R-Vision

Security Governance, Risk & Compliance Platform **(SGRC)**

www.rvision.ru

Линейка продуктов R-Vision

IRP

Автоматизация мониторинга и реагирования на инциденты

SENSE

Продвинутая аналитика для выявления угроз и аномалий

TIP

Платформа анализа информации об угрозах

TDP

Автоматизированное обнаружение атак с помощью имитации ИТ-инфраструктуры

КИИ

Автоматизация категорирования объектов КИИ и процесса обеспечения соответствия 187-ФЗ

SGRC

Управление ИБ, оценка рисков и комплаенс-контроль

CERS

Построение центра реагирования на угрозы и уязвимости

R-Vision SGRC

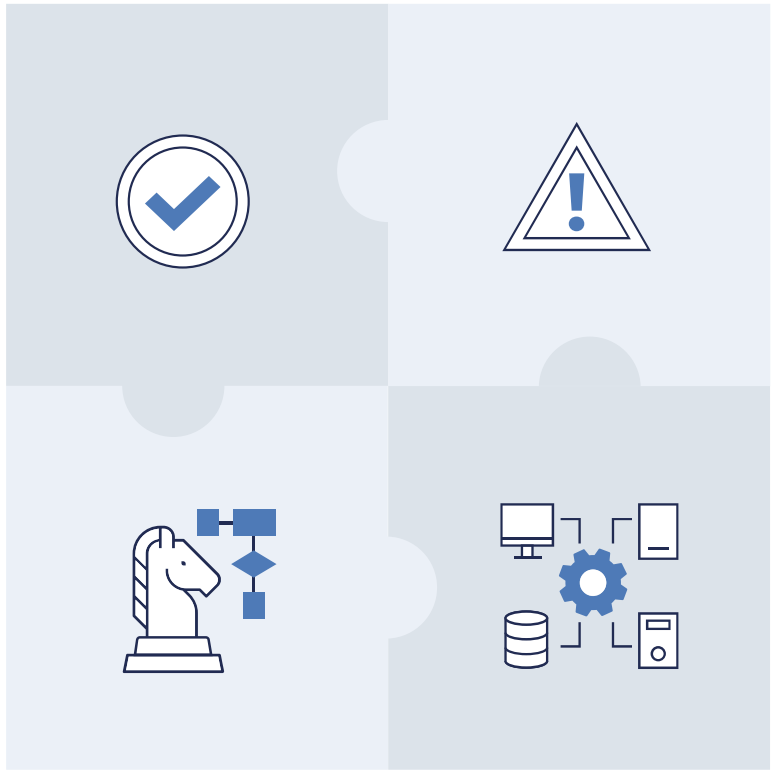
Эффективная система управления информационной безопасностью за счет автоматизации процессов:

Compliance

Управление аудитами и контроль соответствия требованиям

Risk management

Анализ и управление рисками информационной безопасности



Governance

Управление информационной безопасностью

Asset management

Управление активами и контроль ИТ-инфраструктуры

Центр управления ИБ

Инфраструктура

СЗИ

Сканеры уязвимостей

Пользователи

Регуляторы

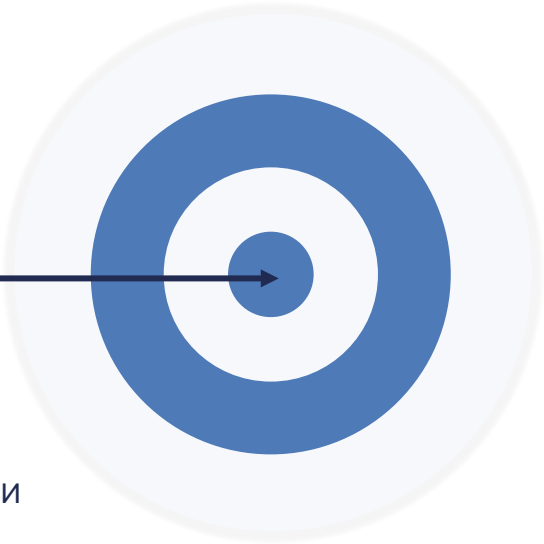
R-Vision SGRC

Asset Management	Vulnerability Management	Risk Management	Compliance Control	Security Management
Информация, бизнес-процесс Информационные системы Физические активы (пользователи, ПО, оборудование, орг.структура)	Агрегированный список уязвимостей Анализ, приоритизация Контроль статуса устранения	Схемы оценки рисков (ISO, NIST, OCTAVE, пользовательская) Анализ рисков, прогнозирование, план обработки Оценка бюджета и эффективности	ISO 27001, NIST, PCI DSS и другие проверки Заполнение форм аудита Список замечаний по аудиту	Чек-листы, планы, база документации Управление задачами, контроль исполнения, совместная работа Визуализация данных, отчетность

