

Дмитрий Кузнецов

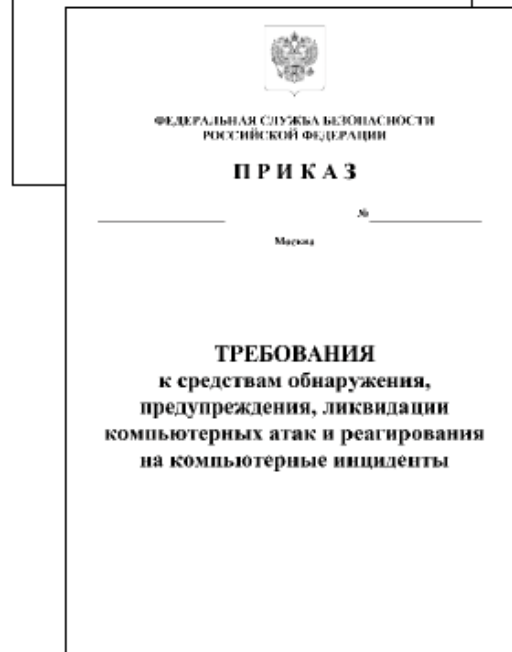
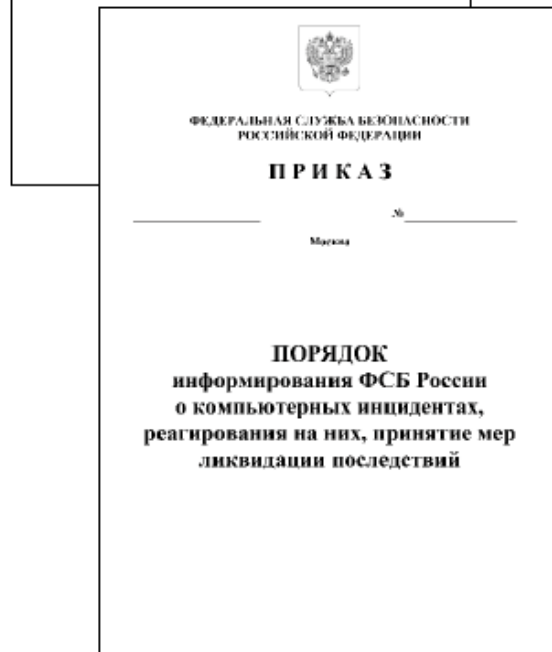
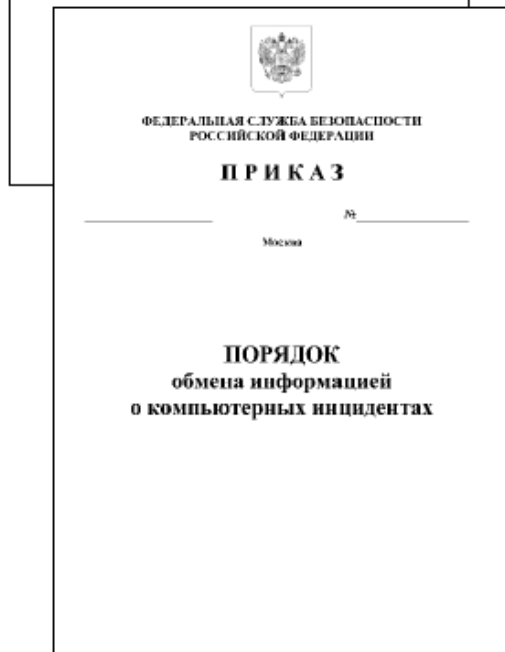
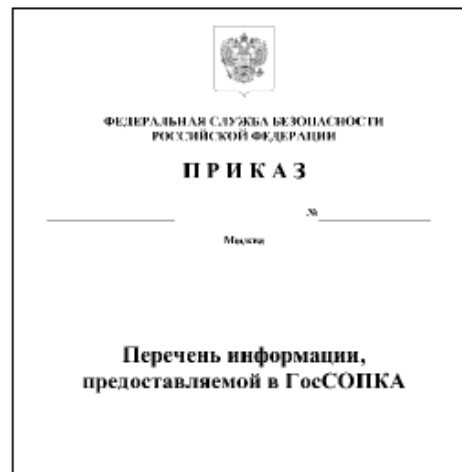
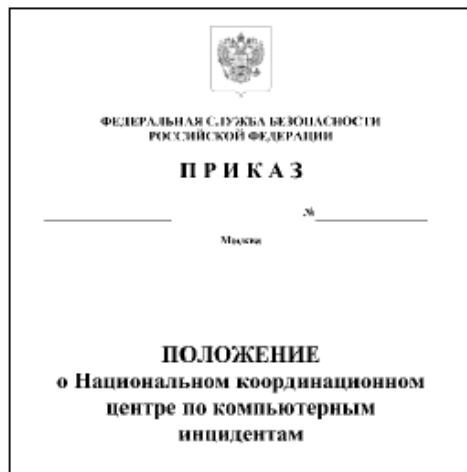
Директор по методологии и стандартизации

