



Автоматизация полного цикла соответствия 187-ФЗ с помощью R-Vision SGRC



Всеслав Соленик
Директор Центра экспертизы R-Vision

КТО МЫ?

R-Vision – разработчик систем кибербезопасности.

С 2011 года мы создаем решения и сервисы, которые помогают бизнесу и государственным организациям по всему миру обеспечивать надежное управление ИБ.

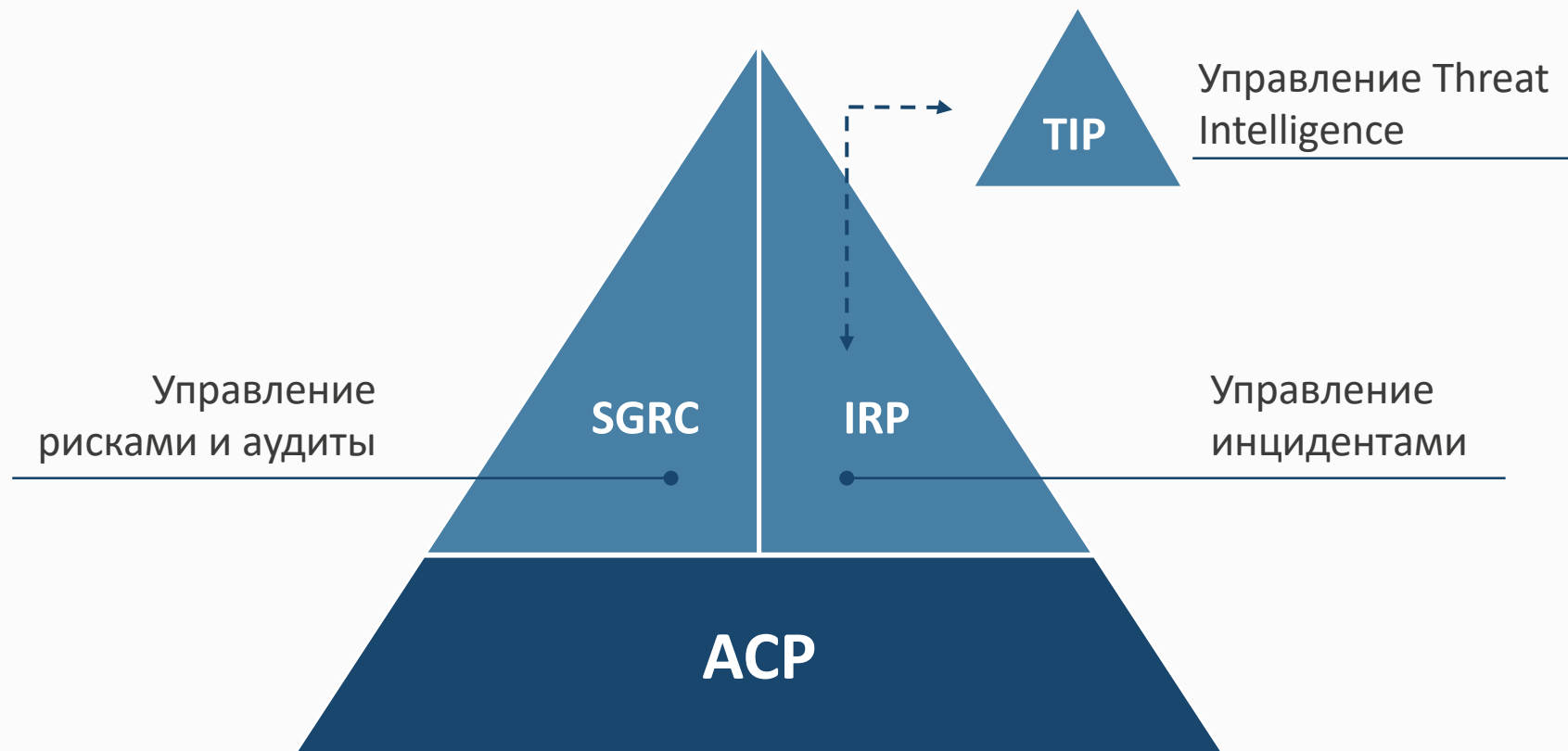


Мы верим в то, что для успешного развития любого бизнеса и государства важна безопасность, а