

# INNOSTAGE SOAR

# Компания Innostage



**20+**

Лет опыта команды экспертов в области информационной безопасности

**В ТОП 10**

Крупнейших компаний в сфере защиты информации в РФ\*

**6 МЕСТО**

Среди крупнейших поставщиков ИБ-услуг\*

**В ТОП-10**

Крупнейших поставщиков решений в сфере ИБ в РФ\*

**1200+**

Сотрудников

**150+**

Клиентов

**1000+**

Реализованных проектов

**60+**

Регионов РФ, где мы реализуем проекты

Москва

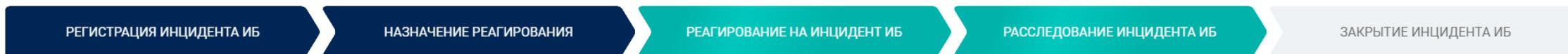
Саратов

Казань

Иннополис

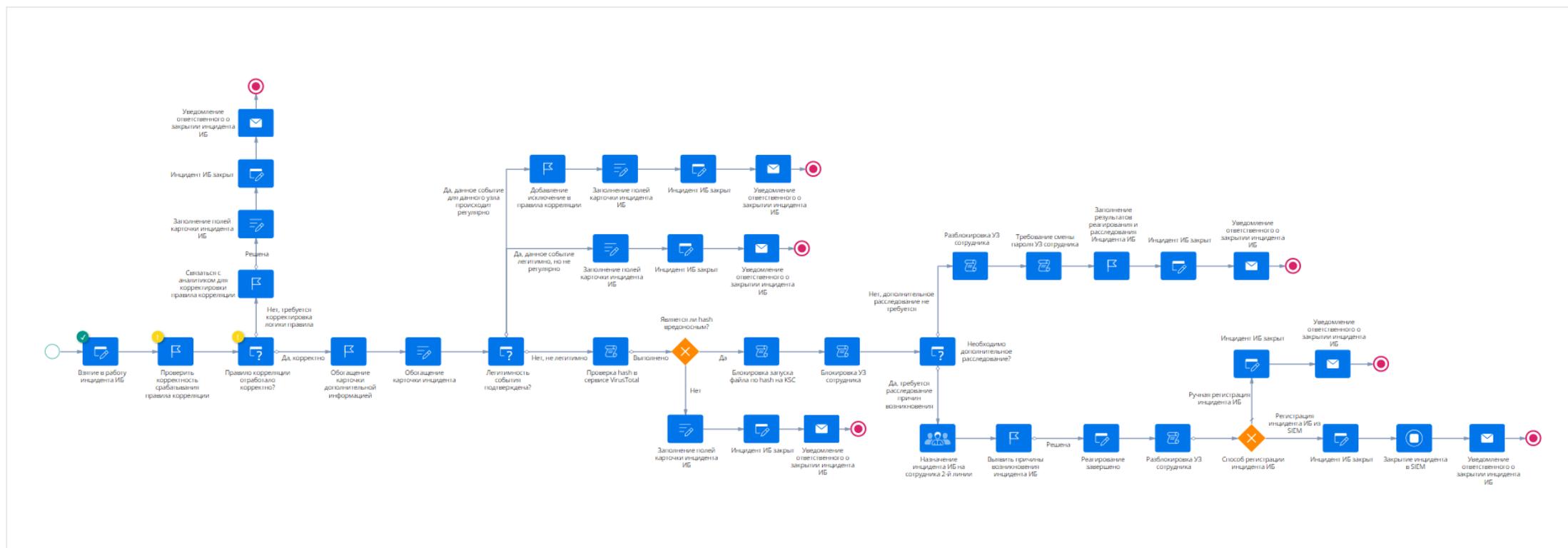
\* По данным отраслевых рейтингов CNews

## Автоматизирует процесс реагирования на инциденты



- ← ОБЩИЕ СВЕДЕНИЯ
- СБОР ДАННЫХ
- ПЛАН РЕАГИРОВАНИЯ**
- РЕАГИРОВАНИЕ
- РАССЛЕДОВАНИЕ
- СВЯЗИ
- СКРИПТЫ
- УВЕДОМЛЕНИЯ
- ФАЙЛЫ
- ЛЕНТА
- 

План реагирования	Статус	Дата запуска	Дата завершения
Вирусное заражение	Выполняется	30.01.2024 16:56	



## **ПОЛНЫЙ ЦИКЛ ОБРАБОТКИ КИБЕРИНЦИДЕНТОВ**

**Автоматизация ключевых  
процессов SOC и  
сценариев реагирования  
на инциденты ИБ**

## **ЭКСПЕРТИЗА И ЛУЧШИЕ ПРАКТИКИ РЫНКА ИБ**

**Многолетний опыт SOC  
CyberArt, одного из  
ведущих SOC в РФ**

## **ПОДДЕРЖКА ТРЕБОВАНИЙ РЕГУЛЯТОРОВ**

**Предоставление  
информации об  
инцидентах ИБ в центр  
ГосСОПКА**

- 01** Управление уязвимостями

---

- 02** Управление ИТ-активами

---

- 03** Управление инцидентами ИБ

---

- 04** Автоматизация реагирования на инциденты ИБ (модуль оркестрации)

---

- 05** Категорирование объектов КИИ

---

- 06** Моделирование угроз (модуль ЦМУ)

---

- 07** Взаимодействие с ГосСОПКА

---

- 08** Готовые интеграции

## CEO

- Снижение репутационных рисков и простоя бизнеса
- Предотвращение и минимизация ущерба
- Исключение нештатных ситуаций и кражи данных
- Соответствие требованиям регуляторов

## CISO

- Обеспечение высокого уровня защиты данных и инфраструктуры
- Статистика по закрытию инцидентов
- Контроль за состоянием ИБ, информация для принятия решений
- Поддержание в актуальном состоянии базы ИТ-активов

## РУКОВОДИТЕЛЬ SOC

- Оперативное обнаружение уязвимостей
- Консолидация работы с инцидентами
- Контроль результатов деятельности SOC и групп реагирования
- Быстрая адаптация новых операторов SOC

## АНАЛИТИК SOC

- Оперативное выявление новых угроз
- Сокращение времени на сбор информации и расследование
- Готовые сценарии реагирования
- Автоматизация ручных задач с помощью playbook

# Обработка инцидента



✓ ≈ **6 МИН.** Среднее время реагирования на инциденты ИБ в день **с автоматизацией**

✗ ≈ **213 МИН.** Среднее время реагирования на инциденты ИБ в день **без автоматизации**



## Гибкая интеграция с SIEM

---

Настройка передачи инцидентов ИБ из SIEM по правилам корреляции (черный/белый список), обогащение карточки инцидента корреляционными событиями из SIEM



## Конструктор сценариев реагирования

---

Гибкий No-Code конструктор сценариев реагирования на инциденты ИБ с разграничением доступа по ролям



## Поддержка сквозных сценариев

---

Разделение сценария реагирования в карточке инцидента ИБ на отдельные блоки для выполнения их различными рабочими группами SOC



## Взаимодействие с внешними исполнителями

Привлечение к процессу работы с инцидентом сотрудников, не являющихся операторами SOC, без предоставления доступа в IRP/SOAR систему



## No-Code конструктор карточек и дашбордов

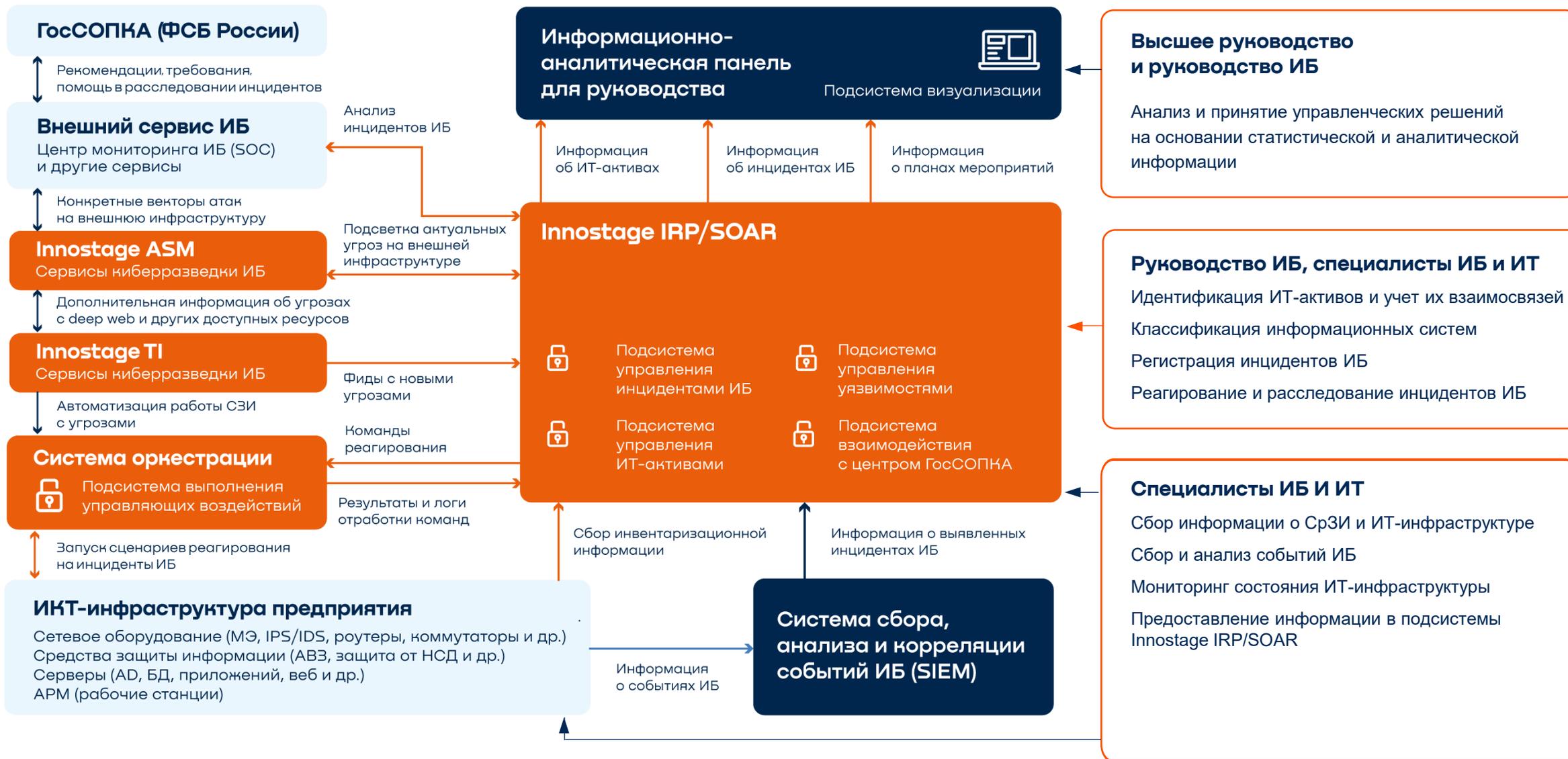
Редактирование карточек объектов и дашбордов с использованием визуальных методов моделирования, без привлечения разработчика и написания кода



## Сервисная изолированность

Автоматизация реагирования на инциденты и выполнения блокирующих операций с использованием отдельного компонента — системы оркестрации Innostage Orchestrator

# Архитектура Innostage SOAR



# Продуктовый портфель Innostage



**INNOSTAGE  
SOAR**

**INNOSTAGE  
ORCHESTRATOR**

**МАТРИЦА  
ДОСТУПА**

**INNOSTAGE  
TI**

**INNOSTAGE  
ASM**

**IN-DAP**

**NGSC**

**ЕОК**

**IN-PROFILE**

**PRISMA**

**СКАНЕР  
СИСТЕМА  
ИНВЕНТАРИЗАЦИИ  
СЕТЕВЫХ УСТРОЙСТВ**

**INNDATA  
(BIGDATA)**

**ЦИФРОВАЯ  
МОДЕЛЬ УГРОЗ**

**INNOSTAGE  
PAM**

**ЦИФРОВОЙ  
ШТАБ**

# СПАСИБО ЗА ВНИМАНИЕ

## **INNOSTAGE**

Казань, ул. Подлужная, 60

+7 (843) 567-42-90

[SOAR@innostage-group.ru](mailto:SOAR@innostage-group.ru)