POSITIVE TECHNOLOGIES

Ильяс Киреев

Продвижение и развитие продуктов

Обеспечение соответствия 187-ФЗ: практический опыт

187-ФЗ базис

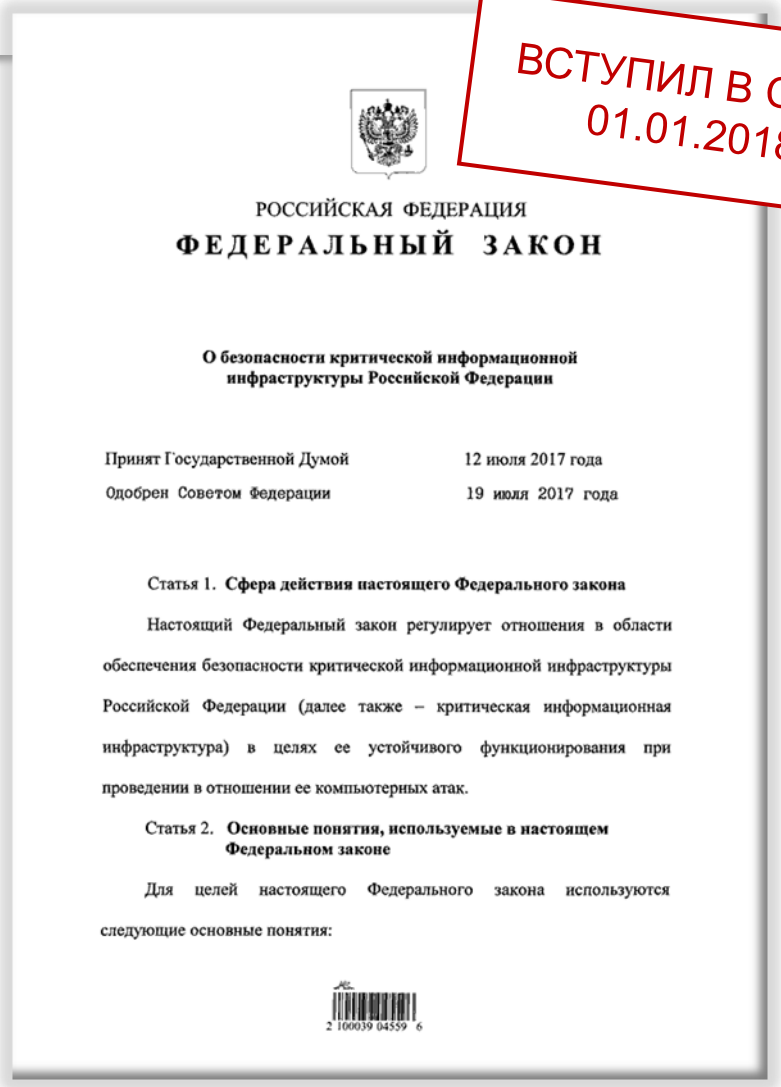
ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

ВСТУПИЛ В СИЛУ 01.01.2018

Субъекты КИИ - гос. органы и учреждения, юр. лица и ИП

Объекты КИИ - **ИС, ИТС, АСУ** в сферах:

…3 категории **значимых объектов КИИ**…



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

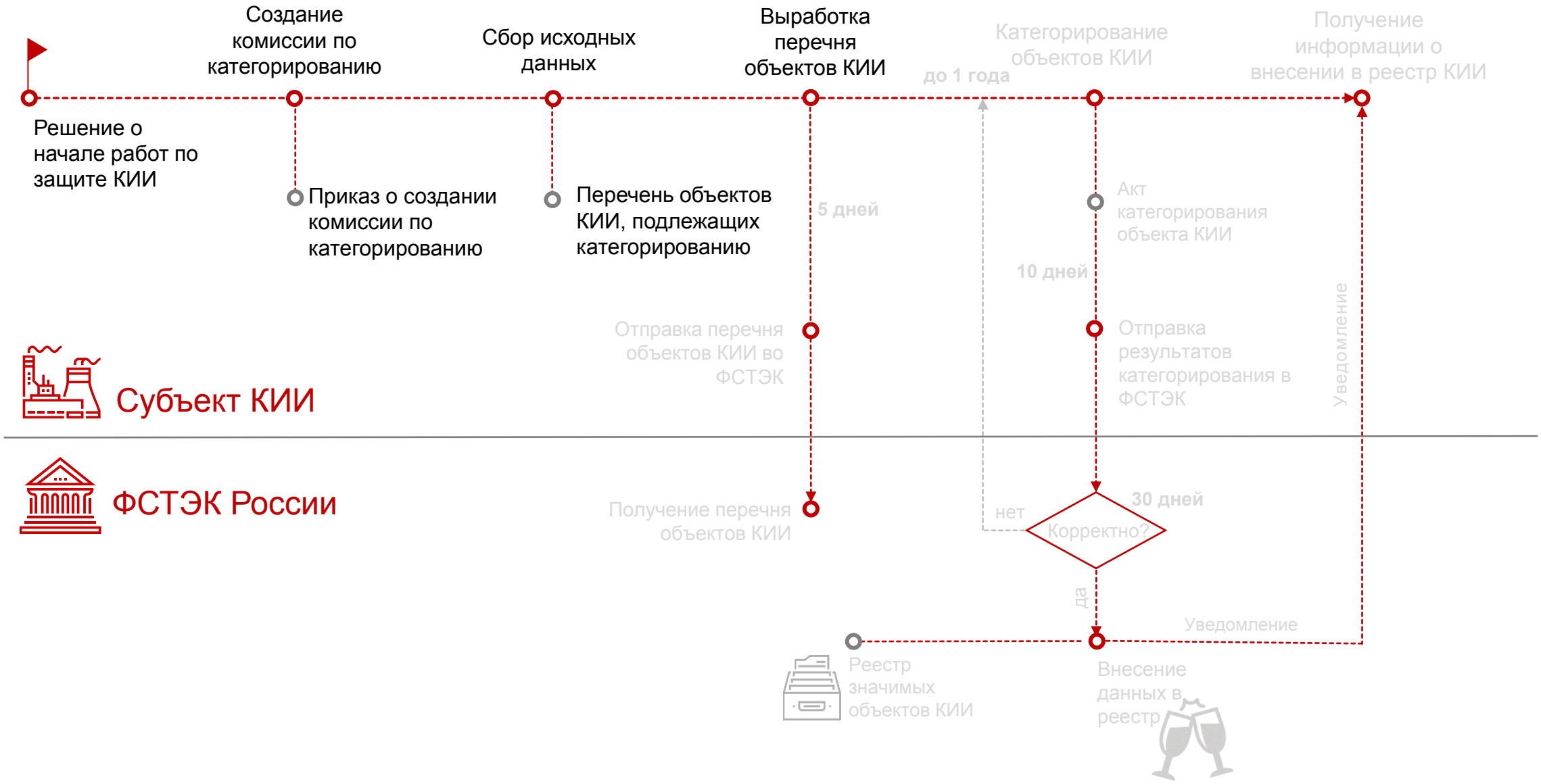
Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

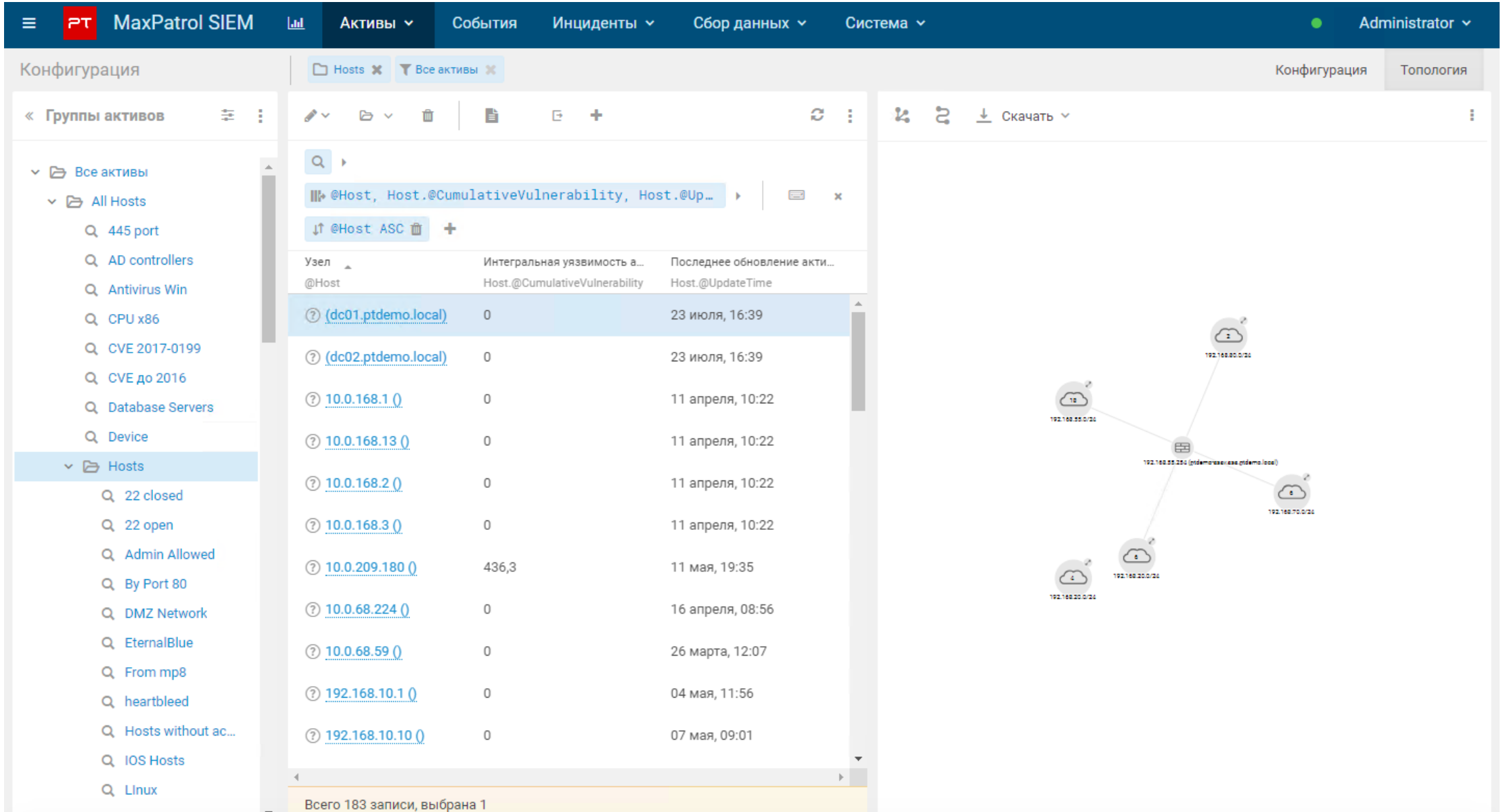
Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

