ТЕХНОСЕРВ

Практика обеспечения кибербезопасности АСУ ТП в электроэнергетике

22 октября 2015 г.

Сергей Терехов

Руководитель направления кибербезопасности АСУ ТП

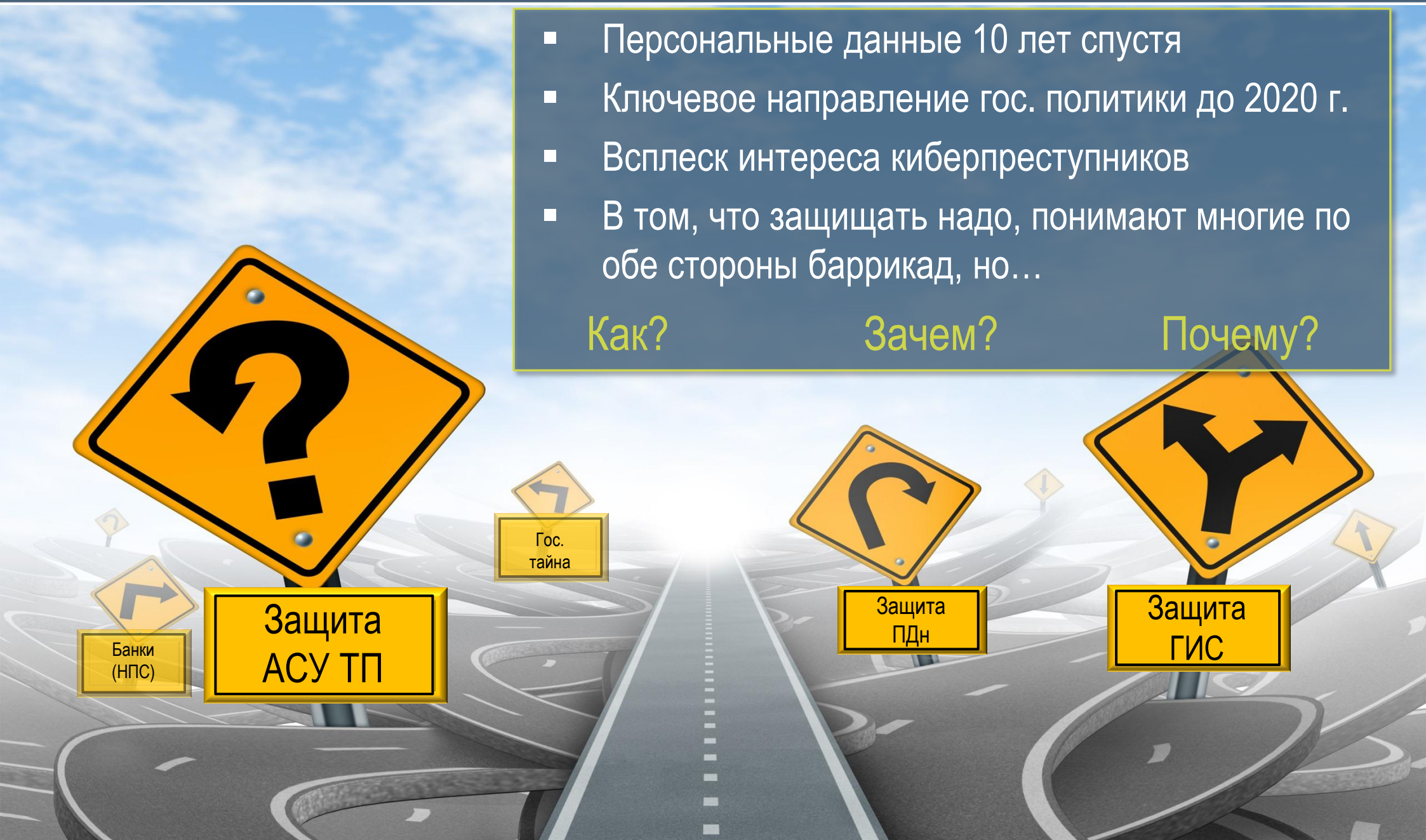
Центра компетенций по информационной безопасности

Повышение интереса к защите АСУ ТП

ТЕХНОСЕРВ

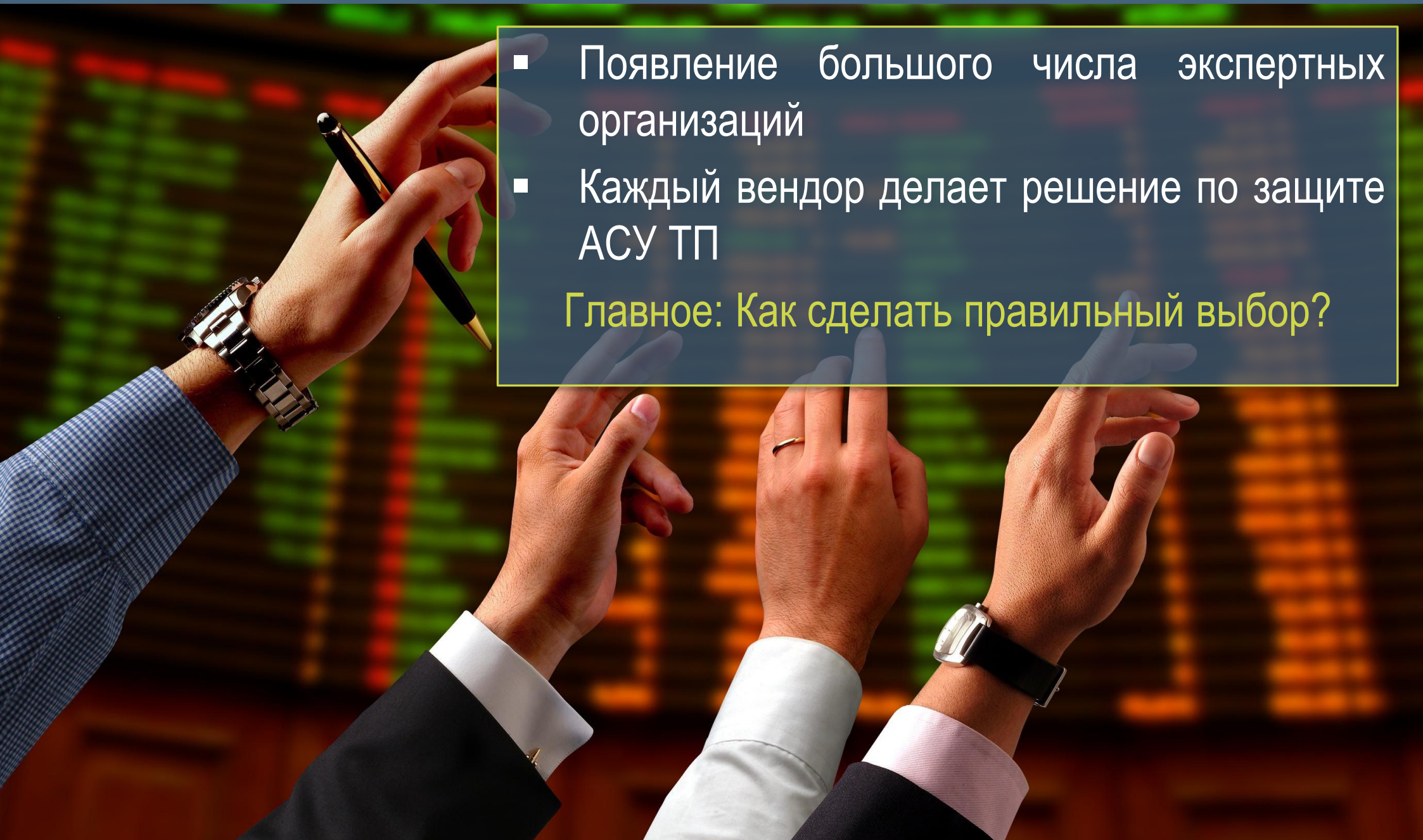
- Персональные данные 10 лет спустя
- Ключевое направление гос. политики до 2020 г.
- Всплеск интереса киберпреступников
- В том, что защищать надо, понимают многие по обе стороны баррикад, но…

Как? Зачем? Почему?



Проблемы

ТЕХНОСЕРВ



- Появление большого числа экспертных организаций
- Каждый вендор делает решение по защите АСУ ТП

Главное: Как сделать правильный выбор?

Требования законодательства

ТЕХНОСЕРВ

Совет безопасности: «Основные направления государственной политики в области обеспечения безопасности АСУ ТП КВО РФ»

256-ФЗ «О безопасности объектов ТЭК»
16-ФЗ «О транспортной безопасности»
116-ФЗ «О промышленной безопасности»

«Система признаков критически важных объектов…» (Совет безопасности, 08.11.2005 г.)

В разработке:
Проект ФЗ «О безопасности критической информационной инфраструктуры»

Нормативно-методические документы ФСТЭК России (2007 г.)

- Общие требования по обеспечению безопасности информации в КСИИ
- Рекомендации по обеспечению безопасности информации в КСИИ
- Базовая модель угроз безопасности информации в КСИИ
- Методика определения актуальных угроз безопасности информации в КСИИ

Приказ ФСТЭК №31 от 14.03.2014 г. «Об утверждении требований к обеспечению защиты информации в АСУ ТП…»

Проекты 4-х документов ФСТЭК по защите АСУ ТП (2016 г.)

- Меры защиты в АСУ
- Методика определения угроз безопасности информации в АСУ
- Порядок выявления и устранения уязвимостей в АСУ
- Порядок реагирования на инциденты, связанные с нарушением безопасности информации

Национальные стандарты, рекомендации и руководства

- NIST SP800-82.r2. Guide to Industrial Control Systems (ICS) Security (05.2015)
- IEC 62443 (ISA99), Security for Industrial Automation and Control Systems
- Стандарты безопасности NERC (North American Electric Reliability Corporation)
- Department of Homeland Security: Cyber Security Procurement Language for ICS
- Разработки US-CERT (Руководства, модели нарушителей, уязвимостей и др.)
- ….

Проект новой доктрины информационной безопасности

ТЕХНОСЕРВ

Пять ключевых блоков угроз

№ 1: Наращивание потенциала зарубежных стран в сфере ИКТ, в том числе **для воздействия на критическую информационную инфраструктуру РФ** (электросети, системы управления транспортом и др.) и технической разведки в отношении российских госорганов, научных организаций и предприятий оборонно-промышленного комплекса.

По данным Коммерсантъ.ru

Новые-старые действующие ГОСТы

ТЕХНОСЕРВ

Вступают в силу 01.01.2016

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56205— 2014 IEC/TS 62443-1-1:200

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 1-1

Терминология, концептуальные положения и модели

IEC/TS 62443-1-1:2009
Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models
(IDT)

Издание официальное

Москва
Стандартинформ
2014

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62443-2-1– 2015

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 2-1

Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

IEC 62443-2-1:2010
Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program
(IDT)

Издание официальное

Москва
Стандартинформ
2015

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56498– 2015/ IEC/PAS 62443-3: 2008

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 3

Защищенность (кибербезопасность) промышленного процесса измерения и управления

IEC/PAS 62443-3:2008
Industrial communication networks – Network and system security – Part 3: Security for industrial process measurement and control
(IDT)

Издание официальное

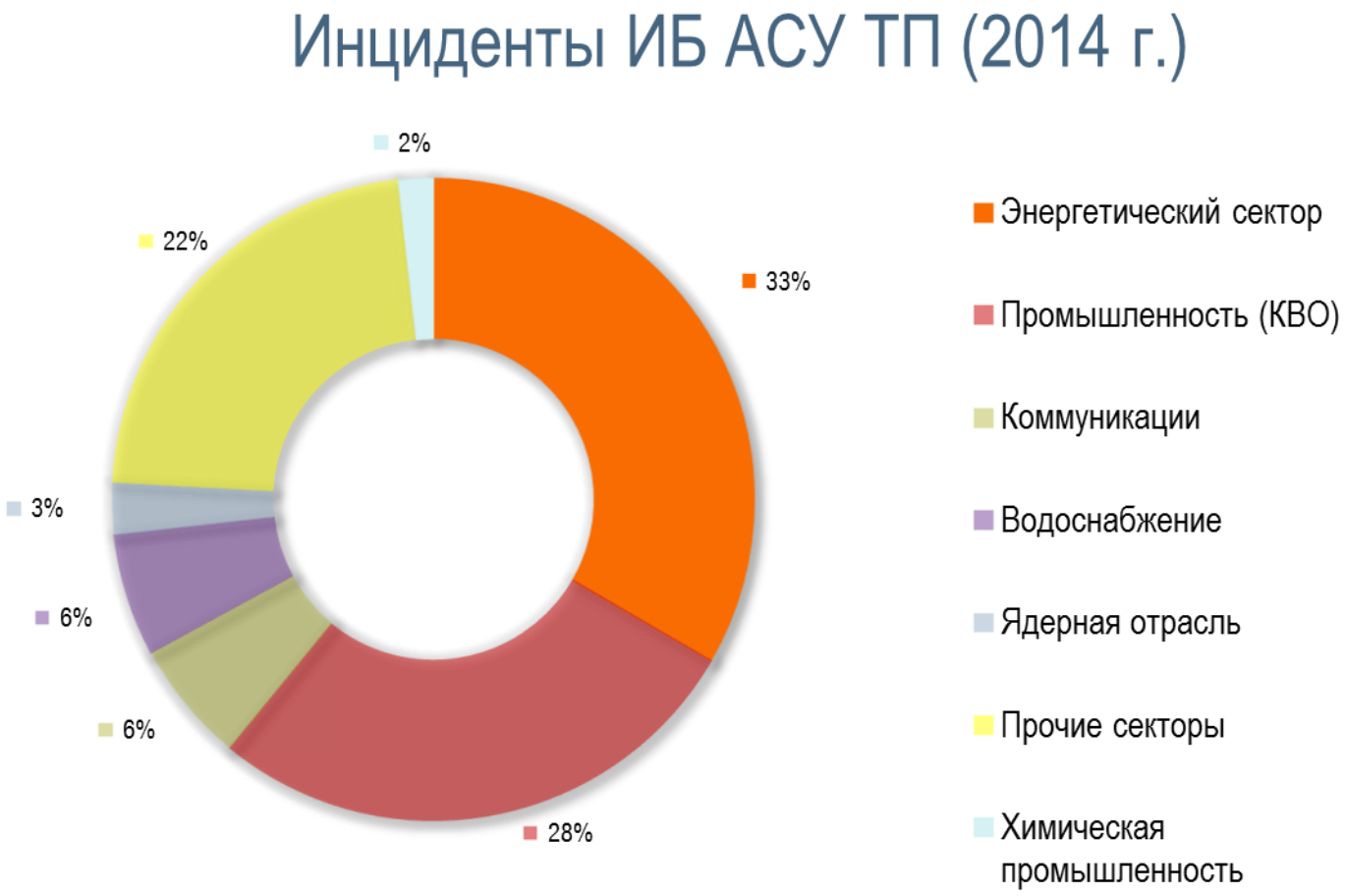
Москва
Стандартинформ
2015

Статистика инцидентов кибербезопасности АСУ ТП

ТЕХНОСЕРВ

ВСЕГО:

245 инцидентов кибербезопасности АСУ ТП (КВО)*



Многие атаки на промышленные объекты осуществляются по политическим причинам

** По данным ICS-CERT*

Рассвет угроз для АСУ ТП энергетики

ТЕХНОСЕРВ

HAVEX (2014 г.) – разработан целенаправленно для АСУ ТП:

- Заражение дистрибутивов с обновлениями SCADA на сайте производителей
- Поиск и инвентаризация OPC-серверов
- Объекты ТЭК США, Европы и России

Что дальше? Кто следующий?

Пока гром не грянет

ТЕХНОСЕРВ

Типичные мифы:

- Нет законодательной базы
- Нет никаких угроз с 2005 года
- Мы защищены
- Мы никому не нужны
- Безопасность – вторична, главное – непрерывность функционирования

На практике:

- Технологическая и корпоративная сети – одно целое
- Использование для защиты оборудования SOHO
- Неконтролируемый доступ подрядчиков, включая западные (американские) компании
- Нехватка кадров
- Уязвимости не исправляются годами

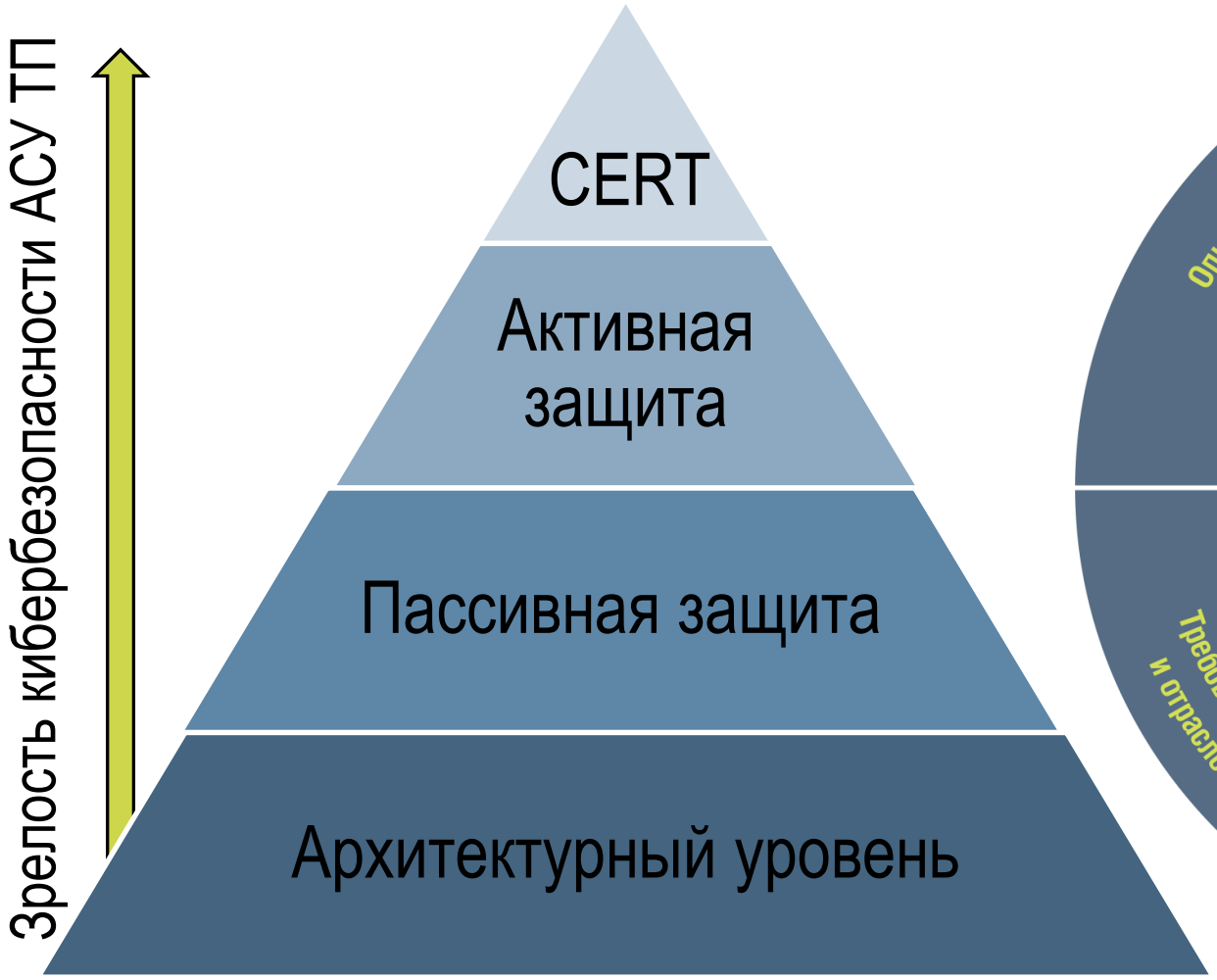
А Вы уверены, что в филиалах все хорошо?

ТЕХНОСЕРВ

Превентивные, детектирующие или сдерживающие меры?

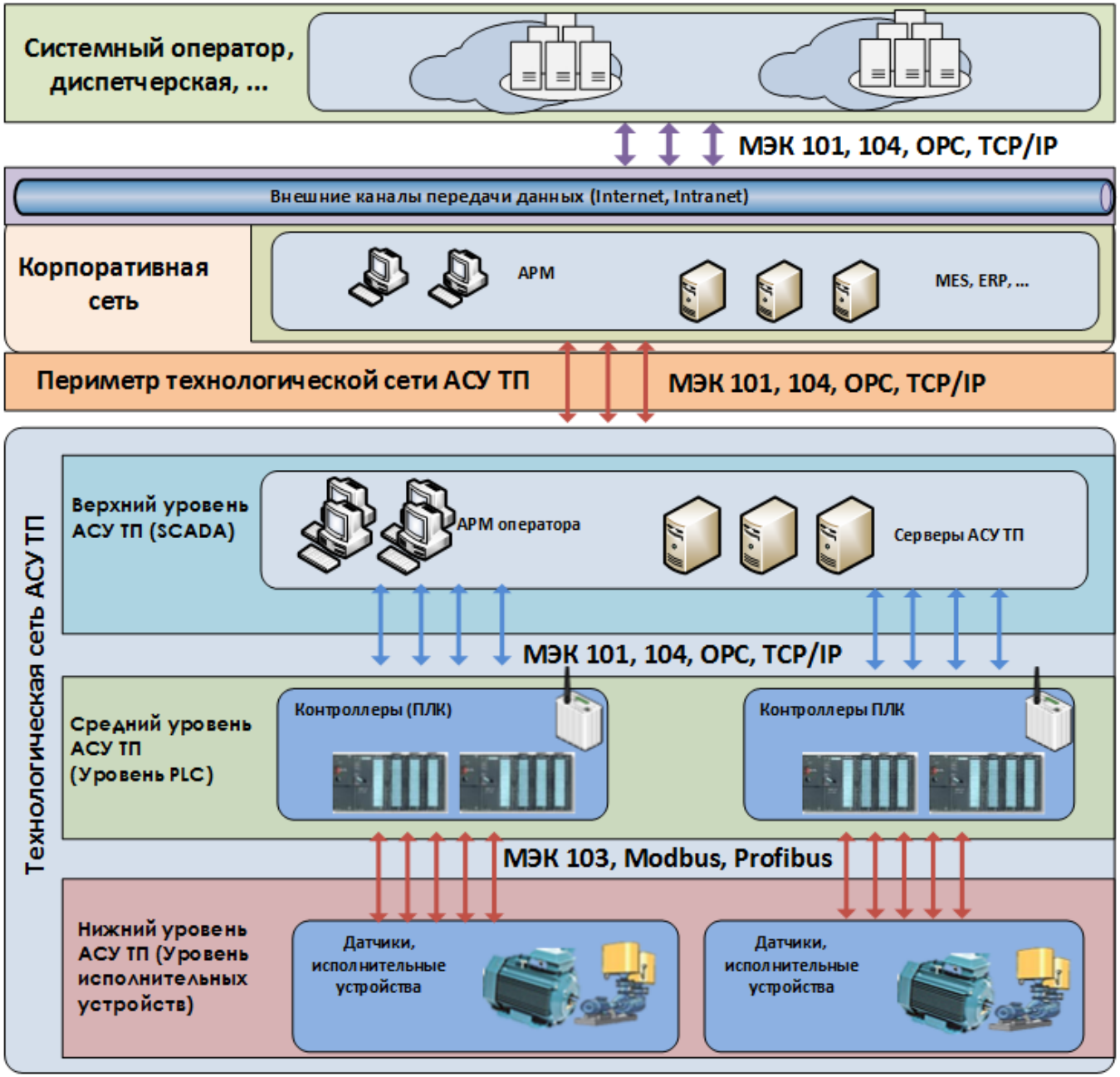
Практика «Техносерва»

ТЕХНОСЕРВ



Типовая архитектура АСУ ТП электроэнергетики

ТЕХНОСЕРВ



Корпоративные технологии, требования по защите (исходя из уровня рисков). Классические меры защиты при отсутствии однонаправленных взаимодействий.

Корпоративные технологии, высокие пропускные способности, меньше требований к физическому исполнению.

Стык корпоративных и промышленных технологий. Требования к задержкам и производительности. Требования к физическому исполнению.

«Сетевая обвязка». Высокие требования к связности и задержкам. Особые требования к физическому исполнению.

Основа: рискоориентированный подход и классификация АСУ ТП

ТЕХНОСЕРВ

Объекты защиты

- **Информация о параметрах управляемого объекта или процесса** (входная/выходная информация, управляющая (командная) информация, контрольно-измерительная информация и иная критически важная (технологическая) информация).
- **Программно-технический комплекс**, включающий технические средства (в том числе АРМ, промышленные серверы, телекоммуникационное оборудование, каналы связи, PLC, исполнительные устройства), ПО (микропрограммное, общесистемное, прикладное), а также СЗИ.

Классификация АСУ ТП по типам обрабатываемой информации

- АСУ ТП, обрабатывающая командную информацию
- АСУ ТП, обрабатывающая контрольно-измерительную информацию (телемеханика)

Классификация по особенностям архитектуры

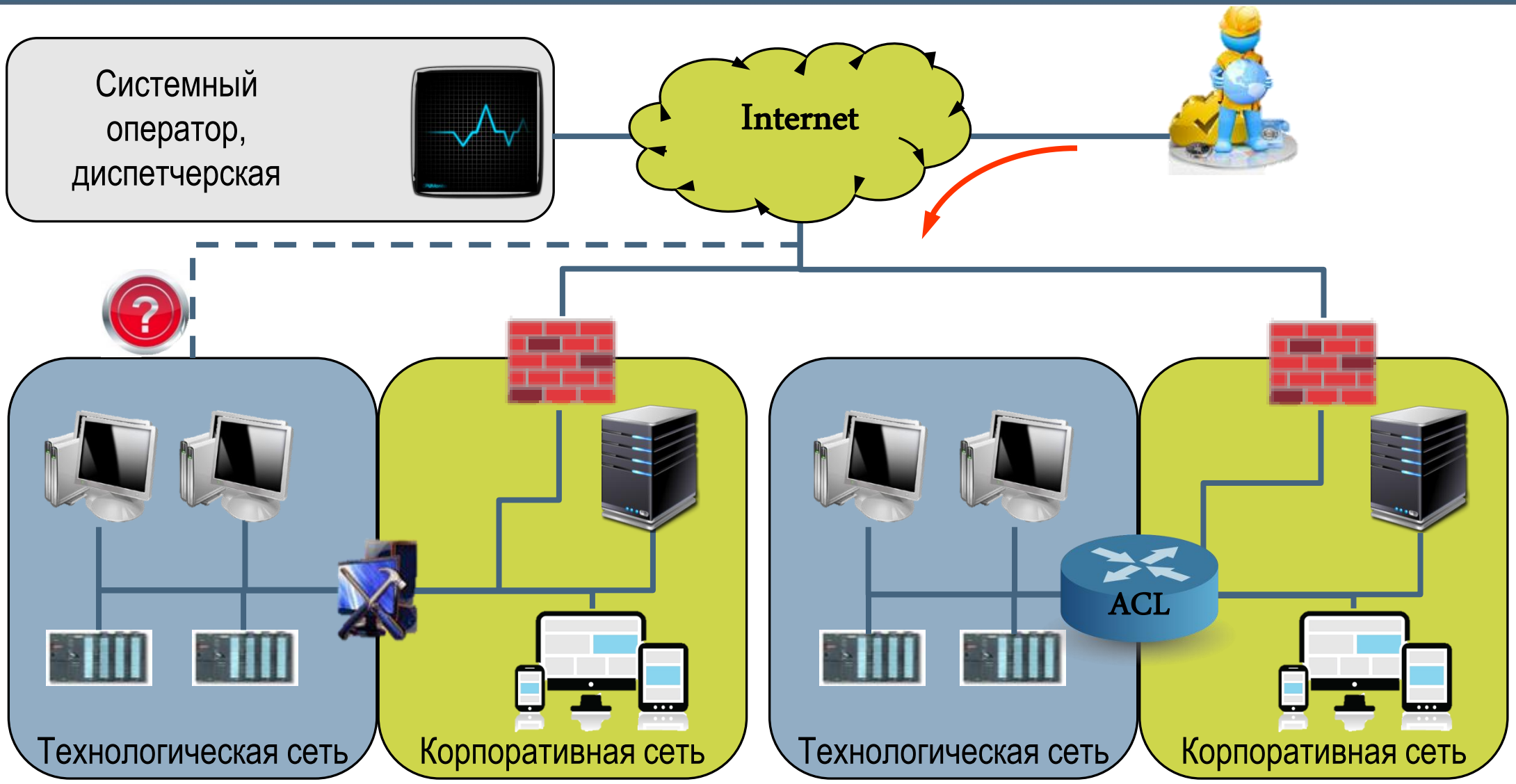
- Наличие подключений к КСПД, Интернет
- Наличие защитных мер периметра технологической сети
- Наличие удаленного доступа
- Наличие беспроводных сетей Wi-Fi в технологической сети

Классификация по степени критичности

Уровень значимости информации		Класс защищенности АСУ
Высокая	$УЗ^{-1}$	$К^{1}$
Средняя	$УЗ^{-2}$	$К^{2}$
Низкая	$УЗ^{-3}$	$К^{3}$

Проблема № 1: Стык технологической и корпоративной сетей

ТЕХНОСЕРВ

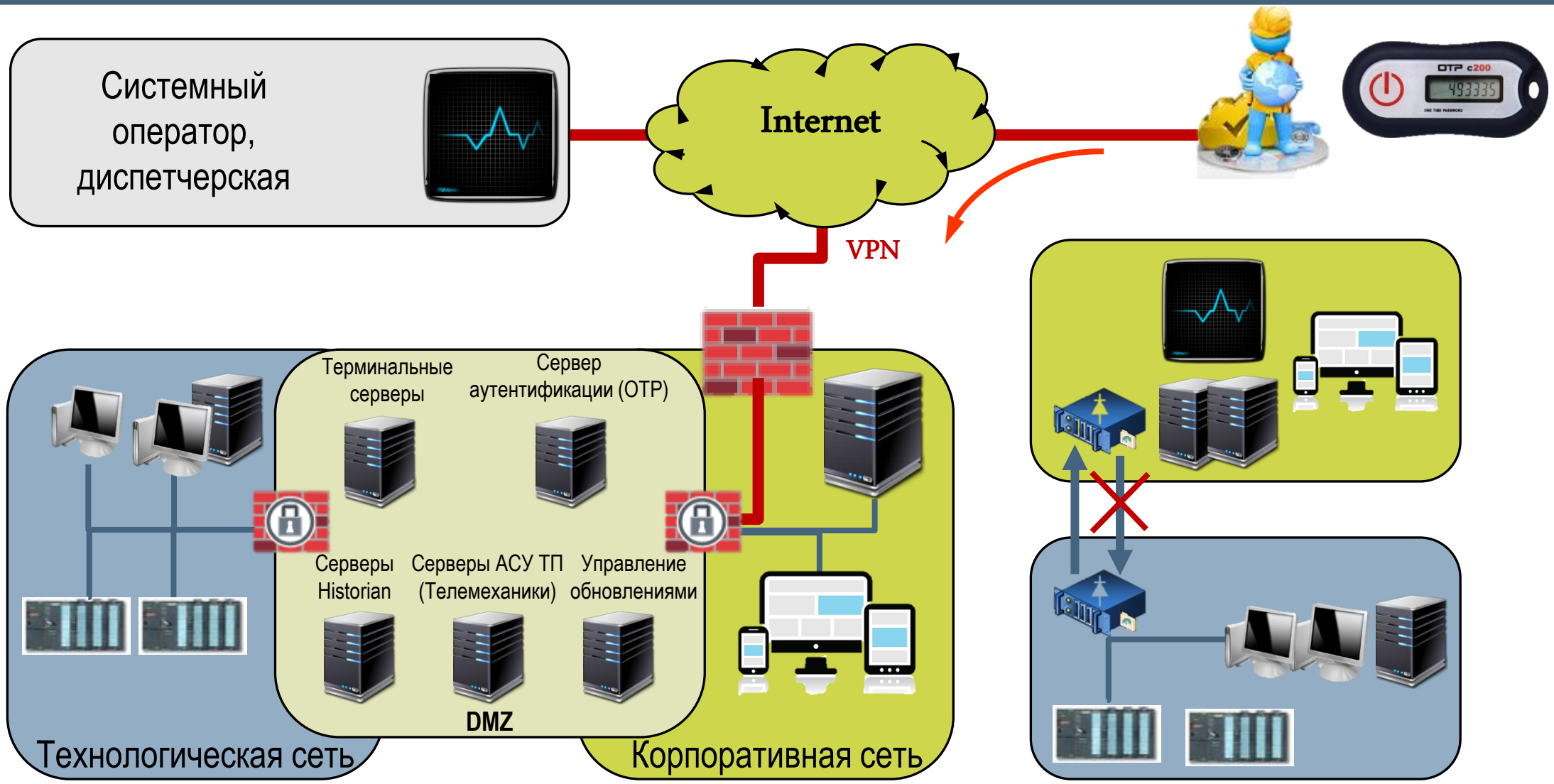


АРМ с двумя сетевыми картами

Оборудование SOHO, ACL на маршрутизаторе

Защита периметра АСУ ТП

ТЕХНОСЕРВ

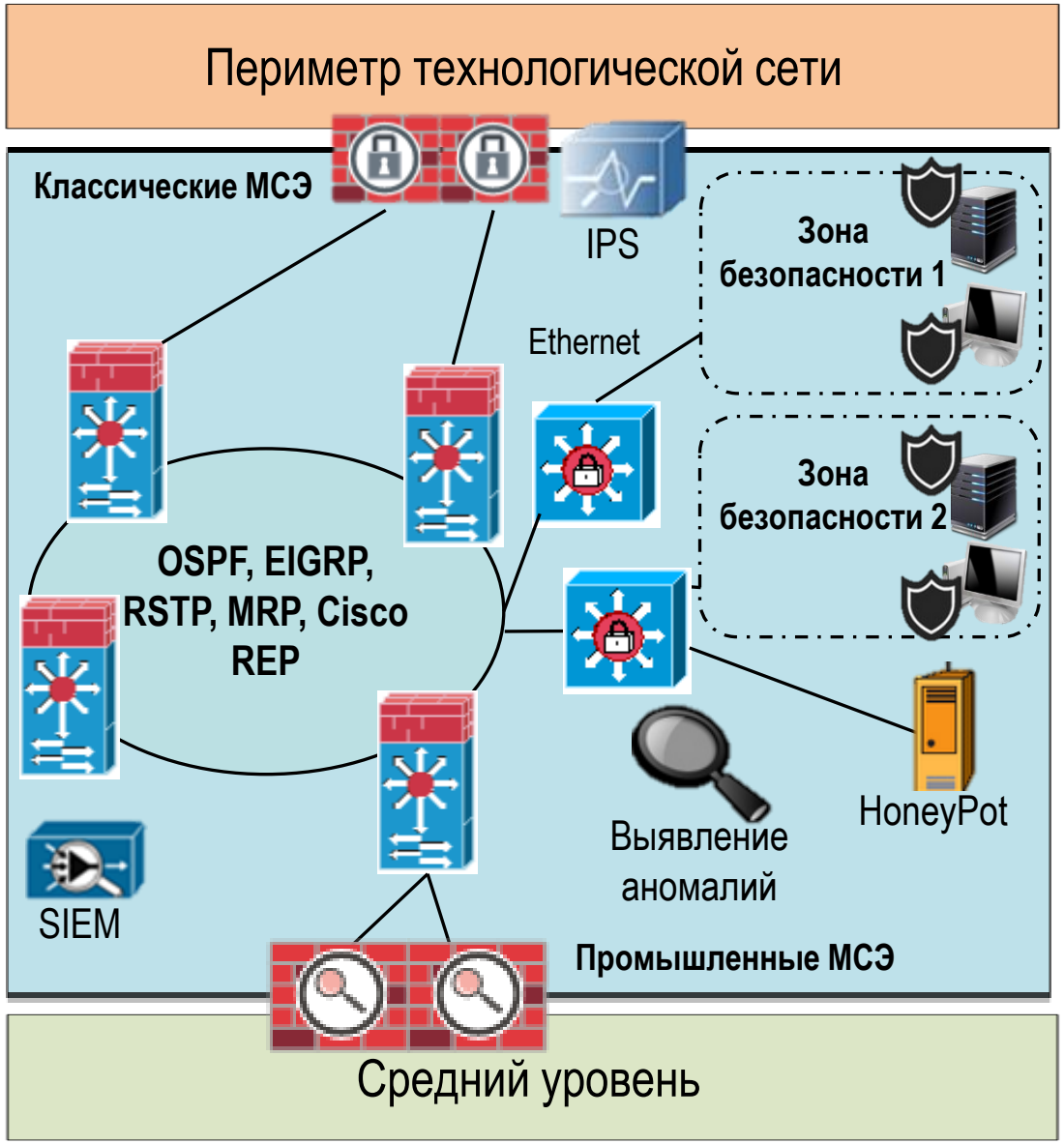


При низких и средних рисках - **DMZ**

При высоких – системы однонаправленной передачи (при возможности)

Защита на верхнем уровне АСУ ТП

ТЕХНОСЕРВ



Архитектурный уровень

- Сегментация и разделение на зоны безопасности
- Отказоустойчивость и доступность

Промышленные межсетевые экраны (IPS, маршрутизаторы, коммутаторы)

- Контроль сессий
- Инспектирование промышленных протоколов (Modbus, OPC, МЭК 104)
- Возможность работы в прозрачном режиме и режиме обучения (простота внедрения)

Анализ защищенности

- Наличие модуля выявления уязвимостей в SCADA

Мониторинг целостности

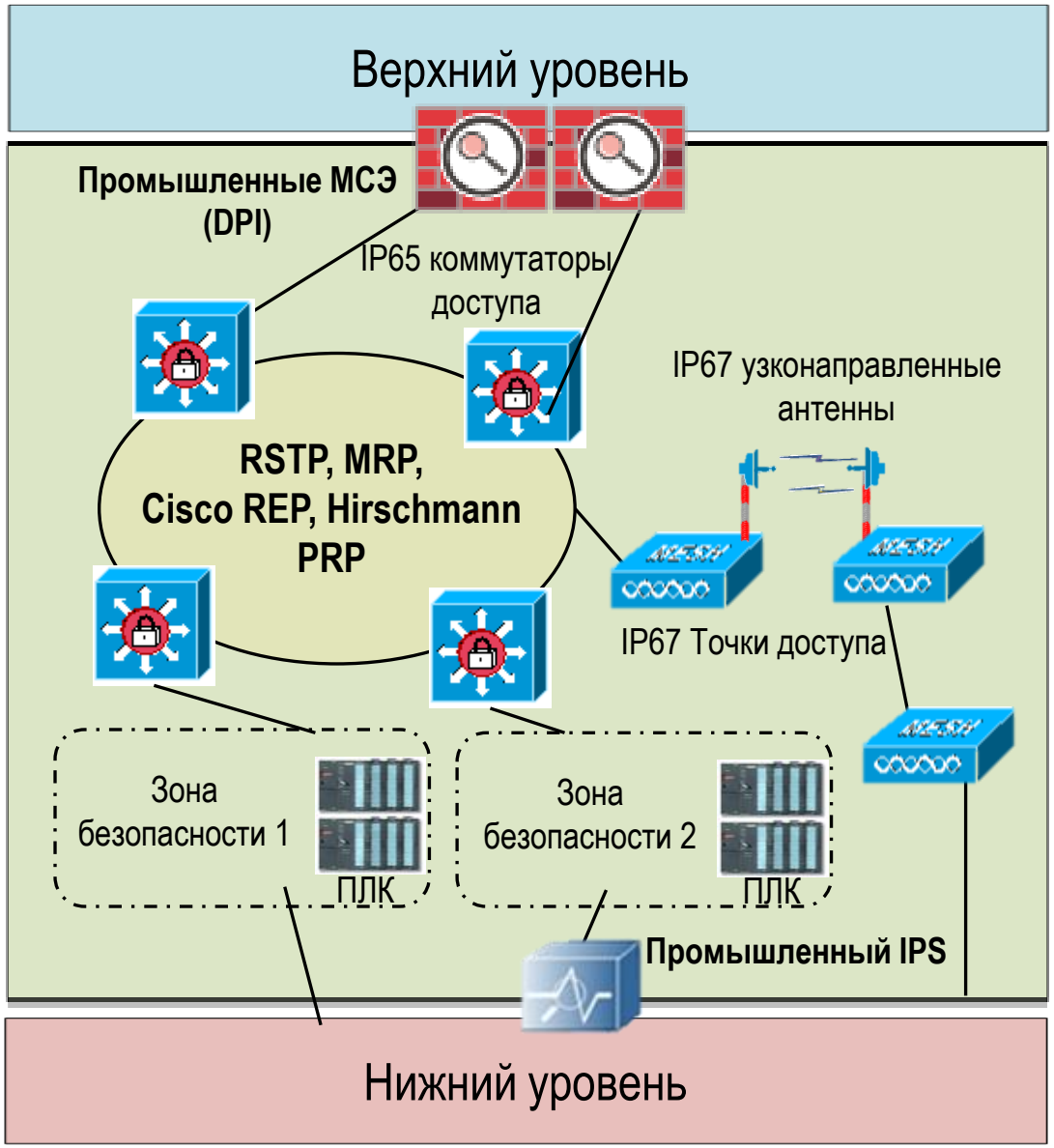
- Выявление вмешательства в SCADA, ЧМИ
- Контроль непропатченных систем

Антивирусная защита

- Наличие сигнатур, позволяющих выявлять вирусы для SCADA

Защита на среднем уровне АСУ ТП

ТЕХНОСЕРВ



Архитектурный уровень

- Сегментация и разделение на зоны безопасности
- Отказоустойчивость и доступность
- Реализация в промышленном исполнении
- Защита промышленных Wi-Fi

Промышленные IPS

- Наличие сигнатур промышленных протоколов (Modbus, OPC, МЭК 104)
- Устойчивость к вибрациям, пыли, влаге, температуре

Промышленные межсетевые экраны (IPS, маршрутизаторы, коммутаторы)

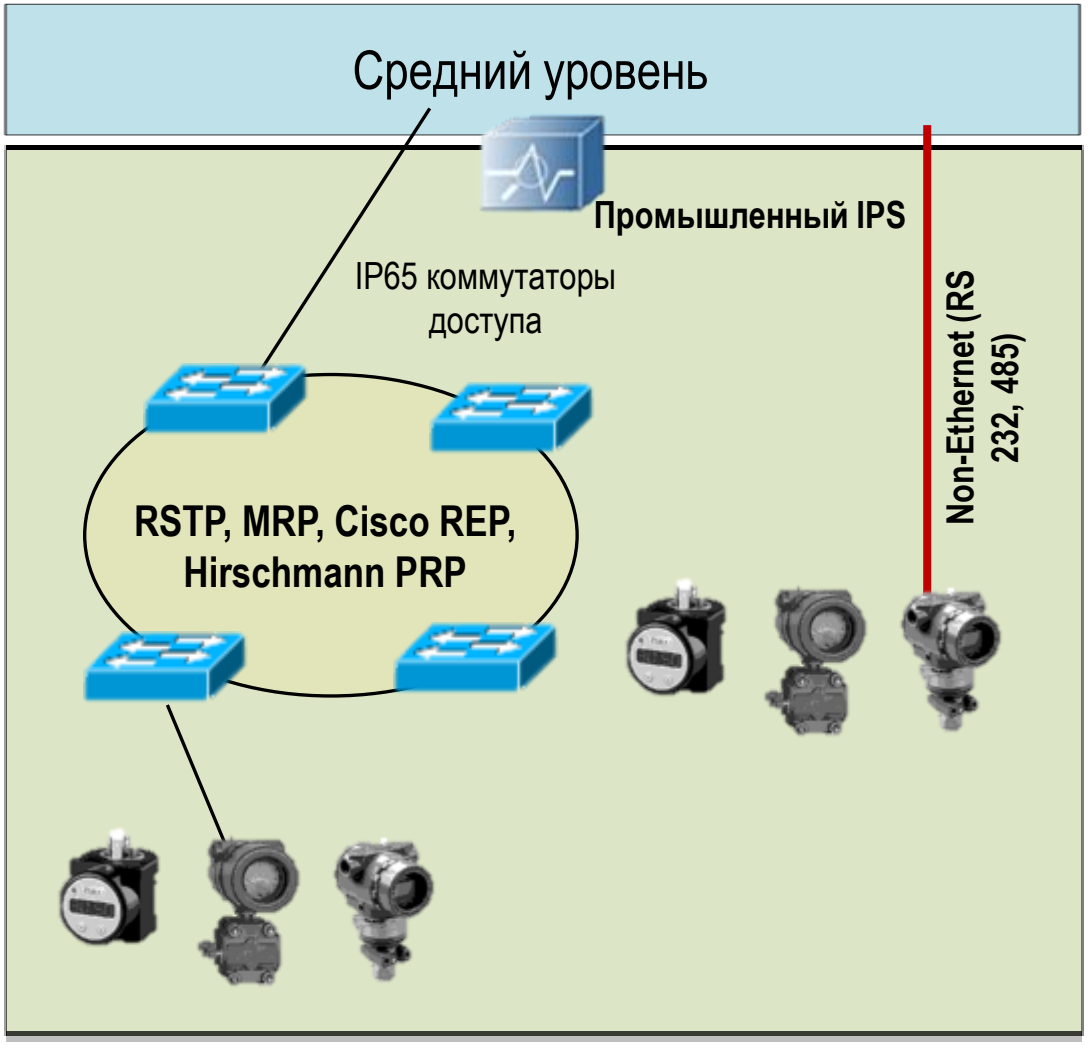
- Контроль сессий
- Инспектирование промышленных протоколов (Modbus, OPC, МЭК 104)
- Возможность работы в прозрачном режиме и режиме обучения (простота внедрения)
- Устойчивость к вибрациям, пыли, влаге, температуре

Мониторинг целостности

- Выявление вмешательства в ПЛК
- Контроль непропатченных систем

Защита на нижнем уровне АСУ ТП

ТЕХНОСЕРВ



Архитектурный уровень

- Отказоустойчивость и доступность
- Реализация в промышленном исполнении

Промышленный IPS низового уровня

- Предотвращение вторжений
- Требования по малому времени сходимости и отклика
- Анализ и контроль электрических сигналов от контроллеров к исполнительным механизмам

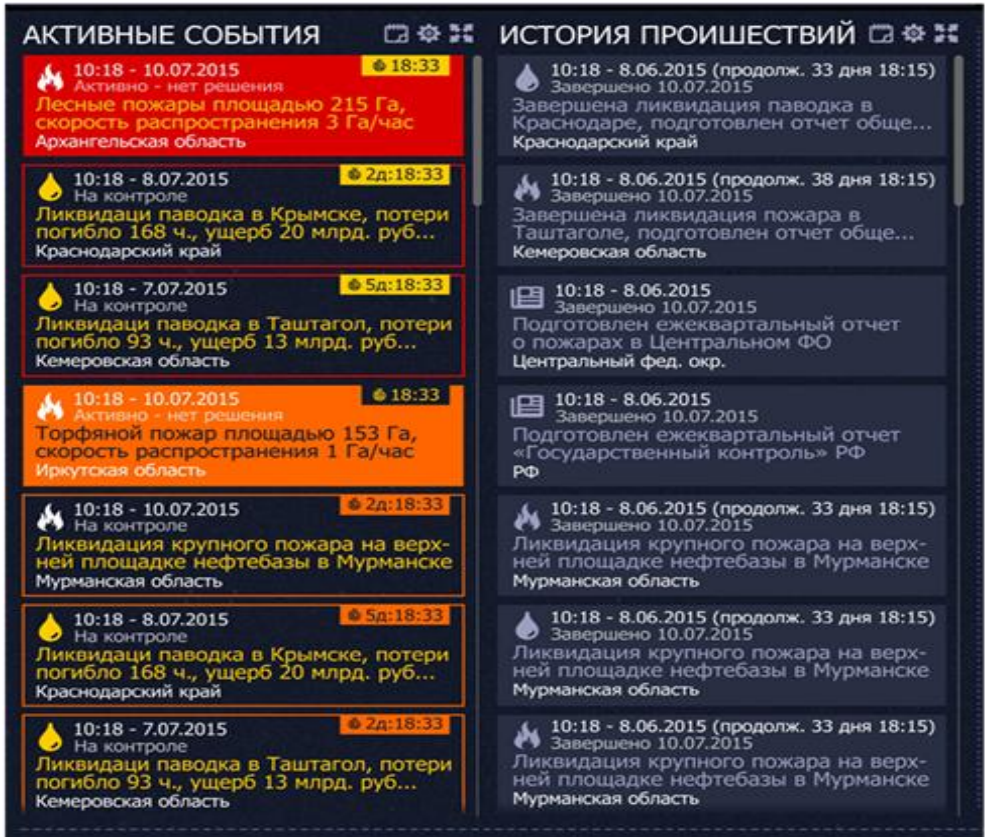
Построение центра мониторинга кибербезопасности АСУ ТП (SCADA-IS-CERT)

ТЕХНОСЕРВ

Аналитика

Прогнозирование

Отчетность



Мониторинг событий

Контроль событий

Предупреждение угроз

Контроль угроз

Устранение угроз

IEIT
INSTITUTE OF ENGINEERING & INFORMATION TECHNOLOGIES

Спасибо за внимание!

Москва, ул. Юности д. 13А
Т: +7 (495) 648-08-08
Ф: +7 (495) 648-08-07
www.technoserv.com