Функциональные возможности
системы RS-Discovery (R-Sight)

RS TEAM

rs.team

СОДЕРЖАНИЕ

1 МОДУЛЬ УПРАВЛЕНИЯ АКТИВАМИ

Модуль управления активами предоставляет комплексные инструменты для управления жизненным циклом ваших ИТ-активов: от закупки и хранения до развертывания, обслуживания и последующего вывода из эксплуатации.

Обзор

Управление активами в R-Sight выходит за рамки возможностей традиционной CMDB, предоставляя следующие функции:

- **Управление компаниями:** Отслеживание того, какому юридическому лицу принадлежит каждый актив.
- **Распределение по центрам затрат:** Привязка активов к финансовым единицам для отслеживания бюджета.
- **Управление филиалами (Sites):** Отслеживание физических локаций, где развернуты активы.
- **Управление складами (Stockrooms):** Управление запасными частями, инвентарем и местами хранения.
- **Отслеживание жизненного цикла:** Мониторинг активов через 14 статусов жизненного цикла.
- **История назначений:** Автоматическая фиксация дат первого и последнего назначения актива.
- **Старение устройств:** Мониторинг возраста парка оборудования и планирование его обновления (refresh).
- **Управление гарантией:** Автоматический поиск информации о гарантии.

Раздел «Актив» (Asset)

При редактировании конфигурационной единицы (КЕ) раздел «Актив» объединяет все поля владения и жизненного цикла в одном месте:

Поле	Описание
Статус (Status)	Текущий статус жизненного цикла (Активен, На складе, Списан и т. д.).
Назначен (Assigned To)	Лицо, которое использует актив в данный момент.
Компания (Company)	Юридическое лицо, которому принадлежит данный актив.
Филиал (Site)	Физическое местоположение, где развернут актив.
Центр затрат (Cost Center)	Финансовое подразделение, ответственное за расходы по данному активу.
Склад (Stockroom)	Место хранения (для активов со статусом «На складе»).
Дата окончания гарантии	Дата завершения гарантийного обслуживания.
Дата первого назначения	Дата, когда актив был назначен впервые (заполняется автоматически, только для чтения).
Дата последнего назначения	Дата самого последнего назначения актива (заполняется автоматически, только для чтения).

Цепочка владения активами

R-Sight предоставляет структурированную иерархию для отслеживания принадлежности и местоположения активов:

Компания (Company) — *Кто владеет?*
└──── **Центр затрат (Cost Center)** — *Кто платит?*
└──── **Филиал (Site)** — *Где находится?*
└──── **Склад (Stockroom)** — *Где хранится?*

Эта иерархия позволяет осуществлять:

- **Финансовую отчетность** в разрезе компаний и центров затрат.
- **Физические аудиты** по конкретным площадкам и складам.
- **Контроль compliance** путем привязки активов к ответственным юридическим лицам.

- **Управление парком устройств** (Fleet management) сразу в нескольких бизнес-структурах.

Ключевые функции

Управление компаниями

Определите организационные единицы, владеющие вашими ИТ-активами:

- **Типы компаний:** Холдинг, дочернее предприятие, филиал, подразделение, партнер.
- **Контактная информация:** Адреса и реквизиты для каждой сущности.
- **Уникальные коды:** Кодификация компаний для быстрой идентификации.

Центры затрат и склады

Отслеживайте финансовые и физические параметры активов:

- **Центры затрат:** Иерархические финансовые единицы с возможностью отслеживания бюджета.
- **Склады (Stockrooms):** Физические места хранения с контролем вместимости и детальными полями адресации.

Управление филиалами (Sites)

Отслеживайте физические локации и привязывайте к ним активы:

- **Типы филиалов:** Офис, дата-центр, склад, удаленная точка.
- **Координаты и часовые пояса:** Полные адресные данные и гео-координаты.
- **Связь с IP-диапазонами:** Автоматическая привязка обнаруженных активов к филиалу на основе их IP.

Управление жизненным циклом

Отслеживайте активы через 14 статусов, охватывающих все фазы:

- **Фаза развертывания:** Ожидается (Pending), На складе (In Stock), Зарезервировано (Reserved), В пути (In Transit).
- **Операционная фаза:** Активен (Active), Развернут (Deployed), В лизинге (Leased).
- **Фаза обслуживания:** Неактивен (Inactive), Обслуживание (Maintenance), Карантин (Quarantine).
- **Завершение эксплуатации:** Списан (Retired), Утилизирован (Disposed), Утерян (Lost), Украден (Stolen).

Старение устройств (Aging)

Контролируйте возраст парка и планируйте замену оборудования:

- **Автоматический расчет возраста** на основе даты покупки, первого назначения или даты создания записи.
- **Отчеты по возрастным категориям:** Распределение парка по пяти «корзинам» возраста.
- **Анализ старения на складах** для эффективного управления запасами.

Управление гарантией

Автоматическое отслеживание гарантии через API вендоров:

- **Ручной ввод** для любых других вендоров.
- **Уведомления** об истечении срока гарантии.

Отчеты по активам

R-Sight включает несколько встроенных отчетов:

- **Отчеты о возрасте устройств:** Распределение парка по категориям: 0–1, 1–2, 2–3, 3–5 и 5+ лет.
- **Отчеты по складам:**
  - Список устройств на складе.
  - Количество устройств по каждому складу (столбчатая диаграмма).
  - Типы КЕ по складам и распределение статусов.
  - Средний возраст устройств на конкретном складе.

Лучшие практики

1. **Начало работы:** Сначала создайте записи компаний и центров затрат, затем настройте филиалы и склады, и только после этого привязывайте КЕ.

2. **Оперативность:** Своевременно меняйте статус жизненного цикла при перемещении актива.
3. **Ежемесячный аудит:** Проверяйте отчеты о старении, чтобы вовремя заметить оборудование, требующее замены.
4. **Квартальная инвентаризация:** Сопоставляйте физическое наличие на складах с данными в системе.

Часто задаваемые вопросы (FAQ)

- **В: Как часто обновляется информация о гарантии?** О: Данные могут обновляться по запросу или автоматически по расписанию.
- **В: Что если у актива нет даты покупки?** О: Система использует дату первого назначения, а если нет и её — дату создания КЕ в базе.
- **В: Как работают даты первого/последнего назначения?** О: Они устанавливаются автоматически при изменении поля «Назначен» (Assigned To). Дата первого назначения фиксируется один раз и не перезаписывается.

2 УПРАВЛЕНИЕ ФИЛИАЛАМИ (SITE MANAGEMENT)

Управление филиалами позволяет определять и организовывать физические локации вашей организации. Это упрощает отслеживание мест размещения активов и поиск контактных лиц в каждом конкретном филиале.

Доступ к управлению филиалами

1. Перейдите в раздел **Настройки** (Settings) в главном меню.
2. Выберите пункт **Филиалы** (Sites) в параметрах настроек.
3. В представлении «Список филиалов» отобразятся все настроенные локации.

Создание нового филиала

Шаг 1: Откройте диалоговое окно добавления филиала

Нажмите кнопку **Добавить филиал** (Add Site) в правом верхнем углу списка филиалов.

Шаг 2: Введите базовую информацию

Поле	Обязательно	Описание
Название (Name)	Да	Полное название филиала (например, «Штаб-квартира в Москве»)
Код (Code)	Нет	Краткий идентификатор для быстрого поиска (например, «MOS-HQ»)
Описание (Description)	Нет	Дополнительные сведения о филиале
Тип (Type)	Да	Классификация филиала
Статус (Status)	Да	Текущий операционный статус

Шаг 3: Введите адресную информацию

Поле	Описание
Улица (Street)	Адрес (улица, дом)
Город (City)	Название города
Регион/Район (State/Province)	Регион или район
Почтовый индекс (Postal Code)	Почтовый индекс
Страна (Country)	Название страны

Шаг 4: Настройте детали местоположения

Поле	Описание
Широта (Latitude)	GPS-координата широты
Долгота (Longitude)	GPS-координата долготы
Часовой пояс (Timezone)	Местный часовой пояс

Шаг 5: Добавьте основное контактное лицо

Поле	Описание
Контактное имя (Contact Name)	Имя основного контактного лица
Контактный Email (Contact Email)	Адрес электронной почты для связи
Контактный телефон (Contact Phone)	Номер телефона для срочных вопросов

Шаг 6: Свяжите IP-диапазоны

Выберите одно или несколько расписаний Discovery для ассоциации с этим филиалом. Это связывает сетевые диапазоны с физическими локациями для автоматического сопоставления активов с филиалами.

Шаг 7: Сохраните

Нажмите «Создать филиал» (Create Site), чтобы сохранить новый филиал.

Типы филиалов (Site Types)

Выберите подходящий тип для каждого филиала:

Тип	Вариант использования
Офис (Office)	Стандартные офисные помещения с рабочими станциями пользователей
Дата-центр (Datacenter)	Основные вычислительные центры с серверами и инфраструктурой
Склад (Warehouse)	Складские помещения, могут содержать системы учета инвентаря
Филиал (Branch)	Небольшие офисы, обычно удаленные от штаб-квартиры
Удаленный офис (Remote)	Сателлитные локации или домашние офисы
Другое (Other)	Локации, не подходящие под другие категории

Статус филиала (Site Status)

Отслеживайте операционный статус каждого филиала:

Статус	Описание
Активен (Active)	Филиал полностью функционирует
Неактивен (Inactive)	Филиал в данный момент не используется
Обслуживание (Maintenance)	В филиале проводятся технические работы или ремонт

Связь с IP-диапазонами

Привязка расписаний Discovery (IP-диапазонов) к филиалам обеспечивает:

- **Автоматическое назначение местоположения:** Активы, обнаруженные в сетевом диапазоне, автоматически закрепляются за соответствующим филиалом.
- **Географическая отчетность:** Генерация отчетов на основе физического местоположения.
- **Маппинг сети на физическую инфраструктуру:** Понимание взаимосвязи между топологией сети и физической инфраструктурой.

Фильтрация и поиск филиалов

Список филиалов поддерживает:

- **Поиск:** Поиск филиалов по названию, коду или городу.
- **Фильтр по статусу:** Отображение только активных, неактивных филиалов или филиалов на обслуживании.
- **Фильтр по типу:** Отображение только определенных типов филиалов.

Лучшие практики

Соглашения об именовании

Используйте последовательные названия, включающие:

1. Идентификатор местоположения (город, регион).
2. Тип филиала.
3. Опциональный порядковый номер.

Примеры:

- MOS-DC-01 (Дата-центр 1 в Москве).
- SAR-OFFICE (Офис в Саранске).
- APAC-BRANCH-MONG (Филиал APAC в Монголии).

Контактная информация

- Всегда назначайте основное контактное лицо.
- Поддерживайте контактную информацию в актуальном состоянии.
- По возможности используйте электронные почтовые ящики ролей (например, datacenter-ops@company.com).

Картирование IP-диапазонов

- Привяжите все production сетевые диапазоны к филиалам.
- Проверяйте связи IP-диапазонов после изменений в сети.
- Используйте понятные названия для расписаний Discovery, чтобы упростить их привязку к филиалам.

Интеграция с CMDB

Филиалы интегрируются с CMDB несколькими способами:

- **Назначение КЕ:** КЕ могут быть закреплены за конкретным филиалом.
- **Интеграция с Discovery:** Обнаруженные активы автоматически привязываются к филиалам на основе IP-диапазонов.
- **Отчетность:** Генерация отчетов с фильтрацией по филиалам.
- **Анализ влияния:** Понимание масштаба инцидентов в разрезе филиалов.

3 УПРАВЛЕНИЕ ГАРАНТИЕЙ (WARRANTY MANAGEMENT)

Управление гарантией помогает отслеживать статус гарантийного обслуживания оборудования, планировать продления и избегать непредвиденных расходов на поддержку.

Обзор

R-Sight предоставляет комплексные возможности для отслеживания гарантий:

- **Автоматический поиск гарантии:** Интеграция с API для автоматического получения данных.
- **Отслеживание истечения срока:** Мониторинг дат окончания гарантии во всем вашем парке устройств.
- **Права на обслуживание (Entitlements):** Понимание того, какой уровень покрытия имеет каждый актив.
- **Ручной ввод:** Возможность добавления данных о гарантии для любого актива от любого вендора.

Просмотр информации о гарантии

Просмотр отдельного актива

1. Перейдите в раздел **CMDB > Конфигурационные единицы** (Configuration Items).
2. Выберите нужный актив.
3. Ознакомьтесь с разделом **«Информация о гарантии»** (Warranty Information) в деталях КЕ.

Панель гарантии отображает:

- Общий статус гарантии (индикатор «Активна»/«Истекла»).
- Ключевые даты (истечение, отгрузка, дата последней проверки).
- Информацию о продукте.
- Все права на обслуживание с периодами их действия.

Пакетный просмотр гарантий

Для контроля гарантий во всем парке устройств:

1. Перейдите в раздел **Отчеты (Reports) > Отчеты по активам (Asset Reports)**.
2. Выберите **Отчет о статусе гарантии (Warranty Status Report)**.
3. Используйте фильтры по:
   - Статусу гарантии (Активна/Истекла).
   - Диапазону дат истечения.
   - Филиалу или отделу.

Ручной ввод гарантии

Для активов от вендоров без поддержки API:

1. Откройте актив в CMDB.
2. Перейдите в раздел **Актив (Asset)**.
3. Введите **Дату окончания гарантии (Warranty Expiry Date)**.
4. Сохраните изменения.

Для детальной информации используйте кастомные поля КЕ, чтобы зафиксировать:

- Поставщика гарантии.
- Номер контракта.
- Тип покрытия.
- Контакты Service Desk.

Обновление гарантии (Warranty Refresh)

Обновление по запросу

Чтобы обновить данные для одного актива:

1. Откройте карточку актива.
2. Нажмите **Обновить гарантию (Refresh Warranty)**.
3. Дождитесь ответа API и проверьте обновленную информацию.

Обновление по расписанию

Настройте автоматическое обновление:

1. Перейдите в **Настройки (Settings) > Планировщик задач (Scheduled Tasks)**.
2. Найдите задачу **Warranty Refresh**.
3. Настройте расписание (рекомендуется: еженедельно).
4. Выберите область действия (все поддерживаемые активы или конкретные группы).

Лучшие практики

Проактивное управление

- **Предупреждение за 30 дней:** Настройте оповещения о гарантиях, истекающих через месяц.
- **Ежеквартальный аудит:** Раз в квартал проверяйте все истекающие гарантии.
- **Планирование продлений:** Используйте данные о гарантиях для формирования бюджета.

Качество данных

- **Регулярность:** Настройте еженедельное обновление данных.
- **Проверка номеров:** Убедитесь, что серийные номера и сервис-тэги введены без ошибок.

Оптимизация затрат

- **Анализ покрытия:** Изучите уровни прав на обслуживание перед продлением.
- **Групповые продления:** Ведите переговоры о скидках, объединяя продление гарантий в пакеты.

4 УПРАВЛЕНИЕ КОМПАНИЯМИ (COMPANY MANAGEMENT)

Управление компаниями позволяет определять организационные структуры, которые владеют вашими ИТ-активами и эксплуатируют их. Связывая конфигурационные единицы (КЕ) с компаниями, вы получаете четкое представление о том, какая бизнес-структура несет ответственность за каждый актив.

Обзор

Во многих организациях ИТ-активы распределены между несколькими компаниями, дочерними предприятиями, подразделениями или партнерскими организациями. Модуль управления компаниями в R-Sight предоставляет структурированный способ:

- **Отслеживания владения активами** в рамках нескольких юридических лиц.
- **Разделения активов по бизнес-единицам** для отчетности и compliance.
- **Управления многопрофильными средами**, такими как холдинги с дочерними компаниями.
- **Связки центров затрат и бюджетов** с соответствующими бизнес-субъектами.

Доступ к управлению компаниями

1. Перейдите в раздел **Настройки** (Settings) в основном меню навигации.
2. Выберите пункт **Компании** (Companies) в меню настроек.
3. В «Списке компаний» отобразятся все настроенные организации.

Создание компании

Шаг 1: Откройте диалоговое окно добавления компании

Нажмите кнопку **Добавить компанию** (Add Company) в правом верхнем углу списка компаний.

Шаг 2: Введите базовую информацию

Поле	Обязательно	Описание
Название (Name)	Да	Юридическое или операционное название компании.
Код (Code)	Нет	Краткий идентификатор (например, «ACME», «SUB-EU»). Автоматически переводится в верхний регистр.
Описание (Description)	Нет	Дополнительная информация о компании.

Шаг 3: Выберите тип компании

Выберите классификацию, которая лучше всего описывает сущность:

Тип	Вариант использования
Предприятие (Enterprise)	Основная родительская организация.
Дочерняя компания (Subsidiary)	Полностью или частично принадлежащая дочерняя структура.
Филиал (Branch)	Региональный филиал родительской организации.
Подразделение (Division)	Внутреннее бизнес-подразделение или департамент.
Партнер (Partner)	Внешний партнер или клиент на управляемом обслуживании.
Другое (Other)	Сущности, не подходящие под другие категории.

Шаг 4: Введите адресную информацию

Поле	Описание
Улица (Street)	Физический адрес компании.
Город (City)	Город.
Штат/Провинция	Регион, район, штат, провинция
Почтовый индекс	Почтовый индекс.
Страна (Country)	Страна.

Шаг 5: Добавьте контактную информацию

Поле	Описание
Имя основного контакта	Имя основного контактного лица по вопросам ИТ.
Email основного контакта	Электронная почта для связи.
Телефон основного контакта	Номер телефона для срочных вопросов.
Сайт компании	URL-адрес веб-сайта компании.
Телефон компании	Общий номер телефона компании.
Email компании	Общий адрес электронной почты компании.

Шаг 6: Сохраните

Нажмите **Создать** (Create), чтобы сохранить новую компанию.

Назначение активов компаниям

После определения компаний вы можете связать любую конфигурационную единицу (КЕ) с организацией:

1. Откройте КЕ в CMDB.
2. В разделе **Актив (Asset)** найдите выпадающий список **Компания (Company)**.
3. Выберите подходящую компанию.
4. Сохраните изменения.

Иерархия компаний

Компании работают совместно с другими организационными единицами для создания полной структуры владения активами:

Компания (*кто владеет*)
└── **Центр затрат** (*кто платит*)
└── **Филиал** (*где находится физически*)
└── **Склад** (*где хранится*)

Эта иерархия обеспечивает широкие возможности фильтрации и отчетности:

- Просмотр всех активов, принадлежащих конкретной дочерней компании.
- Отслеживание ИТ-расходов по компаниям и центрам затрат.
- Формирование отчетов о compliance для каждого юридического лица.

Отчетность по компаниям

Благодаря назначению компаний вы можете:

- Фильтровать списки КЕ по компаниям, чтобы видеть только релевантные активы.
- Запускать отчеты в рамках конкретной организации.
- Отслеживать количество устройств на компанию для распределения лицензий.
- Мониторить статус гарантии в различных бизнес-структурах.

Лучшие практики

Соглашения об именовании

- Используйте официальные юридические названия для отчетности о соответствии требованиям (compliance).
- Используйте краткие, узнаваемые коды (например, «ACME-BEL» для белорусского филиала).
- Для ясности указывайте тип организации в описании.

Мультисервисные среды

- Определите головную компанию с типом **Предприятие (Enterprise)**.
- Создайте каждую дочернюю структуру с типом **Дочерняя компания (Subsidiary)**.
- Связывайте центры затрат с соответствующими компаниями.
- Используйте коды компаний в тегах активов для быстрой идентификации.

Качество данных

- Поддерживайте контактную информацию в актуальном состоянии.

- Проверяйте принадлежность к компаниям во время проведения аудитов активов.
- Архивируйте неактивные компании вместо их удаления.

Центры затрат и Склады (Cost Centers & Stockrooms)

Центры затрат и Склады обеспечивают финансовое и физическое измерения управления активами. Центры затрат отслеживают, кто платит за активы, а Склады — где физически хранятся запасные и находящиеся в наличии активы.

Центры затрат (Cost Centers)

Что такое Центры затрат?

Центры затрат представляют собой финансовые подразделения вашей организации, ответственные за расходы на ИТ-активы. Они позволяют:

- Распределять ИТ-затраты на соответствующий отдел или проект.
- Сопоставлять бюджеты с фактическими расходами на активы.
- Формировать отчетность по расходам на ИТ в разрезе бизнес-единиц.
- Поддерживать модели внутреннего биллинга (chargeback) и отчетности (showback).

Доступ к управлению центрами затрат

1. Перейдите в раздел **Настройки (Settings)** в главном навигационном меню.
2. Выберите **Центры затрат (Cost Centers)** в меню настроек.
3. В представлении «Список центров затрат» отобразятся все настроенные центры затрат.

Создание центра затрат

Поле	Обязательно	Описание
Название (Name)	Да	Название центра затрат (например, «IT Operations», «Marketing»).
Код (Code)	Нет	Краткий идентификатор, автоматически переводится в верхний регистр (например, «IT-OPS»).
Описание (Description)	Нет	Дополнительный контекст о назначении центра затрат.
Компания (Company)	Нет	Компания, которой принадлежит этот центр затрат.
Родитель (Parent)	Нет	Родительский центр затрат для создания иерархических структур.
Менеджер (Manager)	Нет	Пользователь, ответственный за этот центр затрат.
Тип (Type)	Да	Классификация: Отдел, Проект, Подразделение, Команда или Другое.
Статус (Status)	Да	Текущий статус: Активен, Неактивен или Архимирован.

Отслеживание бюджета (Budget Tracking)

Каждый центр затрат может включать бюджетную информацию:

Поле	Описание
Годовой бюджет (Annual Budget)	Годовой объем ИТ-бюджета, выделенный этому центру затрат.
Валюта (Currency)	Код валюты (например, USD, EUR, GBP).

Иерархия центров затрат

Центры затрат поддерживают древовидную иерархическую структуру:

- **ИТ-дивизион (Уровень 0)**
  - ├── **ИТ-эксплуатация (Уровень 1)**
  - │ ├── Группа инфраструктуры (Уровень 2)
  - │ └── Группа Help Desk (Уровень 2)
  - ├── **ИТ-разработка (Уровень 1)**
  - │ ├── Группа Frontend (Уровень 2)
  - │ └── Группа Backend (Уровень 2)
  - └── **ИТ-безопасность (Уровень 1)**

Уровень иерархии рассчитывается автоматически при назначении родительского центра затрат.

Типы центров затрат

Тип	Вариант использования
Отдел (Department)	Стандартный организационный отдел
Проект (Project)	Временное распределение затрат на основе проекта
Дивизион (Division)	Крупное бизнес-подразделение
Команда (Team)	Отдельная команда внутри департамента
Другое (Other)	Пользовательская классификация

Склады (Stockrooms)

Что такое Склады?

Склады представляют собой физические места хранения, где ИТ-активы содержатся в то время, когда они не находятся в эксплуатации. Они необходимы для:

- **Управления инвентарем** запасного и резервного оборудования.
- **Отслеживания активов**, находящихся в наличии перед развертыванием.
- **Управления зонами подготовки** (staging areas) для обновления парка оборудования.
- **Планирования вместимости** складских помещений.

Доступ к управлению складами

1. Перейдите в раздел **Настройки (Settings)** в главном меню.
2. Выберите **Склады (Stockrooms)** в меню настроек.
3. В «Списке складов» отобразятся все сконфигурированные складские помещения.

Создание склада

Поле	Обязательно	Описание
Название (Name)	Да	Имя склада (например, «Основной ИТ-склад», «Серверная Б»).
Код (Code)	Нет	Краткий идентификатор, автоматически переводится в верхний регистр (например, «WH-MAIN»).
Описание (Description)	Нет	Дополнительные сведения о складе.
Филиал (Site)	Нет	Физическая локация, где расположен этот склад.
Центр затрат	Нет	Центр затрат, ответственный за этот склад.
Родитель (Parent)	Нет	Родительский склад для создания вложенных зон хранения.
Ответственный	Нет	Пользователь, управляющий этим складом.
Тип (Type)	Да	Классификация зоны хранения.
Статус (Status)	Да	Текущий операционный статус.

Типы складов (Stockroom Types)

Тип	Вариант использования
Склад (Warehouse)	Крупный объект для хранения оптовых партий инвентаря.
Кладовая (Storage Room)	Склад общего назначения внутри здания.
Серверная (Server Room)	Место для хранения серверов и сетевого оборудования.
Хоз. шкаф (Supply Closet)	Небольшое место хранения периферии и аксессуаров.
Защищенное хранилище	Склад с ограниченным доступом или под замком.
Другое (Other)	Пользовательская классификация хранилища.

Статус склада (Stockroom Status)

Статус	Описание
Активен (Active)	Открыт и принимает оборудование.
Неактивен (Inactive)	Временно не используется.
Обслуживание	Проводится реорганизация или ремонт.
Заполнен (Full)	Достигнута максимальная вместимость, новые предметы не принимаются.

Детали физического местоположения

Для максимально точного поиска актива внутри склада вы можете указать следующие данные:

Поле	Описание
Здание (Building)	Название или номер здания
Этаж (Floor)	Номер этажа
Комната (Room)	Номер или название комнаты
Ряд (Aisle)	Обозначение прохода или ряда
Стеллаж (Rack)	Идентификатор стойки или полки

Отслеживание вместимости (Capacity Tracking)

Позволяет контролировать степень заполненности каждого склада:

Поле	Описание
Макс. предметов	Максимальное количество предметов, которое может вместить склад
Текущее кол-во	Текущее количество хранящихся предметов
Единица измерения	Единица учета (штуки, юниты в стойке и т. д.)

Назначение активов центрам затрат и складам

При редактировании конфигурационной единицы (КЕ) в разделе «Актив» (Asset) доступны выпадающие списки для обоих параметров:

1. Откройте КЕ в CMDB.
2. В разделе **Актив (Asset)**:
   - Выберите **Центр затрат (Cost Center)** для распределения бюджета.
   - Выберите **Склад (Stockroom)**, если актив находится на хранении.
3. Сохраните изменения.

Использование складов со статусами КЕ

Склады органично интегрированы с жизненным циклом КЕ:

Статус КЕ	Использование склада
На складе (In Stock)	Актив физически находится на складе в ожидании развертывания.
Зарезервировано (Reserved)	Актив находится на складе, но закреплен под конкретную цель.
Активен/Развернут	Актив эксплуатируется — поле склада должно быть очищено.
В пути (In Transit)	Актив перемещается между складами или к месту установки.

Отчеты по складам

R-Sight включает несколько встроенных отчетов для управления складами:

- **Устройства в наличии (Devices In Stock):** Таблица всех КЕ, назначенных на склад (имя, тип, статус).
- **Устройства по складам:** Гистограмма, показывающая количество устройств на каждом складе.

- **Типы КЕ по складам:** Подробная таблица с разбивкой типов КЕ (серверы, рабочие станции и т. д.).
- **Статус устройств по складам:** Стековая диаграмма распределения статусов внутри каждого склада.
- **Возраст устройств на складе:** Таблица среднего возраста устройств, помогающая выявить оборудование для списания или обновления.

Чтобы найти эти отчеты, перейдите в раздел **Отчеты (Reports)** и выберите категорию **Склад (Stockroom)**.

Цепочка владения активом

Вместе Компании, Центры затрат, Филиалы и Склады формируют полную цепочку ответственности и местоположения:

Сущность	Вопрос	Пример
Компания	Кто владеет?	Компания ГРУПП
Центр затрат	Кто платит?	ИТ-эксплуатация
Филиал	Где это находится?	Штаб-квартира (MSK)
Склад	Где это хранится?	ИТ-склад — Стеллаж А3

Лучшие практики

Управление центрами затрат

- **Отражайте оргструктуру:** Совмещайте центры затрат с реальной иерархией вашей компании.
- **Используйте понятные коды:** Например, IT-OPS или FIN-ACC для быстрой идентификации.
- **Назначайте менеджеров:** У каждого центра затрат должно быть ответственное лицо.

Управление складами

- **Именуйте по локации:** Включайте здание и номер комнаты в название склада.
- **Отслеживайте вместимость:** Установите лимиты, чтобы получать уведомления до переполнения склада.
- **Регулярный аудит:** Периодически сверяйте физическое наличие оборудования с записями в системе.

5 УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ (LIFECYCLE MANAGEMENT)

Управление жизненным циклом позволяет отслеживать каждую конфигурационную единицу (КЕ) на протяжении всего её пути: от первоначальной закупки и развертывания до окончательного вывода из эксплуатации и утилизации. Понимание того, на каком этапе находится каждый актив, критически важно для планирования, бюджетирования и соблюдения нормативных требований (compliance).

Обзор

Каждый ИТ-актив проходит через предсказуемый жизненный цикл. R-Sight предоставляет исчерпывающий набор статусов для отслеживания каждой фазы.

Последовательное управление статусами жизненного цикла позволяет:

- **Планировать обновление оборудования** до того, как активы станут ненадежными.
- **Отслеживать готовность к развертыванию** нового оборудования.
- **Контролировать окна обслуживания** для критически важных активов.
- **Обеспечивать надлежащую утилизацию** и гарантированное уничтожение данных.
- **Соблюдать нормативные требования (compliance)**, обязывающие вести учет активов.

Статусы жизненного цикла КЕ

R-Sight поддерживает 14 статусов жизненного цикла, охватывающих все этапы владения активом:

Фаза развертывания (Deployment Phase)

Статус	Описание	Типичное использование
Ожидание (Pending)	Ожидает развертывания или настройки	Новые активы в процессе конфигурирования
На складе (In Stock)	Находится на складе, доступен для выдачи	Запасной инвентарь
Зарезервировано (Reserved)	Зарезервирован под конкретную цель/проект	Предварительно распределенное оборудование
В пути (In Transit)	Пересылается или перемещается между локациями	Перемещения и новые поставки

Операционная фаза (Operational Phase)

Статус	Описание	Типичное использование
Активен (Active)	КЕ функционирует и используется	Статус по умолчанию для обнаруженных активов
Развернут (Deployed)	Активно эксплуатируется в среде	Промышленные серверы и рабочие станции
В лизинге (Leased)	Оборудование взято в аренду/лизинг	Активы по лизинговым соглашениям

Фаза обслуживания (Maintenance Phase)

Статус	Описание	Типичное использование
Неактивен (Inactive)	Не используется (выключен, хранится)	Временно неиспользуемые активы
Обслуживание (Maintenance)	Проходит техобслуживание или ремонт	Активы в сервисном центре
Карантин (Quarantine)	Изолирован по соображениям безопасности	Скомпрометированные или подозрительные устройства

Фаза завершения эксплуатации (End of Life Phase)

Статус	Описание	Типичное использование
Списан (Retired)	Срок службы окончен, больше не используется	Выведенные из эксплуатации активы

Утилизирован (Disposed)	Физически утилизирован или переработан	Активы, удаленные из инвентаря
Утерян (Lost)	Местоположение невозможно определить	Пропавшие активы
Украден (Stolen)	Заявлен как украденный	Активы, переданные в службу безопасности

Установка статуса актива

При создании КЕ

При ручном создании новой КЕ установите начальный статус в разделе **Актив (Asset)**:

1. Перейдите в **CMDB > Добавить конфигурационную единицу**.
2. В разделе **Актив** выберите подходящий **Статус**.

- **Типичные начальные статусы:** На складе (находится на хранении), Ожидание (в процессе настройки) или Активен (уже развернут).

При автоматическом обнаружении (Discovery)

Активам, обнаруженным в ходе сканирования сети, автоматически присваивается статус **Активен**, так как они были найдены работающими в сети.

Обновление статуса

1. Откройте КЕ в CMDB.
2. В разделе **Актив** измените значение в выпадающем списке **Статус**.
3. Сохраните изменения.

- Изменение статуса фиксируется в журнале аудита КЕ для отслеживания соответствия (compliance).

Отслеживание назначений

R-Sight автоматически отслеживает, когда активы закрепляются за пользователями:

Поле «Кем используется» (Assigned To)

Это поле фиксирует текущего пользователя актива. При изменении этого поля система автоматически записывает:

Поле	Описание
Дата первого назначения	Дата, когда актив был впервые назначен любому пользователю. После установки эта дата больше не меняется.
Дата последнего назначения	Дата самого последнего закрепления. Обновляется каждый раз при смене ответственного лица.

Эти даты отслеживаются автоматически и отображаются как поля «только для чтения» в разделе «Актив». Они помогают ответить на такие вопросы, как:

- «Как долго этот актив находится в эксплуатации?» (время с даты первого назначения).
- «Когда этот актив переназначался в последний раз?» (дата последнего назначения).
- «Развертывался ли этот актив когда-либо вообще?» (наличие или отсутствие даты первого назначения).

Отчетность по жизненному циклу

Используйте встроенные отчеты для мониторинга состояния вашего парка активов:

- **Распределение устройств по возрасту (Device Age Distribution):** Наглядная сегментация парка по возрастным группам (например, 0–2 года, 3–5 лет, 5+ лет).
- **Устройства на складе (Devices In Stock):** Оперативный список всех активов, находящихся в местах хранения.
- **Статус устройств по складам (Device Status by Stockroom):** Анализ стадий жизненного цикла активов, находящихся на хранении (например, сколько из них зарезервировано, а сколько доступно).

Чтобы получить доступ к этим данным, перейдите в раздел **Отчеты (Reports)**.

Лучшие практики

Дисциплина статусов

- **Своевременное обновление:** Изменяйте статус немедленно при смене состояния актива.
- **Точность выбора:** Выбирайте наиболее специфичный статус из доступных.

- **Последовательность:** Не пропускайте этапы (например, перевод из «В пути» сразу в «Списан» без фазы эксплуатации).
- **Регулярный аудит:** Проверяйте активы, которые «зависли» в переходных статусах (*Pending*, *In Transit*).

Отслеживание назначений

- **Обязательное закрепление:** У каждого развернутого актива должен быть указан ответственный (*Assignee*).
- **Очистка при возврате:** Удаляйте пользователя из поля «Assigned To», когда оборудование возвращается на склад.
- **Анализ использования:** Используйте даты первого и последнего назначения для оценки интенсивности эксплуатации.

Соответствие требованиям (Compliance)

- **Сквозной трекинг:** Убедитесь, что утилизированные активы имеют полную историю перемещений.
- **Документирование причин:** Используйте описание или заметки к КЕ для пояснения причин смены статуса (например, основание для списания).
- **Протокол карантина:** Немедленно переводите в статус *Quarantine* любые активы, замешанные в инцидентах безопасности.

6 ВОЗРАСТ УСТРОЙСТВ И ОТЧЕТЫ (DEVICE AGING & REPORTS)

Инструменты анализа возраста устройств помогают понять, насколько устарел ваш ИТ-парк, своевременно планировать замену оборудования и выявлять устаревший инвентарь, который может представлять риски для надежности или безопасности.

Обзор

По мере старения оборудование становится более склонным к сбоям, может лишиться поддержки вендора и стать уязвимым местом в системе безопасности. R-Sight отслеживает возраст устройств, используя несколько источников данных:

- **Дата покупки (Purchase Date)** — наиболее точный показатель.
- **Дата первого назначения (First Assigned Date)** — когда актив начал эксплуатироваться пользователем.
- **Дата создания KE (Creation Date)** — резервный вариант (когда запись была создана в системе).

Система использует наиболее приоритетную из доступных дат для расчета возраста.

Как рассчитывается возраст устройства

Возраст определяется в соответствии со следующим приоритетом:

Приоритет	Поле даты	Источник
1	Дата покупки	Вводится вручную или подтягивается из данных гарантии.
2	Дата первого назначения	Устанавливается автоматически при первой выдаче актива.
3	Дата создания KE	Генерируется системой при создании записи о KE.

Для получения наиболее точных данных:

- Указывайте **Дату покупки** при создании или редактировании KE.
- Всегда заполняйте поле **Кем используется (Assigned To)** при развертывании (это заполнит **Дату первого назначения**).
- Используйте **интеграцию с гарантиями**, которая автоматически импортирует даты отгрузки.

Отчет: Распределение устройств по возрасту

Этот отчет представляет собой гистограмму, отображающую профиль вашего парка в пяти временных интервалах:

Интервал	Описание	Рекомендация к действию
0–1 год	Новые активы, недавно развернуты.	Действия не требуются.
1–2 года	Активы в рамках стандартного цикла.	Мониторинг производительности.
2–3 года	Приближение к порогу типичного обновления.	Планирование замены.
3–5 лет	Устаревающие активы.	Приоритетная замена.
5+ лет	Активы в конце срока службы (EOL).	Рекомендуется немедленная замена.

Доступ к отчету

1. Перейдите в раздел **Отчеты** (Reports).
2. Найдите отчет **Распределение устройств по возрасту** (Device Age Distribution) в категории «Активы» (Asset).
3. Гистограмма отобразит количество активных серверов и рабочих станций в каждой возрастной группе.

