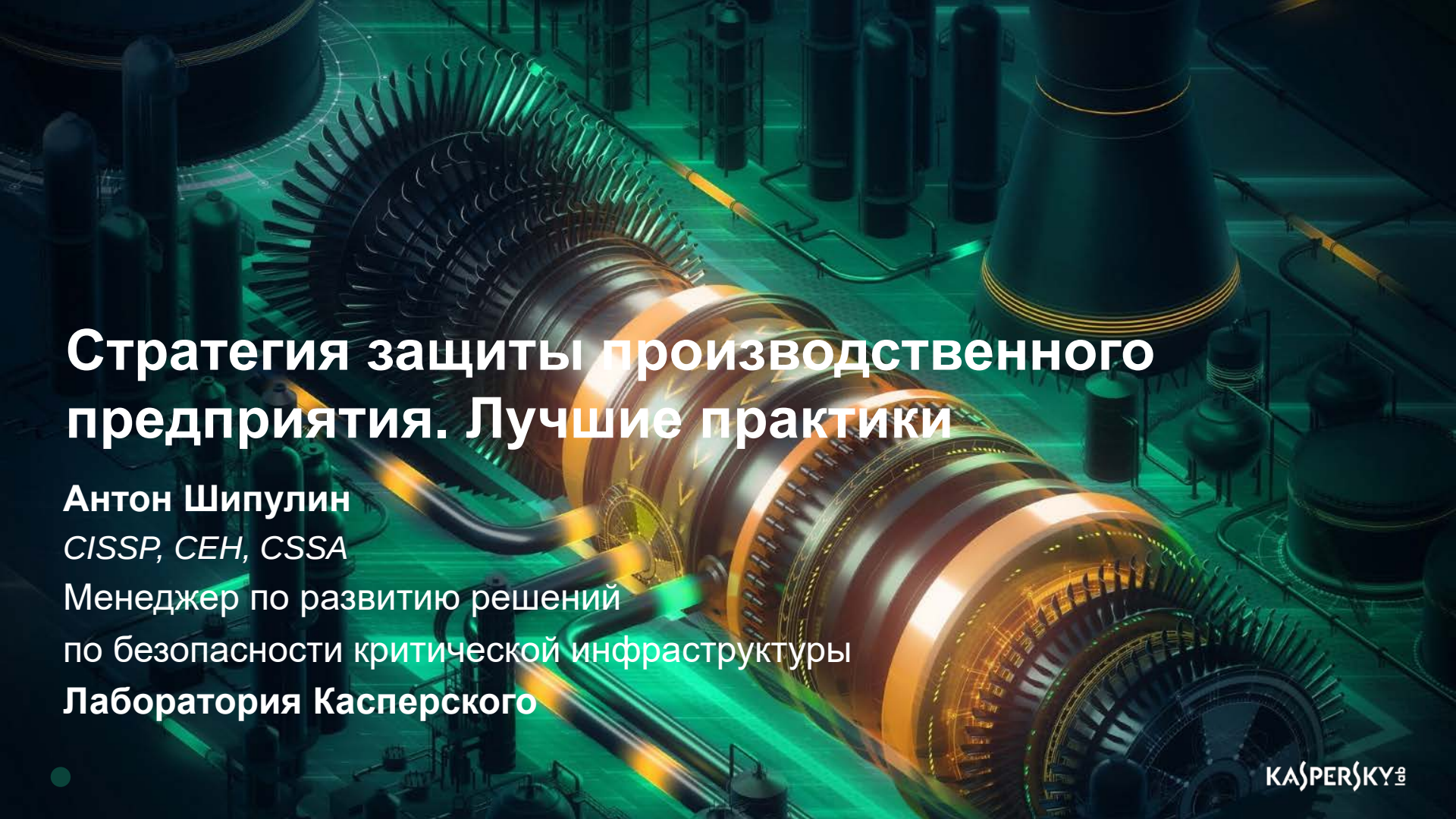
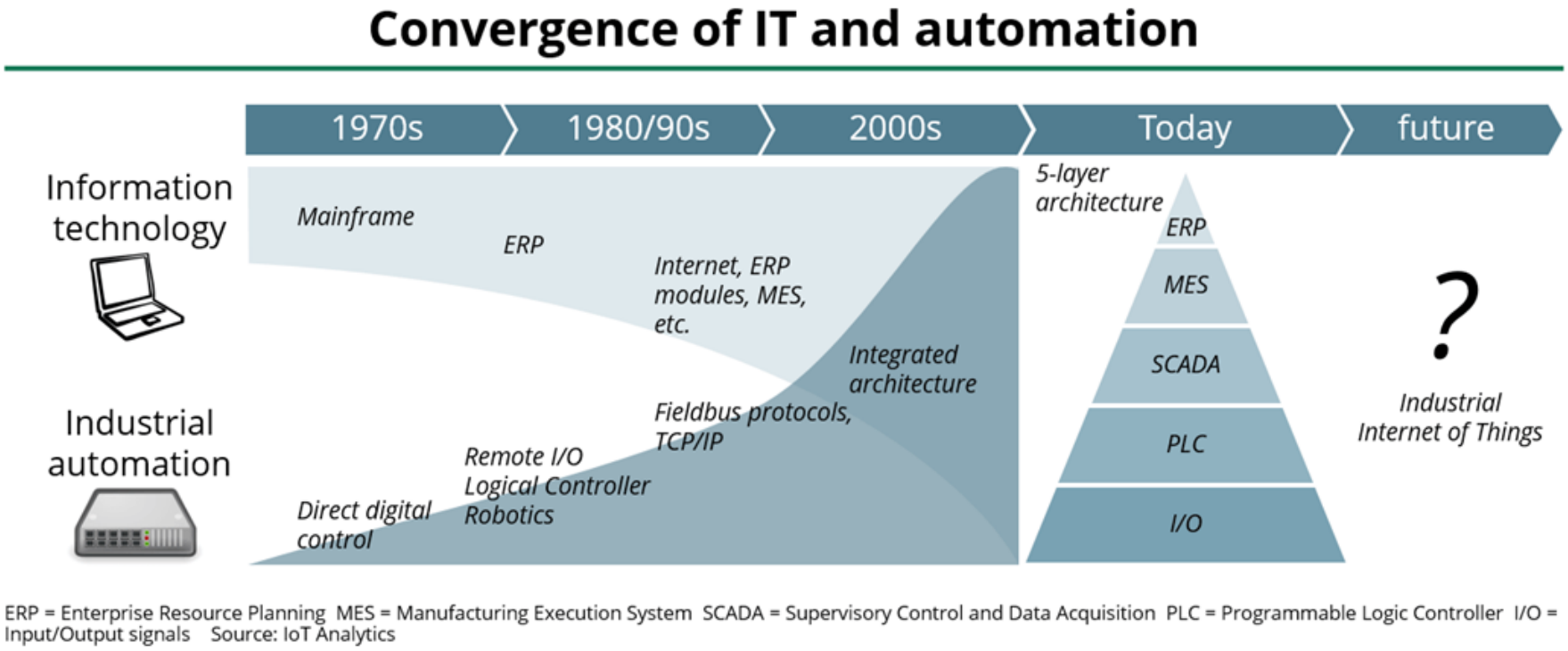


Стратегия защиты производственного предприятия. Лучшие практики

Антон Шипулин
CISSP, CEH, CSSA
Менеджер по развитию решений
по безопасности критической инфраструктуры
Лаборатория Касперского

KASPERSKY lab

Сближение технологий IT и OT



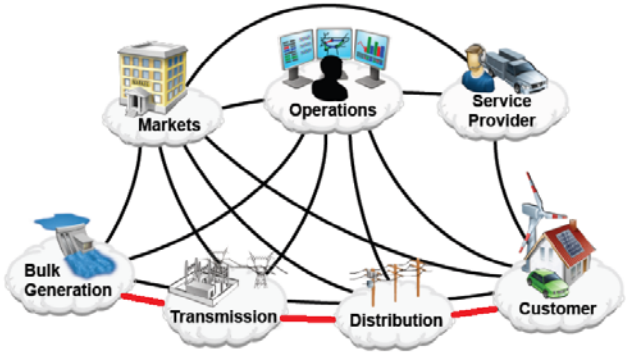
ERP = Enterprise Resource Planning MES = Manufacturing Execution System SCADA = Supervisory Control and Data Acquisition PLC = Programmable Logic Controller I/O = Input/Output signals Source: IoT Analytics

Сближение технологий IT и OT

Smart & Safe City

Industry 4.0 / IIoT

Smart Public Transport



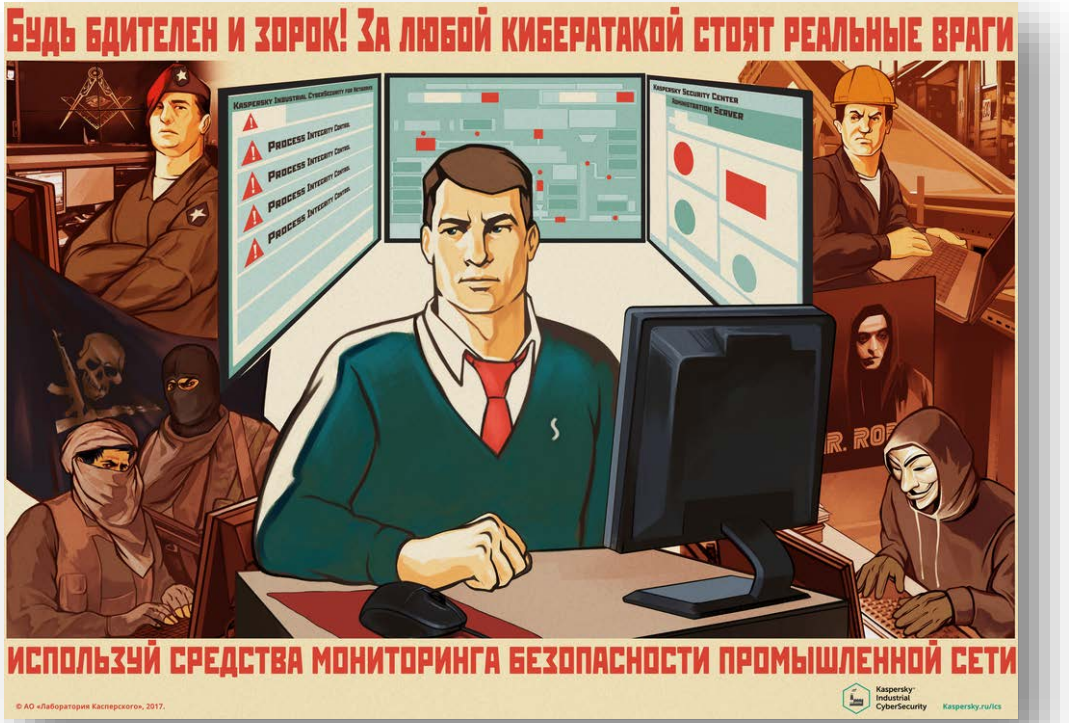
Smart Grid

Разница между IT и OT

Категория	IT	OT
Производительность	Non Real Time	Real Time
Надежность	Задержки не критичны	Задержки недопустимы
Приоритеты защиты	Конфиденциальность	Жизнь людей, непрерывность процессов, окружающая среда
Обновления	Автоматические	Ограничены
Емкость ресурсов	Достаточно для СЗИ	Нет ресурсов для СЗИ
Коммуникации	Стандартные протоколы	Проприетарные
Управление изменениями	Автоматизированные	Сложный процесс
Поддержка	Возможны замены провайдеров	Привязаны к одному поставщику
Жизненный цикл	3-5 лет	10-15 лет
Доступность	Легкая	Изолированная, Физическая

Модель угроз

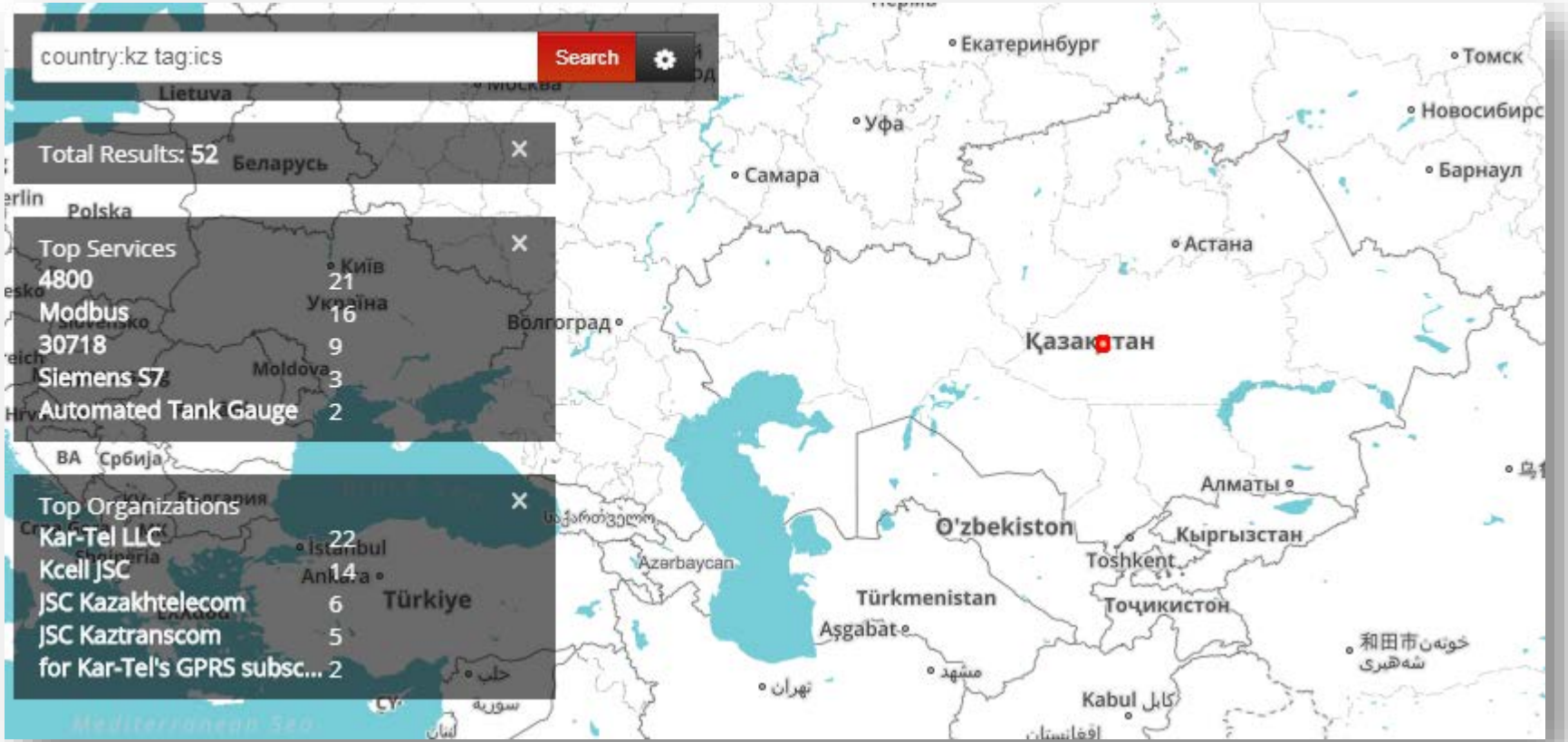
- Хактивисты
- Террористы
- Киберармии
- Криминальные структуры
- Конкуренты
- Сотрудники или подрядчики
- Неумышленные источники



Проблемы и уязвимости

- Недостаточно обученные сотрудники
- Недостаточно защищенная сеть
- Недостаточно защищенная конфигурация оборудование
- Некорректное управление антивирусной защитой
- Недостаточный процесс управления изменениями
- Недостаточный процесс управления обновлениями
- Недостаточное резервирование данных
- Недостаточный процесс управления учетными записями
- Использование общих и встроенных учетных записей
- Недостаточный процесс реагирования на инциденты

Проблемы и уязвимости



Последствия

ПОВРЕЖДЕНИЕ/РАЗРУШЕНИЕ ОБОРУДОВАНИЯ

- Перегрузка оборудование и преждевременный износ
- Выход работы оборудования за безопасные пределы

ПОВРЕЖДЕНИЕ ПРОДУКЦИИ ПРЕДПРИЯТИЯ/ОБЪЕКТА

- Остановка работы предприятия
- Кража сырья и продукции
- Снижение качества или объема выпуска продукции
- Повышение затрат сырья на производство продукции
- Повышение нагрузки на процесс техобслуживания производства продукции

НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА И ОТРАСЛЕВЫХ НОРМ

- Причинение вреда жизни и здоровью людей
- Нанесение реального вреда охране труда и экологической безопасности
- Нарушение нормативных пределов выбросов/загрязнения окружающей среды
- Нарушение контрактных обязательств по выпуску продукции

Публичные инциденты

2017, Атака на производство бумаги, США

- Бывший IT специалист подключился к системам управления внес изменения в логику, простои принесли потери $1,1 млн

2016, Атака на водоочистные сооружения, США

- Были изменены пропорции химикатов

2015 + 2016, Атака на электроподстанции, Украина

- 225 000 потребителей были отключены

2014, Атака на металлургический завод, Германия

- Печь была выведена из строя

2010, Атака на завод по обогащению урана, Иран

- Вывод из строя центрифуг, остановка ядерной программы

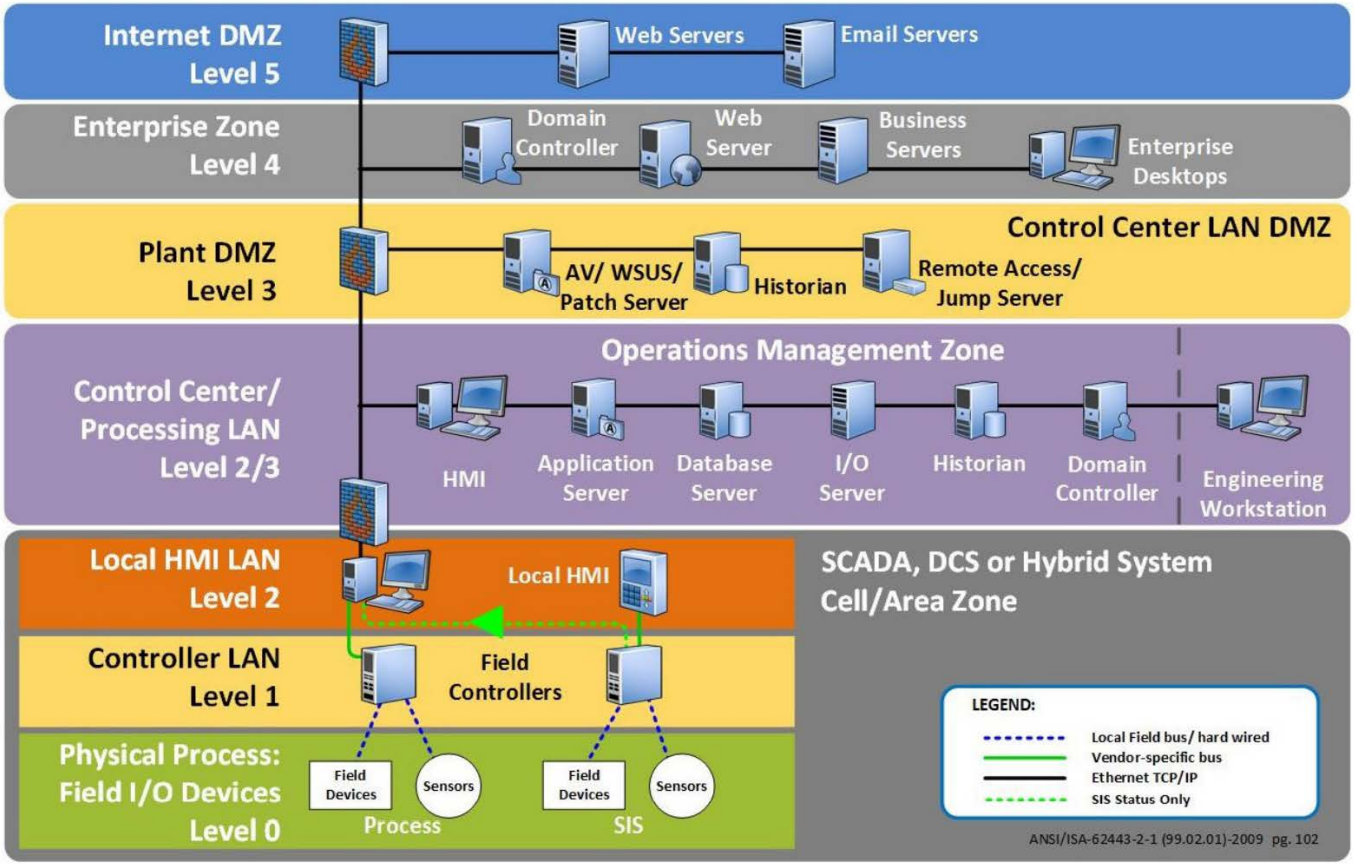
INDUSTRIES vs RANSOMWARE / WANNACRY / PETYA

- Dacia (**Auto**)
- Nissan (**Auto**)
- Honda (**Auto**)
- Renault (**Auto**)
- Gas Natural (**Gas**)
- Iberdrola (**Power**)
- Maersk (**Ports**)
- Reckitt Benckiser (**Farma**)
- Merck (**Farma**)
- Cadbury (**Food**)
- Rosneft (**Oil**)
- NCOC (**Oil**)
- RZHD (**Railways**)
- …

Industrial Cyber Security Program / NIST Cybersecurity Framework

Framework Functions	Activities			
Identify	Create an inventory of all IT and OT assets	Assess the risk of cyber incident	Define a cybersecurity management policy	Awareness and training
Protect	Secure network and equipment	Protect sensitive information	Manage access to systems and equipment	
Detect	Define methods for monitoring	Define responsibilities for monitoring	Identify improvements	
Respond	Maintain an incident-response plan	Practice response processes	Identify improvements	
Recover	Maintain backups of all systems and equipment	Practice recovery processes	Identify improvements	

Сегментация сети



Возможные решения по безопасности АСУ ТП

1. Промышленные межсетевые экраны / **Industrial FW**
2. Однонаправленные шлюзы / **Unidirectional Gateways**
3. **Защиты конечных узлов / Endpoint Security**
4. Контроль доступа администраторов / подрядчиков / **PIM**
5. Криптографическая защита каналов связи / **VPN**
6. Управление доступом к сети / **NAC**
7. Многофакторная аутентификации

1. **Обнаружение сетевых атак и аномалий / IDS / NBAD / DPI**
2. Мониторинг событий безопасности / **SIEM**
3. Мониторинг беспроводных сетей / **WIPS**
4. Анализ уязвимостей (активный / пассивный / конфигураций)
5. Контроль утечек информации / **DLP**
6. Анализ правил сетевого доступа
7. **Контроль целостности данных**
8. Системы ловушки / Honeypots
9. Сервисы разведки киберугроз

Kaspersky Industrial CyberSecurity

LEVEL 4

Business planning and logistics

Managing end-to-end supply chain.
Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3

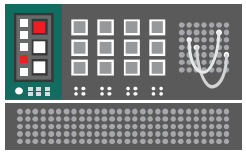
Manufacturing Operations management

Work flow/recipe control to produce the desired end products.
Maintaining records and optimizing the production process.

LEVEL 2, 1

Batch Control.
Continuous Control.
Discrete Control.

Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

LEVEL 0

Physical

Physical devices

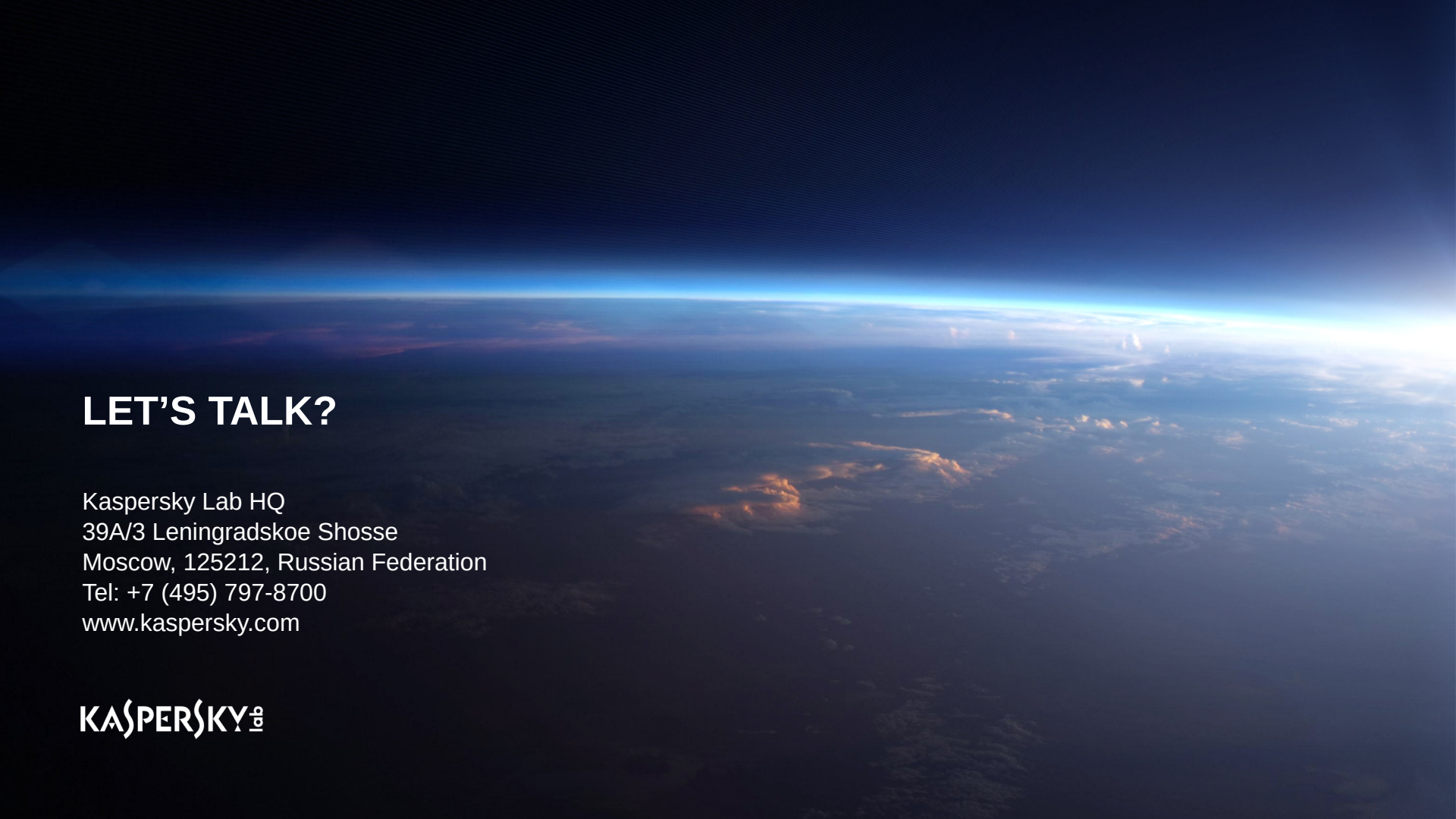
Kaspersky Security for Business + Professional Services

Kaspersky Industrial CyberSecurity

Physical security

Жизненный цикл атаки / Kill Chain

Этап	Сценарий	Реагирование
Доступ / Access	• Зараженный USB device, модем, Wi-Fi адаптер • Точка доступа в сеть: ноутбук, wireless access point • Установка соединения, получение доступа в сеть	• Device control • Application control • Antimalware • Network Integrity Control (WL) • Intrusion Detection System
Разведка / Discovery	• Сканирование сети, поиск устройств и служб • Подбор пароля к оборудованию • Получение конфигурации, параметров и сбор трафика для изучения и планирования атаки	• Network Integrity Control (WL) • Intrusion Detection System • Process Integrity Control (DPI)
Cyber-Physical Attack	• Запись вредоносной программы ПЛК через локальное подключение • Запись вредоносной программы ПЛК по сети • Изменение параметра в памяти ПЛК • Подмена параметров, команд в сетевом трафике • Отправка вредоносных команд на ПЛК	• PLC Integrity Checker • Network Integrity Control • Intrusion Detection System (Whitelisting) • Process Integrity Control (DPI)



LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab