

АЕГИС

Методика работ и отчётность

Границы проверки, решения по находкам, структура отчёта и контроль устранения.

ПОНЯТЬ УСТРОЙСТВО. ОБСУДИТЬ ПОДКЛЮЧЕНИЕ.

От задачи организации — к рабочему составу продукта.

Содержание

Методика работ и отчётность

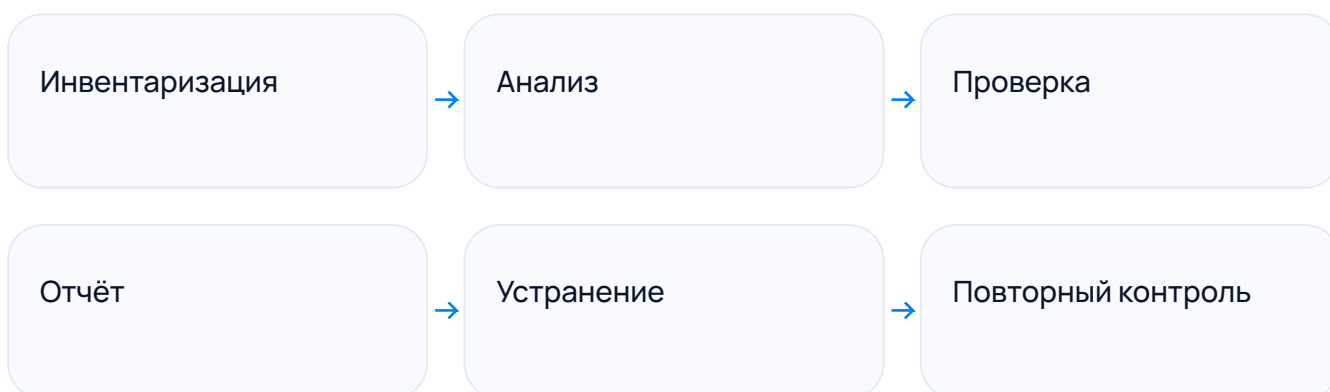
01	Цикл управления уязвимостями	3
02	Границы и согласование	4
03	Инвентаризация и источники	5
04	Приоритизация и проверка	6
05	Статусы и основания решений	7
06	Резюме для руководства	8
07	Структура технического отчёта	9
08	Доказательства и рекомендации	10
09	Исправления и повторная проверка	11
10	Данные и регламенты безопасности	12
11	Подготовка к подключению	13
	Контакты и консультация	14

Цикл управления уязвимостями

Методика связывает актив, результат проверки и решение по устранению.

Работу начинают с инвентаризации и границ. Результаты анализа связывают с активами, приоритетами и доказательствами. Затем формируют рекомендации и согласуют исправления.

Повторная проверка подтверждает изменение состояния. Если условия работы изменились, результат рассматривают в новом контексте, сохраняя историю первоначального решения.



Границы и согласование

Проверка проводится только в определённых и согласованных границах.

Фиксируют домены, адреса, приложения и исключения. Для активных действий согласуют условия выполнения и ответственных за остановку или изменение работ.

Границы задают не только список целей, но и ограничения: какие данные допустимо сохранять, какие действия разрешены и каким способом передавать результат.

- Перечень объектов и исключений.
- Разрешённые действия и условия выполнения.
- Ответственные и порядок изменения границ.

Инвентаризация и источники

Реестр должен отражать принадлежность и происхождение сведений об активе.

На старте собирают идентификаторы объектов и связывают их с нужной областью. Данные из разных источников сопоставляют, чтобы не принять одну и ту же запись за разные активы.

История изменения и метки помогают поддерживать контекст. Исключённые объекты отделяют от актуального перечня, сохраняя основание решения.