Что включает в себя отчет

- Только серверы и рабочие станции (исключает ПО, мониторы, периферийные устройства).
- Только активные активы (исключает неактивные, списанные и утилизированные).

- Возраст, рассчитанный на основе наиболее точной доступной даты.

Отчеты о возрасте оборудования на складах

Возраст устройств по складам (Device Age by Stockroom) Этот отчет показывает средний возраст устройств, хранящихся на каждом складе, помогая определить:

- Устаревающий инвентарь, который необходимо развернуть или утилизировать.
- Новый запас, доступный для немедленного развертывания.
- Склады со старым оборудованием, требующим внимания.

Доступ к отчетам по складам

1. Перейдите в раздел **Отчеты** (Reports).
2. В категории **Склад** (Stockroom) найдите:
   - **Возраст устройств по складам** — средний возраст на каждый склад.
   - **Устройства в наличии** — полный список складских запасов.
   - **Устройства по складам** — распределение по количеству.
   - **Типы КЕ по складам** — разбивка по типам на каждом складе.
   - **Статус устройств по складам** — распределение по статусам на каждом складе.

Планирование обновления оборудования

Используйте данные о возрасте для управления процессом планирования обновлений:

Шаг 1: Анализ возрастного распределения

Откройте отчет «Распределение устройств по возрасту», чтобы понять текущий возрастной профиль вашего парка.

Шаг 2: Выявление активов в зоне риска

Сосредоточьтесь на группах «3–5 лет» и «5+ лет»:

- Что это за активы?
- Распространяется ли на них гарантия?
- Какова их критичность?

Шаг 3: Сопоставление с данными о гарантии

Активы из возрастных групп с истекшей гарантией имеют наивысший приоритет для замены. Используйте отчеты по гарантиям, чтобы выявить активы, которые одновременно являются старыми и не имеют покрытия.

Шаг 4: Планирование закупок

- Рассчитайте количество замен на основе возрастных групп.
- Учитывайте сроки поставки и развертывания.
- Спланируйте бюджет, используя распределение по центрам затрат.

Шаг 5: Выполнение обновления

- Закажите новое оборудование (новые активы: «На складе» или «В пути»).
- Настройте новые активы (статус: «Ожидание»).
- Разверните и закрепите за пользователями (статус: «Активен»).
- Спишите старые активы (статус: «Списан», затем «Утилизирован»).

Повышение качества данных о возрасте

Вводите даты покупки

Наиболее эффективное улучшение — обеспечение записи дат покупки:

1. Отредактируйте КЕ в CMDB.
2. В разделе **Оборудование** (Hardware) введите **Дату покупки** (Purchase Date).
3. Сохраните изменения.

Назначайте активы своевременно

При развертывании новых активов немедленно заполняйте поле **Кем используется** (Assigned To). Это автоматически запишет **Дату первого назначения**, обеспечив точную временную метку начала эксплуатации.

Лучшие практики

Тип актива	Рекомендуемое обновление	Обоснование
Рабочие станции	3–4 года	Снижение производительности, истечение срока гарантии

Серверы	4–5 лет	Вопросы надежности, энергоэффективность
Сетевые устройства	5–7 лет	Жизненный цикл поддержки встроенного ПО
Мониторы	5–7 лет	Более длительный срок службы, низкая вероятность отказов

Гигиена данных

- Фиксируйте даты покупки в момент закупки.
- Своевременно обновляйте статус при смене фазы жизненного цикла актива.
- Ежемесячно просматривайте отчеты о возрасте устройств для проактивного планирования.
- Очищайте склады от залежалого инвентаря, который хранится слишком долго.

Финансовое планирование

- Используйте распределение по возрасту для прогнозирования ежегодных бюджетов на замену.
- Отслеживайте затраты на каждую возрастную группу для обоснования сроков обновления.
- Сравнивайте стоимость расширенной гарантии и полной замены оборудования.
- Предоставляйте отчеты о возрасте руководству для утверждения бюджета.

7 УПРАВЛЕНИЕ СОГЛАШЕНИЯМИ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ (SLA)

Фреймворк управления SLA в RS-Discovery (R-Sight) помогает организациям поддерживать стабильное качество услуг с помощью автоматизированного отслеживания, интеллектуальной эскалации и детальной отчетности. Обеспечьте соответствие ИТ-услуг ожиданиям бизнеса с помощью проактивного мониторинга.

Обзор фреймворка SLA

Платформа предоставляет полную видимость производительности услуг по отношению к согласованным целям:

- **Управление временем ответа:** Отслеживание времени первой реакции с учетом приоритетов и рабочих часов.
- **Контроль времени решения:** Сквозной мониторинг от создания до закрытия инцидента с проактивными предупреждениями о риске нарушения.
- **Мониторинг доступности:** Расчет аптайма (uptime) в реальном времени с исключением периодов планового обслуживания.

Уровни обслуживания и целевые показатели

Типовые уровни (Tiers)

Уровень	Доступность	Отклик	Решение (Crit)	Режим работы
Platinum	99.99%	15 мин	2 часа	24x7
Gold	99.9%	30 мин	4 часа	Бизнес-часы
Silver	99.5%	1 час	8 часов	Бизнес-часы

Цели на основе приоритетов

- **Критический:** Отклик — 15 мин, Решение — 2 часа.
- **Высокий:** Отклик — 30 мин, Решение — 4 часа.
- **Средний:** Отклик — 2 часа, Решение — 8 часов.

Операционные соглашения (OLA)

RS-Discovery (R-Sight) поддерживает внутренние обязательства команд (**OLAs**), чтобы гарантировать выполнение общего SLA:

- **Базы данных:** 30 минут на отклик.
- **Сети:** 15 минут на отклик.
- **Безопасность:** Немедленная реакция на взломы.

Проактивная эскалация и предотвращение нарушений

Система использует интеллектуальные триггеры для предотвращения просрочек:

- **Уровень 1 (80% времени):** Уведомление исполнителя и менеджера команды, визуальное выделение на панели мониторинга.
- **Уровень 2 (90% времени):** Эскалация на уровень менеджмента, мобилизация дополнительных ресурсов.
- **Уровень 3 (95% времени):** Запуск протоколов «War Room», уведомление руководства и подготовка коммуникаций с клиентом.

Аналитика и отчетность по SLA

Ключевые показатели (KPI)

- **Общее соответствие (Compliance):** Цель >95%.
- **First Call Resolution (FCR):** Доля инцидентов, решенных при первом контакте (цель >70%).
- **Анализ причин нарушений:** Нехватка ресурсов (35%), пробелы в процессах (25%), сложность задачи (20%).

Прогнозная аналитика

ИИ RS-Discovery (R-Sight) анализирует текущую нагрузку и сложность запроса, чтобы предсказать вероятность нарушения SLA еще на этапе создания инцидента.

Бизнес-ценность и ROI

Преимущество	Метрика	Типовое улучшение

Снижение нарушений SLA	Количество просрочек	-25–40%
Время ответа	Среднее время отклика	-35–50%
Удовлетворенность (CSAT)	Оценка пользователей	+20–30%
Продуктивность	Запросов на инженера	+20–35%

8 МАППИНГ УСЛУГ (SERVICE MAPPING)

Обзор маппинга услуг (Service Mapping)

Маппинг услуг в RS-Discovery (R-Sight) автоматически обнаруживает и сопоставляет взаимосвязи между бизнес-услугами и лежащей в их основе ИТ-инфраструктурой. Используя обнаружение на базе ИИ и отслеживание зависимостей в реальном времени, модуль обеспечивает полную видимость архитектуры ваших услуг и их взаимодействий.

Что такое маппинг услуг?

Service Mapping создает комплексную живую карту ваших бизнес-услуг путем:

- **Обнаружения всех компонентов**, составляющих услугу (серверы, БД, балансировщики, микросервисы).
- **Маппинга зависимостей** между компонентами для понимания путей прохождения трафика.
- **Визуализации архитектуры** и потоков данных в удобном графическом интерфейсе.
- **Отслеживания состояния (Health)** и производительности каждого узла в контексте услуги.
- **Анализа влияния** изменений и сбоев на конечный бизнес-результат.

Уровни системы маппинга

Для создания точной картины ИТ-ландшафта RS-Discovery (R-Sight) использует многоуровневый подход к обработке данных:

1. Уровень обнаружения (Discovery Layer)

Автоматически сканирует среду для идентификации:

- **Сетевых соединений** и паттернов взаимодействия между узлами.
- **Компонентов приложений** и их специфических конфигураций.
- **Систем баз данных** и хранилищ данных.
- **API-эндпоинтов** и внешних интеграций.

2. Движок маппинга (Mapping Engine)

Анализирует собранные данные, чтобы:

- Выявить зависимости между отдельными компонентами.
- Понять логику трафика и потоков данных.
- Парсить конфигурационные файлы для поиска скрытых взаимосвязей.
- Использовать ИИ для распознавания стандартных архитектурных паттернов.

3. Сервисная модель (Service Model)

Организует информацию в иерархическую структуру:

- **Бизнес-услуги:** Функции, видимые конечному пользователю.
- **Технические услуги:** Поддерживающие ИТ-компоненты.
- **Инфраструктура:** Физические и виртуальные серверы, сети и хранилища.
- **Потоки данных:** Маршруты перемещения информации между уровнями.

4. Визуализация (Visualization)

Представляет данные через:

- **Интерактивные карты топологии** услуг.
- **Графы взаимосвязей** (Dependency Graphs).
- **Визуализацию анализа влияния** (Impact Analysis).
- **Панели мониторинга состояния** в реальном времени.

Ключевые концепции

Бизнес-услуги

Представляют собой критически важные для бизнеса возможности. **Пример: Услуга интернет-магазина (Online Shopping Service)**

- **Критичность:** Критическая (Critical).
- **Точки входа:** Веб-фронтенд, мобильное приложение, CDN.
- **Уровень приложений:** Корзина, каталог товаров, платежный шлюз, сервис заказов.
- **Middleware:** Очереди сообщений, кластер кэширования, API-шлюз.
- **Уровень данных:** Базы данных клиентов, товаров и заказов.
- **Инфраструктура:** Балансировщики нагрузки, серверы приложений и БД.

Зависимости услуг (Service Dependencies)

Определяют, как компоненты полагаются друг на друга:

- **Прямые зависимости:** Связь между веб-сервером и его базой данных.
- **Косвенные зависимости:** Влияние сетевого коммутатора на работу кластера приложений.
- **Внешние зависимости:** Сторонние API (например, банковские шлюзы или облачные сервисы).

Понимание зависимостей

- **Прямые зависимости:** Компоненты, которые взаимодействуют напрямую.
- **Транзитивные зависимости:** Компоненты, связанные через посредников.
- **Критический путь:** Цепочка зависимостей, которая должна быть доступна для работы услуги.
- **Тип зависимости:** База данных, API, очередь сообщений, кэш и т. д.

Иерархия услуг

Услуги организованы иерархически — от уровня бизнеса до инфраструктуры.

Четырехуровневая иерархия:

1. **Бизнес-услуга (верхний уровень):** Ориентирована на клиента и бизнес-ценность, регулируется SLA. Пример: «Интернет-магазин».
2. **Техническая услуга (поддерживающий слой):** Общие компоненты и технические возможности. Пример: «Обработка платежей».
3. **Компонент приложения (слой реализации):** Отдельные приложения, микросервисы, базы данных. Пример: «Order Management API».
4. **Инфраструктура (фундаментальный слой):** Серверы, сетевые устройства, системы хранения. Пример: «Сервер приложений 01».

Методы обнаружения

Автоматизированное обнаружение

RS-Discovery (R-Sight) использует несколько методов автоматического поиска:

- **Обнаружение на основе трафика:** Анализирует сетевой трафик, идентифицирует протоколы, измеряет объем данных и задержки.
- **Обнаружение на основе конфигураций:** Парсит файлы конфигурации, извлекает строки подключения, анализирует шаблоны IaC (инфраструктура как код).
- **Анализ логов:** Изучает логи приложений для поиска паттернов взаимодействия и путей прохождения данных.

Картографирование на базе ИИ

Движок ИИ-маппинга:

- **Распознает паттерны:** Идентифицирует типовые архитектуры услуг.
- **Проверяет зависимости:** Подтверждает обнаруженные взаимосвязи.
- **Предсказывает недостающие компоненты:** Предлагает вероятные, но не обнаруженные зависимости.
- **Обучается на изменениях:** Повышает точность на основе ручных правок.

Моделирование услуги

Определение услуги

Каждый сервис в RS-Discovery (R-Sight) включает:

- **Метаданные:** Имя, описание, версия, уровень критичности и соответствие стандартам (PCI-DSS, HIPAA и др.).
- **Владение:** Бизнес-владелец, технический владелец и контакты дежурной команды.
- **SLA:** Цели по доступности, времени ответа и пропускной способности.
- **Компоненты:** Точки входа, микросервисы, базы данных и внешние зависимости (сторонние API).

Динамическое обнаружение

Процесс идет непрерывно, чтобы находить точки входа, прослеживать соединения, классифицировать компоненты, строить граф зависимостей и определять границы услуг.

Возможности визуализации

Интерактивные карты услуг

Варианты разметки:

- **Иерархическая:** Показывает слои от бизнеса до железа.

- **Силовая (Force-directed):** Отображает органические связи между узлами.
- **Матричная:** Представляет зависимости в виде сетки.

Визуальные элементы:

- **Формы и иконки:** Указывают на тип компонента (БД, сервер и т.д.).
- **Цветовая кодировка:** Отражает состояние здоровья (Health Status).
- **Связи:** Толщина линий показывает объем трафика, а стиль (сплошная/пунктир) — тип соединения (синхронное/асинхронное).

Анализ влияния (Impact Analysis)

- **Прогноз влияния изменений:** Перед внесением правок система оценивает прямой эффект, каскадные последствия для других услуг и риски для бизнеса.
- **Симуляция сбоев:** При аварии система находит затронутые услуги, оценивает количество пострадавших пользователей, прогнозирует время восстановления и предлагает стратегии минимизации ущерба.

Оптимизация услуги

Система выявляет архитектурные анти-паттерны:

- **Циклические зависимости:** Создающие жесткую связанность.
- **Единые точки отказа:** Отсутствие избыточности.
- **Проблемы производительности:** Узкие места, высокая задержка или перегруженные компоненты.
- **Оптимизация затрат:** Избыточные ресурсы и неэффективная архитектура.

Интеграция и возможности

- **CI/CD:** Проверка зависимостей перед деплоем и обновление карт в реальном времени после него.
- **Мониторинг:** Автоматическая настройка алертов на основе критичности услуги и корреляция инцидентов с топологией.
- **Каталог сервисов:** Поиск по владельцу или технологии, доступ к документации (runbooks) и планам аварийного восстановления (DR).

9 АНАЛИЗАТОР БИЗНЕС-УСЛУГ

Обзор

Business Service Analyzer — это интеллектуальная функция на базе ИИ, которая автоматически обнаруживает, сопоставляет и анализирует бизнес-услуги в вашей ИТ-инфраструктуре. Она объединяет обнаружение ПО, сетевой анализ и ИИ-аналитику для формирования комплексного представления о критически важных бизнес-услугах.

Ключевые возможности

- **ИИ-обнаружение услуг:** Автоматическая идентификация серверов, соединений и зависимостей на основе паттернов ПО и процессов.
- **Многошаговый мастер (Wizard):** Пошаговое руководство пользователя через этапы определения, обогащения, обнаружения и анализа услуги.
- **Интеллектуальная классификация:** Использование ИИ для определения ролей серверов (веб-сервер, сервер приложений, БД) и уровней (frontend, application, data, infrastructure).
- **Визуальный маппинг:** Интерактивные сетевые диаграммы, отображающие топологию услуги и зависимости.
- **Комплексная аналитика:** Генерируемый ИИ анализ архитектуры услуги, рисков и рекомендаций.

Как это работает

1. **Определение услуги:** Пользователь вводит название, описание, категорию (ERP, почта, БД) и выбирает начальное ПО из каталога.
2. **ИИ-обогащение:** Система предлагает связанные процессы, идентифицирует типовые порты и рекомендует паттерны поиска для обнаружения.
3. **Автоматическое обнаружение:** Анализатор ищет серверы с указанными процессами, сопоставляет сетевые соединения и находит компоненты инфраструктуры.
4. **Классификация и анализ:** ИИ распределяет компоненты по ролям и уровням, присваивая каждому элементу оценку достоверности.
5. **Генерация инсайтов:** ИИ готовит отчет, включающий обзор архитектуры, оценку влияния на бизнес, технический анализ (отказоустойчивость, масштабируемость) и рекомендации по улучшению.

Сценарии использования

- **Документирование:** Автоматическое создание документации для существующих услуг.
- **Маппинг зависимостей:** Понимание связей перед внесением изменений.
- **Оценка рисков:** Выявление единых точек отказа (SPOF).
- **Комплаенс:** Документирование архитектуры для аудитов.
- **Планирование миграции:** Полный аудит компонентов перед переносом в облако.

Техническая архитектура и данные

Система интегрируется с сетевым сканером, CMDB (для создания связей между КЕ типа «Бизнес-услуга»), ИИ-сервисами (Claude AI) и нормализованным каталогом ПО.

- **Модель данных:** Бизнес-услуги сохраняются как объекты КЕ с привязанными ИИ-инсайтами, метаданными обнаружения и связями с серверами.
- **Безопасность:** Изоляция данных на уровне арендатора (tenant), ролевой доступ (RBAC) и аудит всех операций. **Конфиденциальные данные не отправляются в ИИ-сервисы.**

Преимущества

- **Экономия времени:** Сокращение процесса маппинга с недель до минут.
- **Точность:** ИИ находит скрытые зависимости, которые часто упускаются вручную.
- **Прозрачность:** Единый стандарт документации услуг для всей организации.

10 ОТЧЕТНОСТЬ

Обзор отчетности

Модуль отчетности RS-Discovery (R-Sight) преобразует данные вашей CMDB в практически значимую информацию с помощью генерации отчетов на базе ИИ, настраиваемых шаблонов и интерактивных панелей мониторинга. Создавайте профессиональные отчеты и визуализации, чтобы понимать состояние вашей инфраструктуры, отслеживать производительность и принимать решения на основе данных.