Стратегическое управление ИБ

Единая база
политик, процедур,
регламентов
и инструкций по ИБ

Стратегическое планирование,
контроль за задачами
и дедлайнами



Определение
стратегии ИБ,
соответствующей
бизнес-целям Компании

Риск-ориентированный подход
к управлению
безопасностью

Визуализация
проблем безопасности
и эффективности
проводимых
мероприятий

Контроль ИТ-активов

Мастер-ресурс по всем активам
с агрегированными данными
из множества источников
и взаимосвязями

3-х уровневая схема активов:
информация и бизнес-процессы,
информационные системы,
инфраструктура

Выявление критичных
активов и процессов

Управление жизненным циклом актива

Визуализация информации по активам:
геокарта, L2-схема сети, планы помещений, взаимосвязи,
«индикация проблем», ресурсно-сервисная модель

Управление уязвимостями

- Единая база уязвимостей, агрегированных из разных источников
- Приоритизация, отсев нерелевантных уязвимостей
- Централизованная постановка задач ИТ-персоналу
- Учет устранения, контроль SLA
- Оперативное обновление статусов уязвимостей
- Полная отчетность для служб ИТ и ИБ

Управление рисками

Автоматизированная оценка риска

Настраиваемая схема оценки рисков, готовые методологии (ISO, OCTAVE, NIST, R-Vision, etc.)

Анализ рисков

Оценка вероятности реализации угроз, косвенные риски, прогноз возможного ущерба

Обработка рисков

Формирование плана мероприятий по обработке рисков, сопоставление с бюджетом на ИБ, контроль реализации

Оценка эффективности

Оценка бюджета, приоритизация мер в зависимости от их стоимости и эффективности

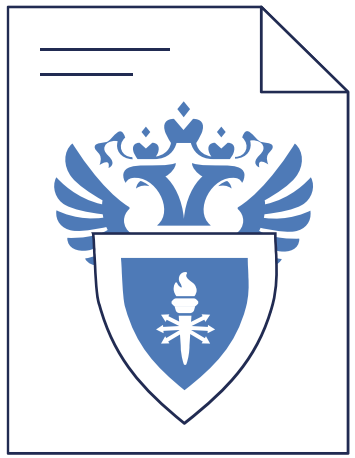
Контроль уровня риска

Постоянный мониторинг изменений во времени

Визуализация и отчетность

Настраиваемые дашборды и аналитика для принятия решений, формирование отчетов

Моделирование угроз по ФСТЭК



- **Встроенный Банк данных угроз безопасности** информации ФСТЭК
- **Автоматическое выявление актуальных угроз** в соответствии с «Методикой определения угроз безопасности информации в информационных системах»
- **Формирование перечня возможных угроз** на основании БДУ ФСТЭК
- Генерация документа «Модель угроз безопасности информации» **в автоматическом режиме**

Аудиты и контроль соответствия

Проверки соответствия

- ISO 27001
- PCI DSS
- SWIFT CSP
- Собственные корпоративные стандарты

Автоматизация жизненного цикла аудита

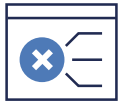
- Планирование
- Автоматическое назначение ответственных, контроль сроков
- Дашборды и аналитика в режиме реального времени

Контрольные проверки

- Учет пересекающихся требований различных ИБ-стандартов
- Контроль реализации защитных мер

Конструктор аудитов

- Использование пользовательских методик с гибкими настройками
- Простые и сводные аудиты

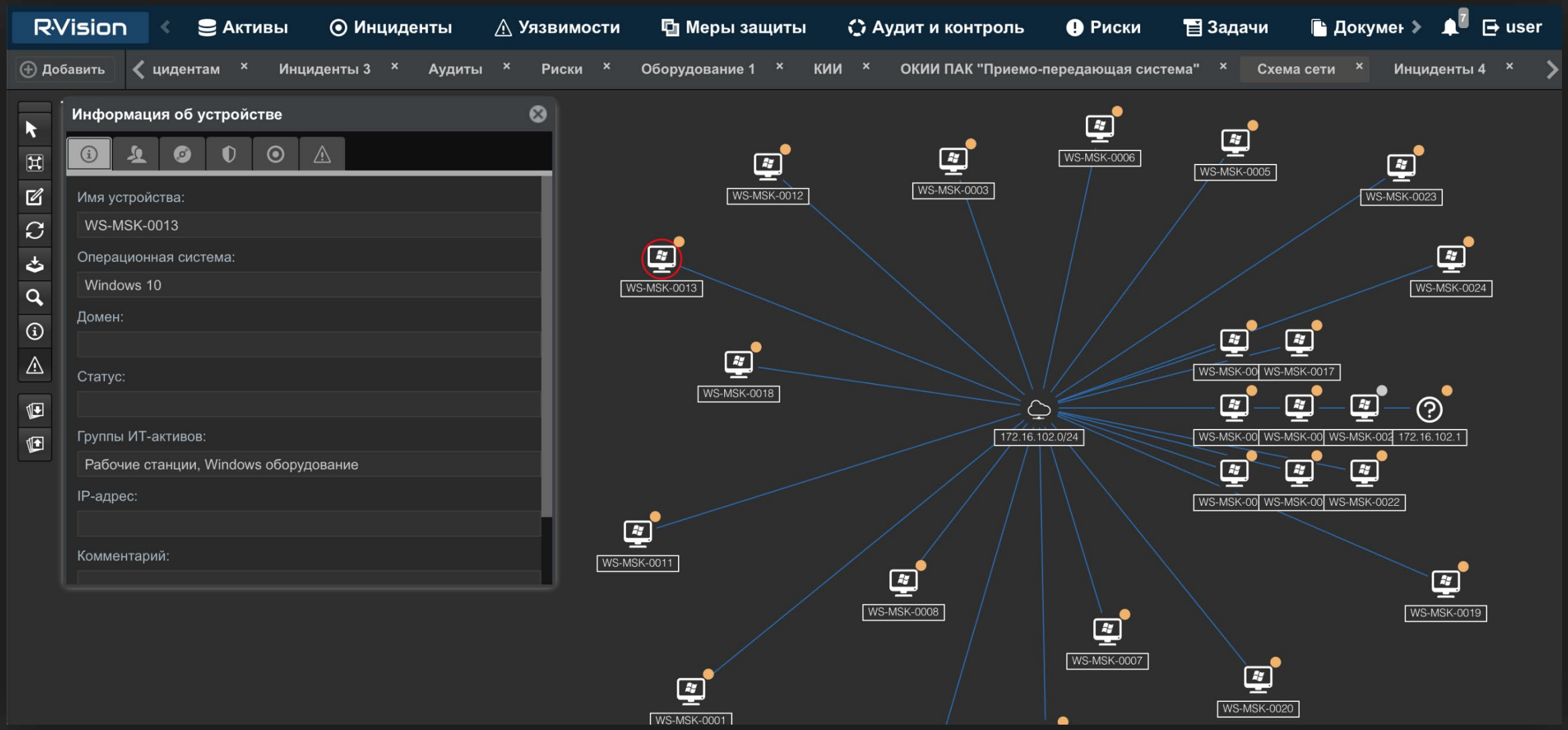


Выявление замечаний по аудиту

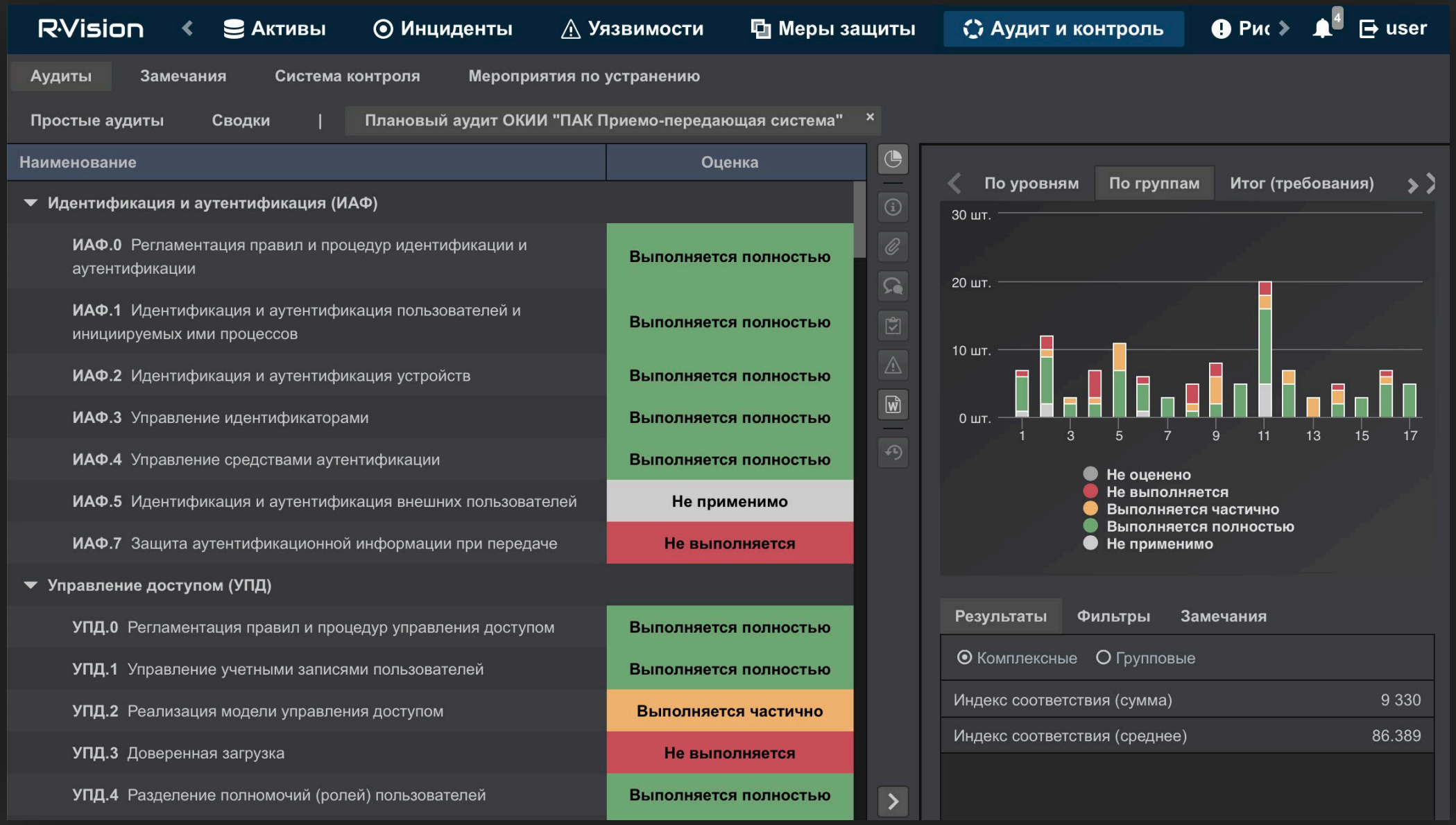
- Автоматическое формирование списка замечаний
- Формирование плана мероприятий по устранению замечаний

Централизованная система контроля

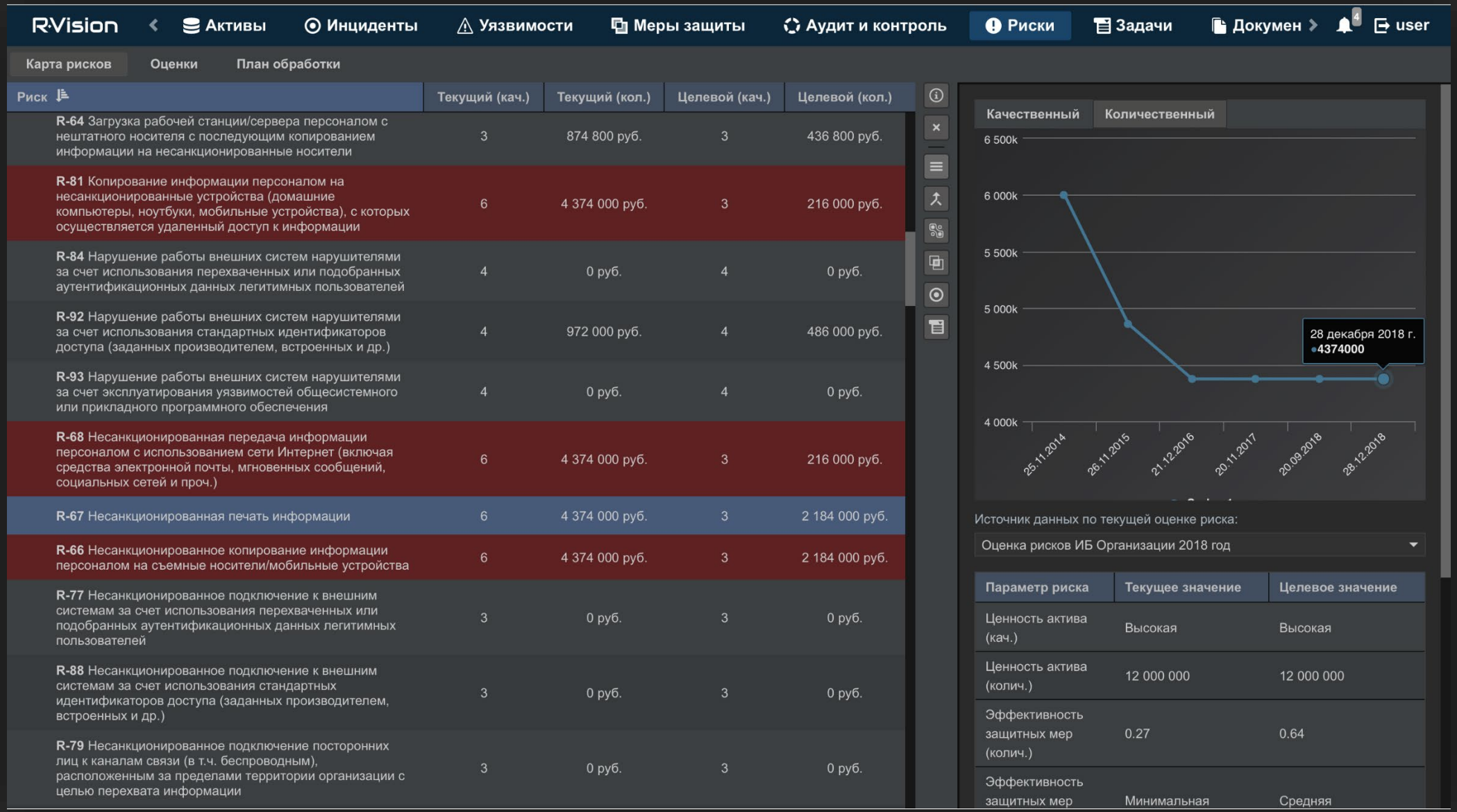
- Прозрачный процесс оценки соответствия требованиям внутри всей организации
- Единая база нормативной документации



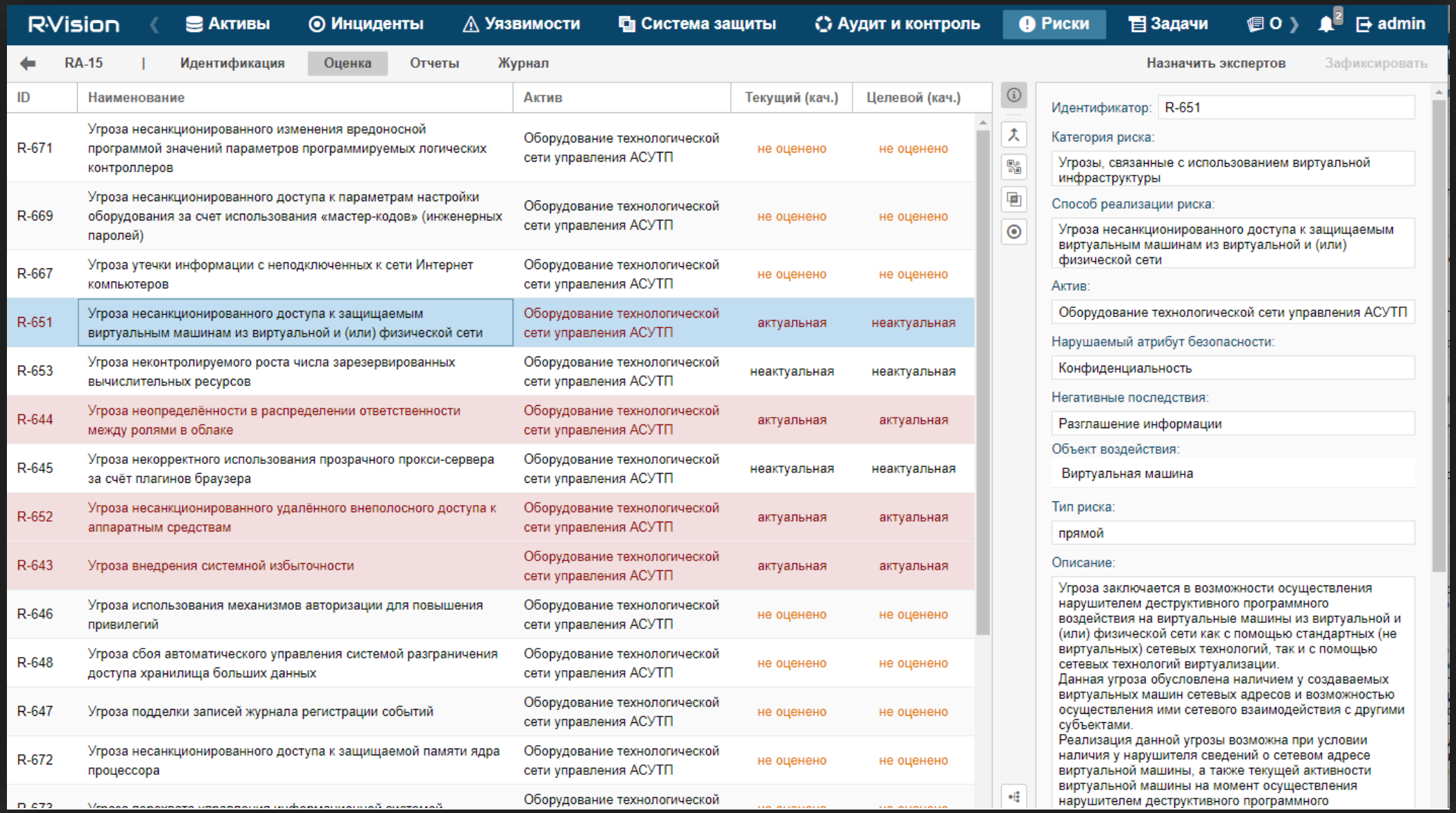
Управление активами


R-Vision
Активы
Инциденты
Уязвимости
Меры защиты
Аудит и контроль
Рис
4
user
Аудиты
Замечания
Система контроля
Мероприятия по устранению
Простые аудиты
Сводки
Плановый аудит ОКИИ "ПАК Приемо-передающая система"
Наименование
Оценка
Идентификация и аутентификация (ИАФ)
ИАФ.0 Регламентация правил и процедур идентификации и аутентификации
Выполняется полностью
ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов
Выполняется полностью
ИАФ.2 Идентификация и аутентификация устройств
Выполняется полностью
ИАФ.3 Управление идентификаторами
Выполняется полностью
ИАФ.4 Управление средствами аутентификации
Выполняется полностью
ИАФ.5 Идентификация и аутентификация внешних пользователей
Не применимо
ИАФ.7 Защита аутентификационной информации при передаче
Не выполняется
Управление доступом (УПД)
УПД.0 Регламентация правил и процедур управления доступом
Выполняется полностью
УПД.1 Управление учетными записями пользователей
Выполняется полностью
УПД.2 Реализация модели управления доступом
Выполняется частично
УПД.3 Доверенная загрузка
Не выполняется
УПД.4 Разделение полномочий (ролей) пользователей
Выполняется полностью
По уровням
По группам
Итог (требования)
30 шт.
20 шт.
10 шт.
0 шт.
1
3
5
7
9
11
13
15
17
Не оценено
Не выполняется
Выполняется частично
Выполняется полностью
Не применимо
Результаты
Фильтры
Замечания
Комплексные
Групповые
Индекс соответствия (сумма)
9 330
Индекс соответствия (среднее)
86.389