dkuznetsov@ptsecurity.com

Требования к техническим средствам ГосСОПКА глазами проектировщика

POSITIVE TECHNOLOGIES

ptsecurity.ru

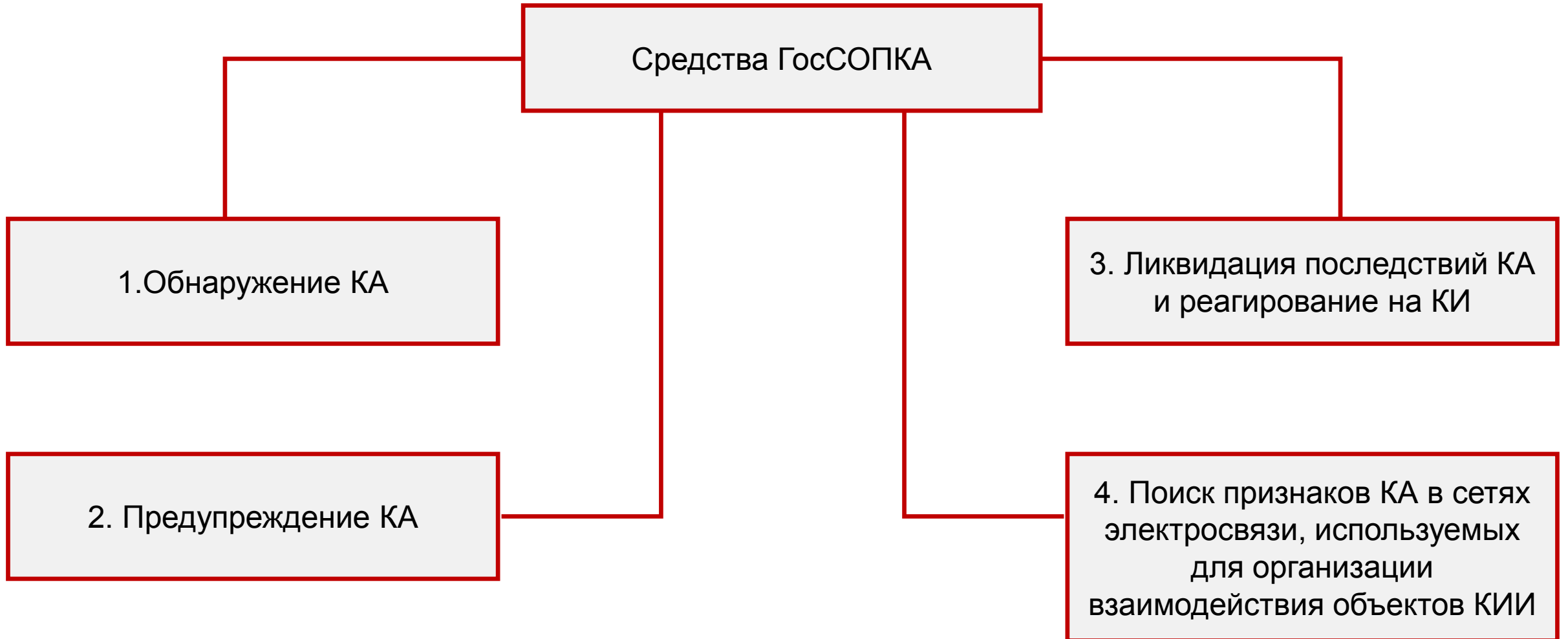


Развитием ГосСОПКА
занимается НКЦКИ –
Национальный
координационный центр по
компьютерным инцидентам



ГОССОПКА

Федеральная служба
безопасности
Российской Федерации



- Сбор и обработка инвентаризационной информации
- Сбор и обработка справочной информации
 - Сведения о “репутации” узлов
 - Сведения о “владельцах” узлов
 - Сведения о геолокации узлов
- Сбор и обработка сведений о защищенности
- Учет угроз безопасности информации

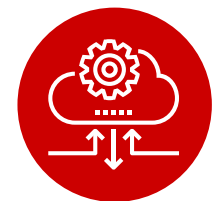
САЗ



База знаний

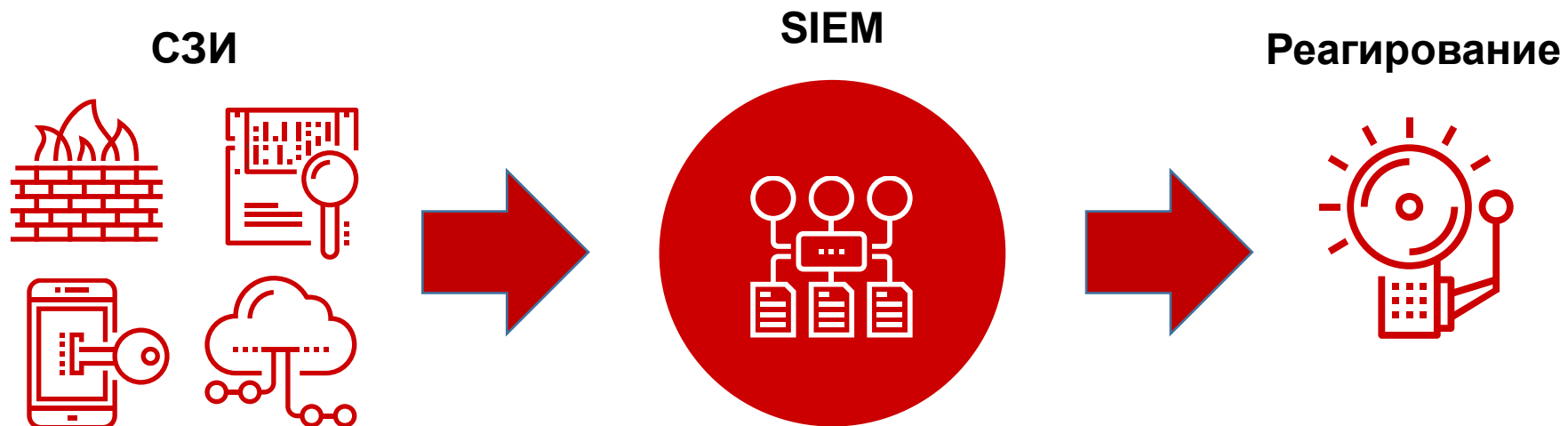


Внешние источники

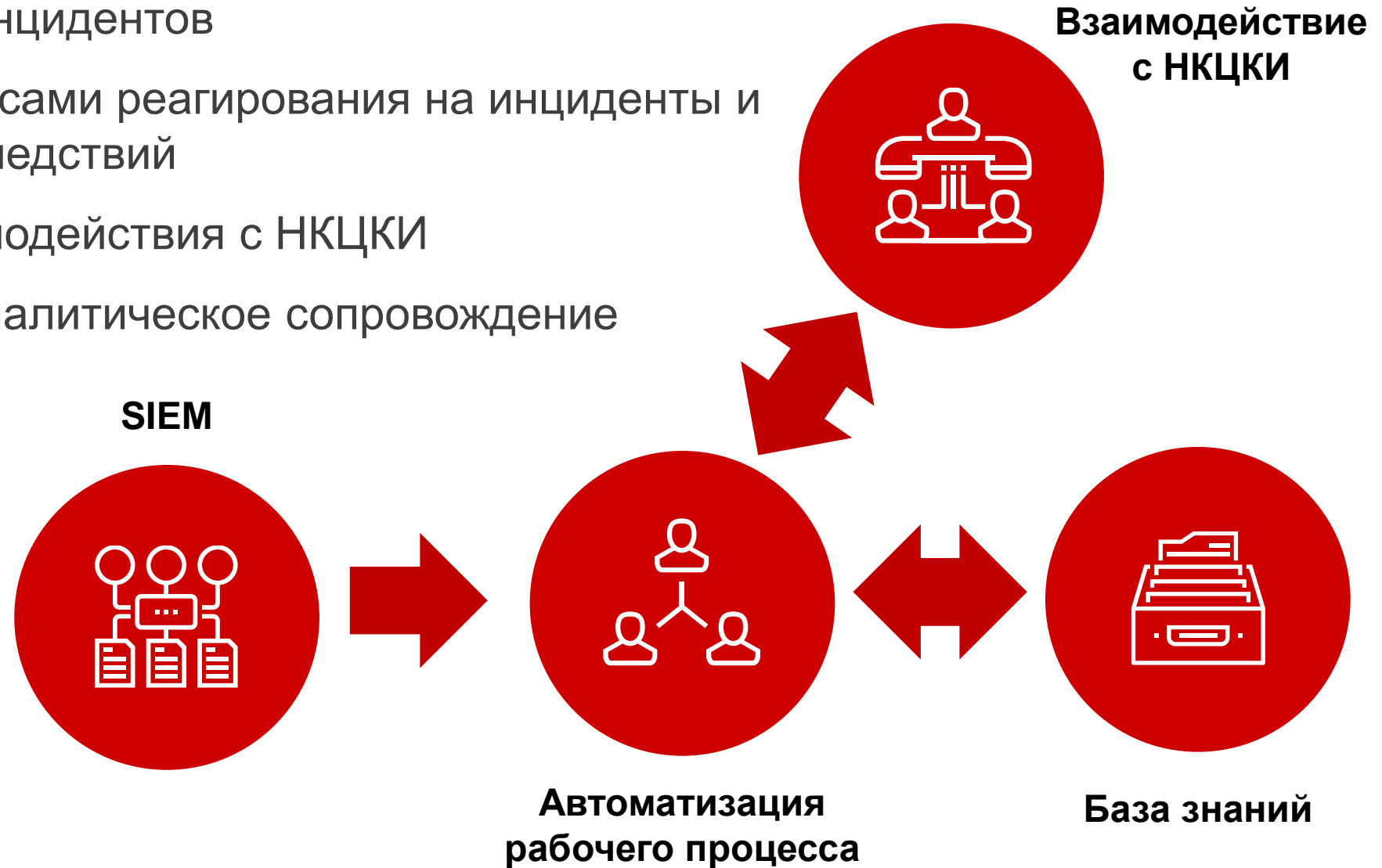


Средства обнаружения КА – функциональные возможности решений класса SIEM

- Сбор и первичная обработка событий ИБ из различных источников
