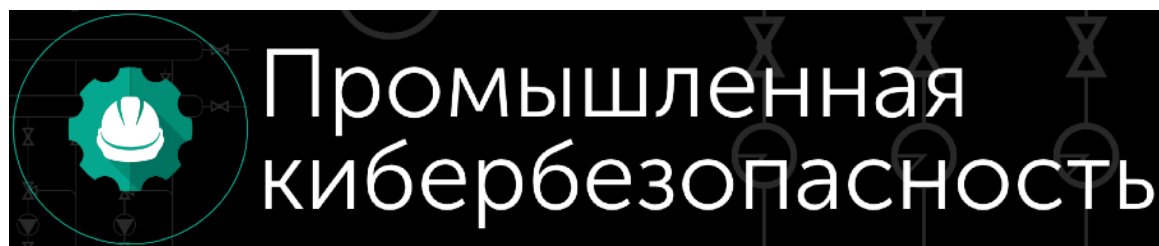


Выбор средств защиты информации (СрЗИ) для промышленных систем

Взгляд бизнеса, регулятора и злоумышленника

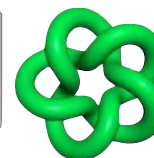


Сочи, Pullman Sochi Center Hotel, зал Камелия
20 сентября 2018 года, 16:20 - 16:40



Алексей Комаров

Менеджер по развитию решений
Уральский Центр Систем Безопасности



akomarov@USSC.ru
<https://ZLONOV.ru/>

УЦСБ и ИБ АСУ ТП

- Разработка корпоративных стандартов
- **Аудиты** действующих АСУ ТП
- Проектирование, ввод в эксплуатацию и поддержка систем обеспечения ИБ АСУ ТП
- Разработка собственного решения - **ДАТАРК**
- **Реализация требований 187-ФЗ**
- **Вебинары**, семинары, курсы



РОСЭНЕРГОАТОМ
ВНИИАЭС



РОС
ЭНЕРГО
АТОМ

ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ
ДИВИЗИОН РОСАТОМА



Северсталь

 **ЕВРАЗ**



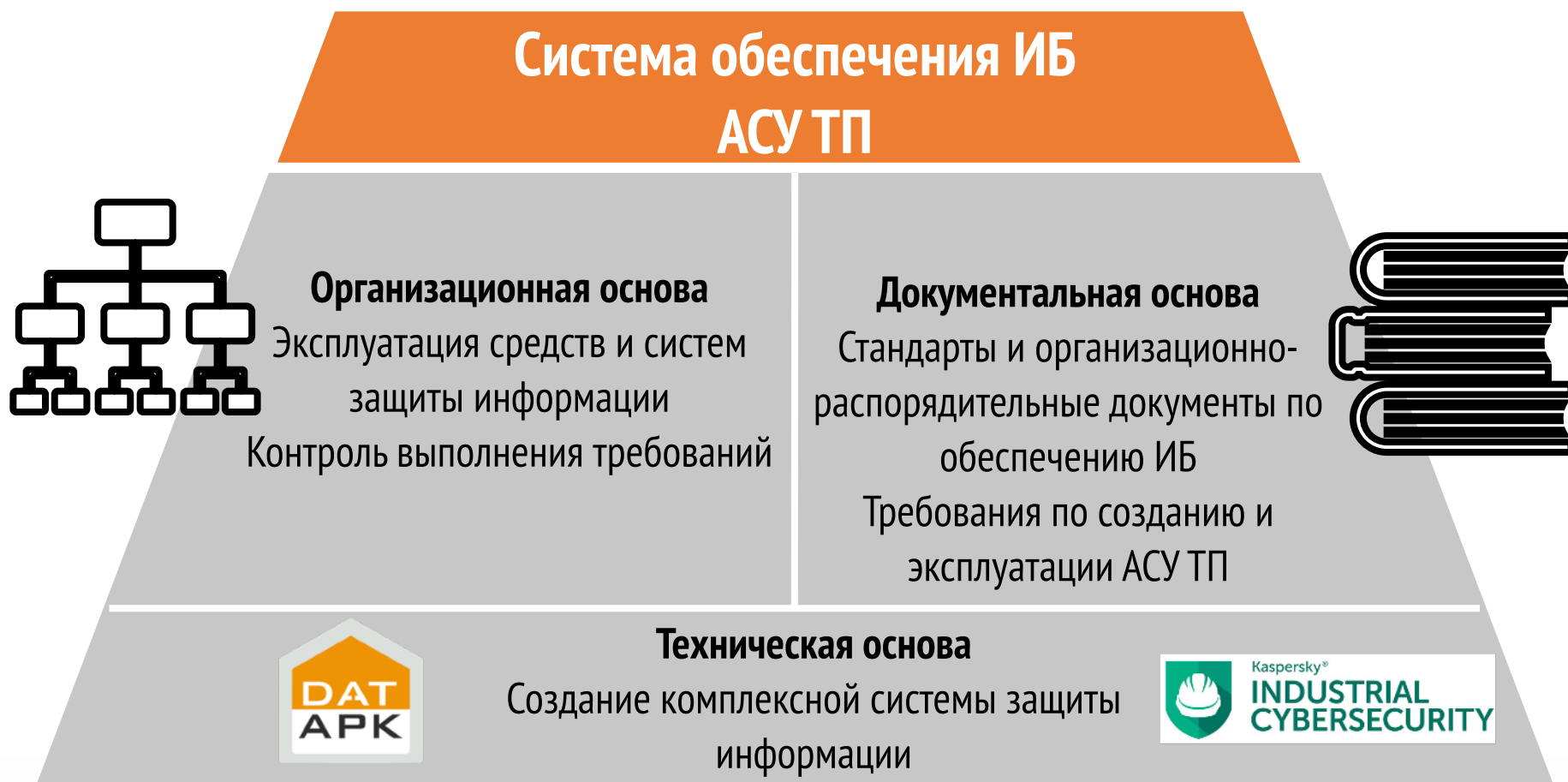
МАГНИТОГОРСКИЙ
МЕТАЛЛУРГИЧЕСКИЙ
КОМБИНАТ



