узел	трафик RTSP от камер; нагрузка растёт с числом камер и раскладок
Интеграционные шлюзы (OPC UA-сервер, Modbus TCP-сервер)	сервер; при передаче наружу — граница сегмента	единственные компоненты, публикующие данные во внешние системы
ГАУС Супервизор	серверный сегмент	мониторинг компонентов и автоматическое резервное копирование
Edge-компоненты	панели и шкафы на объекте	локальная автономная работа; синхронизация с центром при наличии связи
Десктоп-клиент	АРМ диспетчеров и инженеров (Windows)	также используется как среда разработки проекта — доступ по ролям
Веб- и мобильный клиенты	браузер / устройства пользователей	доступ через веб-интерфейс платформы; вне периметра — только через решения удалённого доступа заказчика
ГАУС.Copilot (ассистент + MCP-сервер)	сервис ассистента — серверный сегмент или АРМ; MCP-шлюз — внутри десктоп-клиента (локально); LLM — локальный узел или облако	подробно — раздел 7
СУБД (PostgreSQL / SQLite)	совместно с сервером или по политике заказчика	проект и данные платформы; резервное копирование обязательно

3. Сетевые взаимодействия

Таблица направлений соединений — основа для правил межсетевых экранов. Указаны **порты по умолчанию** из конфигураций компонентов; при развёртывании все они настраиваются.

Откуда	Куда	Протокол · порт по умолч.	Назначение · защита
Десктоп-клиент	Центральный сервер	HTTP 8082 / HTTPS 8083 · gRPC 9082	рабочий обмен АРМ и среды разработки · TLS (8083)
Веб-/мобильный клиент	Центральный сервер	HTTPS 8083 · WSS 8084	веб-интерфейс и живые обновления · TLS
Драйверы, Edge-узлы, шлюзы	Сервер (модуль сбора данных)	gRPC · 12000	поток значений · взаимный TLS (mTLS); подтверждения + файловый буфер при обрыве
Сервер (модуль сбора)	Драйверы протоколов	gRPC · 11000–11011	управление и конфигурация драйверов (свой порт у каждого драйвера)
Центральный сервер	Служба архива (Historian)	gRPC 14000 · HTTP 14001	запись/чтение временных рядов; клиенты ходят только через прокси платформы (/api/historian на 8083) — прямые порты архива в проде закрываются
Компоненты платформы	Сервис журнала	gRPC · 13000	глобальный журнал событий
Компоненты платформы	PostgreSQL	TCP · 5432 (резерв 5433)	проект и данные; пул платформы рассчитан под max_connections=100
ИТ-служба (браузер)	Супервизор	HTTP · 24680	веб-интерфейс мониторинга и бэкапов — только для служебного персонала
Драйвер OPC UA	OPC UA-серверы оборудования	opc.tcp · 4840*	опрос и управление; поддерживаются политики безопасности OPC UA
Драйвер Modbus TCP	контроллеры	TCP · 502*	опрос и управление
Драйвер BACnet/IP	устройства BACnet	UDP · 47808*	опрос, обнаружение устройств; через маршрутизируемые сети — BBMD
Драйвер SNMP	ИТ-оборудование	UDP · 161/162*	опрос метрик, приём трапов
Драйвер MQTT	брокер MQTT	TCP · 1883/8883*	подписка на топики; 8883 — с TLS
Видеосервис	IP-камеры, регистраторы	RTSP · 554* / ONVIF	приём видеопотоков; клиентам раздаёт HTTP 8085 / WebRTC
Внешняя SCADA	Шлюз Modbus TCP платформы	Modbus TCP · 11010	чтение опубликованных тегов (режим slave); состав публикации ограничен настройкой
Внешняя SCADA	Шлюз OPC UA платформы	opc.tcp · по конфигурации	чтение опубликованных тегов; адрес конечной точки задаётся при развёртывании
Внешние ИТ-системы	REST API / gRPC / WebSockets	HTTPS 8083 · gRPC 9082	интеграция ERP/ТОиР/BI · TLS, авторизация
Сервер (уведомления)	Telegram / SMTP / SMS-шлюз	HTTPS / SMTP	исходящие уведомления; при запрете внешних соединений — отключается
Компоненты платформы	NTP-сервер заказчика	UDP · 123*	синхронизация времени — обязательна для корректности журналов

* Стандартные порты соответствующих протоколов; фактические значения зависят от настройки оборудования заказчика. Внутри серверного сегмента работают также служебные сервисы платформы (сценарии 8143, вычисляемые выражения 5043, отчёты 38082/39082, лицензионный сервис 48082/49082, хранилище медиа 8086, видео gRPC 29082, резервный узел 18082/19082, шина архива NATS 4222 — при включении) — наружу сегмента они не публикуются. Диагностические pprof-порты по умолчанию выключены и включаются только на время разбора инцидентов.

ПРИНЦИП

Все соединения инициируются изнутри периметра платформы или клиентами заказчика. Платформа не требует входящих соединений из интернета; внешний доступ (мобильные пользователи вне площадки) организуется штатными средствами удалённого доступа заказчика (VPN и аналоги).

4. Сегментация сети

Рекомендуемое разбиение на зоны (согласуется с политикой заказчика и требованиями к КИИ):

ЗОНА 1 **Полевой сегмент**

Контроллеры, приборы, камеры, Edge-узлы. Доступ — только хостам ввода-вывода и видеосервису платформы. Прямой доступ пользователей и корпоративной сети — запрещён.

ЗОНА 2 **Серверный сегмент платформы**

Центральный сервер (и резерв), архив, Супервизор, СУБД, шлюзы, узел LLM (при on-premise). Межсетевой экран пропускает только направления из таблицы раздела 3.

ЗОНА 3 **Клиентский сегмент**

АРМ диспетчеров и инженеров, видеостена. К серверному сегменту — только клиентские порты платформы; в полевой сегмент доступа нет.

ЗОНА 4 **Корпоративная сеть / внешние системы**

Веб-пользователи, ERP/ТОиР/BI, вышестоящие SCADA. Взаимодействие — только через веб-интерфейс, API и интеграционные шлюзы; публикация данных наружу — выборочная.

- Мобильный доступ извне — через VPN-контур заказчика; платформа не публикуется в интернет напрямую.
- При требованиях однонаправленной передачи в корпоративный сегмент применяются шлюзы платформы в сочетании со средствами однонаправленной передачи заказчика.
- Для территориально распределённых объектов (архитектуры А4/А5) связь площадок с центром — по защищённым каналам заказчика; при обрывах данные буферизуются на площадках и досылаются автоматически.

5. Требования к окружению

Категория	Требование
ОС сервера	Windows, Linux — включая Astra Linux и РЕД ОС (сертификаты совместимости); версии — уточняется
ОС АРМ	Windows; веб-клиент — Chrome, Safari, Firefox (Windows, Linux, macOS)
СУБД	PostgreSQL (порт 5432; при резервировании БД — вторая на 5433), SQLite; архив — специализированное хранение временных рядов. Пул соединений платформы рассчитан под стандартный max_connections=100 (30 — ядро, 30 — модуль сбора, остальное — резерв)
Виртуализация	развёртывание в ВМ поддерживается; перечень проверенных гипервизоров — уточняется
Ресурсы серверов	подбираются по масштабу проекта — методика сайзинга в KIS-TO-PLT-2026-001, разделы 7 и 9
Синхронизация времени	NTP-источник заказчика для всех компонентов — обязательна (корректность журналов и трендов)
Антивирусная защита	подтверждена совместимость с Kaspersky Industrial CyberSecurity; работа под наложенными СЗИ
Резервное копирование	автоматические копии проекта и настроек Супервизором; хранение копий — по политике заказчика

6. Каталог функций информационной безопасности

Функция	Реализация в платформе
Идентификация и аутентификация	собственные учётные записи с парольной политикой; импорт пользователей и групп из LDAP / Active Directory
Разграничение доступа (RBAC)	роли и группы; права на разделы системы, страницы, устройства и управление — вплоть до элемента экрана; скрытие элементов интерфейса по правам
Защита каналов	TLS/HTTPS на клиент-серверном обмене и между компонентами платформы
Регистрация событий безопасности	журнал действий пользователей (входы, изменения уставок и конфигурации, квитирования), глобальный системный журнал, журнал действий ИИ-агента; фильтры и выгрузки
Целостность и доступность данных	гарантированная доставка данных между компонентами (подтверждения, буферизация); горячее резервирование; зеркалирование архива; автономность Edge-узлов
Резервное копирование	автоматические копии проекта по расписанию (Супервизор); восстановление по документированной процедуре
Контроль публикации данных	во внешние системы передаётся только явно разрешённый набор тегов (шлюзы OPC UA / Modbus TCP)
Мониторинг компонентов	Супервизор: состояние служб, диагностика, уведомления о неисправностях
Режим без браузера	полнофункциональный десктоп-клиент для предприятий с запретом браузеров

7. Контур ГАУС.Copilot с точки зрения ИБ

ИИ-ассистент не создаёт нового канала доступа к данным: каждое поручение транслируется MCP-сервером в штатную операцию платформы от имени текущего пользователя и проходит те же проверки прав, что и ручные действия.

Аспект	Гарантия
Права	ассистент работает строго в границах прав сеанса пользователя; расширить доступ запросом невозможно
Отдельные разрешения	ассистенту можно разрешить меньше, чем пользователю (например, только чтение)
Изменения	применяются только после явного подтверждения человеком; каждое действие — в журнале платформы
Размещение языковой модели	по выбору службы ИБ: локальная (on-premise) — данные не покидают контур, вариант для КИИ и закрытых сетей; либо облачная
База знаний объекта	документы заказчика индексируются в базе знаний ассистента в контуре платформы
Сетевой след	шлюз ассистента работает внутри десктоп-клиента и слушает только локальный интерфейс АРМ (по умолчанию 127.0.0.1:7700) — в сеть не публикуется
Отключение	ИИ-контур — отдельный компонент: может не разворачиваться вовсе; его отсутствие не влияет на платформу

8. Соответствие мерам приказов ФСТЭК №31 и №239

Таблица показывает, какими механизмами платформа **поддерживает** реализацию базовых групп мер защиты для АСУ ТП (приказ ФСТЭК №31) и значимых объектов КИИ (приказ №239). Итоговый состав мер определяется категорированием и проектом системы защиты заказчика; часть мер по определению реализуется организационно и наложенными СЗИ.

Группа мер	Поддержка платформой	Организационно / СЗИ
ИАФ — идентификация и аутентификация	учётные записи, парольная политика, LDAP/AD	политика паролей, MFA средствами инфраструктуры
УПД — управление доступом	ролевая модель до элемента экрана; раздельные права на чтение/управление/конфигурирование	регламент выдачи и пересмотра прав
РСБ — регистрация событий безопасности	журналы действий, системный журнал, журнал ИИ-агента; выгрузка для SIEM через БД/API	SIEM и анализ инцидентов
ОЦЛ / ОДТ — целостность и доступность	гарантированная доставка, горячий резерв, зеркалирование архива, автономные Edge, бэкапы	ИБП, резервирование каналов связи
ЗИС — защита информационной системы и каналов	TLS между компонентами; выборочная публикация тегов наружу	сегментация, МЭ, криптошлюзы, однонаправленные шлюзы
АНЗ — анализ защищённости	работа под наложенными СЗИ (совместимость с Kaspersky ICS)	сканеры защищённости, аудит
АВЗ — антивирусная защита	совместимость с Kaspersky Industrial CyberSecurity	развёртывание и политика АВЗ
УКФ — управление конфигурацией	проект в БД, журнал изменений конфигурации, резервные копии, восстановление	регламент управления изменениями

ПРИМЕЧАНИЕ

Таблица — предварительная карта поддержки, подготовлена для обсуждения со службами ИБ; не является заключением о соответствии. Детальная таблица «мера → механизм → настройка» по составу мер конкретного проекта — уточняется.

9. Чек-лист защищённой настройки

Минимальный набор шагов при вводе системы в эксплуатацию:

9.1. Учётные записи и доступ

- ☐ Сменены пароли всех предустановленных учётных записей; заведены персональные учётки (без общих «operator»)
- ☐ Роли настроены по принципу минимальных прав: диспетчеру — управление, наблюдателю — чтение, подрядчику — только его контур
- ☐ Права на конфигурирование проекта — только у инженеров-настройщиков
- ☐ При использовании LDAP/AD — синхронизация групп проверена, увольнение сотрудника блокирует доступ
- ☐ Ассистенту ГАУС.Copilot заданы отдельные разрешения (если развёрнут); режим подтверждения изменений включён

9.2. Сеть и каналы

- ☐ TLS включён на клиент-серверных и межкомпонентных соединениях
- ☐ Правила межсетевых экранов ограничены таблицей раздела 3; неиспользуемые направления закрыты
- ☐ Сегментация по зонам раздела 4 реализована; прямого доступа корпоративной сети в полевой сегмент нет
- ☐ Внешний доступ — только через VPN-контур заказчика; платформа не опубликована в интернет
- ☐ NTP-синхронизация настроена для всех компонентов
- ☐ Прямые порты службы архива (14000/14001) закрыты для клиентов — доступ только через прокси платформы; диагностические pprof-порты выключены

9.3. Данные и живучесть

- ☐ Автоматическое резервное копирование включено; восстановление из копии проверено на практике
- ☐ При повышенных требованиях к доступности — горячее резервирование и зеркалирование архива развёрнуты и протестированы переключением
- ☐ Публикация тегов во внешние системы сверена: наружу отдаётся только необходимый набор
- ☐ Журналы включены; глубина хранения журналов согласована с ИБ; выгрузка в SIEM настроена (при наличии)
- ☐ Уведомления во внешние сервисы (Telegram, e-mail, SMS) согласованы с ИБ или отключены

9.4. Эксплуатация

- ☐ Установлена актуальная версия платформы; порядок получения обновлений согласован (тариф поддержки)
- ☐ Наложенные СЗИ (антивирус, контроль целостности) развёрнуты по политике заказчика
- ☐ Изменения конфигурации проходят по регламенту заказчика; проверка на симуляции перед применением к оборудованию

- [ ] Физический доступ к серверам и щитам с Edge-узлами ограничен

10. Обновления, резервное копирование, жизненный цикл

- **Обновления платформы.** Регулярные релизы; обновление версии — с сохранением прикладного проекта. Изменения прикладного проекта не требуют останова. Доступ к новым версиям — по тарифам поддержки (от «Базового»).
- **Исправления безопасности.** Устранение подтверждённых уязвимостей и неисправностей — в рамках технической поддержки; уведомление заказчиков по договорам поддержки.
- **Резервное копирование.** Супервизор выполняет автоматические копии проекта и настроек по расписанию; ответственность за хранение копий вне узла — на стороне заказчика (политика 3-2-1 рекомендуется).
- **Окончание поддержки версий.** Заблаговременное информирование публикацией и уведомлением заказчиков по договорам поддержки.

11. Контакты

Вопросы по разделам документа, уточнение конфигурации портов под конкретный проект, проработка проекта системы защиты — техническая поддержка и инженеры производителя.

ООО «Комплексные Инфосистемы» · группа компаний ТехноИнжиниринг
8 800 600 15 87 · sales@info-systems.pro

Технические консультации
по запросу, с участием инженера