K2 кибер безопасность

Егор Куликов
Руководитель направления
безопасности КИИ и АСУ ТП

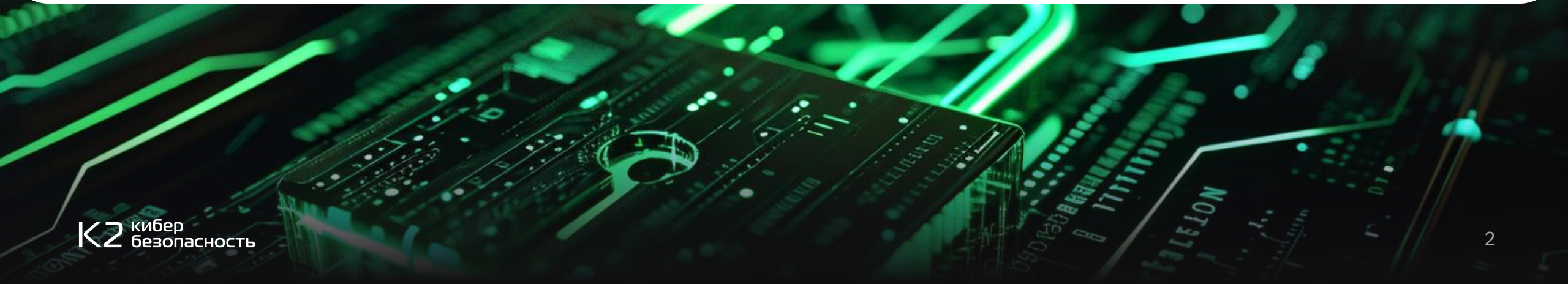
Надежность средств защиты АСУ ТП : взгляд эксперта

Надежность средств защиты АСУ ТП

Расскажем

- На что обратить внимание при выборе ПО и железа
- Как предусмотреть основные риски
- Как обеспечить стабильную работу системы

Надежность = ПО ⊕ железо ⊕ интеграция



Наиболее часто применяемые механизмы безопасности в АСУ ТП:

01
Встроенные механизмы безопасности

02
Межсетевые экраны (МСЭ)

03
Средства криптографической защиты информации (СКЗИ)

04
Антивирусная защита

05
Система обнаружения вторжений (СОВ)

06
SIEM-системы

Типичные сложности на уровне предприятий

Неготовность инфраструктуры к внедрению средств защиты

Обеспечение совместимости средств защиты с АСУ ТП

Устаревшие либо неполные данные, полученные при обследовании

Дефицит технологических окон

Организационные сложности

Типовые кейсы
Заниженные технические характеристики СЗИ

Ситуация

Изначально получили неточную информацию от заказчика

На практике количество трафика оказалось больше, чем ожидали

Последствия

- Технические характеристики решения были заложены некорректно
- Вышли из строя жесткие диски на серверах

Решение

- Получили точные данные по трафику
- Провели апгрейд оборудования
- Докупили жесткие диски большего объема

Рекомендации

- Проводить регулярный аудит
- Иметь в наличии ЗИП
- **10%** — обязательный запас для заказчиков с территориально-распределенной инфраструктурой

Типовые кейсы
Слабые АРМ и серверы

Ситуация

В АСУ ТП используются устаревшие АРМ или серверы

Хосты работают на пределе возможностей

Последствия

Дополнительная нагрузка

Средства защиты снизили производительность и время отклика

Рекомендации

- Предварительное тестирование для систем, с которыми отсутствует подтверждение совместимости с СЗИ
- Замена или апгрейд устаревшего оборудования
- **Гибкая настройка средств защиты**
  Оставить только базовые функции защиты и отключить дополнительные

Типовые кейсы
МСЭ блокирует важный сетевой трафик

Ситуация

В результате обследования были получены неточные данные от заказчика по типу проходящего трафика

Сети создавались хаотично, а из-за текучести кадров в организации часть информации о настройке сети была утеряна

Последствия

Возникла проблема на уровне решения – МСЭ блокирует важный трафик

Рекомендации

- После установки МСЭ необходимо как минимум 1-2 недели отслеживать проходящий через МСЭ трафик. В режиме мониторинга, не включая режим блокирования
- Регулировка настройки доступа трафика
- По результатам мониторинга — дополнение правил на МСЭ