РОСНЕФТЬ ЕВРОХИМ

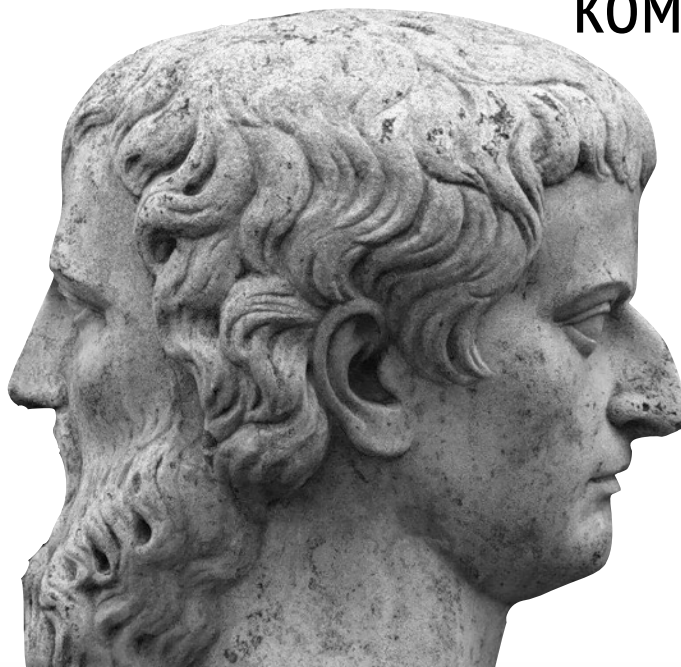


Структура системы обеспечения ИБ

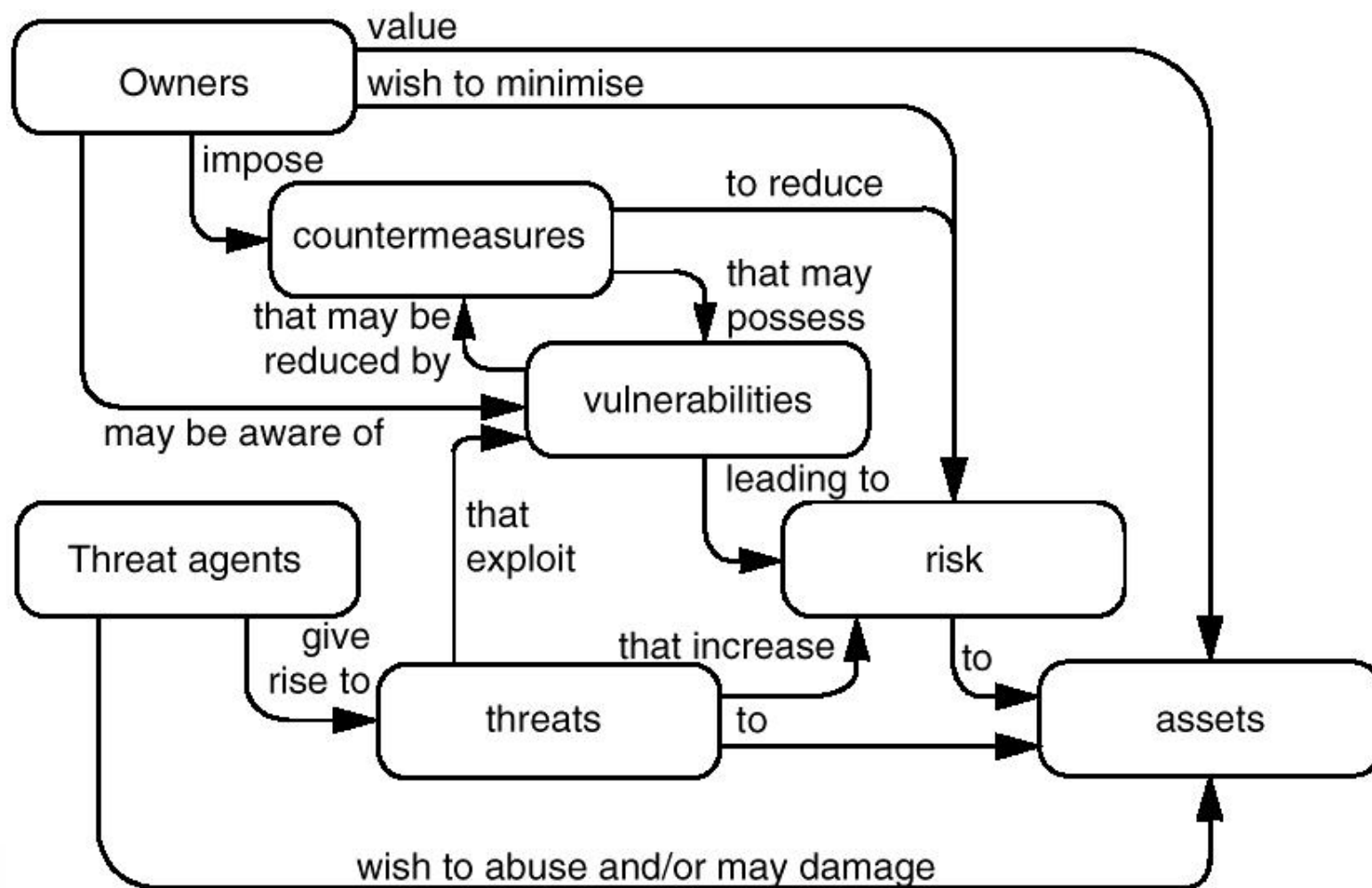


УЦСБ и ИБ АСУ ТП

