Реализация фреймворка ИБ АСУ ТП ОА

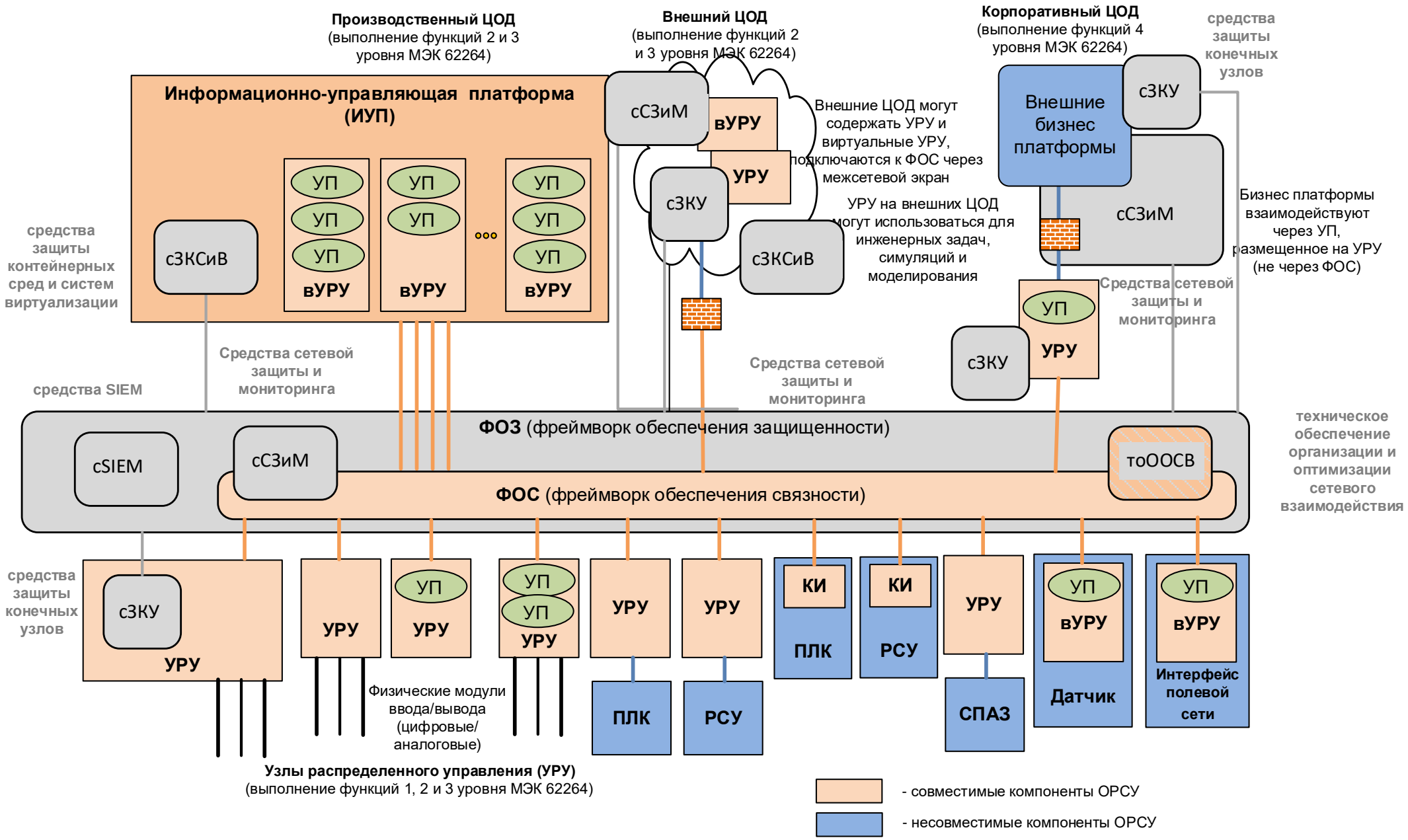
Ключевые принципы и необходимые мероприятия

kaspersky

Часть 2 стандарта O-PAS определяет фреймворк обеспечения защищенности промышленных систем автоматизации

Цель O-PAS— интеграция ANSI/ISA 62443 в структуру O-PAS, обеспечивая соответствие требованиям кибербезопасности и лучшим отраслевым практикам

https://pubs.opengroup.org/open-process-automation/standard/opas2.1/part2.html


Производственный ЦОД
(выполнение функций 2 и 3 уровня МЭК 62264)
Внешний ЦОД
(выполнение функций 2 и 3 уровня МЭК 62264)
Корпоративный ЦОД
(выполнение функций 4 уровня МЭК 62264)
средства защиты конечных узлов
Информационно-управляющая платформа (ИУП)
сСЗиМ
вУРУ
УРУ
сЗКУ
сЗКСиВ
УП
вУРУ
Внешние ЦОД могут содержать УРУ и виртуальные УРУ, подключаются к ФОС через межсетевой экран
УРУ на внешних ЦОД могут использоваться для инженерных задач, симуляций и моделирования
Внешние бизнес платформы
Бизнес платформы взаимодействуют через УП, размещенное на УРУ (не через ФОС)
средства защиты контейнерных сред и систем виртуализации
средства SIEM
Средства сетевой защиты и мониторинга
ФОЗ (фреймворк обеспечения защищенности)
ФОС (фреймворк обеспечения связности)
cSIEM
toOOCB
техническое обеспечение организации и оптимизации сетевого взаимодействия
средства защиты конечных узлов
КИ
ПЛК
РСУ
СПАЗ
Датчик
Интерфейс полевой сети
Физические модули ввода/вывода (цифровые/ аналоговые)
Узлы распределенного управления (УРУ)
(выполнение функций 1, 2 и 3 уровня МЭК 62264)
- совместимые компоненты ОРСУ
- несовместимые компоненты ОРСУ

Фреймворк обеспечения связности из проекта ПНСТ использует стандартизированные протоколы связи и модели данных и **обеспечивает безопасный информационный обмен** между компонентами, однако не указано, **как именно достигается безопасный обмен (и что именно означает безопасность!**)

Чтобы внести ясность, предлагается более подробно рассмотреть концепцию **Фреймворка обеспечения защищенности**

Фреймворк обеспечения защищенности (ФОЗ) –

набор правил, принципов и механизмов для поддержания защищенности инфраструктуры открытой распределенной системы управления (ОРСУ), использующей типовые архитектуры, модели, технологии, протоколы и компоненты для бесшовной интеграции с фреймворком обеспечения связности

Пять ключевых принципов ФОЗ

1.Переход от парадигмы защиты периметра (периметров) к защите технологий и активов

2. Интеграция механизмов информационной безопасности между собой, кросс-уровневая безопасность

3.Интеграция показателей общей безопасности в среде ОАСУТП за счет корреляции событий и машинного обучения/ИИ (ML/AI)

4. Применение концепции конструктивной безопасности (Security by design) при создании систем ОАСУТП

5. Распределение ответственности за реализацию ИБ при проектировании, создании, интеграции, эксплуатации компонентов и систем ОАСУ ТП

Ключевые принципы ФОЗ (Фреймворк обеспечения защищенности)

- 1. Переход от парадигмы защиты периметра (периметров) к защите технологий и активов

Необходимые технологии информационной безопасности для ФОС и активов в инфраструктуре ОАСУТП

Необходимые шаблоны проектирования и реализации защищенных сред

Необходимые профили ПАК, технические требования к безопасности активов, требования к разработке безопасного ПО

Необходимые технологии безопасности для технологий и активов

a. технологии обеспечения безопасности отдельных объектов и активов (конечных узлов, оборудования)
b. технологии сетевой защиты и мониторинга
c. технологии защиты контейнерных сред и систем с виртуализацией
d. технологическое обеспечение и оптимизация сетевого взаимодействия в гетерогенной инфраструктуре, обеспечение доверенного и безопасного оборудования для внутрисетевого и внешнего взаимодействия (шлюзы, конвертеры...)
e. To Be Determined (TBD)

Необходимые шаблоны проектирования и реализации защищенных сред

a. Защита конечных узлов с приложениями на уровнях F,I
b. Мониторинг сетевой среды в brownfield/greenfield
c. Защита сетевой среды в brownfield/greenfield
d. Защита контейнерных сред и вертуализаии
e. TBD

Необходимые профили ПАК, технические требования к безопасности активов, требования к РБПО

a. Шлюзы сетевого взаимодействия
b. Конвертеры протоколов
c. сЗКУ – система защиты конечных устройств
d. сСЗиМ- средства сетевой защиты и мониторинга
e. сЗКСиВ – средства защиты контейнерных сред и виртуализации
f. TBD

2 Интеграция механизмов информационной безопасности между собой, кросс-уровневая безопасность

Слой ФОЗ (фреймворк обеспечения защищенности) разворачивается в параллель ФОС (фреймворку обеспечения связности) и слою управления и способствует более эффективному отслеживанию событий и состояния безопасности в промышленных средах

3. Интеграция показателей общей безопасности в среде ОАСУТП за счет корреляции событий и машинного обучения/ИИ (ML/AI)

Интеграция функциональной, физической, информационной, и специальных отраслевых видов безопасности, которая помогает распознать сложные атаки и перейти от стратегии догоняющего в ИБ (*мониторинг, обнаружение, респонс*) к стратегии опережения (*аналитика на отраслевой модели или модели предприятия, предотвращение, мониторинг*).

Ключевые принципы

4. Применение концепции конструктивной безопасности (Security by design) при создании систем ОАСУТП

о безопасности АСУТП задумываются с момента проектирования системы, где цели безопасности интегрируют в себя функциональную безопасность, надежность, устойчивость системы

решения в области обеспечения безопасности отражаются в архитектуре систем и инфраструктур рекурсивно

уменьшаются затраты на безопасность с одновременным повышением ее эффективности

Ключевые принципы

5. Распределение ответственности за защищенность и устойчивость инфраструктуры

Предлагается проработать проблему распределения ответственности следующих участников и факторов

1 Проектировщик
2 Вендор оборудования
3 Интегратор
4 Эксплуатант
5 Отраслевой регулятор
6 Цепочка поставок