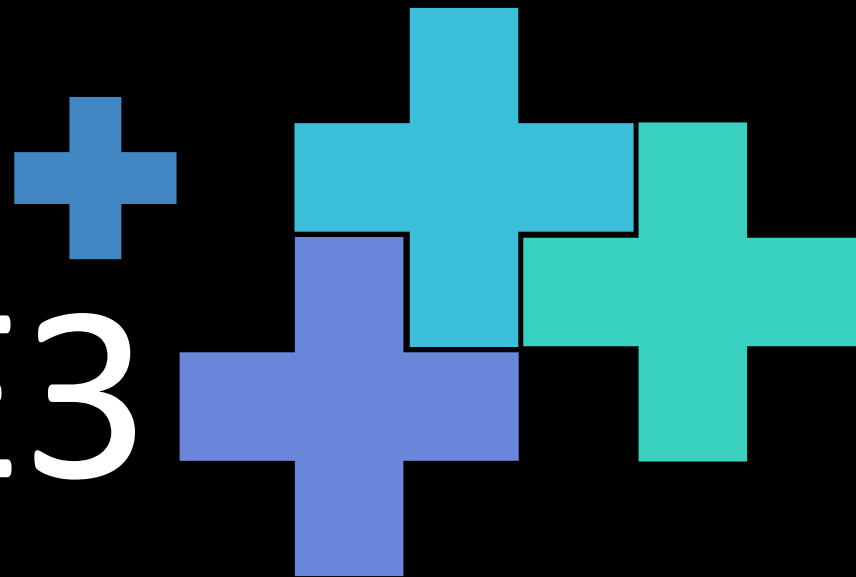


ИНФОбЕЗ

Natus est Scientia



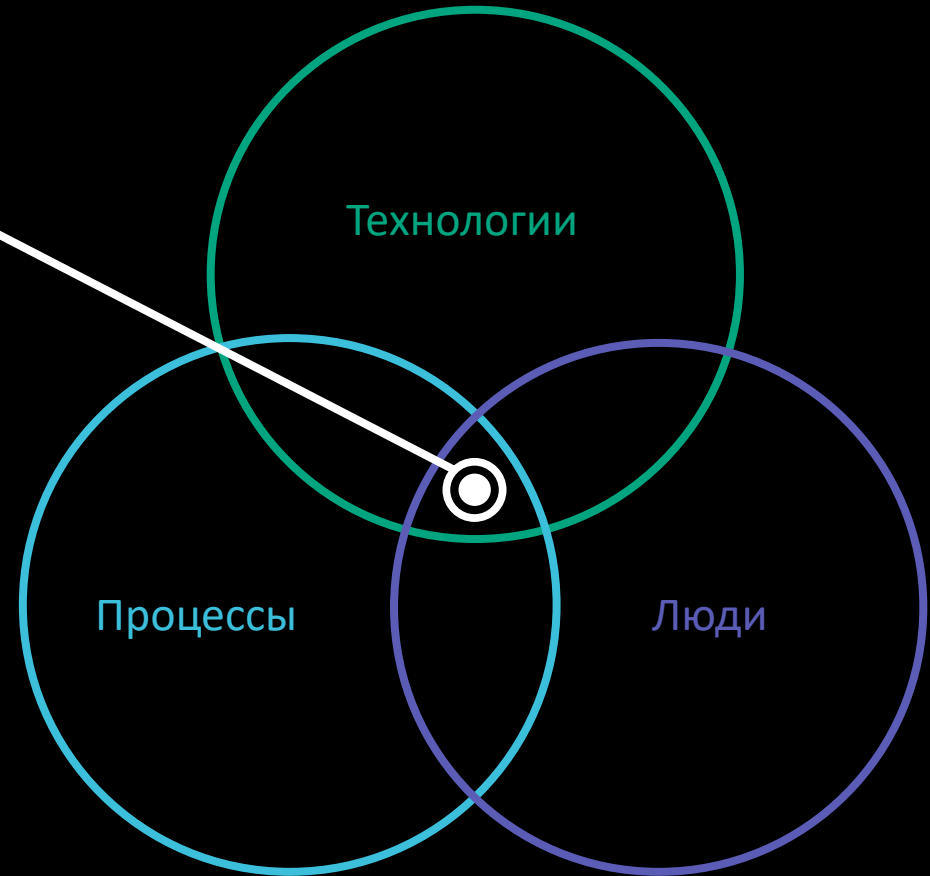
PROJECT SAFE DIGIT

4 уровень SOMM

Оценка SOC - Осмысленный

Эффективность SOC регулярно оценивается по метрикам производительности.
Процессы выстраиваются для достижения максимально возможного KPI

SOC



1 тип продукции:

- Device Lock
- Континент
- ROSA

2 тип продукции:

- OSSIM
- OpenVAS



Персонал

Руководитель
SOC

1-я линия

Первичная оценка
инцидентов,
отработка ложных
срабатываний

2-я линия

Детальный анализ
артефактов
инцидентов

3-я линия

Детальное
расследование
инцидентов

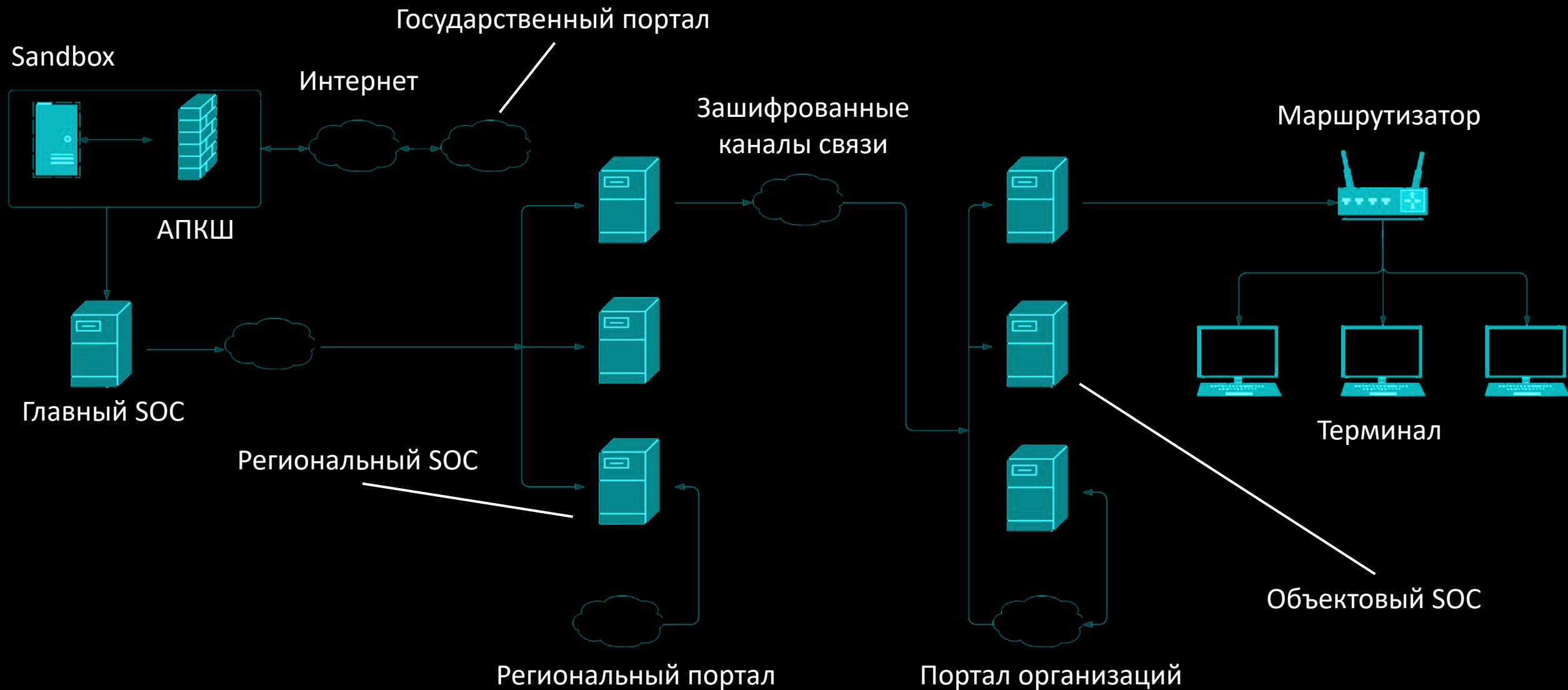
Аналитики

Написание
сценариев
реагирования,
внутренний анализ
угроз

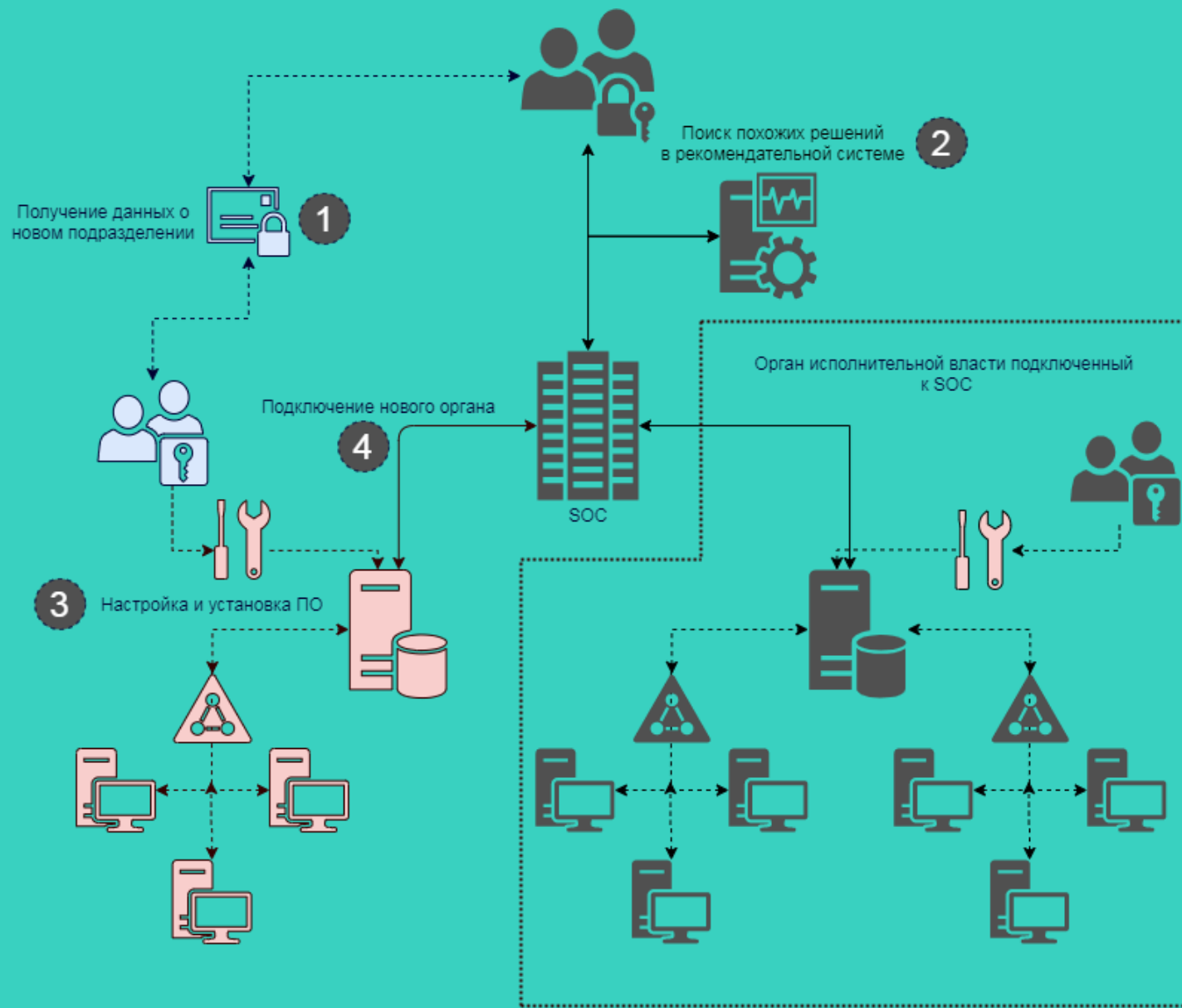
NN специалисты

Разработка и
обучение
нейронной сети для
выдачи инструкций

Масштабируемость

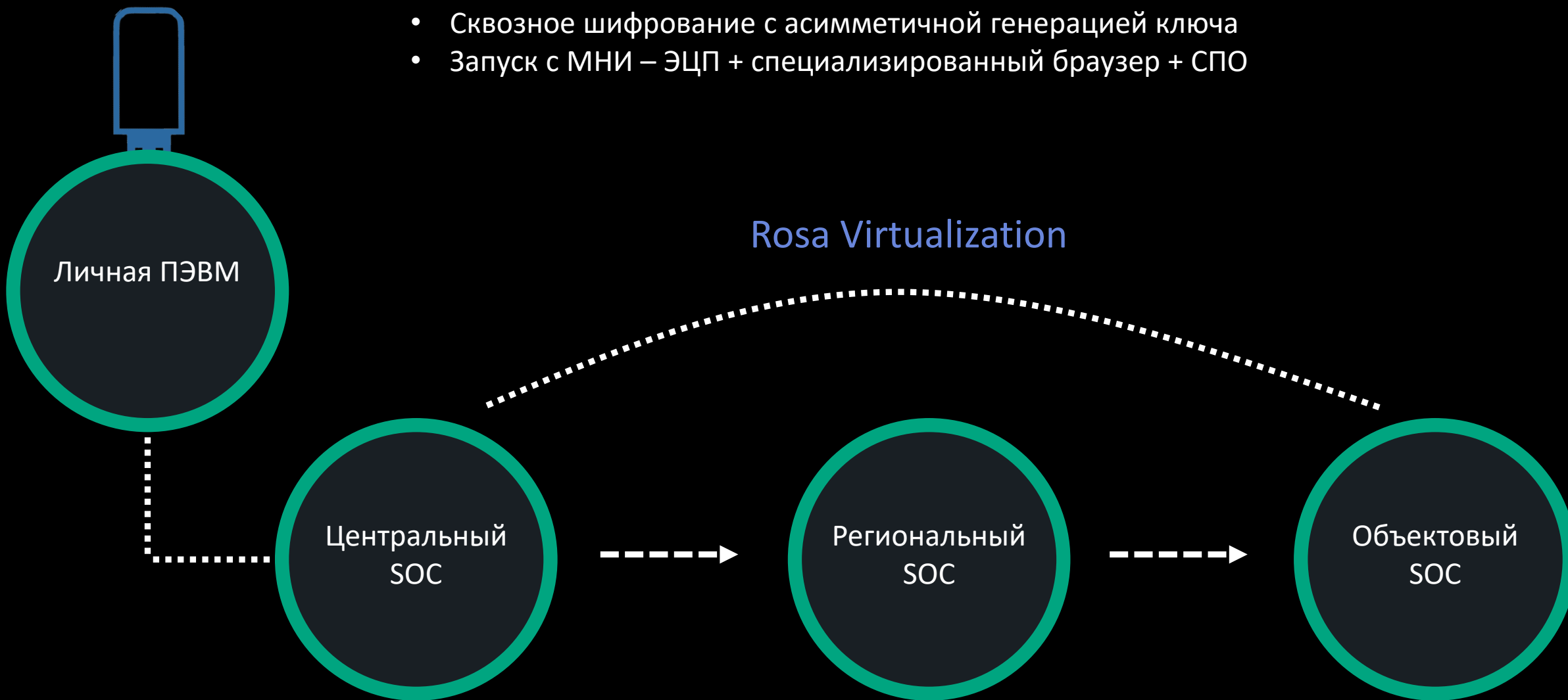


Рекомендательная система



Удаленная работа

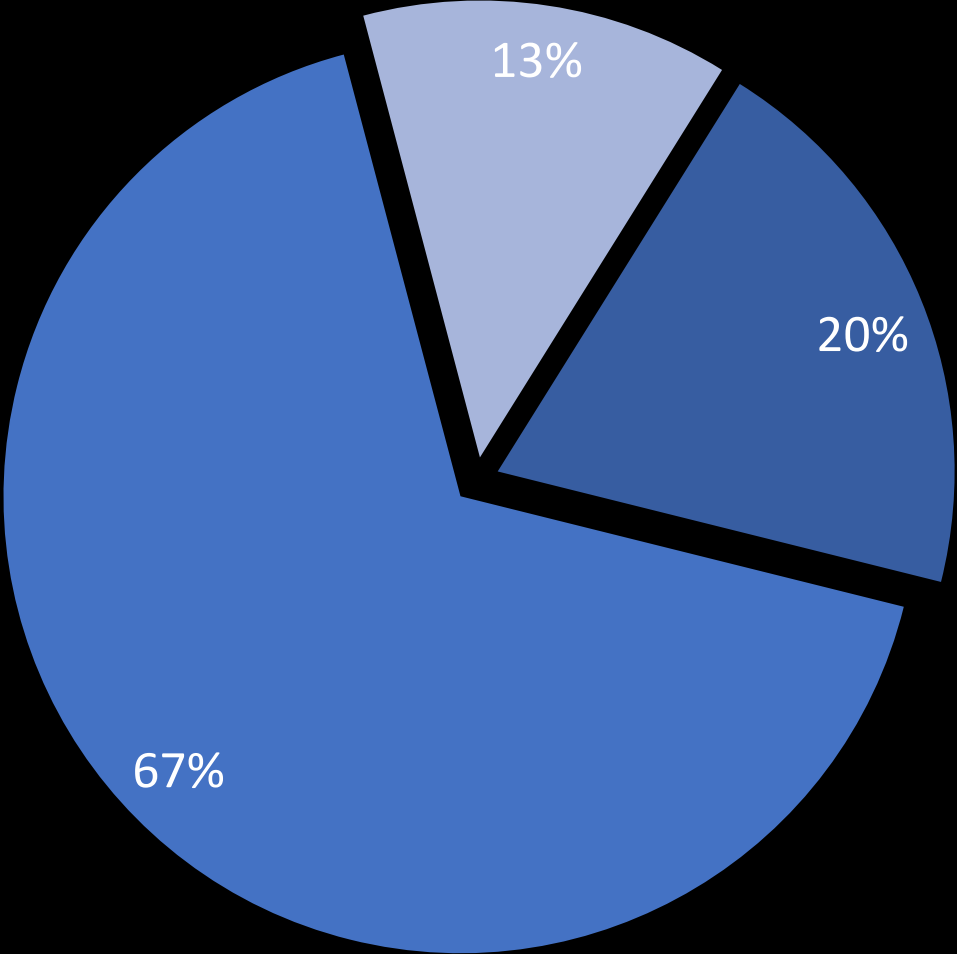
- Сквозное шифрование с асимметричной генерацией ключа
- Запуск с МНИ – ЭЦП + специализированный браузер + СПО



Экономический эффект

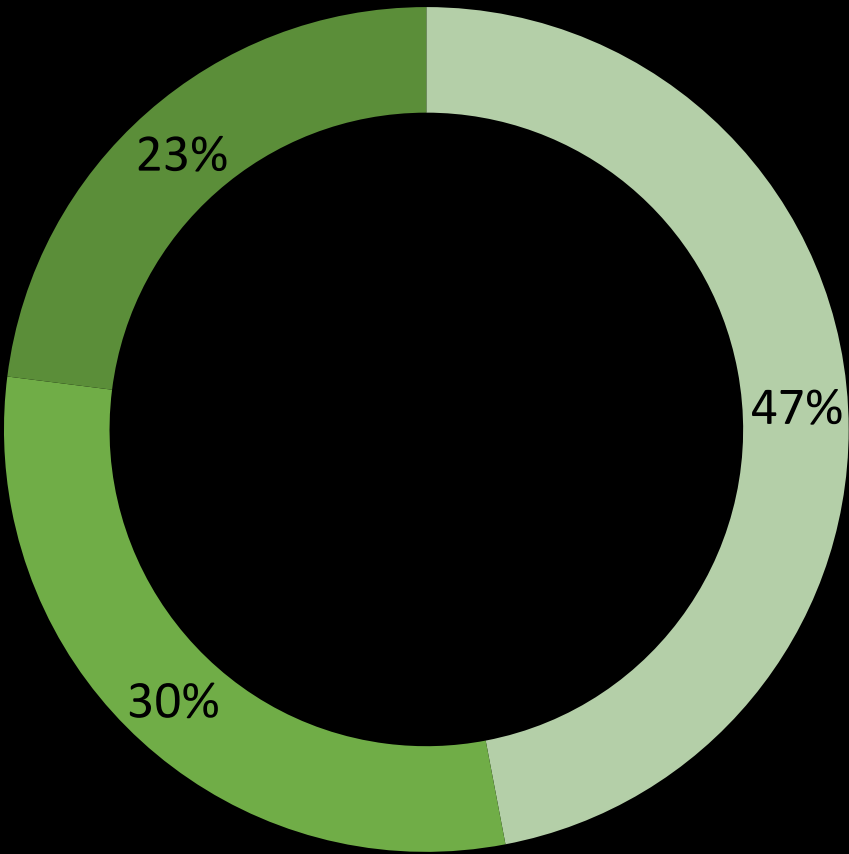


Использование аутсорсинга информационной безопасности



■ Да ■ Нет ■ Не знаю

Какие средства защиты подключены к системе мониторинга и управления ИБ



■ система мониторинга не используется
■ Все, имеющиеся в наличии
■ Подключены частично

Центральный SOC -
18 507 472р (30 ПЭВМ + 5 ПБ)

- АВЗ – средняя цена 2000р на год
- Secret Net LSP от 6000 р на год
- SafeERP Code Security 5000р
- СУСВ ROSA Virtualization 18400р
- АПКШ ЦУС Континент 3.6 – 1 212 560р.
- Threatcare – free
- DCImanager 98 628 р
- Щборудование в датацентр - 559 172 р

ПЭВМ 21 000р (10 000р)

- АВЗ – средняя цена 2000р на год
- Device Lock от 2000 р на год
- Secret Net LSP от 6000 р на год
- ROSA «Кобальт» 11 000Р либо ROSA Fresh - бесплатно



Расчетное время для начала
функционирования системы

Лето 2021

Итоговая готовность

Конец 2021



Кичкидов
Артем
@Yutzus



Новиков
Алексей
@Allifan



Масюков
Александр
@cerber_like_a_cat



Разроев
Александр
@Mr_Kak_Tak

Natus est Scientia



**KEEP
CALM
AND
FIX
BUGS**