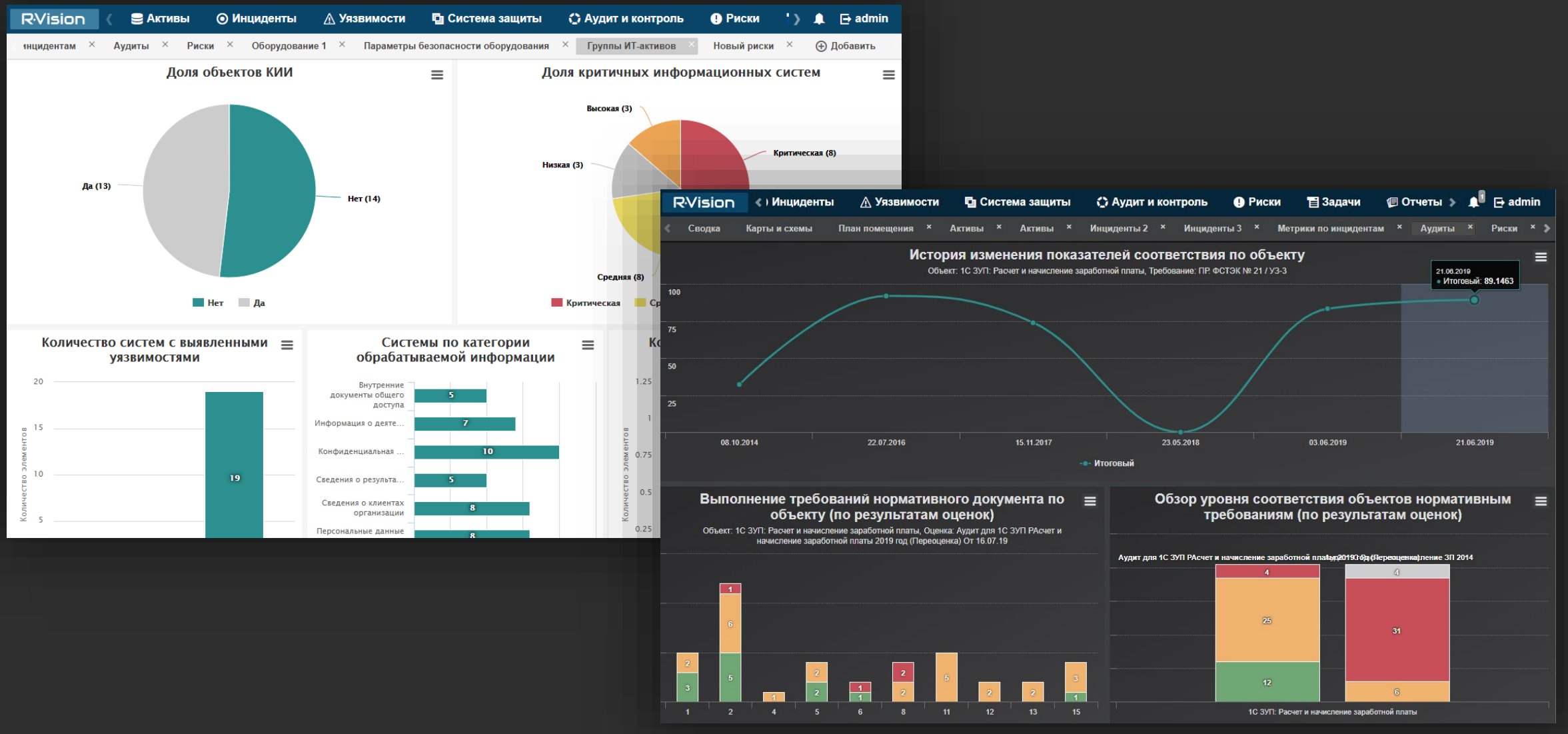
Аудиты


R-Vision
Активы
Инциденты
Уязвимости
Меры защиты
Аудит и контроль
Риски
Задачи
Докумен
user
Карта рисков
Оценки
План обработки
Риск
Текущий (кач.)
Текущий (кол.)
Целевой (кач.)
Целевой (кол.)
R-64 Загрузка рабочей станции/сервера персоналом с нештатного носителя с последующим копированием информации на несанкционированные носители 3 874 800 руб. 3 436 800 руб.
R-81 Копирование информации персоналом на несанкционированные устройства (домашние компьютеры, ноутбуки, мобильные устройства), с которых осуществляется удаленный доступ к информации 6 4 374 000 руб. 3 216 000 руб.
R-84 Нарушение работы внешних систем нарушителями за счет использования перехваченных или подобранных аутентификационных данных легитимных пользователей 4 0 руб. 4 0 руб.
R-92 Нарушение работы внешних систем нарушителями за счет использования стандартных идентификаторов доступа (заданных производителем, встроенных и др.) 4 972 000 руб. 4 486 000 руб.
R-93 Нарушение работы внешних систем нарушителями за счет эксплуатирования уязвимостей общесистемного или прикладного программного обеспечения 4 0 руб. 4 0 руб.
R-68 Несанкционированная передача информации персоналом с использованием сети Интернет (включая средства электронной почты, мгновенных сообщений, социальных сетей и проч.) 6 4 374 000 руб. 3 216 000 руб.
R-67 Несанкционированная печать информации 6 4 374 000 руб. 3 2 184 000 руб.
R-66 Несанкционированное копирование информации персоналом на съемные носители/мобильные устройства 6 4 374 000 руб. 3 2 184 000 руб.
R-77 Несанкционированное подключение к внешним системам за счет использования перехваченных или подобранных аутентификационных данных легитимных пользователей 3 0 руб. 3 0 руб.
R-88 Несанкционированное подключение к внешним системам за счет использования стандартных идентификаторов доступа (заданных производителем, встроенных и др.) 3 0 руб. 3 0 руб.
R-79 Несанкционированное подключение посторонних лиц к каналам связи (в т.ч. беспроводным), расположенным за пределами территории организации с целью перехвата информации 3 0 руб. 3 0 руб.
Качественный
Количественный
6 500k
6 000k
5 500k
5 000k
4 500k
4 000k
