K2 кибер безопасность

Защита на максимум: как выстроить безопасность АСУ ТП эффективно

Егор Куликов
Руководитель направления безопасности КИИ и АСУ ТП

Подходы к защите АСУ ТП: разбираем их особенности

01

Формальный подход с учетом требований Приказа № 239

Сценарий

Разработка полного комплекта документов с учетом требований Приказа № 239

Каждая мера защиты имеет четкое описание и регламентированное выполнение без учета реалий производства

Строго определены этапы:

- Проектирование
  Отчет, МУ, ТЗ, ТРП, РД, ОРД, ЭД
- Реализация
  СМР, ПНР, ПМИ, ОЭ, перевод в промышленную эксплуатацию

Классический подход к проведению проекта

Обследование

01 Формирование рекомендаций, выявление и категорирование объектов КИИ, подготовка материалов для отправки регулятору

Требования

02 Разработка моделей угроз и требований к системам безопасности значимых объектов КИИ

Проектирование

03 Проектирование систем безопасности значимых объектов КИИ

Закупка ПО и оборудования

04 Закупка ПО и оборудования для построения СОИБ

Внедрение

05 Внедрение систем безопасности значимых объектов КИИ, включая обеспечение автоматизированного взаимодействия с органами исполнительной власти

Формальный подход с учетом требований Приказа № 239
Особенности

- Затяжные процессы согласований
- Долгий срок реализации
- Формальное закрытие мер приказа, реальная защита на втором плане
- Сертифицированные СЗИ устаревших версий
- Реализация по принципу «Работает — не трогай»

Если компания не подпадает под требования к КИИ
Сценарий

Эффективность на первом месте

Этапность зависит от приоритетности

Быстрейший запуск СЗИ без длительного проектирования

Далее второстепенные этапы и документы

Оптимизированный подход к этапам проекта

01 Обследование | Требования

Определение ключевых точек подключения оборудования

Подготовка первоочередных проектных документов

Подготовка требований к количеству оборудования и характеристикам

Необязательно — ТЗ

02 Закупка ПО и оборудования

Закупка ПО и материалов по спецификации

03 Проектирование | Внедрение

Оформление проектной документации

Внедрение систем безопасности

Если компания не подпадает под требования к КИИ
Особенности

Упрощенный процесс согласований

Срок реализации значительно меньше

Выбор СЗИ экспертным методом, в первую очередь ключевые СЗИ

Возможность применения последних версий СЗИ

Подготовка критичных документов для реализации — в первую очередь

Не только для КИИ: почему всем организациям нужно задумываться об эффективности ИБ вне требований регуляторов

02

Почему всем предприятиям надо задумываться об эффективности ИБ

В каждом бизнесе есть критичные процессы, которые влияют на непрерывность производства и остановка которых влечет ущерб:

- Финансовый
- Репутационный
- Жизни и здоровью человека и общества

Злоумышленники действуют из политических целей, и им интересны разные отрасли, а не ОКИИ

Нелегитимные действия сотрудников, имеющих доступ к компонентам АСУ ТП

K2 кибер безопасность

Эффективность ИБ вне требований регулятора

Эффекти́вность (лат. effectivus) — соотношение между достигнутым результатом и использованными ресурсами

Не ограничивайтесь базовым набором — опирайтесь на требования к категориям и оценивайте эффективность исходя из особенностей инфраструктуры

Базовый набор

- МЭ
- ВМБ
- SIEM
- СОВ
- Защита конечных точек

Расширенный набор решений и мер

- Защищенный удаленный доступ
- СКЗИ
- Анализ защищенности
- МЭ
- ВМБ
- SIEM
- СОВ
- Защита конечных точек
- EDR:
  — Реагирование
  — Процессы, запущенные на узле
  — Открытые сетевые соединения
  — Изменения файлов
  — Изменения объектов системного реестра Windows

Набираем скорости: как сократить срок реализации проекта

03

Кто и что позволяет сократить срок реализации проекта

Функциональный заказчик, который хорошо понимает специфику производства и ее инфраструктуру, а также готов сформировать требования

Экспертный анализ инфраструктуры для определения, какие СЗИ требуют первоочередной реализации

