Киреев Ильяс
Продвижение и развитие продуктов
ikireev@ptsecurity.com

Обеспечение безопасности объектов КИИ согласно ФЗ-187

POSITIVE TECHNOLOGIES

ptsecurity.com

187-ФЗ – вершина айсберга

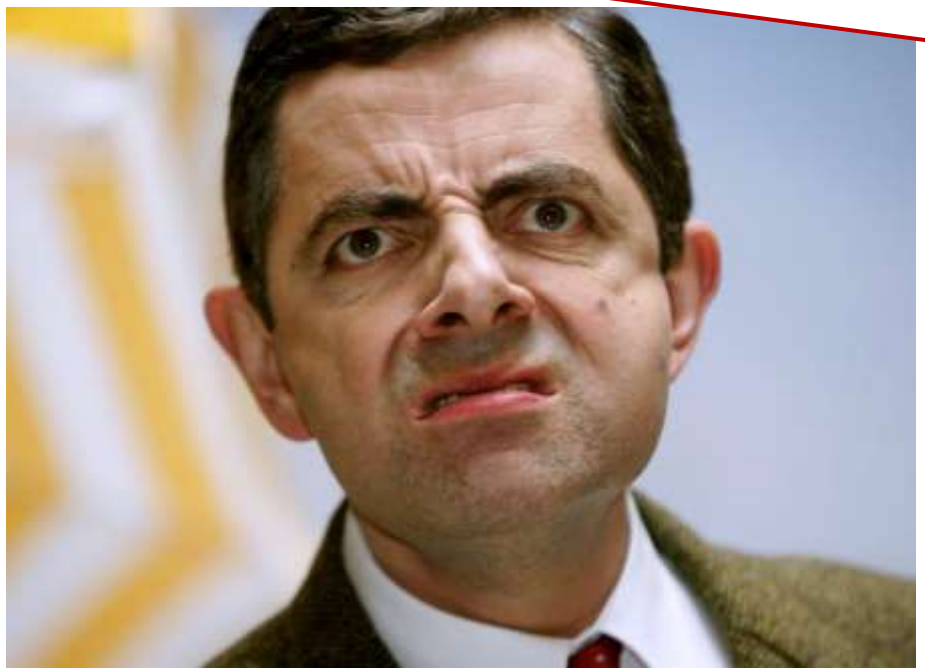
POSITIVE TECHNOLOGIES

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

ВСТУПИЛ В СИЛУ 01.01.2018

*«**Субъект** КИИ - гос. органы и учреждения, юр. лица и ИП»*

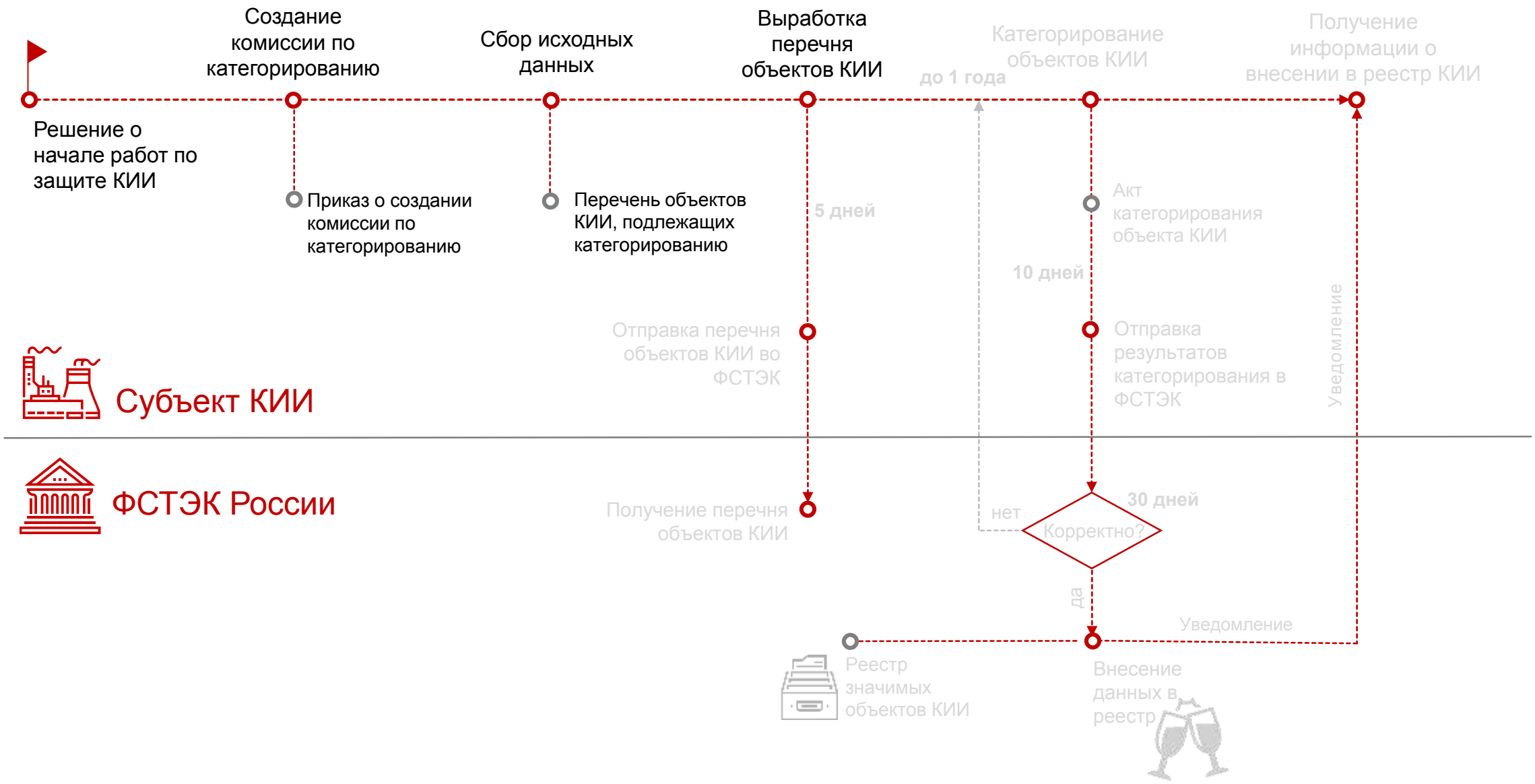
*«**Объекты** КИИ - **ИС, ИТС, АСУ** в сферах:*



*«3 категории **значимых объектов КИИ**»*

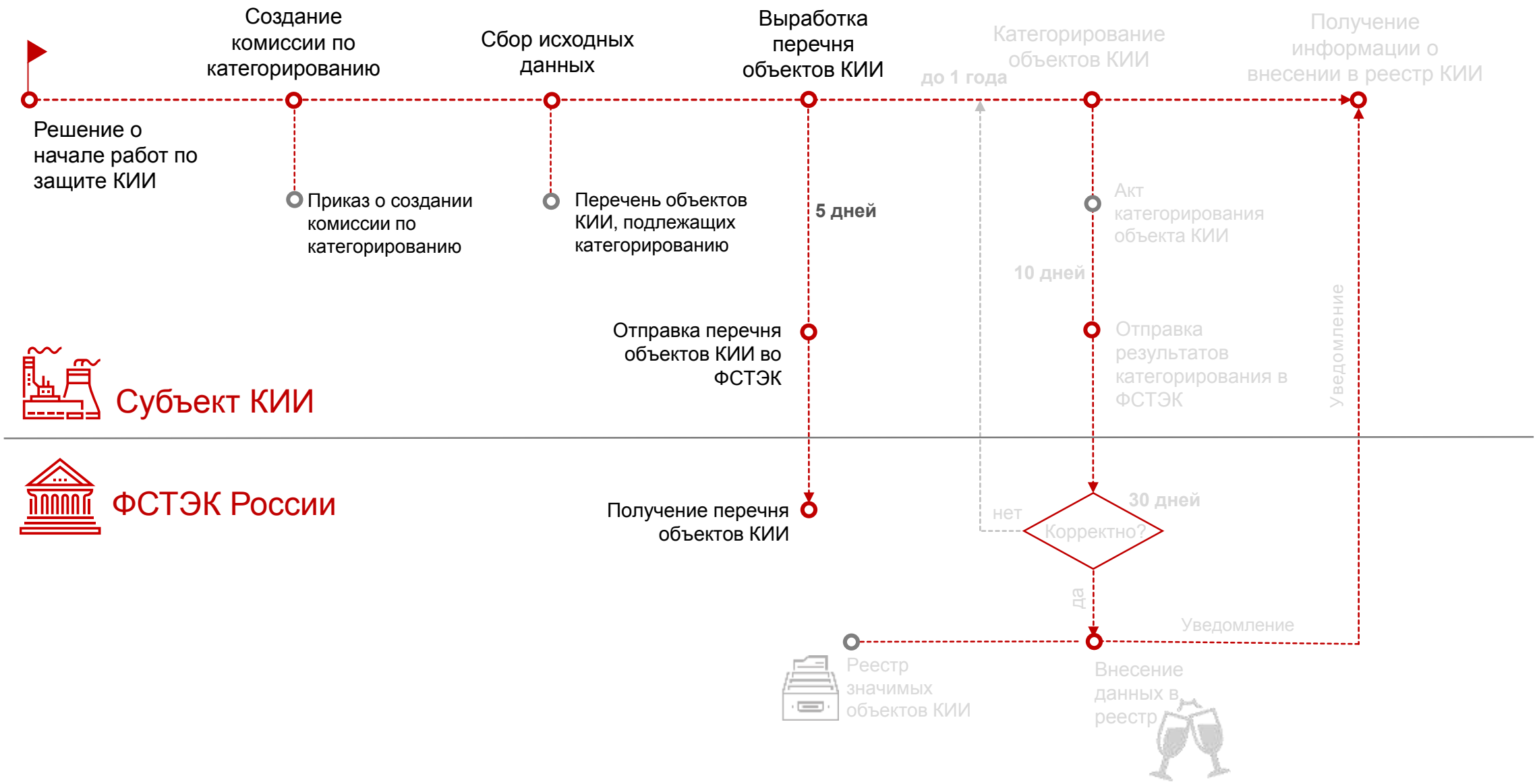
Порядок категорирования объектов КИИ

POSITIVE TECHNOLOGIES



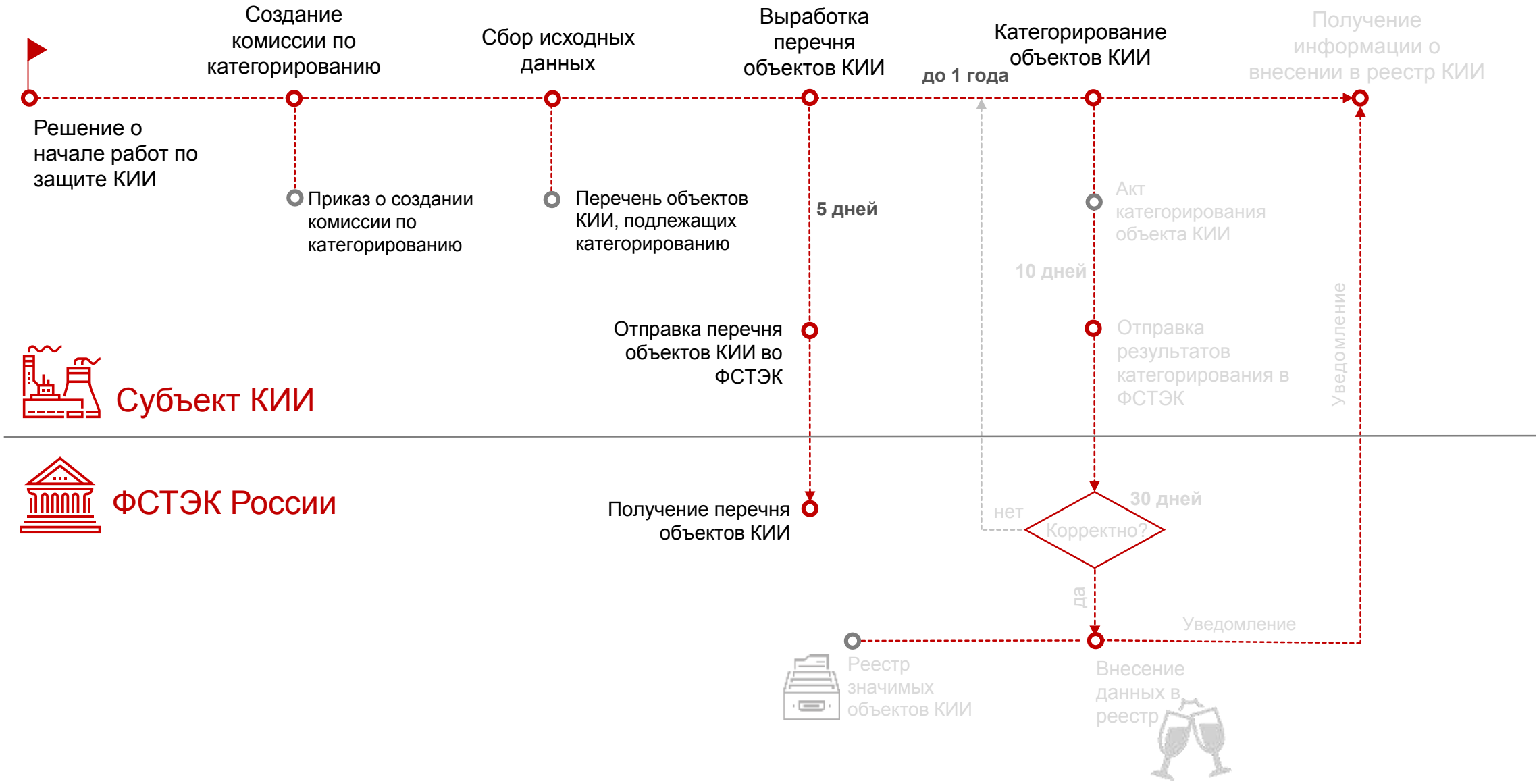
Порядок категорирования объектов КИИ

POSITIVE TECHNOLOGIES



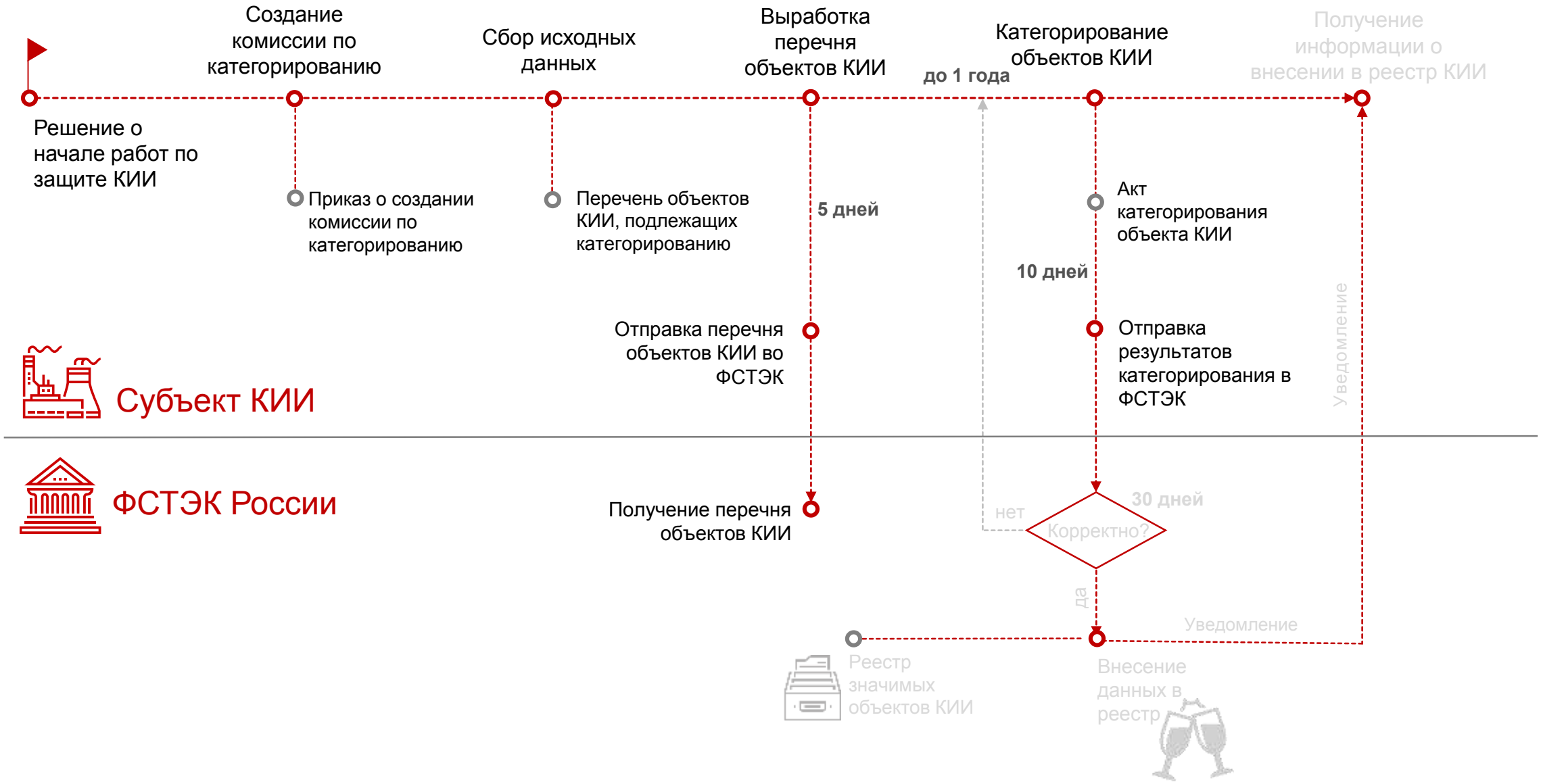
Порядок категорирования объектов КИИ

POSITIVE TECHNOLOGIES



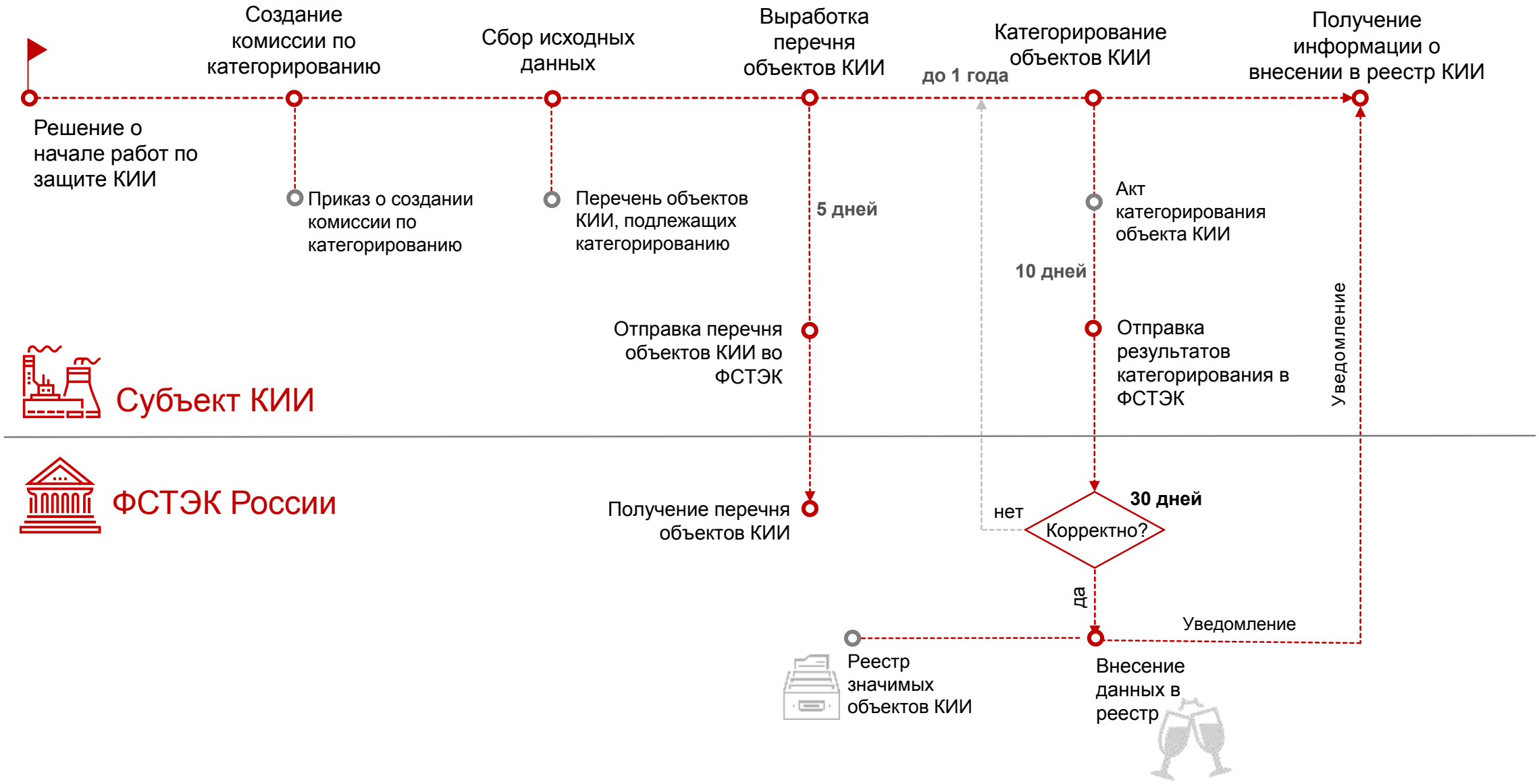
Порядок категорирования объектов КИИ

POSITIVE TECHNOLOGIES



Порядок категорирования объектов КИИ

POSITIVE TECHNOLOGIES



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

POSITIVE TECHNOLOGIES

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 к 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	+	+	+

	ничение программной среды (ОПС)			
	ки ограничения программной среды		+	+
	ском (обращениями) компонентов ммного обеспечения			+
	овкой (инсталляцией) компонентов ммного обеспечения		+	+
	ние временными файлами			
	шинных носителей информации (ЗНИ)			
	щиты машинных носителей информации	+	+	+
	ных носителей информации	+	+	+
	им доступом к машинным носителям информации	+	+	+
	я машинных носителей информации за ы контролируемой зоны			
	ности несанкционированного чтения машинных носителях информации			
	вания интерфейсов ввода (вывода) машинные носители информации	+	+	+
	ка) информации на машинные носители информации			+
	ния машинных носителей информации	+	+	+
	е) информации на машинных носителях информации	+	+	+
	Аудит безопасности (АУД)			
	олитики аудита безопасности	+	+	+
	ния информационных ресурсов	+	+	+
	вимостей и их устранение	+	+	+
	ченных меток и (или) синхронизация стемного времени	+	+	+
	ния событий безопасности	+	+	+
	и анализ сетевого трафика			+
	мации о событиях безопасности	+	+	+
	иторинг безопасности	+	+	+
	при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+

	Проведение внешних аудитов			+
	VI. Антивирусная защита (АВЗ)			
	отка политики антивирусной защиты	+	+	+
	ализация антивирусной защиты	+	+	+
	защита электронной почты и иных сервисов	+	+	+
	использования архивных, исполняемых и зашифрованных файлов			+
	ие базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
	ие средств антивирусной защиты различных производителей			+
	твращение вторжений (компьютерных атак) (СОВ)			
	ка политики предотвращения вторжений (компьютерных атак)		+	+
	ие и предотвращение компьютерных атак		+	+
	новление базы решающих правил		+	+
	VIII. Обеспечение целостности (ОЦЛ)			
	тка политики обеспечения целостности	+	+	+
	елостности программного обеспечения	+	+	+
	нтроль целостности информации			
	и по вводу информации в информационную (автоматизированную) систему			+
	данных, вводимых в информационную (автоматизированную) систему		+	+
	ных действий пользователей по вводу и (или) рмации и предупреждение пользователей об ошибочных действиях		+	+
	ние и (или) деидентификация информации			
	IX. Обеспечение доступности (ОДТ)			
	тка политики обеспечения доступности	+	+	+
	ние отказоустойчивых технических средств		+	+
	зервирование средств и систем		+	+
	ктного функционирования средств и систем		+	+
ОДТ.4	Резервное копирование информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+

	ационной (автоматизированной) системы			
	достаточных вычислительных урсов и каналов связи	+	+	+
	а технических средств и систем (ЗТС)			
	а защиты технических средств и систем	+	+	+
	ии от утечки по техническим каналам			
	щита контролируемой зоны	+	+	+
	ение физическим доступом	+	+	+
	ств вывода (отображения) информации, ие несанкционированный просмотр	+	+	+
	а от внешних воздействий	+	+	+
	ных компонентов системы относительно ной к обработке информации			
	(автоматизированной) системы и ее компонентов (ЗИС)			
	олитики защиты информационной анной) системы и ее компонентов	+	+	+
	по управлению (администрированию) втоматизированной) системой с иными функциями	+	+	+
	информационной (автоматизированной) системы	+	+	+
	ащита информационной атизированной) системы	+	+	+
	информационной (автоматизированной) системы		+	+
	ия демилитаризованной зоны	+	+	+
	ление сетевыми потоками			
	мулятора среды функционирования го обеспечения ("песочница")			
	уры и конфигурации информационной атизированной) системы	+	+	+
	ние гетерогенной среды			
	много обеспечения, функционирующего личных операционных систем			
	адержки или прерывания выполнения м приоритетом со стороны процессов с низким приоритетом			
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.13	Защита неизменяемых данных		+	+

Задачи системы безопасности объекта КИИ в соответствии с 187-ФЗ

POSITIVE TECHNOLOGIES

Защита от неправомерного доступа к информации, обрабатываемой КИИ

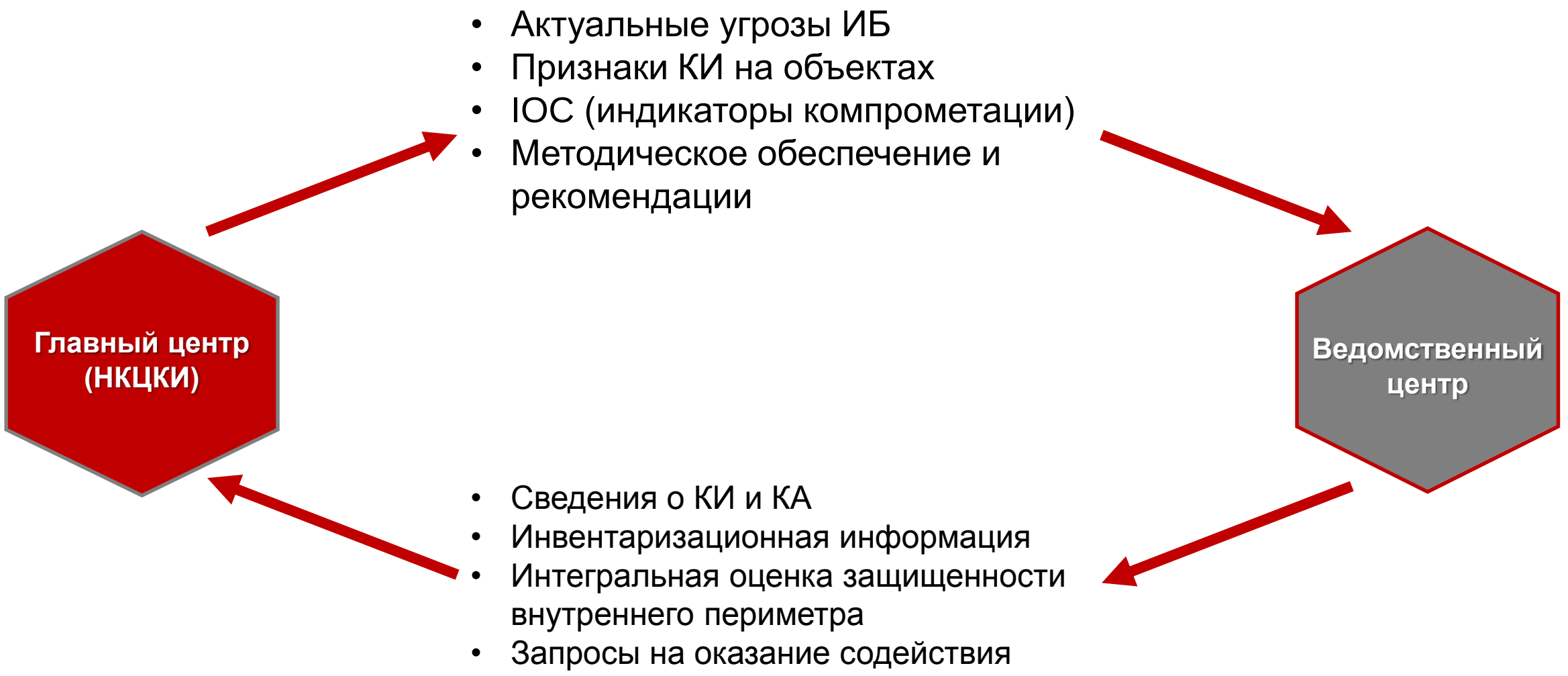
Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ

Восстановление функционирования объекта КИИ

Непрерывное взаимодействие с ГосСОПКА

ГосСОПКА. Обмен информацией с НКЦКИ

POSITIVE TECHNOLOGIES



ГосСОПКА. Методические рекомендации ФСБ России

POSITIVE TECHNOLOGIES

Повышение осведомленности персонала и пользователей

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз

Рекомендации

- Анализ данных о событиях безопасности
- Прием сообщений о возможных инцидентах
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

Обнаружение компьютерных атак

ГосСОПКА. Методические рекомендации ФСБ России

POSITIVE TECHNOLOGIES

PT Application Inspector

MaxPatrol 8

MaxPatrol SIEM

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз

Повышение осведомленности персонала и пользователей

Рекомендации

Обнаружение компьютерных атак

- Анализ данных о событиях безопасности
- Прием сообщений о возможных инцидентах
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

ГосСОПКА. Методические рекомендации ФСБ России

POSITIVE TECHNOLOGIES

PT Application Inspector

MaxPatrol 8

MaxPatrol SIEM

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз

Повышение осведомленности персонала и пользователей

Рекомендации

- Анализ данных о событиях безопасности
- Прием сообщений о возможных инцидентах
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

Обнаружение компьютерных атак

PT ISIM

PT Application Firewall

PT MultiScanner

PT Network Attack Discovery

ГосСОПКА. Методические рекомендации ФСБ России

POSITIVE TECHNOLOGIES

Повышение осведомленности персонала и пользователей

PT Application Inspector

MaxPatrol 8

MaxPatrol SIEM

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз

Рекомендации

- Анализ данных о событиях безопасности
- Прием сообщений о возможных инцидентах
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

MaxPatrol SIEM

ПТ Ведомственный центр

Обнаружение компьютерных атак

PT ISIM

PT Application Firewall

PT MultiScanner

PT Network Attack Discovery

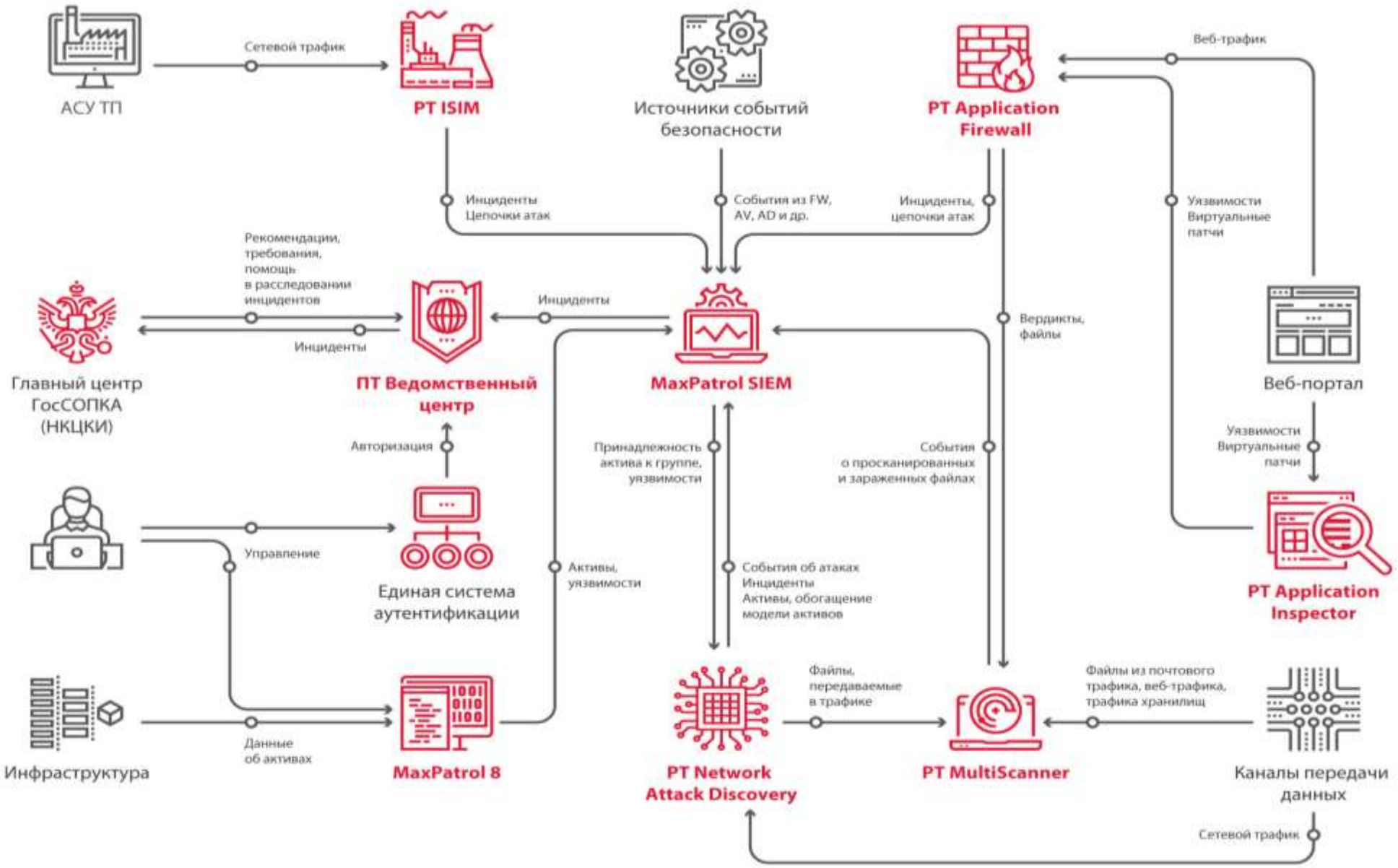
ГосСОПКА. Функции центра

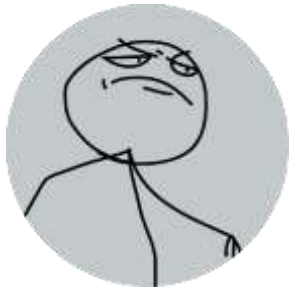
POSITIVE TECHNOLOGIES

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз
- Повышение осведомленности персонала и пользователей
- Обнаружение компьютерных атак
- Анализ данных о событиях безопасности
- Прием сообщений о возможных инцидентах
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

ГосСОПКА. Архитектура

POSITIVE TECHNOLOGIES





ГосСОПКА. Крупные инфраструктуры. Этапы создания

POSITIVE TECHNOLOGIES

1

Периметр

Инвентаризация внешних ИС: MaxPatrol 8, PT ABC, MaxPatrol SIEM

Анализ типовых уязвимостей
MaxPatrol 8

Обнаружение атак на внешние веб-интерфейсы
PT Application Firewall

ГосСОПКА. Крупные инфраструктуры. Этапы создания

POSITIVE TECHNOLOGIES

1 Периметр

Инвентаризация внешних ИС: MaxPatrol 8, PT ABC, MaxPatrol SIEM

Анализ типовых уязвимостей
MaxPatrol 8

Обнаружение атак на внешние веб-интерфейсы
PT Application Firewall

2 Внутренняя инфраструктура

Инвентаризация ИС: MaxPatrol 8, MaxPatrol SIEM
Анализ типовых уязвимостей:
MaxPatrol 8

Анализ сетевого трафика:
PT Network Attack Discovery
Обнаружение атак:
PT Application Firewall

Анализ событий безопасности:
MaxPatrol SIEM
Взаимодействие с ГЦ ГосСОПКА:
ПТ Ведомственный центр

ГосСОПКА. Крупные инфраструктуры. Этапы создания

POSITIVE TECHNOLOGIES

1 Периметр

Инвентаризация внешних ИС: MaxPatrol 8, PT ABC, MaxPatrol SIEM

Анализ типовых уязвимостей
MaxPatrol 8

Обнаружение атак на внешние веб-интерфейсы
PT Application Firewall

2 Внутренняя инфраструктура

Инвентаризация ИС: MaxPatrol 8, MaxPatrol SIEM
Анализ типовых уязвимостей:
MaxPatrol 8

Анализ сетевого трафика:
PT Network Attack Discovery
Обнаружение атак:
PT Application Firewall

Анализ событий безопасности:
MaxPatrol SIEM
Взаимодействие с ГЦ ГосСОПКА:
ПТ Ведомственный центр

3 Комплексные и нетипичные атаки

Расследование инцидентов:
MaxPatrol SIEM + внедренные средства

Анализ исходного кода: PT Application Inspector
Ретроспективный анализ вредоносного ПО: PT MultiScanner

Взаимодействие с ГЦ ГосСОПКА:
ПТ Ведомственный центр

ГосСОПКА. Крупные инфраструктуры. Этапы создания

POSITIVE TECHNOLOGIES

1 Периметр

Инвентаризация внешних ИС: MaxPatrol 8, PT ABC, MaxPatrol SIEM

Анализ типовых уязвимостей
MaxPatrol 8

Обнаружение атак на внешние веб-интерфейсы
PT Application Firewall

2 Внутренняя инфраструктура

Инвентаризация ИС: MaxPatrol 8, MaxPatrol SIEM
Анализ типовых уязвимостей:
MaxPatrol 8

Анализ сетевого трафика:
PT Network Attack Discovery
Обнаружение атак:
PT Application Firewall

Анализ событий безопасности:
MaxPatrol SIEM
Взаимодействие с ГЦ ГосСОПКА:
ПТ Ведомственный центр

3 Комплексные и нетипичные атаки

Расследование инцидентов:
MaxPatrol SIEM + внедренные средства

Анализ исходного кода: PT Application Inspector
Ретроспективный анализ вредоносного ПО: PT MultiScanner

Взаимодействие с ГЦ ГосСОПКА:
ПТ Ведомственный центр

Аутсорсинг на **PT ESC**

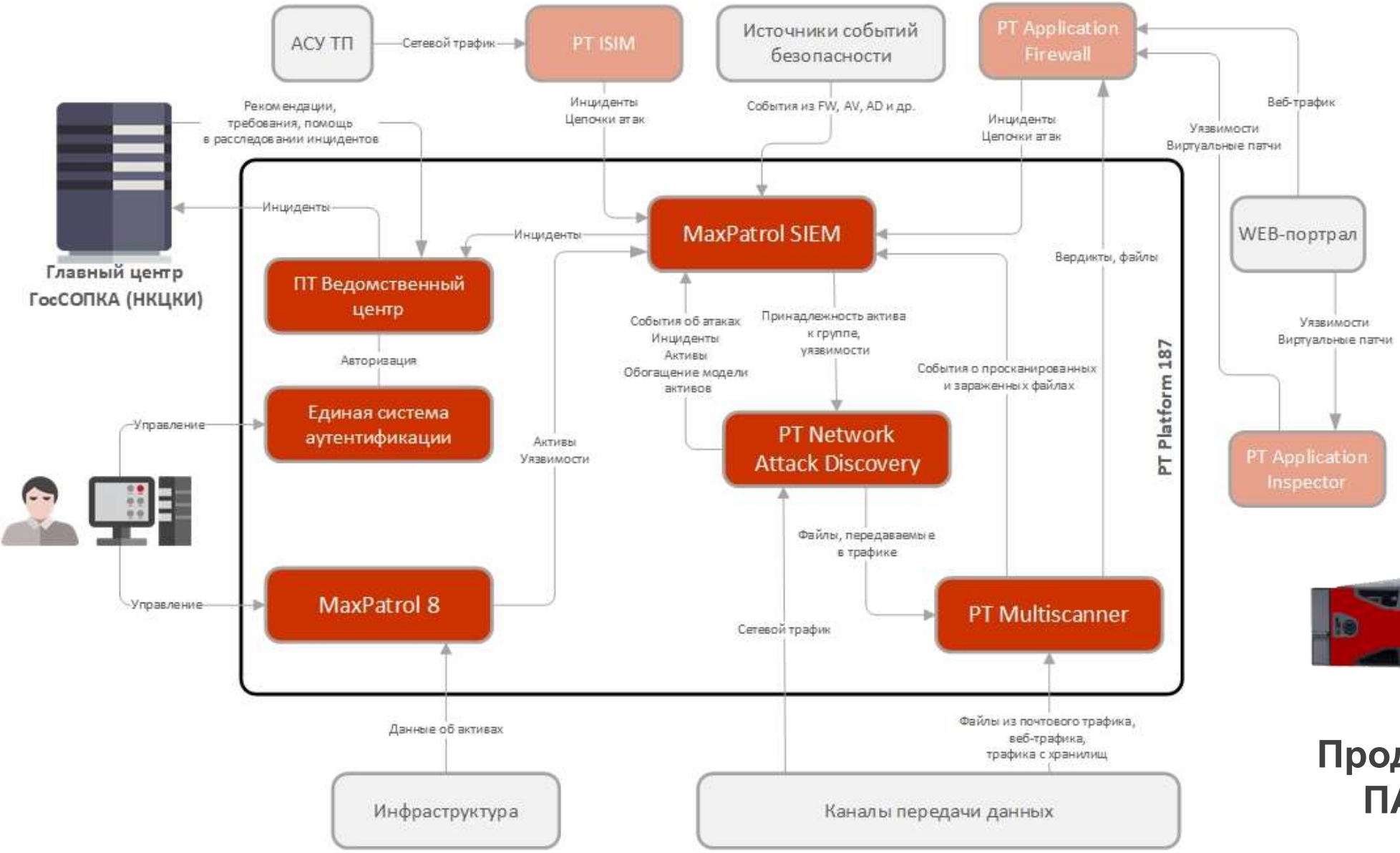
- Экспертный анализ уязвимостей внешних ИС
- Анализ событий безопасности для внешних ИС
- Реагирование на инциденты
- Взаимодействие с ГЦ ГосСОПКА