АЕГИС УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ Рабочая область Активы Находки Проверки Настройки Белый Веб	Консоль / Активы		
	Реестр активов		
	Принадлежность, тип, источник и состояние объекта		
	Объект	Тип	Область
	Шлюз доступа	Сетевой узел	Внешний контур
	Каталог учётных записей	Инфраструктура	Внутренний контур
	Прикладной интерфейс	Веб-приложение	Внешний контур
	Сервер приложений	Инфраструктура	Внутренний контур
	Рабочая станция	Рабочий узел	Внутренний контур
АЕГИС · Единый контекст активов и результатов			

- Идентификатор, тип и принадлежность.
- Источник и подтверждение сведений.
- Связи, метки и основания исключений.

Приоритизация и проверка

Приоритет объясняет, почему находкой нужно заниматься в выбранном порядке.

Учитывают доступность актива, его значимость, характер недостатка и подтверждённый результат. Автоматический сигнал не заменяет итоговое заключение специалиста.

Проверка должна оставить материалы, позволяющие понять основание вывода. Рекомендации формулируют в терминах изменений, которые команда может согласовать и проверить.

Основание	Вопрос для разбора
Актив	Какой объект затронут?
Доступность	В каких условиях проявляется проблема?
Доказательства	На чём основано заключение?
Исправление	Как проверить результат изменения?

Статусы и основания решений

Статус находки сохраняют вместе с объяснением и материалами.

Подтверждена: результат обоснован проверкой. Не эксплуатируется: проблема не подтверждена в согласованных условиях. Принятый риск: ответственное лицо зафиксировало решение и его основания.

Ложное срабатывание: исходное наблюдение не подтверждает заявленную проблему. Изменение условий или новые сведения могут потребовать повторного рассмотрения.

Статус	Основание
Подтверждена	Материалы проверки
Не эксплуатируется	Условия и результат проверки
Принятый риск	Решение ответственного
Ложное срабатывание	Аргументы и проверенный контекст

Резюме для руководства

Резюме связывает технический результат с необходимым решением.

В начале отчёта описывают границы и основные выводы. Затем выделяют причины приоритета, затронутые направления и предлагаемые действия.

Резюме не дублирует весь реестр. Его задача — дать понятное основание для согласования исправлений и ответственных, сохраняя ссылку на подробные материалы.

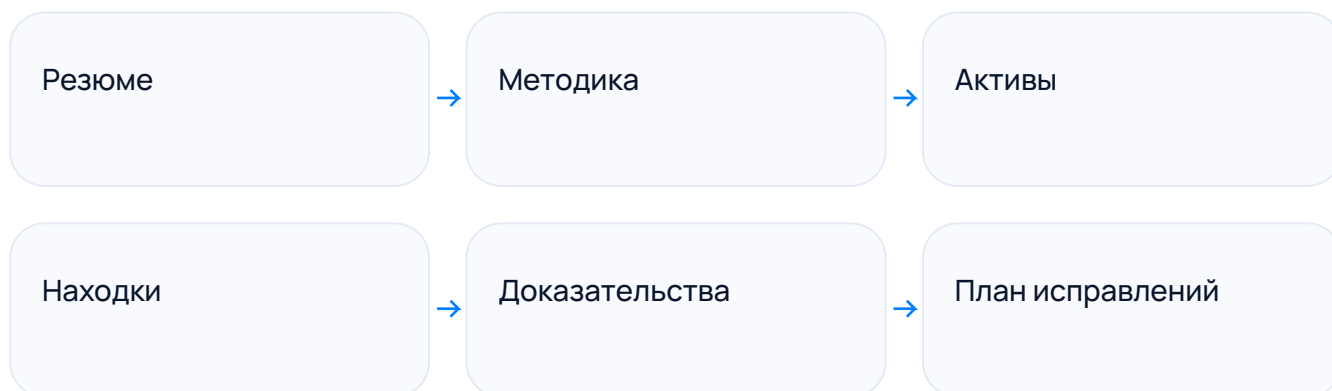
- Цель и согласованные границы.
- Ключевые выводы с основаниями.
- Рекомендуемые действия и дальнейшая проверка.

Структура технического отчёта

Отчёт позволяет проследить путь от объекта проверки до рекомендации.