Что вы можете делать

Мгновенная генерация отчетов

- Используйте готовые шаблоны для стандартных сценариев
- Задавайте вопросы на простом английском языке и получайте отчеты автоматически
- Визуализируйте данные с помощью графиков, таблиц и статистики
- Создавайте пользовательские отчеты, адаптированные под ваши нужды

Построение интерактивных панелей мониторинга

- Объединяйте несколько отчетов в комплексные панели мониторинга
- Добавляйте виджеты KPI и метрики в реальном времени
- Делитесь панелями мониторинга со своей командой
- Адаптивный дизайн работает на любом устройстве

Аналитика на базе ИИ

- Описывайте то, что вы хотите увидеть, на естественном языке
- Получайте интеллектуальные выводы и рекомендации
- Автоматизированный анализ трендов и закономерностей
- Умные предложения по визуализации

Доступные возможности

Шаблоны отчетов

- **Готовые шаблоны:** отчеты, готовые к использованию в стандартных сценариях
- **Пользовательские шаблоны:** создание отчетов с помощью конструктора шаблонов
- **Генерация ИИ:** создание отчетов путем описания того, что вам нужно
- **Библиотека шаблонов:** сохранение и обмен шаблонами с вашей командой

Визуализации

- **Графики:** столбчатые, линейные, круговые, кольцевые, с областями и точечные диаграммы
- **Таблицы:** сортируемые и фильтруемые таблицы данных с пагинацией
- **Статистика:** показатели KPI с индикаторами трендов
- **Шкалы (Gauges):** индикаторы прогресса с цветовой кодировкой пороговых значений
- **Интерактивность:** клик для перехода к детализированным данным (drill down)

Источники данных

- **CMDB:** конфигурационные единицы и связи
- **Запросы на обслуживание:** данные тикетов и рабочих процессов
- **Системные события:** журналы активности и изменений
- **Метрики производительности:** данные об использовании ресурсов

Функции панелей мониторинга

- **Drag & Drop:** удобное расположение виджетов
- **Адаптивность:** работа на десктопах, планшетах и мобильных устройствах
- **Автообновление:** поддержание актуальности данных с настраиваемыми интервалами
- **Общий доступ:** совместное использование с отдельными лицами или командами
- **Разрешения:** контроль того, кто может просматривать и редактировать

Как это работает

Генерация отчетов на базе ИИ

1. **Ввод на естественном языке:** опишите ваш отчет простым языком
2. **Анализ намерений:** ИИ понимает, какие данные вам нужны
3. **Генерация запроса:** автоматическое создание запросов к базе данных
4. **Выбор визуализации:** выбор наилучшего типа диаграммы
5. **Создание отчета:** генерация полного шаблона отчета

Система шаблонов

- **Многократное использование:** сохранение шаблонов для повторного использования
- **Настраиваемость:** изменение шаблонов под ваши задачи
- **Возможность обмена:** совместное использование шаблонов внутри организации
- **Версионность:** отслеживание изменений и обновлений

Интеграция с панелями мониторинга

- **Библиотека виджетов:** преобразование любого отчета в виджет панели мониторинга
- **Управление макетом:** адаптивные макеты на основе сетки
- **Обновления в реальном времени:** настраиваемые интервалы обновления
- **Мультитенантность:** разделение данных по департаментам или командам

Лучшие практики

Создание эффективных отчетов

- **Начинайте с простого:** начните с базовых графиков и таблиц
- **Знайте свою аудиторию:** разные представления для разных ролей
- **Фокусируйтесь на инсайтах:** включайте контекст и рекомендации
- **Используйте фильтры:** сужайте данные до релевантных периодов времени
- **Тщательно тестируйте:** проверяйте отчеты на реальных данных

Дизайн панелей мониторинга

- **Самое важное — в начале:** размещайте ключевые метрики сверху
- **Логическая группировка:** группируйте связанные виджеты вместе
- **Согласованность размеров:** похожие виджеты должны быть схожих размеров
- **Производительность:** балансируйте актуальность данных с нагрузкой на систему
- **Удобство для мобильных устройств:** обеспечьте читаемость на небольших экранах

Качество данных

- **Проверяйте источники:** убедитесь в точности данных перед составлением отчета
- **Работайте с отсутствующими данными:** учитывайте неполную информацию
- **Документируйте допущения:** четко указывайте ограничения данных
- **Регулярные обновления:** поддерживайте актуальность отчетов свежими данными

Распространенные варианты использования

Управление инфраструктурой

- **Инвентаризация активов:** отслеживание аппаратных и программных активов
- **Анализ конфигураций:** мониторинг соответствия конфигураций
- **Планирование мощностей:** прогнозирование потребностей в ресурсах
- **Влияние изменений:** понимание последствий изменений

Управление услугами

- **Аналитика запросов:** мониторинг эффективности службы поддержки
- **Здоровье услуг:** отслеживание доступности и производительности
- **Удовлетворенность пользователей:** измерение качества услуг
- **Улучшение процессов:** выявление «узких мест»

Мониторинг операций

- **Производительность системы:** мониторинг ключевых метрик
- **Анализ инцидентов:** понимание паттернов сбоев

- **Соответствие безопасности:** отслеживание состояния безопасности
- **Анализ затрат:** мониторинг расходов на ИТ

Устранение неполадок

Общие проблемы

- **Данные не отображаются:** проверьте диапазоны дат и фильтры
- **Низкая производительность:** уменьшите объем данных или добавьте фильтры
- **Графики не загружаются:** проверьте требования к формату данных
- **Ошибки доступа:** убедитесь в наличии соответствующих прав доступа

Получение помощи

- **Документация:** подробные руководства и примеры
- **Поддержка:** свяжитесь с вашим системным администратором
- **Сообщество:** форумы пользователей и база знаний
- **Обучение:** видеоуроки и лучшие практики

11 КОНСТРУКТОР ПАНЕЛЕЙ МОНИТОРИНГА

Конструктор панелей мониторинга RS-Discovery (R-Sight) позволяет создавать интерактивные панели мониторинга, объединяя шаблоны отчетов в настраиваемые дисплеи для отслеживания данных в реальном времени. Создавайте комплексные представления вашей инфраструктуры, услуг и операций с помощью простого интерфейса drag-and-drop.

Что вы можете собрать

Типы панелей мониторинга

- **Личные:** ваше частное рабочее пространство с пользовательскими виджетами
- **Командные:** общие представления для конкретных отделов или команд
- **Системные:** панели масштаба всей компании для руководителей и операционных служб

Доступные виджеты

- **Графики:** столбчатые, линейные, круговые, кольцевые, с областями и точечные диаграммы
- **Статистика:** показатели KPI с индикаторами трендов и прогресс-барами
- **Таблицы:** сортируемые и фильтруемые сетки данных с пагинацией
- **Списки:** последние действия, алерты и уведомления
- **Шкалы (Gauges):** индикаторы прогресса с цветовой кодировкой пороговых значений

Функции панели мониторинга

Управление макетом

- **Сеточный макет:** 12-колоночная адаптивная система сетки
- **Drag & Drop:** легкое позиционирование виджетов
- **Автоматический подбор размера:** виджеты подстраиваются под содержимое
- **Обнаружение столкновений:** предотвращает наложение виджетов друг на друга
- **Мобильная адаптивность:** работа на устройствах любого размера

Конфигурация виджетов

- **Автообновление:** установка интервалов обновления от 1 до 15 минут
- **Фильтрация данных:** применение фильтров к данным виджета
- **Пользовательская стилизация:** настройка цветов, шрифтов и внешнего вида
- **Drill-Down:** клик по графикам для просмотра детальных данных
- **Варианты экспорта:** экспорт отдельных виджетов (если доступно)

Обновления в реальном времени

- **Живые данные:** виджеты обновляются автоматически согласно интервалам
- **Индикаторы статуса:** показ времени последнего обновления данных
- **Состояния загрузки:** визуальная обратная связь во время обновления данных
- **Обработка ошибок:** четкие сообщения об ошибках при сбое загрузки данных

Как это работает

1. Создание виджета

При добавлении виджета на панель мониторинга:

- Выберите шаблон отчета в качестве источника данных
- Выберите тип визуализации (график, таблица, статистика и т. д.)
- Настройте параметры отображения и фильтры
- Установите интервал обновления и предпочтения по размеру
- Виджет добавляется в сетку вашей панели мониторинга

2. Поток данных

- **Запрос шаблона:** виджет использует запрос из шаблона отчета
- **Извлечение данных:** система получает данные из MongoDB
- **Обработка:** данные обрабатываются и форматируются
- **Визуализация:** библиотека графиков отрисовывает изображение

- **Обновления:** процесс повторяется согласно интервалу обновления

3. Движок макета

- **Система сетки:** использует react-grid-layout для адаптивного позиционирования
- **Контрольные точки (Breakpoints):** подстраивается под разные размеры экрана
- **Сохранение:** макет сохраняется автоматически
- **Обработка столкновений:** предотвращает перекрытие виджетов

Доступные типы виджетов

Виджеты графиков

- **Столбчатые диаграммы:** сравнение значений по категориям; горизонтальные или вертикальные столбцы; поддержка нескольких серий данных.
- **Линейные диаграммы:** отображение трендов во времени; несколько метрик на одном графике; плавные или ступенчатые стили линий.
- **Круговые/Кольцевые диаграммы:** отображение пропорциональных данных; интерактивные сегменты; настраиваемые цветовые схемы.
- **Диаграммы с областями:** визуализация изменения объема во времени; поддержка стекирования (наслоения); плавные градиенты.

Виджеты метрик

- **Статистика KPI:** отображение крупных чисел; индикаторы трендов (стрелки вверх/вниз); прогресс-бары; цветовые пороги.
- **Шкалы (Gauges):** показ прогресса относительно целей; цветовые зоны (красный/желтый/зеленый); анимированное движение стрелки.

Виджеты отображения данных

- **Таблицы данных:** сортируемые столбцы; фильтруемые строки; поддержка пагинации; возможность экспорта.
- **Списки активности:** последние события и изменения; прокручиваемый контент; форматирование меток времени.

Управление панелями мониторинга

Разрешения

- **Владелец:** полный контроль над панелью мониторинга
- **Редактор:** может изменять виджеты и макет
- **Зритель:** может только просматривать панель мониторинга
- **Доступ команды:** совместное использование с конкретными командами

Варианты совместного доступа

- **Публичная ссылка:** доступ для любого пользователя по URL
- **Командный доступ:** совместное использование с участниками конкретной команды
- **Только для чтения:** зрители не могут изменять панель мониторинга
- **Клонирование:** создание копий для последующей настройки

Настройки панели мониторинга

- **Автообновление:** включение/выключение автоматических обновлений
- **Интервал обновления:** установка глобальной частоты обновления
- **Диапазон дат:** период времени по умолчанию для всех виджетов
- **Тема:** выбор цветовой схемы и стиля
- **Полноэкранный режим:** скрытие навигации для выделенных дисплеев

Лучшие практики

Дизайн панелей мониторинга

- **Начинайте с цели:** какие решения поддерживает эта панель мониторинга?
- **Важное — в начало:** размещайте ключевые метрики в верхнем левом углу
- **Логическая группировка:** располагайте связанные виджеты рядом
- **Единообразие размеров:** похожие виджеты должны иметь схожие размеры
- **Оставляйте свободное пространство:** не перегружайте панель мониторинга

Оптимизация производительности

- **Разумная частота обновления:** балансируйте актуальность и нагрузку

- **Ограничение количества виджетов:** избыток виджетов может замедлить работу
- **Использование фильтров:** сокращайте объем данных, где это возможно
- **Мониторинг времени загрузки:** регулярно проверяйте скорость работы виджетов

Распространенные варианты использования

- **Центр ИТ-операций:** здоровье услуг, активные алерты, метрики производительности (CPU, память).
- **Для руководителя:** высокоуровневые бизнес-метрики, доступность услуг, соответствие SLA, затраты на ИТ.
- **Для Service Desk:** открытые тикеты по приоритетам, время решения, удовлетворенность клиентов.
- **Для compliance:** статус безопасности, готовность к аудиту, индикаторы рисков.

Устранение неполадок

- **Виджет не загружается:** проверьте соединение с источником данных и права доступа.
- **Низкая производительность:** увеличьте интервал обновления или уменьшите число виджетов.
- **Проблемы с макетом:** попробуйте обновить страницу или сбросить макет.
- **Данные не обновляются:** проверьте настройки автообновления и источник данных.

Текущие ограничения

Пока не доступно:

- Обновления через WebSocket в реальном времени (сейчас используется опрос/polling)
- Расширенные типы виджетов: сетевые диаграммы, тепловые карты (heatmaps)
- Функционал экспорта: нельзя экспортировать панели мониторинга в PDF/изображение
- Планирование: отсутствие автоматической рассылки панелей мониторинга
- Кросс-виджетная фильтрация: виджеты работают независимо

12 ШАБЛОНЫ ОТЧЕТОВ

RS-Discovery (R-Sight) включает в себя обширную библиотеку из более чем 32 готовых шаблонов отчетов, которые помогут вам быстро приступить к работе. Эти шаблоны охватывают распространенные сценарии управления ИТ и могут быть использованы в исходном виде или настроены под ваши конкретные нужды.

Доступные шаблоны

Отчеты по CMDB и инфраструктуре

- **CI Status Overview (Обзор статуса КЕ)**
  - **Описание:** Визуальный обзор всех конфигурационных единиц по их текущему статусу.
  - **Визуализация:** Круговая диаграмма, показывающая статусы «Активен», «Неактивен» и другие.
  - **Варианты использования:** Быстрая проверка состояния вашей инфраструктуры.
  - **Размер виджета:** 4x3 единицы сетки.
  - **Обновление:** Каждые 5 минут.
- **CI Types Distribution (Распределение типов КЕ)**
  - **Описание:** Разбивка вашей инфраструктуры по типам конфигурационных единиц.
  - **Визуализация:** Кольцевая диаграмма, показывающая серверы, рабочие станции, ПО и т. д.
  - **Варианты использования:** Понимание состава вашей инфраструктуры.
  - **Размер виджета:** 4x3 единицы сетки.
  - **Обновление:** Каждые 10 минут.
- **Active CI Count (Количество активных КЕ)**
  - **Описание:** Общее количество активных конфигурационных единиц.
  - **Визуализация:** Крупный статистический показатель с индикатором тренда.
  - **Варианты использования:** Виджет для KPI-дашборда, краткая сводка для руководства.
  - **Размер виджета:** 3x2 единицы сетки.
  - **Обновление:** Каждые 10 минут.
- **Total CI Count (Общее количество КЕ)**
  - **Описание:** Общее количество всех конфигурационных единиц в вашей CMDB.
  - **Визуализация:** Карточка статистики с индикатором тренда.
  - **Варианты использования:** Панели мониторинга для руководителей, обзор инфраструктуры.
  - **Размер виджета:** 3x2 единицы сетки.
  - **Обновление:** Каждые 10 минут.
- **Total Server Count (Общее количество серверов)**
  - **Описание:** Общее количество серверов в CMDB.
  - **Визуализация:** Карточка статистики с числом.
  - **Варианты использования:** Метрики инфраструктуры, планирование мощностей.
  - **Размер виджета:** 3x2 единицы сетки.
  - **Обновление:** Каждые 10 минут.
- **Total Workstation Count (Общее количество рабочих станций)**
  - **Описание:** Общее количество рабочих станций в CMDB.
  - **Визуализация:** Карточка статистики с числом.
  - **Варианты использования:** Управление рабочими местами, планирование лицензий.
  - **Размер виджета:** 3x2 единицы сетки.
  - **Обновление:** Каждые 10 минут.

Отчеты по обнаружению устройств (Discovery)

- **Device Count by Type (Количество устройств по типу)**
  - **Описание:** Общее количество серверов и рабочих станций в CMDB.

- **Визуализация:** Круговая диаграмма, показывающая распределение «Сервер vs Рабочая станция».
- **Device Discovery by Year (Обнаружение устройств по годам)**
  - **Описание:** Показывает обнаруженные устройства, сгруппированные по годам.
  - **Визуализация:** Столбчатая диаграмма с годовыми трендами.
- **Device Discovery Monthly Timeline (Ежемесячная шкала обнаружения устройств)**
  - **Описание:** Ежемесячная разбивка обнаружения устройств.
  - **Визуализация:** Линейная диаграмма или диаграмма с областями, показывающая тренды обнаружения.
- **Device Discovery by Day of Week (Обнаружение устройств по дням недели)**
  - **Описание:** Распределение обнаружений по дням недели.
  - **Визуализация:** Столбчатая диаграмма, показывающая еженедельные паттерны.
- **Recently Discovered Devices (Недавно обнаруженные устройства)**
  - **Описание:** Список самых последних обнаруженных устройств.
  - **Визуализация:** Таблица с деталями устройств.
- **Device Age Distribution (Распределение устройств по возрасту)**
  - **Описание:** Показывает возраст устройств на основе даты их обнаружения.
  - **Визуализация:** Столбчатая диаграмма с возрастными диапазонами.

Отчеты по операционным системам

- **Operating System Distribution (Распределение операционных систем)**
  - **Описание:** Показывает устройства, сгруппированные по операционной системе (Windows 11, Windows 10, Linux и т. д.).
- **OS Distribution Matrix - All Devices (Матрица распределения ОС — все устройства)**
  - **Описание:** Комплексное распределение ОС по всем устройствам.
  - **Визуализация:** Матрица/Таблица с подробными версиями.
- **OS Distribution Matrix - Servers (Матрица распределения ОС — серверы)**
  - **Описание:** Распределение ОС только для серверов.
- **OS Distribution Matrix - Workstations (Матрица распределения ОС — рабочие станции)**
  - **Описание:** Распределение ОС только для рабочих станций.

Отчеты по оборудованию (Hardware)

- **Server Memory Distribution (Распределение памяти серверов)**
  - **Описание:** Распределение объема памяти по серверам (4GB, 8GB, 16GB и т. д.).
- **Workstation Memory Distribution (Распределение памяти рабочих станций)**
  - **Описание:** Распределение объема памяти по рабочим станциям.
- **Disk Type Distribution (Распределение типов дисков)**
  - **Описание:** Распределение типов дисков (SSD, HDD, NVMe).
- **Workstation CIs by Model Name (КЕ рабочих станций по названию модели)**
  - **Описание:** Распределение рабочих станций по производителю и модели.