Дорожная карта реализации СОИБ

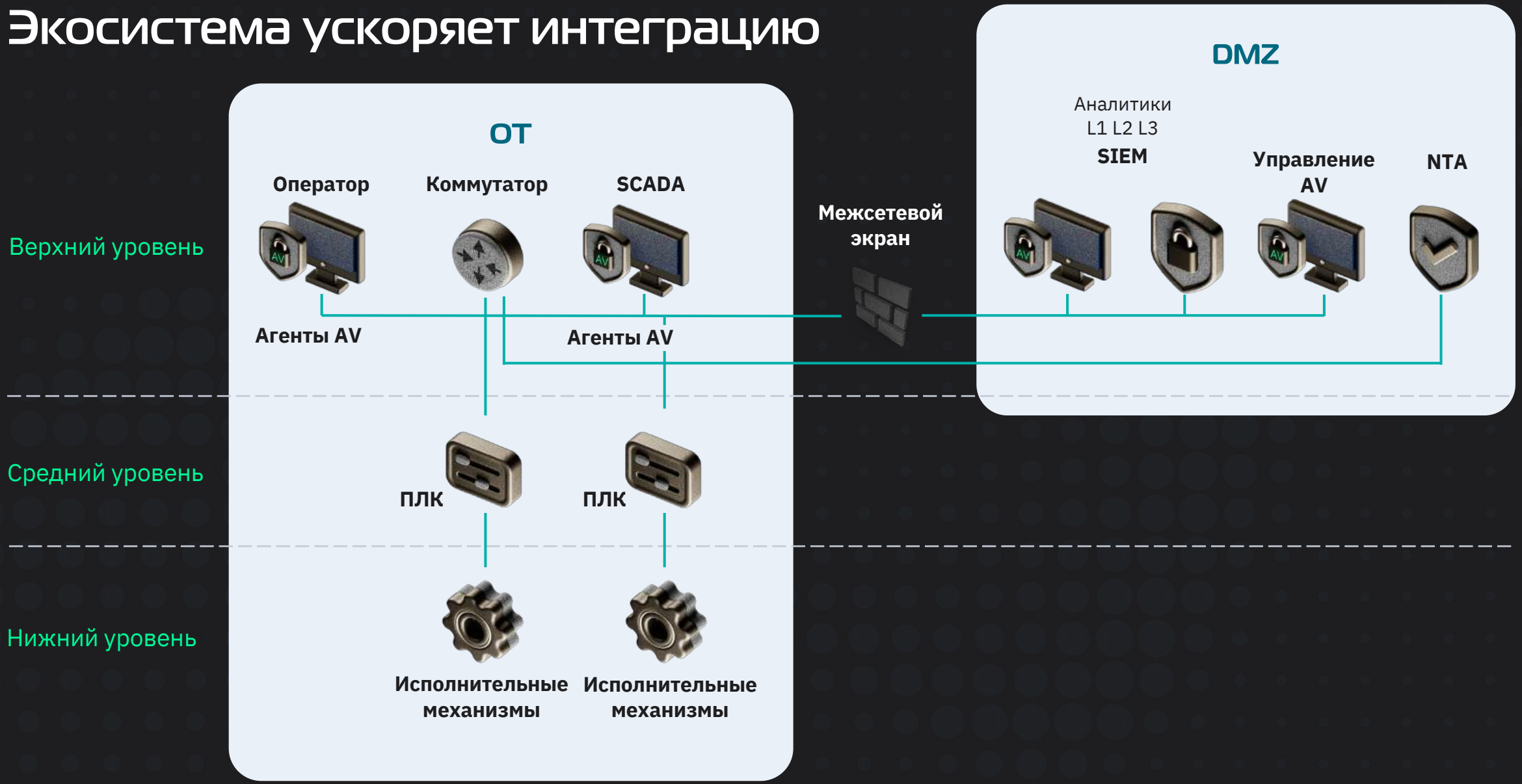
Четкое разграничение ролей участников проекта между смежными ИТ-, ИБ- и службами АСУ ТП

Выбор квалифицированного исполнителя — обязательно личное интервью при его выборе

Секрет успеха результативного проекта, или Причем тут грамотно выстроенная архитектура и экосистемность

04

Экосистема ускоряет интеграцию



Подход к выбору решений

Уже есть СЗИ в сегменте АСУ ТП

1. Анализ применяемых СЗИ
2. Определить дополнительный набор СЗИ
3. Оценить возможность интеграции ключевых решений в экосистему

Строим с нуля

1. Выбор ядра экосистемы, вокруг чего собирается набор решений — SIEM, СОВ
2. Выбор дополнительных СЗИ — МСЭ, EDR и т.д.

Проектный опыт

Проектирование защиты АСУ ТП

4 месяца на проект | **4 выезда** на площадку | **450 агентов** антивируса на АРМ и серверах | **10 производственных VLAN** подключили к NTA

О клиенте

Клиент — крупный производитель из отрасли легкой промышленности с множеством технологических процессов в рамках фабрики. Ранее предприятие входило в зарубежную группу компаний, а после — полностью локализовано на территории РФ.

Что сделали

- Провели детальный анализ событий от АРМ
- Сделали глубокий анализ событий сетевого трафика
- Реализовали интеграцию конечных точек с KICS for Networks посредством KEA

Результат

- Настроили антивирус в блокирующий режим
- Получили корректный список разрешающих правил для NTA
- Получили подробную инвентаризацию защищаемых активов и возможность для реагирования на события ИБ

Ждем вас на нашем стенде № 6.2

Егор Куликов

Руководитель направления безопасности КИИ и АСУ ТП

E-Mail: EKulikov@k2int.ru

Telegram: @egork79

K2 кибер безопасность