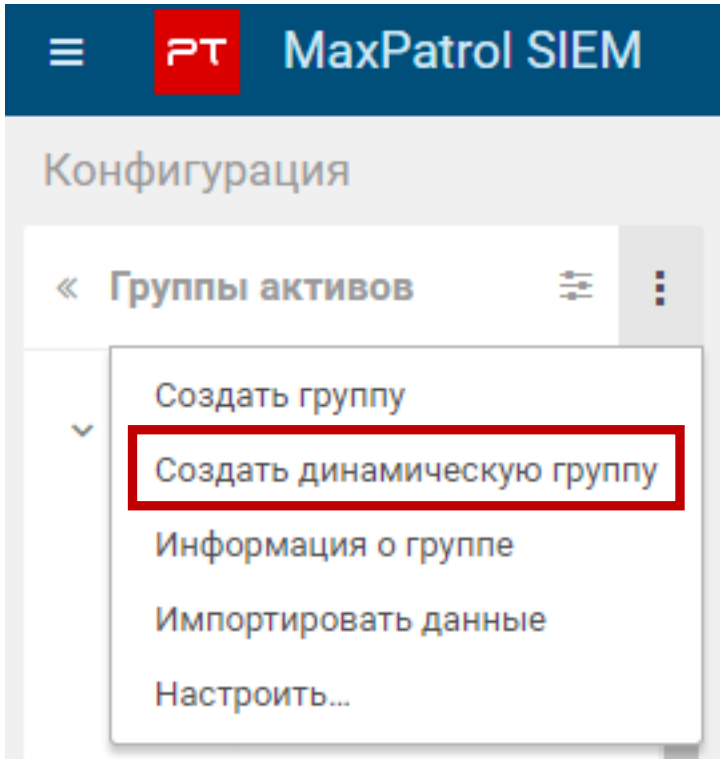
Порядок категорирования объектов КИИ



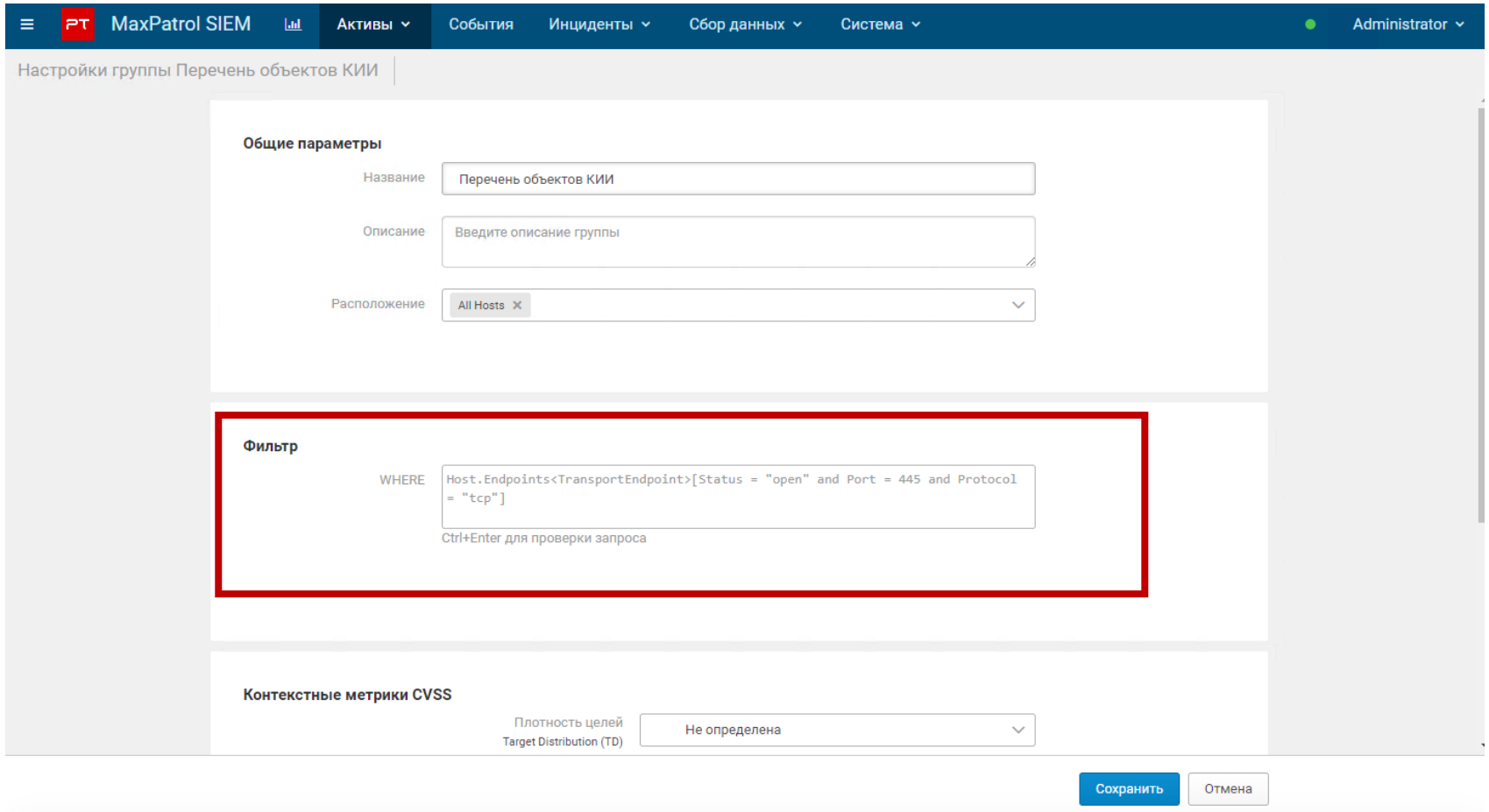
Сбор исходных данных с помощью SIEM



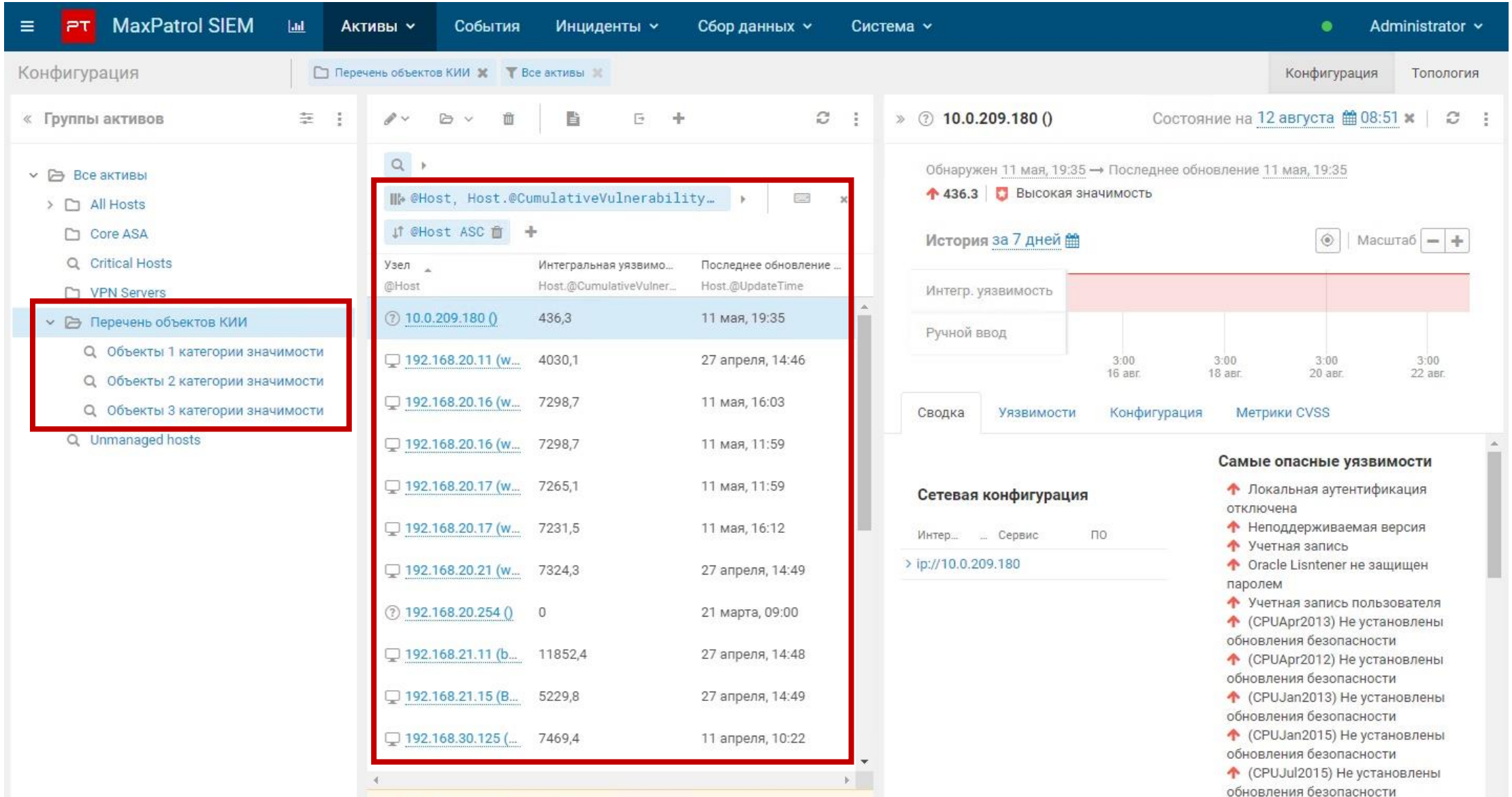
Формирование перечня объектов КИИ



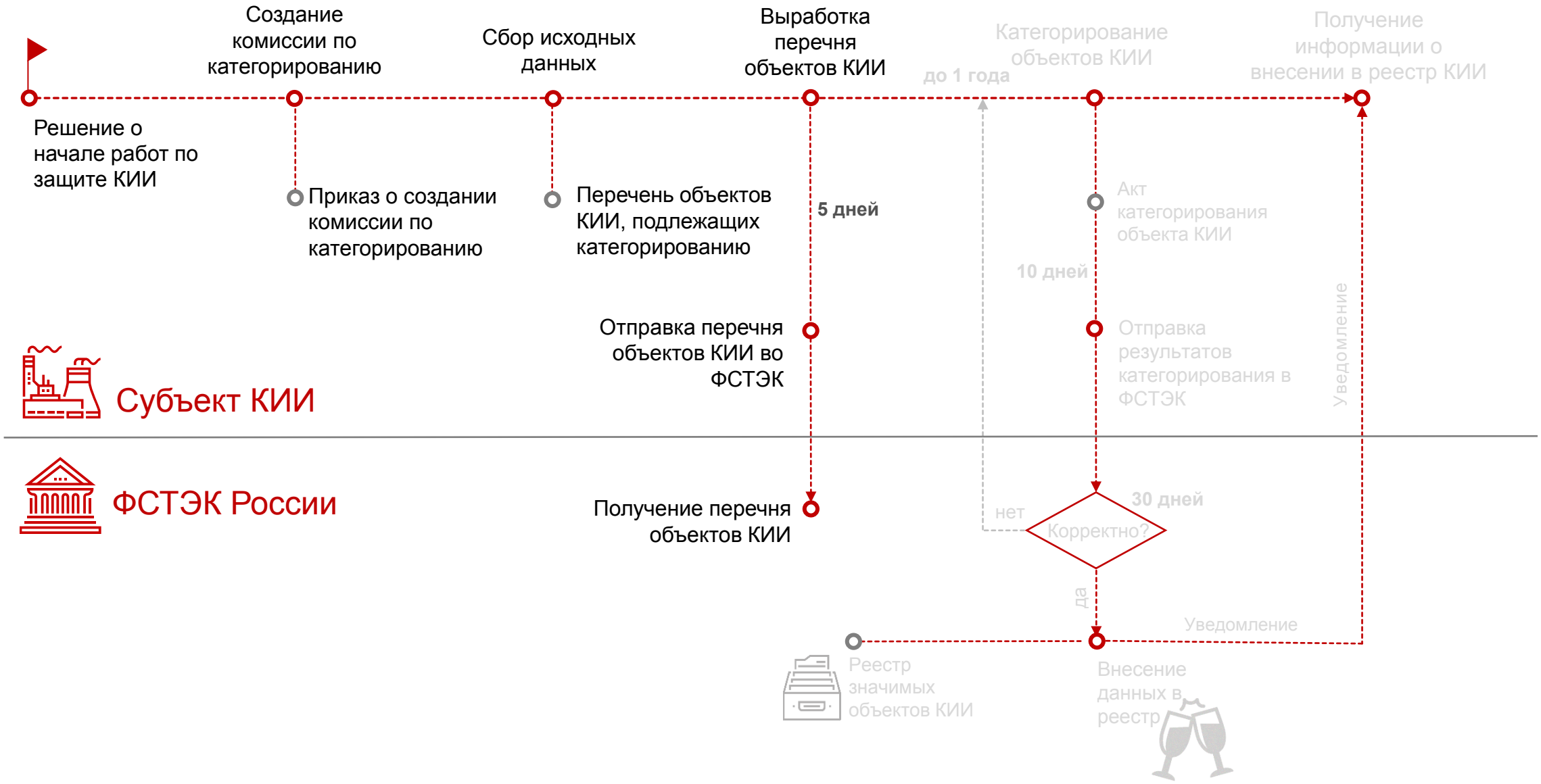
С помощью динамических групп можно сформировать перечень объектов КИИ