Отчеты по программному обеспечению

- **Total Software Instance Count (Общее количество экземпляров ПО)**
  - **Описание:** Общее количество отслеживаемых инсталляций ПО.
- **Database Software Distribution (Распределение программного обеспечения БД)**
  - **Описание:** Показывает всё ПО баз данных, установленное в инфраструктуре (SQL Server, Oracle, MySQL, PostgreSQL и т. д.).
- **Top Server Applications (Топ серверных приложений)**
  - **Описание:** Самые часто устанавливаемые серверные приложения (Топ-20).
- **Top Workstation Applications (Топ приложений для рабочих станций)**
  - **Описание:** Самые часто устанавливаемые десктопные приложения (Топ-20).
- **Software by Vendor (ПО по поставщикам)**
  - **Описание:** Распределение ПО, сгруппированное по вендорам.

Отчеты по управлению услугами (Service Management)

- **Open Requests by Priority (Открытые запросы по приоритетам)**
  - **Описание:** Текущие открытые запросы на обслуживание, сгруппированные по уровню приоритета.
- **Task Status Summary (Сводка по статусам задач)**
  - **Описание:** Обзор показателей завершения задач по всем проектам.
  - **Визуализация:** Таблица, показывающая количество и процентное соотношение статусов.

Сетевые отчеты

- **Hardware Count by IP Range (Количество оборудования по IP-диапазонам)**
  - **Описание:** Распределение устройств по IP-диапазонам.
- **IP Subnet Distribution (Распределение по IP-подсетям)**
  - **Описание:** Визуальное представление использования сетевых подсетей.

Операции и мониторинг

- **Recent Activities (Последние действия)**
  - **Описание:** Список недавних системных действий и изменений.
- **CMDB Data Freshness Score (Оценка актуальности данных CMDB)**
  - **Описание:** Показывает, насколько недавно обновлялись данные КЕ.
- **Stale CI Detection (Обнаружение устаревших КЕ)**
  - **Описание:** Идентифицирует КЕ, которые давно не обновлялись.

Конфигурация шаблона

Источники данных Шаблоны могут получать данные из:

- **CMDB:** конфигурационные единицы и связи.
- **Service Requests:** данные тикетов и рабочих процессов.
- **System Events:** журналы действий и изменений.
- **Performance Metrics:** данные об использовании ресурсов.

Примечание: Интеграции с внешними API запланированы в будущих релизах.

Настройка фильтров

- **Диапазоны дат:** последние 7 дней, 30 дней, произвольные периоды.
- **Департаменты:** фильтрация по организационным подразделениям.
- **Типы устройств:** серверы, рабочие станции, сетевые устройства.
- **Статус:** активен, неактивен, обслуживание.

Лучшие практики

- **Выбор шаблона:** Начинайте с цели — на какой вопрос вы пытаетесь ответить?
- **Советы по настройке:** Всегда создавайте копию предопределенных шаблонов перед редактированием.
- **Оптимизация производительности:** Используйте фильтры, чтобы ограничить диапазоны данных.
- **Интеграция с панелями мониторинга:** Группируйте связанные виджеты по теме или функции.

Расширенные возможности

- **Шаблоны с поддержкой ИИ:** Включают умные инсайты (автоматический анализ), обнаружение аномалий и анализ трендов.
- **Возможности Drill-Down:** Нажмите на элементы графика, чтобы увидеть детальные данные или перейти к связанным отчетам.

Будущие функции автоматизации

- **Автоматическая генерация:** запуск отчетов по расписанию.
- **Доставка по почте:** автоматическая отправка заинтересованным лицам.
- **Оповещения по порогам:** уведомление, когда значения превышают лимиты.

Устранение неполадок

- **В шаблоне нет данных:** Проверьте диапазон дат (может быть слишком узким), проверьте права доступа и настройки фильтров.
- **Низкая производительность:** Сократите диапазон дат или добавьте более специфичные фильтры.
- **График не отображается:** Убедитесь, что формат данных соответствует визуализации и присутствуют все обязательные поля.

13 ПОЛЬЗОВАТЕЛЬСКИЕ ОТЧЕТЫ

Конструктор пользовательских отчетов RS-Discovery (R-Sight) позволяет создавать специализированные отчеты, отвечающие вашим конкретным бизнес-задачам. Если вам нужно отслеживать соответствие активов, анализировать эффективность услуг или контролировать состояние инфраструктуры, конструктор пользовательских отчетов обеспечивает интуитивно понятный способ преобразования данных вашей CMDB в практически значимую информацию.

Что такое пользовательские отчеты?

Пользовательские отчеты позволяют создавать персонализированные представления данных вашей ИТ-инфраструктуры путем:

- Выбора конкретных данных из коллекций вашей CMDB
- Применения фильтров для фокусировки на релевантной информации
- Выбора типов визуализации, которые лучше всего представляют ваши данные
- Настройки расписания автоматической генерации отчетов
- Предоставления доступа к отчетам членам команды и заинтересованным лицам

Создание пользовательских отчетов

Генерация отчетов с помощью ИИ

RS-Discovery (R-Sight) включает в себя конструктор отчетов на базе ИИ, который понимает запросы на естественном языке и автоматически генерирует соответствующую конфигурацию отчета. Как использовать генерацию отчетов с помощью ИИ:

1. Перейдите в раздел «Отчеты и панели мониторинга»
2. Нажмите «Создать пользовательский отчет»
3. Выберите «Генерация с помощью ИИ»
4. Опишите то, что вы хотите увидеть, обычными словами

Примеры запросов:

- «Покажи мне все серверы в продуктивной среде»
- «Подсчитай конфигурационные единицы по типу»
- «Выведи список Windows-серверов с оперативной памятью более 32 ГБ»
- «Покажи инциденты обслуживания за прошлую неделю, сгруппированные по приоритету»
- «Отобрази статус соответствия по бизнес-подразделениям»

ИИ анализирует ваш запрос и:

- Идентифицирует соответствующие источники данных
- Определяет подходящие фильтры и группировки
- Предлагает лучший тип визуализации
- Генерирует предварительный просмотр вашего отчета

Затем вы можете просмотреть, изменить и сохранить шаблон отчета для использования в будущем.

Ручное создание отчета

Для более точного контроля вы можете создавать отчеты вручную через интерфейс конструктора отчетов. Шаги для создания отчета вручную:

1. Нажмите «Создать пользовательский отчет» и выберите «Ручной конструктор»
2. Выберите источник данных (КЕ, Услуги, События, Уязвимости и т. д.)
3. Выберите поля, которые вы хотите включить
4. Настройте фильтры для сужения результатов
5. Выберите тип визуализации
6. Предварительно просмотрите ваш отчет
7. Сохраните как шаблон

Доступные типы отчетов

Сводные отчеты (Summary Reports)

Отображают высокоуровневые метрики и ключевые показатели эффективности. Лучше всего использовать для:

- Панелей мониторинга для руководства

- Быстрых обзоров статуса
- Отслеживания KPI
- Сводок по трендам

Общие примеры:

- Общее количество активов по типу
- Процент доступности услуг
- Количество открытых инцидентов
- Сводки по оценке соответствия (compliance score)

Детальные списки (Detailed Lists)

Показывают комплексные данные в табличном формате с возможностью сортировки и фильтрации. Лучше всего использовать для:

- Инвентаризации активов
- Журналов аудита (audit trails)
- Детальных расследований
- Экспорта данных

Общие примеры:

- Полная инвентаризация серверов со спецификациями
- Список несоответствующих конфигурационных единиц
- Установленное ПО по системам
- История изменений для конкретных услуг

Анализ трендов (Trend Analysis) Визуализируют изменения данных во времени для выявления закономерностей и прогнозирования будущих состояний. Лучше всего использовать для:

- Планирования мощностей
- Мониторинга производительности
- Анализа влияния изменений
- Исторических сравнений

Общие примеры:

- Тренды использования CPU за 90 дней
- Объем инцидентов по неделям
- Паттерны роста хранилищ данных
- Доступность услуг во времени

Сравнительные отчеты (Comparison Reports)

Сравнивают данные по различным категориям, периодам времени или организационным единицам. Лучше всего использовать для:

- Бенчмаркинга
- Решений по распределению ресурсов
- Сравнения производительности
- Анализа затрат

Общие примеры:

- Использование ресурсов по департаментам
- Производительность услуг по регионам
- Оценки соответствия по бизнес-подразделениям
- Сравнительный анализ поставщиков

Отчеты о связях (Relationship Reports)

Отображают соединения и зависимости между конфигурационными единицами и услугами. Лучше всего использовать для:

- Анализа влияния (impact analysis)
- Планирования изменений
- Картирования услуг (service mapping)
- Визуализации зависимостей

Общие примеры:

- Деревья зависимостей услуг
- Взаимосвязи компонентов приложений
- Представления топологии сети
- Карты бизнес-услуг

Варианты визуализации

Диаграммы и графики

Столбчатые диаграммы

- Сравнение значений по категориям
- Отображение рейтингов и распределений
- Вывод сгруппированных сравнений

Линейные графики

- Отслеживание трендов во времени
- Отображение темпов изменений
- Вывод нескольких метрик на одной оси

Круговые диаграммы

- Отображение пропорций и процентных соотношений
- Визуализация структуры состава
- Отображение доли рынка или распределения

Диаграммы с областями

- Акцент на накопленных итогах
- Отображение соотношения части к целому во времени
- Вывод вклада категорий в стеке (наслоении)

Точечные диаграммы

- Выявление корреляций
- Обнаружение аномалий (выбросов)
- Отображение паттернов распределения

Таблицы

Интерактивные таблицы данных

- Сортировка по любому столбцу
- Фильтрация и поиск данных
- Экспорт в Excel или CSV
- Настройка видимости столбцов

Сводные таблицы

- Динамическая реорганизация данных
- Кросс-табличный анализ
- Множественные функции агрегации
- Возможности детализации (drill-down)

Ключевые показатели эффективности

Карточки KPI

- Отображение одиночных метрик
- Индикаторы трендов (стрелки вверх/вниз)
- Сравнение с целевыми показателями
- Цветовые индикаторы статуса

Расширенные визуализации

Тепловые карты

- Отображение паттернов интенсивности
- Идентификация «горячих точек»
- Вывод матриц корреляции
- Временные паттерны активности

Древовидные карты

- Иерархическое представление данных
- Представления распределения ресурсов
- Отображение использования хранилищ
- Сравнение вложенных категорий

Сетевые диаграммы

- Визуализация связей
- Картирование зависимостей
- Анализ влияния
- Архитектура услуг

Фильтрация и настройка

Типы фильтров

Фильтры полей

- Текстовое соответствие (содержит, равно, начинается с)
- Числовые сравнения (больше чем, меньше чем, между)
- Диапазоны дат (последние 7 дней, этот месяц, произвольный диапазон)
- Опции множественного выбора
- Логические условия (Boolean)

Динамические фильтры

- Данные конкретного пользователя (мои активы, мои тикеты)
- Фильтрация на основе ролей
- Данные конкретного арендатора (тенанта)
- Контекстные фильтры на основе текущего выбора

Временные фильтры

- Относительные временные диапазоны (последний час, сегодня, эта неделя)
- Абсолютные диапазоны дат (1 января – 31 марта)
- Скользящие окна (последние 30 дней)
- Расчет рабочих дней

Параметры настройки

Группировка данных

- Группировка по категории, типу или статусу
- Иерархическая группировка (департамент > команда > сотрудник)
- Пользовательские определения групп
- Автоматическая разбивка числовых значений по сегментам (bucketing)

Агрегации

- Подсчет записей
- Суммирование числовых значений
- Вычисление средних значений
- Поиск минимальных/максимальных значений
- Подсчет уникальных значений

Сортировка

- По возрастанию или убыванию
- Множественные уровни сортировки
- Пользовательский порядок сортировки
- Автоматическое ранжирование

Форматирование

- Форматы чисел (валюта, проценты, десятичные знаки)
- Форматы дат (локальные предпочтения)
- Цветовая кодировка по значению
- Условное форматирование

Совместная работа и обмен данными

Общий доступ к отчетам

Доступ для пользователей

- Откройте ваш пользовательский отчет
- Нажмите кнопку «Поделиться» (Share)
- Выберите пользователей или группы
- Установите уровень разрешений (только просмотр или возможность редактирования)
- Нажмите «Поделиться»
- Получатели увидят общий отчет в своем списке отчетов.

Доступ для команд

- Доступ для целых департаментов
- Доступ для проектных групп
- Доступ для управленческих групп
- Доступ на уровне всей организации

Уровни разрешений

Только просмотр

- Может запускать отчет
- Может применять фильтры
- Может экспортировать данные
- Не может изменять конфигурацию отчета

Может редактировать

- Все разрешения на просмотр
- Может изменять фильтры
- Может изменять визуализации
- Может обновлять настройки отчета

Владелец

- Все разрешения на редактирование
- Может делиться с другими
- Может удалять отчет
- Может управлять разрешениями

Встроенные отчеты

Отчеты могут быть встроены в:

- Пользовательские панели мониторинга
- Записи каталога услуг
- Страницы конфигурационных единиц (KE) в CMDB
- Внешние порталы (при наличии надлежащей аутентификации)

Шаблоны отчетов

Использование предопределенных шаблонов

RS-Discovery (R-Sight) включает готовые к использованию шаблоны отчетов для стандартных сценариев:

Инфраструктурные отчеты

- Инвентаризация серверов по операционным системам
- Статус сетевых устройств
- Сводка по использованию хранилищ
- Распределение виртуальных машин

Сервисные отчеты

- Панели мониторинга доступности услуг
- Объем инцидентов по услугам
- Карта зависимостей услуг
- Отслеживание соблюдения SLA

Отчеты о соответствии (Compliance)

- Сводка по нарушениям политик
- Обнаружение дрейфа конфигураций (drift detection)
- Оценка состояния безопасности
- Отчет о готовности к аудиту

Отчеты по управлению активами

- Статус жизненного цикла оборудования
- Соответствие лицензий ПО
- Закрепление активов по департаментам
- Отслеживание вывода из эксплуатации (End-of-life)

Создание шаблонов отчетов

Сохраняйте часто используемые отчеты как шаблоны для удобного повторного использования:

- Создайте и настройте ваш пользовательский отчет
- Протестируйте его с различными фильтрами для обеспечения гибкости
- Нажмите «Сохранить как шаблон»
- Укажите описательное имя и категорию
- Добавьте теги для удобного поиска
- Выберите, стоит ли делать шаблон общим

Шаблоны могут включать:

- Предварительно настроенные источники данных
- Фильтры по умолчанию (с возможностью переопределения)
- Настройки визуализации

- Предпочтения форматирования
- Параметры расписания

Расписание и автоматизация

Отчеты по расписанию

Запускайте отчеты автоматически через регулярные интервалы:

- Откройте сохраненный отчет
- Нажмите «Расписание» (Schedule)
- Установите частоту (ежечасно, ежедневно, еженедельно, ежемесячно)
- Выберите время и день
- Выберите способ доставки
- Настройте получателей

Варианты доставки

Доставка по Email

- PDF-вложение
- Таблица Excel
- Файл данных CSV
- Ссылка на живой отчет

Снимки отчетов (Snapshots)

Создавайте снимки данных на определенный момент времени для:

- Исторических сравнений
- Документации по соответствию
- Отслеживания изменений
- Требований аудита

Снимки сохраняют:

- Данные на дату создания снимка
- Примененные фильтры и параметры
- Конфигурацию визуализации
- Аннотации и заметки

14 ЭКСПОРТ ОТЧЕТОВ (EXPORTING REPORTS)

Форматы экспорта (Export Formats)

PDF

- Отформатирован для печати
- Включает диаграммы и визуализации
- Сохраняет фирменный стиль
- Идеален для презентаций

Excel

- Необработанные данные в формате электронных таблиц
- Несколько листов для сложных отчетов
- Формулы и сводные таблицы
- Подходит для дальнейшего анализа

CSV

- Экспорт данных в виде простого текста
- Совместим со всеми системами
- Легко импортировать в другие системы
- Хорош для миграции данных

HTML

- Интерактивный веб-формат
- Сохраняет интерактивность
- Можно делиться через ссылку
- Подходит для встраивания в порталы

Параметры экспорта

Полный отчет (Full Report)

- Включает все данные и визуализации
- Сохраняет форматирование и стили
- Содержит метаданные и метки времени

Только данные (Data Only)

- Набор необработанных данных без форматирования
- Быстрее для больших наборов данных
- Подходит для массовой обработки

Только сводка (Summary Only)

- Ключевые метрики и основные моменты
- Формат обзора для руководителей
- Презентация на одну страницу

Лучшие практики

Дизайн отчетов

Соблюдайте простоту

- Сосредоточьтесь на ответах на один или два ключевых вопроса
- Избегайте загромождения слишком большим количеством метрик
- Используйте четкие, описательные заголовки
- Включайте контекст и пояснения

Выбирайте правильную визуализацию

- Используйте столбчатые диаграммы (bar charts) для сравнений
- Используйте линейные графики (line charts) для трендов
- Используйте круговые диаграммы (pie charts) для пропорций
- Используйте таблицы (tables) для детальных данных

Учитывайте вашу аудиторию

- Руководителям нужны сводки высокого уровня
- Аналитикам нужны детальные данные
- Операционным службам нужна информация для действий
- Комплаенсу (Compliance) нужны журналы аудита

Оптимизация производительности

Фильтруйте на раннем этапе

- Применяйте фильтры перед агрегацией
- Используйте индексированные поля , когда это возможно

- Ограничивайте диапазоны дат необходимыми периодами
- Избегайте чрезмерно широких запросов

Управляйте объемом данных

- Устанавливайте разумные лимиты строк
- Используйте выборку для больших наборов данных
- Внедряйте пагинацию для таблиц
- Планируйте тяжелые отчеты на часы минимальной нагрузки

Тестируйте на продуктивных данных

- Проверяйте производительность на реалистичных объемах данных
- Проверяйте наличие медленных запросов
- Подтверждайте эффективность фильтров
- Убедитесь, что визуализации отрисовываются правильно

Обслуживание

Регулярные проверки

- Проверяйте точность данных ежемесячно
- Обновляйте фильтры по мере изменения потребностей бизнеса
- Удаляйте неиспользуемые отчеты
- Обновляйте шаблоны в соответствии с новыми требованиями

Контроль версий

- Документируйте изменения в отчетах
- Храните резервные копии критически важных отчетов
- Отслеживайте, кто вносил изменения
- Ведите историю изменений

Гарантия качества

- Проверяйте расчеты и агрегации
- Сверяйте данные с исходными данными
- Тестируйте доставку по расписанию
- Проверяйте разрешения и настройки общего доступа

Распространенные варианты использования

Управление инфраструктурой (Infrastructure Management)

Отслеживание жизненного цикла серверов (Server Lifecycle Tracking) Контролируйте возраст оборудования и планируйте замену путем отслеживания дат покупки серверов, истечения срока гарантии и метрик производительности.

Планирование мощностей (Capacity Planning) Выявляйте ресурсы, приближающиеся к лимитам емкости, анализируя тренды использования вычислительных ресурсов, ресурсов хранения и сетевых ресурсов.

Соответствие конфигураций (Configuration Compliance) Обнаруживайте дрейф конфигураций (configuration drift), сравнивая текущие конфигурации с утвержденными базовыми показателями (baselines) и стандартами.

Управление услугами (Service Management)

Панели мониторинга здоровья услуг (Service Health Dashboard) Отображайте статус услуг в реальном времени, недавние инциденты и метрики производительности в едином консолидированном представлении.

Анализ инцидентов (Incident Analysis) Анализируйте паттерны инцидентов для выявления повторяющихся проблем, среднего времени устранения (mean time to resolution) и трендов корневых причин (root cause trends).

Процент успеха изменений (Change Success Rate) Отслеживайте показатели успеха и сбоев изменений для улучшения процессов управления изменениями и снижения рисков.

Безопасность и соответствие (Security and Compliance)

Панели мониторинга уязвимостей (Vulnerability Dashboard) Контролируйте открытые уязвимости по степени критичности (severity), возрасту и затронутым системам для приоритизации усилий по устранению.

Состояние соответствия (Compliance Posture) Отслеживайте статус соответствия в рамках нескольких структур с возможностью детализации (drill-down) до конкретных требований.

Тренды событий безопасности (Security Event Trends) Выявляйте паттерны и аномалии безопасности, анализируя ошибки аутентификации, нарушения политик и индикаторы угроз.

Управление активами (Asset Management)

Соответствие лицензий ПО (Software License Compliance) Сравнивайте установленное программное обеспечение с закупленными лицензиями для выявления избыточного развертывания или возможностей оптимизации.

Инвентаризация оборудования (Hardware Inventory) Поддерживайте точный инвентарный учет оборудования со спецификациями, местоположением и информацией о назначении.

Использование активов (Asset Utilization) Выявляйте недоиспользуемые ресурсы, которые могут быть перепрофилированы или выведены из эксплуатации для снижения затрат.

15 ИИ-АНАЛИТИКА

ИИ-аналитика RS-Discovery (R-Sight) предоставляет интеллектуальные данные об использовании вашей системы отчетности, оптимизирует производительность запросов и помогает улучшить общий пользовательский опыт с помощью автоматизированного анализа и рекомендаций.

Что предоставляет ИИ-аналитика

Анализ производительности запросов

- **Мониторинг времени ответа:** Отслеживание скорости обработки ИИ-запросов.
- **Отслеживание успешности:** Мониторинг доли успешных и неудачных запросов.
- **Популярные паттерны:** Идентификация наиболее часто используемых типов запросов.
- **Рекомендации по оптимизации:** Советы по повышению производительности запросов.

Анализ поведения пользователей

- **Частота запросов:** Самые востребованные типы отчетов и данных.
- **Удовлетворенность пользователей:** Анализ отзывов и рейтингов.
- **Паттерны использования:** Когда и как пользователи взаимодействуют с отчетами.
- **Внедрение функций:** Определение наиболее ценных ИИ-функций.

Оптимизация системы

- **Эффективность шаблонов промптов:** A/B-тестирование инструкций для ИИ.
- **Автооптимизация:** Непрерывное улучшение ответов ИИ.
- **Использование ресурсов:** Мониторинг затрат на ИИ-сервисы и их эффективности.
- **Анализ паттернов ошибок:** Выявление и устранение типичных проблем.

Доступные функции

1. Панели мониторинга аналитики запросов

Доступ к комплексной статистике использования ИИ:

- **Всего запросов:** Количество обработанных ИИ-запросов.
- **Доля успеха:** Процент успешных операций.
- **Среднее время ответа:** Метрики производительности.
- **Оценки пользователей:** Рейтинги и комментарии.

2. Система обратной связи

Сбор и анализ мнений пользователей:

- **Рейтинги:** Оценка ответов ИИ по 5-балльной шкале.
- **Полезно/Бесполезно:** Кнопки быстрой обратной связи.
- **Подробные комментарии:** Текстовые отзывы для внесения улучшений.
- **Выбор результатов:** Отслеживание того, какие именно данные пользователи считают наиболее полезными.

3. Анализ паттернов запросов

Понимание взаимодействия пользователей с ИИ:

- **Типовые структуры:** Часто используемые формулировки запросов.
- **Тренды:** Популярные темы запросов данных в динамике.
- **Предпочтения:** Паттерны использования на уровне отдельных сотрудников и команд.

4. Оптимизация шаблонов промптов

Повышение качества ответов ИИ:

- **A/B-тестирование:** Проверка различных вариаций промптов.
- **Метрики шаблонов:** Отслеживание эффективности конкретных инструкций.
- **Контроль версий:** Отслеживание изменений и улучшений в логике ИИ.

Использование ИИ-аналитики (Инструкция)

1. Доступ к панели мониторинга

Чтобы начать работу, перейдите в меню **Reports** → **AI Analytics**. Здесь вы найдете:

- **Общие метрики производительности:** Время обработки и объем данных.
- **Тренды запросов:** Самые популярные темы и категории отчетов.
- **Удовлетворенность:** Сводные оценки и отзывы пользователей системы.

2. Обратная связь (Feedback)

Ваше участие помогает ИИ обучаться. При просмотре отчетов:

- Используйте **звездный рейтинг** (1–5 звезд).
- Нажимайте кнопки **«Полезно»** или **«Бесполезно»**.
- Добавляйте **детальные комментарии**, если ИИ упустил важные данные или ошибся.
- Помечайте **наиболее полезные результаты** — это поможет системе в будущем предлагать их в первую очередь.

3. Мониторинг производительности

Отслеживайте состояние системы в динамике:

- **Response Times:** Время, за которое ИИ формирует ответ.
- **Success Rates:** Процент успешно выполненных запросов без ошибок.
- **Error Patterns:** Анализ типичных сбоев для их быстрого устранения.
- **Resource Usage:** Прозрачный контроль стоимости и эффективности ИИ-мощностей.

4. Работа с рекомендациями

Регулярно проверяйте раздел предложений по оптимизации:

- **Prompt Improvements:** ИИ подскажет, как переформулировать запрос для более точного результата.
- **Performance Optimizations:** Рекомендации по ускорению получения сложных отчетов.
- **Обучение:** Выявление пробелов в знаниях пользователей для проведения доп. тренингов.

Панели мониторинга аналитики

Ключевые метрики

- **Total AI Queries:** Общее количество обработанных запросов.
- **Success Rate:** Процент успешных ответов системы.
- **Average Response Time:** Скорость обработки запросов ИИ.
- **User Satisfaction:** Средний рейтинг на основе обратной связи.
- **Popular Query Types:** Самые востребованные типы отчетов.

Тренды производительности

- **Response Time Over Time:** Динамика улучшения производительности.
- **Query Volume:** Паттерны роста использования системы.
- **Error Rates:** Метрики надежности и стабильности.
- **User Engagement:** Тренды адаптации и вовлеченности пользователей.

Функции оптимизации

1. A/B-тестирование шаблонов промптов

Тестирование различных вариаций инструкций для ИИ:

- **Создание вариантов:** Проверка разных формулировок одного и того же запроса.
- **Сравнение производительности:** Анализ качества ответов для каждого варианта.
- **Автоматический выбор:** Система сама выбирает наиболее эффективный промпт.

2. Оптимизация запросов

Повышение технической эффективности:

- **Распознавание паттернов:** Выявление повторяющихся структур запросов.
- **Стратегии кэширования:** Сохранение результатов часто запрашиваемых данных.
- **Оптимизация индексов:** Повышение производительности БД.

3. Улучшение пользовательского опыта (UX)

- Повышение точности и качества ответов.
- Сокращение времени ожидания (задержек).
- Минимизация количества ошибок и сбоев.

- **Персонализация:** Адаптация ответов под стиль работы пользователя.

Лучшие практики

Предоставление обратной связи

- **Будьте конкретны:** Детальные комментарии помогают ИИ учиться быстрее.
- **Объективность:** Используйте всю шкалу рейтинга (1–5 звезд).
- **Фиксация успехов:** Отмечайте случаи, когда ИИ сработал идеально.

Оптимизация запросов пользователем

- **Четкость:** Формулируйте запросы максимально специфично.
- **Примеры:** Предоставляйте контекст для получения лучших результатов.
- **Итеративность:** Уточняйте запросы на основе полученных ранее ответов.

16 ФУНКЦИИ НА БАЗЕ ИИ

RS-Discovery (R-Sight) интегрирует искусственный интеллект во все уровни платформы для автоматизации сложных задач, выявления важных инсайтов и снижения нагрузки на ИТ-специалистов.

Обзор

Возможности ИИ в RS-Discovery (R-Sight) делятся на три категории:

1. **Автоматическое обнаружение и анализ** — фоновая работа ИИ во время сканирования и обработки событий.
2. **Интеллект по запросу** — аналитика ИИ, которую можно запросить для любого актива или услуги.
3. **Диалоговый доступ** — запросы на естественном языке через ИИ-чат-бота.

Анализатор бизнес-услуг (Business Service Analyzer)

Автоматическое обнаружение и построение карт бизнес-услуг на основе анализа взаимосвязей в инфраструктуре.

- **Что он делает:** Анализирует описание услуги, предлагает связанные компоненты инфраструктуры, классифицирует их по ролям (frontend, приложения, данные) и строит карты зависимостей с оценкой рисков.
- **Как использовать:** Перейдите в **Service Mapping** → **Business Service Analyzer**, опишите услугу (например, «E-commerce платформа»), нажмите **Enrich** (Обогатить) для получения рекомендаций и **Discover** для поиска инфраструктуры.
- **Ценность:** Сокращение времени документирования с недель до часов. Автоматическое выявление единых точек отказа (SPOF).

Аналитика КЕ

Получение ИИ-анализа для любой **Конфигурационной единицы (КЕ)**, чтобы понять ее роль, критичность и риски.

- **Функции:** Объясняет назначение актива, оценивает влияние на бизнес, выявляет возможности для оптимизации и отслеживает историю изменений.
- **Бизнес-эффект:** Быстрая адаптация новых сотрудников и улучшение контекста для **управления изменениями** (Change Management).

ИИ-обнаружение взаимосвязей (AI Relationship Discovery)

Автоматическое определение зависимостей между системами на основе паттернов сетевого трафика.

- **Функции:** Анализирует сетевые соединения, определяет типы связей (авторизация, передача данных и др.) и присваивает им показатели достоверности (confidence scores).
- **Бизнес-эффект:** Снижение трудозатрат на ручное построение связей на 70%+. Понимание того, «что сломается», если система отключится.

ИИ-чат-бот (AI Chatbot)

Задавайте вопросы об инфраструктуре на обычном языке.

- **Примеры:** *«Покажи все продуктовые серверы баз данных»*, *«Какие приложения зависят от MySQL?»*, *«Были ли инциденты с почтовыми серверами недавно?»*.
- **Ценность:** Доступ к данным CMDB без знания сложных поисковых синтаксисов.

ИИ-анализ событий (Event AI Analysis)

Автоматический анализ событий и инцидентов для поиска аномалий и потенциальных первопричин.

- **Функции:** Рассчитывает показатель аномальности (anomaly score), выдвигает гипотезы о **корневой причине (Root Cause)** и предлагает действия по устранению.
- **Бизнес-эффект:** Ускорение решения инцидентов (MTTR) за счет готовых подсказок.

Семантический поиск (Semantic Search)

Поиск активов по смысловому описанию, а не по точному совпадению ключевых слов.

- **Как использовать:** В разделе **CMDB** → **Search** выберите «Semantic Search» и введите запрос (например, «системы, похожие на наш MySQL-сервер»).
- **Ценность:** Поиск систем без знания их точных имен.

Автоматическая расстановка тегов (AI Auto-Tagging)

Автоматическая категоризация КЕ с помощью значимых тегов.

- **Категории:** Среда, Критичность, Комплаенс (Соответствие), Безопасность, Жизненный цикл, Владелец, Локация, Роль и др.
- **Бизнес-эффект:** Единообразие данных во всей ИТ-среде без ручного ввода.

Обогащение каталога ПО (Software Catalog Enrichment)

ИИ-помощник для наполнения каталога ПО метаданными о вендорах, лицензировании и классификации.

Генератор праздников (Holiday Generator)

Создание точных календарей праздников любой страны для планирования регламентных работ и корректного расчета **SLA**.

Сводная таблица функций

Функция	Триггер (Запуск)	Ключевое преимущество
Business Service Analyzer	Инициатива пользователя	Автоматическое построение карт инфраструктуры
CI Insights	По запросу	Быстрое понимание сути актива
Relationship Discovery	Автоматически (при сканировании)	Автоматизация построения зависимостей
AI Chatbot	Запрос пользователя	Доступ на естественном языке
Event AI Analysis	Автоматически (при событии)	Определение первопричины (Root Cause)
Semantic Search	Запрос пользователя	Поиск активов по описанию
AI Auto-Tagging	Автоматически (при создании КЕ)	Единая классификация данных
Software Enrichment	По запросу	Автоматизация метаданных ПО
Holiday Generator	По запросу	Автоматизация календарей для SLA

17 ИИ-МЕНЕДЖЕР ИЗМЕНЕНИЙ ДЛЯ R-SERVICE

Обзор

AI Change Manager — это мощный модуль интеграции между RS-Discovery (R-Sight) и R-Service, который обеспечивает автоматизированную оценку рисков для ИТ-запросов на изменение с помощью ИИ. При инициировании изменения в R-Service, ИИ RS-Discovery (R-Sight) анализирует влияние, зависимости и сопутствующие риски, предоставляя лицам, принимающим решения, исчерпывающую информацию для уверенного согласования изменений.

Ключевые возможности

Автоматизированная оценка рисков

- **Анализ в реальном времени:** Мгновенный анализ запросов на изменение при их создании или обновлении в R-Service.
- **Многомерная оценка рисков:** Анализ технических и бизнес-рисков, а также рисков зависимостей и исторических данных.
- **Уровни достоверности:** ИИ предоставляет показатели уверенности (confidence scores) для каждой оценки.

Комплексный анализ влияния (Impact Analysis)

- **Картирование зависимостей:** Идентификация всех систем и услуг, затронутых изменением.
- **Обнаружение критических систем:** Выделение воздействий на критически важную инфраструктуру.
- **Оценка времени простоя:** Реалистичный прогноз времени простоя (downtime) на основе сложности работ.
- **Оценка влияния на пользователей:** Количественное определение числа затронутых пользователей.

Интеллектуальные рекомендации

- **Действия перед внедрением:** Конкретные шаги, которые необходимо выполнить до начала работ.
- **Руководство в процессе:** Рекомендации в режиме реального времени во время реализации.
- **Валидация после внедрения:** Шаги проверки для подтверждения успешного завершения.
- **Тезисы для CAB:** Ключевые вопросы для обсуждения на заседаниях Комитета по изменениям.

Предварительные требования

Перед настройкой AI Change Manager убедитесь, что у вас есть:

Требования со стороны RS-Discovery (R-Sight):

- Активная развернутая система RS-Discovery (R-Sight) с наполненной базой CMDB.
- Работающие агенты обнаружения (Discovery), собирающие данные об инфраструктуре.
- Настроенные связи KE (сетевые соединения, программные зависимости).
- ИИ-обогащенные связи для получения более точной аналитики.

Требования со стороны R-Service:

- Активная учетная запись R-Service с правами администратора.
- Включенный API-доступ для вашего экземпляра R-Service.
- Возможность создания правил автоматизации и webhooks.

API-токен R-Service: Необходимо создать персональный токен (Personal Access Token) в R-Service со следующими областями видимости (scopes):

- **Правила автоматизации, Webhook** — Чтение, Создание, Обновление, Удаление.
- **KE, Организации, Лица, Задачи, Шаблоны задач, Команды, Расширения UI** — Чтение, Создание, Обновление.
- **Комментарий** — Чтение, Создание.
- **Продукт, Категория продукта** — Чтение, Создание, Обновление.

Принцип работы

1. Инициация изменения

Когда в R-Service создается запрос на изменение, включающий Конфигурационные единицы (КЕ):

- Правило автоматизации фиксирует новое изменение.
- Срабатывает webhook, отправляющий детали изменения в RS-Discovery (R-Sight).
- Передаваемые данные включают ID конфигурационных единиц, описание изменения и метаданные.

2. Процесс ИИ-анализа

ИИ-движок RS-Discovery (R-Sight) проводит комплексную проверку:

- **Идентификация КЕ:** поиск затронутых КЕ в базе CMDB.
- **Обнаружение зависимостей:** построение карты всех связанных систем и сервисов.
- **Расчет рисков:** оценка рисков по нескольким направлениям.
- **Оценка влияния:** определение последствий для бизнеса и технической части.
- **Формирование рекомендаций:** создание списка конкретных действий.

3. Доставка результатов

Результаты анализа автоматически возвращаются в R-Service:

- **Обновление пользовательских полей:** заполнение 21 специализированного поля данными оценки (включая 2 поля в формате JSON).
- **Заметка к задаче:** добавление краткого резюме в задачу для быстрого ознакомления.
- **Обновление в реальном времени:** результаты появляются в течение 10–30 секунд.

