Kaspersky Industrial Cybersecurity Conference 2023

Best practice по сокращению пути внедрения комплексных систем защиты АСУ ТП

Андрей Заикин
Директор по развитию бизнеса в направлении кибербезопасности K2Tex

kaspersky

Исследование готовности и реакции бизнеса к законодательным требованиям защиты КИИ

Целевая аудитория:

Субъекты КИИ

Собственная выручка > 5 млрд рублей

90%

компаний приступили
к выполнению требований 187-ФЗ

На каком этапе сейчас реализация проектов?

8% завершили проекты

15% на завершающих этапах

38% в процессе организационной работы

39% только начинают или планируют начать

K2TEX

Сложности при реализации проектов

В каждой 5-ой

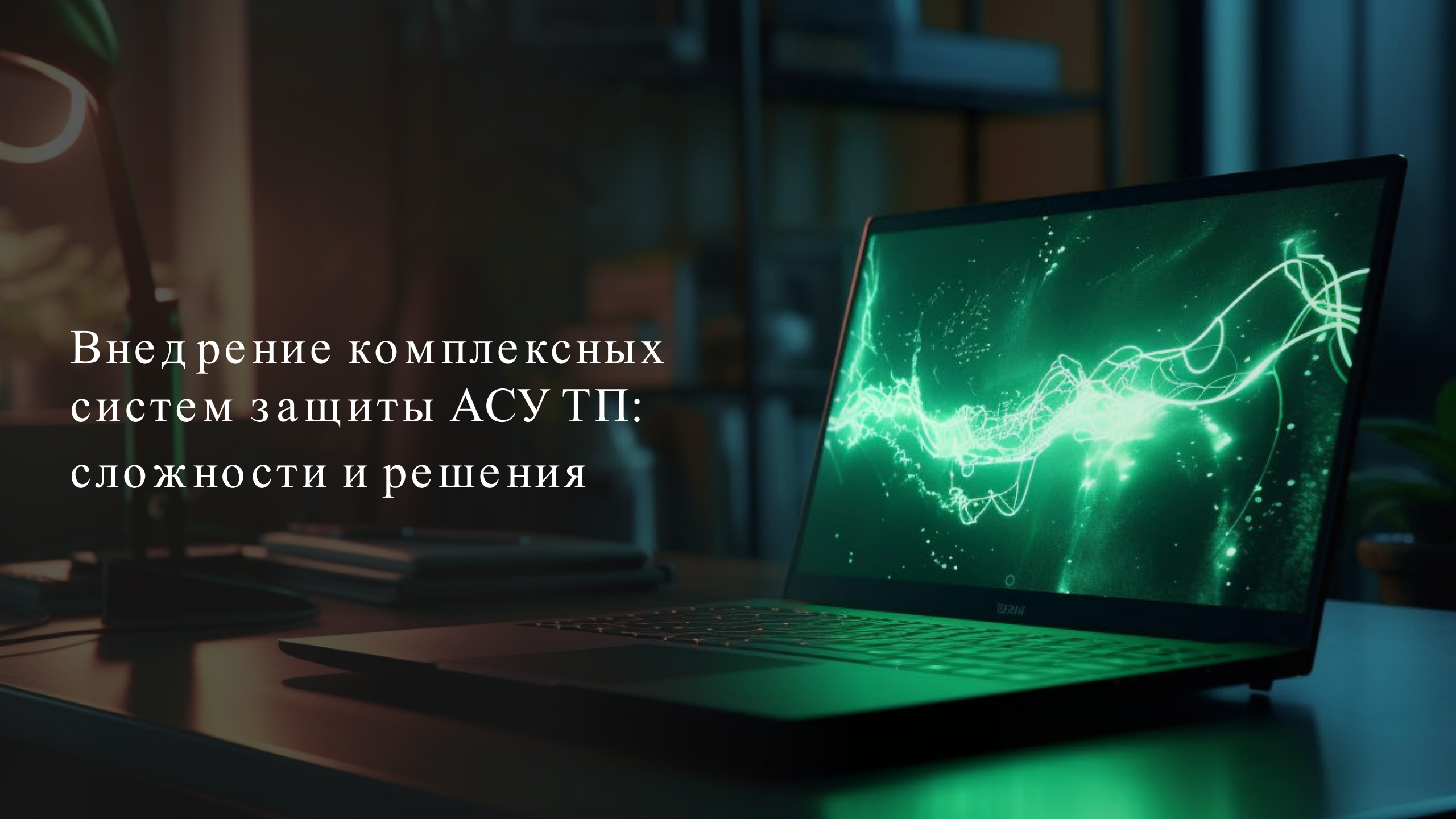
не успеют реализовать проекты к 2025 году

27%

испытывают проблемы при подборе и закупке российских решений, замене иностранных

K2TEX

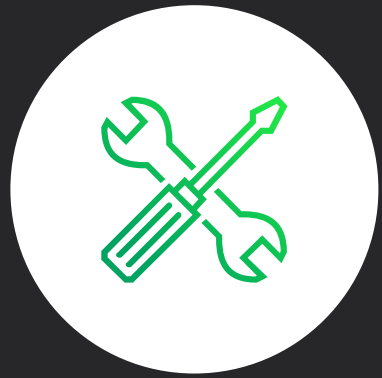
Внедрение комплексных систем защиты АСУ ТП: сложности и решения



Типичные сложности на уровне предприятий

Организация защищенной сетевой инфраструктуры

Неготовность инфраструктуры к внедрению средств защиты



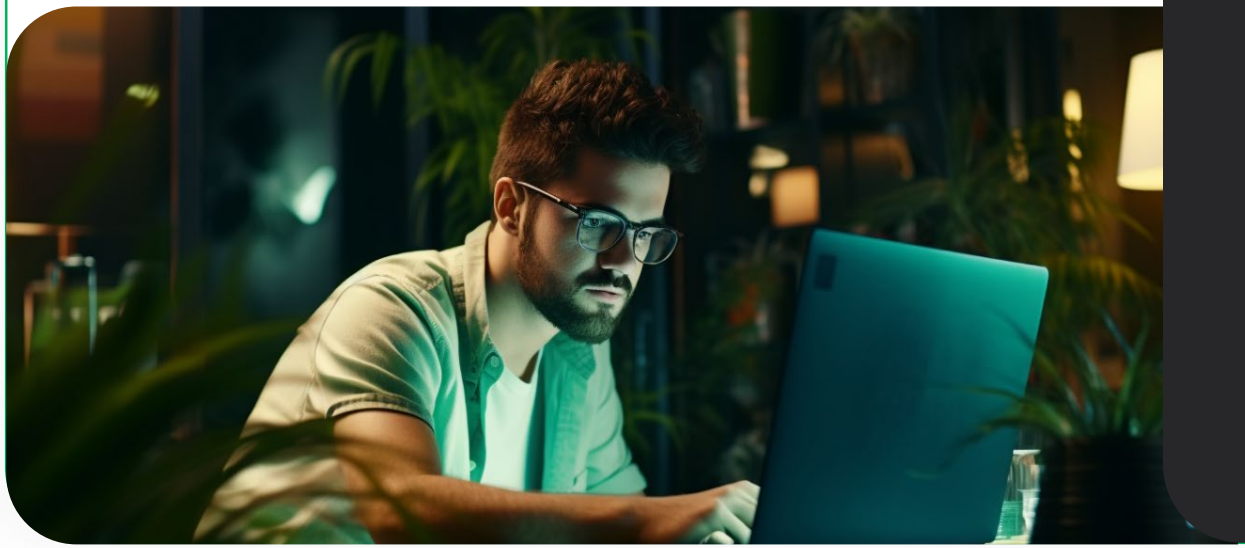
Устаревшие либо неполные данные, полученные при обследовании

Обеспечение совместимости средств защиты с АСУ ТП

Организационные проблемы

Ситуация

Устаревшие либо неполные данные,
полученные при обследовании



Рекомендации

Собрать информацию:

- об объектах АСУ ТП
- о смежных системах
- о готовности инженерной инфраструктуры

Уточнить отраслевую специфику

Организовать встречи
с представителями технического блока

Проблемы сетевой сегментации

Ситуация

Кейс 1

Корпоративная и технологическая сети физически находятся в одной плоской сети, нет межсетевых экранов и маршрутизаторов

Кейс 2

ЗОКИИ находятся в единой сети с другими системами АСУ ТП

Рекомендации

Выполнить физическое разделение корпоративной и технологической сетей

Провести сегментацию технологической сети с учетом категорирования АСУ ТП

- провести инвентаризацию оборудования АСУ ТП
- выполнить перепроектирование сетей

Неготовность инфраструктуры к внедрению средств защиты

Ситуация

Потребность в прокладке СКС

В шкафах нет места для оборудования средств защиты

Недостаточно питания и охлаждения для оборудования средств защиты

Рекомендации

- Обследовать инженерную инфраструктуру для размещения оборудования средств защиты
- Заложить в сметы необходимое оборудование на этапе техно-рабочего проектирования

Вопросы технической совместимости средств защиты и компонентов АСУ ТП

Как и чем подтвердить совместимость средств защиты с компонентами АСУ ТП?

Системы отсутствуют в перечне совместимых со средствами защиты, что делать?

Устаревшие системы, возможно ли получить для них официальное подтверждение совместимости?

Могут ли **обновления средств защиты** повлиять на функционирование АСУ ТП?

Системы на гарантийной поддержке вендора АСУ ТП, как установить средства защиты?

Слабые АРМ и серверы

Ситуация

В АСУ ТП используются устаревшие АРМ или серверы. Хосты работают на пределе возможностей, дополнительная нагрузка в виде средств защиты может снизить производительность и время отклика.

Рекомендации

Гибкая настройка средств защиты

- Настроить только базовые функции защиты, отключить дополнительные
- Заменить устаревшее оборудование

Нагрузка при обновлении

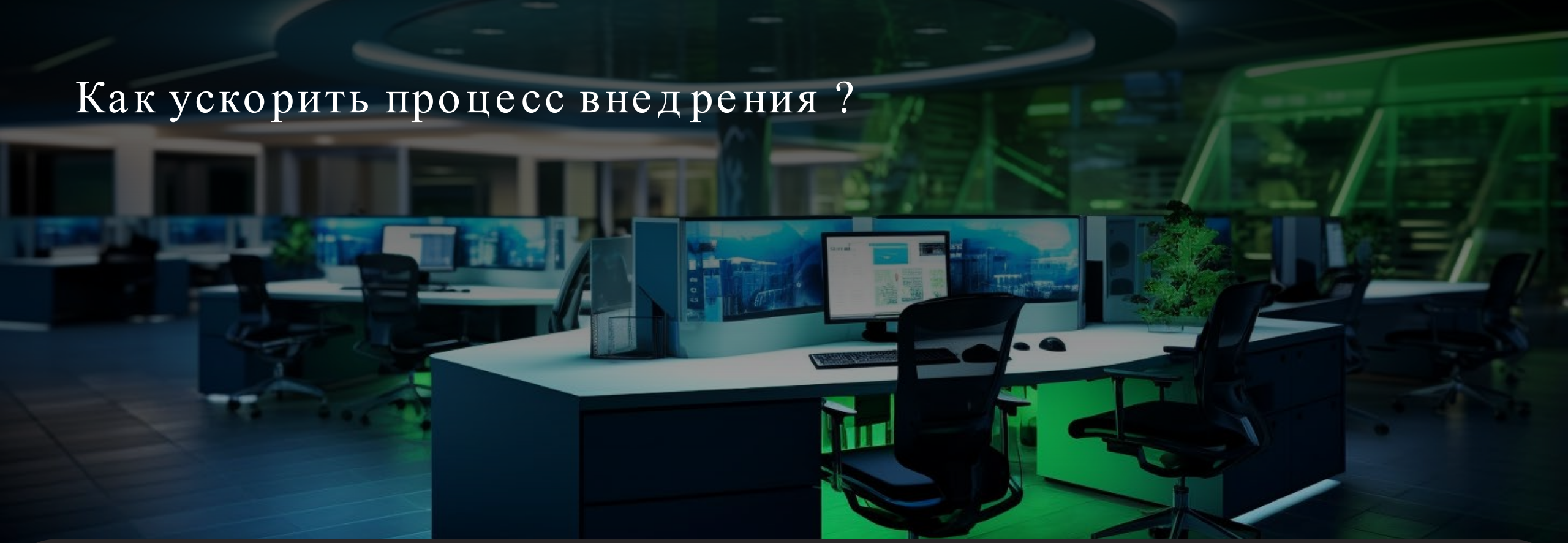
Ситуация

При обновлении антивирусных баз АРМ или сервер испытывает дополнительную нагрузку. Возможны ложные срабатывания антивируса – серьезная угроза для критичного оборудования.

Рекомендации

Настроить разное время обновления баз и проверок для более и менее критичных АРМ и серверов

Как ускорить процесс внедрения ?



01

Работа
с персоналом
АСУ ТП

02

Назначение
ответственных
по площадкам

03

Внедрение
за рамками
технологических
окон

04

Применение
конфигурационных
файлов

05

Временная работа
межсетевого экрана
в режиме мониторинга

K2TEX

Резюме

Преимущества работы с K2Tex

Комплексный подход

на проектах работают команды ИБ, инфраструктуры, телекоммуникаций

2000+

проектов по ИБ

Команда

инженеров ИБ + АСУ ТП

Практический опыт

построения безопасности для ЗОКИИ

azaikin@k2.tech

kaspersky