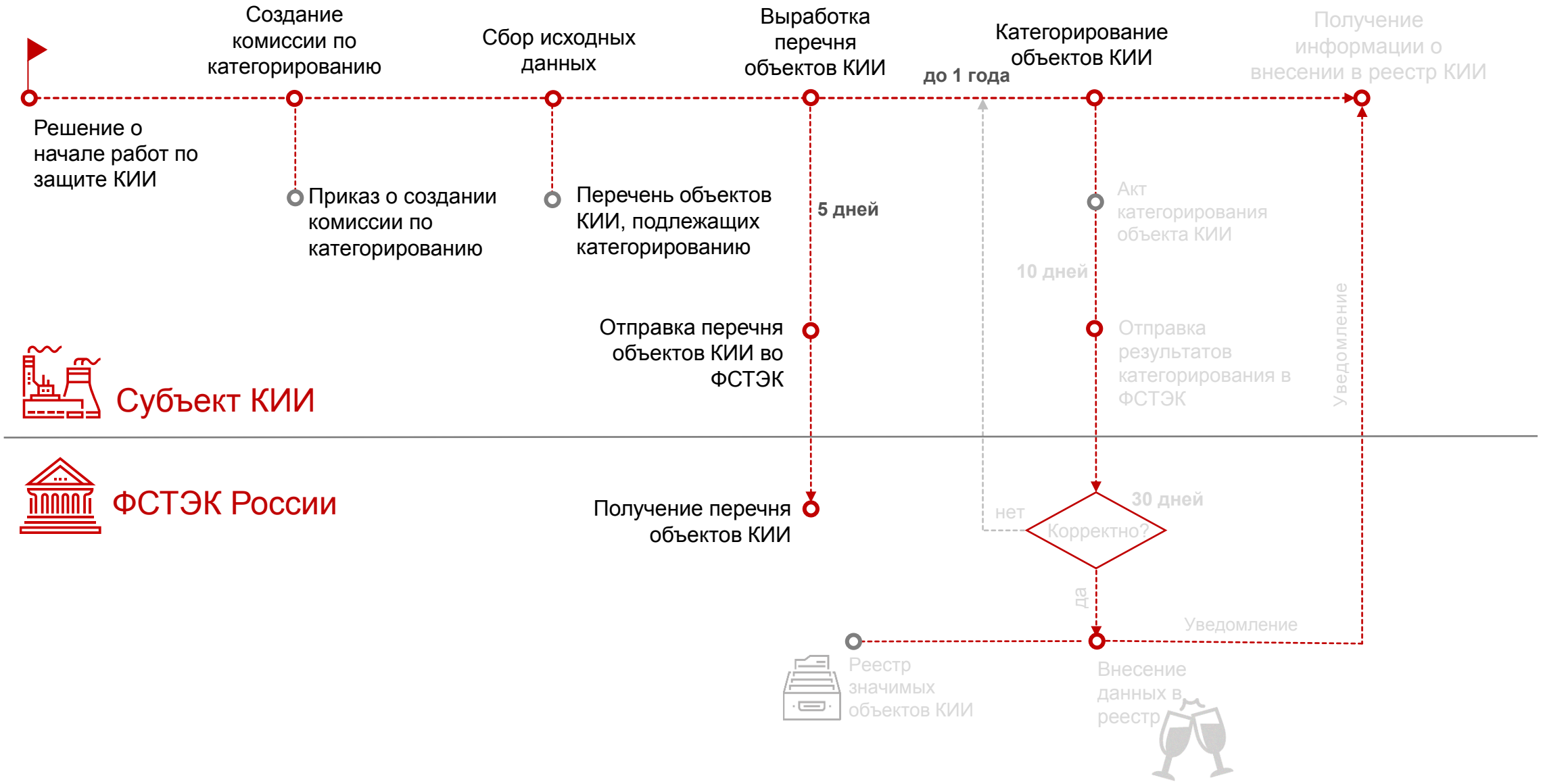
Перечень объектов КИИ по категориям



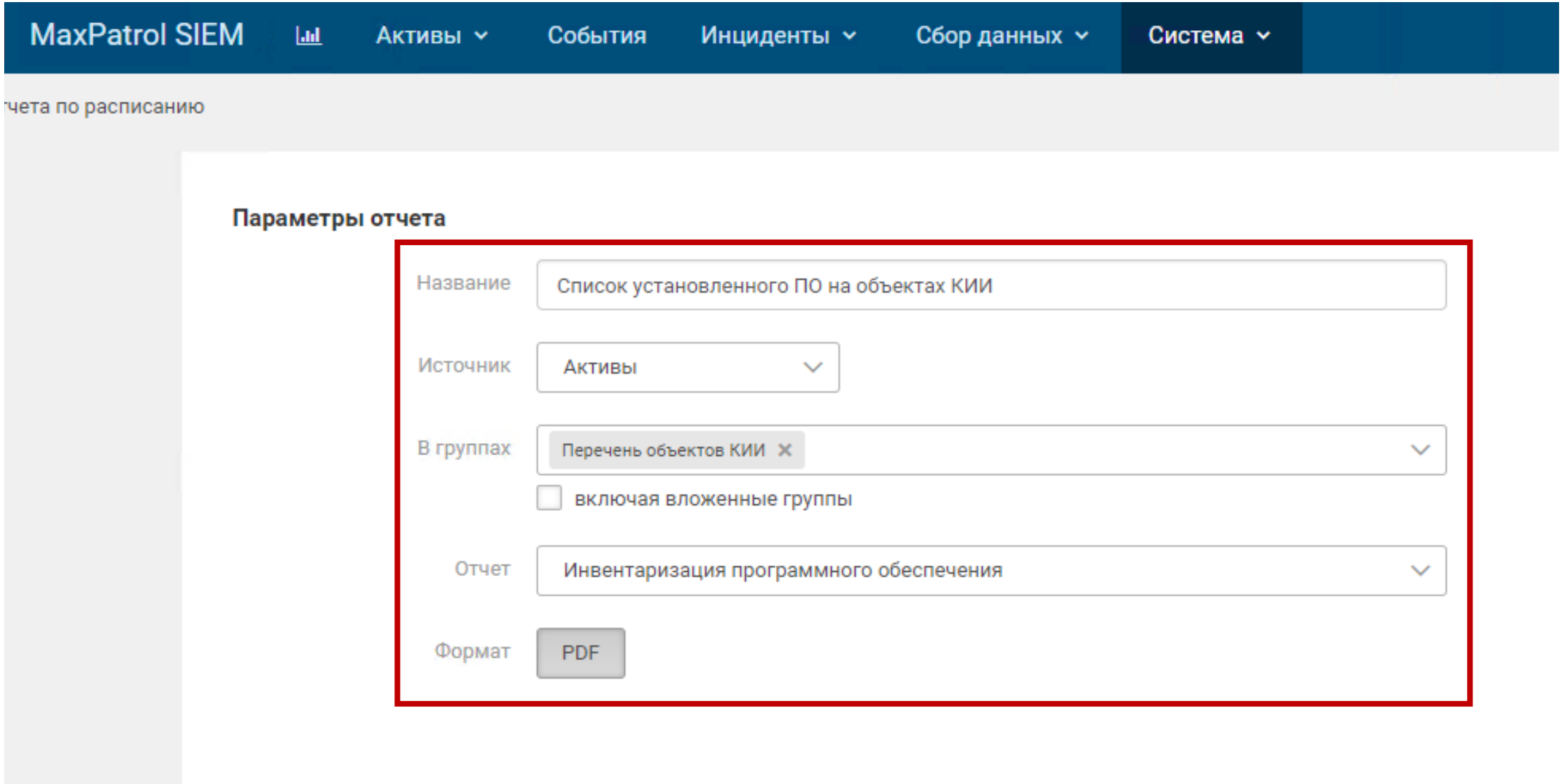
Порядок категорирования объектов КИИ



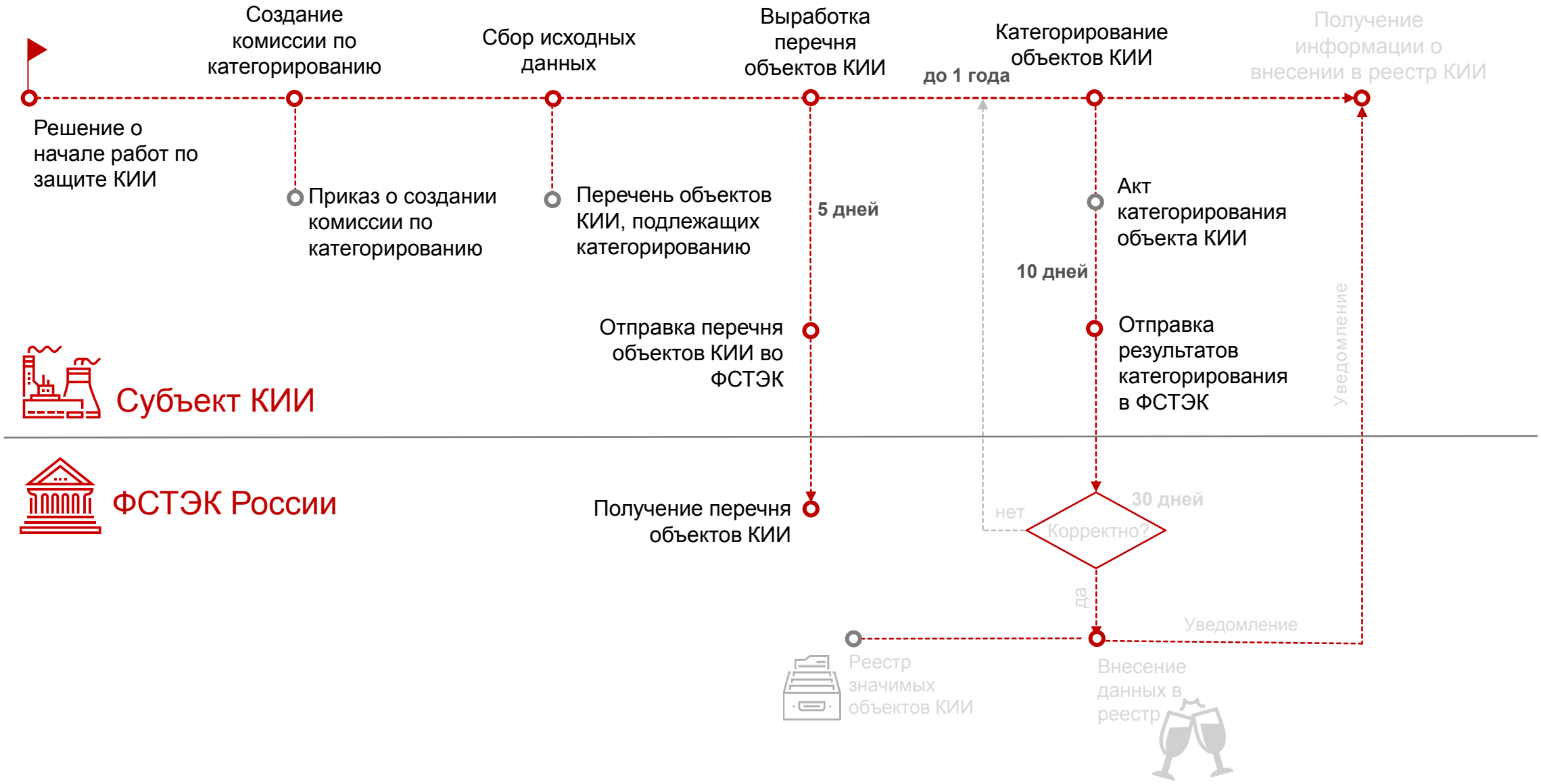
Порядок категорирования объектов КИИ



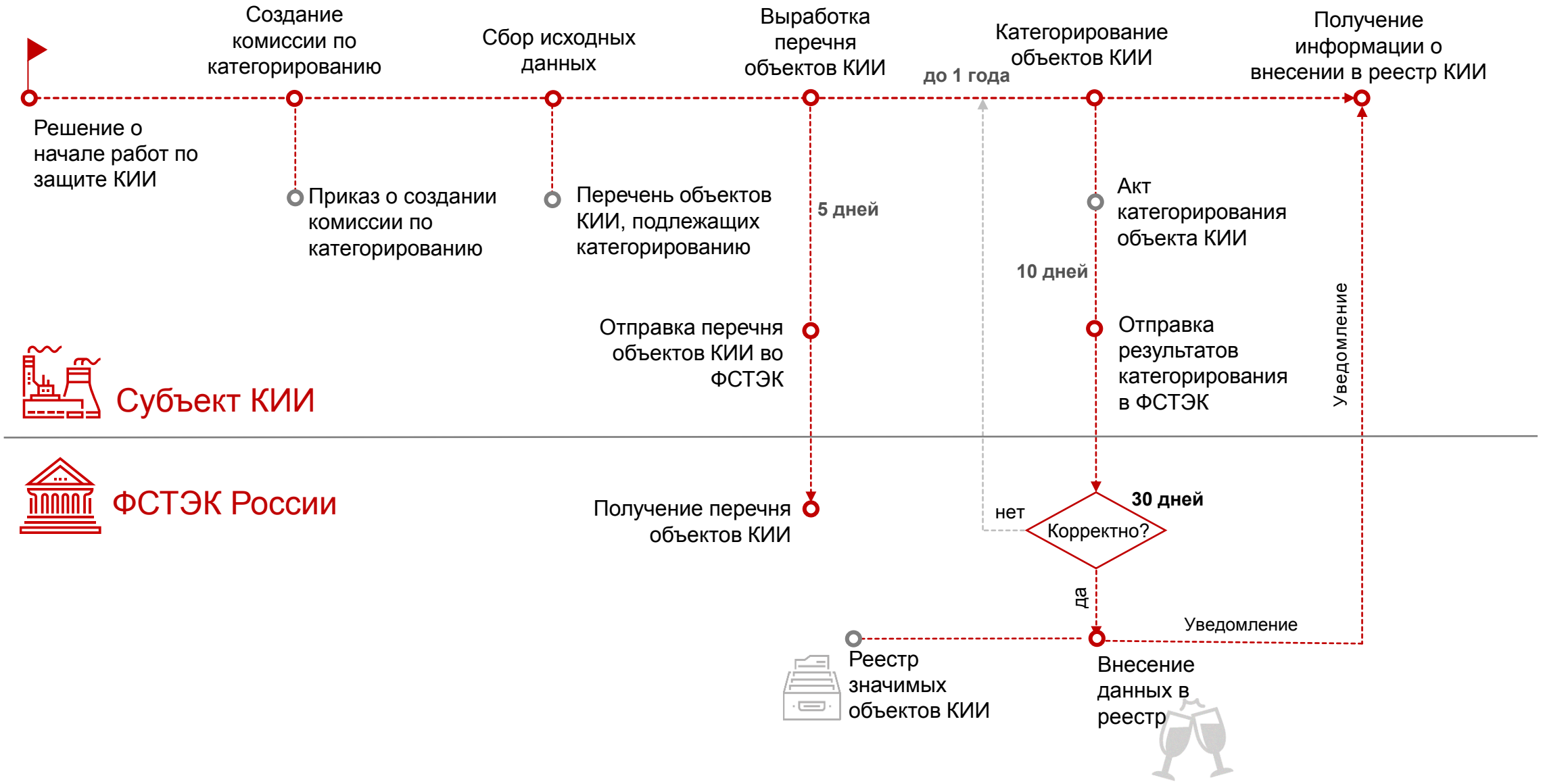
Список установленного ПО на объектах КИИ



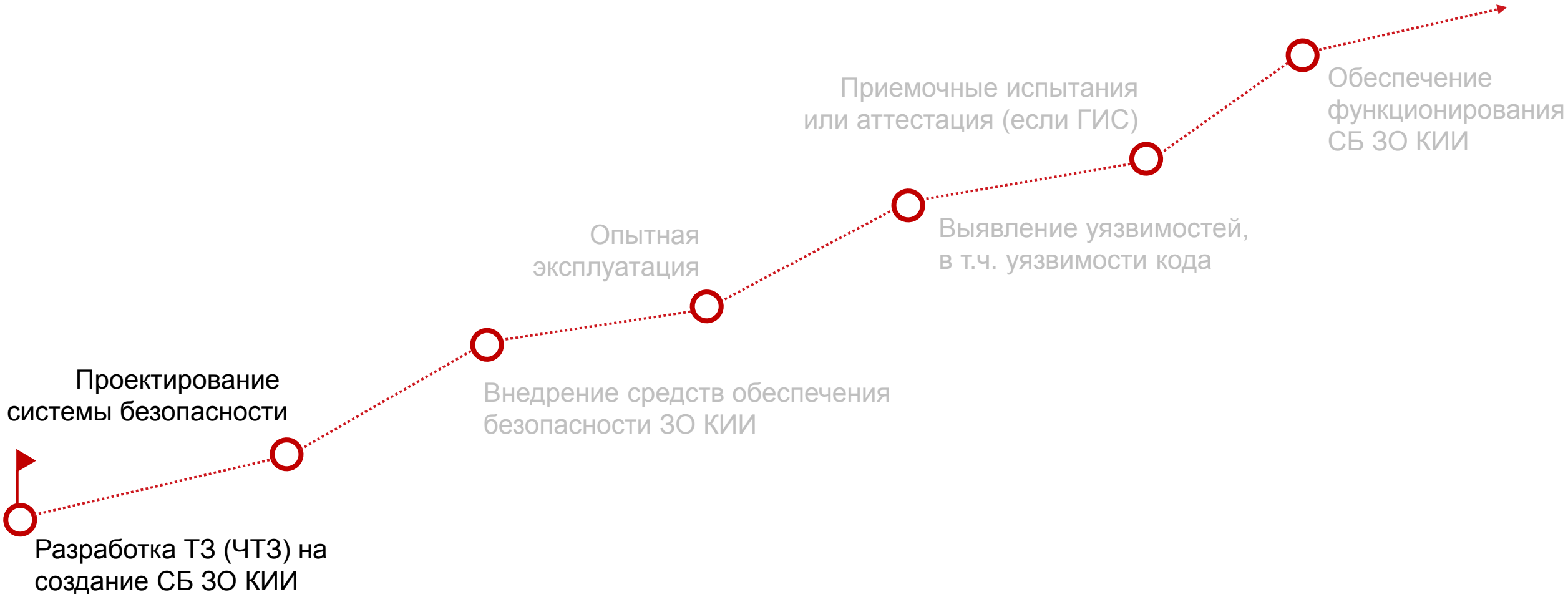
Порядок категорирования объектов КИИ



Порядок категорирования объектов КИИ



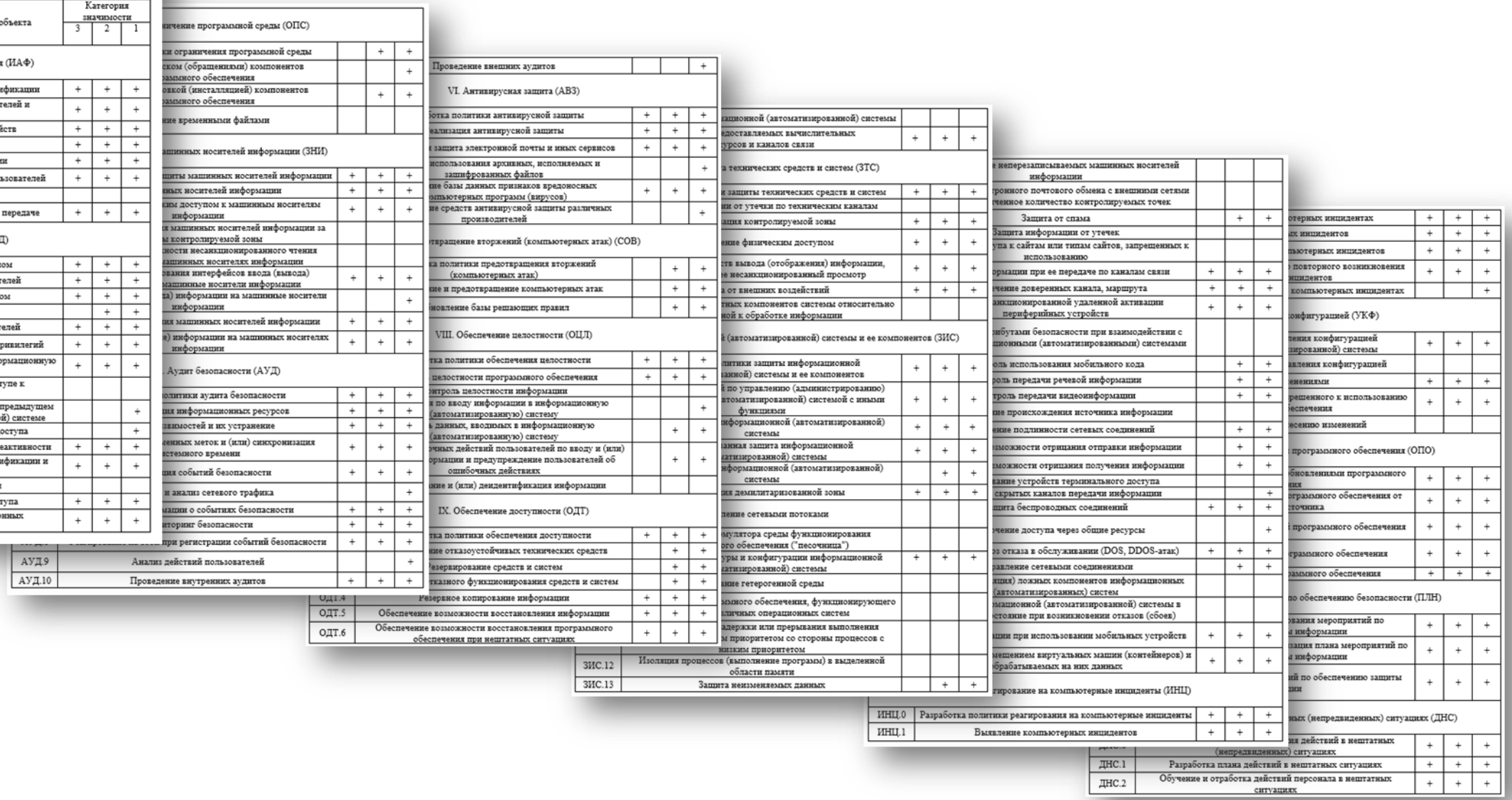
Создание системы безопасности ЗО КИИ



Требования ФСТЭК России (приказ №239): базовый набор мер

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
	I. Идентификация и аутентификация (ИАФ)			
ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
	II. Управление доступом (УПД)			
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступом	+	+	+
УПД.3	Доверенная загрузка		+	+
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам			
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			+
УПД.9	Ограничение числа параллельных сеансов доступа			+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+
УПД.12	Управление атрибутами безопасности			
УПД.13	Реализация защищенного удаленного доступа	+	+	+
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+