- Автоматический анализ событий ИБ и выявление КИ
- Ретроспективный анализ



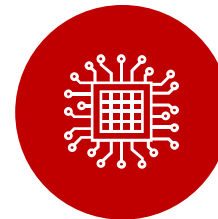
- Учет и обработка инцидентов
- Управление процессами реагирования на инциденты и ликвидации их последствий
- Обеспечение взаимодействия с НКЦКИ
- Информационно-аналитическое сопровождение



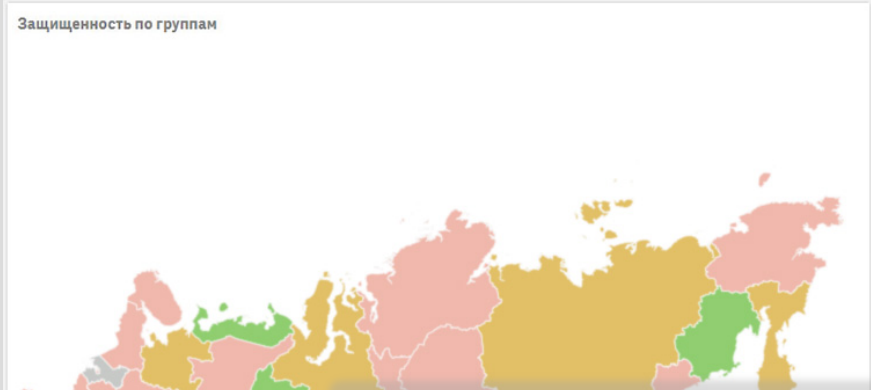
- Контроль настроек телеком оборудования
- Обнаружение признаков управления
- Обнаружение аномалий трафика и признаков компьютерных атак
- Анализ и хранение копий трафика
- Извлечение файлов из трафика
- Уведомление о фактах обнаружения признаков компьютерных атак



САЗ



**Средства анализа
сетевого трафика**



418 активов

- 582 активов можно добавить в систему
- 418 активов с запрещенным ПО (100%)
- 378 активов с уязвимостями высокого уровня (90%)
- 78 активов вовлечены в инциденты (19%)

175772 уязвимости

- 144388 уязвимостей высокого уровня (82%)
- 31149 уязвимостей среднего уровня (18%)

Показатели информационной безопасности инфраструктуры за Q3

Контроль защищенности

- Обнаружено High уязвимостей: 29,3%
- Обнаружено Medium уязвимостей: 41,7%
- Количество уязвимостей больше, чем в Q2, на: -
- Количество узлов с High уязвимостями: 49,3%
- Количество узлов с Medium уязвимостями: 26,6%
- Количество уязвимых узлов выросло с Q2 на: -

Контроль эффективности ИБ

- Устранено уязвимостей: -
- План сканирования узлов выполнен на: 29,3%
- Количество просканированных узлов выросло с Q2 на: -38,4%
- Заданная регулярность сканирования узлов соблюдена на: 50,4%
- План ввода в эксплуатацию компонентов МР выполнен на: 23,4%
- Работоспособность компонентов МР за период: ---

MaxPatrol SIEM

Стартовая страница События

Количество инцидентов за 24 часа

12

Количество активов за 24 часа

10 971

Средний поток событий (EPS) за 24 часа

5 000

Инциденты по критичности за 14 дней

Высокая Средняя Низкая

ТОП 10 уязвимых активов за 24 часа

IP/Domain	High	Medium	Low
10.0.208.165 (dc01-iss01.example.com)	10062,5	10062,5	10062,5
10.16.0.122	7981,3	7981,3	7981,3
10.20.1.167 (dc02-ad01.example.com)	7632,9	7632,9	7632,9
10.20.1.19 (dc02-sap01.example.com)	6932,2	6932,2	6932,2
10.20.1.19 (dc02-sap03.example.com)	5809,0	5809,0	5809,0
10.0.220.240	4244,6	4244,6	4244,6
10.0.209.255	2582,1	2582,1	2582,1

Инциденты по категориям за 14 дней

Обнаружение вредоносного ПО: 2 (40%)

Атака: 3 (60%)

Уязвимости по уровню за 24 часа

Низкий Средний Высокий

Управление активами

- Активы с запрещенным ПО: 3,7%
- Активы с обязательным ПО: 16,7%
- Соответствие лицензионной политики: ---
- Соответствие конфигурации оборудования: ---

Соответствие стандартам

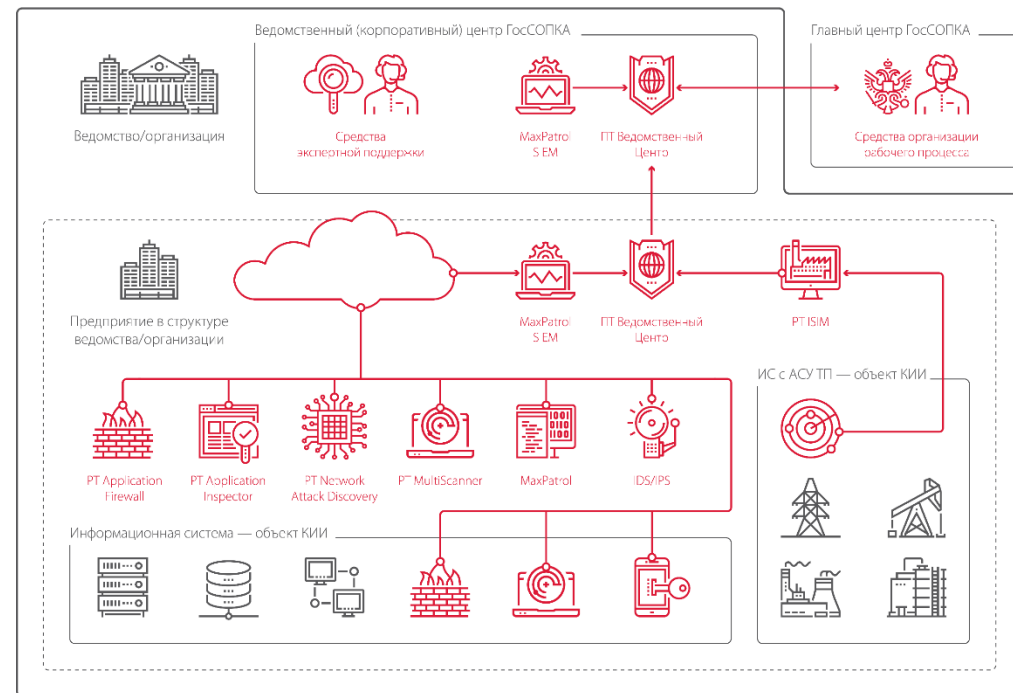
- Архангельской области: 31
- Архангельской области № 1: 1
- Архангельской области № 7: 7
- Иркутской области: 1
- Иркутской области № 1: 1
- Иркутской области № 2: 2
- Иркутской области № 3: 3
- Иркутской области № 4: 4
- Иркутской области № 5: 5
- Иркутской области № 6: 6
- Иркутской области № 7: 7
- Иркутской области № 8: 8
- Иркутской области № 9: 9
- Иркутской области № 10: 10
- Иркутской области № 11: 11
- Иркутской области № 12: 12
- Иркутской области № 13: 13
- Иркутской области № 14: 14
- Иркутской области № 15: 15
- Иркутской области № 16: 16
- Иркутской области № 17: 17
- Иркутской области № 18: 18
- Иркутской области № 19: 19
- Иркутской области № 20: 20
- Иркутской области № 21: 21
- Иркутской области № 22: 22
- Иркутской области № 23: 23
- Иркутской области № 24: 24
- Иркутской области № 25: 25
- Иркутской области № 26: 26
- Иркутской области № 27: 27
- Иркутской области № 28: 28
- Иркутской области № 29: 29
- Иркутской области № 30: 30
- Иркутской области № 31: 31
- Иркутской области № 32: 32
- Иркутской области № 33: 33
- Иркутской области № 34: 34
- Иркутской области № 35: 35
- Иркутской области № 36: 36
- Иркутской области № 37: 37
- Иркутской области № 38: 38
- Иркутской области № 39: 39
- Иркутской области № 40: 40
- Иркутской области № 41: 41
- Иркутской области № 42: 42
- Иркутской области № 43: 43
- Иркутской области № 44: 44
- Иркутской области № 45: 45
- Иркутской области № 46: 46
- Иркутской области № 47: 47
- Иркутской области № 48: 48
- Иркутской области № 49: 49
- Иркутской области № 50: 50
- Иркутской области № 51: 51
- Иркутской области № 52: 52
- Иркутской области № 53: 53
- Иркутской области № 54: 54
- Иркутской области № 55: 55
- Иркутской области № 56: 56
- Иркутской области № 57: 57
- Иркутской области № 58: 58
- Иркутской области № 59: 59
- Иркутской области № 60: 60
- Иркутской области № 61: 61
- Иркутской области № 62: 62
- Иркутской области № 63: 63
- Иркутской области № 64: 64
- Иркутской области № 65: 65
- Иркутской области № 66: 66
- Иркутской области № 67: 67
- Иркутской области № 68: 68
- Иркутской области № 69: 69
- Иркутской области № 70: 70
- Иркутской области № 71: 71
- Иркутской области № 72: 72
- Иркутской области № 73: 73
- Иркутской области № 74: 74
- Иркутской области № 75: 75
- Иркутской области № 76: 76
- Иркутской области № 77: 77
- Иркутской области № 78: 78
- Иркутской области № 79: 79
- Иркутской области № 80: 80
- Иркутской области № 81: 81
- Иркутской области № 82: 82
- Иркутской области № 83: 83
- Иркутской области № 84: 84
- Иркутской области № 85: 85
- Иркутской области № 86: 86
- Иркутской области № 87: 87
- Иркутской области № 88: 88
- Иркутской области № 89: 89
- Иркутской области № 90: 90
- Иркутской области № 91: 91
- Иркутской области № 92: 92
- Иркутской области № 93: 93
- Иркутской области № 94: 94
- Иркутской области № 95: 95
- Иркутской области № 96: 96
- Иркутской области № 97: 97
- Иркутской области № 98: 98
- Иркутской области № 99: 99
- Иркутской области № 100: 100

1. Средства ГосСОПКА субъекта КИИ – комплексная система

2. Только часть функций выполняется “коробочными” решениями

3. Средства ГосСОПКА взаимосвязаны с системой защиты объекта КИИ

4. Трудно обойтись без централизации





Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru