VI научно-практическая конференция «Информационная безопасность АСУ ТП КВО», Москва, 27–28 февраля 2018 г. The VI scientific and practical conference "Information security of automated control systems for technological processes of critical objects", Moscow, February 27-28, 2018.

А.В. Корнеев, руководитель Центра проблем энергетической безопасности Института США и Канады РАН, Москва.
Andrei V. Korneyev, Ph.D. (Econ.), Head, Center of Energy Security Problems, Institute for the USA and Canadian Studies, RAS, Moscow.

Принципы организации и контроля политики безопасности АСУ ТП КВО в США

Organizational and monitoring principles of the security policy to operate automated control systems for technological processes of critical objects in the USA

Москва, 2018 || Moscow, 2018

Новые опасные условия, тренды и факторы на примере КВО ТЭК США

- *Ключевые тенденции и новые факторы*:

- Новые риски: дистанционный взлом производственных информсетей и деактивация производственной физической защиты, компактное электромагнитное импульсное оружие военного и террористического назначения, облачные среды и системы автоматизированного производственного контроля и управления.

- Внедрение новых технологий активно-адаптивных или «интеллектуальных» энергетических сетей (ААЭС – Smart Grids) и цифровых систем автоматизации управления производственными процессами (АСУТП – SCADA) вызывает дополнительные многосторонние риски.

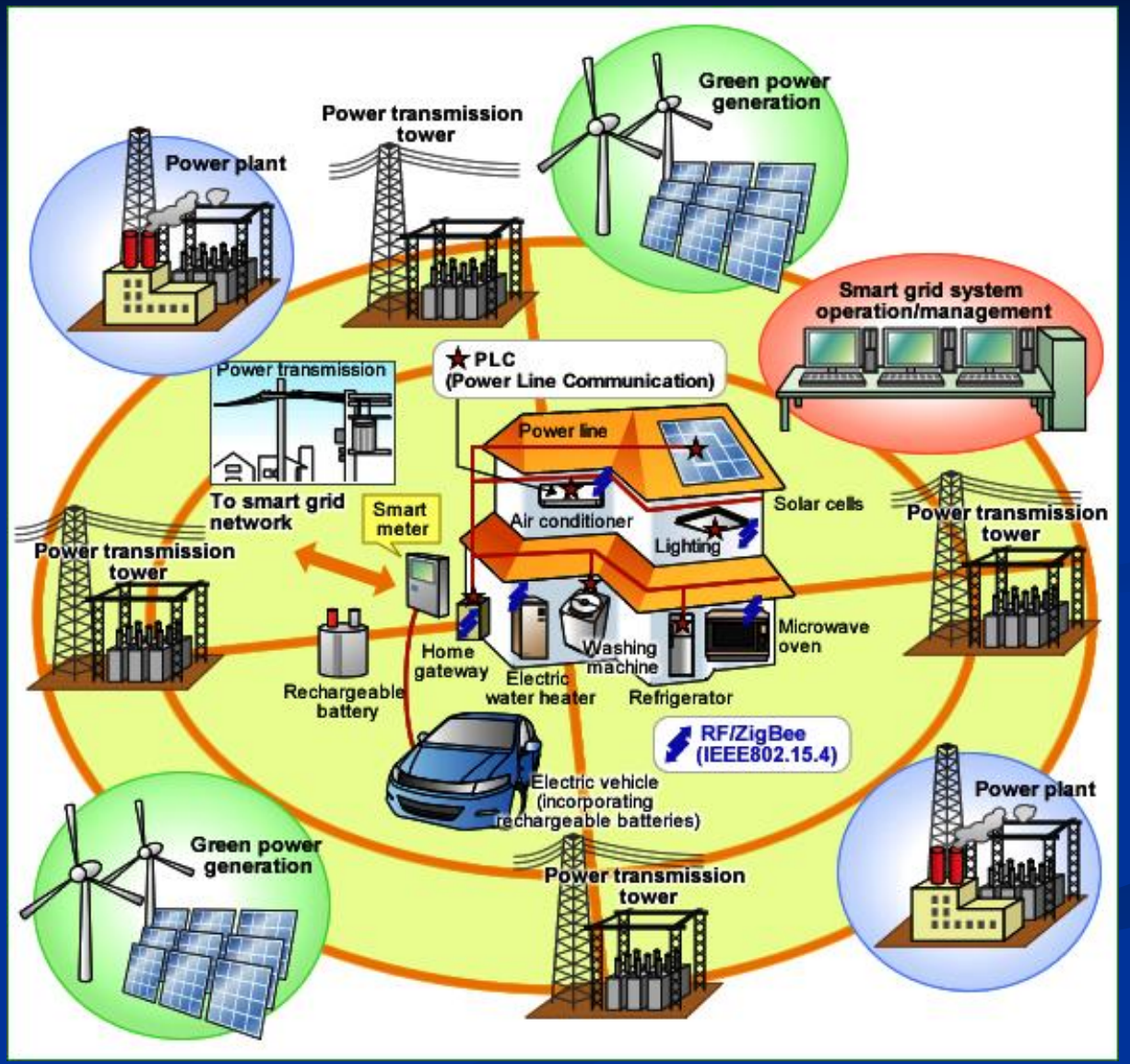
- Смена формации и технологических укладов, растущее несоответствие возможностей реакции человека новым требованиям. Дефицит навыков когнитивного мышления.

- ➔ *Постиндустриальный барьер. Фазовый переход на уровень следующего технологического уклада. Трудность адаптации, необходимость новых средств и методов обучения.*

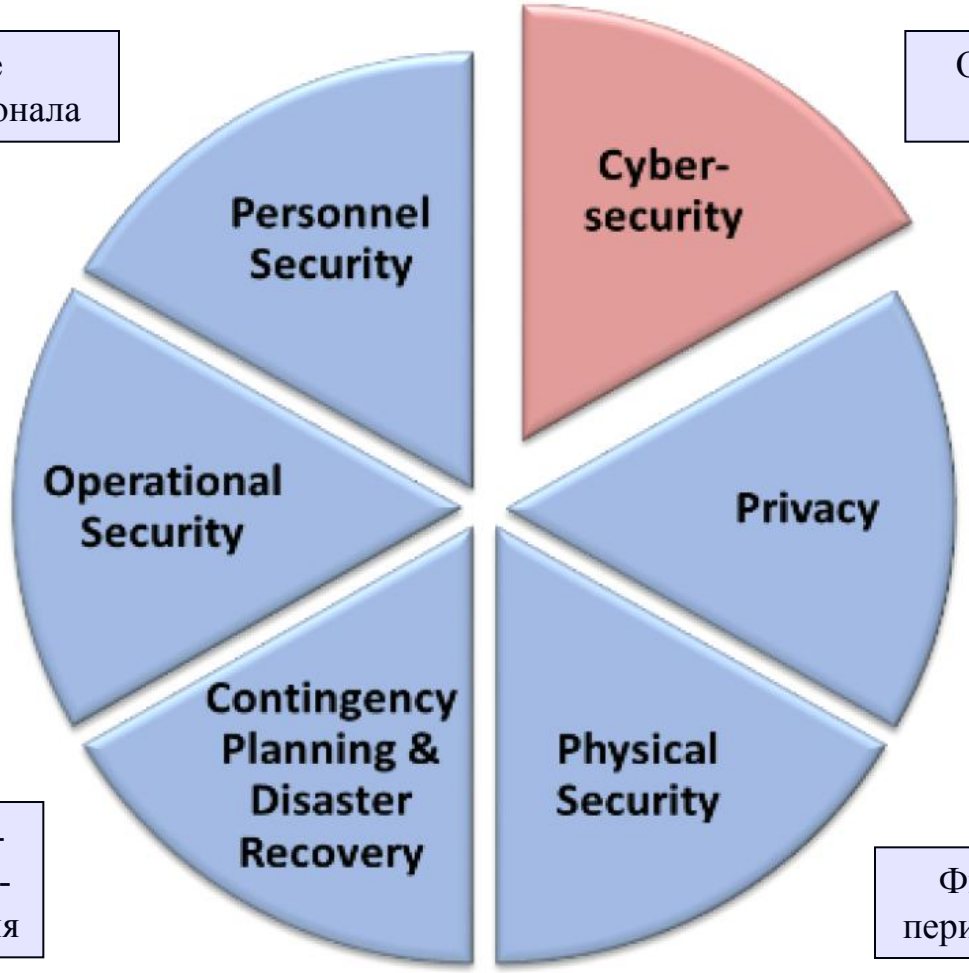
Трудности процесса перехода к интеллектуальным энергетическим сетям

➔ Схема процесса построения сложных интегрированных энергосистем в США.

- *Разнородность объектов, проблемы совместимости и синхронизации энергетических и информационных потоков.*
- *Проблемы устойчивости управляемого функционирования сетей по пикам нагрузки и аккумуляции.*
- *Длительная будущая встроенность подсистем возобновляемых и минеральных источников энергии.*
- *Информационная уязвимость, угроза кибертерроризма.*



Основные элементы политики обеспечения безопасности АСУ ТП КВО в США



Обеспечение надежности персонала

Обеспечение режима кибербезопасности

Обеспечение операционной безопасности процесса управления

Защита личной информации и статуса персонала

Планирование непредвиденных потерь и аварийного восстановления

Физическая защита периметра предприятий

Задача – встроить устойчивое воспроизводство режима оптимальной безопасности в культуру всего корпоративного управления бизнесом.

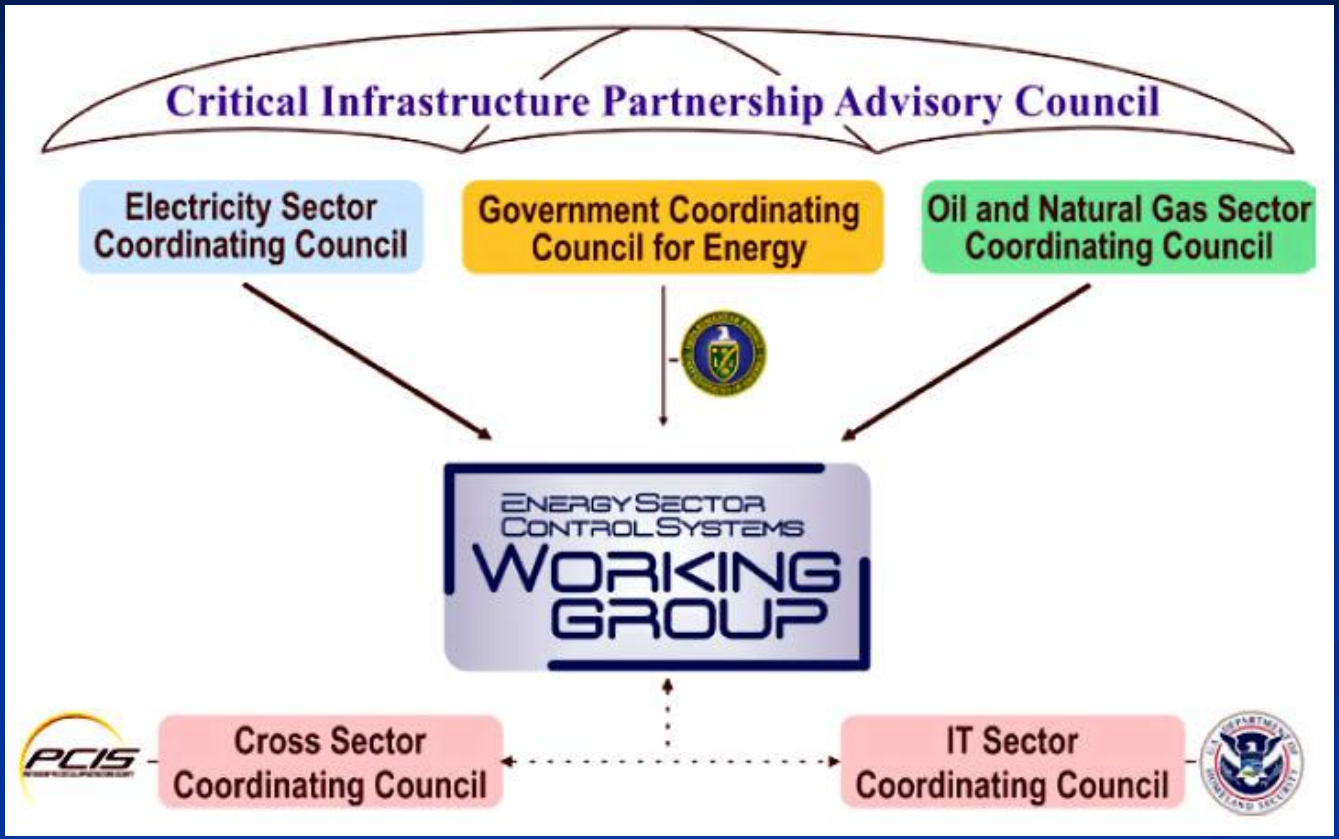
«Дорожная карта» обеспечения кибербезопасности энергосистем США

- «Дорожная карта» обеспечения кибербезопасности энергосистем США к 2020 г. (Road-map to Achieve Energy Delivery Systems Cybersecurity 2011).
- Режим кибербезопасности – предотвращение повреждений, защита и восстановление компьютеров, систем и услуг электронных коммуникаций, проводной и беспроводной связи, а также рабочих данных для сохранения их бесперебойной доступности, целостности, надежной аутентификации и конфиденциальности.

- Май 2017 г.: Д. Трамп подписал распоряжение об укреплении кибербезопасности и защите критической инфраструктуры страны от кибератак. Государственное финансирование этого направления составляет свыше 7 млрд долл. в год.

- Группа быстрого реагирования на чрезвычайные ситуации промышленных систем управления Министерства внутренней безопасности США (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) работает в рамках инфраструктурных секторов вместе с правоохранительными и разведывательными службами.
- ICS-CERT координирует действия федеральных, отраслевых и местных органов управления, владельцев АСУ ТП, операторов и поставщиков. Сотрудничает с международными и частными группами быстрого реагирования для проведения контроля инцидентов с системами безопасности и ликвидации их последствий.

Межведомственный консультативный Совет по безопасности критической энергетической инфраструктуры США



Задача – защита КВО ТЭК от терроризма и диверсий. Цель – обезопасить свои энергосистемы при расширении возможностей ведения разведывательных, политических и силовых воздействий в отношении других государств в американских интересах. Верховный суд: – в 2016 г. введено «право атаки» ФБР по решению суда на любой компьютер в мире, в том числе за пределами границ США.

Межведомственный консультативный Совет по безопасности критической энергетической инфраструктуры США

- Внутренний состав консультативного Совета по безопасности критической энергетической инфраструктуры США (Critical Infrastructure Partnership Advisory Council):

- *Government Coordinating Council for Energy* – Правительственный координационный Совет по энергетике.
- *Electricity Sector Coordinating Council* – Координационный Совет электроэнергетического сектора.
- *Oil and Natural Gas Sector Coordinating Council* – Координационный Совет нефтегазового сектора.
- *Energy Sector Control Systems Working Group* – Рабочая группа по системам управления энергетическим сектором.
- *Cross Sector Coordinating Council* – Межотраслевой координационный Совет.
- *IT Sector Coordinating Council* – Координационный Совет сектора информационных технологий.
- *Совет работает в контакте с **Национальным Центром кибербезопасности** (National Cybersecurity Center) министерства внутренней безопасности США в рамках национальной программы по кибербезопасности 2008 г. (Comprehensive National Cybersecurity Initiative, CNCI, NSPD-54/HSPD −23).*

Разработка и первичная начальная адаптация плана кибербезопасности АСУ ТП КВО

❑ Схема **стартового цикла** отраслевой и локальной адаптации плана дорожной карты обеспечения кибербезопасности энергетических распределительных систем в США.

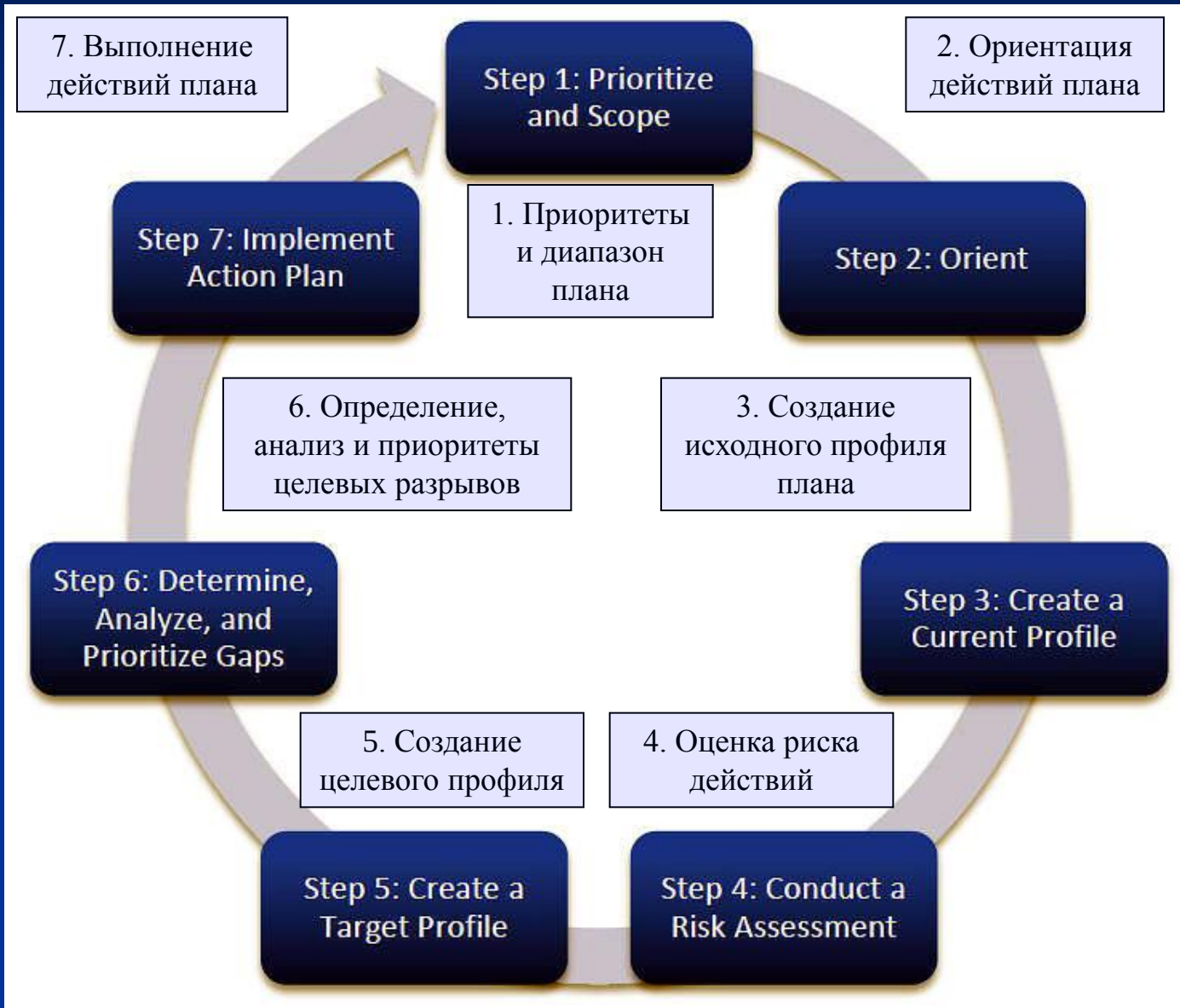
➢*Локализация ведется по отдельным предприятиям ТЭК.*

➢*Важность оценки рисков действий по плану и страхования.*

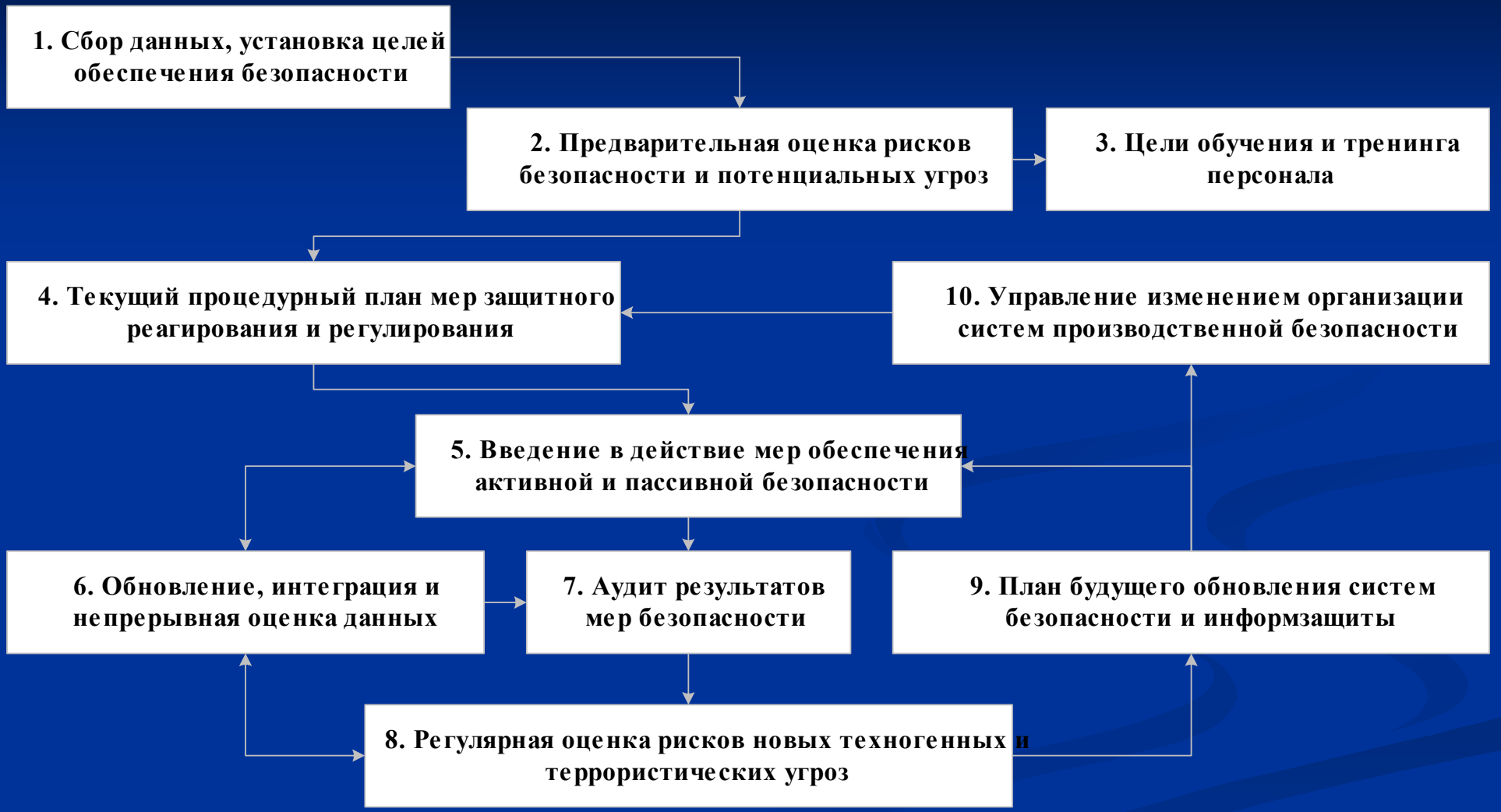
➢*Схема: задача – профильная ситуация – риски – цели – разрывы – приоритеты – реализация.*

➢*Цель, метод, результат.*

➢*Готовый план ставится на режим циклического обновления и связывается с регулярной переподготовкой и контролем работы персонала.*



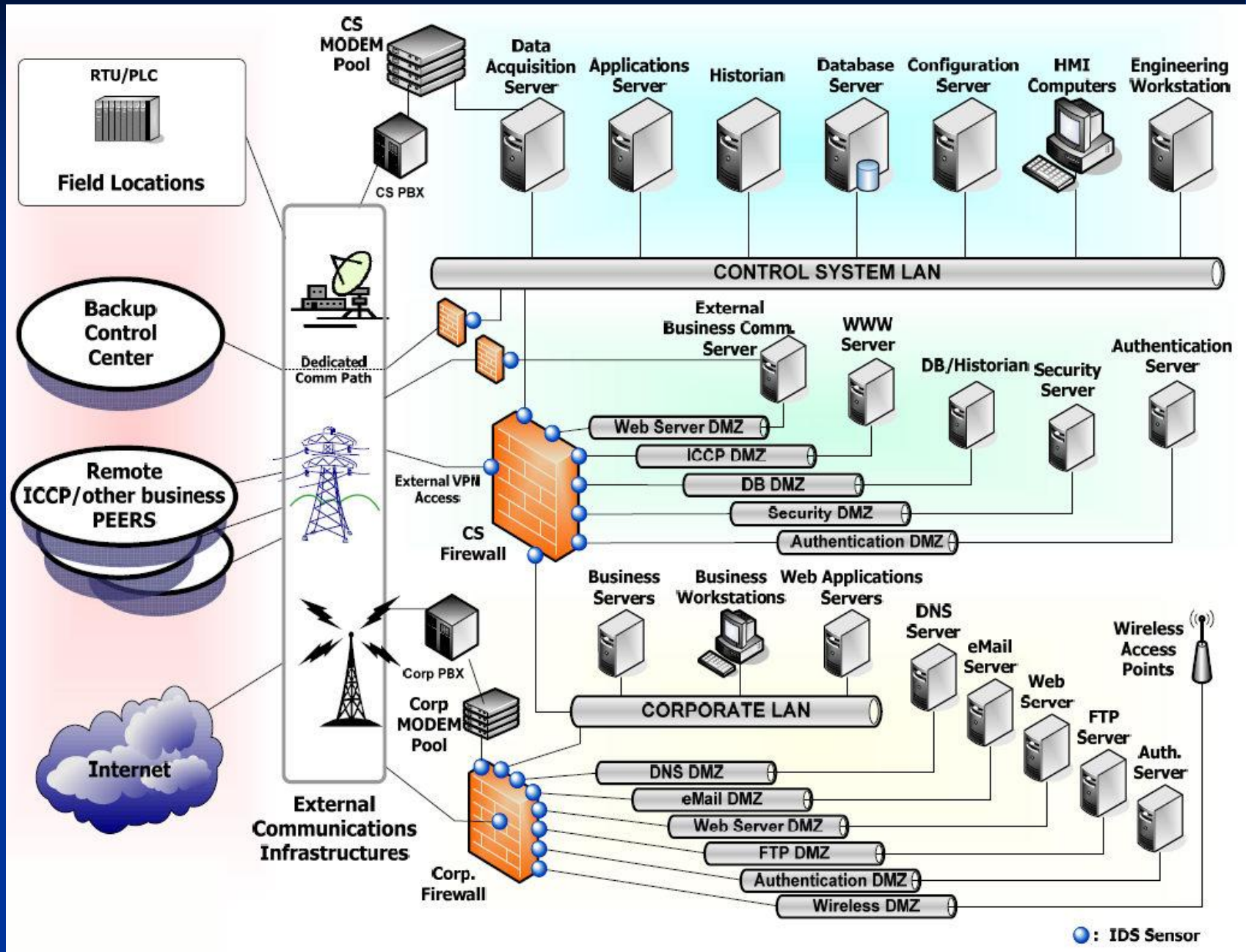
Циклическая схема регулярного обновления планов обеспечения производственной безопасности АСУ ТП КВО



Типовая общая схема взаимодействия систем обеспечения безопасности АСУ ТП КВО

- На схеме представлены:

- *внешние системы и внутренние сети связи;*
- *локальная сеть системы контроля безопасности;*
- *рабочая локальная сеть предприятия;*
- *внешние и внутренние защитные сетевые экраны.*



Типовая общая схема взаимодействия систем обеспечения безопасности АСУ ТП КВО

- Обозначения элементов предыдущей схемы:

- *RTU/PLC field locations* – УСО/ПЛК, устройство связи с объектом / программируемый логический контроллер для рабочих сетей на местах;
- *Backup Control Center* – центр контроля резервного копирования данных;
- *Remote ICCP / other business PEERS* – удаленная система связи по протоколу ICCP (Inter-Control Center Communications Protocol, IEC 60870-6) / пи́ринговая оверлейная компьютерная сеть для связи с другими предприятиями;
- *Internet* – общедоступный Интернет;
- *CS modem pool* – модемной пул системы управления для передачи данных между центральной частью системы управления полевыми контроллерами и устройствами ввода-вывода.
- *CS PBX (CS Private Branch Exchange)* – автоматический коммутатор системы управления на основе протокола IP операторского уровня.
- *Dedicated Comm. Path* – выделенный коммуникационный канал;
- *External Communications Infrastructure* – внешняя коммуникационная инфраструктура;
- *Data Acquisition Server* – сервер сбора данных;

Типовая общая схема взаимодействия систем обеспечения безопасности АСУ ТП КВО

- *Applications Server* – сервер программных приложений;
- *Historian* – сервер резервных контрольных записей;
- *Database Server* – сервер баз данных;
- *Configuration Server* – сервер данных конфигурации;
- *HMI computers* – компьютеры обеспечения человеко-машинного интерфейса,ЧМИ.
- *Engineering Workstation* – инженерная рабочая станция.
- *Control System LAN* – локальная сеть системы управления;
- *External Business Comm. Server* – сервер внешних бизнес-коммуникаций;
- *WWW Server* – веб-сервер;
- *DB Historian* – сервер базы данных резервных контрольных записей;
- *Security Server* – сервер данных безопасности;
- *Authentication Server* – сервер аутентификации;
- *External VPN* – внешняя виртуальная частная сеть;
- *CS Firewall* – защитный сетевой экран системы управления;
- *Web Server DMZ* – демилитаризованная зона веб-сервера;
- ICCP DMZ – демилитаризованная зона связи по протоколу ICCP;

Типовая общая схема взаимодействия систем обеспечения безопасности АСУ ТП КВО

- *DB DMZ* – демилитаризованная зона баз данных;
- *Security DMZ* – демилитаризованная зона данных безопасности;
- *Authentication DMZ* – демилитаризованная зона данных аутентификации;
- *Corp. PBX* – автоматический корпоративный коммутатор предприятия на основе протокола IP операторского уровня;
- *Corp. Modem Pool* – корпоративный модемной пул предприятия;
- *Corporate LAN* – корпоративная локальная сеть предприятия;
- *Business Servers* – бизнес-сервера;
- *Business Workstations* – бизнес-рабочие станции;
- *Web Applications Servers* – сервера программных веб-приложений;
- *DNS Server* – авторитативный сервер доменных имен;
- *eMail Server* – сервер электронной почты;
- *Web Server* – веб-сервер;
- *FTP Server* – сервер протокола передачи данных;
- *Auth. Server* – сервер аутентификации;
- *Corp. Firewall* – корпоративный сетевой защитный экран предприятия;

Типовая общая схема взаимодействия систем обеспечения безопасности АСУ ТП КВО

- *DNS DMZ* – демилитаризованная зона данных доменных имен;
- *eMail DMZ* – демилитаризованная зона данных электронной почты;
- *Web Server DMZ* – демилитаризованная зона данных веб-сервера;
- *FTP DMZ* – демилитаризованная зона протокола передачи данных;
- *Authentication DMZ* – демилитаризованная зона данных аутентификации;
- *Wireless DMZ* – демилитаризованная зона беспроводной передачи данных;
- *Wireless Access Point* – точка доступа беспроводной передачи данных;
- *IDS Sensor* – датчик системы обнаружения несанкционированных вторжений (Intrusion Detection System).

- ***Наиболее вероятные факторы риска:*** 1) незакрытые известные уязвимости, ошибки человеко-машинного интерфейса; 2) уязвимые протоколы удаленного мониторинга; 3) неправильное управление административным доступом; 4) переполнение буфера в службах АСУ ТП; 5) манипуляции данными и вброс командных сообщений; 6) внедрение вредоносного кода на языке структурированных запросов (SQL-кода); 7) использование стандартных протоколов для аутентификации "открытым текстом" уязвимых для общедоступных стандартных средств декодирования; 8) незащищенная передача учетных данных рабочих программных приложений.

❑ *Схема целевой сегментации элементов обеспечения комплексной безопасности АСУ ТП.*

➢*Криптографические блоки в контрольно-измерительных приборах, исполнительных механизмах и датчиках систем управления.*

➢*Скрытые контрольные виртуальные каналы в компьютерных сетях.*

➢*Контроль вскрытия аппаратуры, алгоритмы блокировки и востановления программного обеспечения.*

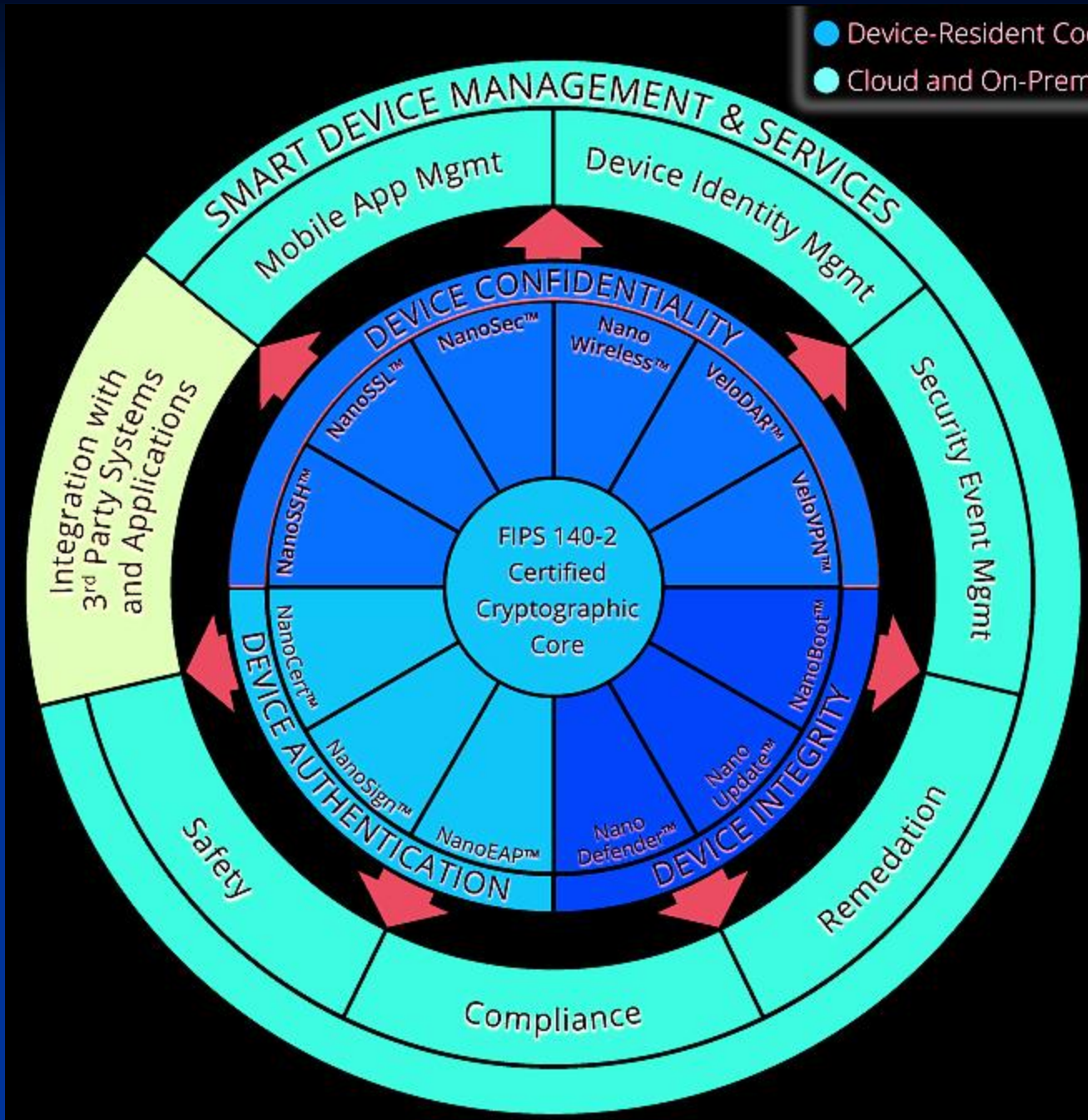


Схема целевой сегментации элементов обеспечения безопасности АСУ ТП КВО

- Обозначения основных элементов предыдущей схемы:

- *Device-Resident code* – программный код аппаратного размещения;
- *Cloud and On-Premise Services* – облачные и локальные сервисы;
- *Integration with 3-rd Party Systems and Applications* – интеграция с дополнительными системами и программными приложениями;
- *Smart Device Management* & Services – управление и обслуживание «умных» устройств;
- *Mobile App. Mgmt.* – управление мобильными программными приложениями;
- *Device Identity Mgmt.* – управление идентификацией устройств;
- *Security Event Mgmt.* – управление событиями политики безопасности;
- *Remediation* – санация нарушений безопасности;
- *Compliance* – соблюдение условий режимов;
- Safety – обеспечение состояния безопасности;
- *Device Authentication, Confidentiality, Integrity* – аутентификация, конфиденциальность, целостность устройств;
- *FIPS (Federal Information Processing Standard) 140-2 Certified Cryptographic Core* – сертифицированный криптографический модуль по федеральному стандарту обработки информации США 140-2.

Спасибо за внимание!

Источники:

U.S. Department of Energy Cyber Strategy. – Wash.: U.S. Department of Energy, 2015. – 17 pp.

Energy Delivery Systems Cybersecurity Roadmap. – Wash.: The Energy Sector Control Systems Working Group, 2011. – 17 pp.

Small Business Information Security: The Fundamentals. – Wash.: National Institute of Standards and Technology, 2016. – 54 pp.

Vulnerability Analysis of Energy Delivery Control Systems. – Idaho Falls: Idaho National Laboratory, 2011. – 183 pp.

Energy Sector Cybersecurity Framework Implementation Guidance. – Wash.: The U.S. Department of Energy, 2015. – 53 pp.