

АЕГИС

Архитектура, развёртывание и безопасность

Компоненты, размещение, доступ, обмен данными и
распределение ответственности.

ПОНЯТЬ УСТРОЙСТВО. ОБСУДИТЬ ПОДКЛЮЧЕНИЕ.

От задачи организации — к рабочему составу продукта.

Содержание

Архитектура, развёртывание и безопасность

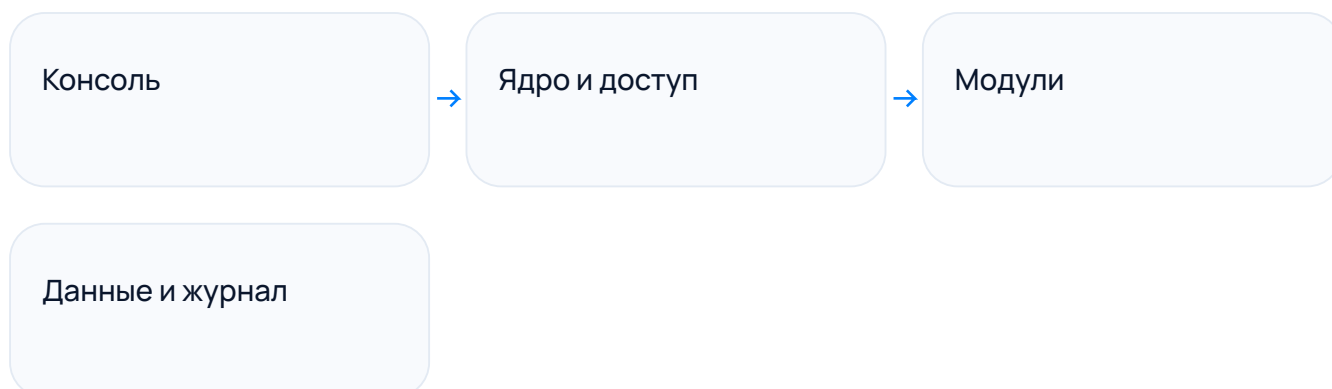
01	Архитектура вокруг единого контекста	3
02	Консоль оператора	4
03	Ядро и объектная модель	5
04	Облачное размещение	6
05	Установка в контуре организации	7
06	Изолированный контур	8
07	Рабочие области и изоляция данных	9
08	Ролевая модель доступа	10
09	Аутентификация и идентификация	11
10	Журнал действий	12
11	Материалы проверки и хранение	13
12	Категории интеграций	14
13	API и уведомления по событиям	15
14	Обновления и управление изменениями	16
15	Окружение и ответственность	17
	Контакты и консультация	18

Архитектура вокруг единого контекста

Общее ядро связывает доступ, рабочие области, активы, находки и материалы проверки.

Пользователь работает через консоль. Проверка полномочий определяет доступ к объектам выбранной области. Модули используют общую модель результатов и журналирования.

Такое разделение позволяет рассматривать изменение объекта вместе с его происхождением и ответственным действием. Состав компонентов и подключений фиксируют в конфигурации поставки.



Консоль оператора

Интерфейс связывает список объектов с их рабочими карточками.

Для активов важны тип, идентификатор, метки и источник. Для находок — состояние, комментарии и доказательства. Просмотр карточки должен сохранять контекст рабочей области.

Доступные действия зависят от роли. Разделение просмотра и изменения помогает организовать совместную работу аналитика, специалиста по оценке и администратора.

The screenshot displays the 'АЕГИС' (AEgis) interface, specifically the 'Консоль / Активы' (Console / Assets) section. The left sidebar contains navigation links: 'Рабочая область' (Working Area), 'Активы' (Assets), 'Находки' (Findings), 'Проверки' (Checks), and 'Настройки' (Settings). The main content area is titled 'Реестр активов' (Assets Register) and shows a table of assets. The table has four columns: 'Объект' (Object), 'Тип' (Type), 'Область' (Area), and 'Состояние' (Status). The data rows are as follows:

Объект	Тип	Область	Состояние
Шлюз доступа	Сетевой узел	Внешний контур	В работе
Каталог учётных записей	Инфраструктура	Внутренний контур	В работе
Прикладной интерфейс	Веб-приложение	Внешний контур	На проверке
Сервер приложений	Инфраструктура	Внутренний контур	В работе
Рабочая станция	Рабочий узел	Внутренний контур	В работе

At the bottom of the interface, there is a footer with the text 'Белый Веб' (White Web) and 'АЕГИС - Единый контекст активов и результатов' (AEgis - Unified context of assets and results).

- Навигация между активом и результатом.
- Права на чтение и изменение.
- Материалы и история решений.

Ядро и объектная модель

Единые сущности задают связи между этапами работы.

Актив задаёт контекст. Находка описывает проблему. Проверка уточняет результат. Доказательство обосновывает вывод. Комментарий объясняет решение участника.

Связи помогают избежать отрыва результата от источника: при разборе можно вернуться к объекту, материалу и основанию изменения статуса.

Объект	Рабочая роль
Актив	Граница и принадлежность
Находка	Описание проблемы
Проверка	Уточнение результата
Доказательство	Основание заключения
Комментарий	Контекст решения

Облачное размещение

Облачный вариант обсуждают с учётом состава данных и требований организации.

До размещения определяют разрешённые источники, место хранения, каналы передачи и границы администрирования. Для защищаемых данных согласуют порядок доступа и обращения с материалами.

Параметры окружения зависят от конфигурации и источников. Организация и поставщик фиксируют зоны ответственности в документации подключения.

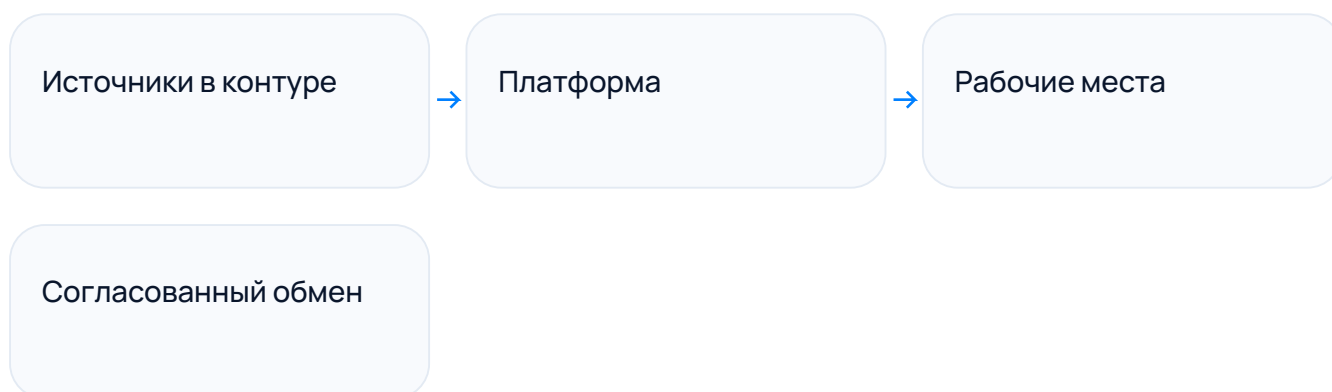
- Место хранения и категории данных.
- Защищённые каналы и допустимый обмен.
- Администрирование и порядок обращения.

Установка в контуре организации

Гибридный формат дополняет облачное ядро узлом-сканером внутри сети организации.

Организация определяет сегмент размещения, источники данных и сетевые ограничения. Поставщик согласует компоненты, точки подключения и порядок проверки работоспособности.

Эксплуатационные требования рассматривают вместе с резервированием, обновлениями и доступом администраторов. Требования к ресурсам определяются при согласовании.



Изолированный контур

Полный образ в контуре без выхода в интернет находится в разработке.

При согласовании определяют разрешённые способы передачи пакетов, проверку их целостности и порядок ввода изменений. Источники сведений и правила проверки должны быть доступны в выбранном контуре.

Процесс обновления включают в эксплуатационный регламент: кто принимает пакет, кто разрешает изменение и как фиксируется результат. Возможности изолированной конфигурации уточняют для поставки.

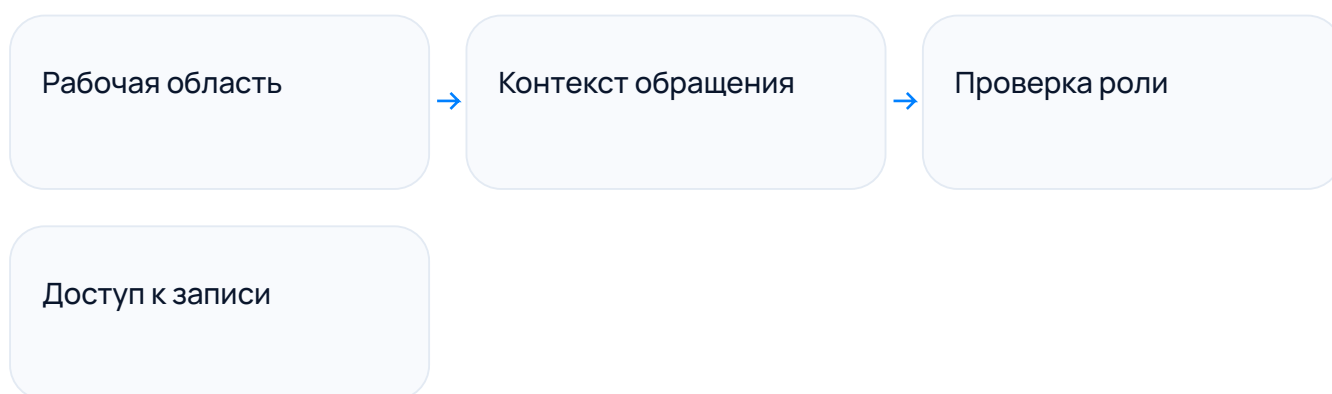
- Разрешённый перенос пакетов.
- Проверка происхождения и целостности.
- Регламент обновления и контроль результата.

Рабочие области и изоляция данных

Разделение данных учитывается на уровне приложения и базы.

Контекст рабочей области сопровождает обращение к объектам. Ограничение записей в базе дополнительно отделяет сведения разных областей.

Права пользователя определяют доступ внутри выбранного контекста. Изоляцию проверяют на операциях чтения, изменения и доступа к связанным материалам.



Ролевая модель доступа

RBAC связывает разрешённые действия с ролью пользователя.

Аналитику нужен просмотр контекста и разбор результатов. Специалисту по оценке — работа с проверками и находками. Администратору — управление доступом и настройками в своей области.

Привилегированные действия выделяют отдельно. При согласовании матрицы прав определяют, кто читает сведения, кто изменяет их и кто принимает решения.

Группа действий	Что согласовать
Просмотр	Объекты и материалы
Изменение	Статусы, метки и комментарии
Администрирование	Учётные записи и настройки
Принятие решения	Ответственные и полномочия

Аутентификация и идентификация

Доступ начинается с подтверждения пользователя и его принадлежности к рабочей области.

Интеграцию с корпоративной системой идентификации рассматривают при подключении. Для неё определяют требования к единому входу, дополнительному подтверждению и управлению учётными записями.

Поддерживаемые способы федерации и дополнительного подтверждения фиксируются для конкретной конфигурации. Изменения доступа должны соответствовать кадровым и организационным процедурам.

- Источник учётных записей.
- Порядок подтверждения личности.
- Выдача, изменение и прекращение доступа.

Журнал действий

Журнал сохраняет основание для разбора изменений и привилегированных операций.

Для события нужны исполнитель, объект, действие и время. Контекст рабочей области позволяет связать запись с нужным набором данных.

При согласовании определяют доступ к журналу, срок хранения и порядок выгрузки. Журнал рассматривается вместе с управлением доступом: возможность изменить объект и право просмотреть историю разделяют.

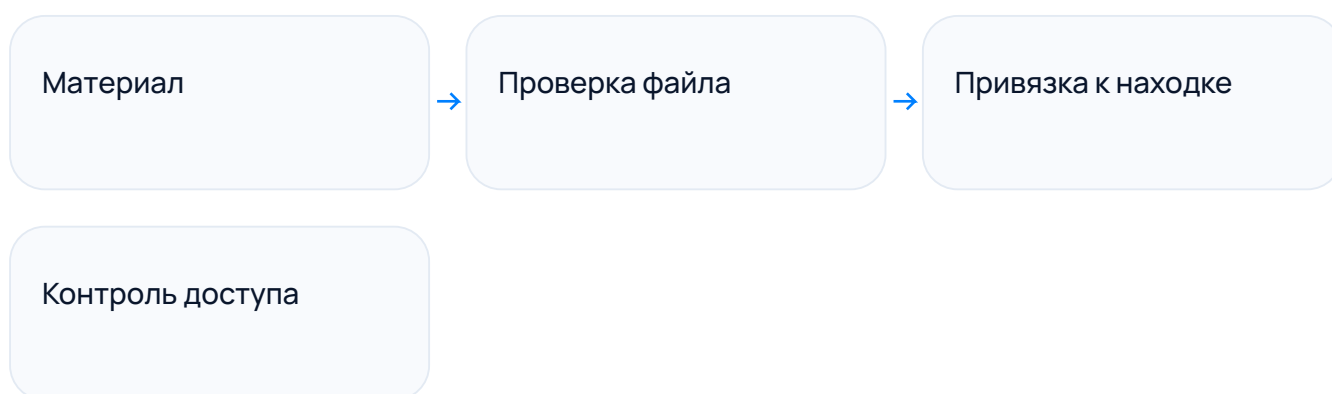
- Исполнитель и объект действия.
- Рабочая область и основание изменения.
- Правила доступа к истории и выгрузкам.

Материалы проверки и хранение

Доказательства содержат сведения, важные для подтверждения результата.

Права доступа к материалам связывают с карточкой находки и рабочей областью. Проверка загружаемых файлов и правила обращения с ними помогают отделить технические артефакты от обычных вложений.

Состав сохраняемых данных, сроки и допустимые форматы согласуют заранее. Избыточные сведения не должны попадать в итоговые материалы без необходимости.



Категории интеграций

Подключения описывают по назначению и направлению передачи данных.

Для мониторинга нужны сигналы и контекст событий. Для систем задач — описание недостатка, ответственное действие и изменение статуса. Для каналов уведомлений — адресат и условия отправки.

Наличие нужного способа обмена и состав коннектора уточняют при согласовании. Названия используемых в организации систем указывают в документации подключения.

Категория	Вход	Выход
Мониторинг	События и сигналы	Связанный контекст
Учёт задач	Состояние работ	Задача и рекомендации
Уведомления	Настройки адресатов	Согласованное сообщение
Источники активов	Сведения об объектах	Обновлённый реестр

API и уведомления по событиям

Машинный обмен должен сохранять контекст, права и понятные правила повторной обработки.

Для API согласуют набор объектов, способы идентификации и доступные операции. Для уведомлений по событиям — условия отправки, принимающую сторону и обработку ошибки.

Секреты подключения относят к отдельной зоне доступа. Передача данных не должна расширять полномочия участника или раскрывать материалы другой рабочей области.

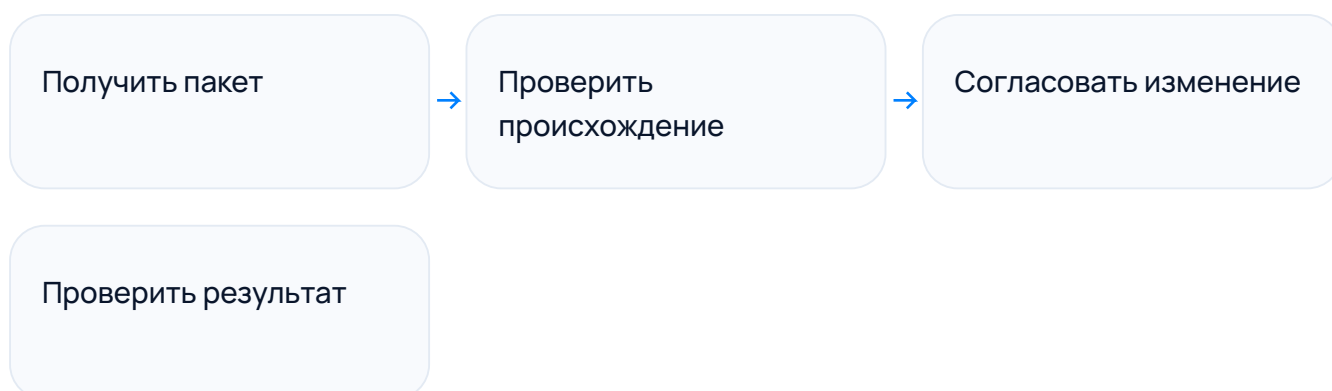
- Состав полей и разрешённые операции.
- Идентификация и защита секретов.
- Обработка ошибок и повторного обмена.

Обновления и управление изменениями

Обновление — согласованное изменение рабочей конфигурации.

До установки определяют источник пакета, порядок проверки целостности и ответственного за разрешение изменения. После установки проверяют доступность нужных функций и сохранность рабочего контекста.

Для изолированного размещения дополнительно согласуют перенос пакетов и локальных источников. Порядок подписания релизов и проверки подписей фиксируют в условиях поставки.



Окружение и ответственность

Требования к окружению определяются при согласовании состава и способа размещения.

Организация определяет защищаемый контур, ответственных и правила обращения с данными. Поставщик согласует состав компонентов, способы подключения и эксплуатационные процедуры.

Решения о месте хранения, резервировании, восстановлении и обновлении документируют до начала работы. Точки взаимодействия должны быть понятны участникам технической и организационной части.

Организация	Поставщик
Границы и разрешения	Состав компонентов
Доступ к источникам	Требования к подключению
Правила хранения	Порядок настройки
Ответственные за изменения	Эксплуатационные рекомендации

Обсудим вашу задачу

Запросить консультацию

Подготовьте описание защищаемого контура, действующие процессы и ожидаемый результат. Состав продукта и параметры подключения определяются при согласовании.

info@whitevweb-security.ru

+7 (993) 405-09-02

whitevweb-security.ru/products/aegis

ООО «Белый Веб» / White Web LLC

ИНН 1685022692 · ОГРН 1251600038084

420132, г. Казань, ул. Фатыха Амирхана, д. 18а, помещ. 1000

Белый Веб — продукты информационной безопасности

v1.0 · 12 октября 2026