UDV ePlat4m SGRC

Решение создано на low-code платформе собственной разработки, которая позволяет автоматизировать бизнес-процессы и создавать собственные приложения без навыков программирования. Обеспечивает визуальное «кодирование», быструю адаптацию под требования Заказчика, лёгкую интеграцию в инфраструктуру предприятия.

ePlat4m SGRC

- Управление категорированием объектов КИИ
- Учет и классификация объектов защиты
- Управление инцидентами по ИБ
- Управление угрозами и уязвимостями ИБ
- Управления контролем состояния безопасности
- Управление мероприятиями по обеспечению ИБ
- Моделирование угроз безопасности
- Работа с персоналом и третьими лицами по вопросам ИБ
- Управление рисками
- Взаимодействие с НКЦКИ
- Управление требованиями (документами) по ИБ
- Управление обработкой персональных данных

UDV ePlat4m

Модуль управления категорированием ОКИИ

Модуль управления категорированием объектов КИИ предназначен для обеспечения информационно-технологической поддержки и контроля процессов учета и категорирования объектов КИИ за счет автоматизации деятельности по сбору и анализу информации об объектах КИИ.

Модуль позволяет решить следующие задачи:

- реализовать централизованный учет всех объектов КИИ в объеме, достаточном для планирования и контроля мероприятий по обеспечению их безопасности в соответствии с требованиями №187-ФЗ;
- автоматизировать процессы управления безопасностью объектов КИИ Эксплуатирующей организации.

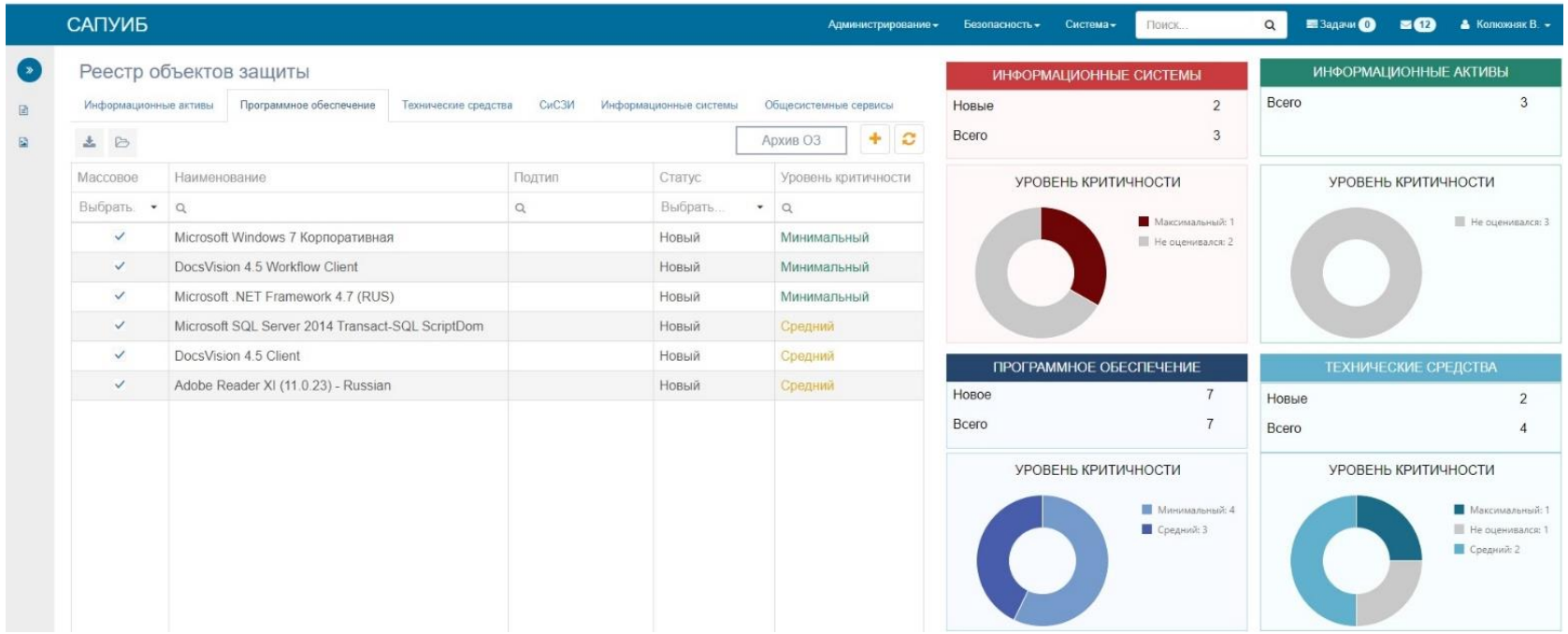
Формирование документов по требованиям ФСТЭК