кибератаки – одна из главных угроз безопасности в современном мире. Поэтому разрабатываем передовые решения и сервисы, которые дают нашим клиентам необходимый технологический уровень, чтобы уверенно противостоять угрозам и действовать быстрее, чем киберпреступники.

Технологии R-Vision используются

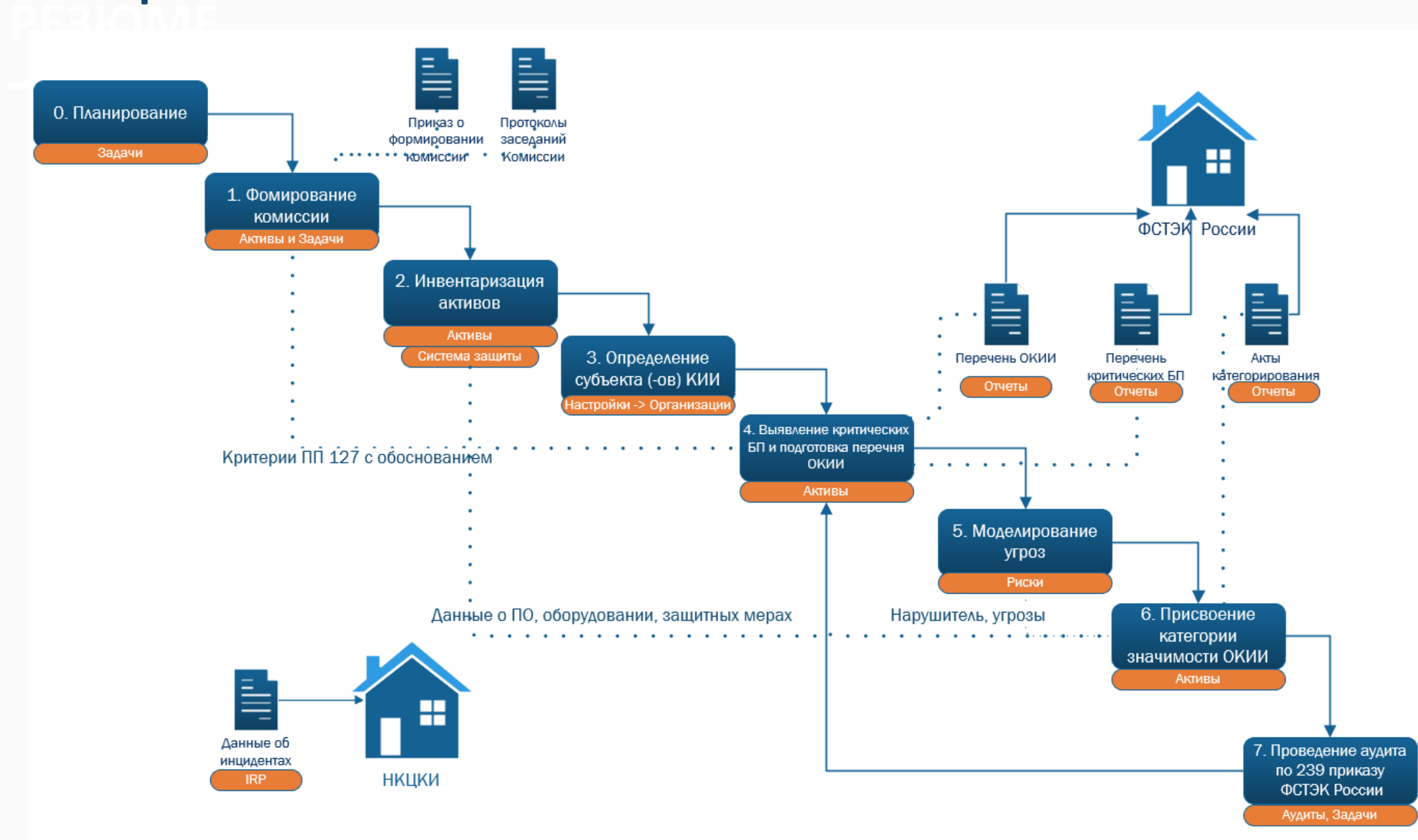
- в банках
- государственных структурах
- нефтегазовой отрасли
- энергетике
- металлургии
- промышленности
- и компаниях других отраслей