Методика объясняет условия работы. Реестр активов описывает границы. Таблица находок показывает проблему, статус, доказательства и рекомендацию.

Материалы отделяют наблюдение от вывода. План исправлений связывает рекомендацию с ответственным действием и условиями повторной проверки.



Доказательства и рекомендации

Каждый вывод должен иметь понятное основание.

В карточке находки фиксируют источник, условия проверки и материалы. Описание должно позволять специалисту понять, почему сделан вывод, без раскрытия избыточных сведений.

Рекомендация описывает требуемое изменение и критерий контроля. Подробности действий и допустимость передачи артефактов согласуют с организацией.

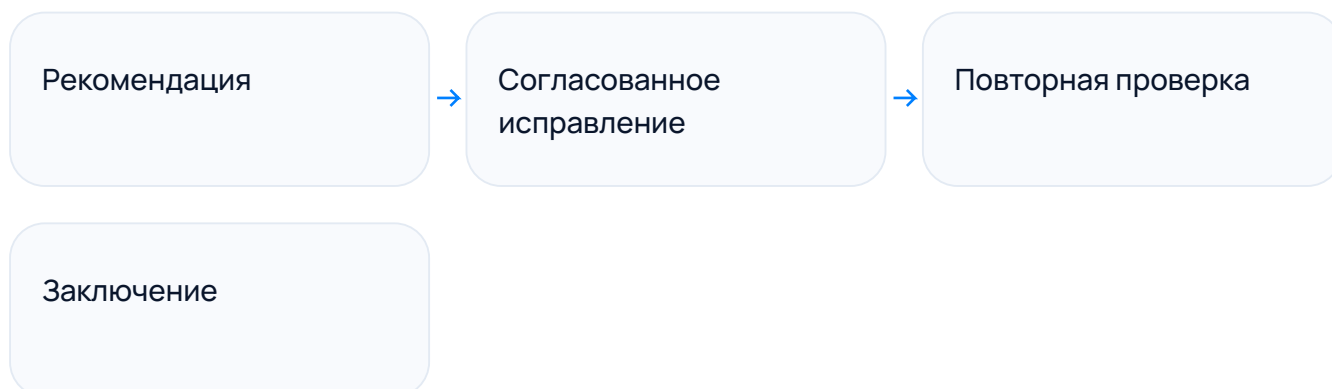
- Связь материала с активом и результатом.
- Разделение факта, интерпретации и рекомендации.
- Контроль доступа к артефактам и вложениям.

Исправления и повторная проверка

Заккрытие задачи и подтверждение устранения рассматриваются как разные действия.

Команда сообщает о выполненном изменении и его границах. Специалист возвращается к исходной находке, проверяет согласованные условия и фиксирует результат.

Если риск сохраняется, основание нового решения включают в историю. Если условия изменились, вывод сопровождают объяснением нового контекста.



Данные и регламенты безопасности

Журналирование, разграничение доступа и размещение данных учитывают при согласовании организационных требований.

Для организаций, работающих с персональными данными или отдельными защищаемыми контурами, важно заранее определить состав материалов, доступ и место хранения.

В обсуждение требований, связанных с 152-ФЗ и 187-ФЗ, включают правила хранения, обновления и передачи сведений. Конкретные меры определяются выбранной конфигурацией и документами организации.

- Категории сохраняемых сведений.
- Место хранения и границы передачи.
- Роли, история действий и порядок обновления.

Подготовка к подключению

Подготовленные сведения позволяют предметно обсудить конфигурацию платформы и результат работ.

Перед консультацией соберите перечень категорий активов, ответственных, действующие источники сведений и требования к размещению. Отдельно укажите ограничения и исключения.

Ожидаемый результат описывайте через решение: какой реестр нужен, кто рассматривает находки и каким способом подтверждается устранение.

- Категории активов и границы.
- Источники данных и действующие процессы.
- Ответственные и матрица доступа.
- Требования к хранению и ограничения.
- Ожидаемая структура отчёта.
- Порядок повторной проверки.

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