ЦЕНТР ГОССОПКА/ SOC

КАК УПРАВЛЯЕМЫЙ СЕРВИС БЕЗОПАСНОСТИ КИИ

187-ФЗ «О БЕЗОПАСНОСТИ КИИ»

Закон регулирует деятельность по обеспечению безопасности объектов критической информационной инфраструктуры (КИИ), работа которых жизненно важна для экономики и в целом обеспечения безопасности личности, общества и государства.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА — совокупность всех объектов КИИ и используемых ими сетей электросвязи.

ОБЪЕКТЫ КИИ

информационные системы

информационно-телекоммуникационные сети

автоматизированные системы управления

СУБЪЕКТЫ КИИ

государственные органы

государственные учреждения

российские юр. лица, ИП (которые владеют объектами КИИ и обеспечивают их взаимодействие)

ОТРАСЛИ КИИ

здравоохранение, наука, транспорт, связь, финансы, атомная и топливная энергетика, промышленность (горнодобывающая, металлургическая, химическая, оборонная, ракетно-космическая)

ТРЕБОВАНИЯ К ЗНАЧИМЫМ ОБЪЕКТАМ КИИ

- Идентификация и аутентификация
- Управление доступом
- Ограничение программной среды
- Защита машинных носителей информации
- Аудит безопасности
- Предотвращение вторжений
- Обеспечение целостности
- Обеспечение доступности

- Защита технических средств и систем
- Защита информационной системы и ее компонентов
- Планирование мероприятий по безопасности
- Управление конфигурацией
- Управление обновлениями ПО
- Реагирование на инциденты ИБ
- Обеспечение действий в нештатных ситуациях
- Информирование и обучение персонала

ОБЯЗАННОСТИ СУБЪЕКТА КИИ

Предоставить сведения о категорировании во ФСТЭК России

Соблюдать требования ФСТЭК России по обеспечению безопасности значимых объектов КИИ

Интегрироваться с ГосСОПКА, реагировать и уведомлять заинтересованных лиц о компьютерных инцидентах

Создать систему обеспечения безопасности объекта КИИ

Оказывать содействие должностным лицам регулятора в проведении надзорных действий

ГосСОПКА

ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ) —

глобальная система сбора и обмена информацией о компьютерных атаках на территории РФ

ЦЕЛЬ

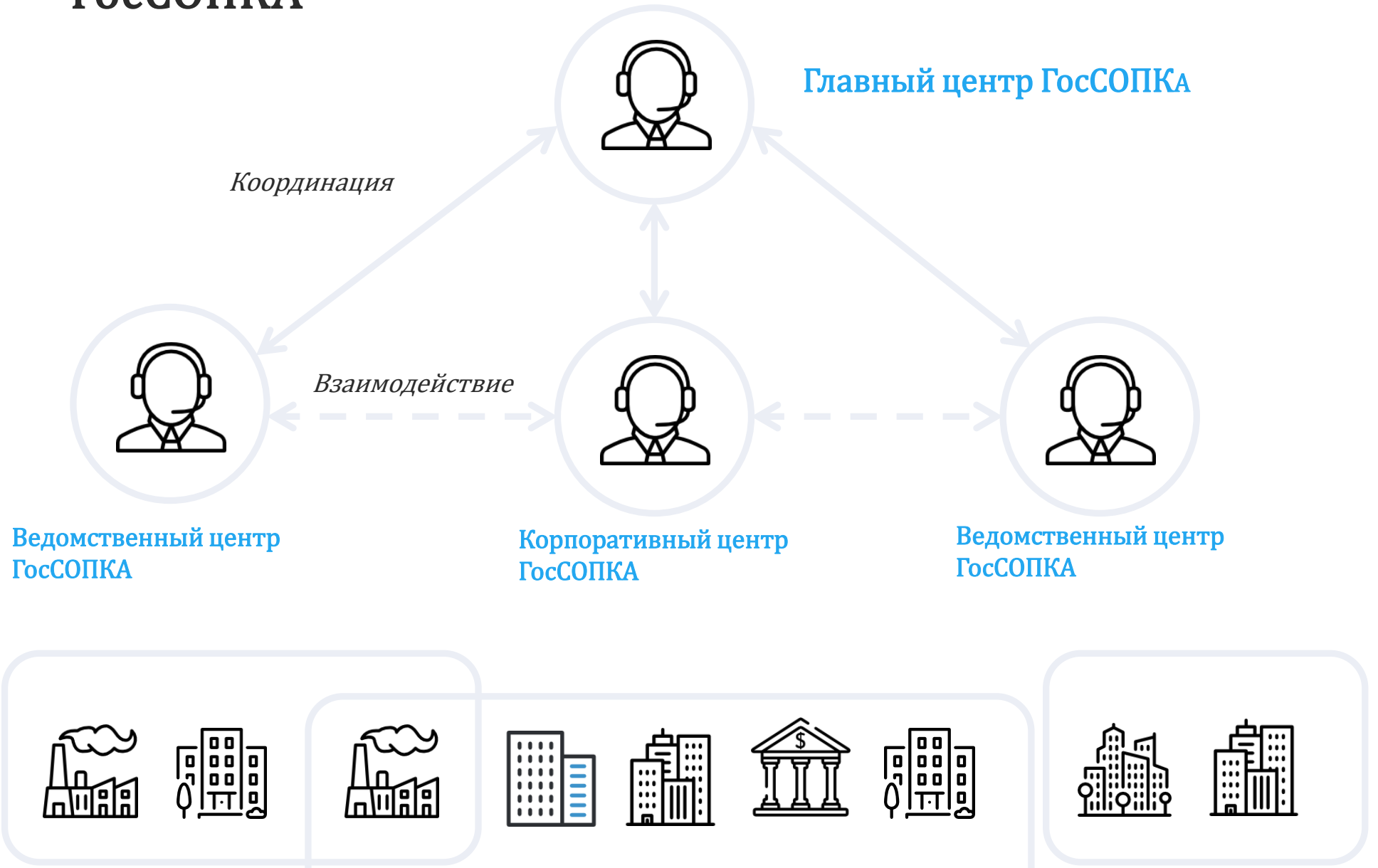
Предотвращение и противодействие атакам за счет непрерывного мониторинга инцидентов ИБ и своевременной выработки защитных мер

ВАРИАНТЫ ВЗАИМОДЕЙСТВИЯ

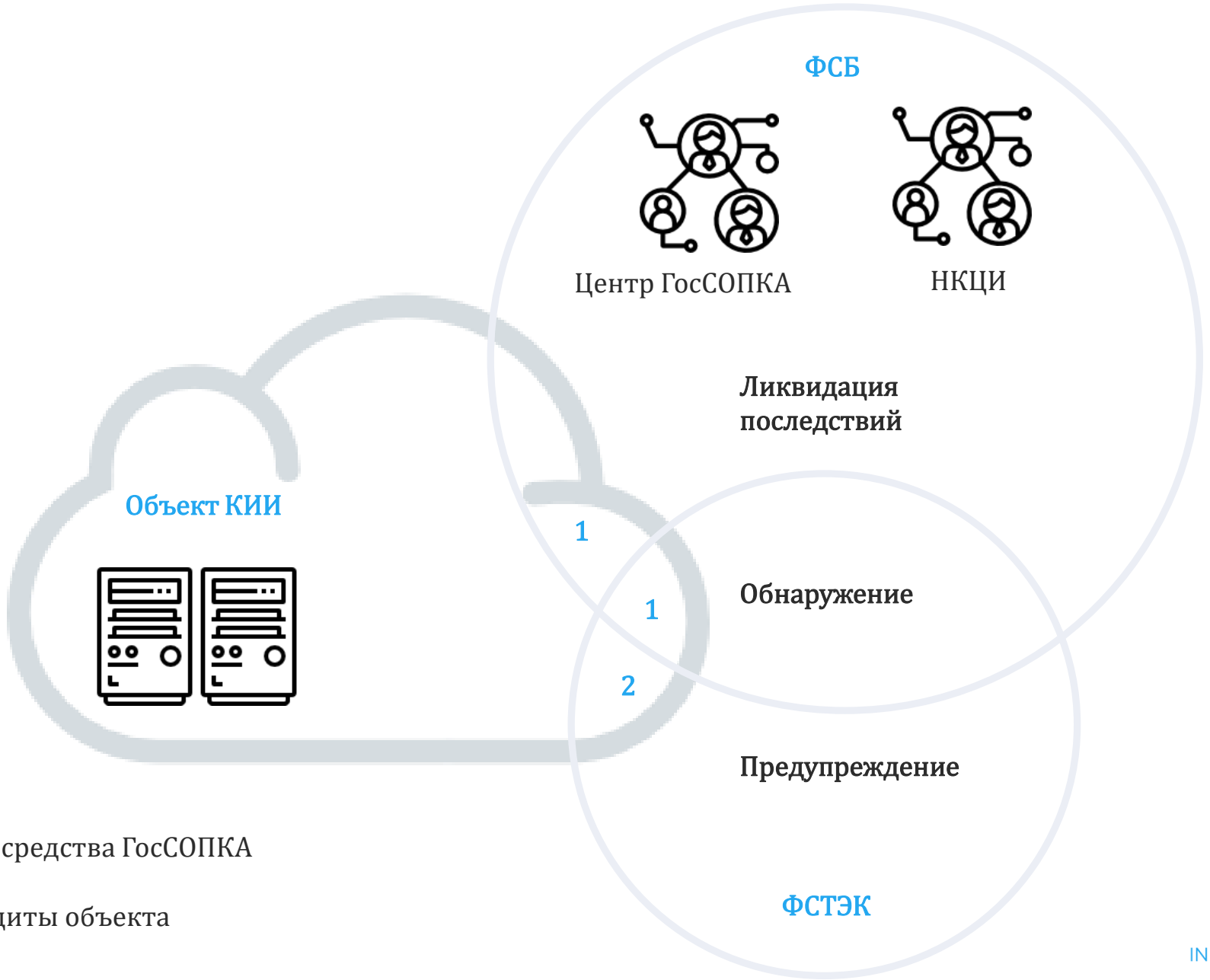
Создание собственного центра ГосСОПКА

Подключение к Корпоративному центру ГосСОПКА

ГосСОПКА


Главный центр ГосСОПКА
Координация
Взаимодействие
Ведомственный центр ГосСОПКА
Корпоративный центр ГосСОПКА
Ведомственный центр ГосСОПКА

СТРУКТУРА ВЗАИМОДЕЙСТВИЯ



1 Технические средства ГосСОПКА

2 Средства защиты объекта

СИСТЕМА ЗАЩИТЫ ЗНАЧИМОГО ОБЪЕКТА КИИ ОТ ИНФОСЕКЬЮРИТИ

ПРОЕКТИРОВАНИЕ

Подготовка предложения по составу СЗИ

Разработка технического проекта и рабочей документации на систему обеспечения безопасности объектов КИИ

Предложение по составу СЗИ системы обеспечения безопасности объектов КИИ

Комплект технорабочей документации

Система обеспечения безопасности объектов КИИ, удовлетворяющая требованиям законодательства РФ

ВНЕДРЕНИЕ

Монтаж и пусконаладка

Проведение опытной эксплуатации

Анализ уязвимостей

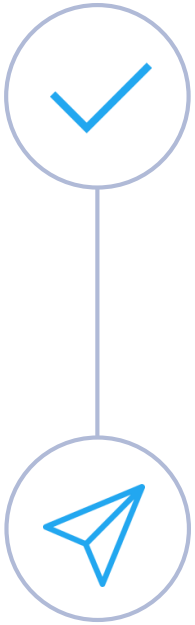
Введение в промышленную эксплуатацию

Зачем нужен SOC

SOC

Центр мониторинга и реагирования на инциденты информационной безопасности + Центр ГосСОПКА

сложный комплекс технических средств, выстроенных процессов и профильных специалистов



Цели

- Снижение рисков хищения данных и денежных средств, прерываний в деятельности бизнеса
- Снижение тяжести последствий инцидентов

Задачи

- Контроль состояния IT-инфраструктуры
- Проактивное предотвращение инцидентов
- Автоматизация процессов управления инцидентами
- Расследование инцидентов

Преимущество аутсорсинга SOC/ГосСОПКА

- Предсказуемые затраты и сроки на внедрение
- Нет необходимости в собственной дорогостоящей инфраструктуре для управления инцидентами
- Решение кадровых проблем
- Перенос ответственности за качество сервиса
- Автоматизация рутинных действий по обеспечению ИБ
- Получение своевременных сведений об угрозах и уязвимостях

Сервис SOC/ГосСОПКА от Infosecurity

- Мониторинг и реагирование 24/7
- Более 25 экспертов в команде
- Выявление инцидентов с помощью настраиваемых механизмов анализа событий
- Автоматическое реагирование на типовые инциденты
- Регулярная отчетность

Варианты реализации

Облачная

Смешанная

Зоны ответственности

Infosecurity SOC

- Выполняет все работы по выявлению и реагированию на инциденты ИБ
- Обеспечивает непрерывность процесса управления инцидентами ИБ

Служба ИБ Заказчика

- Решает задачи по обеспечению функционирования системы безопасности объектов КИИ/организации
- Контролирует выполнение SLA
- Является точкой эскалации по сложным инцидентам

ПОДКЛЮЧЕНИЕ К ГОССОПКА

ПОДКЛЮЧЕНИЕ

Инвентаризация информационных ресурсов

Договор о взаимодействии с корпоративным центром ГосСОПКА

РАБОТЫ

Мониторинг и управление событиями информационной безопасности

РЕЗУЛЬТАТ

Перечни выявленных уязвимостей, угроз, обнаруженных атак, инцидентов ИБ

Отчеты о реагировании на инциденты ИБ и результаты расследования