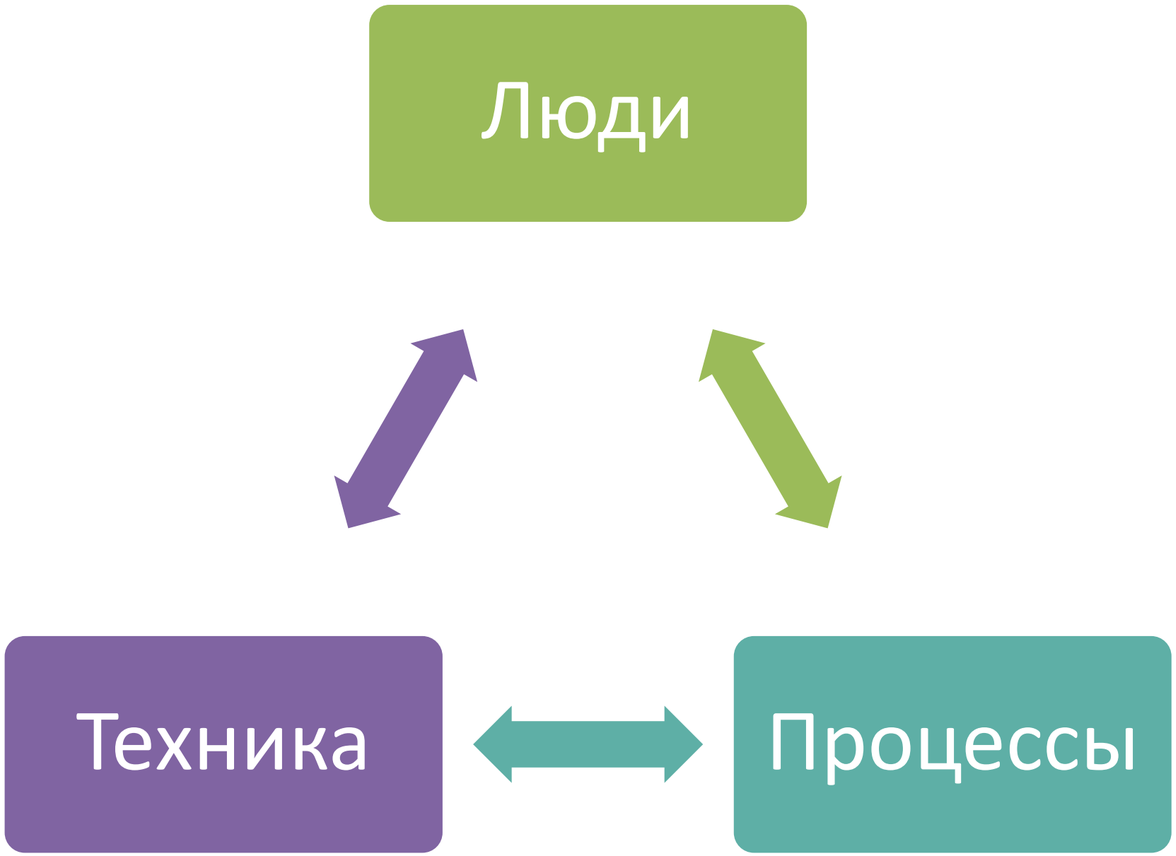
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Техника есть.
А людей и процессов нет.
Варианты решения организационных проблем обеспечения ИБ субъектов КИИ

Александр Пушкин

Технический директор

Три базовые составляющие для ИБ



Специфика КИИ

Техника (Средства)

- СЗИ от НСД
- Межсетевые экраны
- Средства обнаружения (предотвращения) вторжений
- Средства антивирусной защиты
- Средства контроля защищенности
- Средства управления событиями безопасности
- Средства защиты каналов передачи данных

Специфика КИИ

Техника (Средства)

1. 30 марта 2022г. - введены ограничения на приобретение иностранного оборудования и программного обеспечения для субъектов КИИ (Указ Президента от 30.03.2022 №166)

2. с 1 января 2025 г. организациям запрещается использовать средства защиты информации, произведённые в недружественных государствах (Указ Президента от 01.05.2022 №250)

Специфика КИИ

Процессы

1. Подключение к ГосСОПКА
2. Установить определённую структуру ответственности за обеспечение ИБ
3. Возможность привлекать только аккредитованные центры ГосСОПКА
4. Проводить постоянную оценку уровня защищённости своих информационных систем

Специфика КИИ

Люди (Силы)

- «Я не специалист по ИБ, меня из ИТ назначили»
- «У нас вся команда ИБ уволилась»
- «Этот подвед далеко, мы туда не поедем»

Люди — главный недостающий ресурс

Чтобы справляться с существующими угрозами, специалисты должны быть:

Компетентными / Актуальными / Осведомлёнными / Командными

Почему разработчика ПО подготовить легче, чем специалиста SOC?

Разработчик ПО

Специалист SOC

Разобраться, как проводятся атаки на ИС

Разобраться, как устроены типовые ИС

Получить опыт эксплуатации основных типов СЗИ

Основные пути решения кадровых проблем

1. Аутсорсинг функций ИБ
2. Либерализация требований к специалистам ИБ
3. Быстрое повышение квалификации и дополнительное обучение

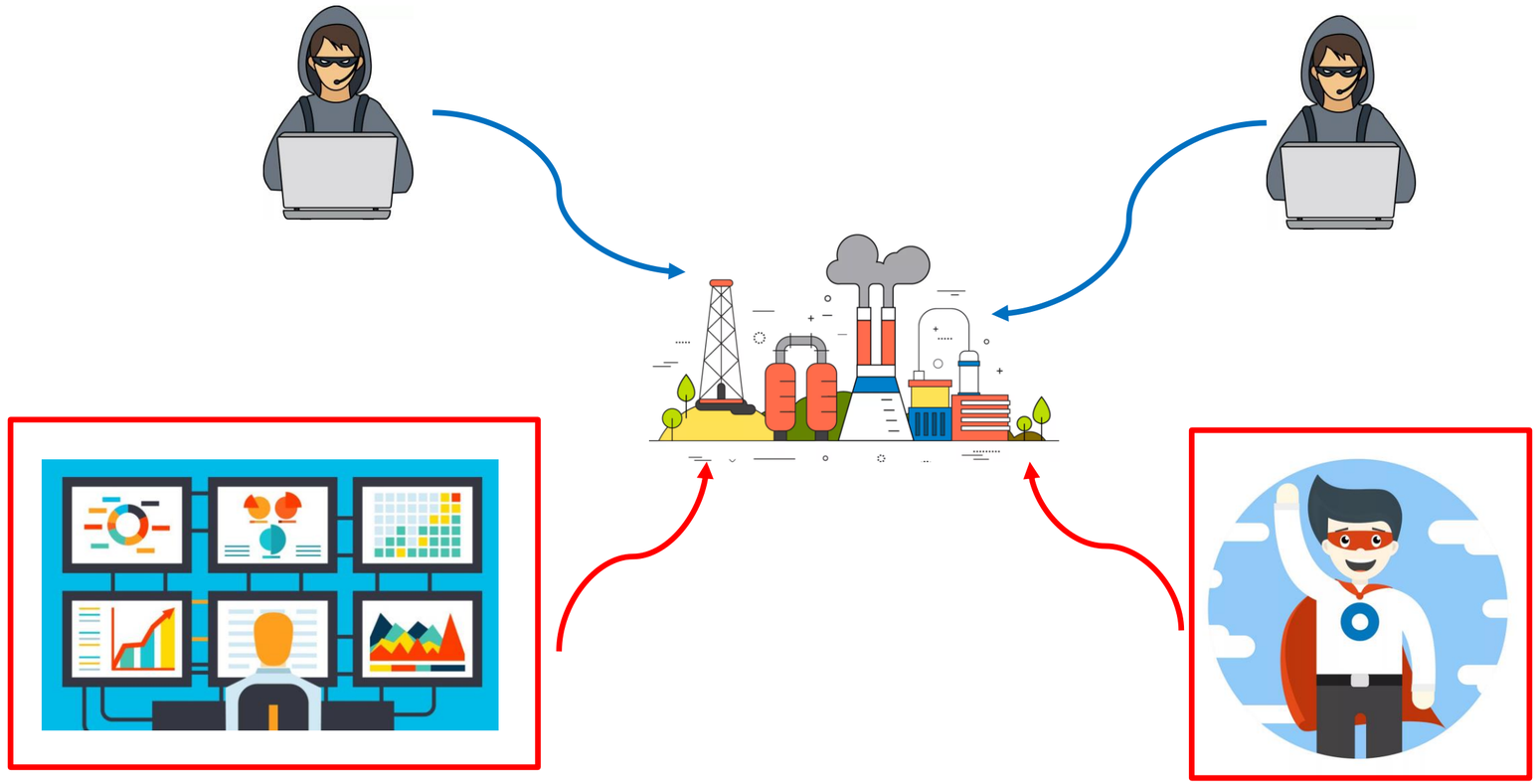
Либерализация требований к специалистам ИБ

1. Вывод ИБ на уровень среднего специального образования
2. Легализация самоучек
3. Создание системы сертификации ИБ специалистов

Быстрое повышение квалификации и дополнительное обучение

1. Стажерские программы для студентов
2. Программы дополнительного профессионального обучения
3. Использование учебно-тренировочных платформ (киберполигонов) для повышения компетенций

Киберполигон
Ampire



Развитие навыков

Проектировать
для защиты

Наблюдать
и управлять

Собирать и
использовать

Расследовать

Использовать и
поддерживать

Охранять и
защищать

Анализировать

Ampire в ВУЗах

Достигнутые результаты

1. Ampire основная практическая платформа для 12 ДПО
2. 72 сертифицированных преподавателя
3. 282 проведенных киберучений
4. 3 учебных программы на базе Ampire

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Александр Пушкин

Технический директор

@Nesergeevich

t.me/pm_public

amonitoring.ru