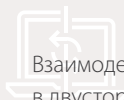


## «ПТ Ведомственный центр»

### СИСТЕМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ И ВЗАИМОДЕЙСТВИЯ С ГОССОПКА

#### ОСОБЕННОСТИ РЕШЕНИЯ



Взаимодействие с ГосСОПКА в двустороннем формате: обмен информацией об инцидентах и актуальных угрозах



Автоматическое создание карточки инцидента в необходимом формате, согласно требованиям НКЦКИ



Автоматическое получение инцидентов из MaxPatrol SIEM с возможностью выбора инфраструктуры для мониторинга, например только критической



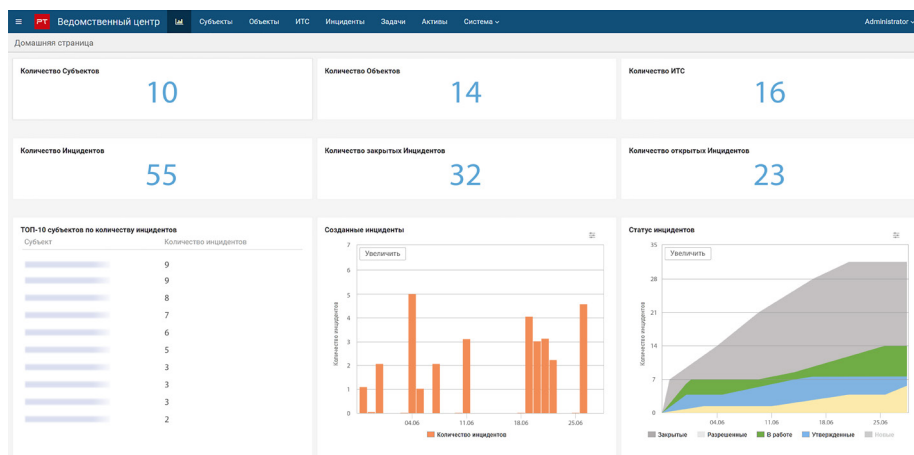
Разграничение прав доступа для специалистов группы реагирования

Согласно Федеральному закону от 26.07.2017 № 187-ФЗ о безопасности критической информационной инфраструктуры, субъекты КИИ обязаны незамедлительно информировать о кибератаках Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

«ПТ Ведомственный центр» — система управления инцидентами, которая автоматизирует процесс реагирования на инциденты и информирует о них НКЦКИ.

#### КЛЮЧЕВЫЕ ЗАДАЧИ

- + Регистрация инцидентов путем создания заявок на их обработку (карточек инцидентов)
- + Назначение приоритетов и статусов
- + Указание источников информации об инцидентах
- + Назначение ответственных за реагирование
- + Назначение сроков реагирования
- + Отработка инцидентов по шаблонам реагирования
- + Отчеты о новых инцидентах
- + Учет взаимодействия с НКЦКИ



Дашборды помогают руководителю контролировать работу центра ГосСОПКА

### ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

- + Учет субъектов (организаций) и их объектов, в том числе дочерних, для контроля зон ответственности
- + Учет критических информационных инфраструктур и ресурсов
- + Сбор информации об уязвимостях информационных систем

### РЕЗУЛЬТАТЫ ПРИМЕНЕНИЯ



**Соответствие требованиям законодательства** о необходимости регистрации инцидентов, управления ими и информирования НКЦКИ.



**Отправка сведений об инцидентах в срок** за счет мониторинга обработки инцидентов.



**Экономия времени специалистов по ИБ** благодаря автоматическому созданию карточки инцидента и применению шаблонов реагирования.

### КАК РАБОТАЕТ «ПТ ВЕДОМСТВЕННЫЙ ЦЕНТР»



### О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.