Создание системы обеспечения ИБ АСТУ электросетевой компании

Игорь Тарви
Ведущий архитектор систем безопасности АСУ ТП
АО «ДиалогНаука»

ДиалогНаука

Тел.: +7 (495) 980 67 76
http://www.DialogNauka.ru
ITarvi@DialogNauka.ru

О компании «ДиалогНаука»

- Системный интегратор в области информационной безопасности, успешно работающий на рынке более 25 лет

- АО «ДиалогНаука» выполняет проекты по разработке, созданию и внедрению систем обеспечения информационной безопасности в банковской, энергетической, промышленной, оборонной и других отраслях

- Компания имеет все необходимые лицензии ФСТЭК, ФСБ и Министерства обороны на выполнения полного комплекса работ по защите информации

Цели создания системы обеспечения ИБ

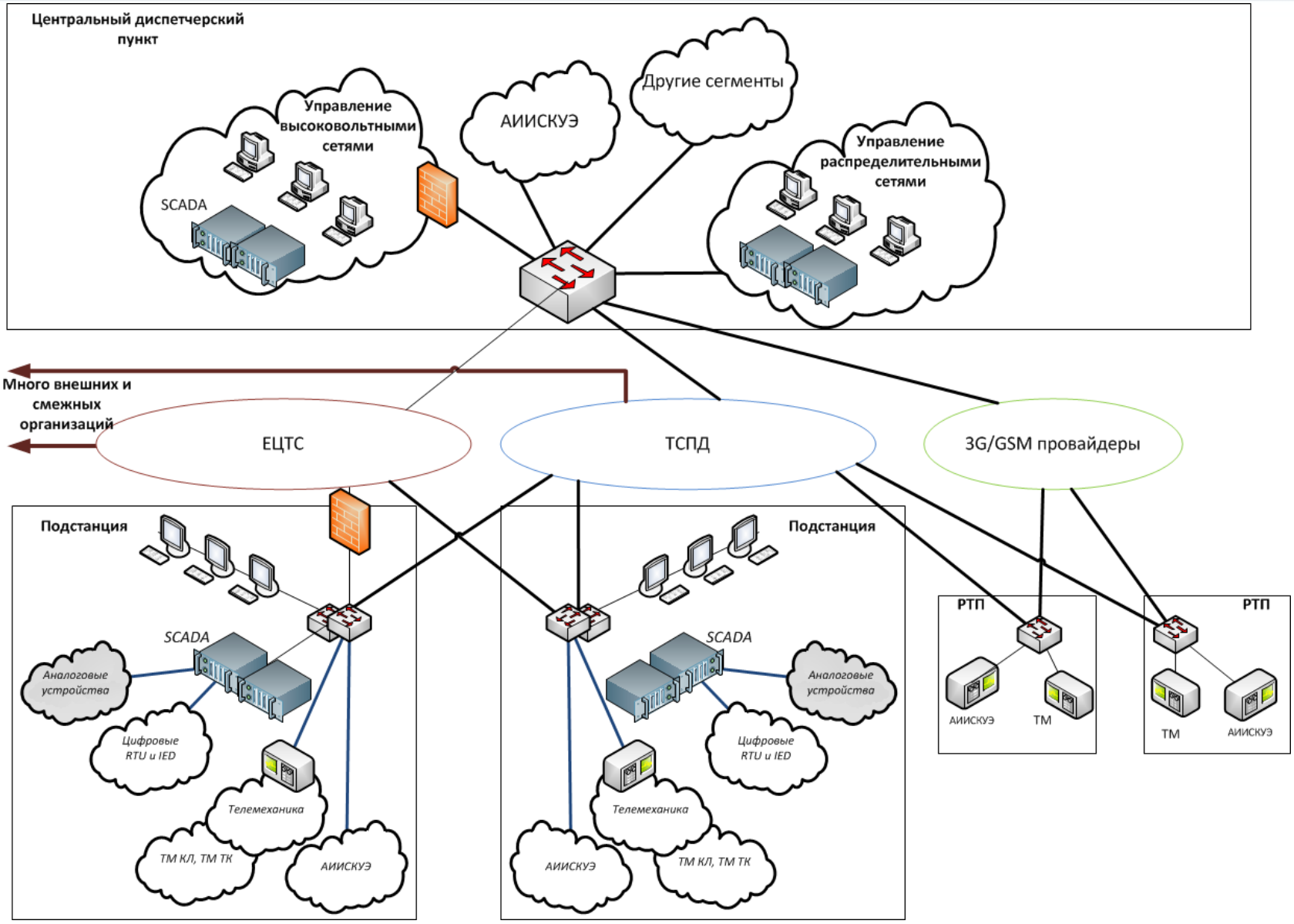
- Обеспечение защиты информационных ресурсов АСТУ от внешних и внутренних угроз безопасности
- Выполнение требований действующего законодательства в области информационной безопасности
- Обеспечение надежности функционирования основного и вспомогательного оборудования АСТУ
- Обеспечение оперативного контроля текущего уровня информационной безопасности АСТУ

Стадии проекта по созданию СОИБ

Нормативные документы

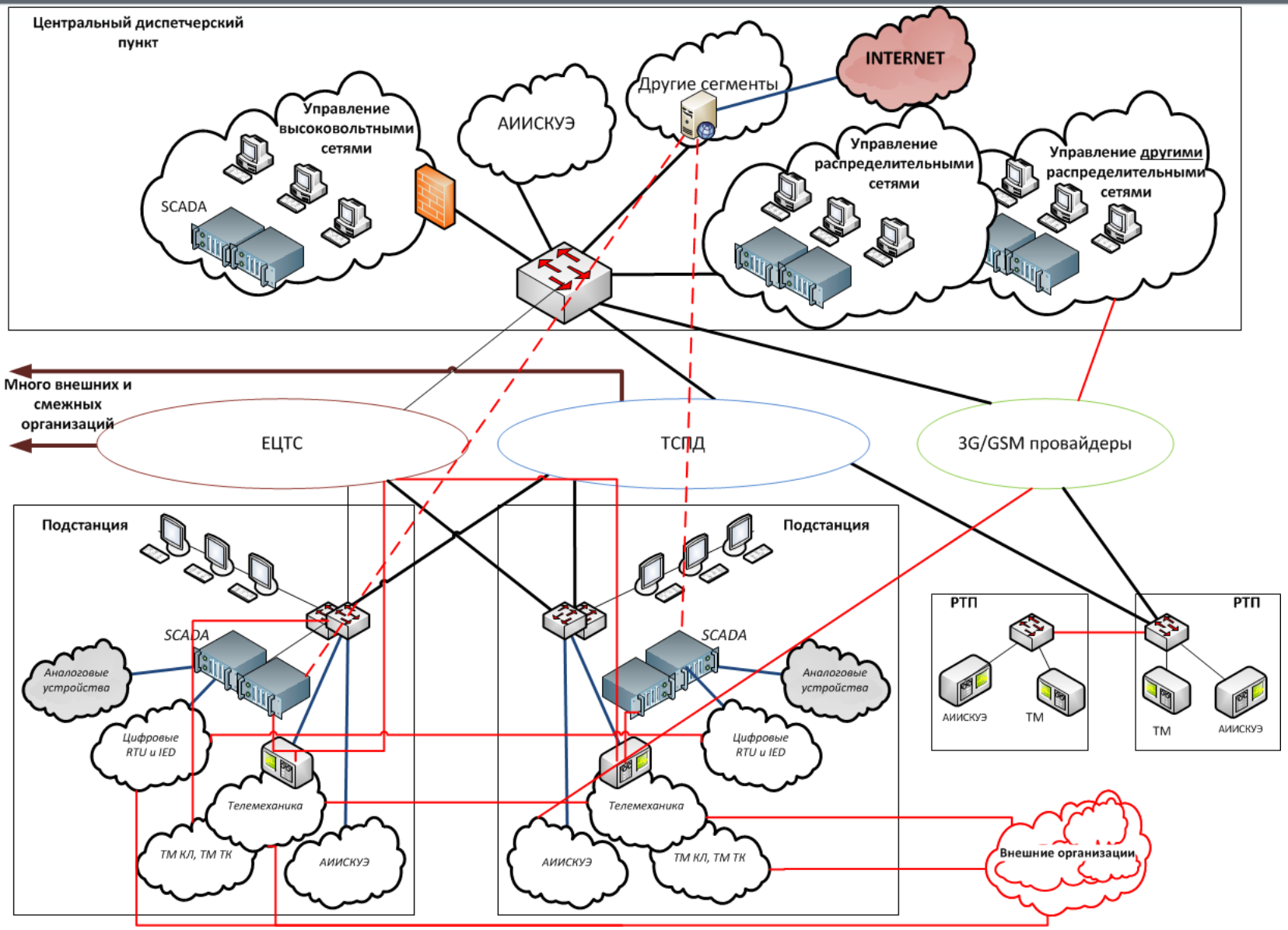
Приказ №31 ФСТЭК России	• Основные требования • Базовый набор мер
Руководящие документы ФСТЭК по защите ключевых систем информационной инфраструктуры (КСИИ)	• Моделирование угроз
IEC 62443, IEC 62351, NIST SP800-82	• Методология аудита • Рекомендации и дополнение мер защиты

Информация о АСТУ до обследования



ДиалОгНаука

Информация о АСТУ после обследования



ДиалОгНаука

Примеры выявленных уязвимостей

Незащищенный удаленный доступ к АСТУ через Интернет

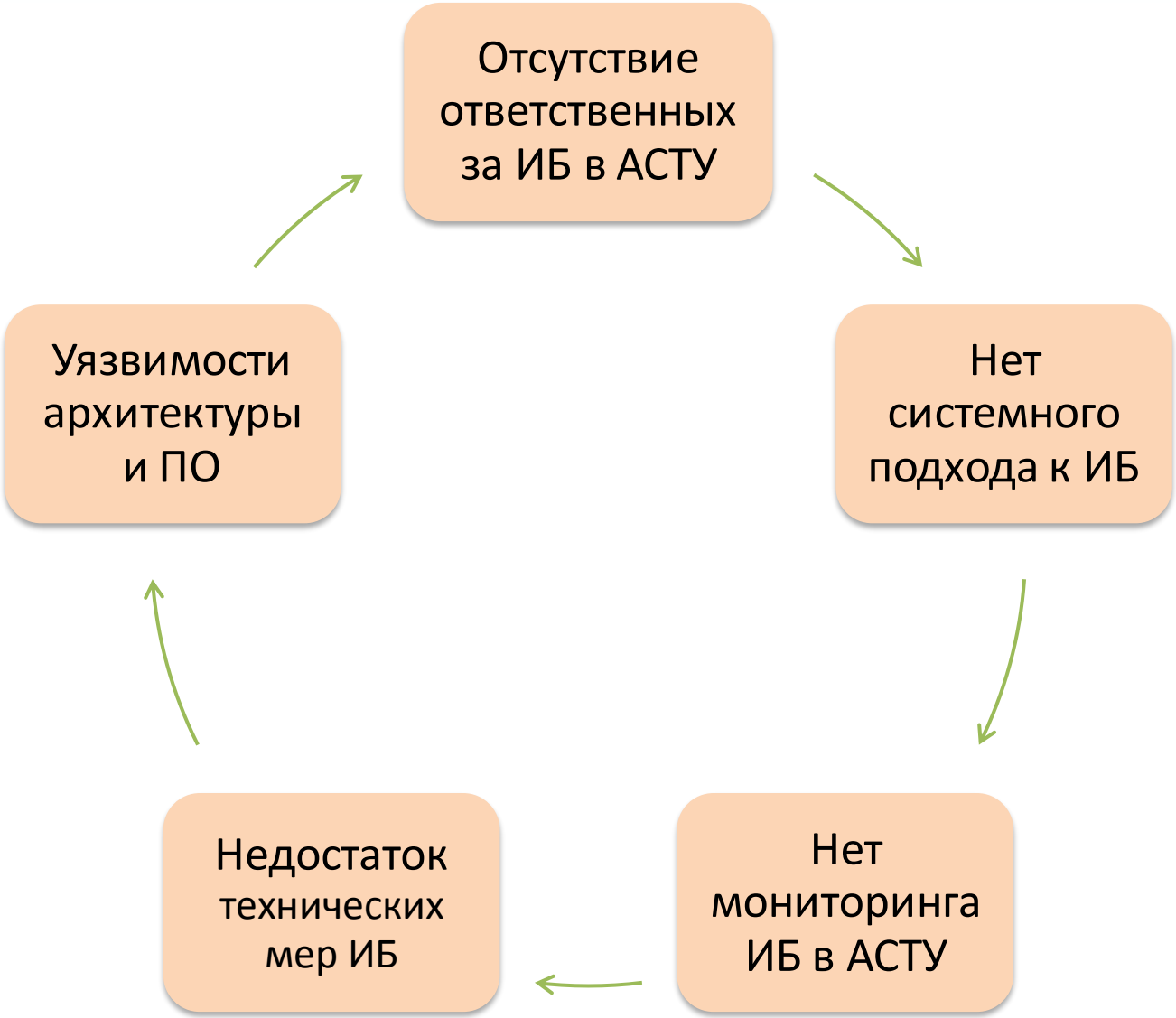
Вредоносное программное обеспечение

Отсутствие правил МЭ (permit any any), или отсутствие самих МЭ, имеющихся в документации

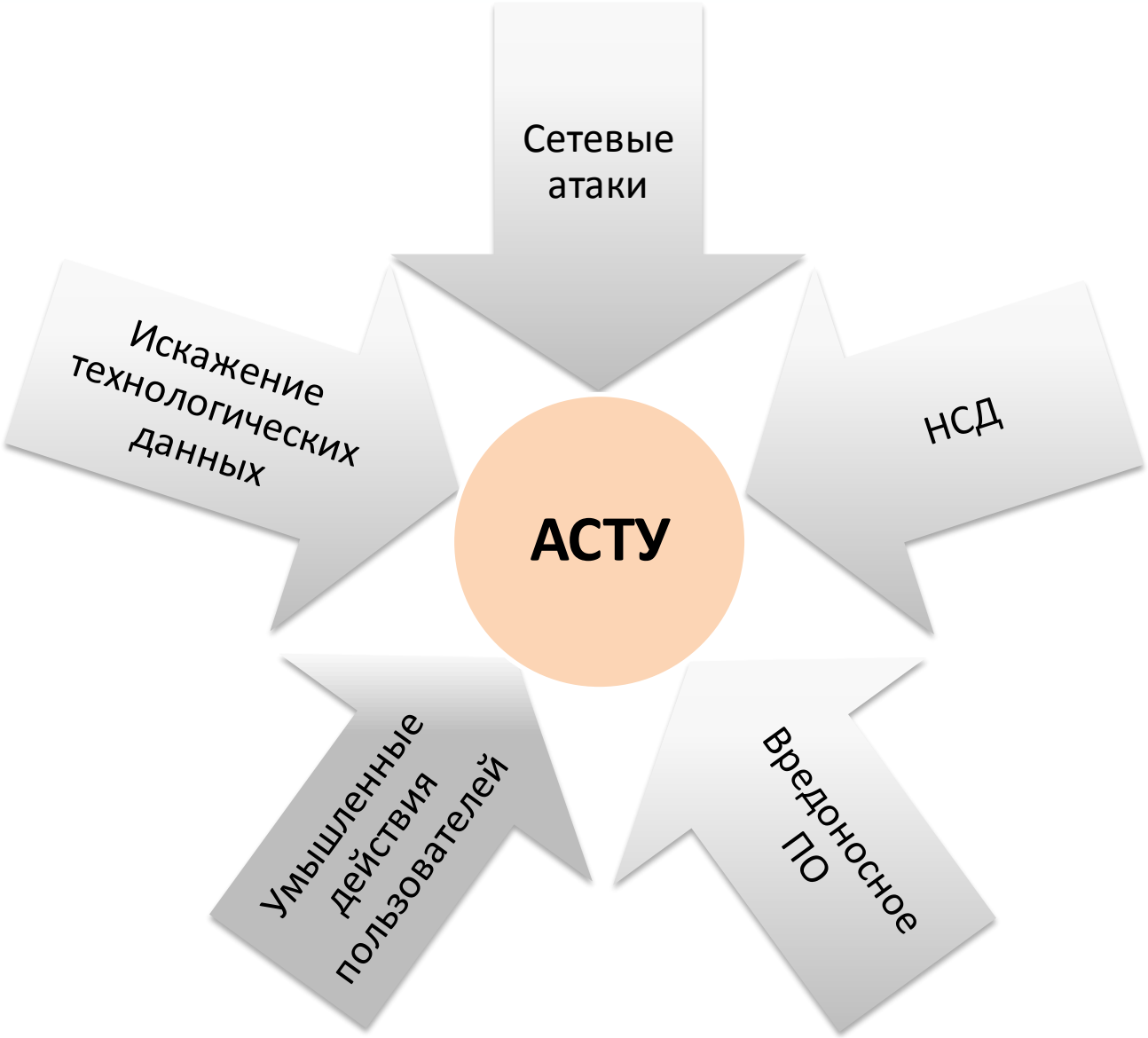
Неконтролируемые и слабо документированные связи на нижнем уровне

Пароли, установленные подрядчиками при создании системы

Ключевые «поводы для беспокойства»



Основные угрозы



Ключевые задачи

Внедрение процессов ИБ

Защита сети

- Сегментирование и защита периметра
- Обнаружение/блокирование сетевых атак, червей и т.п.

Защита конечных устройств

- Защита от вредоносного ПО
- Аутентификация и контроль доступа (в т.ч. для устройств в РТП/ТП/СП)

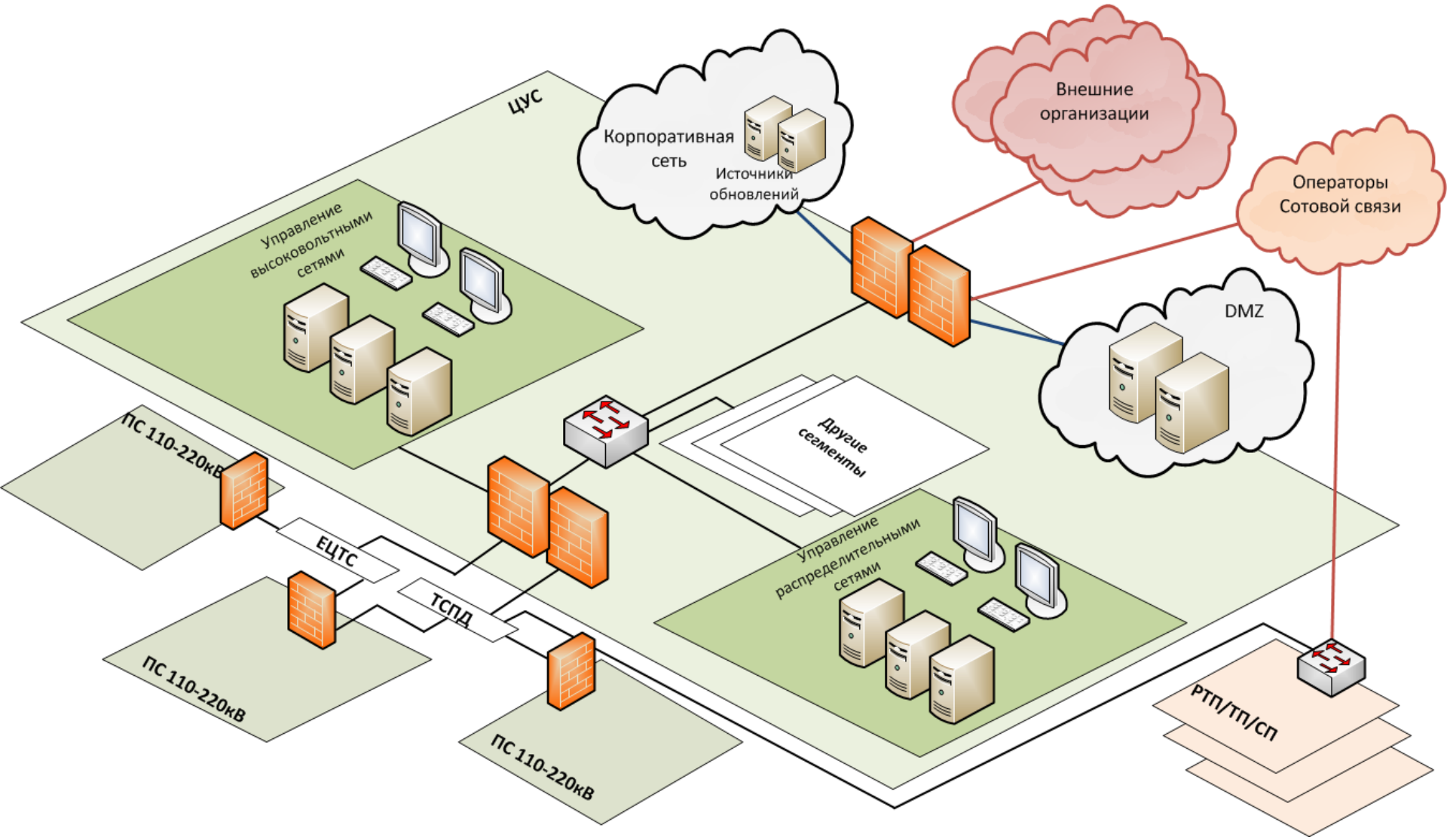
Технологический трафик

- Обеспечение целостности
- Обнаружение несанкционированных действий

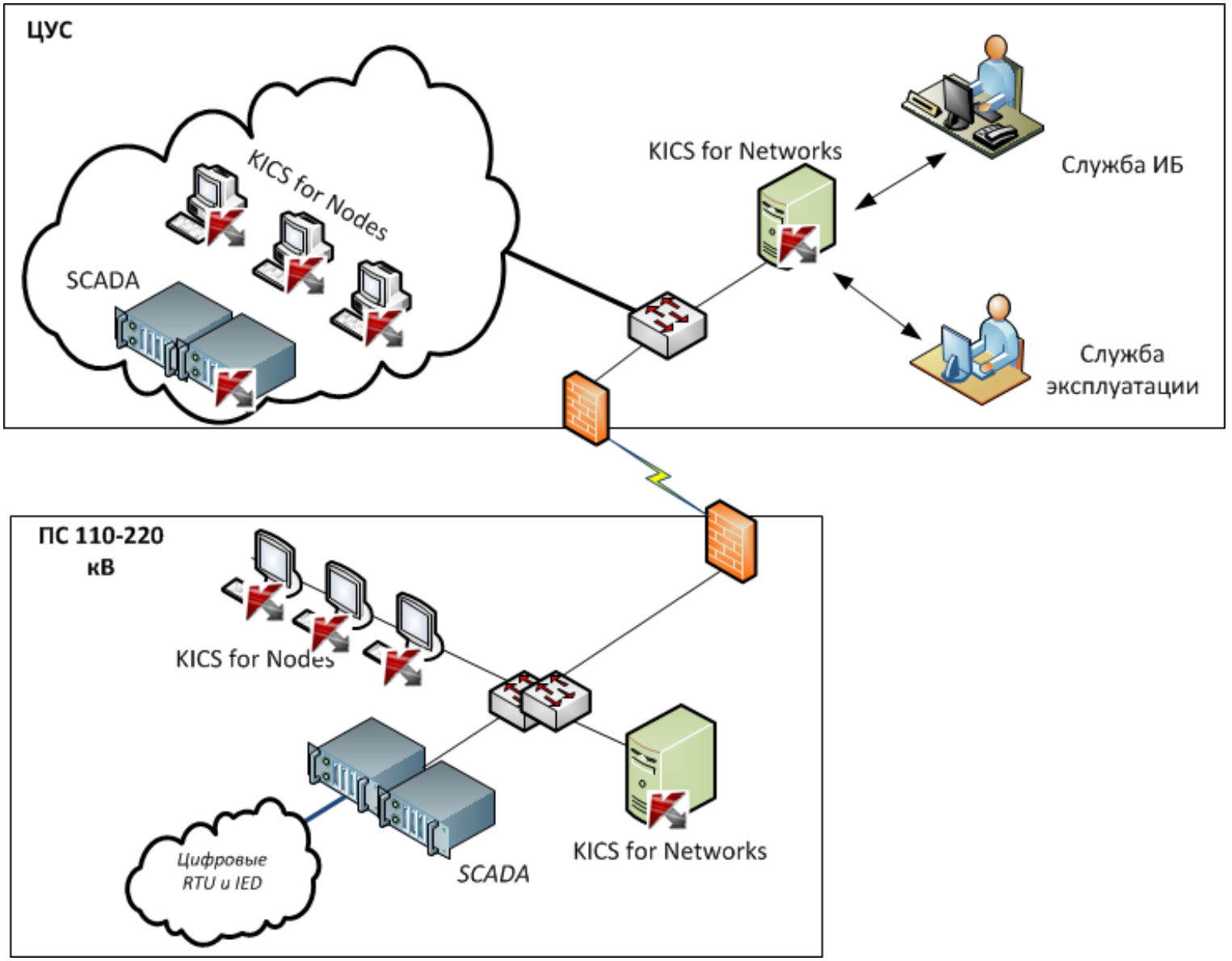
Наблюдаемость

- Обеспечение мониторинга ИБ в АСТУ
- Дополнительный контроль технологического трафика

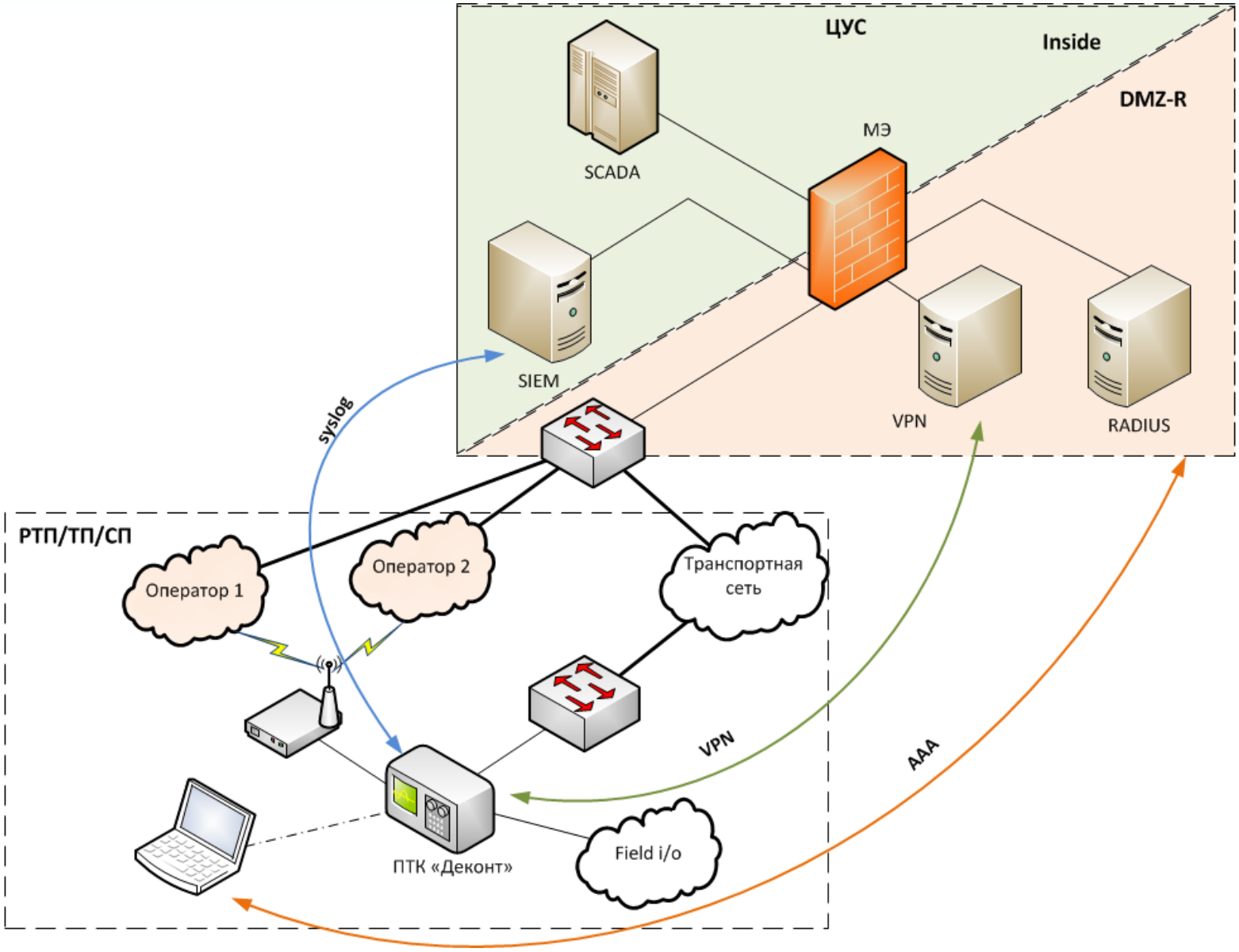
Организация защиты на уровне сети



Организация защиты на уровне АРМ, серверов и мониторинг технологического трафика



Защита РТП/ТП/СП



Рекомендации по ИБ для систем телемеханики

Поддержка VPN для обеспечения целостности передаваемых данных, использование стандартных международных и отечественных криптоалгоритмов (AES/3DES/ГОСТ)

Аутентификация с использованием RADIUS-сервера

Возможность передачи журналов регистрации событий в SIEM-систему по SNMP или SYSLOG

Ключевые выполняемые задачи

Защита от вредоносного ПО

Защита от сетевых атак

Защита от несанкционированного доступа

Обеспечение целостности технологических данных

Мониторинг и реагирование на инциденты ИБ

Требуемая квалификация специалистов по ИБ в АСТУ

Знания принципов ИБ, актуальных угроз и рисков, технологий, мер и средств защиты информации

Понимание технологических процессов АСТУ, знание инфраструктуры и применяемых решений

Информированность об угрозах и методах атак и обеспечения кибербезопасности технологических систем

Опыт администрирования, поддержки и управления применяемыми в СОИБ средствами защиты информации

Спасибо за внимание!