28 декабря 2018 г.
4374000
25.11.2014
26.11.2015
21.12.2016
20.11.2017
20.09.2018
28.12.2018
Источник данных по текущей оценке риска:
Оценка рисков ИБ Организации 2018 год
Параметр риска
Текущее значение
Целевое значение
Ценность актива (кач.) Высокая Высокая
Ценность актива (колич.) 12 000 000 12 000 000
Эффективность защитных мер (колич.) 0.27 0.64
Эффективность защитных мер Минимальная Средняя

Риски



Моделирование угроз по ФСТЭК



Визуализация

Интеграции

Сканеры защищенности	AV & DLP-системы	CMDB / ITSM системы	Другие системы
MaxPatrol	Kaspersky Security Center	Micro Focus UCMDB	MS Active Directory
RedCheck	Infowatch TrafficMonitor/ DeviceMonitor	Micro Focus SM	MS Exchange / Lotus Domino / Communigate
Tenable Nessus/SC	Triton AP-DATA	MS SCCM	VMWare vCenter
Rapid7 Nexpose	Symantec Endpoint Protection	Naumen CMDB	Прямые коннекторы к БД MS SQL, Postgre SQL, Oracle
Qualys	McAfee ePolicy Orchestrator	OmniTracker CMDB/SM	Skybox
OpenVAS	ESET	iTOP	Собственные документированные REST API методы
		JIRA	Zabbix

Результат

Своевременное выявление угроз,

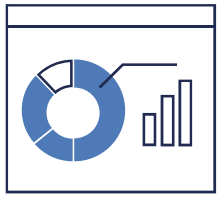
потенциальных нарушителей, оценка ИБ-рисков, прогнозирование

Подбор оптимальных мер защиты,

исходя из оценки ИБ-рисков, текущего состояния системы защиты и доступного бюджета

Обеспечение соответствия требованиям

регуляторов с минимальными издержками



Контроль состояния и эффективности

системы ИБ, защищенности инфраструктуры, отчетность для принятия решений

Кейсы использования R-Vision SGRC

Централизованное управление ИБ, автоматизация контроля соответствия и формирования отчетов по требованиям ЦБ РФ для ряда крупнейших банков из Топ-20

Автоматизация аудитов с помощью мобильного АРМ для одной из крупнейших промышленных компаний с территориально-распределенной инфраструктурой на 100 тыс. хостов

Автоматизация управления активами для государственной организации, инфраструктура которой насчитывает 400 тыс. хостов и более 100 систем

Сертификация по ISO/IEC 27001 и контроль соответствия для крупной телекоммуникационной компании

R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru

Подписывайтесь на наш дайджест ИБ: **rvision.ru/blog**