Приказ ФСТЭК №239

АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.10	Проведение внутренних аудитов
АУД.11	Проведение внешних аудитов

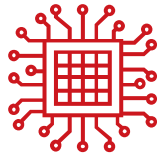
MaxPatrol 8

АУД.1	Инвентаризация информационных ресурсов
АУД.4	Регистрация событий безопасности
АУД.5	Контроль и анализ сетевого трафика
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов

MaxPatrol SIEM

Приказ ФСТЭК №239

АУД.5	Контроль и анализ сетевого трафика
СОВ.1	Обнаружение и предотвращение компьютерных атак
СОВ.2	Обновление базы решающих правил



PT Network Attack Discovery

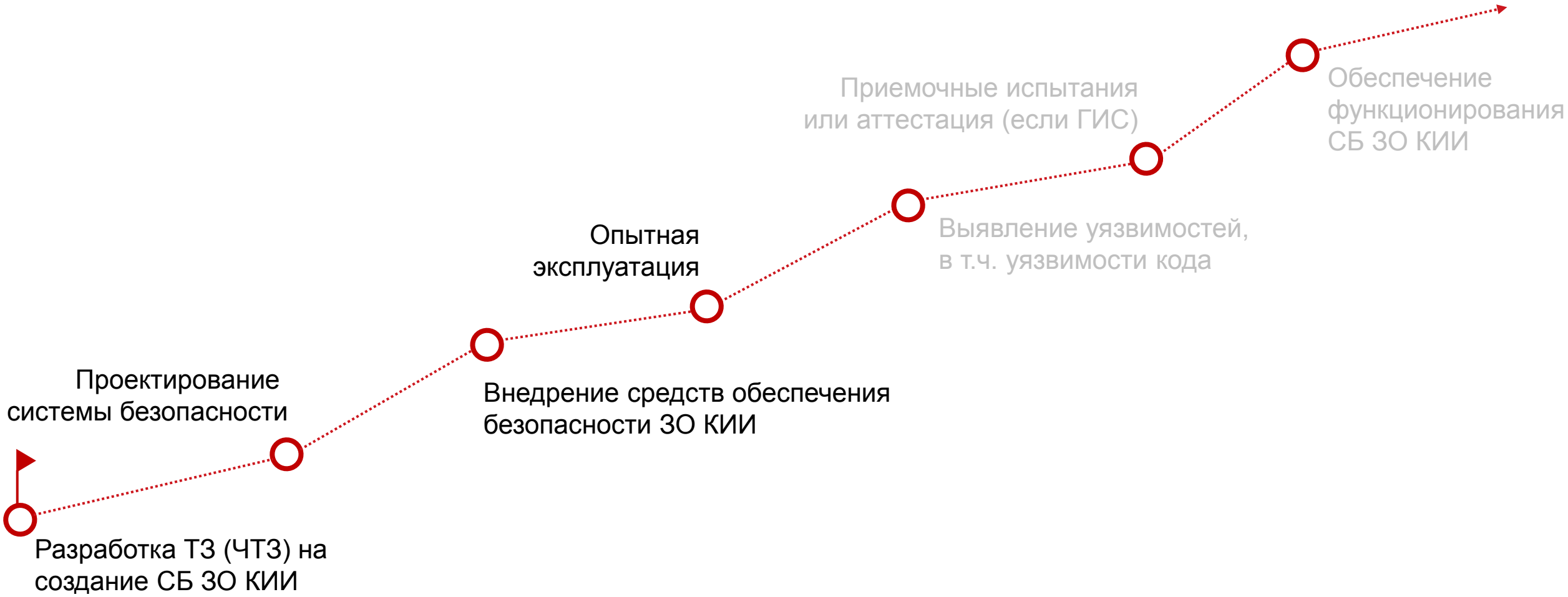
PT ISIM

PT Application Firewall

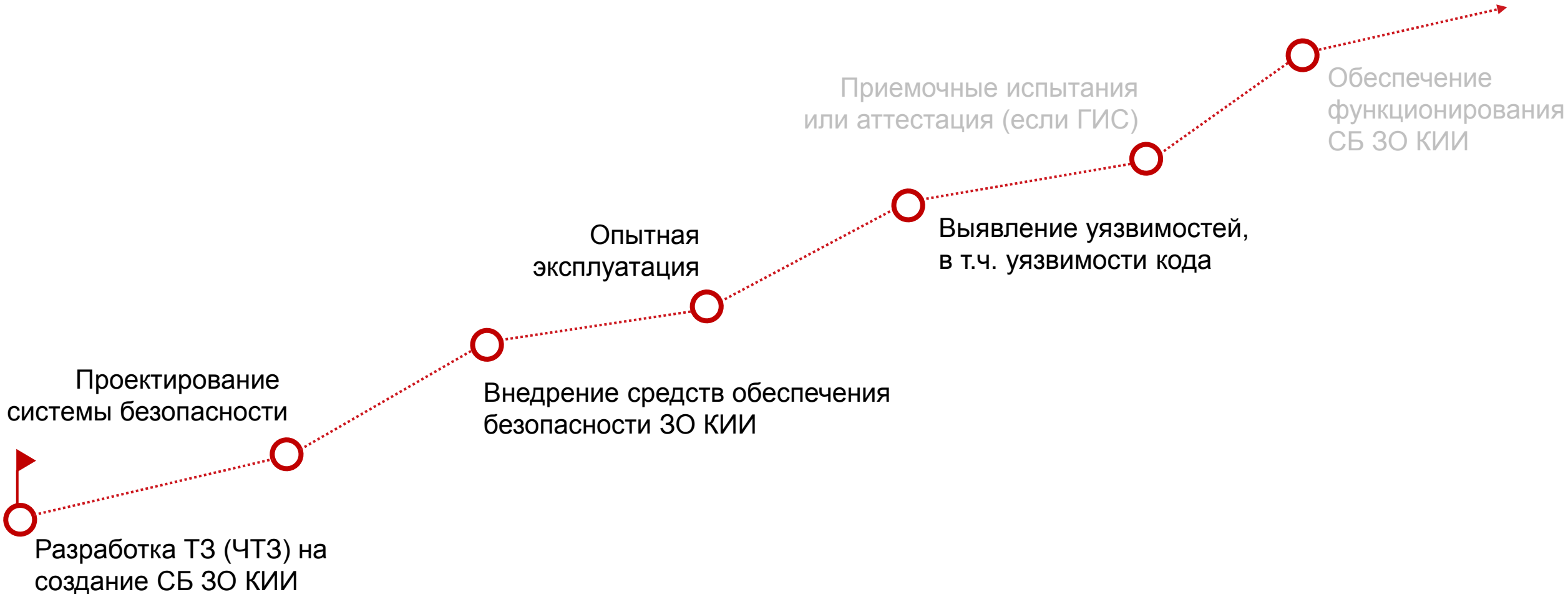
АВЗ.2	Антивирусная защита электронной почты и иных сервисов
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
АВЗ.5	**Использование средств антивирусной защиты различных производителей**
ЗИС.7	**Использование эмулятора среды функционирования программного обеспечения ("песочница")**

