



Kaspersky
Industrial
CyberSecurity

Актуальные вызовы и возможности для информационной безопасности промышленных систем и предприятий

Петухов Алексей
Руководитель направления защиты промышленных систем



Наша роль в мировом сообществе по IT и OT-безопасности



Мы участвуем в расследованиях и операциях по противодействию киберугрозам совместно с мировым сообществом по информационной безопасности, международными организациями, такими как Интерпол и Европол, правоохрательными органами и центрами CERT по всему миру. «Лаборатория Касперского» – официальный партнёр Европола.



Мы организуем регулярные учебные курсы для сотрудников Интерпола, Европола и полицейских структур в ряде стран, например, для полиции Лондона



Наши эксперты выступают на мировых конференциях, например, на Всемирном экономическом форуме в Давосе



Мы ежегодно проводим конференцию Security Analyst Summit, которая объединяет лучших экспертов в вопросах IT-безопасности



Мы участвуем в некоммерческой международной инициативе Securing Smart Cities, направленной на решение проблем кибербезопасности умных городов



Компания является членом Консорциума промышленного Интернета (Industrial Internet Consortium), который помогает организациям максимально быстро и удобно интегрировать физические и цифровые среды

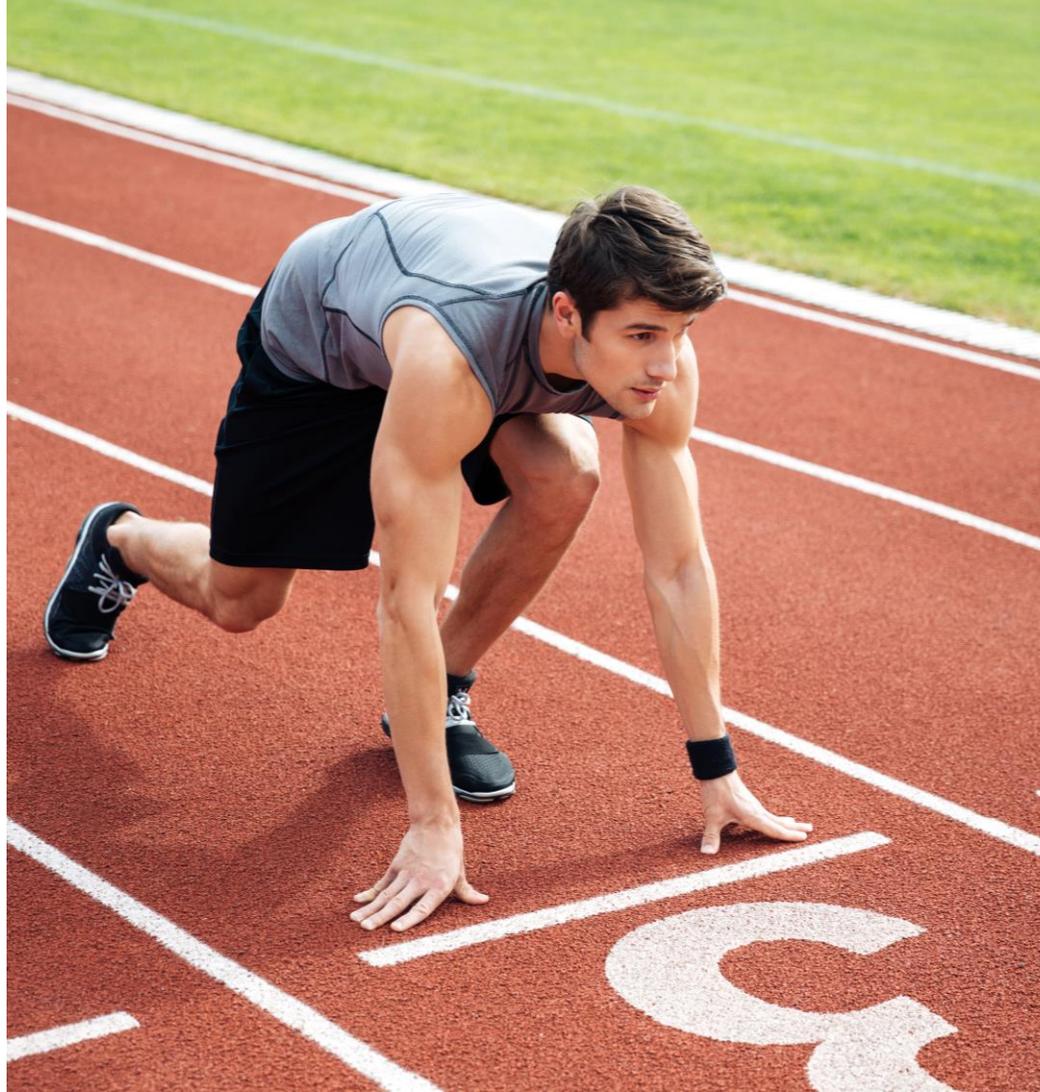
Вызовы:

187 ФЗ

Самоизоляция

Цифровизация

Kaspersky





380 000

Новых уникальных ВПО в день*

509

**Уязвимостей для АСУ ТП
обнаружено в 2019 году***

347 603\$ USA

**усреднённый ущерб
от киберинцидента за 2017 год***

*Согласно аналитическим отчётам ics-cert.kaspersky.ru

**Инфраструктура и модель угроз
меняется быстрее, чем
проектируется ИБ**

**Нехватка квалифицированных
кадров**

**Мизерные источники получения
информации**



Реализация 187 ФЗ

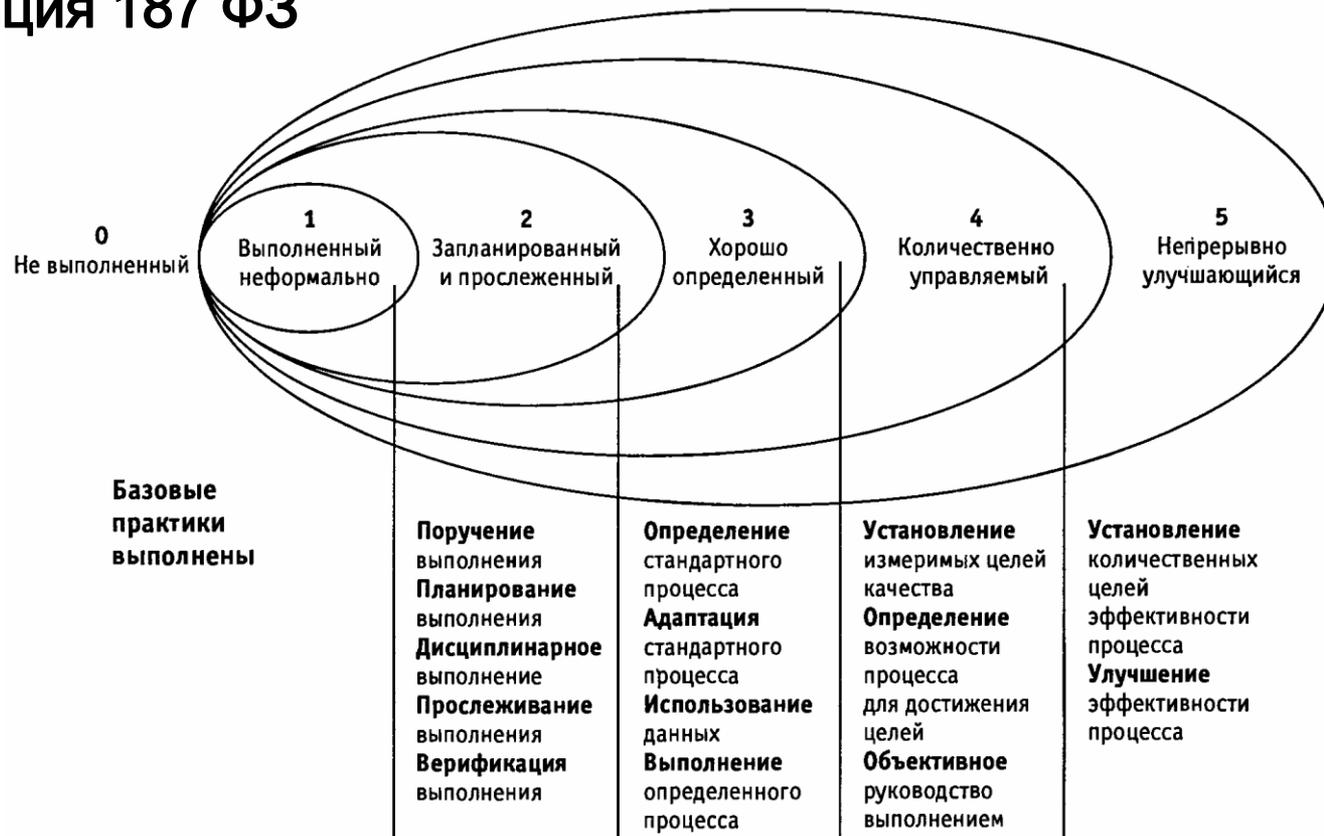
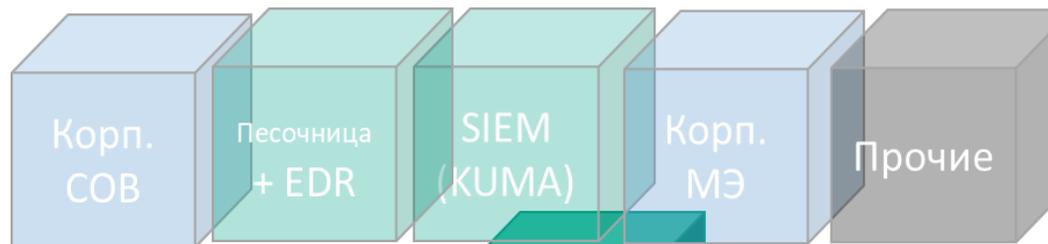


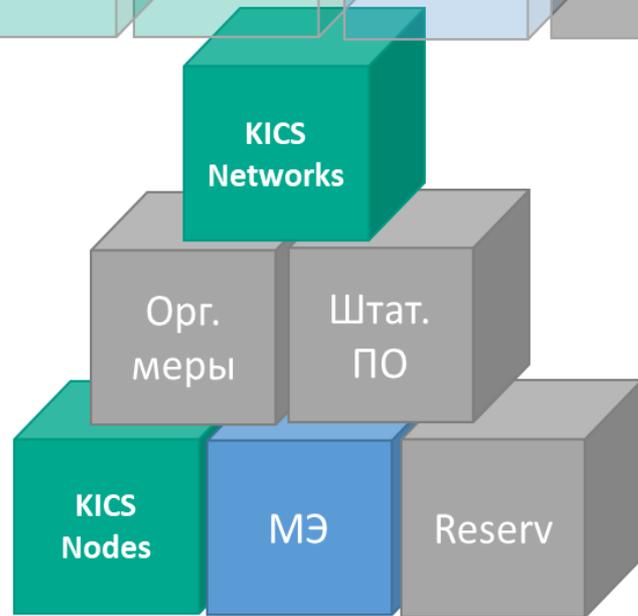
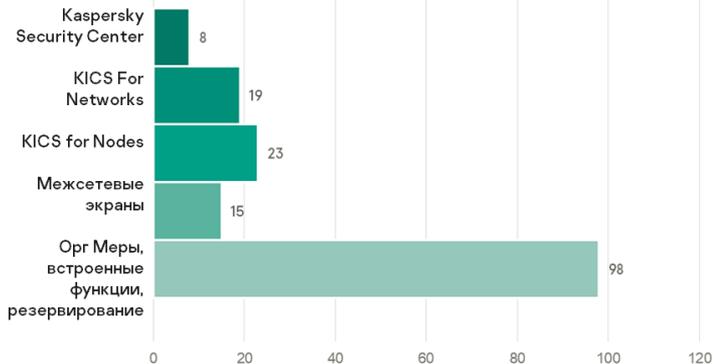
Рис. 26. Уровни возможности представляют зрелость организаций по инжинирингу безопасности

Минимальное решение ИБ АСУ ТП



Пример 239 приказ ФСТЭК, 3 категория

107 обязательных мер



Kaspersky Industrial CyberSecurity



KICS Nodes

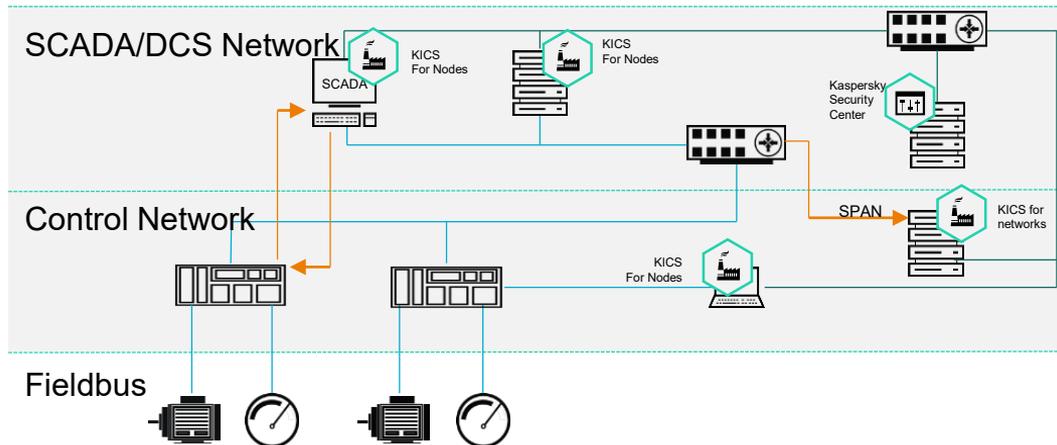
- Белый список приложений
- Антивирус
- Антишифровальщик
- Контроль устройств
- Контроль целостности файлов
- Анализ логов



KICS Networks

- Контроль целостности сети
- Разбор промышленных протоколов
- Система обнаружения вторжений
- Пассивный анализ уязвимостей
- Визуализация карты сети и взаимодействий
- Корреляция событий

Kaspersky



Почему Kaspersky?

Специализированные технологии
для защиты промышленных систем



Kaspersky
Industrial
CyberSecurity

<https://ics.kaspersky.ru/resources/#solution>

Один из лидеров мирового уровня



[Gartner Peer Insights.
Operational Technology Security](#)



[Сравнение
промышленных COB](#)



[VDC Research 2020. «Industrial
CyberSecurity»](#)



[Frost & Sullivan.
Global industrial \(OT/ICS\)
cybersecurity
Company of the Year Award](#)

Интеграция с производителями
решений для промышленности

<https://ics.kaspersky.ru/resources/#certification>

Schneider
Electric

ИнфТех
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ЭКРА

PROSOFT®

SIEMENS

BOSCH
Разработано для жизни

Пример _ МосГаз



Транспортировка природного газа по газораспределительным сетям Москвы

Основано в 1865

Ежегодная отгрузка 23 миллиардов кубометров природного газа

7500 километров газораспределительных сетей

Защищены промышленные узлы и сети

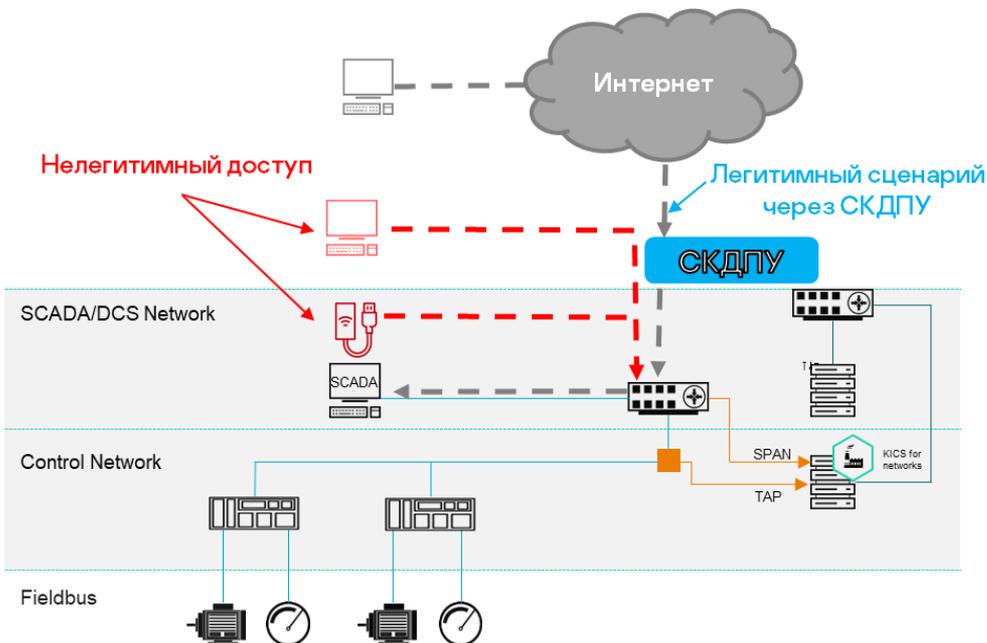
Более 500 газораспределительных станций с KICS for Network

- Всего ~600 ПЛК Siemens
- До 20 клапанов в каждом ПЛК

Группа SCADA-серверов с KICS for Nodes

<https://ics.kaspersky.ru/resources/#stories>

Самоизоляция _ Актуальные сценарии применения



Активная защита (на узлах):

- Контроль подключаемых устройств
- Защита от шифровальщиков
- Контроль запускаемых приложений
- Wi-Fi контроль

Контроль сетевых активностей:

- Анализ действий пользователя
(в части промышленных протоколов и команд)
- История действий в АСУ ТП (для разбора инцидентов)
- Дополнительная защита подключений (анализ команд доверенного пользователя через промышленный IDS)
- Выявление «не согласованных» подключений

Цифровизация _ новая роль ИБ

СНИЖЕНИЕ ВЫНУЖДЕННЫХ ПРОСТОЕВ

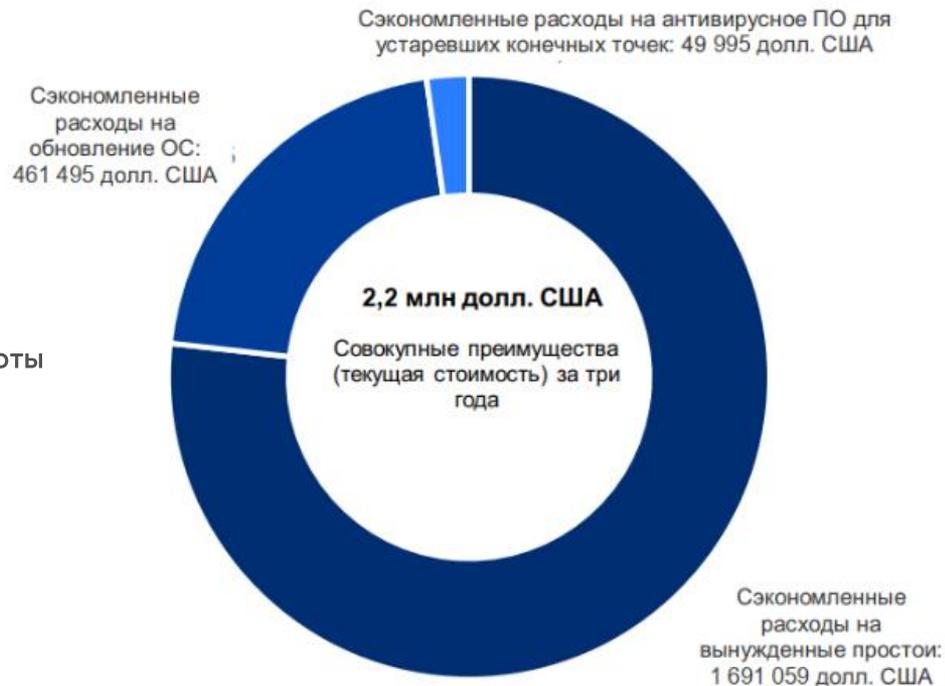
Снижение количества и длительности вынужденных простоев из-за блокирования и замедления работы

УСТРАНЕНИЕ РАСХОДОВ НА ОБНОВЛЕНИЕ ОС

Устранение необходимости затратного обновления ОС для совместимости с традиционным антивирусом

ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ СИСТЕМЫ

Повышение информационной защищённости системы



Давайте взаимодействовать



Специализированные аналитические исследования для определения отраслевых угроз и лучших практик по информационной безопасности

Консалтинг в создание центров мониторинга и реагирования на инциденты

Подготовка специалистов по реагированию на компьютерные инциденты промышленной специализации

Оценка защищенности ПТК, информационных инфраструктур и цепочки поставщиков на уязвимости

OEM использование технологий Kaspersky

kaspersky



Kaspersky
Industrial
CyberSecurity

Активируем будущее вместе

Петухов Алексей

Руководитель направления кибербезопасности промышленных систем

Alexey.Petukhov@Kaspersky.com

+7 963 686 07 83

ics.kaspersky.com