Интерпретация анализа ИИ

Поля оценки рисков (Risk Assessment Fields)

Поле	Описание	Примеры значений
AI Risk Level	Общая классификация уровня риска	Low (Низкий), Medium (Средний), High (Высокий), Critical (Критический)
AI Risk Score	Числовой показатель риска	0–100
AI Technical Risk	Показатель технической сложности изменения	0–100
AI Business Risk	Показатель влияния на бизнес-процессы	0–100
AI Dependency Risk	Оценка сложности взаимосвязей и зависимостей	0–100
AI Historical Risk	Риск, рассчитанный на основе прошлых аналогичных изменений	0–100
AI Risk Details	Полный отчет в формате JSON: оценка рисков, зависимости, исторический контекст, тезисы для CAB и стратегия тестирования	Формат JSON

Поля анализа влияния

Поле	Описание	Примеры значений
AI Affected Systems	Общее количество затронутых систем	5, 10, 25
AI Critical Impacts	Количество затронутых критически важных систем	2000, 1, 3
AI Affected Users	Оценочное количество затронутых пользователей	«100-500 пользователей»
AI Affected Services	Список затронутых ИТ-услуг/сервисов	«Email, Authentication, Database»
AI Business Impact	Качественная оценка влияния на бизнес	«Moderate — влияет на ключевые сервисы»

AI Impact Details	Полный отчет в формате JSON: резюме влияния, анализ времени простоя, рекомендации, инсайты, критерии успеха и точки мониторинга	Формат JSON

Поля прогнозирования простоя (Downtime Estimation)

ИИ рассчитывает временные рамки на основе сложности задачи и накопленной статистики аналогичных работ:

Поле	Описание	Примеры значений
AI Planned Duration	Ожидаемая длительность работ	«2 часа»
AI Risk Adjusted Time	Длительность с учетом буфера на риски	«2.5–3 часа»
AI Service Downtime	Фактическое время недоступности сервиса	«30 минут»
AI Recommended Window	Оптимальное окно для внедрения	«Суббота/Воскресенье, 02:00–05:00»

Поля рекомендаций (Recommendation Fields)

Эти поля содержат пошаговые инструкции для инженеров, минимизируя человеческий фактор:

- **AI Pre Change Rec:** Действия, которые необходимо выполнить **до начала** изменения (например, создание бэкапов, проверка связи).
- **AI During Change Rec:** Руководство и критические точки контроля непосредственно **в процессе** реализации.
- **AI Post Change Rec:** Проверки и шаги валидации **после завершения**, чтобы подтвердить, что всё работает корректно.

Метаданные анализа (Analysis Metadata)

Техническая информация о самой проверке ИИ:

- **AI Summary:** Краткое резюме анализа для руководства (Executive summary).
- **AI Insights:** Ключевые выводы и важные наблюдения, на которые стоит обратить внимание.
- **AI Confidence:** Уровень уверенности ИИ в точности данной оценки (0–100%).
- **AI Analysis Version:** Версия движка анализа, использованная для формирования отчета.

Лучшие практики

1. Качество данных в CMDB

- **Актуальность КЕ:** Следите за тем, чтобы база CMDB регулярно обновлялась данными из систем обнаружения (Discovery).
- **Связи и зависимости:** Сетевые соединения и зависимости программного обеспечения должны быть корректно выявлены.
- **Регулярное сканирование:** Проводите сканирование инфраструктуры на постоянной основе для поддержания свежести данных.

2. Описание изменений

- **Детализация:** Предоставляйте подробные описания изменений для более точного анализа ИИ.
- **Контекст:** Указывайте бизнес-причину и технический подход к реализации.
- **Список КЕ:** Включайте в запрос все системы, которые будут затронуты или модифицированы.

3. Проверка и валидация

- **Анализ инсайтов:** Изучайте оценку ИИ до начала заседаний Комитета по изменениям.
- **Корректировка баллов:** Изменяйте показатели риска вручную, если у вас есть дополнительный контекст.
- **Документирование отклонений:** Фиксируйте случаи, когда фактические результаты отличались от прогнозов ИИ.

4. Непрерывное улучшение

- **Мониторинг точности:** Отслеживайте, насколько предсказания совпадают с реальными исходами.

- **Обратная связь:** Сообщайте о неточных оценках для дообучения и улучшения алгоритмов.
- **Актуализация связей:** Своевременно обновляйте сопоставление (mapping) продуктов.

Безопасность

Защита данных

- **Шифрование:** Все данные передаются по протоколу HTTPS.
- **Аутентификация:** API-токены хранятся в зашифрованном виде.
- **Аудит:** Все изменения логируются для обеспечения соответствия требованиям (compliance).

Контроль доступа

- **Области видимости токенов:** Используйте принцип минимально необходимых привилегий для токенов.
- **Права пользователей:** Ограничьте круг лиц, имеющих доступ к настройке интеграции.
- **Безопасность webhook:** Валидация подписей webhook для предотвращения подмены данных.

18 ОБЗОР УПРАВЛЕНИЯ СООТВЕТСТВИЕМ НОРМАТИВНЫМ ТРЕБОВАНИЯМ (COMPLIANCE MANAGEMENT)

Модуль управления compliance в RS-Discovery (R-Sight) помогает создавать, внедрять и поддерживать комплексную программу соответствия требованиям. Независимо от того, с какими стандартами вы работаете, наш интегрированный подход связывает внешние регуляторные нормы с вашими внутренними политиками, мерами контроля и процедурами оценки.

Ваши возможности

Управление нормативно-правовой базой

- Доступ к предустановленным фреймворкам.
- Просмотр конкретных требований и цитат внутри каждого стандарта.
- Отслеживание обновлений и новых версий нормативных актов.

Разработка внутренних политик

- Создание корпоративных политик, согласованных с внешними нормами.
- Структурирование политик в виде конкретных и исполнимых положений.
- Поддержка версионности и рабочих процессов согласования.

Внедрение мер контроля

- Проектирование контрольных процедур для выполнения требований политики.
- Назначение владельцев контролей и определение зон ответственности.
- Категоризация: **Предотвращающие** (Preventive), **Выявляющие** (Detective), **Исправляющие** (Corrective).
- Настройка частоты проверок (ежедневно, еженедельно, ежемесячно, квартально, ежегодно).

Профили соответствия (Compliance Profiles)

- Группировка ИТ-активов (КЕ) с общими требованиями compliance.
- Создание динамических профилей, которые автоматически включают новые подходящие системы.
- Связывание профилей с контролями для автоматической генерации проверок.

Постоянный мониторинг и оценка

- Автоматическая генерация оценочных листов согласно заданному графику.
- Сбор и организация доказательной базы для аудита.
- Отслеживание статуса комплаенса по каждой системе и выявление пробелов (gaps).

Как это работает (Логическая цепочка)

Ваша программа compliance следует логике от внешних правил к ежедневным действиям: **Нормативная база → Ваши политики → Меры контроля → Профили соответствия → Автоматические проверки**

Ключевые преимущества

- **Прозрачность в реальном времени:** Панели мониторинга показывают общий статус compliance, просроченные проверки и пробелы в защите.
- **Автоматизация инфраструктуры:** Динамические профили сами находят новые серверы в CMDB и включают их в область аудита.
- **Готовность к аудиту:** Все действия логируются, а доказательства хранятся в привязке к проверкам.

Этапы запуска программы (Roadmap)

Этап	Что делаем	Срок	Результат
1. Фундамент	Выбор фреймворков и актуальных требований.	2–4 недели	Понимание регуляторного ландшафта.
2. Политики	Создание внутренних политик и их привязка к нормам.	4–6 недель	Полный свод корпоративных правил.
3. Контроли	Проектирование мер контроля и назначение владельцев.	3–4 недели	График автоматизированных проверок.
4. Профили	Настройка групп систем и правил их включения.	1–2 недели	Автоматическое масштабирование комплаенса.

5. Операции	Запуск проверок, сбор доказательств и отчетность.	Постоянно	Работающая программа мониторинга.

Лучшие практики для успеха

1. **Начинайте с малого:** Сначала внедрите требования самого критичного стандарта.
2. **Используйте динамические профили:** Это избавит вас от ручного добавления каждого нового сервера в списки проверок.
3. **Вовлекайте команду:** Владельцы контролей должны понимать, как собирать доказательства в системе.
4. **Следите за очередью задач:** Проверяйте панель мониторинга фоновых заданий, чтобы генерация тысяч проверок шла без задержек.

Безопасность и конфиденциальность

- **Изоляция данных:** Ваши данные комплаенса полностью отделены от данных других организаций.
- **Защита аудиторского следа:** Все записи о проверках защищены от изменений.
- **Безопасность улик:** Все загруженные документы шифруются и хранятся в защищенном хранилище.

19 УПРАВЛЕНИЕ ПОЛИТИКАМИ

Внутренние политики — это мост между внешними регуляторными требованиями и вашими ежедневными операциями. Они переводят сложные фреймворки в практические и выполнимые правила. Эффективное управление политиками гарантирует, что ваша программа комплаенса будет одновременно и полной, и применимой на практике.

Понятие политик и положений

Организационные политики

Это высокоуровневые документы, определяющие подход организации к конкретным областям:

- **Политика ИТ-безопасности:** защита информационных активов.
- **Политика конфиденциальности данных:** правила обработки персональных и чувствительных данных.
- **Политика управления изменениями:** контроль внесения правок в критические системы.

Положения политики

Это конкретные, измеримые и исполнимые требования внутри каждой политики:

- *«Все сотрудники должны использовать многофакторную аутентификацию (MFA) для доступа к системам».*
- *«Права доступа должны пересматриваться ежеквартально; лишние права подлежат удалению».*

Создание эффективных политик

Шаг 1: Определение основ

При создании новой политики в **Compliance** → **Policies** укажите:

- **Владелец (Owner):** лицо, ответственное за актуальность документа.
- **График пересмотра:** как часто политику нужно обновлять (раз в год или полгода).
- **Статус:** Черновик (Draft), Активна (Active) или Архивна (Archived).

Шаг 2: Написание положений

Хорошее положение политики должно быть:

- **Конкретным:** Вместо «Доступ должен быть защищен» пишите «Доступ должен быть защищен паролем не менее 12 символов».
- **Исполнимым:** Оно должно приводить к конкретному действию.
- **Адресным:** Закреплено за конкретными ролями (например, «Группа ИТ-операций должна...»).

Жизненный цикл политики

1. **Разработка:** Изучение норм, написание черновика, обсуждение с экспертами.
2. **Согласование:** Утверждение руководством и фиксация даты вступления в силу.
3. **Внедрение:** Обучение персонала, настройка рабочих процессов.
4. **Поддержка и обновление:** Регулярный пересмотр (минимум раз в год) или обновление при изменении законодательства.

Лучшие практики

- **Пишите просто:** Избегайте сложного юридического жаргона. Ваша цель — чтобы системный администратор понял, что именно ему нужно сделать.
- **Версионность:** Всегда сохраняйте историю изменений. Аудиторы обязательно попросят показать, какая версия политики действовала в определенный период времени.
- **Централизация:** Храните все политики в RS-Discovery (R-Sight), чтобы они были доступны для поиска и связаны с мерами контроля (Controls).

Типичные проблемы и их решения

- **Политика слишком расплывчата:** Если нельзя измерить выполнение пункта — перепишите его.
- **Политика невыполнима:** Если ИТ-отдел не может технически реализовать требование, политика превращается в «мертвый» документ. Обсуждайте черновики с инженерами.

- **Пропуски в покрытии:** Регулярно проверяйте отчет о покрытии фреймворков, чтобы убедиться, что для каждой важной цитаты закона у вас есть соответствующее правило.

20 МЕРЫ КОНТРОЛЯ И ОЦЕНКА

Контроли определяют, как вы внедряете политики на практике, а оценки подтверждают, что эти контроли эффективно работают во всей ИТ-инфраструктуре.

Понимание мер контроля

Что такое контроли комплаенса?

Это конкретные процедуры или действия, которые реализуют требования политики.

- **Положение политики:** «Права доступа пользователей должны пересматриваться ежеквартально».
- **Мера контроля:** «Процесс ежеквартального аудита доступа пользователей».
- **Действия:** Проверка списков пользователей, подтверждение бизнес-обоснования, удаление лишних прав.

Типы контролей

1. **Предотвращающие (Preventive):** Останавливают проблему до её появления (например, MFA, процесс утверждения изменений, шифрование).
2. **Выявляющие (Detective):** Обнаруживают проблему, когда она уже возникла (мониторинг логов, сканирование уязвимостей, сверка данных).
3. **Исправляющие (Corrective):** Устраняют проблему после её выявления (процедуры реагирования на инциденты, установка патчей, удаление прав).

Автоматизация графиков оценки (Scheduling)

RS-Discovery (R-Sight) может автоматически создавать задачи на проверку (assessments) с заданной частотой:

- **Частота:** Ежедневно, Еженедельно, Ежемесячно, Квартально, Ежегодно или По запросу (Ad-Hoc).
- **Автогенерация:** Система сама создаст задачу, когда подойдет срок.
- **Автоназначение:** Задача сразу упадет в список дел владельца контроля.
- **Кнопка «Generate Assessments Now»:** Позволяет мгновенно запустить проверку вне очереди (например, перед визитом аудитора).

Профили комплаенса (Compliance Profiles)

Профили — это группы ИТ-активов (КЕ), имеющих общие требования к комплаенсу. Они связывают ваши абстрактные правила с реальным «железом» и софтом.

Зачем нужны профили?

- **Масштабируемость:** Примените один контроль сразу к сотням систем.
- **Точность:** Проверка затронет только те системы, которые реально должны ей соответствовать.
- **Автоматизация:** Новые системы попадают под проверку сразу после обнаружения.

Типы участия в профиле:

Тип	Описание	Когда использовать
Динамический (Dynamic)	Авто-включение систем по правилам (например: Тип = Сервер БД + Среда = Prod).	Для крупной инфраструктуры и стандартных типов систем.
Ручной (Manual)	Вы сами выбираете конкретные КЕ из списка CMDB.	Для исключений, временных проверок или специфических малых групп.

Лучшие практики по работе с профилями

- **Имена:** Используйте понятные префиксы (например, PROD-DB, PCI-SCOPE).
- **Логика:** Группируйте системы по среде (Dev/Prod), функции или уровню риска.
- **Приоритет динамике:** Старайтесь использовать правила везде, где это возможно — это избавит вас от ручного обновления списков при покупке новых серверов.

Панель мониторинга compliance и отчетность

Панель мониторинга позволяет отслеживать состояние compliance («позу» compliance) в реальном времени.

Ключевые метрики

- **Общий показатель (Overall Compliance Score):** Процент успешно пройденных проверок.
- **Взвешенный показатель (Weighted Score):** Процент соответствия, скорректированный с учетом важности контролей.
- **Распределение статусов:** Наглядная диаграмма (Compliant, Non-Compliant и т.д.).
- **Просроченные проверки:** Критические задачи, требующие немедленного внимания.
- **Анализ трендов:** Улучшается или ухудшается ситуация с compliance с течением времени.

Взвешенный расчет (Weighted Compliance Scoring)

Система различает «важные» и «второстепенные» проверки:

1. **Простой расчет:** Все контроли равны. (8 из 10 пройдены = 80%).
2. **Взвешенный расчет:** Учитывает приоритет.
   - *Пример:* У вас 2 критических контроля (вес 10) и 8 средних (вес 5). Если вы провалили один критический, это ударит по итоговому баллу гораздо сильнее, чем провал среднего.
   - **Множители:** Соответствует = 100% веса, Частично = 50%, Не соответствует = 0%.

Отчетность для руководства (Executive Reporting)

Система позволяет выгружать отчеты, готовые к подаче аудиторам:

- **Отчет о статусе комплаенса:** Общий уровень по всем фреймворкам, зоны риска и тренды.
- **Отчет об активности:** Скорость выполнения задач сотрудниками, статистика просрочек.
- **Отчет для подготовки к аудиту:** Инвентаризация всех доказательств (Evidence), покрытие контролей тестами и анализ исключений.

21 УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Модуль управления уязвимостями RS-Discovery (R-Sight) обеспечивает полную видимость рисков безопасности в вашей ИТ-инфраструктуре. Вы можете проактивно устранять риски до того, как они станут реальными угрозами.

Зачем использовать этот модуль?

- **Снижение рисков:** Вы видите реальную картину — какие именно уязвимости не закрыты патчами.
- **Приоритезация:** ИИ помогает сфокусироваться на критических уязвимостях, которые уже активно используются злоумышленниками.
- **Экономия ресурсов:** Автоматическое сопоставление версий ПО сокращает количество ложных срабатываний на **89%**.
- **Соответствие требованиям (compliance):** Готовые отчеты для аудитов и полная история процесса устранения.

Как работает обнаружение

Процесс происходит автоматически во время сканирования Discovery:

1. **Сбор данных:** Сканеры собирают инвентарную информацию об установленном ПО и ОС.
2. **Идентификация:** ПО сопоставляется со стандартами.
3. **Сопоставление:** Система сверяет ваши версии ПО.
4. **Фильтрация патчей:** Проверяется, не закрыта ли данная уязвимость уже установленным Windows KB-патчем.
5. **Отчет:** В дашборде появляются только актуальные, неисправленные уязвимости.

Лучшие практики (Best Practices)

1. **Приоритет №1 — Эксплуатируемые угрозы:** В первую очередь устраняйте уязвимости с пометкой **"известный эксплойт"**.
2. **Критичность активов:** Уязвимость на сервере БД важнее, чем на тестовой рабочей станции.
3. **Жизненный цикл:** Используйте статусы (Open → In Progress → Resolved) и назначайте ответственных для каждой критической задачи.

22 ОБЗОР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Что это такое?

Модуль Security Management обеспечивает комплексное обнаружение угроз и мониторинг безопасности. Он объединяет автоматизированную интеграцию данных об угрозах (Threat Intelligence) с мониторингом в реальном времени для выявления подозрительной активности в вашей сети.

Ключевые преимущества

- **Проактивное обнаружение:** Выявление соединений с вредоносной инфраструктурой до того, как будет нанесен ущерб.
- **Threat Intelligence:** Использование ведущих отраслевых фидов (Threat Feeds) для защиты от новых угроз.
- **Сетевая видимость:** Полный контроль сетевых подключений и индикаторов компрометации (IOC).
- **Автоматические алерты:** Мгновенные уведомления об обнаружении угроз.

Основные возможности

1. Threat Intelligence (Разведка угроз)

RS-Discovery (R-Sight) интегрируется с несколькими источниками для поддержания актуальной базы вредоносных индикаторов:

Возможность	Описание
Детекция вредоносных IP	Идентификация соединений с известными C2-серверами (командными центрами).
Мониторинг процессов	Обнаружение подозрительных процессов, связанных с известными угрозами.
Детекция LOLBAS	Выявление злоупотребления легитимными системными инструментами (Living Off The Land).

2. Управление политиками ПО (Software Policy)

Определение и применение политик безопасности для программного обеспечения:

- **Черные списки (Blacklisting):** Блокировка или оповещение о запрещенном ПО.
- **Белые списки (Whitelisting):** Определение разрешенного ПО для compliance.
- **Автоматические действия:** Настройка реакции системы — от уведомления до перемещения в карантин.

3. Сканирование сетевых IOC

Мониторинг сетевых соединений на основе известных Индикаторов Компрометации (Indicators of Compromise):

- **32,000+ вредоносных IP:** Огромная база данных известных «плохих парней».
- **Детекция C2:** Идентификация паттернов связи с командными серверами злоумышленников.
- **Анализ портов:** Обнаружение подозрительных паттернов использования сетевых портов.

Как это работает

Когда система обнаруживает угрозу:

1. **Создается событие безопасности (Security Event)** с полным контекстом.
2. **Связывается с активом (KE):** Вы сразу видите, какой сервер или компьютер под угрозой.
3. **Назначается критичность:** На основе типа угрозы система определяет приоритет.
4. **Уведомление:** Отправляется сообщение в Slack, Email или другую систему.

Интеграция с CMDB

Поскольку модуль неразрывно связан с CMDB, вы получаете:

- **Контекст актива:** Кто владелец системы и какую бизнес-функцию она выполняет.
- **Анализ радиуса поражения (Blast Radius):** Понимание того, какие системы связаны с зараженной и могут пострадать следующими.

Часто задаваемые вопросы (FAQ)

В: Как часто обновляются данные об угрозах?

О: Ежедневно. Это гарантирует защиту от самых свежих угроз.

В: Заменяет ли это антивирус?

О: Нет. Система обнаруживает сетевые соединения и подозрительные процессы. Это отличное дополнение к антивирусу, но не его замена.

В: Могу ли я добавить свои индикаторы?

О: Да, вы можете создавать собственные политики ПО с вашими индикаторами через интерфейс.

23 ПОЛИТИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Что это такое?

Политики ПО позволяют определять правила безопасности для программ, процессов и сетевых соединений во всей организации. Эти правила определяют, какое ПО разрешено (**Whitelist**), запрещено (**Blacklist**) или требует мониторинга.

Зачем они нужны?

- **Соблюдение стандартов:** Блокировка вредоносов и несанкционированного софта.
- **Требования комплаенса:** Документирование списка одобренного ПО для аудитов.
- **Снижение рисков:** Выявление опасных приложений до того, как произойдет инцидент.
- **Автоматизация:** Настройка мгновенной реакции (от уведомления до карантина системы).

Настройка политики

Уровни серьезности (Severity)

Уровень	Описание	Время реакции
Critical	Активное вредоносное ПО, шифровальщики, APT.	Немедленно
High	Известные угрозы, инструменты управления (C2).	В течение 1 часа
Medium	Потенциально нежелательные программы (PUP).	В течение 24 часов
Low	Нарушение корпоративных правил, софт без лицензии.	Плановый обзор

Возможные действия (Actions)

1. **Alert (Оповещение):** Создать событие безопасности и отправить уведомление.
2. **Monitor (Мониторинг):** Записать факт обнаружения в лог без отправки алертов.
3. **Block Install (Блокировка):** Предотвратить новые установки этого ПО.
4. **Quarantine (Карантин):** Изолировать зараженную систему от сети.
5. **Uninstall (Удаление):** Пометить ПО для автоматического или ручного удаления.

Создание политики: два пути

1. Из каталога ПО (Software Catalog)

Самый простой способ. Вы ищете уже известную программе сущность в глобальном каталоге RS-Discovery (R-Sight) и просто назначаете ей статус (например, «Blacklist» для программы µTorrent).

2. Ручной ввод (Manual Entry)

Используется для специфических угроз или самописного вредоносного ПО. Вы сами вводите название, вендора и описание угрозы.

Детализация и обнаружение

Внутри каждой политики можно настроить **паттерны обнаружения**:

- **Name Patterns:** Регулярные выражения (Regex) для имен файлов.
- **Process Names:** Имена исполняемых файлов процессов.
- **File Paths:** Пути установки (например, запуск из папки Temp).

Исключения (Exclusions)

Чтобы избежать ложных срабатываний (False Positives), вы можете добавить исключения:

- Доверенные вендоры.
- Специфические пути, где работа данного ПО легитимна.

Работа с нарушениями (Violations)

Когда политика срабатывает, вы можете мгновенно увидеть:

- На каком хосте обнаружено нарушение.

- Точное время и детали процесса.
- Текущий статус (устранено или активно).

Лучшие практики

1. **Принцип «Черного и Белого»:** Используйте Whitelist для критических серверов (где разрешен только минимум ПО) и Blacklist для офисных ПК.
2. **Регулярный пересмотр:** Проверяйте актуальность политик раз в квартал.
3. **Связь с комплаенсом:** Привязывайте политики к фреймворкам (например, требование PCI-DSS о запрете неавторизованного ПО).

Понимание данных об угрозах

Индикаторы компрометации (IOC)

Это «цифровые улики», указывающие на подозрительную активность:

Тип IOC	Пример	Метод обнаружения
IP-адрес	185.243.112.80	Мониторинг сетевых соединений.
Домен	malware-c2.com	Анализ DNS-запросов.
Хеш файла	SHA256: ...	Проверка целостности файлов.
Процесс	suspicious.exe	Мониторинг запущенных программ.

Уровни достоверности (Confidence Levels)

- **High (Высокий):** Верифицированная угроза. **Требуется немедленная реакция.**
- **Medium (Средний):** Вероятная угроза. Требуется расследование.
- **Low (Низкий):** Подозрительная активность. Рекомендуется мониторинг.

Лучшие практики

1. **Верификация:** Если система обнаружила соединение с вредоносным IP, сначала проверьте, какой процесс его инициировал (например, системный svchost.exe или подозрительный файл).
2. **Контекст пользователя:** Посмотрите, что делал пользователь в момент обнаружения — это поможет отличить реальную атаку от случайного захода на зараженный сайт.
3. **Борьба с ложными срабатываниями:** Иногда легитимные облачные сервисы могут использовать IP, которые раньше были у хакеров. Если вы уверены в безопасности — добавьте исключение (Exclusion).
4. **Приоритизация:** В первую очередь расследуйте события со статусом **Критические**.

24 СКАНИРОВАНИЕ СЕТЕВЫХ IOC

Что такое сканирование сетевых IOC?

Network IOC Scanning — это процесс сопоставления всех сетевых соединений ваших устройств с глобальной базой известных вредоносных адресов. Если ваше устройство (сервер, ПК или ноутбук) инициирует связь с командным сервером (C2) хакеров или сайтом распространения вирусов, система мгновенно фиксирует это и создает алерт.

Почему это важно?

- **Раннее обнаружение:** Вы узнаете о взломе еще на этапе «разведки» или связи с C2, до того как произойдет кража данных (exfiltration).
- **Автоматизация:** Система делает за вас работу целого отдела аналитиков, которым не нужно вручную просматривать терабайты сетевых логов.
- **Огромный охват:** Мониторинг ведется по базе из **32,000+** активных вредоносных IP-адресов.
- **Контекст:** Вы получаете не просто «подозрительный IP», а название семейства малвари (например, *Cobalt Strike* или *AsyncRAT*), которое стоит за этим адресом.

Как это работает: Процесс сканирования

Процесс сканирования интегрирован в общую систему Discovery и Threat Intelligence:

Оптимизированное обнаружение

RS-Discovery (R-Sight) использует метод **обратного поиска** для обеспечения максимальной производительности:

1. Система извлекает все известные вредоносные IP из базы разведки угроз.
2. Сетевые соединения проверяются пакетами (батчами).
3. Полное сканирование по **32,000+** индикаторам занимает примерно **5 секунд**.

Этот подход значительно быстрее, чем проверка каждого отдельного соединения по одному.

Запуск сканирования

Автоматическое сканирование

Проверка сетевых IOC запускается автоматически как часть регулярного процесса Discovery:

- Агент собирает данные о сетевых подключениях.
- Данные проходят через конвейер сканирования.
- При обнаружении совпадений с «черным списком» мгновенно создаются события безопасности.

Сканирование по запросу (On-Demand)

Чтобы запустить проверку вручную:

1. Перейдите в **Security** → **Network Scanning**.
2. Выберите нужную организацию (Tenant).
3. Нажмите **Run IOC Scan**.

Понимание результатов

Чистая сеть (Clean Scan)

Если вредоносных соединений не обнаружено, вы увидите сообщение об этом. В сводке будет указано количество проанализированных соединений (например, 105,000) и время работы сканера.

Обнаружение угрозы (Detection Found)

При обнаружении связи с вредоносным ресурсом система выводит предупреждение.

Вам будет предоставлена детальная информация:

- **Семейство малвари:** (например, Cobalt Strike).
- **Удаленный IP и порт:** (куда шел трафик).
- **Хост:** (какой компьютер заражен).
- **Процесс:** (какая программа инициировала связь, например svchost.exe).

Реагирование на обнаружение

Немедленные действия

1. **Верификация:** Подтвердите, что соединение действительно активно на хосте.
2. **Анализ процесса:** Является ли процесс легитимным или это неизвестный файл?
3. **Изоляция:** Если обнаружена связь с C2-сервером (управление), немедленно изолируйте хост от сети.

Интеграция с CMDB и анализ последствий

Поскольку обнаружение привязано к объектам в CMDB, вы можете мгновенно оценить «радиус поражения» (Blast Radius):

- **Контекст актива:** Какую бизнес-функцию выполняет этот сервер?
- **Зависимости:** Какие сервисы зависят от этого хоста и могут быть скомпрометированы?
- **Данные:** К каким конфиденциальным данным имеет доступ этот компьютер?

Часто задаваемые вопросы (FAQ)

В: В чем разница между этим сканером и моим файрволом?

О: Файрволы блокируют соединения на входе/выходе. IOC-сканирование выявляет соединения, которые **уже произошли**. Это позволяет найти системы, которые уже взломаны, даже если файрвол пропустил трафик.

В: Могу ли я экспортировать результаты?

О: Да, результаты можно выгрузить в форматах CSV или PDF для отчетности и передачи в отдел расследований.

В: Как часто нужно запускать сканирование?

О: Рекомендуется использовать автоматический режим при каждом Discovery. Внеплановые проверки стоит проводить после любых подозрений на инцидент.

Что такое события безопасности (Security Events)?

Security Events — это алерты, создаваемые автоматически при обнаружении потенциальных угроз. Это «пульт управления» вашими инцидентами, который позволяет переходить от простого уведомления к реальному расследованию.

Почему это важно?

- **Централизация:** Все угрозы в одном месте, независимо от того, как они были найдены.
- **Приоритизация:** Вы сразу видите, что нужно исправлять немедленно (**Critical**), а что может подождать.
- **Контекст:** Система связывает событие с конкретным сервером, пользователем и политикой.
- **Аудит:** Полная история того, кто, когда и как отреагировал на угрозу.

Жизненный цикл события

Процесс обработки события в RS-Discovery (R-Sight) выглядит следующим образом:

1. **Open (Открыто):** Событие только что создано. Требуется первичный анализ.
2. **Acknowledged (Принято в работу):** Аналитик начал расследование. Другие участники команды видят, что инцидентом занимаются.
3. **Resolved (Решено):** Проблема устранена (вирус удален, патч поставлен).
4. **Closed (Закрыто):** Финальная стадия. Действий не требуется (например, подтвержден ложный сигнал).

Детализация событий (Event Details)

Основная информация

Каждое событие содержит паспортные данные угрозы:

- **Заголовок (Title):** Краткая суть (например, «Обнаружен C2-трафик Cobalt Strike»).
- **Серьезность (Severity):** Цветовой индикатор приоритета.
- **Статус (Status):** Текущий этап обработки.
- **Временная метка (Timestamp):** Точное время фиксации угрозы.

Контекст обнаружения

Система предоставляет данные для немедленного анализа:

- **Affected Host:** Имя пострадавшего сервера или ПК.
- **CI Link:** Прямая ссылка на объект в CMDB для оценки его бизнес-роли.
- **Policy:** Ссылка на конкретное правило безопасности, которое сработало.
- **Malware Family:** Название семейства малвари (если идентифицировано).

Сетевые подробности (для Network IOC)

- **Remote IP/Port:** Адрес и порт назначения вредоносного трафика.
- **Process Name:** Имя локального процесса, инициировавшего соединение.
- **Connection Count:** Количество зафиксированных попыток связи.

Фильтрация событий (Event Filtering)

Для эффективной работы используйте систему фильтров:

- **По серьезности:** Сосредоточьтесь только на **Critical** и **Major** в начале смены.
- **По статусу:** Скройте решенные события, чтобы видеть только «горящие» задачи (**Open**).
- **По времени:** Просмотрите события за последние 24 часа или неделю для выявления трендов.
- **По хосту:** Проверьте все алерты по конкретному критичному серверу, чтобы увидеть полную цепочку атаки.

Реакция на критические события (Critical Event Response)

Для событий уровня **Critical** (шифровальщики, активные C2-сессии) в RS-Discovery (R-Sight) предусмотрен строгий регламент SLA:

- **Уведомление:** Мгновенная отправка команде ИБ.
- **Принятие (Acknowledge):** В течение **15 минут**.
- **Первичная оценка:** В течение **30 минут**.
- **Решение об изоляции:** В течение **1 часа**.
- **Полное расследование:** В течение **4 часов**.
- **Устранение или эскалация:** В течение **8 часов**.

Отчетность и аудит (Reporting)

Сводка событий (Event Summary)

Система позволяет генерировать отчеты для руководства, включающие:

- Общее количество событий по уровням серьезности.
- Распределение по типам обнаружения (IOC, LOLBAS и т.д.).
- **Метрики эффективности:** Среднее время подтверждения (MTTA) и среднее время решения (MTTR).
- Статистика по конкретным хостам или бизнес-подразделениям.

Документация для комплаенса

Для внешних аудиторов можно экспортировать:

- Полную историю каждого события.
- Все заметки, сделанные в ходе расследования.
- Подробный таймлайн действий сотрудников.

Лучшие практики (Best Practices)

Эффективный триаж (сортировка)

- **Приоритет:** Всегда начинайте с критических событий.
- **Корреляция:** Проверьте, нет ли связанных событий на том же хосте или с тем же типом малвари.
- **Документируйте всё:** Даже если вы выяснили, что угрозы нет («отрицательный результат»), запишите, как вы пришли к этому выводу.

Качество расследования

- **Контекст из CMDB:** Всегда смотрите, какой именно сервер атакован и с какими активами он связан.
- **Сетевые связи:** Проверьте возможность «горизонтального перемещения» (Lateral Movement) малвари на соседние системы.
- **Улики:** Тщательно фиксируйте все найденные доказательства.

Часто задаваемые вопросы (FAQ)

В: Что делать, если событий слишком много?

О: Проверьте политики на наличие паттернов ложных срабатываний. Добавьте исключения для проверенных безопасных процессов и скорректируйте уровни серьезности.

В: Могут ли события закрываться автоматически?

О: **Нет.** События безопасности требуют обязательного участия человека. Это гарантирует, что каждый инцидент был изучен и задокументирован.

В: Как долго хранятся события?

О: История хранится в соответствии с политикой вашей организации, обычно от 1 до 7 лет.

В: Можно ли заново открыть решенное событие?

О: Да, если появилась новая информация. Просто добавьте заметку с объяснением причины повторного открытия.

25 ИНТЕГРАЦИИ

На сегодняшний день R-Service — это основная интеграция:

- **Синхронизация КЕ:** Двусторонний обмен данными о конфигурационных единицах.
- **Service Management (Управление услугами):** Автоматическое создание инцидентов и запросов на изменения.
- **Webhooks:** Уведомления о событиях в реальном времени.
- **UI Extensions (Расширения UI):** Возможность просматривать данные RS-Discovery (R-Sight) прямо в интерфейсе R-Service.

Методы интеграции и API

RS-Discovery (R-Sight) спроектирован как открытая платформа, что позволяет подключать к ней практически любую систему.

Webhooks

- Настраиваемые конечные точки (endpoints).
- Безопасная аутентификация через Bearer-токены.
- Механизмы повтора при сбоях доставки.

REST API

- Полный доступ ко всем ресурсам платформы.
- Возможность массового импорта и экспорта данных.
- **GraphQL:** Для еще более гибких и быстрых запросов к связанным данным.

Лучшие практики при настройке

Принцип	Рекомендация
Маппинг данных	Четко определите, какое поле в RS-Discovery (R-Sight) соответствует полю во внешней системе. Установите приоритет (какая система считается «источником истины»).
Производительность	Используйте массовые операции (bulk) и настраивайте лимиты (rate limiting), чтобы не перегружать API.
Обработка ошибок	Настройте логирование и алерты на случай сбоев синхронизации.
Безопасность	Всегда используйте API-ключи или OAuth 2.0; избегайте хранения паролей в открытом виде.

Ключевые возможности

1. Синхронизация КЕ (Конфигурационных единиц)

RS-Discovery (R-Sight) передает в R-Service полные данные об оборудовании (серверы, рабочие станции), инвентаре ПО и, что самое важное, **связях и зависимостях** между ними.

2. AI Change Manager

Это интеллектуальный помощник для управления изменениями. Когда в R-Service создается запрос на изменение (Change Request), ИИ RS-Discovery (R-Sight) автоматически:

- **Оценивает риски:** Вычисляет баллы технического и бизнес-риска (0–100).
- **Анализирует влияние:** Показывает, какие критические системы могут пострадать.
- **Дает рекомендации:** Формирует список действий до, во время и после внесения изменений.

Стратегии маппинга (сопоставления)

RS-Discovery (R-Sight) предлагает два гибких подхода к тому, как ваши устройства превратятся в «Продукты» внутри R-Service:

Стратегия	Описание	Кому подходит
Single Product Mode	Все устройства одного типа (например, все серверы) привязываются к одному продукту в R-Service.	Для быстрой настройки и однородных сред.
Brand/Model Mapping	Каждая комбинация производителя и модели (например, Dell R740) привязывается к своему уникальному продукту.	Для детального учета, отслеживания гарантий и

		жизненного цикла конкретных моделей.

AI Change Manager: Как это работает в жизни

1. **Создание запроса:** Техник создает запрос на изменение в R-Service.
2. **Триггер:** Webhook отправляет данные в RS-Discovery (R-Sight).
3. **Анализ:** ИИ изучает зависимости КЕ в CMDB, историю инцидентов и критичность услуги.
4. **Результат:** В задачу R-Service записываются баллы риска и текстовые рекомендации для комитета по изменениям (CAB).

Лучшие практики

- **Начните с малого:** Сначала синхронизируйте один тип КЕ (например, Серверы) в небольшом объеме (5–10 штук).
- **Проверьте UI-расширения:** Убедитесь, что в R-Service созданы поля для приема данных от ИИ, иначе результаты анализа не будут видны.
- **Соблюдайте иерархию:** Сначала синхронизируйте оборудование, а затем связи между ними, чтобы граф зависимостей в R-Service построился корректно.