ПРОДУКТЫ R-VISION



Управление активами. База, вокруг которой строятся продукты R-Vision IRP и R-Vision SGRC

ПРОЦЕСС КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КИИ В R-VISION



ВОЗМОЖНОСТИ R-VISION SGRC

ПО ОБЕСПЕЧЕНИЮ СООТВЕТСТВИЯ 187-ФЗ

- **Учет субъектов КИИ**, сводная информация по субъектам КИИ, перечень критических процессов и объектов КИИ
- **Учет объектов КИИ**, автоматический сбор данных о составе компонентов объекта КИИ, инвентаризация оборудования и ПО
- **Обеспечение** работы комиссии по категорированию
- **Автоматическое выставление** категории значимости объекта КИИ
- **Моделирование угроз** для объектов КИИ по требованиям ФСТЭК
- **Автоматический учет** примененных и необходимых мер защиты в отношении объекта КИИ
- **Формирование пакета документов** в автоматическом режиме
- **Проведение аудита** на соответствие требованиям Приказа ФСТЭК №239

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ КАТЕГОРИРОВАНИЯ

- Обеспечение работы комиссии по категорированию
- Назначение и распределение задач между участниками
- Контроль сроков исполнения

КИИ ФСТЭК Компоненты

Критические процессы, обеспечиваемые объектом: ➔

Категория	Всего
Административно-хозяйственное обеспе...	1 ➔
Обслуживание клиентов / населения	1 ➔
Администрирование и ИТ	1 ➔
Взаимодействие с акционерами	1 ➔
Закупки	1 ➔

Архитектура объекта:

Иная архитектура

Категория значимости:

Категория 3

Дата категорирования:

07.08.2019

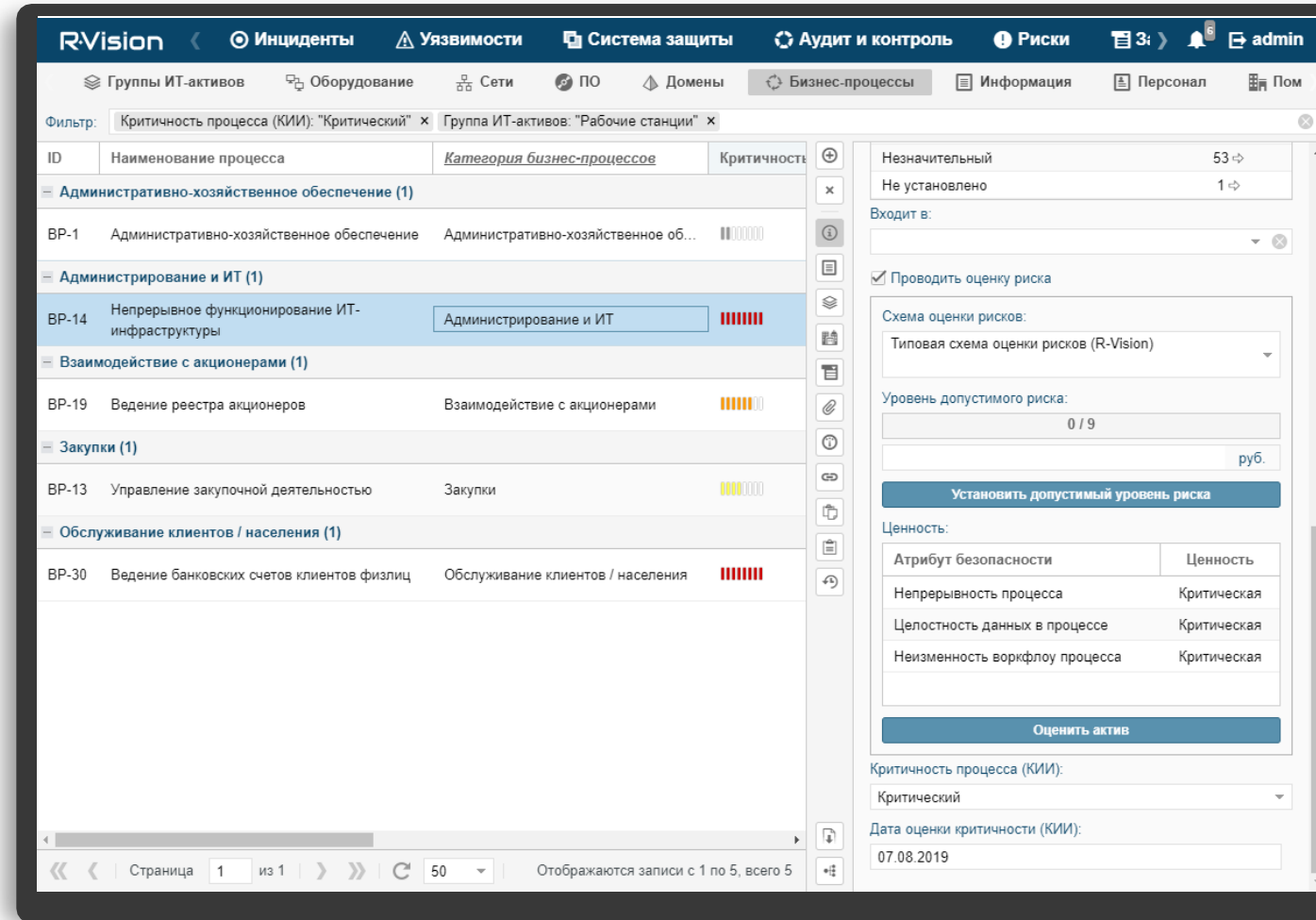
Дополнительные сведения

- ▼ Взаимодействия с сетями электросвязи
- ▼ Сведения о лице, эксплуатирующем объект КИИ
- ▼ Сведения о программных и программно-аппаратных средствах, используемых на объекте
- ▼ Сведения об угрозах безопасности информации и категориях нарушителей
- ▼ Возможные последствия в случае возникновения инцидентов
- ▲ Применяемые меры безопасности
 - ☒ Использовать данные из раздела Система защиты

Тип	Количество
Организационные меры	0
Технические меры	0

УЧЕТ СУБЪЕКТОВ КИИ

- Сводная информация по субъектам КИИ
- Учет выполняемых процессов и состава информации
- Выявление критических процессов
- Контроль даты последней оценки критичности
- Автоматическая отметка систем, связанных с критическими процессами, в качестве объектов КИИ
- Сводная информация по объектам КИИ



УЧЕТ ОБЪЕКТОВ КИИ

- Ведение карточек объектов КИИ
- Автоматический сбор данных о составе компонентов объекта КИИ
- Инвентаризация оборудования и ПО
- Заполнение сведений по объекту КИИ на основе данных инвентаризации
- Контроль даты последнего проведения категорирования в отношении объекта КИИ

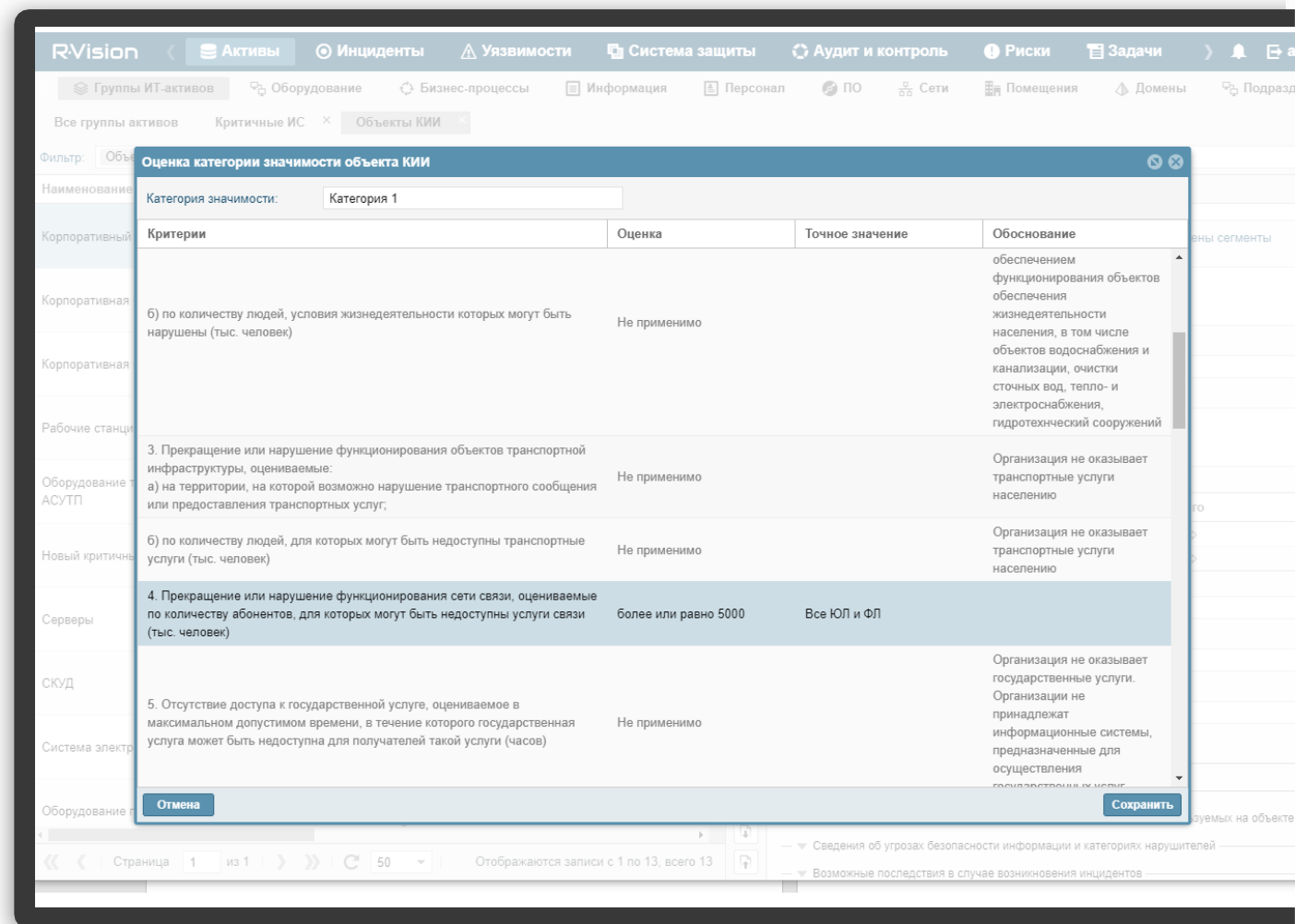
The screenshot displays a web application interface for managing Critical Information Infrastructure (КИИ) objects. The interface is divided into several sections:

- Navigation Bar:** Includes tabs for "КИИ" (selected), "ФСТЭК", and "Компоненты".
- Left Sidebar:** Contains a vertical menu with icons for various functions such as adding, deleting, and viewing objects.
- Main Form:** Titled "Основная информация", it contains the following fields:
 - Тип объекта:** A dropdown menu with the selected value "Автоматизированная система управления".
 - Адреса размещения объекта:** A text input field containing "г. Москва, ул. Моховая, 20".
 - КПП подразделений (филиалов, представительств), в которых размещены сегменты объекта:** A text input field containing "Для распределенных объектов".
 - Сфера деятельности, в которой функционирует объект:** A dropdown menu with the selected value "Топливо-энергетический комплекс".
 - Назначение объекта:** A text input field containing "Технологическая сеть управления АСУТП".
 - Критические процессы, обеспечиваемые объектом:** A table with two columns: "Категория" and "Всего".

Категория	Всего
Обеспечение безопасности (физической...	1 ↗
 - Архитектура объекта:** A dropdown menu with the selected value "Клиент-серверная система".
 - Категория значимости:** A text input field containing "Не присвоена".
 - Дата категорирования:** A text input field containing "19.08.2019".

АВТОМАТИЗАЦИЯ ПРОЦЕДУРЫ КАТЕГОРИРОВАНИЯ

- Автоматическое определение критичности процессов
- Автоматическое выявление неприменимых показателей критериев значимости
- Авто-заполнение обоснования неприменимости показателей критериев значимости
- Автоматический расчет категории значимости
- Учет организационных и технических мер защиты, применяемых в отношении объекта КИИ



МОДЕЛИРОВАНИЕ УГРОЗ ДЛЯ ОБЪЕКТОВ КИИ

- Формирование модели нарушителя
- Определение перечня актуальных угроз на основе БДУ ФСТЭК
- Автоматическое заполнение этих данных в карточке объекта КИИ

The screenshot displays the R-Vision software interface. The top navigation bar includes tabs for 'Инциденты', 'Уязвимости', 'Система защиты', 'Аудит и контроль', and 'Риски'. The 'Риски' tab is active, showing a table of threats and a detailed risk assessment panel on the right.

ID	Наименование	Актив	Текущий (кач.)	Целевой (кач.)
R-910	Угроза пропуска проверки целостности программного обеспечения	Государственная информационная система 1	актуальная	актуальная
R-898	Угроза форматирования носителей информации	Государственная информационная система 1	неактуальная	неактуальная
R-897	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Государственная информационная система 1	актуальная	актуальная
R-900	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Государственная информационная система 1	актуальная	актуальная
R-892	Угроза неопределённости в распределении ответственности между ролями в облаке	Государственная информационная система 1	неактуальная	неактуальная
R-865	Угроза потери и утечки данных, обрабатываемых в облаке	Государственная информационная система 1	неактуальная	неактуальная
R-907	Угроза подмены субъекта сетевого доступа	Государственная информационная система 1	актуальная	актуальная
R-889	Угроза физического устаревания аппаратных компонентов	Государственная информационная система 1	неактуальная	неактуальная
R-884	Угроза преодоления физической защиты	Государственная информационная система 1	актуальная	актуальная
R-887	Угроза несанкционированной модификации защищаемой информации	Государственная информационная система 1	неактуальная	неактуальная
	Угроза неподтверждённого ввода данных	Государственная		

Назначить экспертов Зафиксировать

Негативные последствия: Несанкционированное изменение информации

Объект воздействия:
Носители информации

Тип риска:
прямой

Описание:
Угроза заключается в возможности утраты хранящейся на формируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренности или случайного выполнения процедуры форматирования носителя информации. Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: время, прошедшее после форматирования; тип носителя информации; тип файловой системы носителя; интенсивность взаимодействия с носителем после форматирования и др.