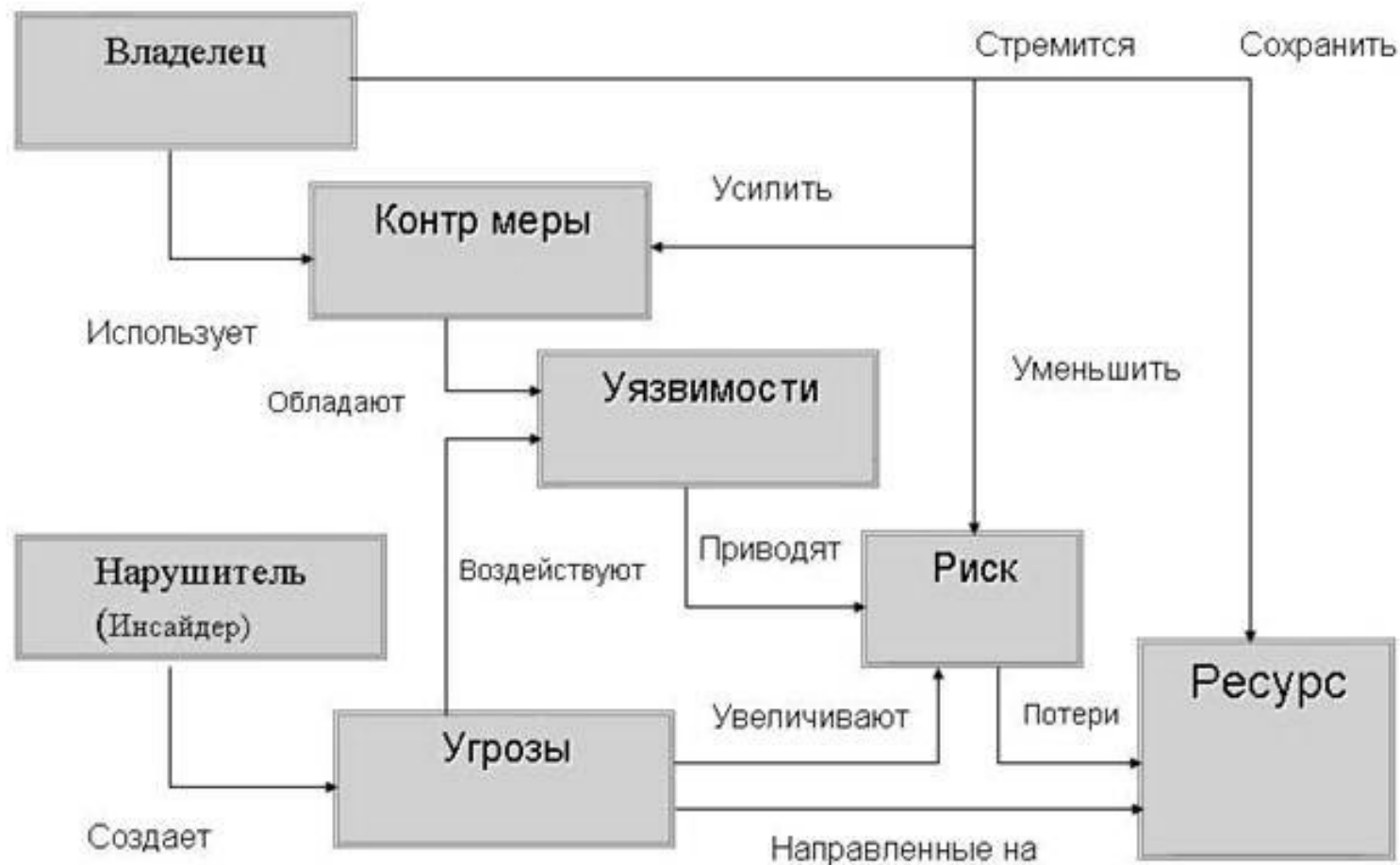
- Интегратор: аудиты, проектирование, внедрение, сопровождение.
- Разработчик/вендор: программно-аппаратный комплекс DATAPK.



ISO/IES 15408



ISO/IES 15408 (перевод)



Интересы сторон

Владелец/Owner

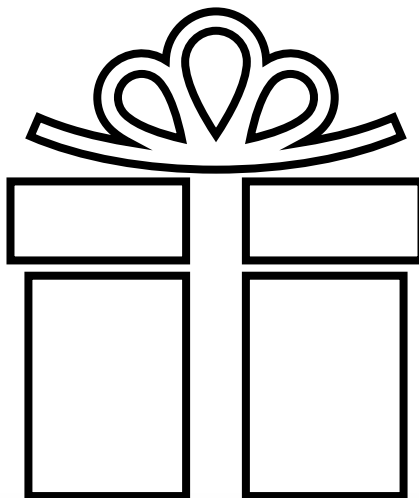
- Непрерывность бизнеса
- Экономическая эффективность
- Соблюдение требований

Нарушитель/Threat agent

- Причинение вреда бизнесу
- Получение личной выгоды
- Политические мотивы

Регулятор/Regulator

- Национальные интересы
- Отраслевые стандарты
- Контроль соблюдения



Интересы сторон

Владелец/Owner

- Непрерывность бизнеса
- Экономическая эффективность
- Соблюдение требований

Нарушитель/Threat agent

- Причинение вреда бизнесу
- Получение личной выгоды
- Политические мотивы

Регулятор/Regulator

- Национальные интересы
- Отраслевые стандарты
- Контроль соблюдения

Идеальное средство защиты для каждой из сторон

- Защищающее
- Недорогое
- Соответствующее требованиям

- Незащищающее
- Дорогое
-

- Защищающее
-
- Соответствующее требованиям

Взгляд интегратора ИБ АСУ ТП

- Проектирование
 - Какие решения выбрать?
- Внедрение/сопровождение
 - Оценка влияния?
 - Кто несёт ответственность?
 - Какие гарантии?



Проектирование ИБ АСУ ТП

- Какие решения выбрать?
- Оценка влияния на АСУ ТП?
- Одобрение производителей АСУ ТП?
- Бюджет?



Внедрение/сопровождение ИБ АСУ ТП

- Основания для модернизации/подключения?
- Как проводить приёмо-сдаточные испытания?
- Кто отвечает за эксплуатацию?
- Кто несёт ответственность?
- Какие гарантии?
- Срок гарантии?



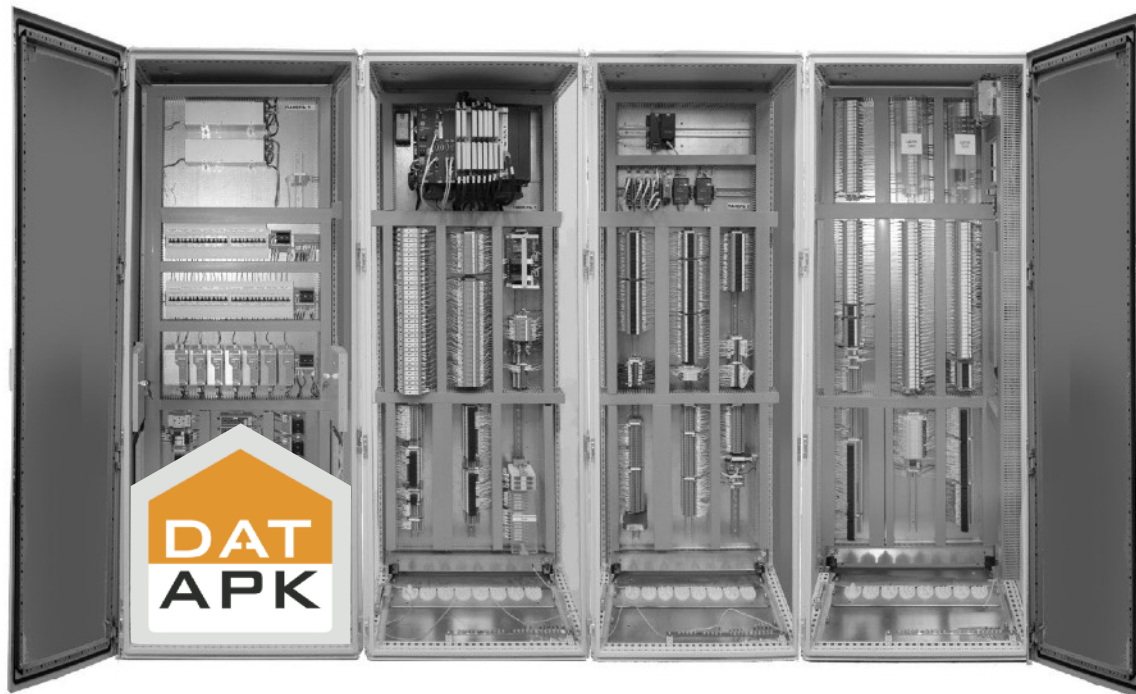
Вендор ИБ АСУ ТП

- Истории успеха и примеры внедрений? (настоящие)
- Одобрение производителей АСУ ТП?
- Оценка влияния на АСУ ТП?
- Компетенции у партнёра?
- Сертификация продукта?



Оптимальный (?) вариант

- Поставка решений по ИБ в составе самих АСУ ТП
 - ИБ - встроенный функционал
 - Единая гарантия и пр.
- НО!
 - Только для новых/
модернизируемых
систем



Техническое задание на средство защиты

Источник требований: реальный мир



Оптимальный баланс между ценой и качеством

Техническое задание на средство защиты

Источник требований: реальный мир



Оптимальный баланс между ценой и качеством

Источник требований: законодательство и стандарты

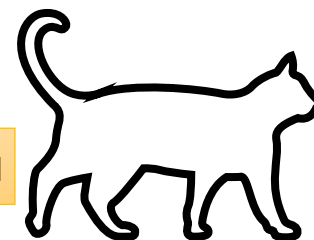


Оптимальный баланс между ценой и
соблюдением требований

Техническое задание на средство защиты

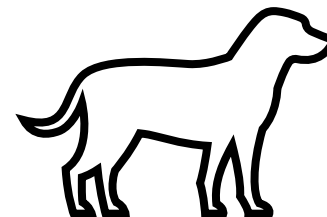
Источник требований: реальный мир

Оптимальный баланс между ценой и качеством

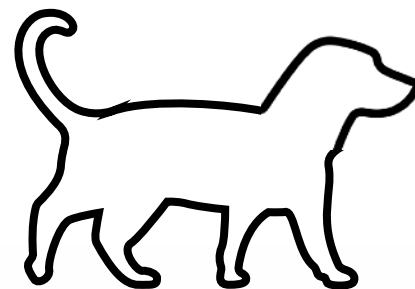


Источник требований: законодательство и стандарты

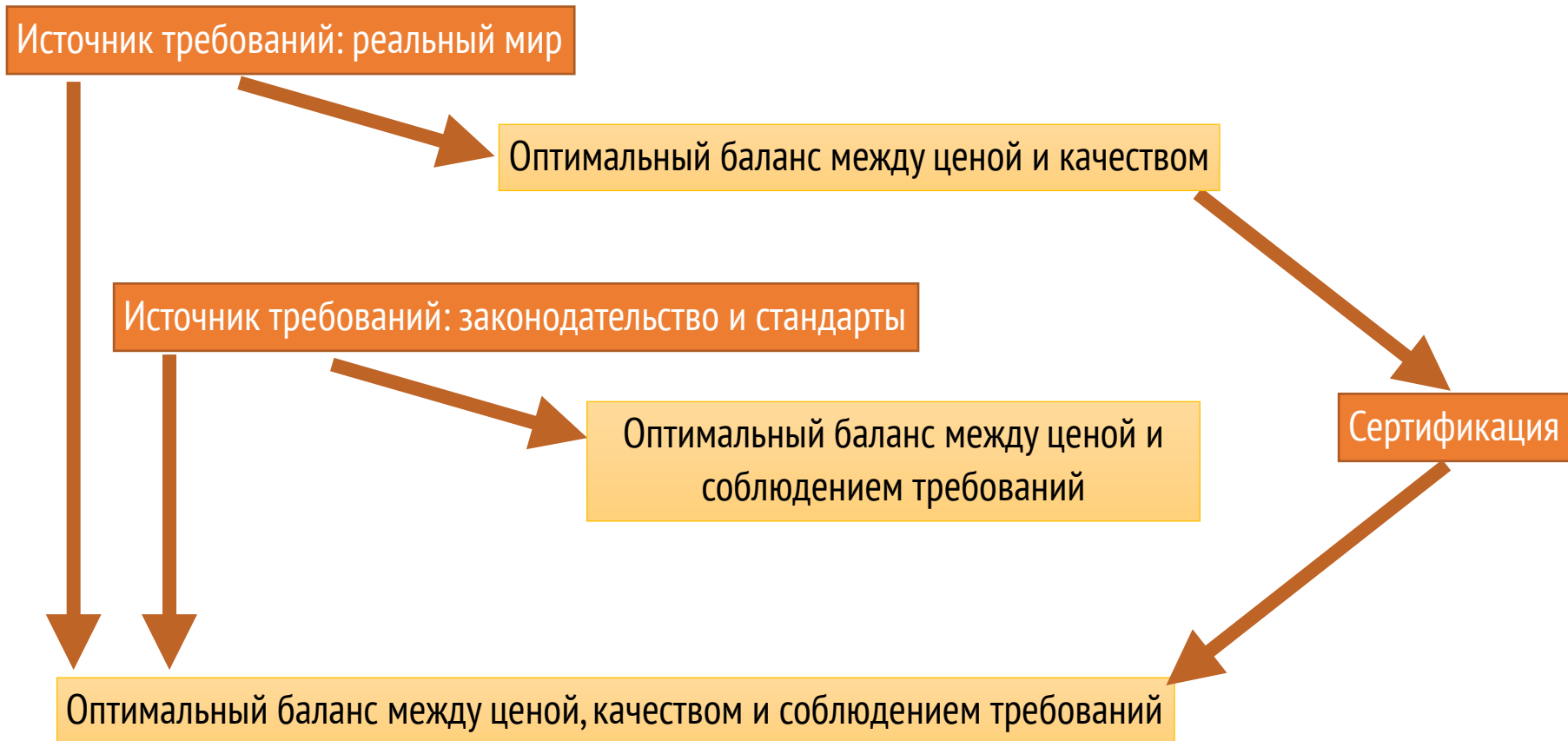
Оптимальный баланс между ценой и
соблюдением требований



Оптимальный баланс между ценой, качеством и соблюдением требований



Техническое задание на средство защиты

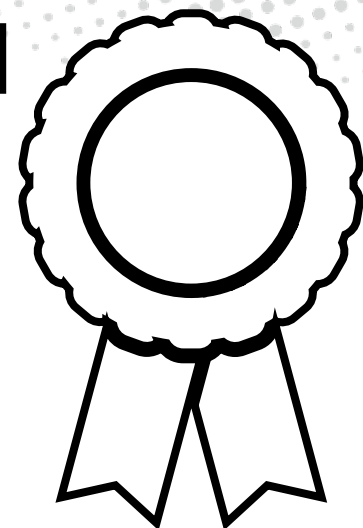


Трудности пути сертификации

- Раскрытие информации (исходного кода)
 - Охрана интеллектуальной собственности
 - Экспортные ограничения на неотечественные решения
- Фиксация исходного кода
 - Трудности с обновлениями
 - Скорость исправления уязвимостей (широкоизвестные, но необновляемые - мечта злоумышленника)

Сертифицированные решения для АСУ ТП

- Межсетевые экраны (отечественные и не только)
- Однонаправленные шлюзы/диоды
- Антивирусы (**KICS for Nodes**)
- Системы обнаружения атак/вторжений (**KICS for Nets**)
- Программный комплекс оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности производственно-технологических комплексов «**DATAPK**»
- ...



Основные функции DATAPK

- Ведение каталога компонентов АСУ ТП, выявление изменений в их составе
- Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
- Контроль и управление конфигурациями компонентов АСУ ТП
- Выявление уязвимостей, контроль защищённости компонентов АСУ ТП
- Анализ сетевых потоков и обнаружение компьютерных атак и аномалий трафика
- Контроль соответствия требованиям по обеспечению ИБ



Сертификат ФСТЭК
№ 3731 от 12.04.17
(до 12.04.20)



Безопасность КИИ 187-ФЗ и RUSCADASEC



- Обсуждение вопросов, связанных с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности КИИ»
 - Telegram-чат КИИ 187-ФЗ <https://t.me/kii187fz>
 - группа Facebook <https://facebook.com/groups/kii187fz>
 - группа ВКонтакте <https://vk.com/kii187fz>
 - Twitter <https://twitter.com/kii187fz>



- RUSCADASEC - сообщество специалистов по Кибербезопасности АСУ ТП
 - Группа в Telegram <https://t.me/RuScadaSec>
 - Канал новостей <https://t.me/RuScadaSecNews>
 - Facebook <https://www.facebook.com/groups/RusCyberSec>
 - Twitter <https://twitter.com/RUSCADASEC>
 - Сайт <https://www.ruscadasec.ru/>

Спасибо! Вопросы?



Алексей Комаров

Менеджер по развитию решений
Уральский Центр Систем Безопасности



akomarov@USSC.ru
<https://ZLONOV.ru>

