

АЕГИС DLP

Описание модуля

Защищаемые данные, каналы контроля, политики и работа с инцидентами.

ПОНЯТЬ УСТРОЙСТВО. ОБСУДИТЬ ПОДКЛЮЧЕНИЕ.

От задачи организации — к рабочему составу продукта.

Содержание

Описание модуля

01	Контроль движения данных	3
02	Каналы контроля	4
03	Политики, классификация и карантин	5
04	Работа команды и ожидаемый результат	6
	Контакты и консультация	7

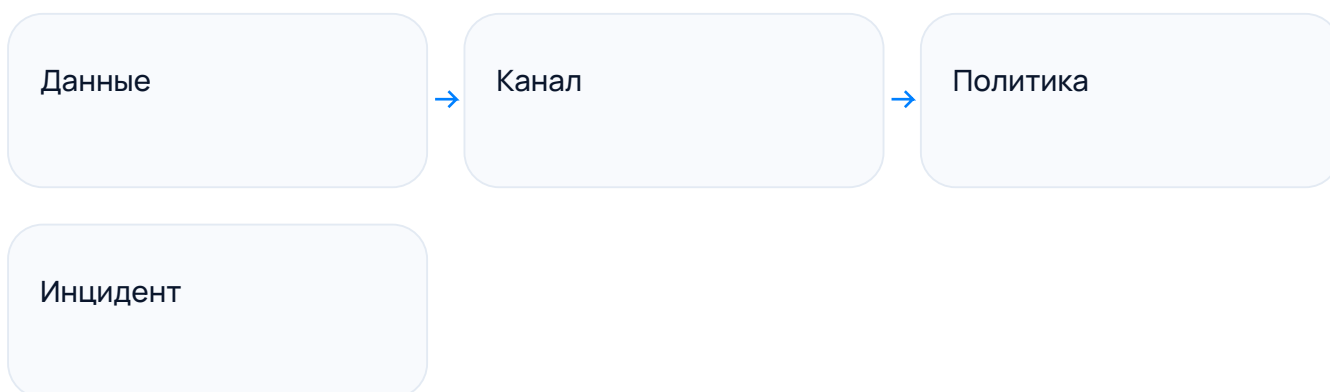
Контроль движения данных

АЕГИС DLP связывает действия с данными, правила контроля и материалы для разбора.

Файл может покинуть рабочий контекст через разные каналы. Чтобы понять происходящее, нужны сведения об объекте, действии и применённой политике.

Модуль использует агентов, события и классификацию для формирования связанного контекста. Подозрительные письма и файлы рассматриваются в отдельном порядке.

Модуль находится в бета-стадии и подключается к подписке АЕГИС. Отдельно не продаётся.



- Контроль действий на рабочих станциях.
- Политики по категориям данных и каналам.
- Материалы для расследования и карантин.

Каналы контроля

Правила рассматривают по каналам, через которые информация создаётся, используется и передаётся.

В описании модуля предусмотрены файлы, сеть, USB, буфер обмена, снимки экрана, почта, облака и процессы. Для каждого канала согласуют категории данных и допустимые действия.

Контекст события позволяет связать передачу с рабочей станцией и применённым правилом. Набор правил не должен подменять согласованный порядок обращения с информацией.

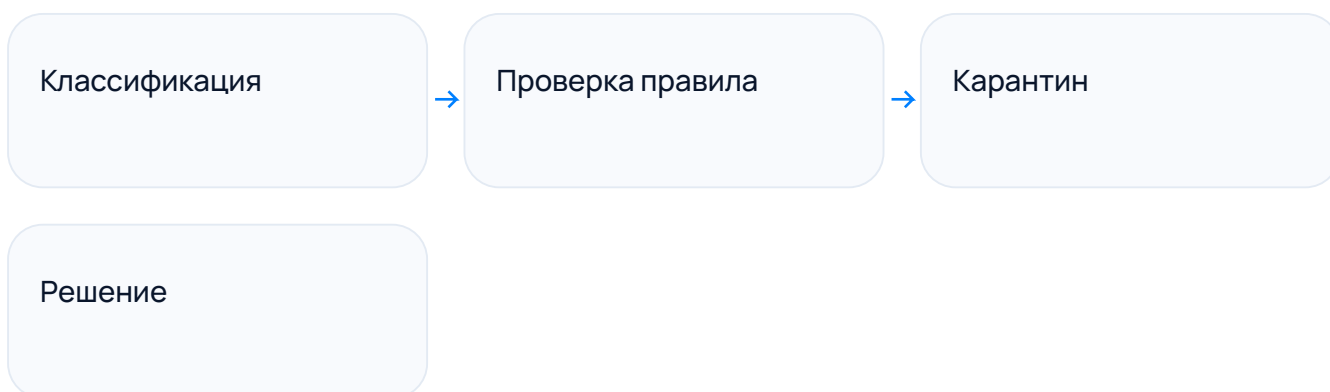
Группа	Каналы
Работа с объектами	Файлы и процессы
Передача	Сеть, USB и облака
Действия пользователя	Буфер обмена и снимки экрана
Сообщения	Почта и вложения

Политики, классификация и карантин

Классификация задаёт контекст, а политика описывает допустимое обращение с данными.

Правила учитывают содержимое и канал. Результат проверки связывается с событием и материалами инцидента.

Карантин выделяет подозрительные объекты для дальнейшего разбора. Порядок принятия решения, доступа и возвращения объекта в рабочий процесс согласуют с организацией.



- Категории информации и каналы.
- Основания срабатывания правила.
- Разбор инцидента с материалами.

Работа команды и ожидаемый результат

Модуль помогает организовать разбор действий с данными в общем контексте.

Специалист видит событие, связанное правило и артефакты. Хронология помогает сопоставить действия и определить необходимые меры.

Перед подключением определяют категории защищаемой информации, рабочие станции, ответственных и права доступа. Итогом согласования становится понятный состав контроля и порядок разбора инцидентов.

- Перечень данных и рабочих станций.
- Согласованные правила и исключения.
- Порядок расследования и ответственные.

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-dlp

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