Параметры риска:

Параметр ...	Текущее зна...	Целевое зна...
Уровень защищенности	Средний	Средний
Потенциал источника	Низкий	Низкий
Степень ущерба	Низкий*	Низкий*
Вероятность реализации	Средняя	Средняя
Актуальность угрозы	неактуальная	неактуальная

ФОРМИРОВАНИЕ ПОЛНОГО ПАКЕТА ДОКУМЕНТОВ

- ✓ Акт категорирования
- ✓ Сведения о присвоении объекту КИИ одной из категорий значимости в соответствии с формой, утвержденной Приказом ФСТЭК от 22.12.2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
- ✓ Перечень объектов критической информационной инфраструктуры
- ✓ Перечень критических процессов
- ✓ Акт проверки объекта КИИ, на основании проведенного в отношении объекта КИИ аудита по Приказу ФСТЭК №239

Стр. 1

УТВЕРЖДАЮ

(подпись, инициалы, фамилия)

« » 20 г.

АКТ
категорирования объекта критической информационной инфраструктуры
Оборудование технологической сети управления АСУТП

На основании приказа от « » 20 г. № комиссия в составе:

председатель комиссии: _____
(долг., должность, фамилия, инициалы)

члены комиссии: _____
(долг., должность, фамилия, инициалы)

_____ (долг., должность, фамилия, инициалы)

_____ (долг., должность, фамилия, инициалы)

в соответствии с требованиями Федерального закона от 26.06.2017 №187, постановления Правительства РФ от 08.02.2018 №127 проведена категорирование объекта критической информационной инфраструктуры Оборудование технологической сети управления АСУТП.

Стр. 2

В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее - КИИ), представленные в Приложении 1.
2. Сведения об угрозах безопасности информации объекта КИИ, представленные в Приложении 2.
3. Реализованные на объекте КИИ меры по обеспечению безопасности, представленные в Приложении 3.
4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости, представленный в Приложении 4.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018 №127 объекту «Оборудование технологической сети управления АСУТП» присвоена категория значимости – Категория 1.

Состав необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, утвержденными приказом ФСТЭК от 25.12.2017 №239, представлен в Приложении 5.

Председатель комиссии: _____
(ФИО, подпись)

Члены комиссии: _____
(ФИО, подпись)

_____ (ФИО, подпись)

_____ (ФИО, подпись)

ДОКУМЕНТЫ ПО ОБЪЕКТАМ КИИ

Выгрузка документов
в различных разрезах:

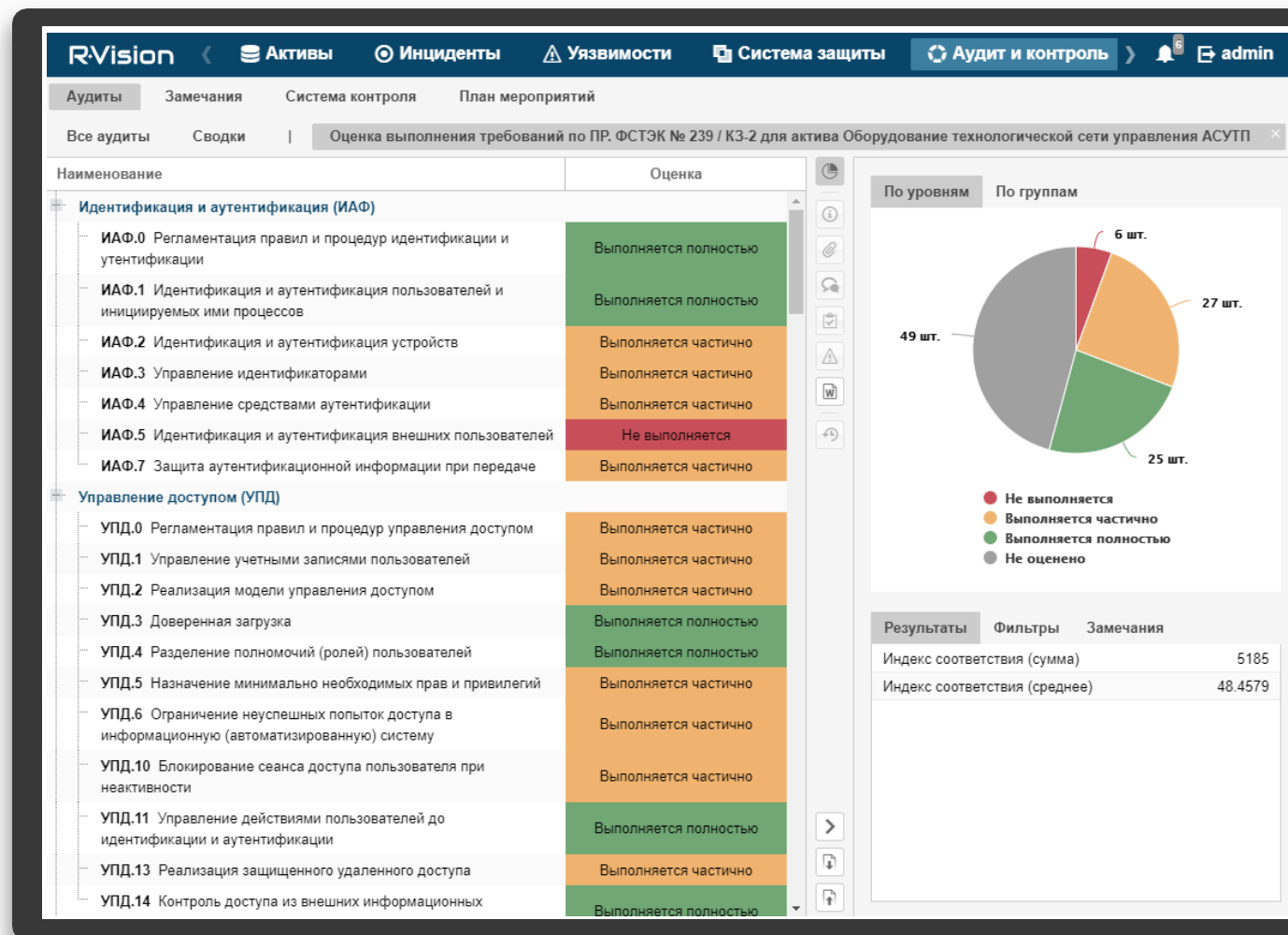
- Для одного объекта КИИ
- Для нескольких объектов КИИ
- По подразделению
- По субъекту КИИ в целом

Учет документов
по объектам КИИ:

- Декларация объекта, паспорт объекта и другие
- Контроль доступа к документам
- Контроль срока действия

АУДИТ ПО ПРИКАЗУ ФСТЭК №239

- **Автоматический расчет** состава мер защиты в зависимости от категории значимости объектов КИИ, согласно требованиям Приказа ФСТЭК №239
- **Сводный аудит** применяемых организационных и технических мер защиты по всем объектам КИИ
- **Фиксация** выявленных замечаний
- **Формирование плана мероприятий** по устранению замечаний, назначение задач, указание сроков
- **Подготовка Акта проверки** объекта КИИ по результатам аудита



РЕЗУЛЬТАТ

Упрощает процесс категорирования

благодаря подготовленным формам и автоматизированным процедурам

Ускоряет подготовку необходимых документов

за счет импорта данных и автоматического заполнения требуемых полей

В разы сокращает трудозатраты

субъектов КИИ, в ведении которых десятки и сотни объектов КИИ

Позволяет обеспечить полное соблюдение требований

187-ФЗ и Приказов ФСТЭК по обеспечению безопасности значимых объектов КИИ

Благодарим за внимание!



R-Vision
At the root of your security

Выпускаем регулярный Дайджест ИБ:
rvision.pro/blog

8 (800) 350 77 57
sales@rvision.pro
www.rvision.pro