Устойчивость систем и частота поломок

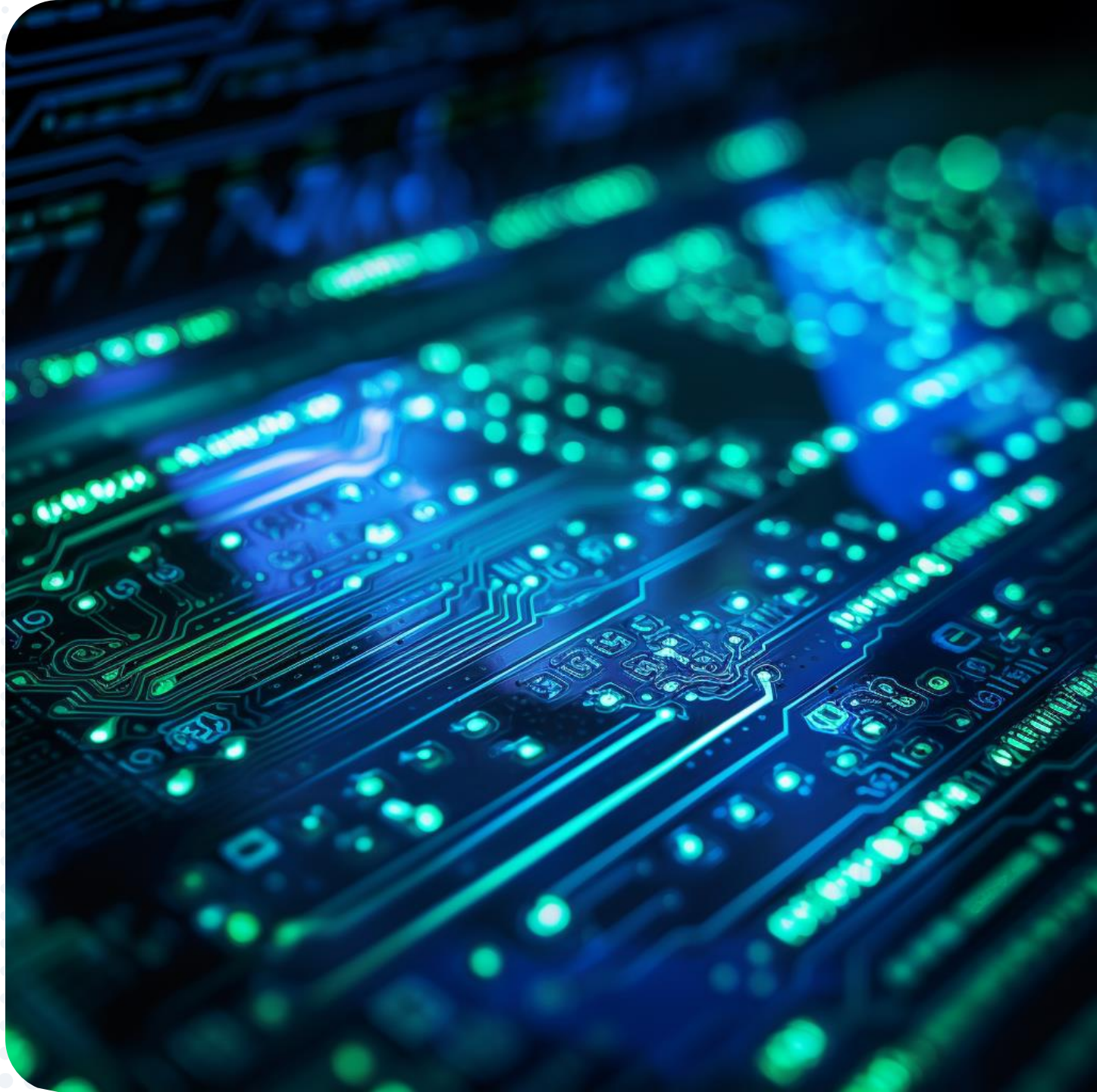
0,1% МСЭ

5% АРМ и серверы

2,5% Проблемы совместимости СЗИ

2,5% Проблемы с оборудованием

10% СОВ (оборудование)



K2 кибер безопасность

Выводы

Использовать решения

- от вендоров с хорошей репутацией на рынке
- прошедшие тестирование на совместимость
- которые могут работать в двух режимах — мониторинг или блокировка
- сертифицированные — важно для тех, кто подпадает под требования регуляторов

Не забывать про резервное копирование и ЗИП

Выбирать специалистов с опытом работы с АСУ ТП и в ИБ

Вместе на пути к вершине кибербезопасности

Аудит структуры АСУ ТП

- Обследование
- Оценка уровня защищенности АСУ ТП

Проектирование

- Подбор оптимальных отечественных решений
- Обеспечение их совместимости

Внедрение и техподдержка

- Настройка решений
- Закупка
- Обучение
- Техподдержка

K2 кибер безопасность

Подробнее на сайте

Ждем вас на нашем стенде
3 этаж, около лестницы