- Данные об объектах и субъектах
- Модели нарушителей
- Модели угроз
- Опросные листы
- Внутренние документы
- Защитные меры

УКОКИИ

- Перечень объектов КИИ, подлежащих категорированию
- Акт категорирования объектов КИИ
- Реестр документов по категорированию КИИ

Модуль учета и классификации объектов защиты

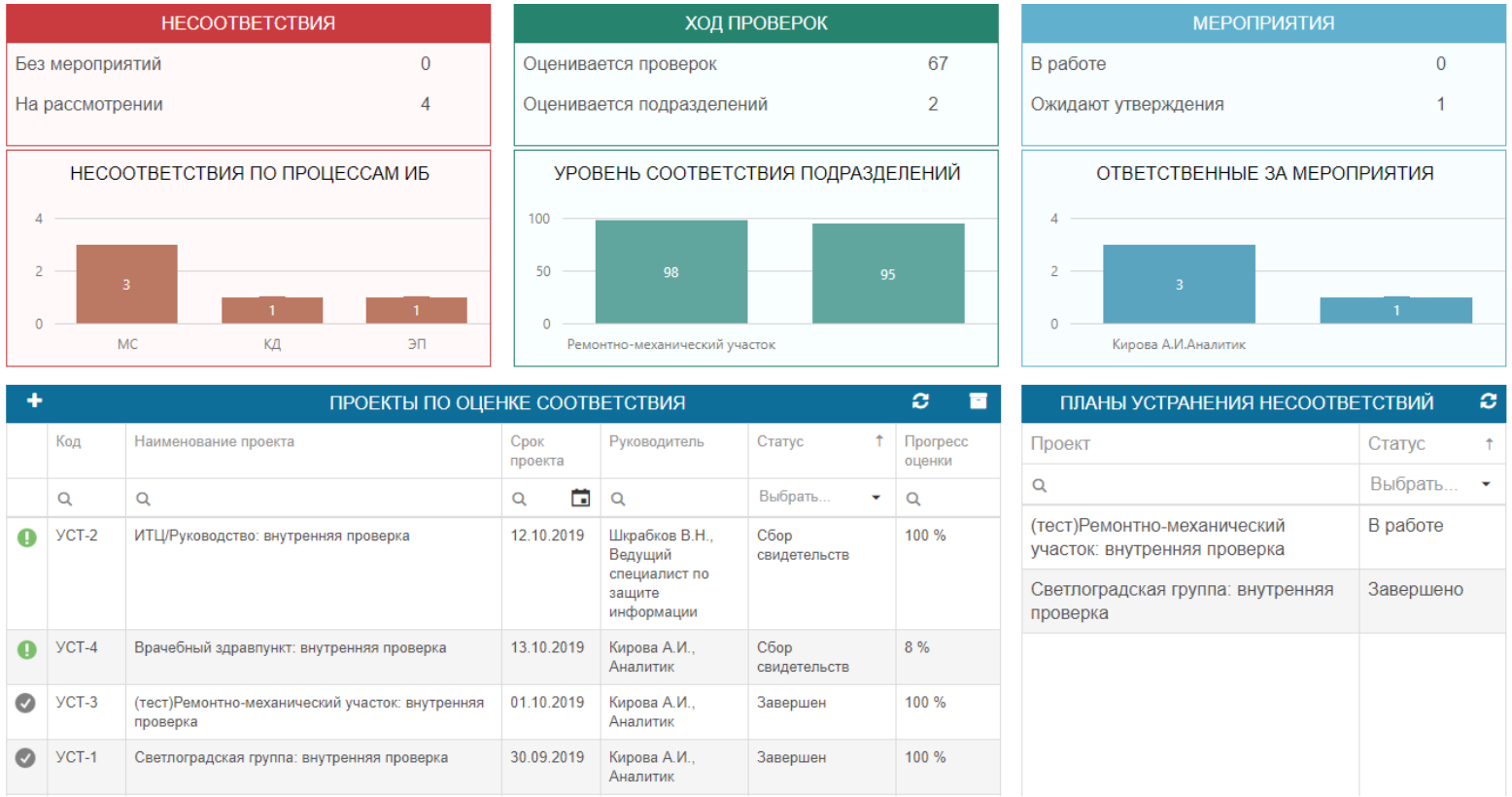


- Инвентаризация объектов защиты предприятия
- Их классификация по уровню критичности для бизнес-процессов в случае нарушения конфиденциальности, целостности и доступности (низкий, средний и высокий уровни критичности)

- Интеграция со сторонними системами инвентаризации для импорта/экспорта данных об объектах защиты
- Ведение вспомогательных реестров (объекты размещения, организаци-онная структура, справочник работников и т.д.).

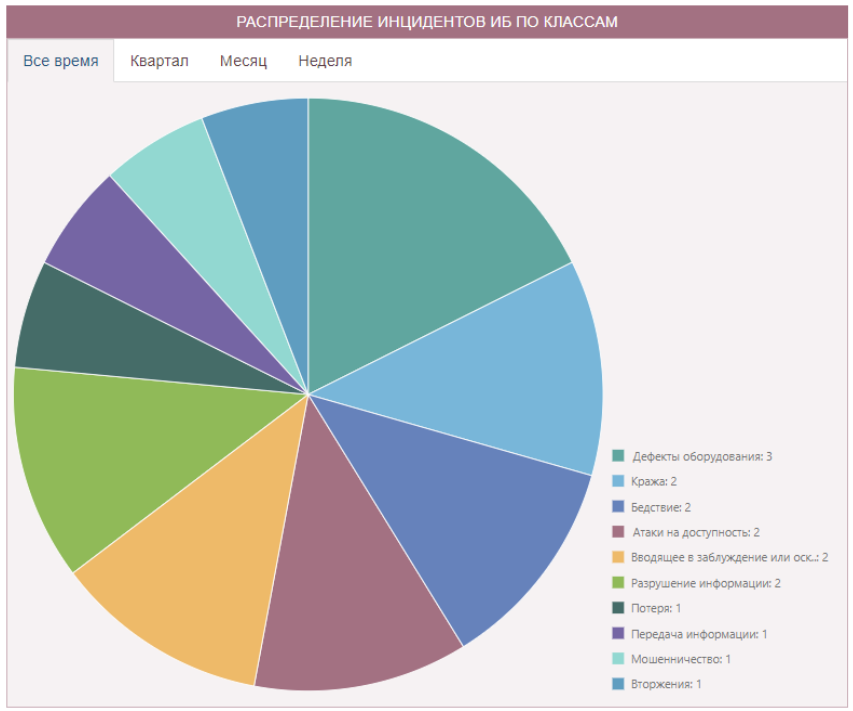
Модуль управления соответствием требованиям по ИБ

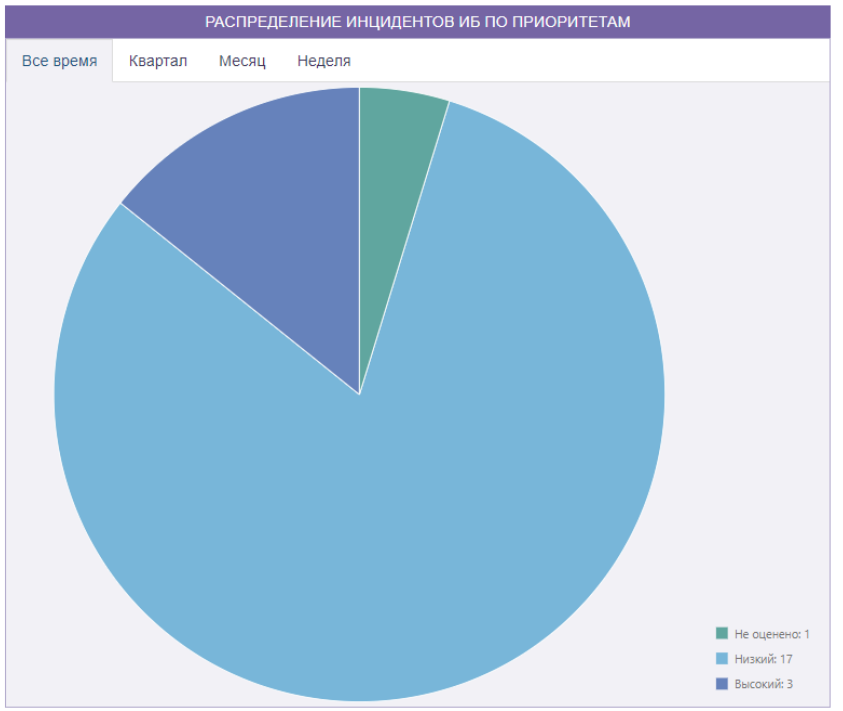
- Автоматизация процедур учета требований по ИБ
- Проведение проверок и контроля состояния соответствия требованиям по ИБ в организации
- Интеграция со сторонними системами аудита информационной безопасности для импорта сведений о выполнении требований ИБ, установленных в организации



Могут быть включены иные методика оценки выполнения требований (ИСО 27001, 152-ФЗ, ИБ КИИ, внутренние методики организации и т.д.)

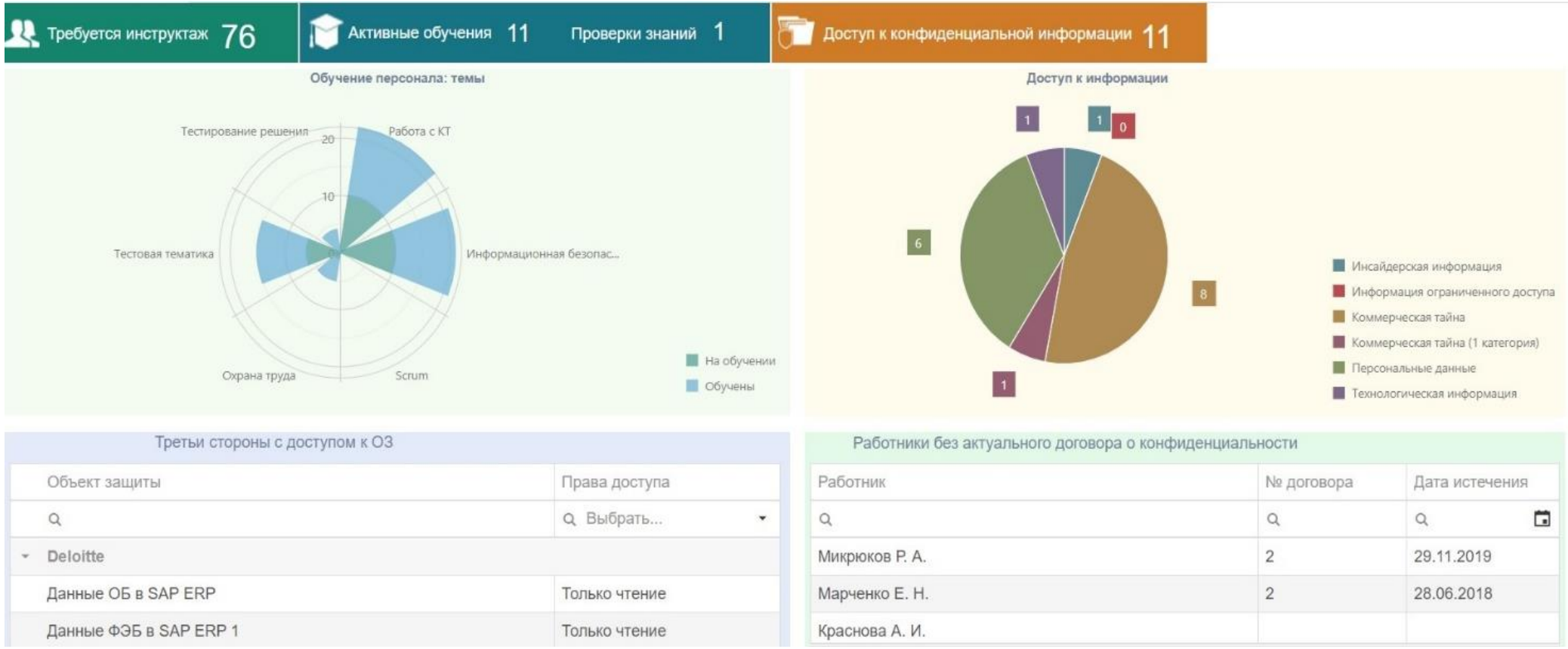
Модуль управления инцидентами по ИБ





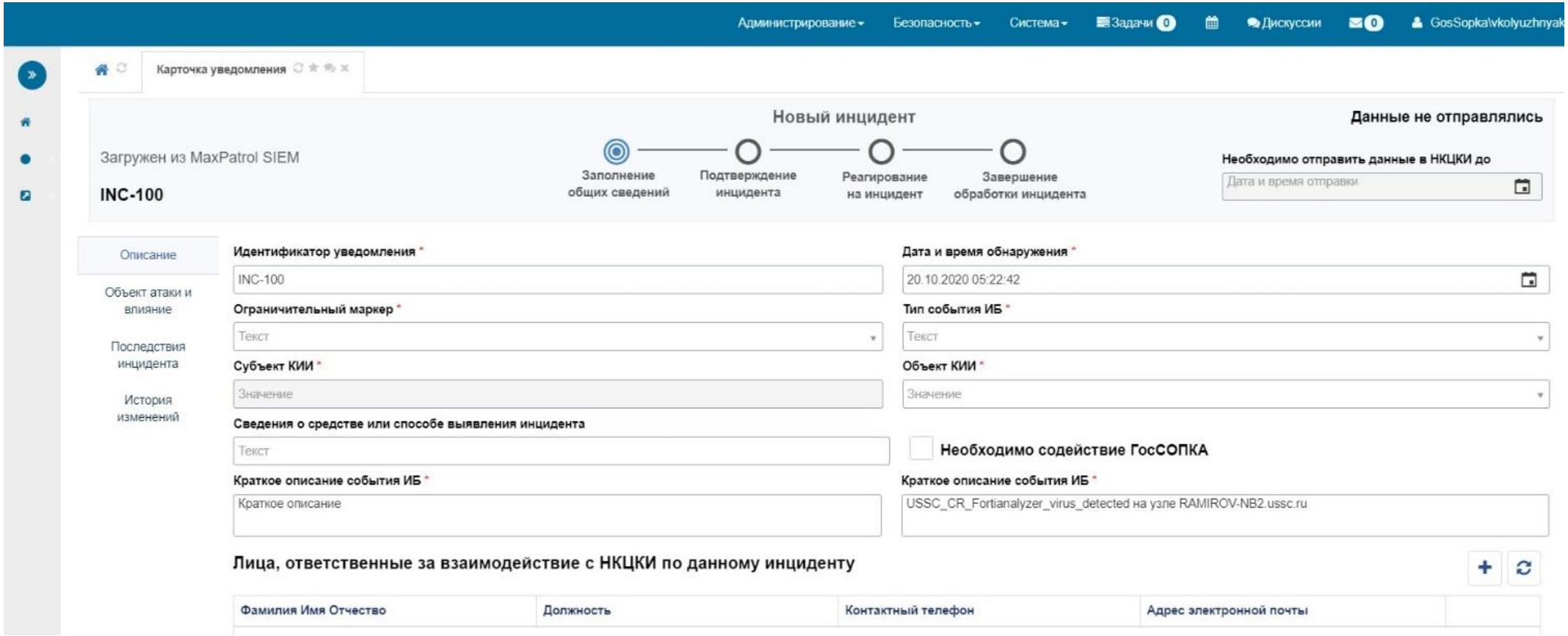
- Автоматизация процесса обработки событий, инцидентов и нештатных ситуаций, связанных с информационной безопасностью;
- Управление группами реагирования на инциденты ИБ;
- Формирование типовых сценариев по реагированию и расследованию;
- Интеграция со смежными системами для импорта/экспорта информации.

Работа с персоналом и третьими лицами по вопросам ИБ



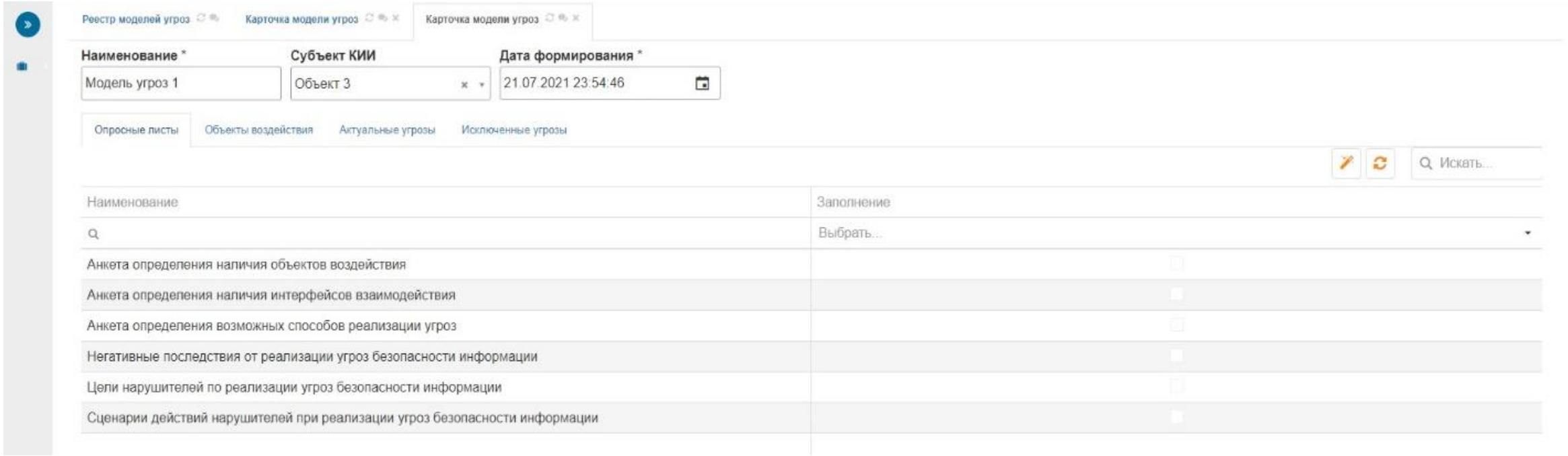
Контроль выполнения требований федерального законодательства при работе с персоналом и сторонними организациями по вопросам конфиденциальности (соглашение и договоры о конфиденциальности, разрешения на доступ к значимой информации и т.д.). Проведение обучения и повышения информированности персонала по вопросам ИБ.

Модуль взаимодействия с НКЦКИ



Автоматизация взаимодействия с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (отправка и получение данных через согласованный протокол передачи информации). Интеграция с внешними системами сбора и корреляции событий (SIEM).

Модуль моделирования угроз безопасности информации



Используется Методика оценки угроз безопасности информации (утверждена ФСТЭК России 05.02.2021)

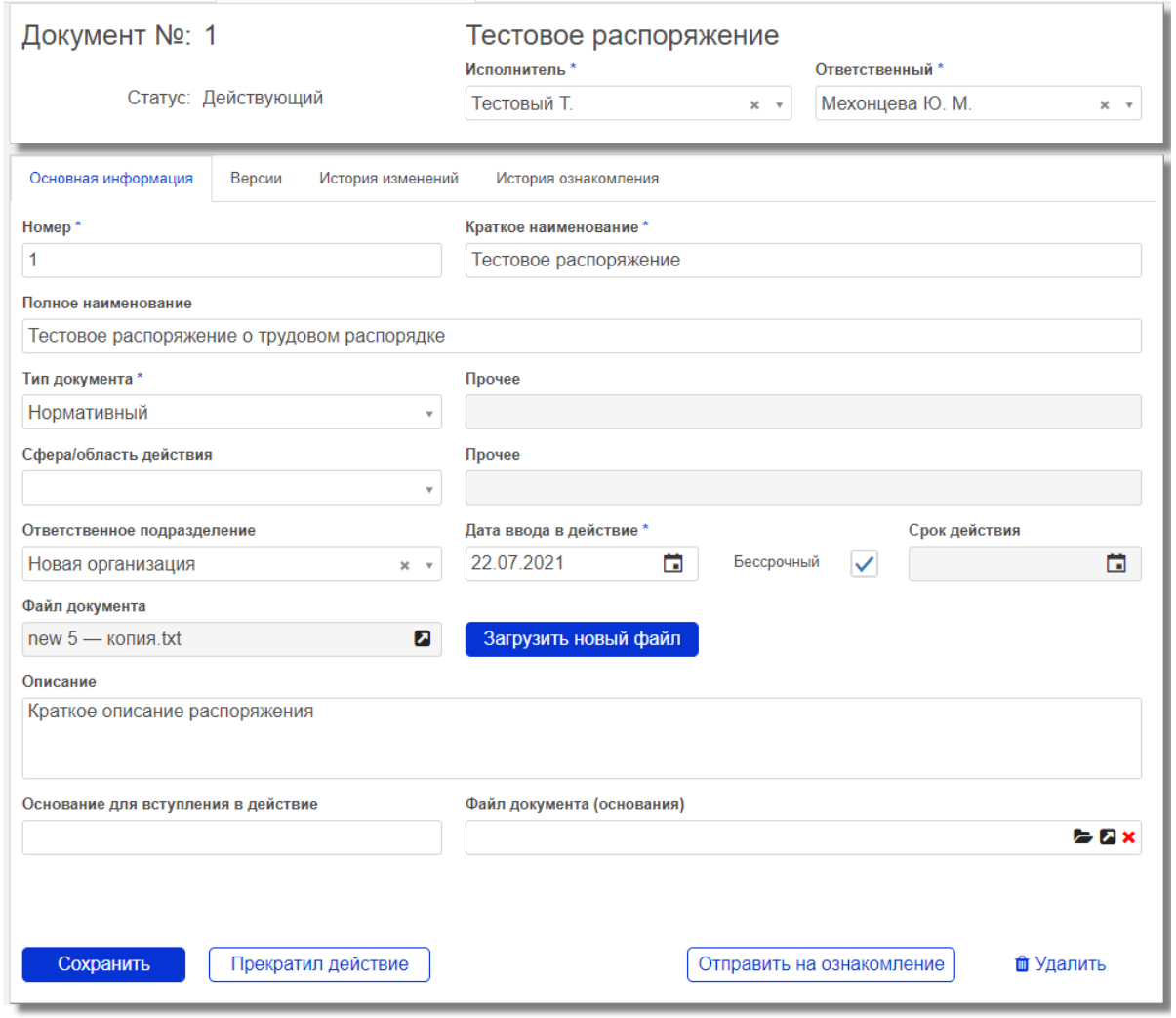
По итогам моделирования возможно сформировать в редактируемом виде проект модели угроз для последующего утверждения

Два способа построения модели угроз: опросные листы экспертов и пошаговое заполнение специалистом по ИБ

Ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии в электронном виде*

* Возможно в соответствии с п. 2.14 Методики.

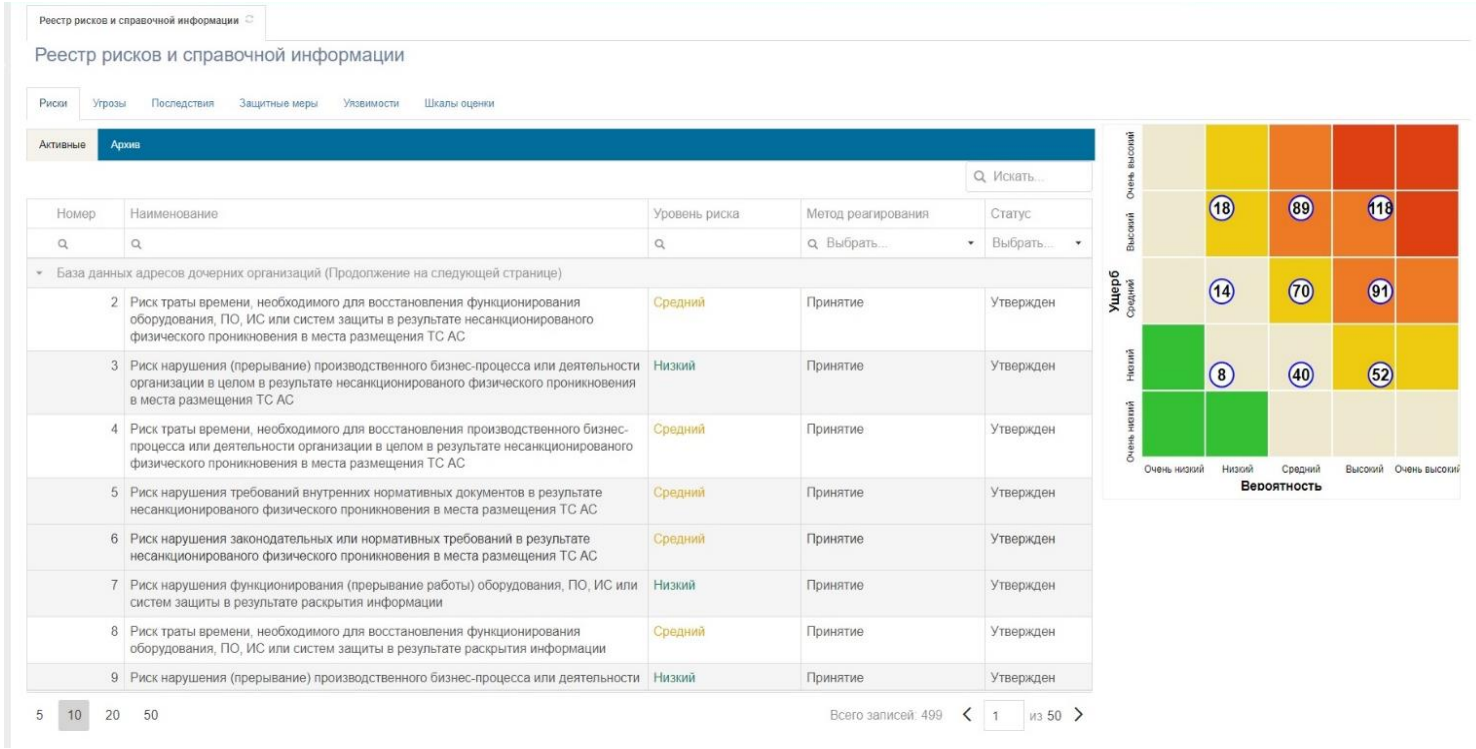
Модуль управления документами по ИБ



- Управление актуальными версиями документов (нормативные документы, ОРД, шаблоны и т.д.);
- Отслеживание версионности, внесенных изменений и сроков действия;
- Автоматическое создание необходимых документов на базе заведенных шаблонов и данных из системы;
- Настройка уведомлений о необходимости актуализации документации;
- Интеграция с системами электронного документооборота для импорта/экспорта документов и сведений о них.

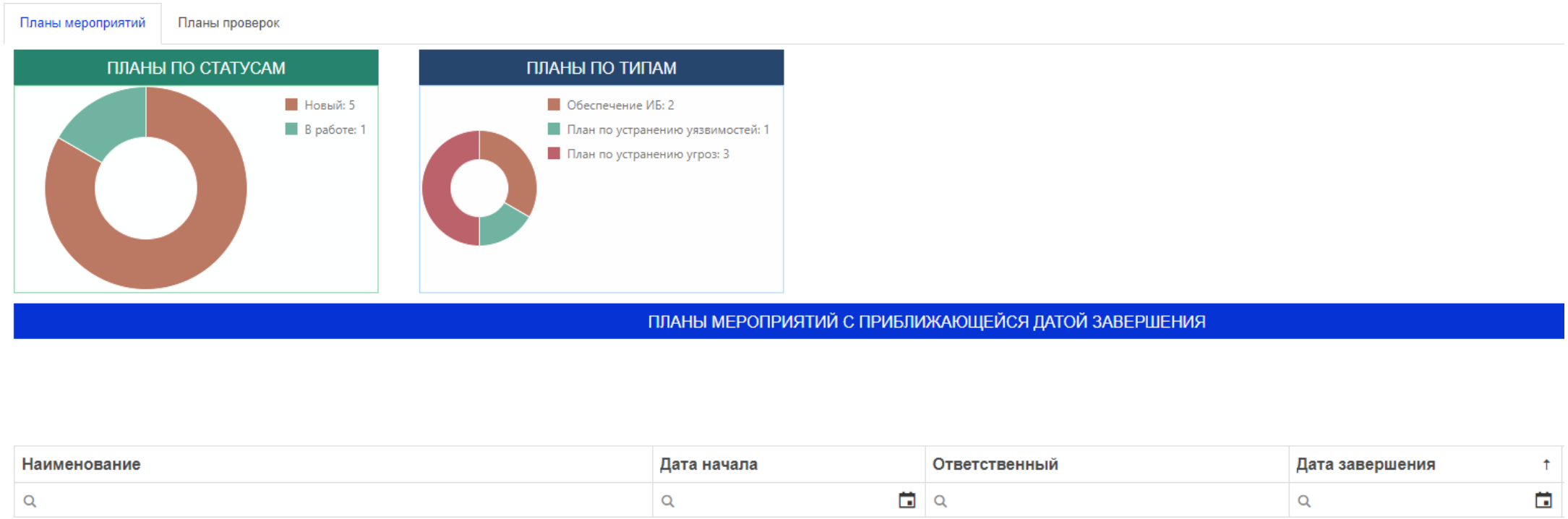
Модуль анализа и оценка рисков

- Полуколичественный метод анализа рисков, который обеспечивает минимально достаточную точность результатов оценки рисков ИБ
- Использование знаний экспертов и типовые перечни угроз, уязвимостей, защитных мер
- планирование мероприятий по снижению (компенсации) рисков
- оценка рисков на основе ISO-27001



Возможен пересмотр методики по оценки рисков в случае наличия подобных требований со стороны Заказчика

Модуль управления мероприятиями по ИБ



Управление планами и мероприятиями по подготовке, проведению и устранению недостатков государственного контроля в области ИБ

Управление планами и мероприятиями по различным направлениям ИБ (устранение угроз, устранение уязвимостей, планирование работ подразделения ИБ и т.д.)

Интеграция с иными модулями и системами task-tracking для быстрого создания мероприятий и хранения актуальной информации