- Экспертный анализ уязвимостей
- Реагирование на неизвестные компьютерные атаки

- Экспертный анализ уязвимостей
- Реагирование на неизвестные компьютерные атаки

PT Platform 187 – базовая платформа для решения задач 187-ФЗ

POSITIVE TECHNOLOGIES



Для небольших инфраструктур – не более 250 узлов

Продажи только в виде ПАК = сервер + ПО

ГосСОПКА – это процесс!

POSITIVE TECHNOLOGIES

Создание системы – длительная работа

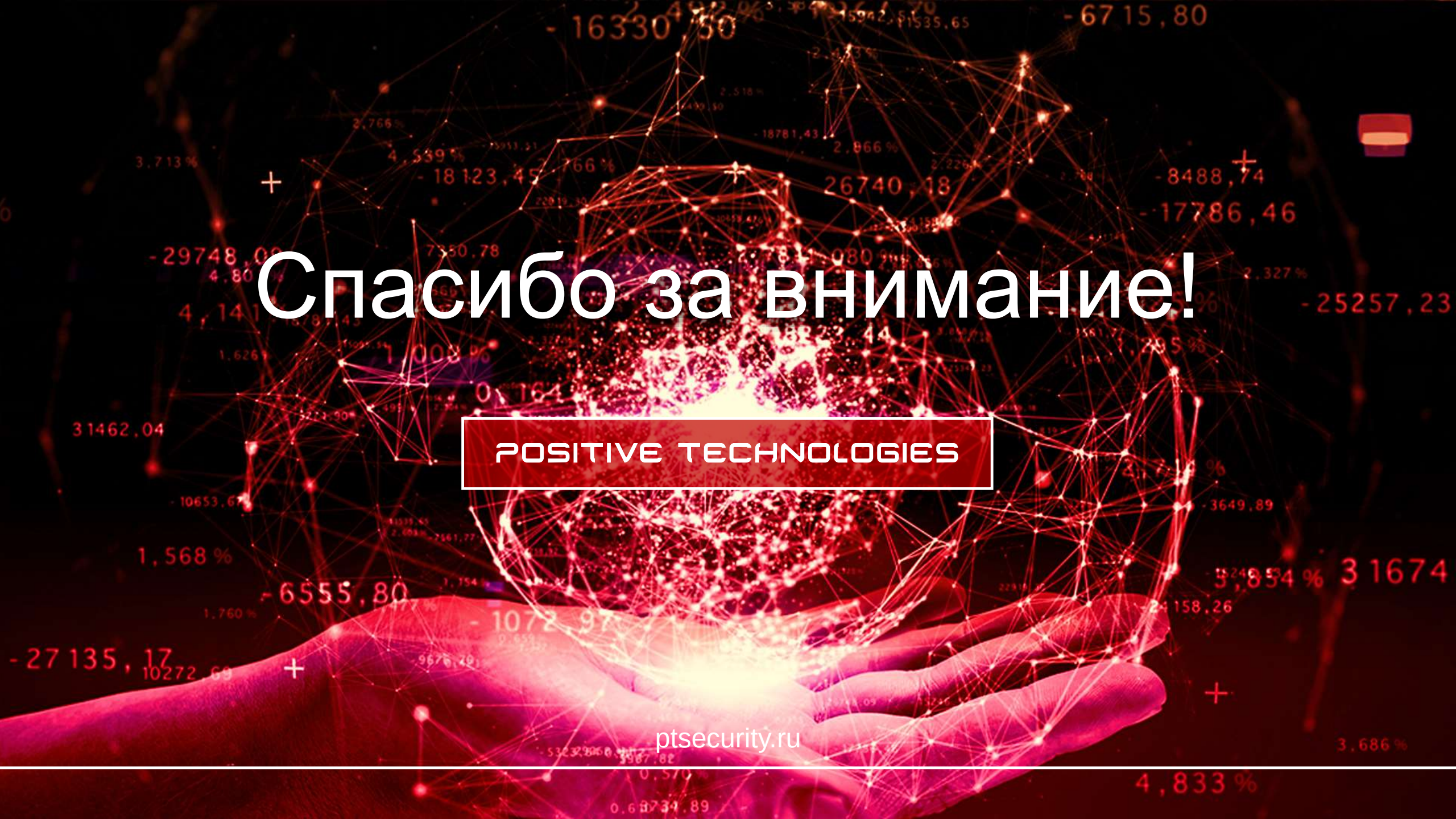
Люди

Процессы

Технические средства

Время

Деньги


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru