

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
категорирование
м 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



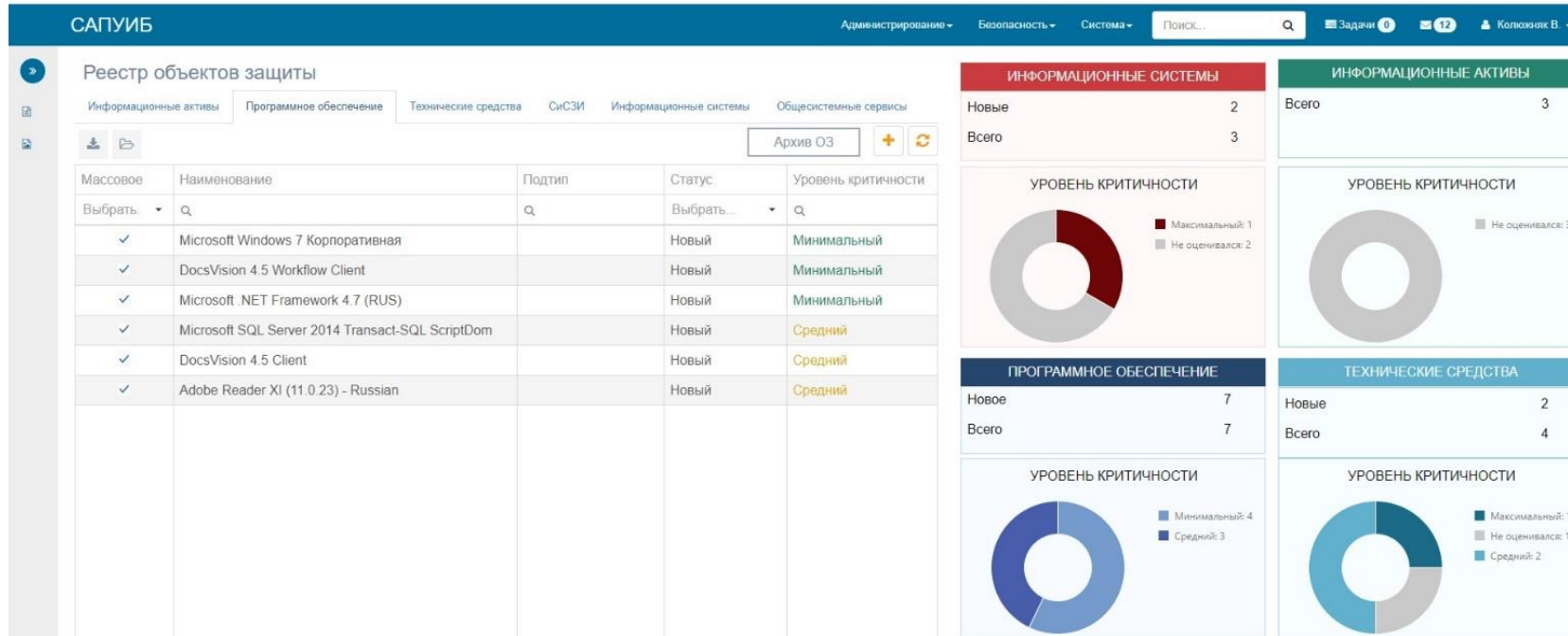
УКОКИИ



- 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, организационная 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

НЕСООТВЕТВИЯ	
Без мероприятий	0
На рассмотрении	4



ХОД ПРОВЕРОК	
Оценивается проверок	67
Оценивается подразделений	2



МЕРОПРИЯТИЯ	
В работе	0
Ожидают утверждения	1



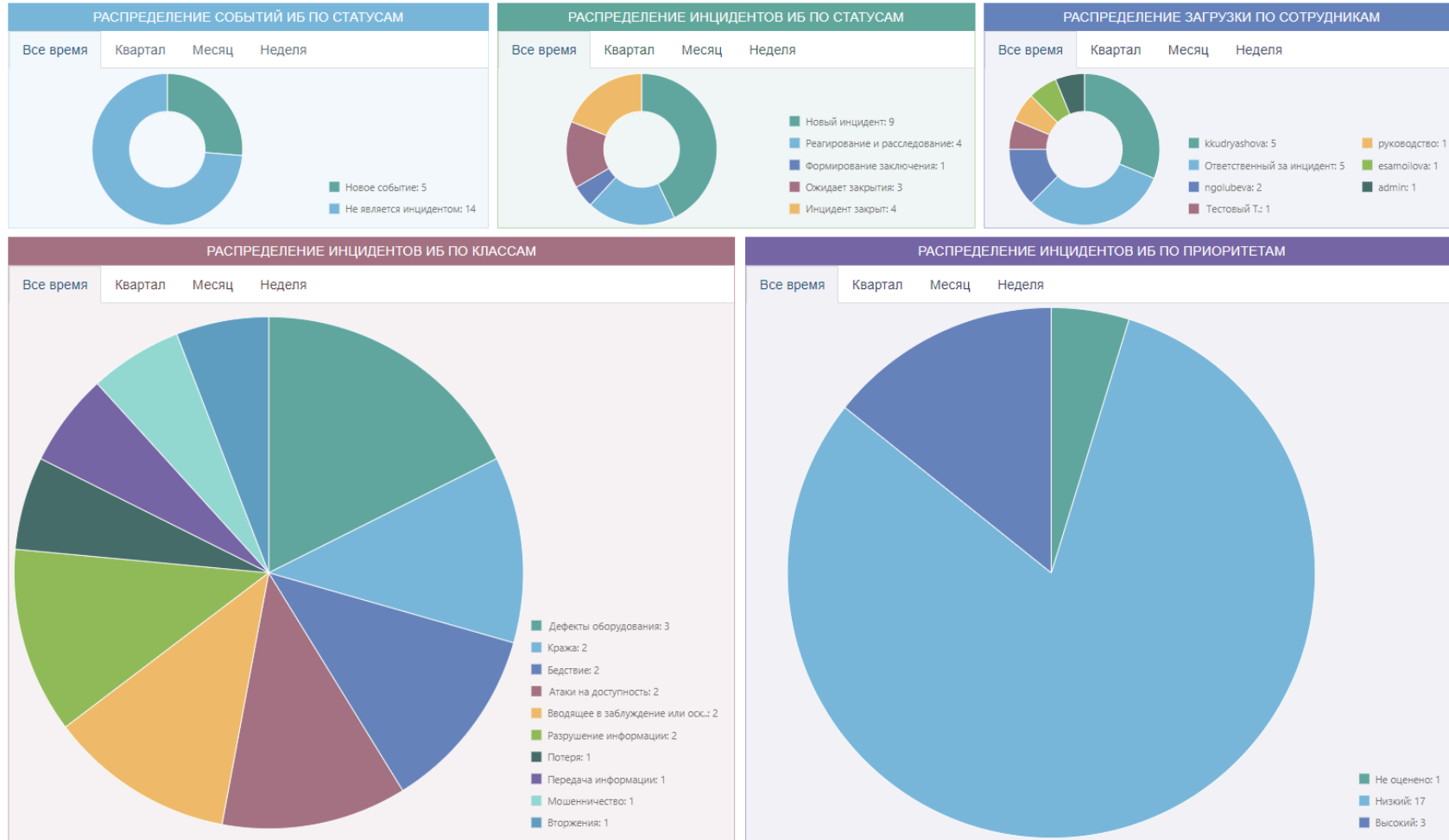
ПРОЕКТЫ ПО ОЦЕНКЕ СООТВЕТВИЯ						
Код	Наименование проекта	Срок проекта	Руководитель	Статус	↑	Прогресс оценки
УСТ-2	ИТЦ/Руководство: внутренняя проверка	12.10.2019	Шкрабков В.Н., Ведущий специалист по защите информации	Сбор свидетельств	↑	100 %
УСТ-4	Врачебный здравпункт: внутренняя проверка	13.10.2019	Кирова А.И., Аналитик	Сбор свидетельств	↑	8 %
УСТ-3	(тест)Ремонтно-механический участок: внутренняя проверка	01.10.2019	Кирова А.И., Аналитик	Завершен	↑	100 %
УСТ-1	Светлоградская группа: внутренняя проверка	30.09.2019	Кирова А.И., Аналитик	Завершен	↑	100 %

ПЛАНЫ УСТРАНЕНИЯ НЕСООТВЕТСТВИЙ	
Проект	Статус
(тест)Ремонтно-механический участок: внутренняя проверка	В работе
Светлоградская группа: внутренняя проверка	Завершено

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

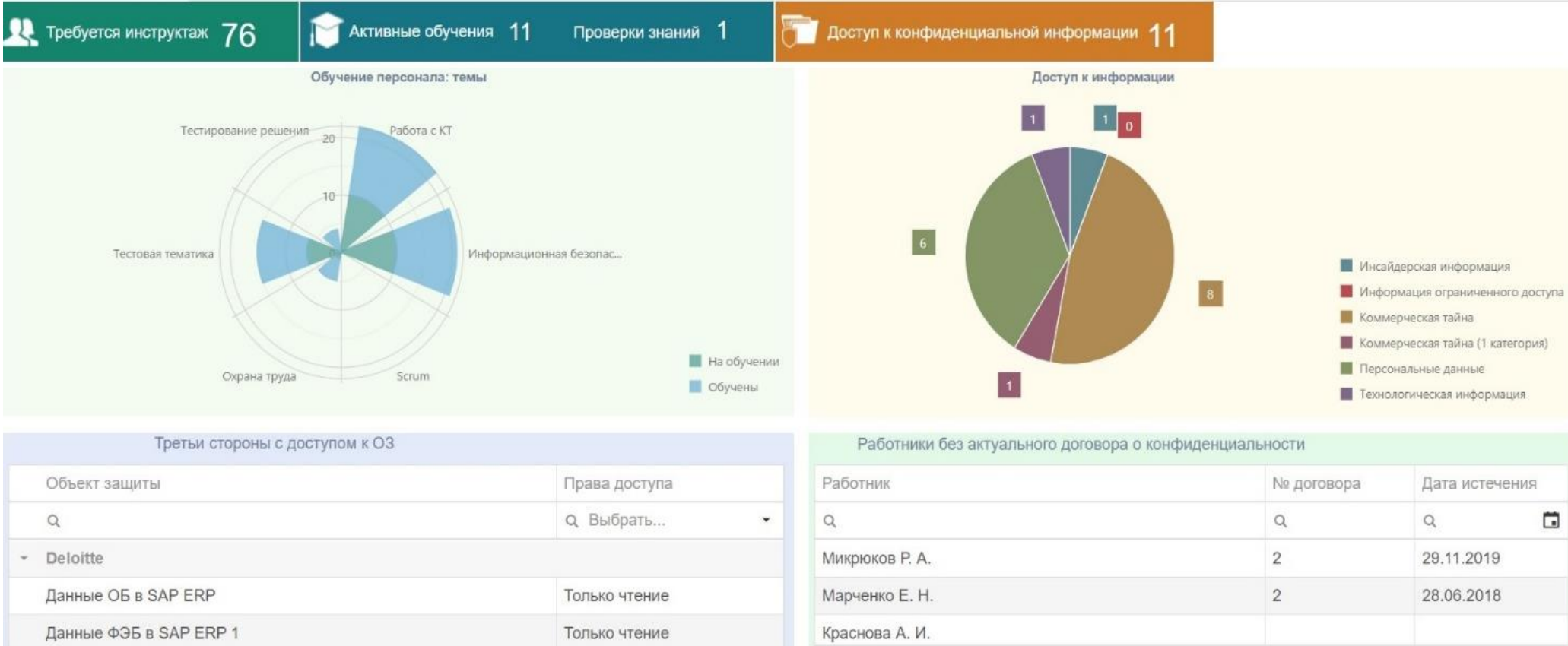


Модуль управления инцидентами по ИБ



- 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

Администрирование ▾ Безопасность ▾ Система ▾ Задачи 0 📅 Дискуссии 📧 0 👤 GosSopka\ykoluzhnyak

Карточка уведомления 🏠 ⌂ ⌘

Новый инцидент

Данные не отправлялись

Загружен из MaxPatrol SIEM

INC-100

Заполнение общих сведений — Подтверждение инцидента — Реагирование на инцидент — Завершение обработки инцидента

Необходимо отправить данные в НКЦКИ до

Дата и время отправки 📅

Описание

Идентификатор уведомления *

INC-100

Дата и время обнаружения *

20.10.2020 05:22:42 📅

Объект атаки и влияние

Ограничительный маркер *

Текст

Тип события ИБ *

Текст

Последствия инцидента

Субъект КИИ *

Значение

Объект КИИ *

Значение

История изменений

Сведения о средстве или способе выявления инцидента

Текст

Необходимо содействие ГосСОПКА

Краткое описание события ИБ *

Краткое описание

Краткое описание события ИБ *

USSC_CR_Fortianalyzer_virus_detected на узле RAMIROV-NB2.ussc.ru

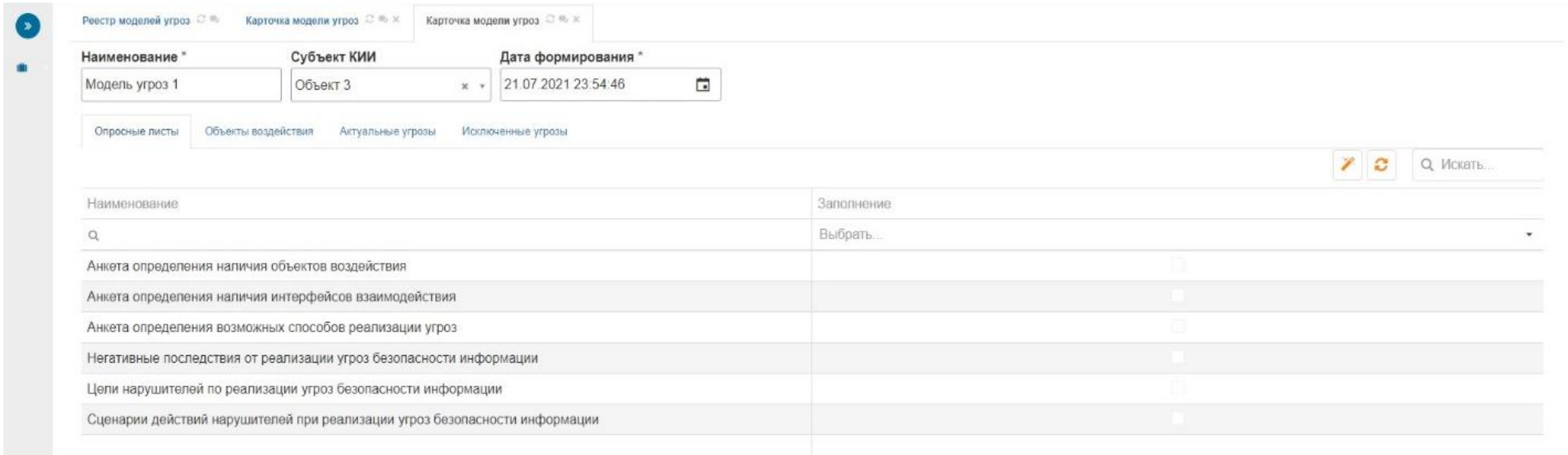
Лица, ответственные за взаимодействие с НКЦКИ по данному инциденту

+ 🔄

Фамилия Имя Отчество	Должность	Контактный телефон	Адрес электронной почты

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



Наименование	Заполнение
Анкета определения наличия объектов воздействия	<input type="checkbox"/>
Анкета определения наличия интерфейсов взаимодействия	<input type="checkbox"/>
Анкета определения возможных способов реализации угроз	<input type="checkbox"/>
Негативные последствия от реализации угроз безопасности информации	<input type="checkbox"/>
Цели нарушителей по реализации угроз безопасности информации	<input type="checkbox"/>
Сценарии действий нарушителей при реализации угроз безопасности информации	<input type="checkbox"/>

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

Документ №: 1 Тестовое распоряжение

Статус: Действующий Исполнитель * Тестовый Т. Ответственный * Мехонцева Ю. М.

Основная информация Версии История изменений История ознакомления

Номер * 1 Краткое наименование * Тестовое распоряжение

Полное наименование
Тестовое распоряжение о трудовом распорядке

Тип документа * Нормативный Прочее

Сфера/область действия Прочее

Ответственное подразделение Новая организация Дата ввода в действие * 22.07.2021 Бессрочный Срок действия

Файл документа
new 5 — копия.txt Загрузить новый файл

Описание
Краткое описание распоряжения

Основание для вступления в действие Файл документа (основания)

Сохранить Прекратил действие Отправить на ознакомление Удалить

- 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

Реестр рисков и справочной информации

Реестр рисков и справочной информации

Риски | Угрозы | Последствия | Защитные меры | Уязвимости | Шкалы оценки

Активные | Архив

Искать...

Номер	Наименование	Уровень риска	Метод реагирования	Статус
2	Риск траты времени, необходимого для восстановления функционирования оборудования, ПО, ИС или систем защиты в результате несанкционированного физического проникновения в места размещения ТС АС	Средний	Принятие	Утвержден
3	Риск нарушения (прерывание) производственного бизнес-процесса или деятельности организации в целом в результате несанкционированного физического проникновения в места размещения ТС АС	Низкий	Принятие	Утвержден
4	Риск траты времени, необходимого для восстановления производственного бизнес-процесса или деятельности организации в целом в результате несанкционированного физического проникновения в места размещения ТС АС	Средний	Принятие	Утвержден
5	Риск нарушения требований внутренних нормативных документов в результате несанкционированного физического проникновения в места размещения ТС АС	Средний	Принятие	Утвержден
6	Риск нарушения законодательных или нормативных требований в результате несанкционированного физического проникновения в места размещения ТС АС	Средний	Принятие	Утвержден
7	Риск нарушения функционирования (прерывание работы) оборудования, ПО, ИС или систем защиты в результате раскрытия информации	Низкий	Принятие	Утвержден
8	Риск траты времени, необходимого для восстановления функционирования оборудования, ПО, ИС или систем защиты в результате раскрытия информации	Средний	Принятие	Утвержден
9	Риск нарушения (прерывание) производственного бизнес-процесса или деятельности	Низкий	Принятие	Утвержден

База данных адресов дочерних организаций (Продолжение на следующей странице)

Ущерб: Очень высокий, Высокий, Средний, Низкий, Очень низкий

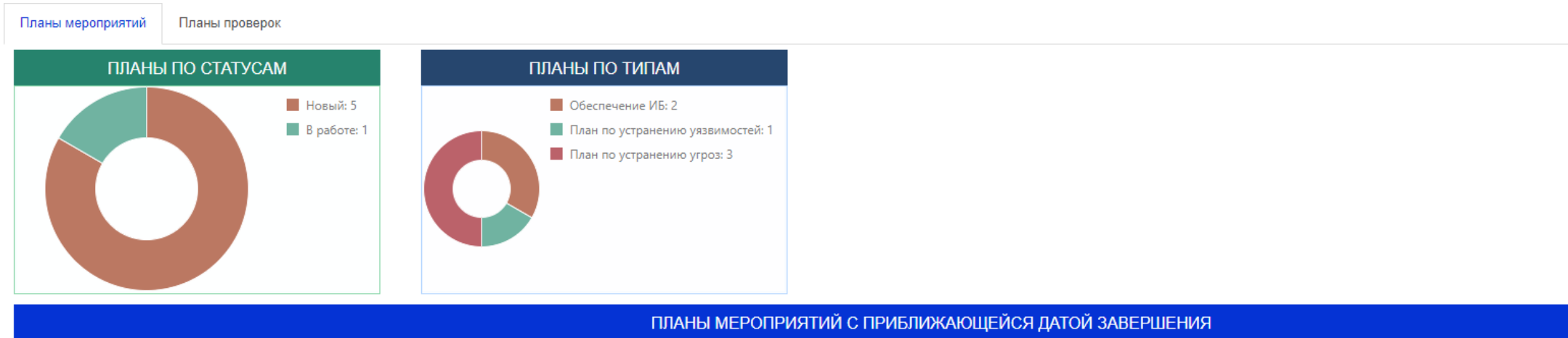
Вероятность: Очень низкий, Низкий, Средний, Высокий, Очень высокий

Всего записей: 499 < 1 из 50 >

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



Модуль управления мероприятиями по ИБ



Наименование	Дата начала	Ответственный	Дата завершения
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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