

POSITIVE TECHNOLOGIES

Ильяс Киреев

Продвижение и развитие продуктов

Обеспечение соответствия 187-ФЗ: практический опыт



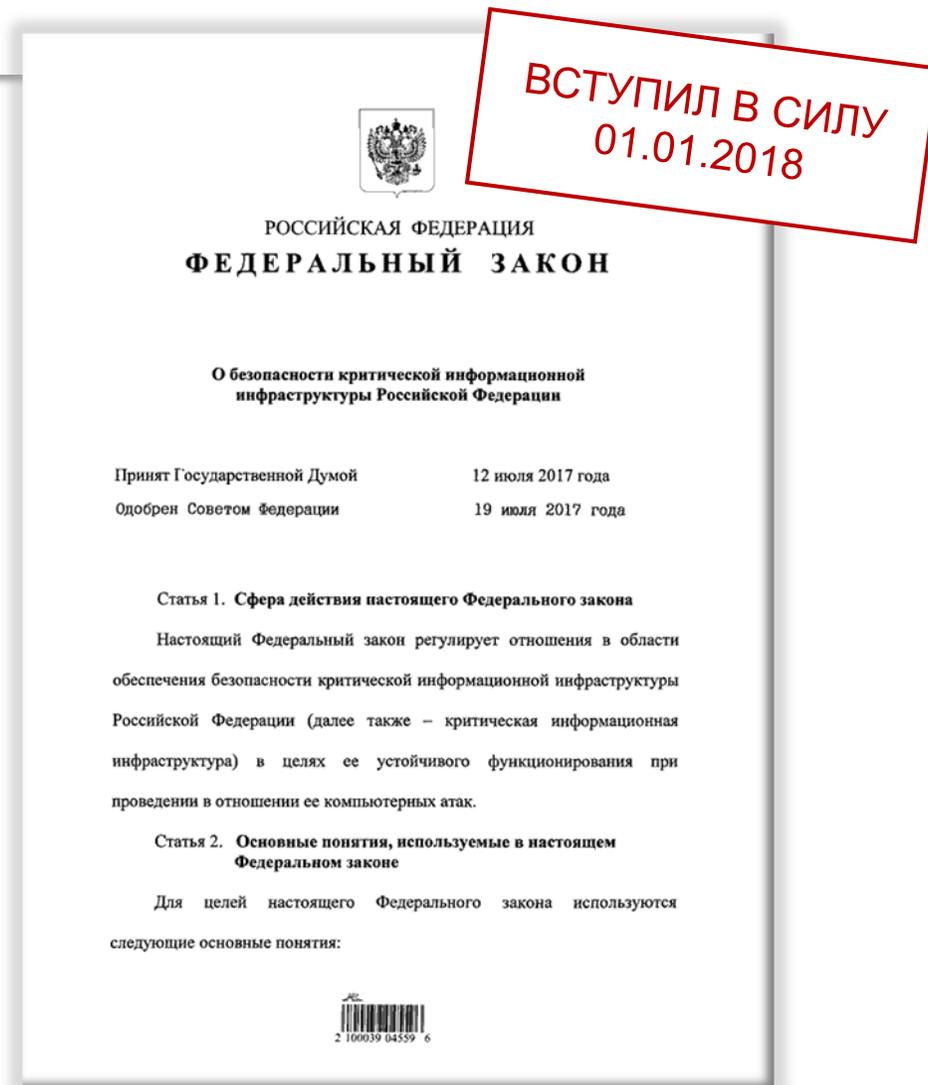
ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

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

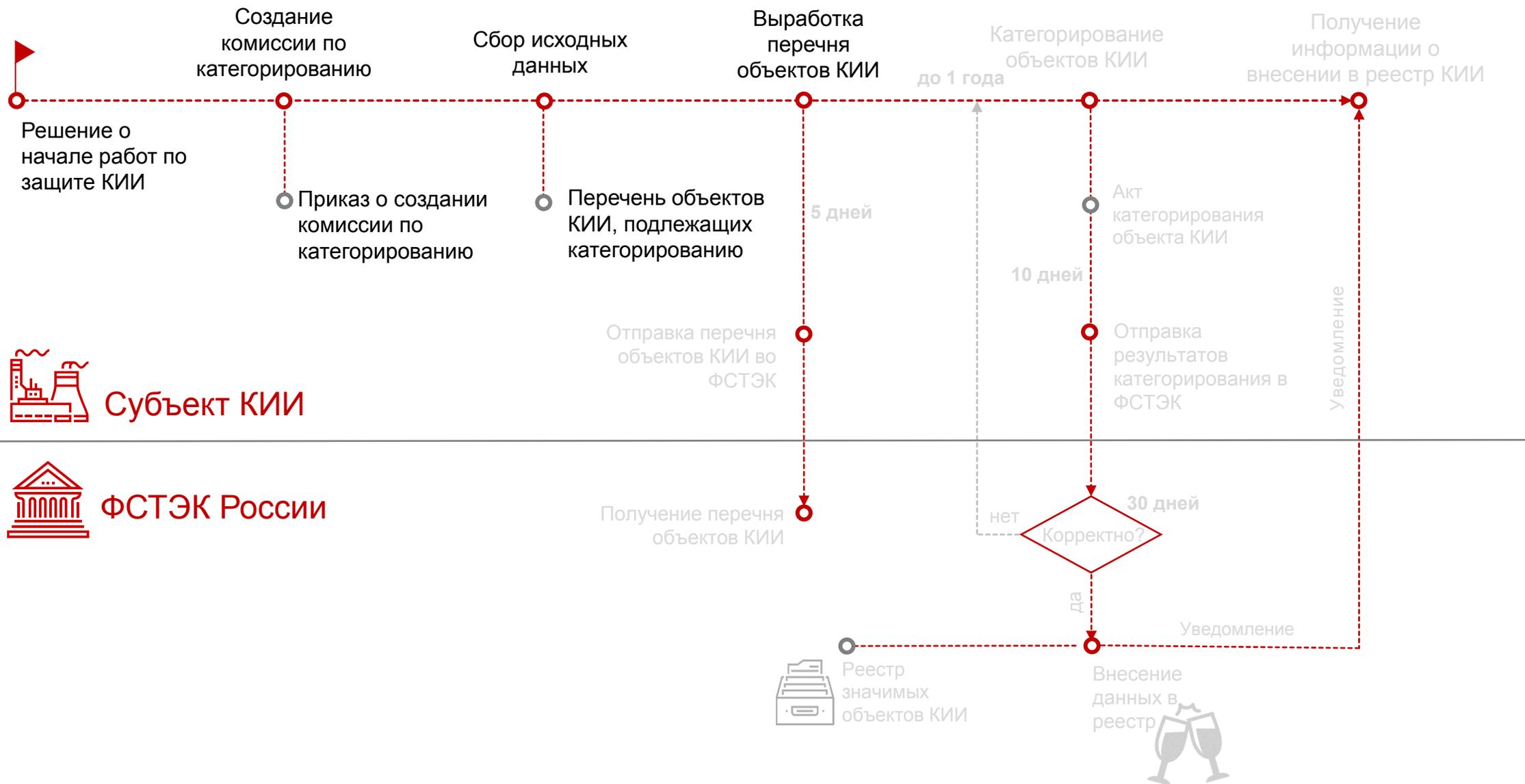
Объекты КИИ - ИС, ИТС, АСУ в сферах:



...3 категории значимых объектов КИИ...”



Порядок категорирования объектов КИИ



Сбор исходных данных с помощью SIEM



MaxPatrol SIEM

Активы ▾ События ▾ Инциденты ▾ Сбор данных ▾ Система ▾ Administrator ▾

Конфигурация

Hosts x Все активы x

Конфигурация Топология

Группы активов

- Все активы
 - All Hosts
 - 445 port
 - AD controllers
 - Antivirus Win
 - CPU x86
 - CVE 2017-0199
 - CVE до 2016
 - Database Servers
 - Device
 - Hosts
 - 22 closed
 - 22 open
 - Admin Allowed
 - By Port 80
 - DMZ Network
 - EternalBlue
 - From mp8
 - heartbleed
 - Hosts without ac...
 - IOS Hosts
 - Linux

Узел

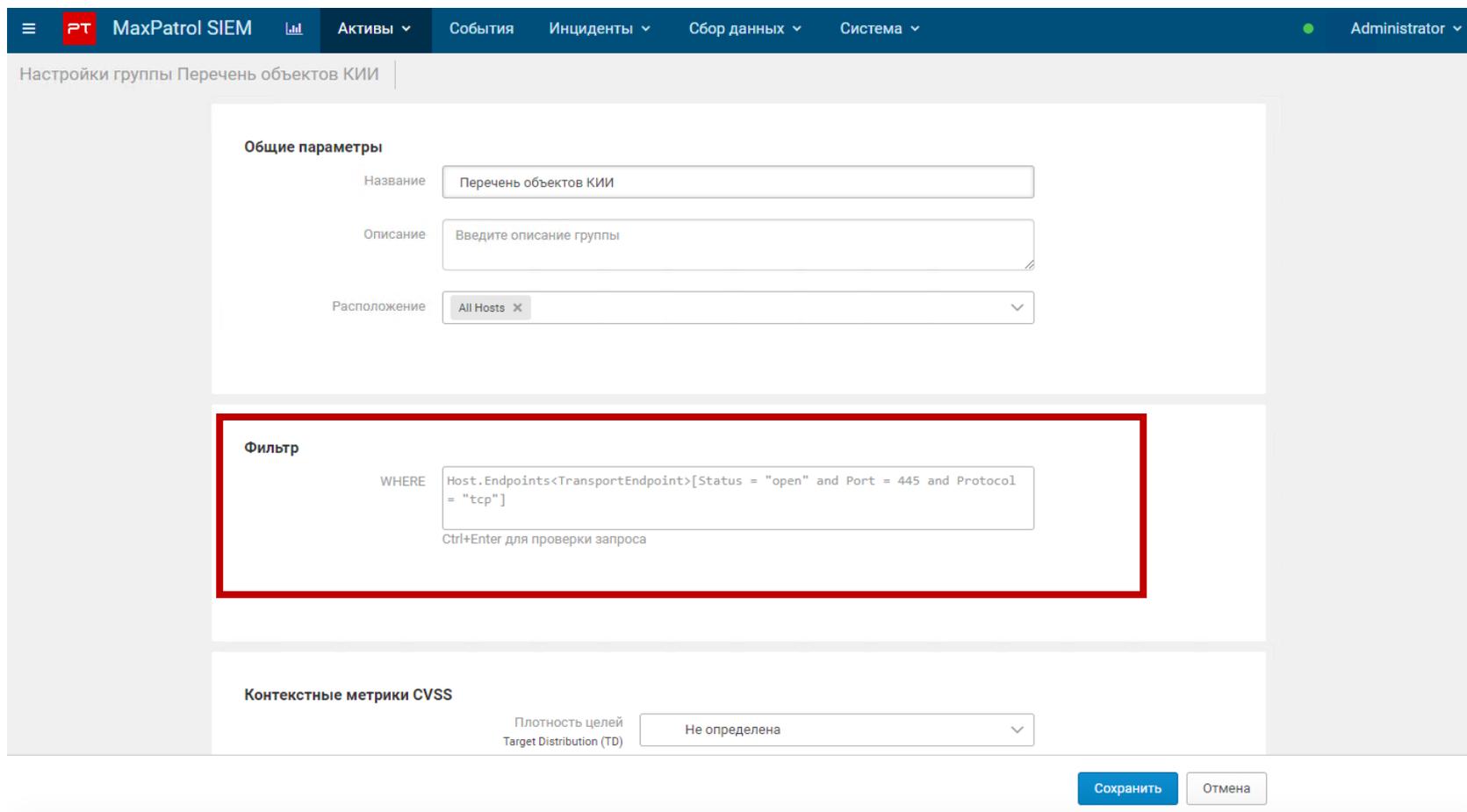
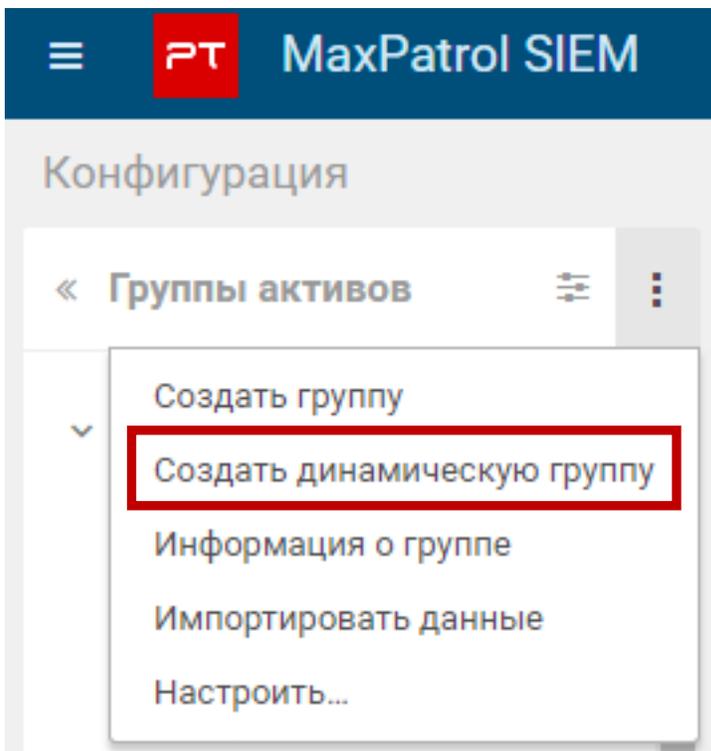
Узел	Интегральная уязвимость а...	Последнее обновление акти...
@Host	Host.@CumulativeVulnerability	Host.@UpdateTime
(dc01.ptdemo.local)	0	23 июля, 16:39
(dc02.ptdemo.local)	0	23 июля, 16:39
10.0.168.1 ()	0	11 апреля, 10:22
10.0.168.13 ()	0	11 апреля, 10:22
10.0.168.2 ()	0	11 апреля, 10:22
10.0.168.3 ()	0	11 апреля, 10:22
10.0.209.180 ()	436,3	11 мая, 19:35
10.0.68.224 ()	0	16 апреля, 08:56
10.0.68.59 ()	0	26 марта, 12:07
192.168.10.1 ()	0	04 мая, 11:56
192.168.10.10 ()	0	07 мая, 09:01

Скачать ▾

Всего 183 записи, выбрана 1

Формирование перечня объектов КИИ

С помощью динамических групп можно сформировать перечень объектов КИИ



Перечень объектов КИИ по категориям



MaxPatrol SIEM Administrator

Конфигурация | Перечень объектов КИИ x | Все активы x

Группы активов

- Все активы
 - All Hosts
 - Core ASA
 - Critical Hosts
 - VPN Servers
 - Перечень объектов КИИ**
 - Объекты 1 категории значимости
 - Объекты 2 категории значимости
 - Объекты 3 категории значимости
 - Unmanaged hosts

Узел	Интегральная уязвимо...	Последнее обновление ...
@Host	Host.@CumulativeVulner...	Host.@UpdateTime
10.0.209.180 ()	436,3	11 мая, 19:35
192.168.20.11 (w...	4030,1	27 апреля, 14:46
192.168.20.16 (w...	7298,7	11 мая, 16:03
192.168.20.16 (w...	7298,7	11 мая, 11:59
192.168.20.17 (w...	7265,1	11 мая, 11:59
192.168.20.17 (w...	7231,5	11 мая, 16:12
192.168.20.21 (w...	7324,3	27 апреля, 14:49
192.168.20.254 ()	0	21 марта, 09:00
192.168.21.11 (b...	11852,4	27 апреля, 14:48
192.168.21.15 (B...	5229,8	27 апреля, 14:49
192.168.30.125 (...)	7469,4	11 апреля, 10:22

10.0.209.180 () Состояние на 12 августа 08:51

Обнаружен 11 мая, 19:35 → Последнее обновление 11 мая, 19:35

↑ 436.3 | Высокая значимость

История за 7 дней

Интегр. уязвимость

Ручной ввод

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Сетевая конфигурация

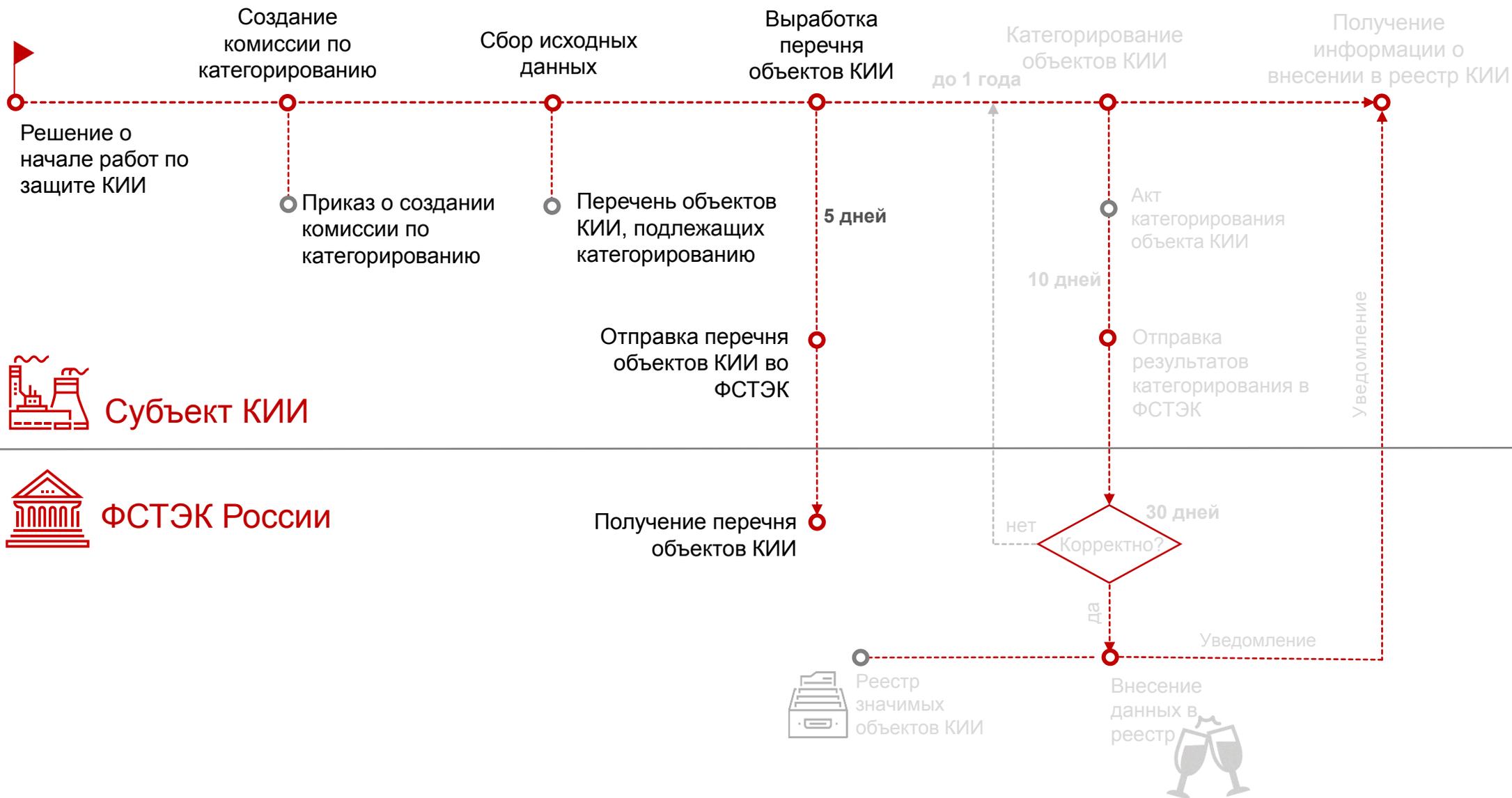
Интер... | Сервис | ПО

> ip://10.0.209.180

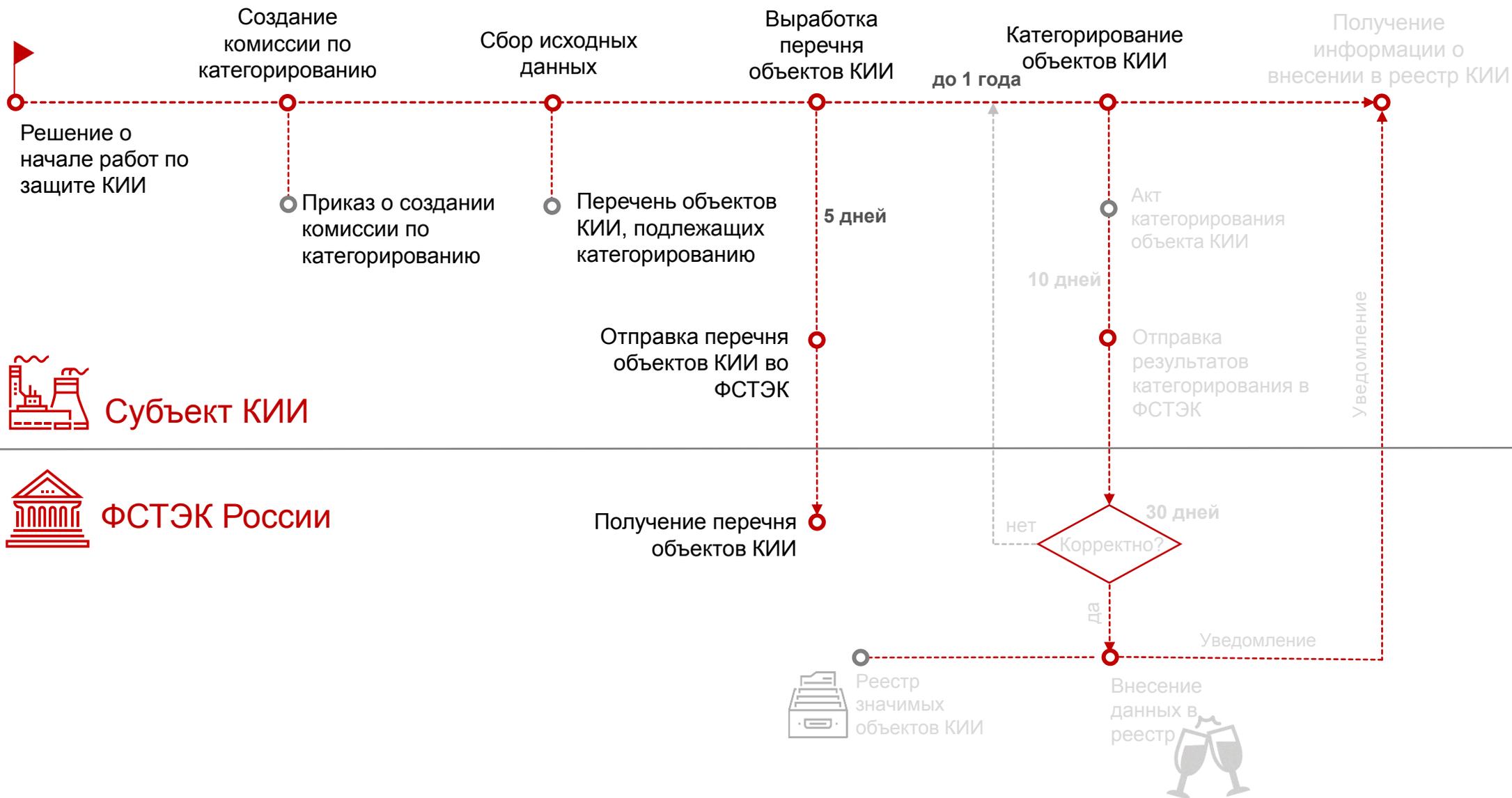
Самые опасные уязвимости

- ↑ Локальная аутентификация отключена
- ↑ Неподдерживаемая версия
- ↑ Учетная запись
- ↑ Oracle Lisntener не защищен паролем
- ↑ Учетная запись пользователя
- ↑ (CPUApr2013) Не установлены обновления безопасности
- ↑ (CPUApr2012) Не установлены обновления безопасности
- ↑ (CPUJan2013) Не установлены обновления безопасности
- ↑ (CPUJan2015) Не установлены обновления безопасности
- ↑ (CPUJul2015) Не установлены обновления безопасности

Порядок категорирования объектов КИИ



Порядок категорирования объектов КИИ



Список установленного ПО на объектах КИИ



MaxPatrol SIEM



Активы ▾

События

Инциденты ▾

Сбор данных ▾

Система ▾

чета по расписанию

Параметры отчета

Название

Источник

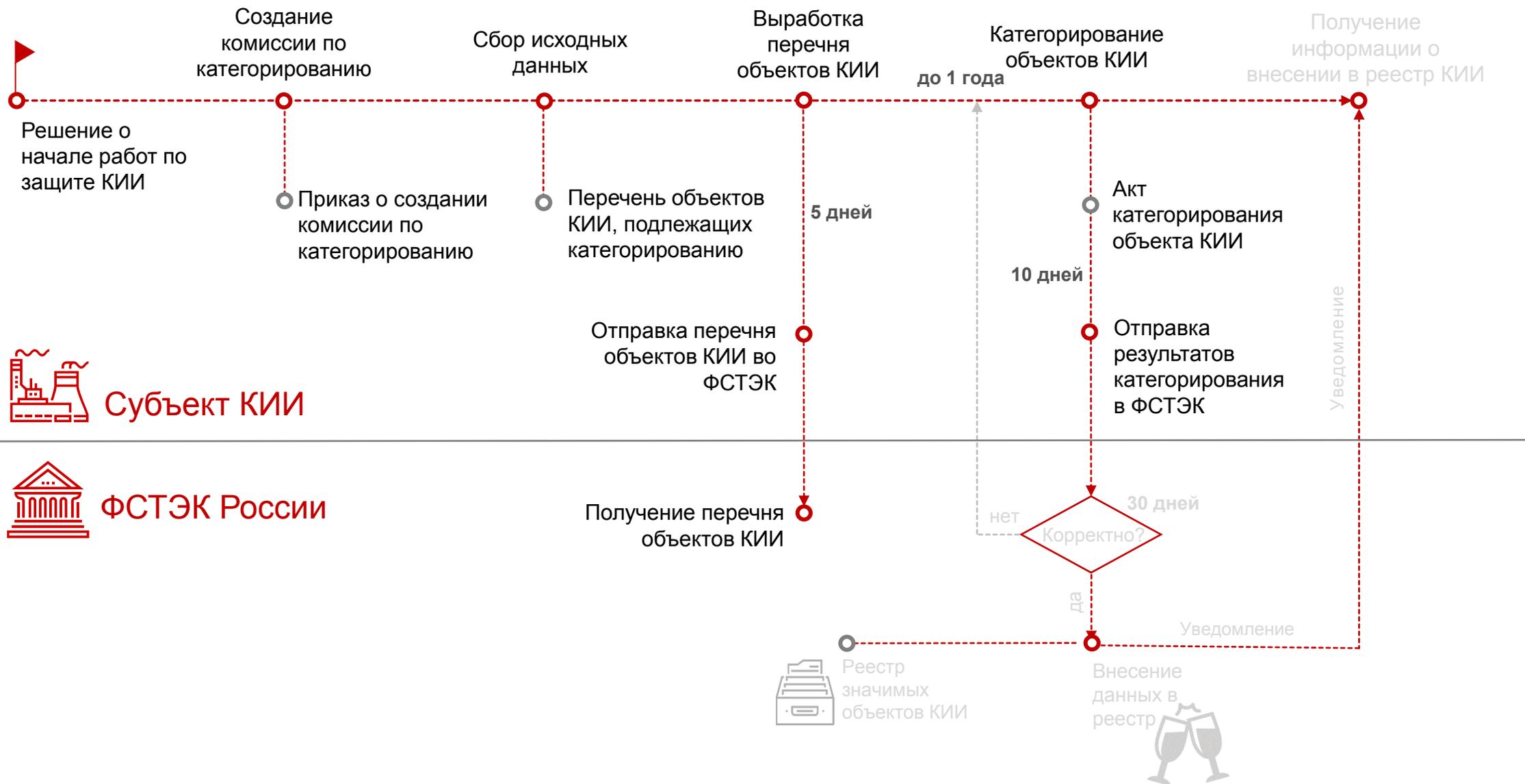
В группах

включая вложенные группы

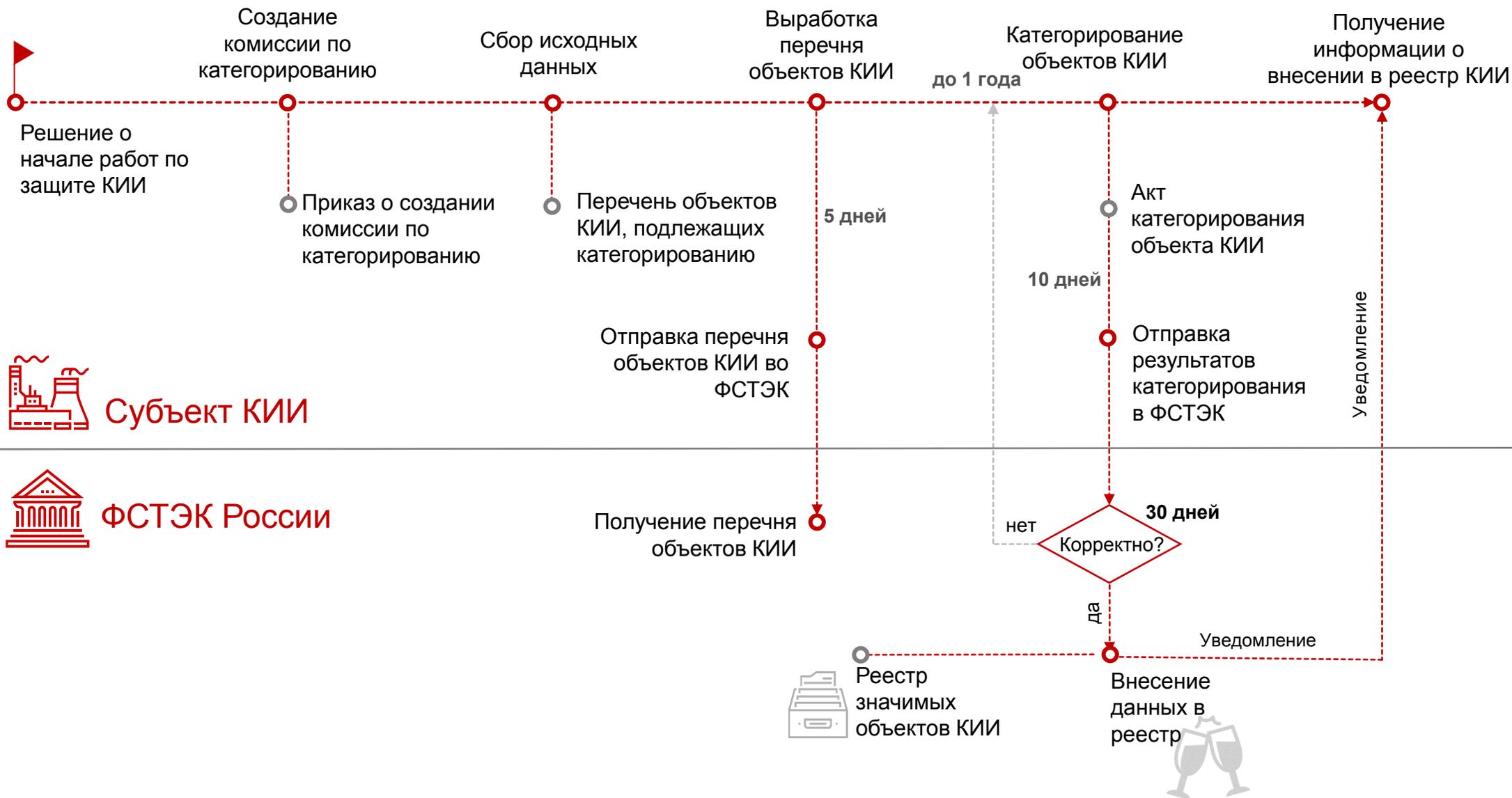
Отчет

Формат

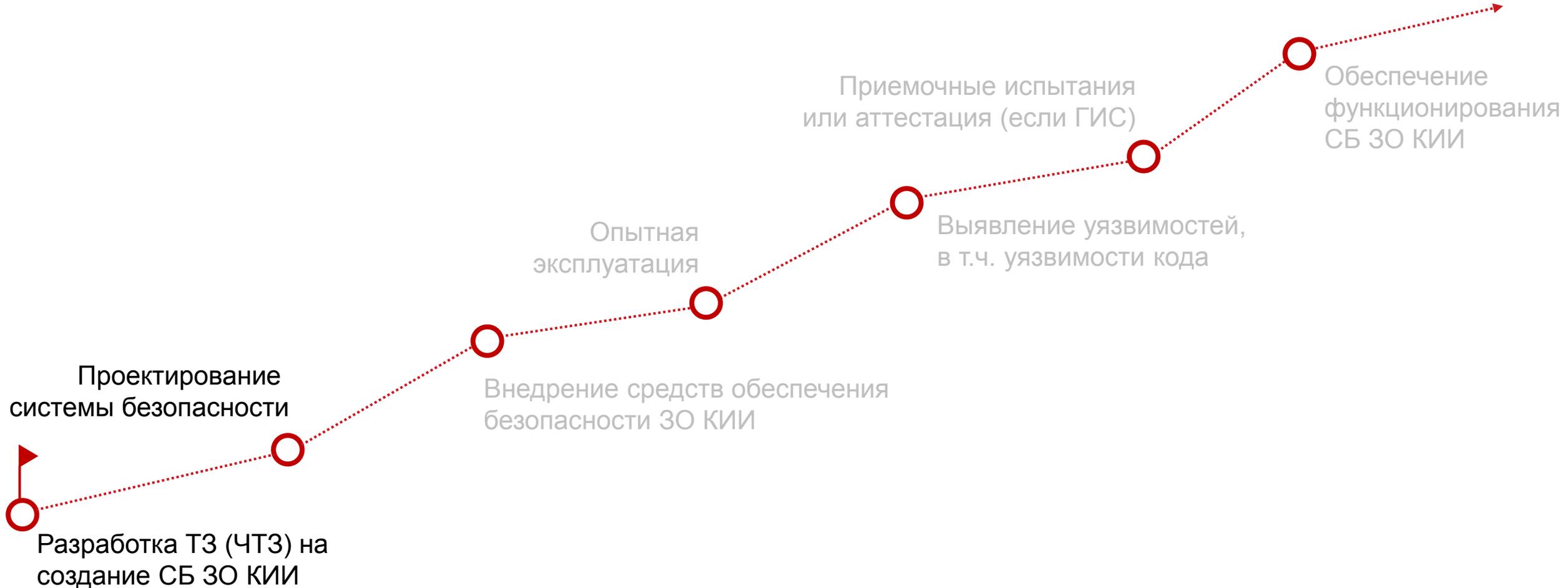
Порядок категорирования объектов КИИ



Порядок категорирования объектов КИИ



Создание системы безопасности ЗО КИИ



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

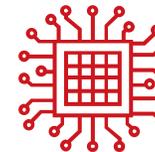


MaxPatrol SIEM

Приказ ФСТЭК №239

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

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 Network Attack Discovery



PT ISIM



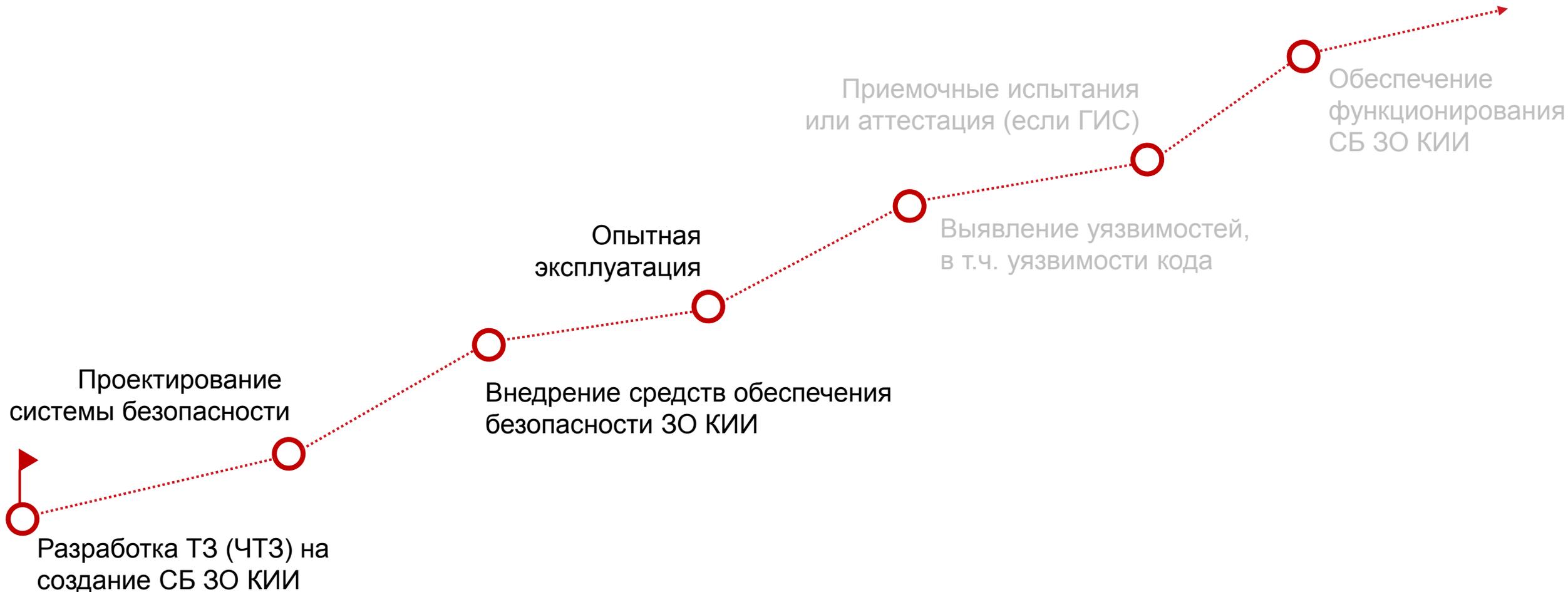
PT Application Firewall



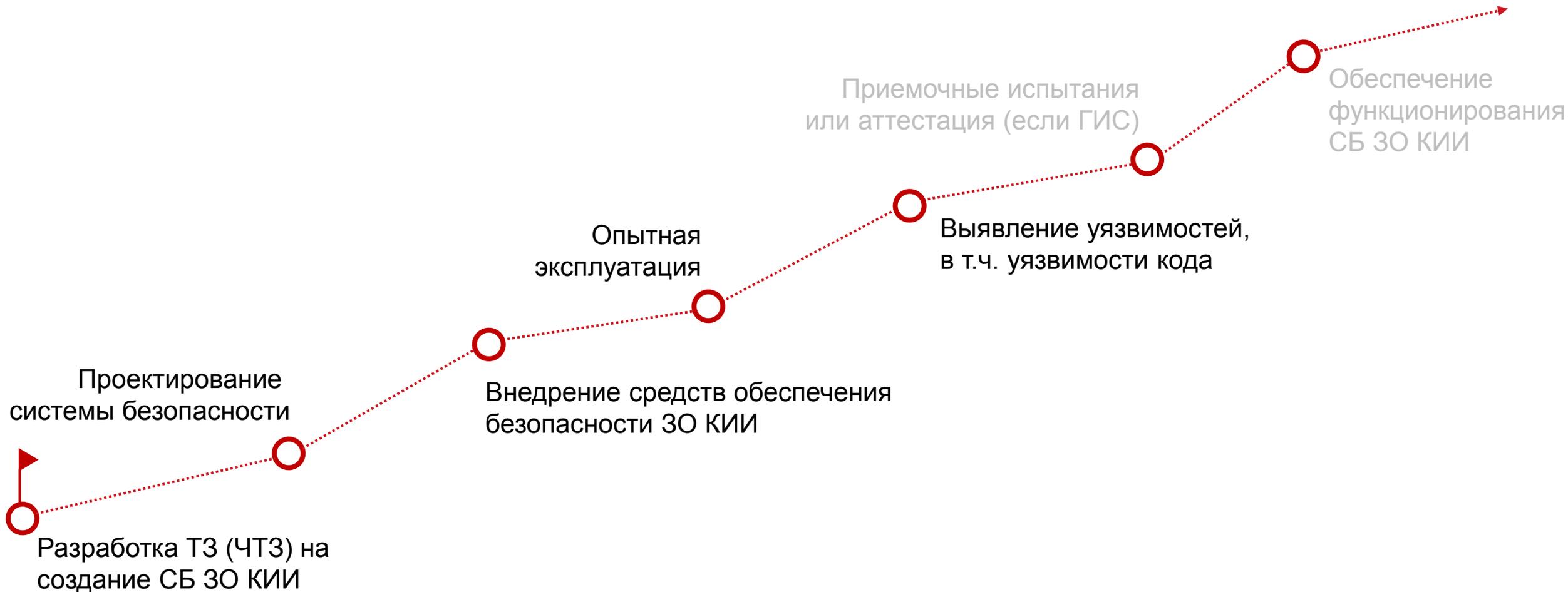
PT MultiScanner



Создание системы безопасности ЗО КИИ



Создание системы безопасности ЗО КИИ



MaxPatrol 8 выявление уязвимостей

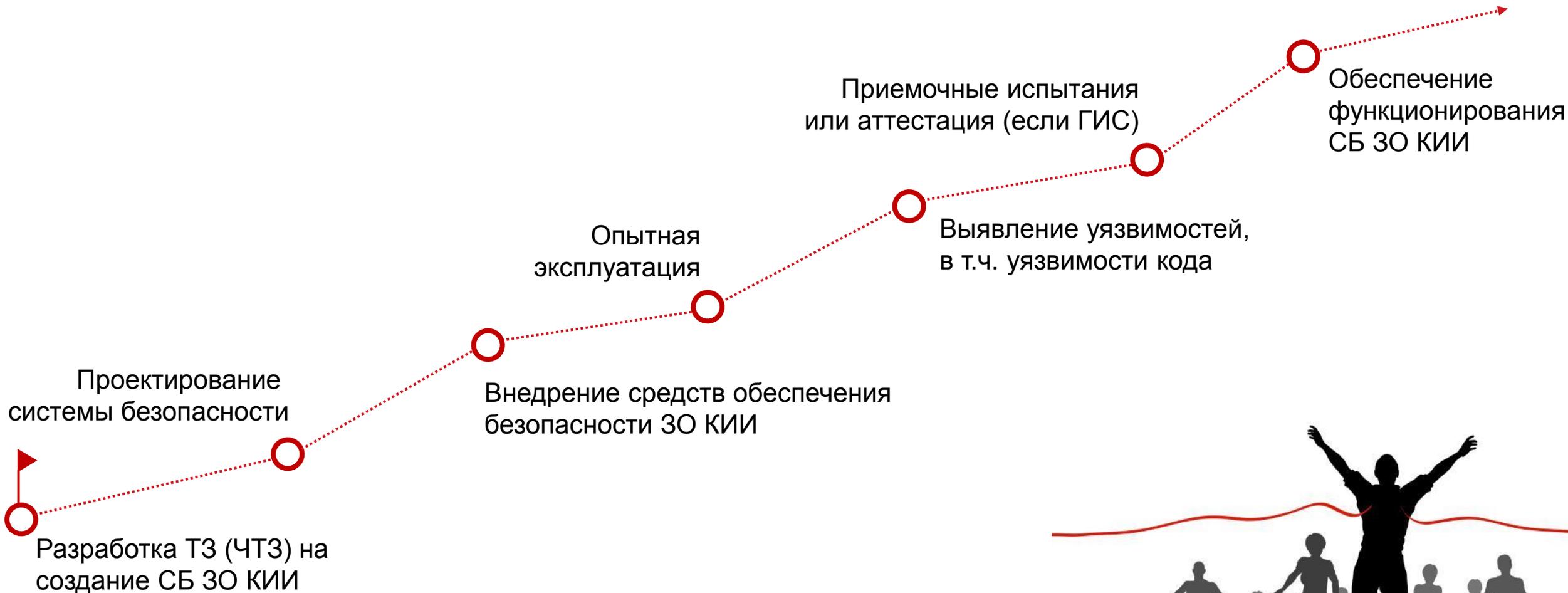


The screenshot displays the MaxPatrol 8 interface with several key sections:

- Активные сканы:** A table with columns for task name, start time, progress, nodes in task, processed nodes, and scanner.
- Профили:** A list of scan profiles such as (Pentest) Bruteforce, (Pentest) DoS scan, (Pentest) Fast Scan, (Pentest) Inventory, (Pentest) PCI DSS ASV, (Pentest) Safe scan, (Pentest) Safe scan подсети ПКД, (Pentest) Service Discovery, (Pentest) Web Scan, Default, HttpContent, PCIDSS ASV, and Аудит и комплаенс.
- Навигатор:** A tree view showing the scan path for IP 192.168.230.35, including categories like Adobe Pepper Flash for Google Chrome, Firefox, JavaTM Platform, Microsoft Excel, Microsoft Office, Microsoft Office InfoPath, Microsoft PowerPoint, Microsoft Publisher, Microsoft Windows, Microsoft Word, Microsoft XML Core Services, OpenSSL, Photo Manager, QuickTime Player, Shockwave Player, Flash Player, Foxit Reader, Microsoft Access, Microsoft Lync, Microsoft Outlook, CryptoPro CSP, Hardware Information, Kaspersky Endpoint Security, Microsoft Internet Explorer, Network Configuration, Operating System, Adobe Acrobat Reader DC, ffdshow, Google Chrome, iCloud, iTunes, Kaspersky Security Center, and Microsoft .NET Framework.
- Аудит и комплаенс:** A section showing audit results for IP 192.168.230.35, including a warning for a serious vulnerability and a high level of compliance.
- Информация:** A summary of scan results for IP 192.168.230.35, including IP address, NetBIOS name (АРКО76), FQDN (not defined), and maximum vulnerability levels (high for both Pentest and Audit) with 573 findings.
- Идентификация:** Shows the IP address 192.168.230.35 as the target in the task.
- Операционная система:** Identifies the system as Microsoft Windows: Windows 7 Professional Service Pack 1 (x64).

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

Создание системы безопасности ЗО КИИ

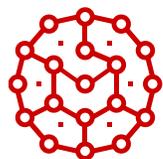




Защита от неправомерного доступа к информации, обрабатываемой КИИ



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



Восстановление функционирования объекта КИИ



Непрерывное взаимодействие с ГосСОПКА



Информирование НКЦКИ

об инцидентах



Обмен информацией

об инцидентах между
субъектами КИИ



Получение рассылок от НКЦКИ

об инцидентах, средствах и
способах проведения атак



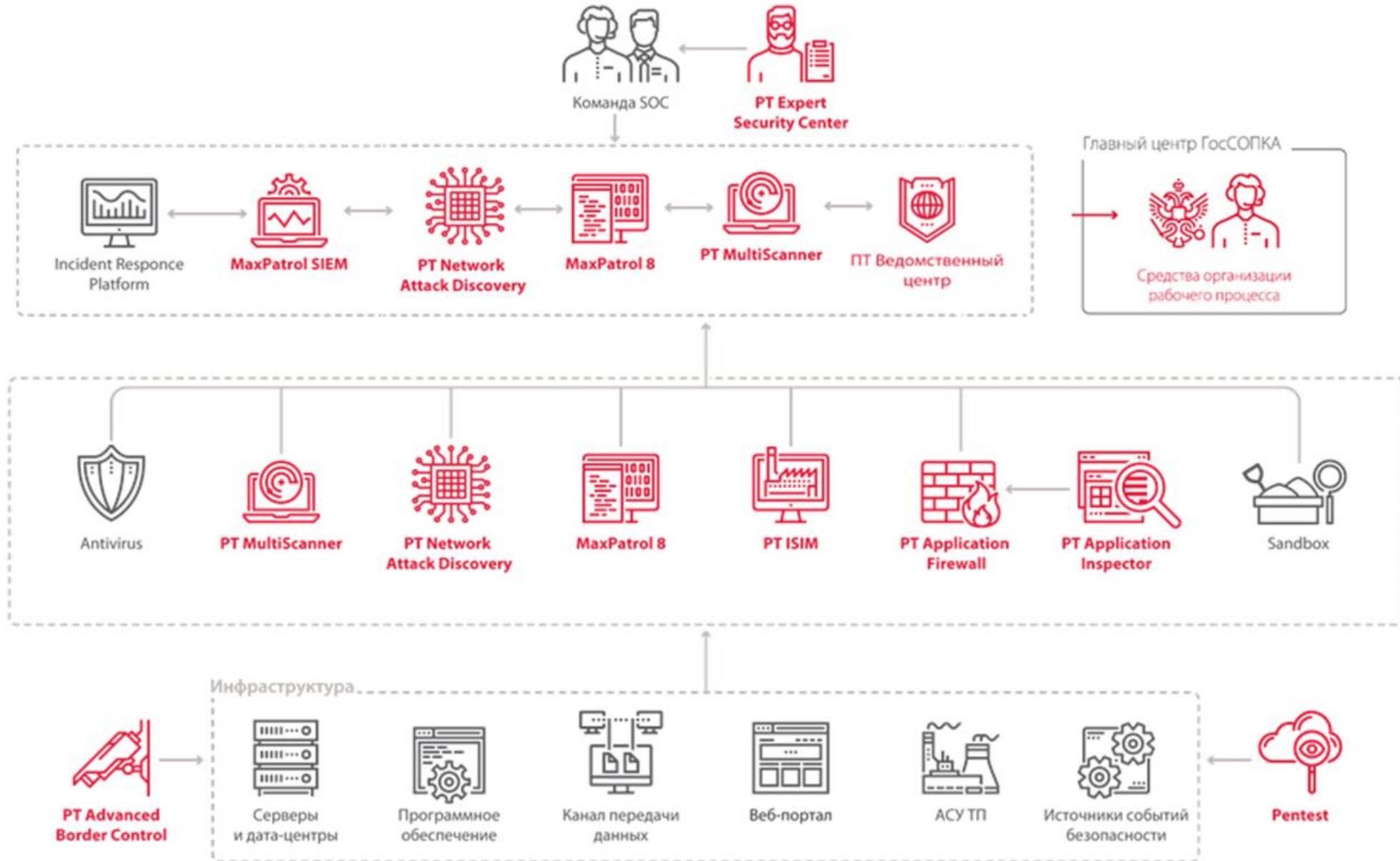
“
На чём в первую очередь необходимо сконцентрировать усилия.
Первое – это совершенствование государственной системы обнаружения,
предупреждения и ликвидации последствий компьютерных атак
на информационные ресурсы России.

В. Путин
Заседание Совета Безопасности
Российской Федерации
26.10.2017 г.

Функции и построение центров ГосСОПКА



Позитивная архитектура центров ГосСОПКА



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



POSITIVE TECHNOLOGIES

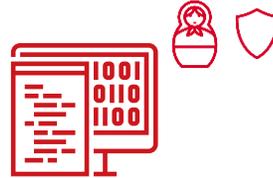
PT Platform 187





MaxPatrol SIEM

Система мониторинга событий и выявления инцидентов



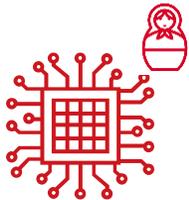
MaxPatrol 8

Система контроля защищенности



PT MultiScanner

Система выявления вредоносного контента



PT Network Attack Discovery

Система комплексного анализа сетевого трафика



PT Ведомственный центр

Система управления инцидентами и взаимодействия с НКЦКИ

Оptionальное подключение:

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

Ограничения

PT

до **250** узлов

включаются в мониторинг
MaxPatrol SIEM и
MaxPatrol 8

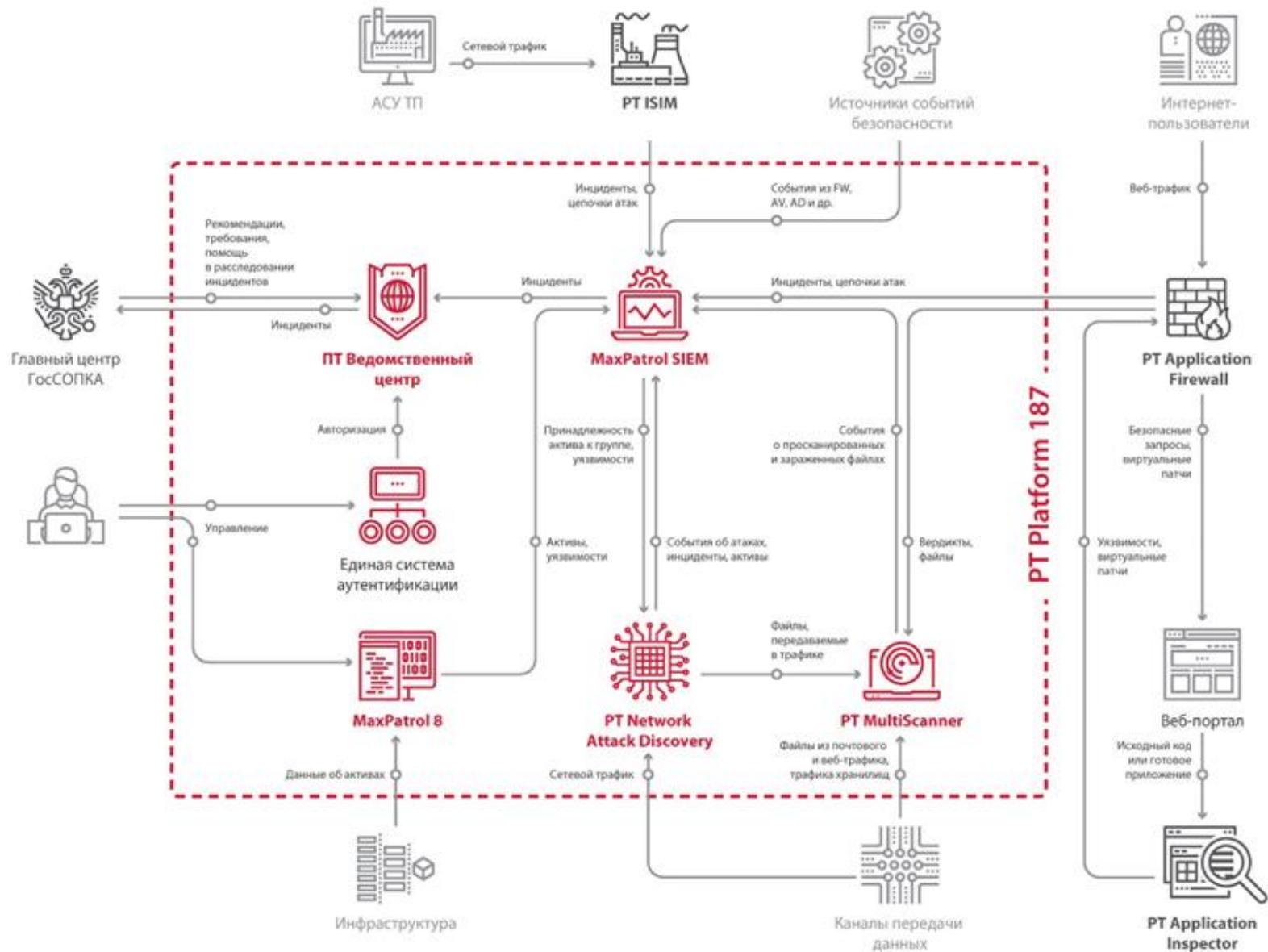
до **100** Мбит/с

пропускная способность
PT Network Attack
Discovery

до **3000** FPH

пропускная способность
PT MultiScanner

Архитектура Platform 187



POSITIVE TECHNOLOGIES

Позитивные результаты



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

The screenshot displays the PT MultiScanner interface with the following details:

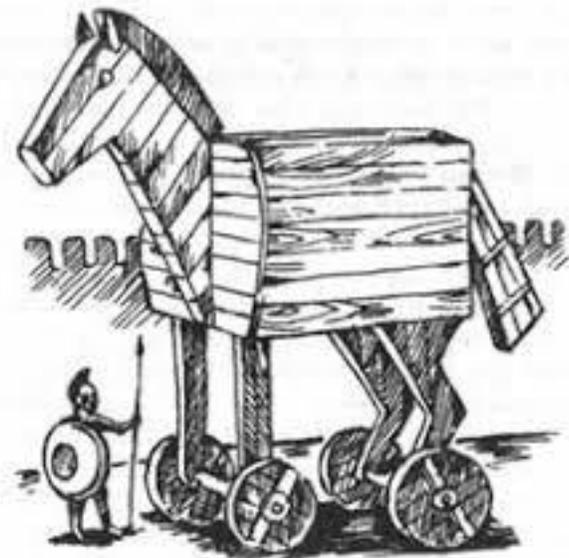
- Navigation:** MS, Сводка, Угрозы, Задания, Файлы, Списки, Система.
- Filters:** За все время, Тип: Все, Состояние обработки: Все.
- Threats Summary:** 516 групп угроз, 517 Все угрозы, 493 День.
- Threat List:** Multiple entries for smtp_1.eml files, identified as Trojan (Троян) and ptnad.
- File Details (smtp_1.eml):**
 - В обработанные, В черный или белый список..., Печать
 - Свойства файла: Подробнее
 - Результат проверки: Обнаружено опасное ПО (Троян)
 - SHA-256: C1D4525DBCDBAD2AEEDBF226D56C6FF14BF3866812533E7D9DE5CDDCC277A18E
 - Размер: 281,75 КБ
 - Названия файла: smtp_1.eml
 - 1 узел возможно заражен: smtp://91. [redacted]:25/smtp_1.eml (ptnad)

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

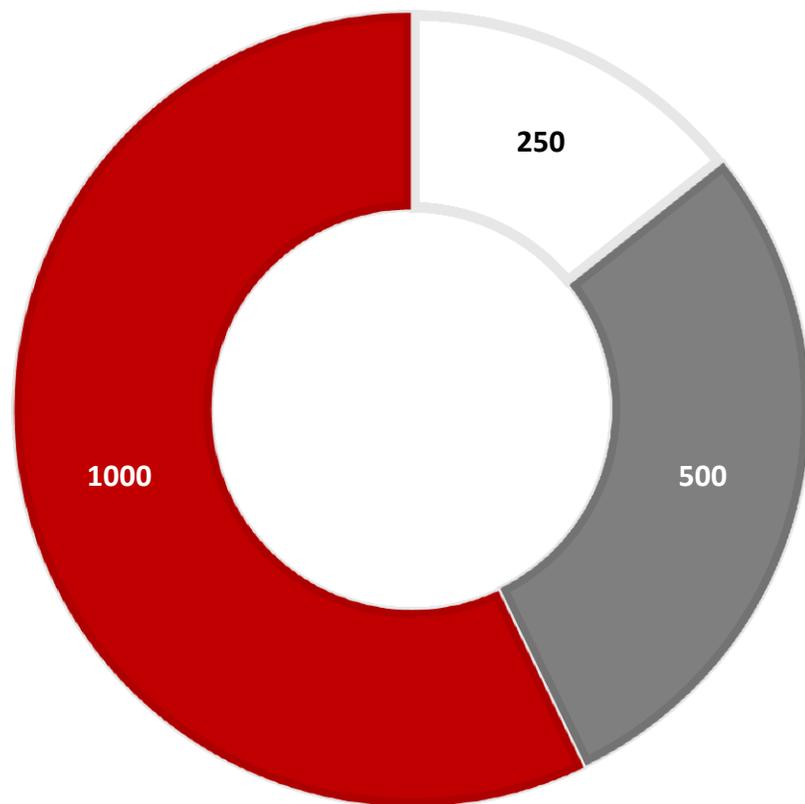
Планы по развитию центра



Развитие центра: 1 задача

МАСШТАБИРОВАНИЕ PLATFORM 187

■ 2018 год ■ 2019 год ■ 2020 год



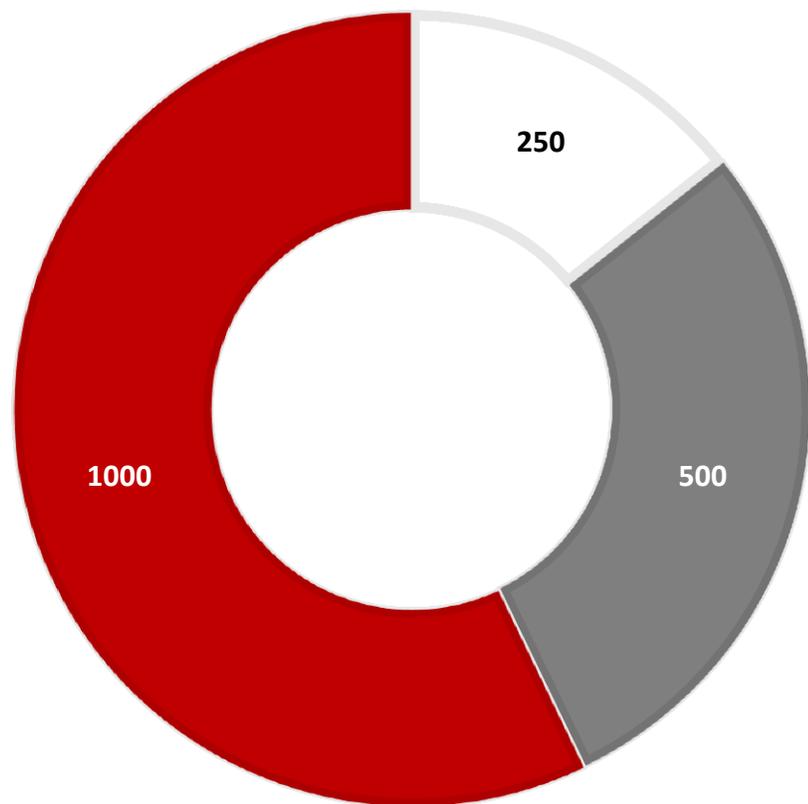
Развитие центра: 2 задача

ЛИНИИ МОНИТОРИНГА И РЕАГИРОВАНИЯ



МАСШТАБИРОВАНИЕ PLATFORM 187

■ 2018 год ■ 2019 год ■ 2020 год



ЛИНИИ МОНИТОРИНГА И РЕАГИРОВАНИЯ



Персонал центра

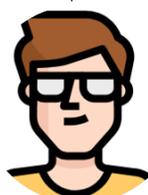


Руководитель SOC



1-я линия:

Первичная оценка инцидентов, отработка ложных срабатываний, обработка по playbookам



2-я линия:

Глубокое расследование инцидентов



3-я линия:

Глубокий анализ артефактов инцидентов



Аналитики:

Написание playbookов, внутренний TI

Жизненный цикл реагирования

2018 год



● Зоны непосредственного участия экспертов РТ

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

Жизненный цикл реагирования

2019 год



● Зоны непосредственного участия экспертов РТ

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

Жизненный цикл реагирования

2020 год



POSITIVE TECHNOLOGIES

Интернет ресурсы



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*

Подробный план по выполнению требований закона № 187-ФЗ

Наши эксперты детально изучили всю нормативно-правовую базу по защите объектов критической информационной инфраструктуры. Они разработали поэтапный план, который поможет субъектам КИИ разобраться в требованиях и выполнить их в срок.

Из плана вы узнаете:

- как определить, что ваша организация – субъект КИИ;
- как провести категорирование объектов КИИ;
- что необходимо для создания системы безопасности значимых объектов КИИ;
- что нужно сделать, чтобы обеспечить безопасность значимого объекта КИИ в ходе и при выводе его из эксплуатации;

Вебинары

PT

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/>



t.me/KII187FZ

POSITIVE TECHNOLOGIES

Спасибо
за внимание