PT MultiScanner

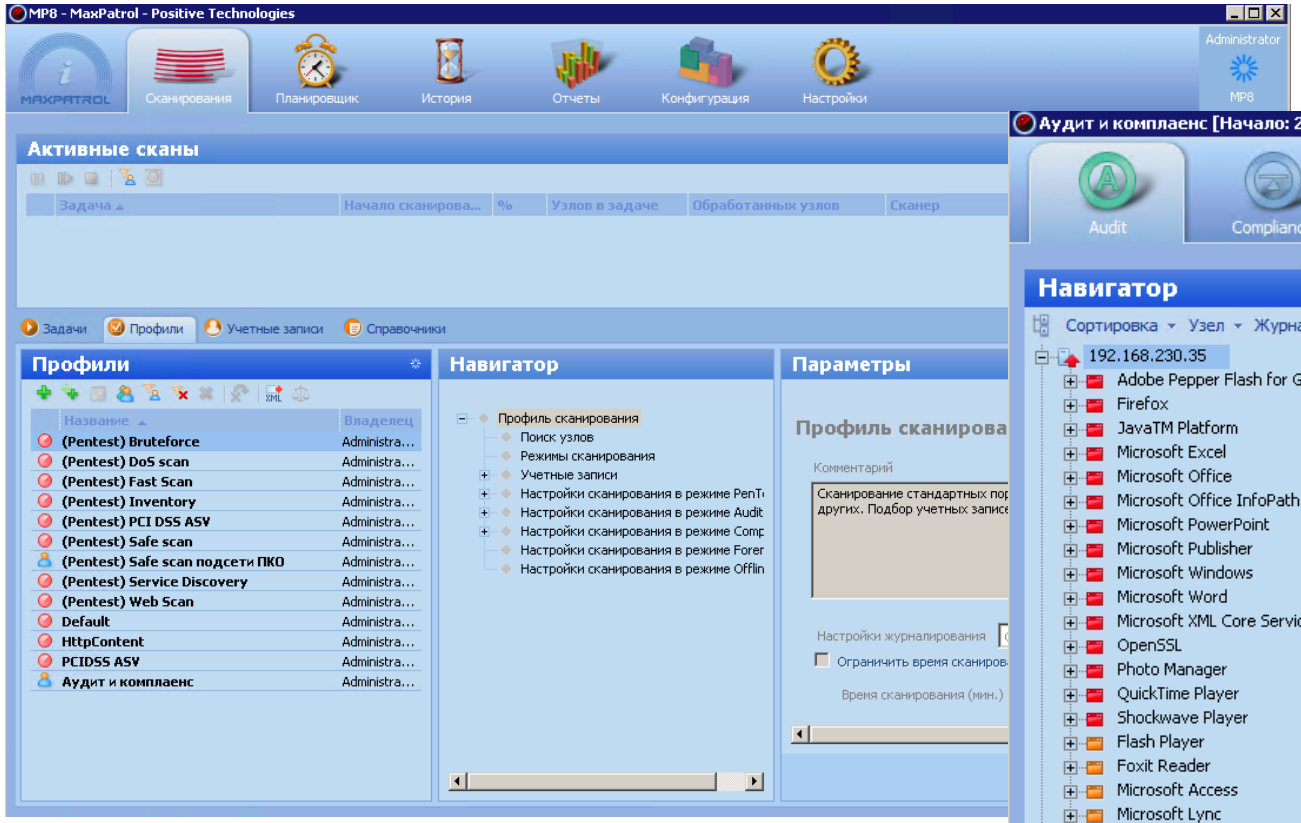
Создание системы безопасности ЗО КИИ

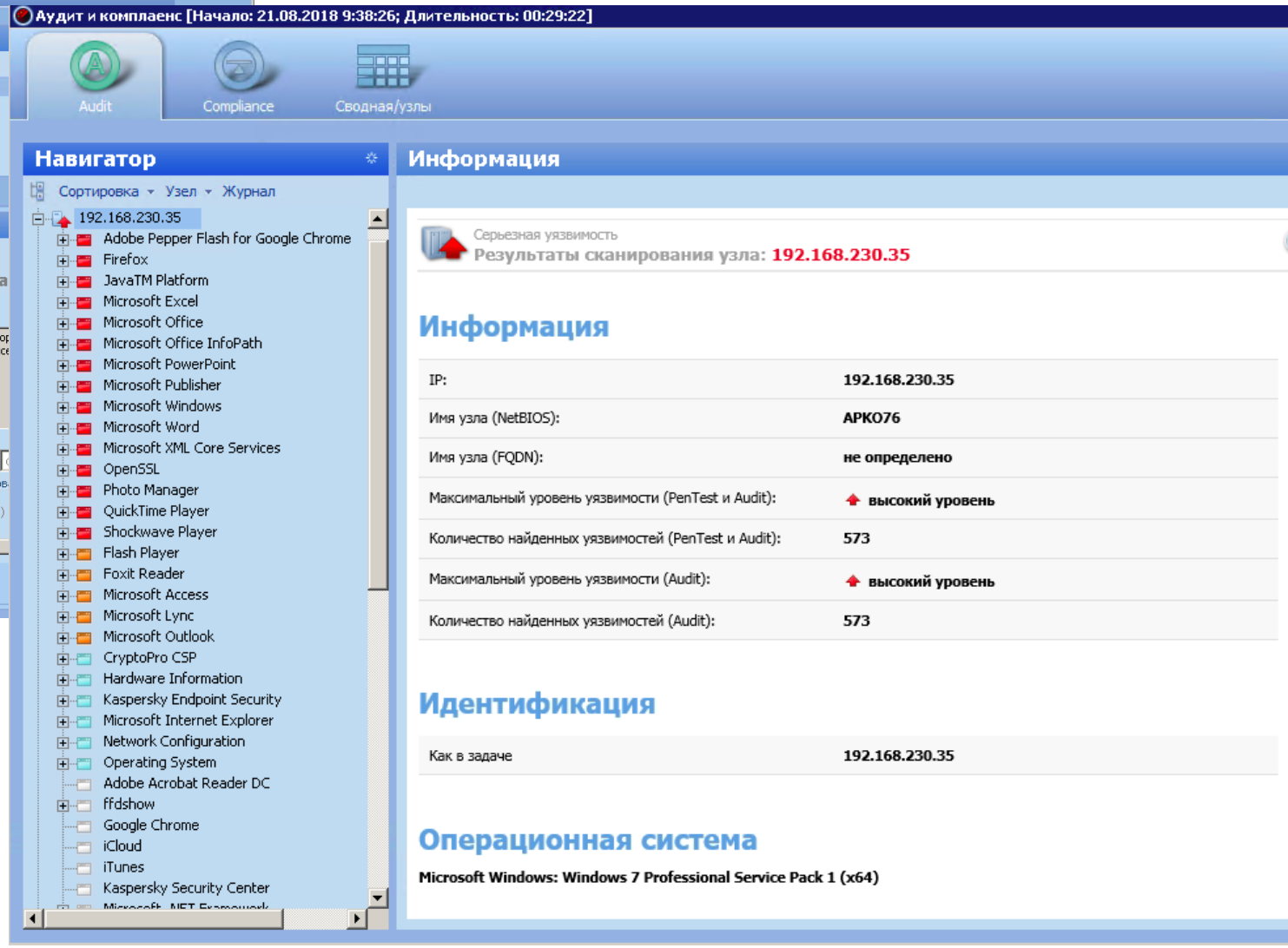


Создание системы безопасности ЗО КИИ



MaxPatrol 8 выявление уязвимостей





- Анализ уязвимостей
- Аудит в режиме – Pentest
- Соответствие стандартам (Compliance)
- Интеграция с БДУ ФСТЭК
- Сертификат ФСТЭК России

Создание системы безопасности ЗО КИИ

Разработка ТЗ (ЧТЗ) на создание СБ ЗО КИИ

Проектирование системы безопасности

Внедрение средств обеспечения безопасности ЗО КИИ

Опытная эксплуатация

Выявление уязвимостей, в т.ч. уязвимости кода

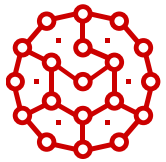
Приемочные испытания или аттестация (если ГИС)

Обеспечение функционирования СБ ЗО КИИ

Задачи по 187-ФЗ

Защита от неправомерного доступа к информации, обрабатываемой КИИ

Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ



Восстановление функционирования объекта КИИ

Непрерывное взаимодействие с **ГосСОПКА**

Взаимодействуй с ГосСОПКА

Информирование НКЦКИ

об инцидентах

Обмен информацией

об инцидентах между субъектами КИИ

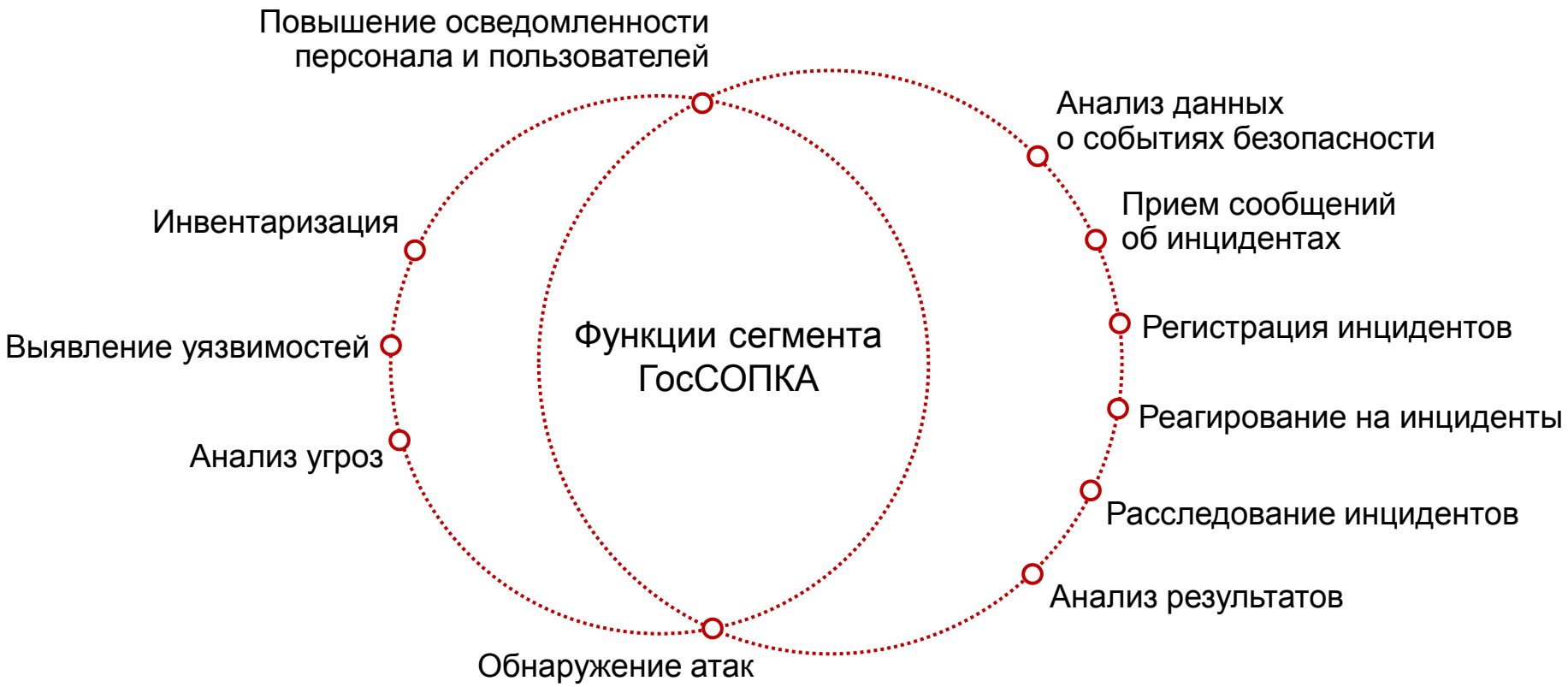
Получение рассылок от НКЦКИ

об инцидентах, средствах и способах проведения атак

На чём в первую очередь необходимо сконцентрировать усилия. Первое – это совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России.

В. Путин
Заседание Совета Безопасности Российской Федерации
26.10.2017 г.

Функции и построение центров ГосСОПКА



MaxPatrol 8

MaxPatrol SIEM

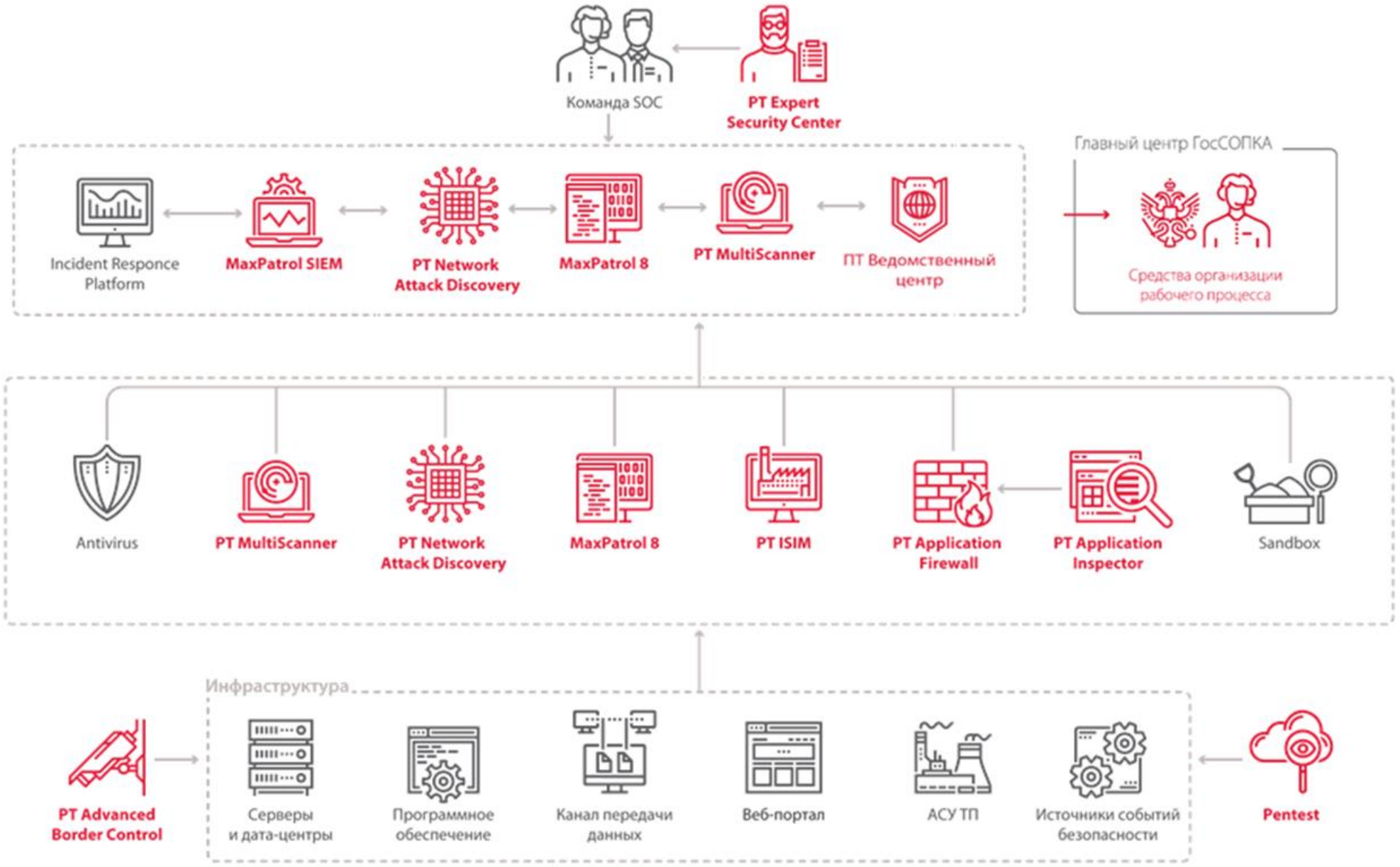
MaxPatrol SIEM

ПТ Ведомственный центр

PT MultiScanner

PT Network Attack Discovery

Позитивная архитектура центров ГосСОПКА



POSITIVE TECHNOLOGIES

Что делать организациям с более ограниченными ресурсами (кадры, деньги, время)?

POSITIVE TECHNOLOGIES

PT Platform 187

Состав

MaxPatrol SIEM

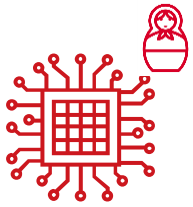
Система мониторинга событий и выявления инцидентов

MaxPatrol 8

Система контроля защищенности

PT MultiScanner

Система выявления вредоносного контента



PT Network Attack Discovery

Система комплексного анализа сетевого трафика

ПТ Ведомственный центр

Система управления инцидентами и взаимодействия с НКЦКИ

Опциональное подключение:

+ PT ISIM
+ PT Application Firewall
+ PT Application Inspector
+ Доп. хранилище до 36 ТБ

Ограничения

до 250 узлов

включаются в мониторинг MaxPatrol SIEM и MaxPatrol 8

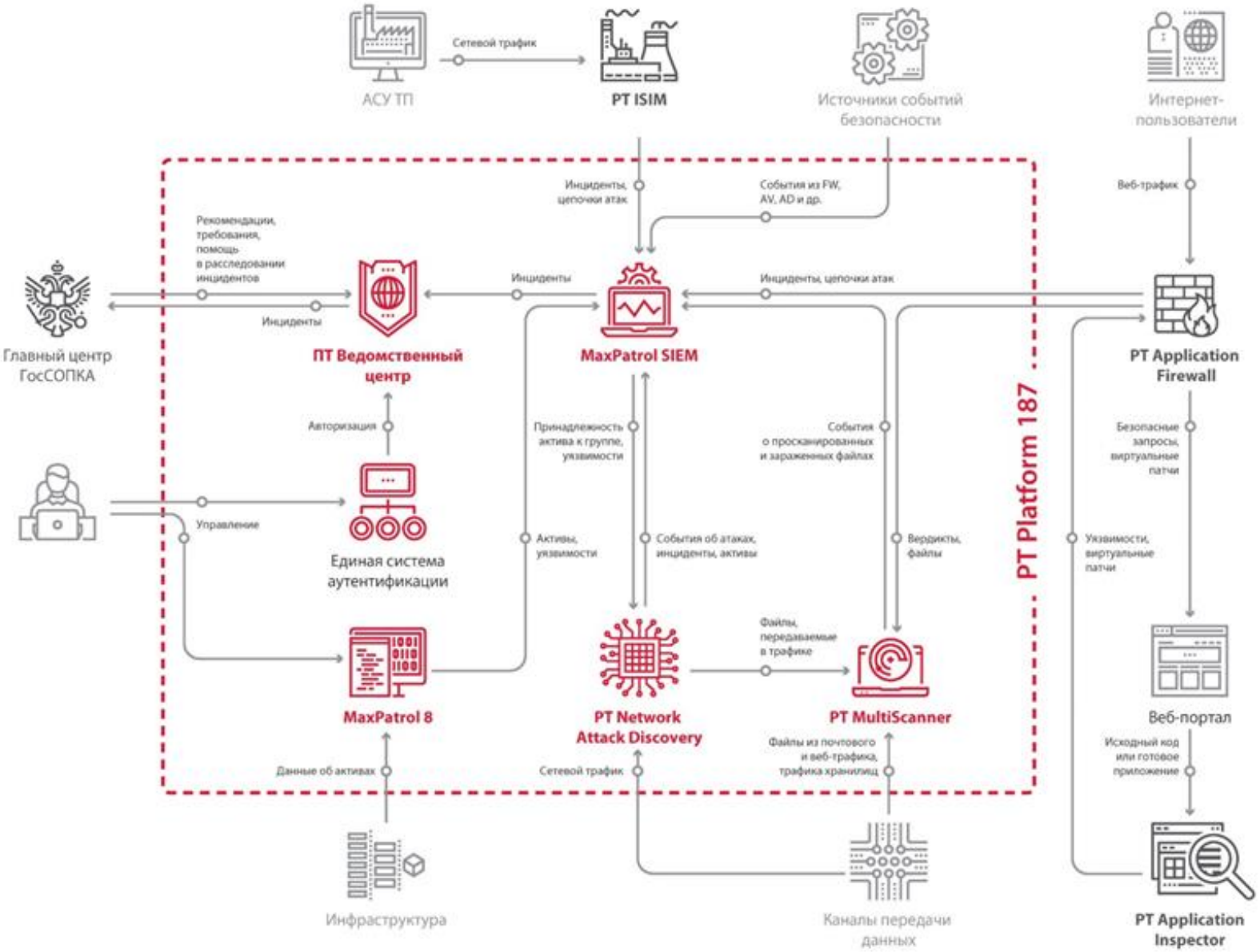
до 100 Мбит/с

пропускная способность PT Network Attack Discovery

до 3000 FPH

пропускная способность PT MultiScanner

Архитектура Platform 187



POSITIVE TECHNOLOGIES

Позитивные результаты

Истории успеха

7 рабочих дней - Platform 187 **настраивают инженеры Positive Technologies**

3 патч-корда - для работы сервера
- *SPAN*
- *iDRAC*
- *Интерфейс управления*

1 месяц - время опытной эксплуатации

5 рабочих дней – чтобы разобраться с базовыми принципами работы продуктов

8 рабочих дней – срок обучения по продуктам Platform 187 в авторизованном учебном центре

Кейс: подготовка инфраструктуры Заказчика

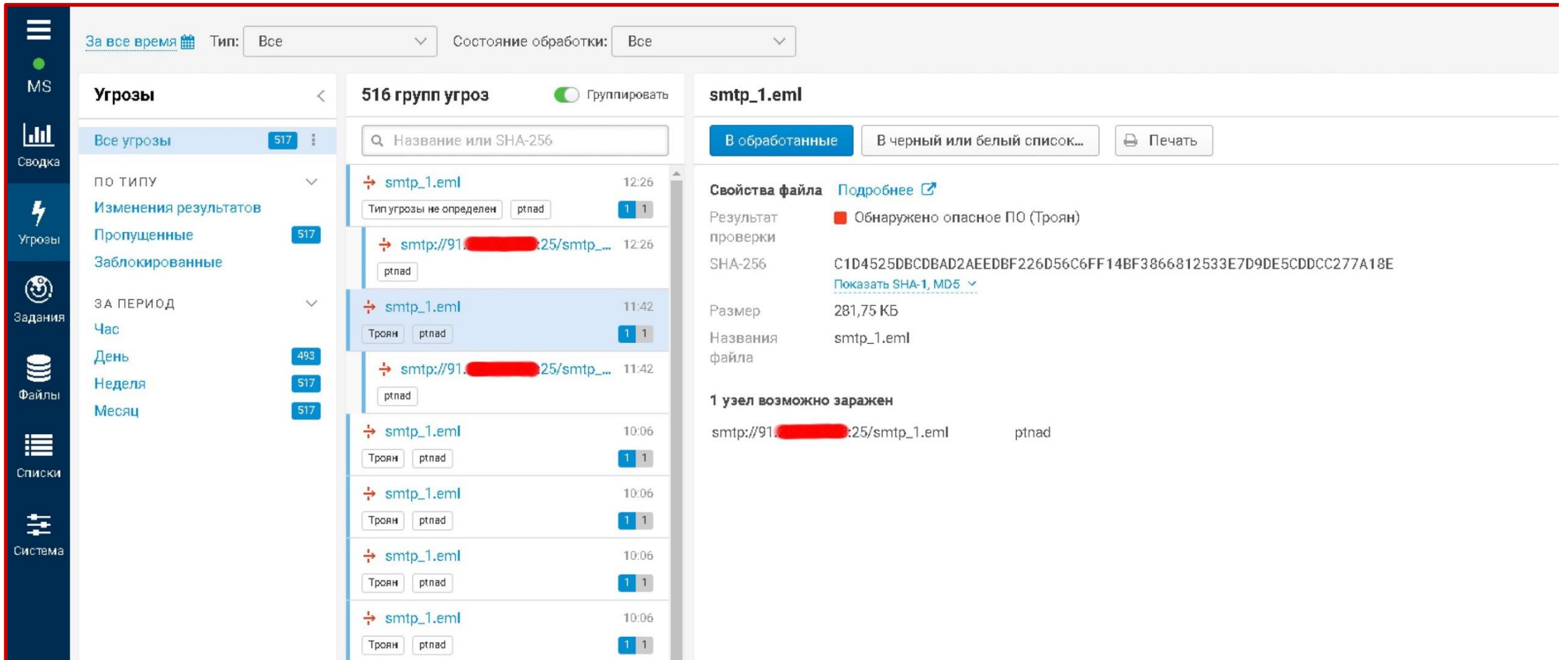
Месяц на подготовку Заказчиком инфраструктуры для пилота

- создание правил доступа МЭ
- настройка активного сетевого оборудования

Типичная проблема – война между ИБ и ИТ департаментами

Признаки ВПО

В первый день работы **PT MultiScanner** обнаружил **493** объекта **ВПО**

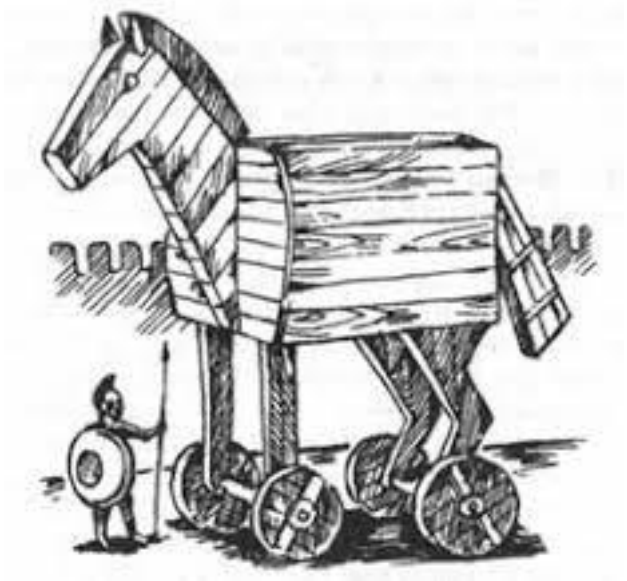


Выявленные атаки

Первая неделя работы Platform 187

Активность вредоносного ПО

- Активность банковского **трояна RTM** и IP адреса C&C
- попытки эксплуатации уязвимости **MS17-010 (CVE-2017-0144)**



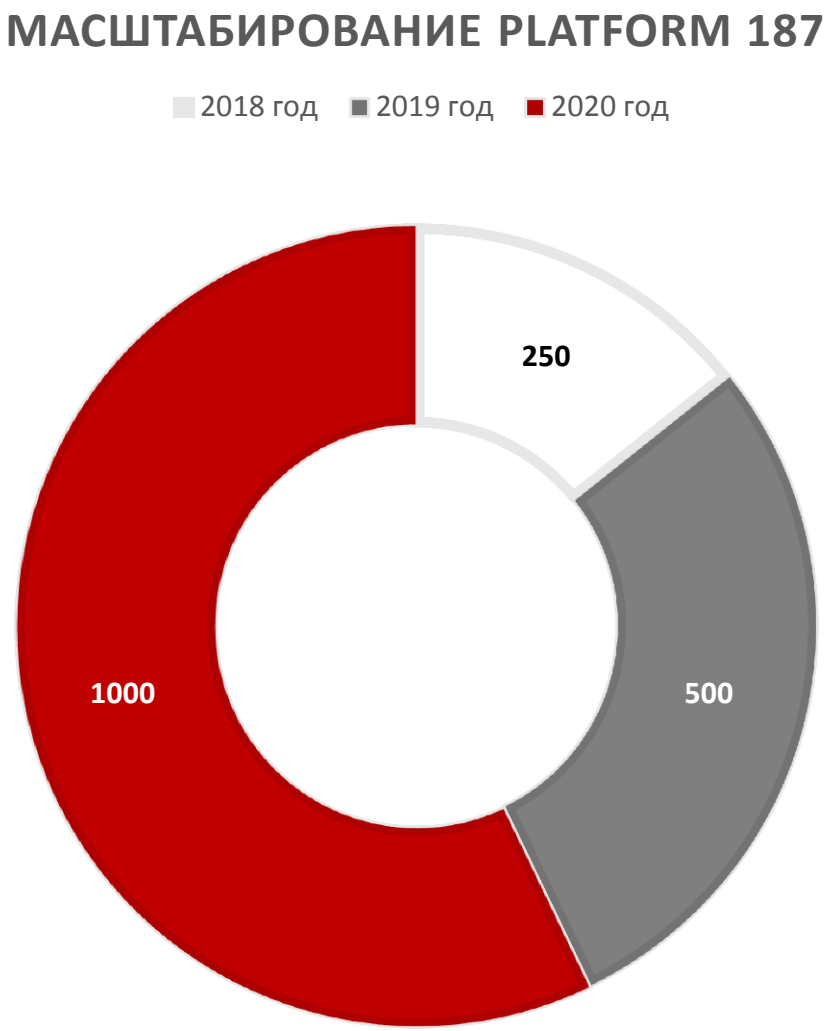
Нарушение регламента ИБ

- активность ПО **TeamViewer**
- активность ПО **Ammy Admin, AeroAdmin**
- использование **FriGate proxy**
- Выгрузка пользователей с контроллера домена по протоколу **SAMR**

POSITIVE TECHNOLOGIES

Планы по развитию центра

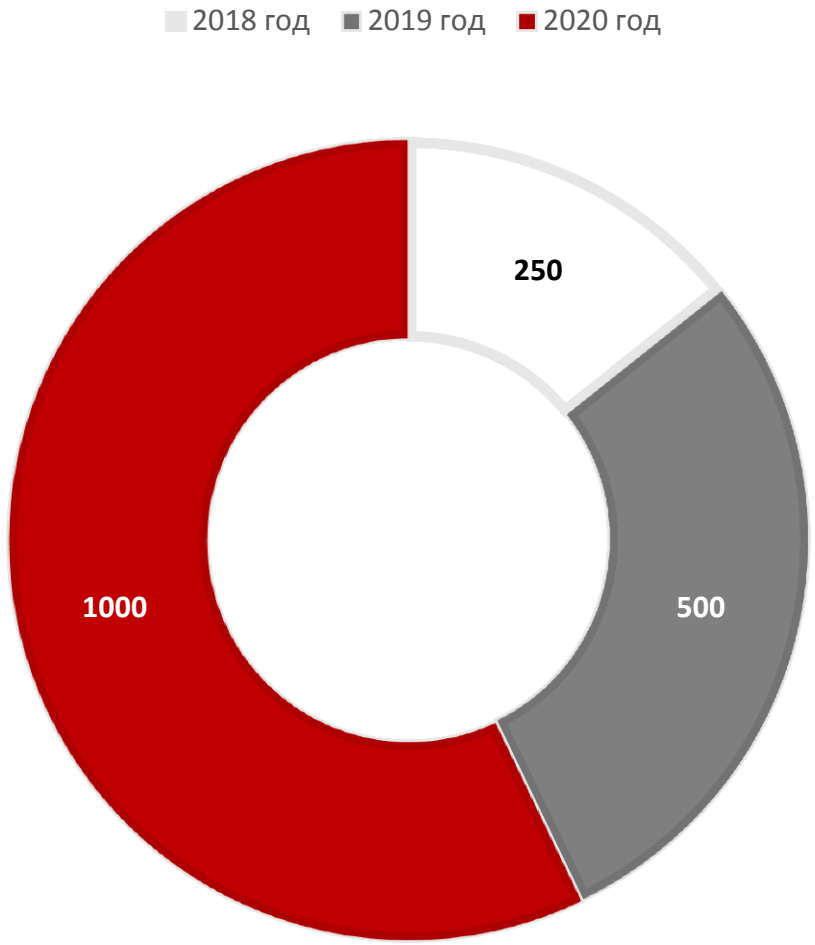
Развитие центра: 1 задача



Развитие центра: 2 задача

Результат

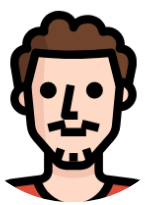
МАСШТАБИРОВАНИЕ PLATFORM 187



ЛИНИИ МОНИТОРИНГА И РЕАГИРОВАНИЯ

Персонал центра

Руководитель SOC



1-я линия:
Первичная оценка инцидентов, отработка ложных срабатываний, обработка по плейбукам

2-я линия:
Глубокое расследование инцидентов

3-я линия:
Глубокий анализ артефактов инцидентов

Аналитики:
Написание плейбуков, внутренний TI

Жизненный цикл реагирования

2018 год

Зоны непосредственного участия экспертов PT

Источник: Модель управления жизненным циклом инцидента (NIST, SANS)

Жизненный цикл реагирования

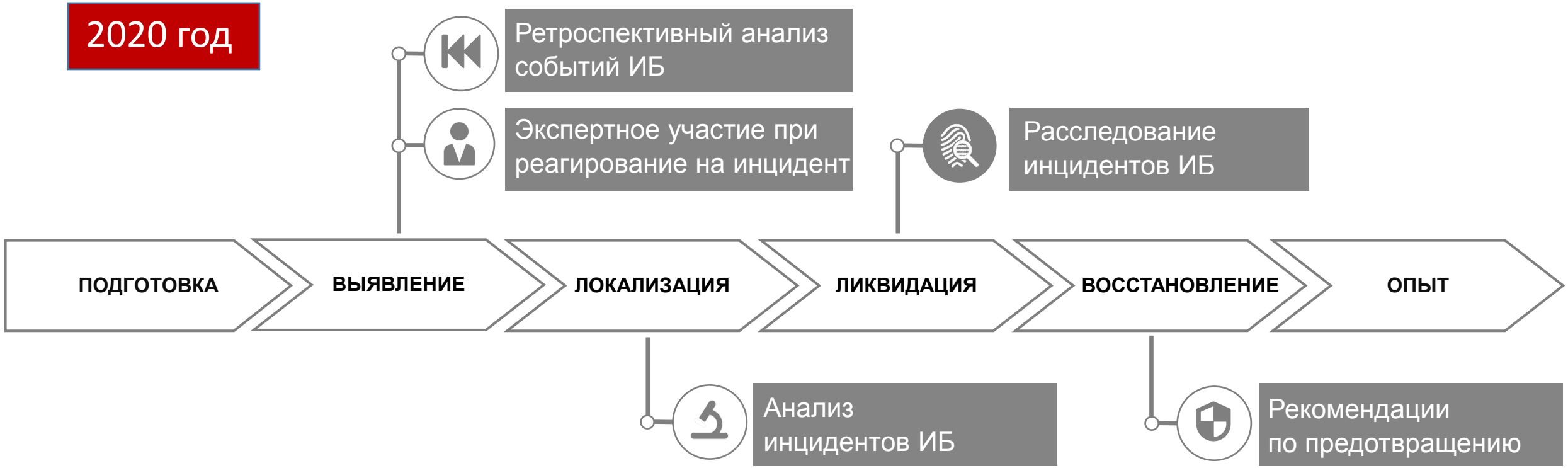
2019 год

Зоны непосредственного участия экспертов PT

Источник: Модель управления жизненным циклом инцидента (NIST, SANS)

Жизненный цикл реагирования

2020 год



Зоны непосредственного участия экспертов PT

Источник: Модель управления жизненным циклом инцидента (NIST, SANS)

POSITIVE TECHNOLOGIES

Интернет ресурсы

План действий

https://www.ptsecurity.com/ru-ru/premium/plan-187-fz/?utm_source=product_page

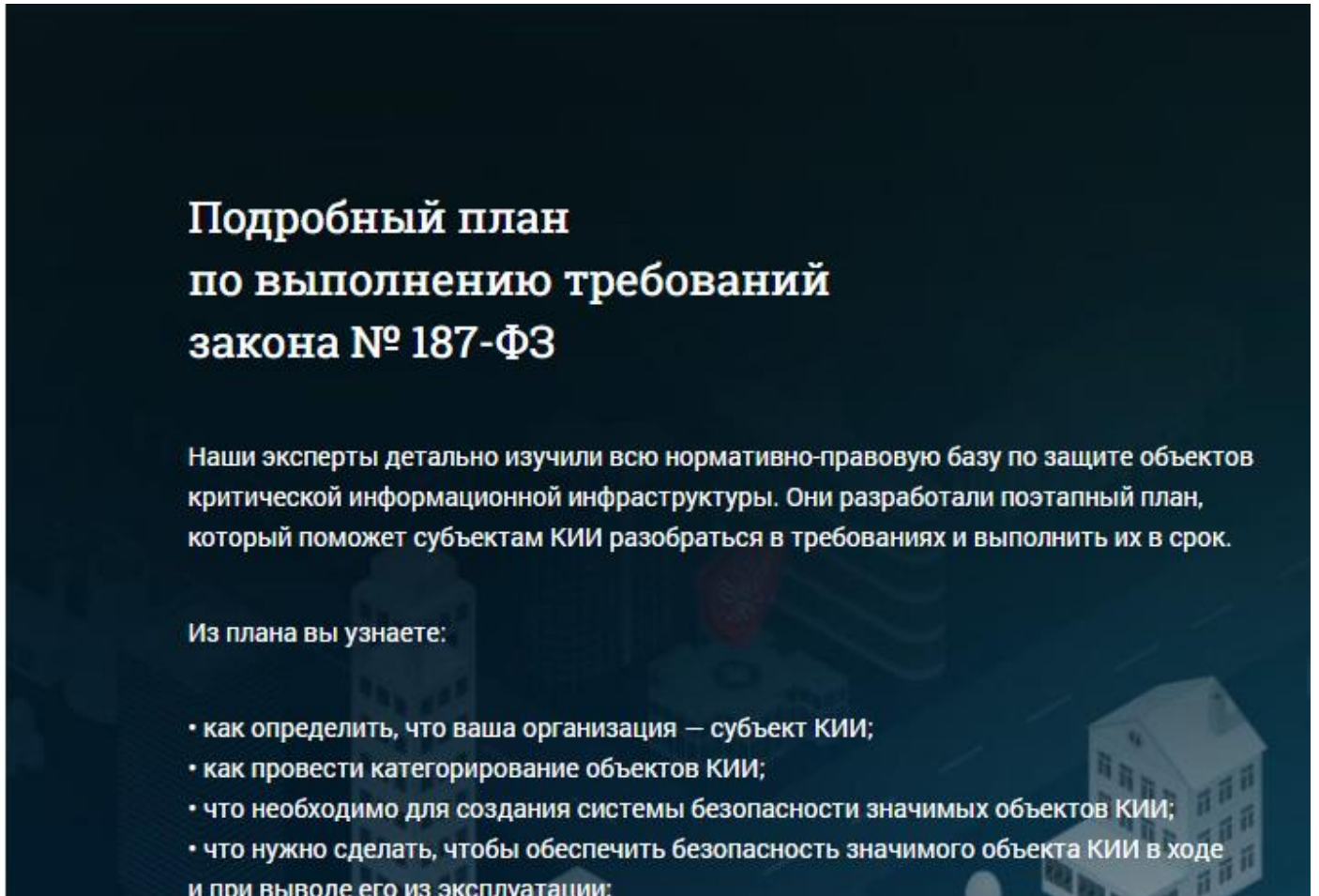
Заполните поля со звездочкой

Имя и фамилия*

Компания*

Должность*

Электронная почта*



Вебинары

Все, что вы хотели знать о ГосСОПКА

https://www.ptsecurity.com/ru-ru/research/webinar/296412/

Порядок выполнения требований 187-ФЗ: пошаговая инструкция

https://www.ptsecurity.com/ru-ru/research/webinar/295156/

PT Platform 187: обеспечение безопасности объектов КИИ для небольших инфраструктур

https://www.ptsecurity.com/ru-ru/research/webinar/292292/

POSITIVE TECHNOLOGIES

Спасибо за внимание