Архитектура безопасности информационных систем в электроэнергетике

Павел Васильевич Литвинов,
начальник аналитического отдела

«Автоматизированные системы управления в распределительных электрических сетях России: достижения и перспективы развития с учетом международного опыта СИГРЭ»

Июнь, 2015

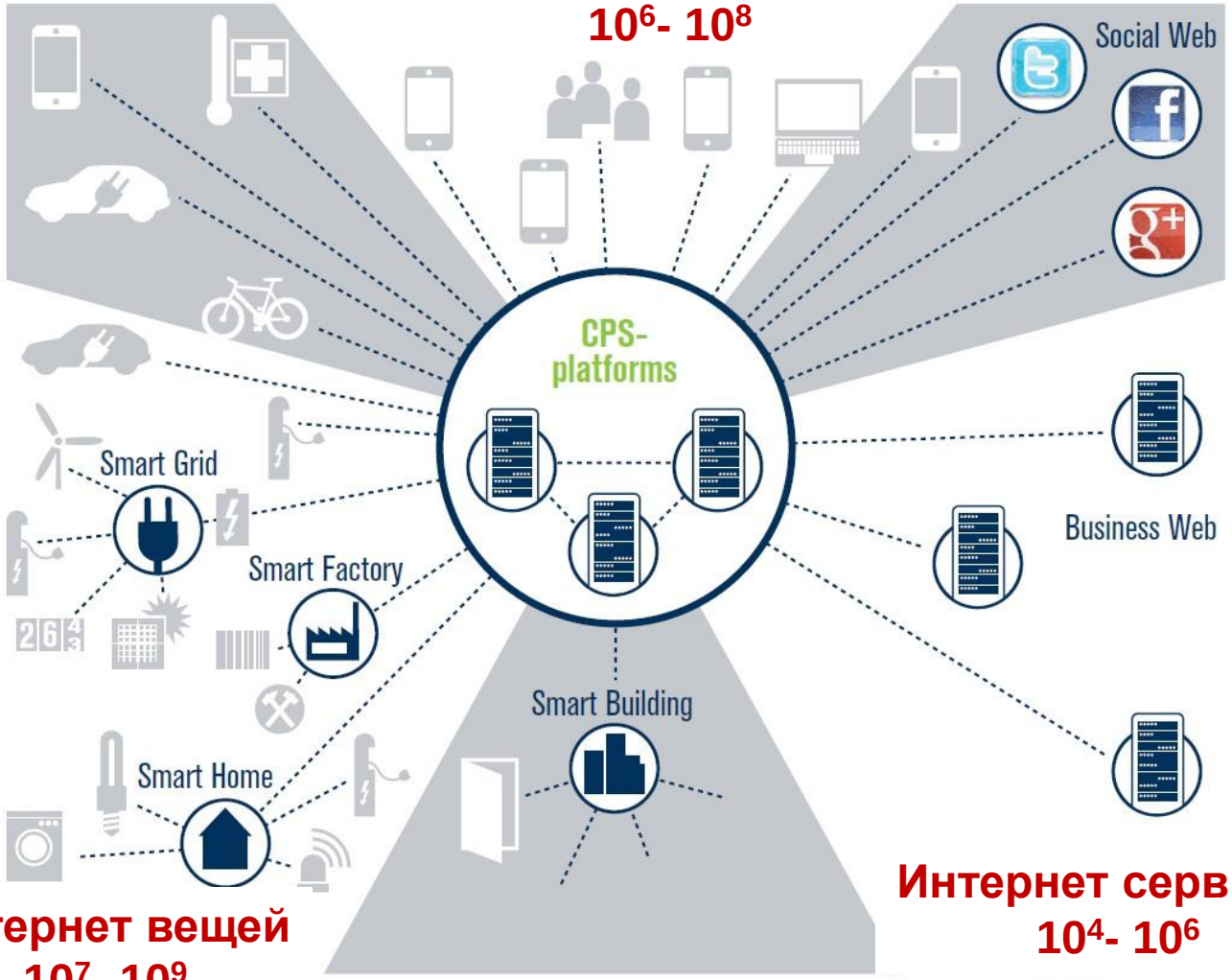
Новые явления

- Конвергенция IT + OT *F(Cloud, BigData(inmemoryDB), IoT, IA, RTI) = **CPS (кибер-физические системы*)**
- IT системы перестают быть информационно-справочными т.е. вспомогательными
- У нас уже 17+ регуляторов ИБ (**ФСБ**, **ФСТЭК**, СВР, МинОбороны, ФСО, **Минкомсвязь**, Роскомнадзор, **МВД**, Банк России, Совет Безопасности, **Минэнерго**, Минэкономразвития, Администрация Президента, **Ростехрегулирование**, Минтруд, Рособразование, …)
- Расширяется спектр и сложность тагетированных или APT (Advanced Persistent Threats) атак
- Использование продвинутых технических средств защиты все чаще сосуществует с наличием элементарных ошибок и просчетов
  (атака будет на самое слабое место!)
- Поисковик уязвимостей SHODAN с 2009 г. работает и есть и другие ☹
- ФСТЭК открыл «Банк данных угроз безопасности информации»

О месте Cyber-physical system (CPS)

«Умные»:

- **Устройства**
- **Сети**
- **Дома**
- **Города**
- **Материалы**
- **Фабрики**
- **…**



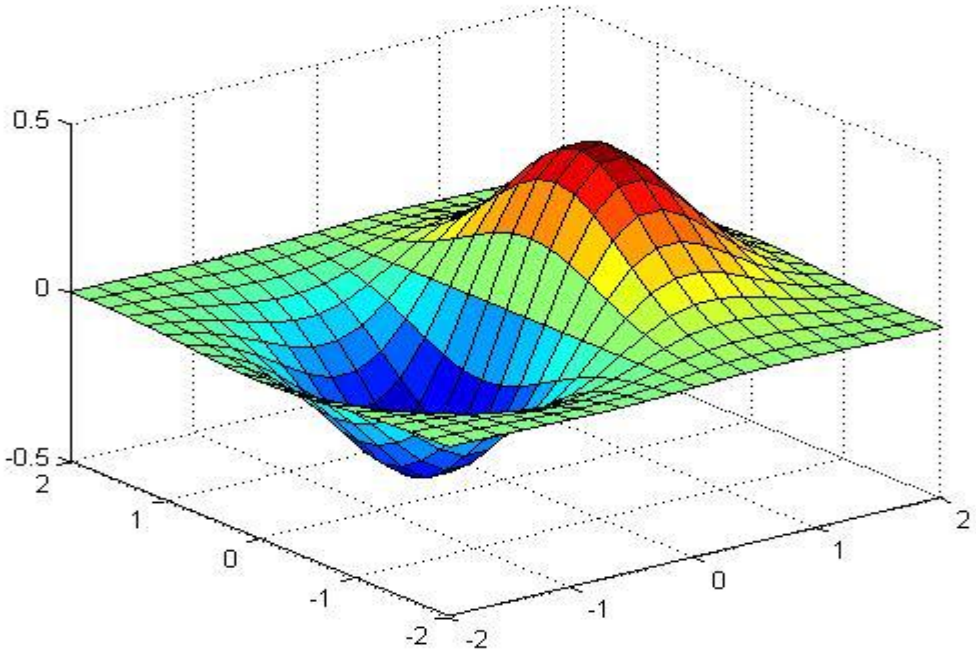
Хорошие новости

МЭК 61850 устоял ☺ в соревновании хакеров

На ПХД цифровую подстанцию не взломали!

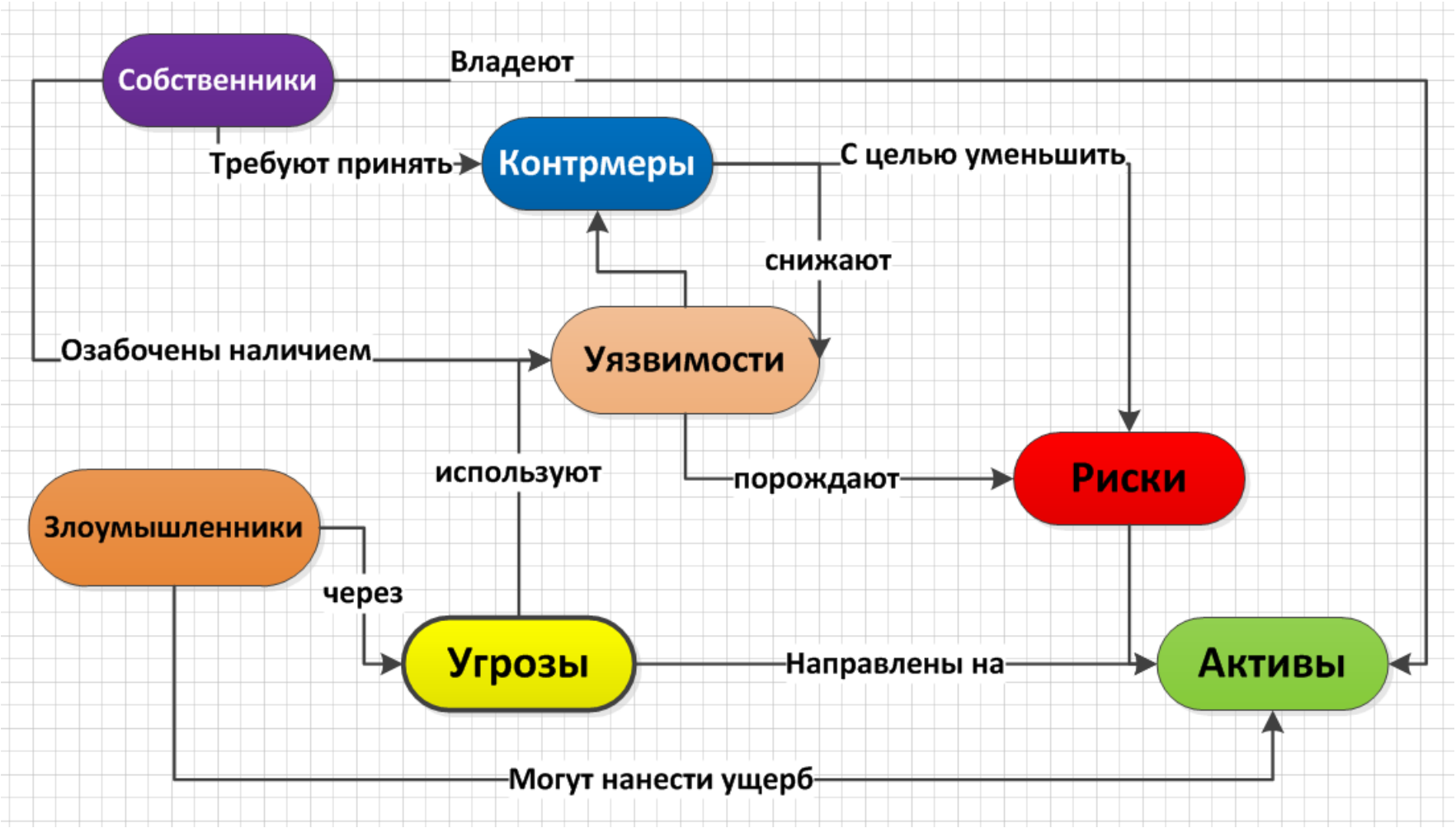
Тезисы

- Проблема отсутствия адекватной защиты современным киберугрозам существует и осознается
- Принимающиеся меры по защите фрагментарны и пока не адекватны уровню угроз (потенциальному ущербу, вероятности и т.п.)
- Регуляторов в области ИБ много, но их документы не гармонизированы и график их появления не синхронизован
- Российская нормативная база продолжает расти и совершенствоваться, но не хватает документов «прямого действия» с учетом отраслевой специфики
- Ситуация меняется (ухудшается) быстрее, чем мы на нее реагируем

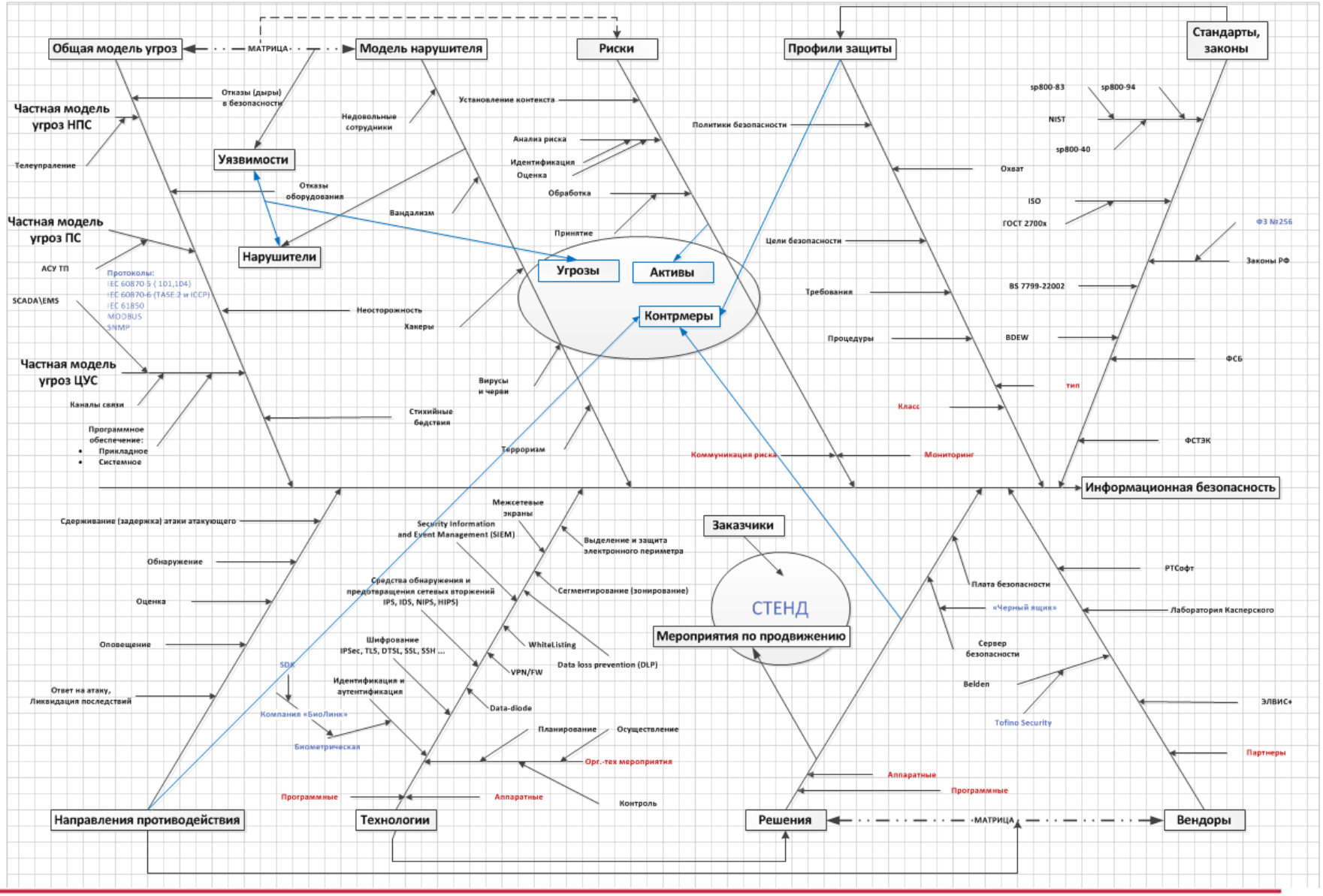


АРХИТЕКТУРА

Концептуальная модель архитектуры безопасности



Онтологическая модель



Сопоставление угроз мерам защиты

IAS

Файл Правка Вид Данные Сервис Окна ?

ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ (ГОСТ Р 51275-2006)

Список Дерево Таблица

- ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ (ГОСТ Р 51275-2006)
  - Объективные
    - Внутренние факторы
      - Передача сигналов
      - Излучения сигналов, функционально присущие техническим средствам (ТС)
      - Побочные электромагнитные излучения
      - Паразитное электромагнитное излучение
      - Наводка
      - Наличие акустоэлектрических преобразователей в элементах ТС ОИ
      - Дефекты, сбои и отказы, аварии ТС и систем ОИ
      - Дефекты, сбои и отказы программного обеспечения ОИ
    - Внешние факторы
      - Явления техногенного характера
      - Природные явления, стихийные бедствия
  - Субъективные
    - Внутренние факторы
      - Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:
      - Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, пут
      - Несанкционированный доступ к информации путем:
        - подключения к техническим средствам и системам ОИ;
        - использования закладочных средств [устройств];
        - использования программного обеспечения технических средств ОИ через:
          - маскировку под зарегистрированного пользователя;
          - дефекты и уязвимости программного обеспечения ОИ;
          - внесение программных закладок;
          - **применение вирусов или другого вредоносного программного**
        - хищения носителя защищаемой информации;
        - нарушения функционирования ТС обработки информации.
      - Недостатки организационного обеспечения защиты информации при:
      - Ошибки обслуживающего персонала ОИ при:
    - Внешние факторы
      - Доступ к защищаемой информации с применением технических средств:
        - разведки:
        - съема информации.
      - Несанкционированный доступ к защищаемой информации путем:
      - Блокирование доступа к защищаемой информации путем перегрузки технических средств обработк
      - Действия криминальных групп и отдельных преступных субъектов:
        - диверсия в отношении ОИ;
        - диверсия в отношении элементов ОИ.
      - Искажение, уничтожение или блокирование информации с применением технических средств путем
        - преднамеренного силового электромагнитного воздействия:
        - преднамеренного силового воздействия различной физической природы;
        - использования программных или программно-аппаратных средств при осуществлении:
        - воздействия программными средствами в комплексе с преднамеренным силовым электромагн

ГОСТ Р 51275-2006

Защита информации

ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

Перечень объективных и субъективных факторов воздействующих на безопасность защищаемой информации объекта информатизации (ОИ)

Состав мер защиты информации

Список Дерево Таблица

- Состав мер защиты информации
  - I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
  - II. Управление доступом субъектов доступа к объектам доступа (УПД)
  - III. Ограничение программной среды (ОПС)
  - IV. Защита машинных носителей информации (ЗНИ)
  - V. Регистрация событий безопасности (РСБ)
  - VI. Антивирусная защита (АВЗ)
    - Разработка правил и процедур (политик) антивирусной защиты
    - **Реализация антивирусной защиты**
    - Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
  - VII. Обнаружение вторжений (СОВ)
  - VIII. Контроль (анализ) защищенности информации (АНЗ)
    - Разработка правил и процедур (политик) контроля (анализа) защищенности
    - Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей
    - Контроль установки обновлений программного обеспечения, включая обновление программн
    - Контроль работоспособности, параметров настройки и правильности функционирования про
    - Контроль состава технических средств, программного обеспечения и средств защиты информ
    - Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных
  - IX. Обеспечение целостности (ОЦЛ)
  - X. Обеспечение доступности (ОДТ)
  - XI. Защита среды виртуализации (ЗСВ)
  - XII. Защита технических средств (ЗТС)
    - Разработка правил и процедур (политик) защиты технических средств
    - Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим
    - Организация контролируемой зоны, в пределах которой постоянно размещаются стационарны
    - Размещение устройств вывода (отображения) информации, исключающее ее несанкциониров
    - Защита от внешних воздействий (воздействий окружающей среды, нестабильности электросн
  - XIII. Защита автоматизированной системы и ее компонентов (ЗИС)
  - XIV. Обеспечение безопасной разработки прикладного (специального) программного обеспечен
  - XV. Управление обновлениями программного обеспечения (ОПО)
    - Разработка правил и процедур (политик) управления обновлениями программного обеспечен
    - Получение обновлений программного обеспечения от разработчика или уполномоченного и
    - Тестирование обновлений программного обеспечения до его установки на макете или в тест
    - Централизованная установка обновлений программного обеспечения
  - XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)
    - Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты
    - Определение лиц, ответственных за планирование и контроль мероприятий по обеспечению
    - Разработка, утверждение и актуализация (обновление) плана мероприятий по обеспечению
    - Контроль выполнения мероприятий по обеспечению защиты информации в автоматизирован
  - XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
    - Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденны
    - Разработка плана действий в случае возникновения нештатных (непредвиденных) ситуаций
    - Обучение и отработка действий пользователей в случае возникновения нештатных (непредв
    - Создание альтернативных мест хранения и обработки информации в случае возникновения н
    - Резервирование программного обеспечения, технических средств, каналов передачи данных
    - Обеспечение возможности восстановления автоматизированных систем управления и (или) е
  - XVIII. Информирование и обучение пользователей (ИПО)
    - Разработка правил и процедур (политик) информирования и обучения пользователей
    - Информирование пользователей об угрозах безопасности информации, о правилах эксплуат
    - Обучение пользователей правилам эксплуатации системы защиты автоматизированной сист

2> RTSOFT tdrts - Open litvinov_pv (192.168.202.254) 46Мб.

ЖЦ программ по обеспечению ИБ

Политика

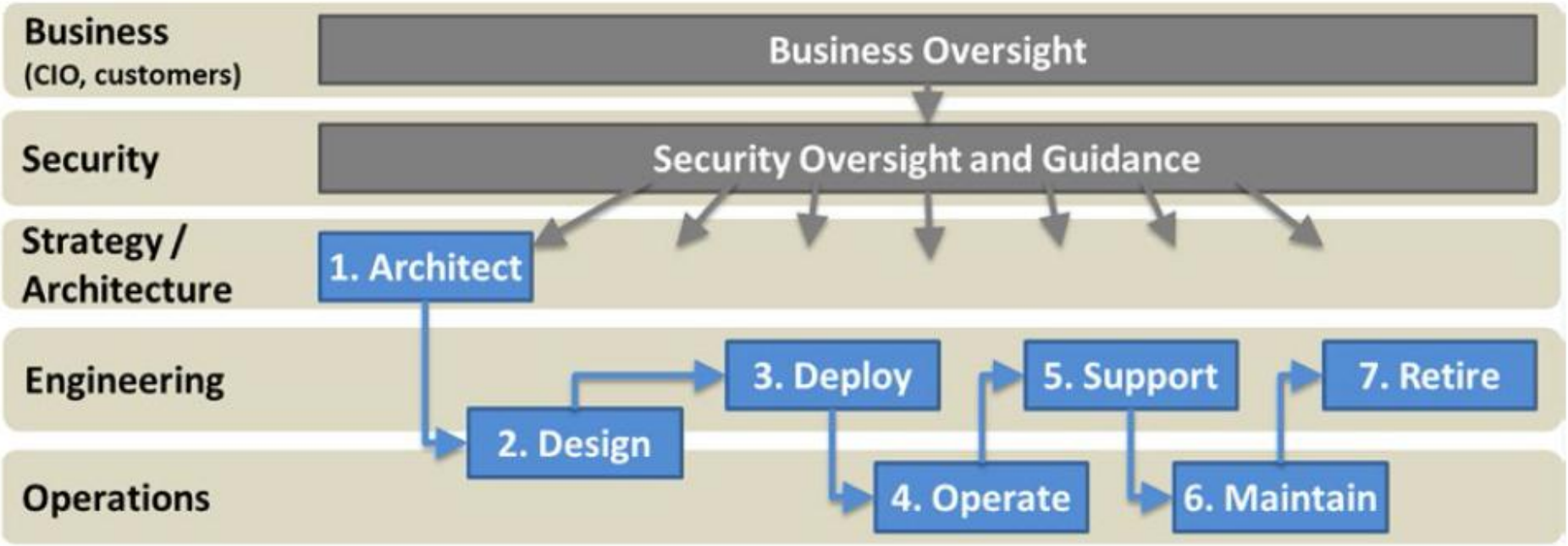
- контроль

План

- Люди
- Бюджет
- Технологии

Выполнение

- Стратегия
- **Архитектура**
- Работы



Принципы проектирования архитектуры ИБ

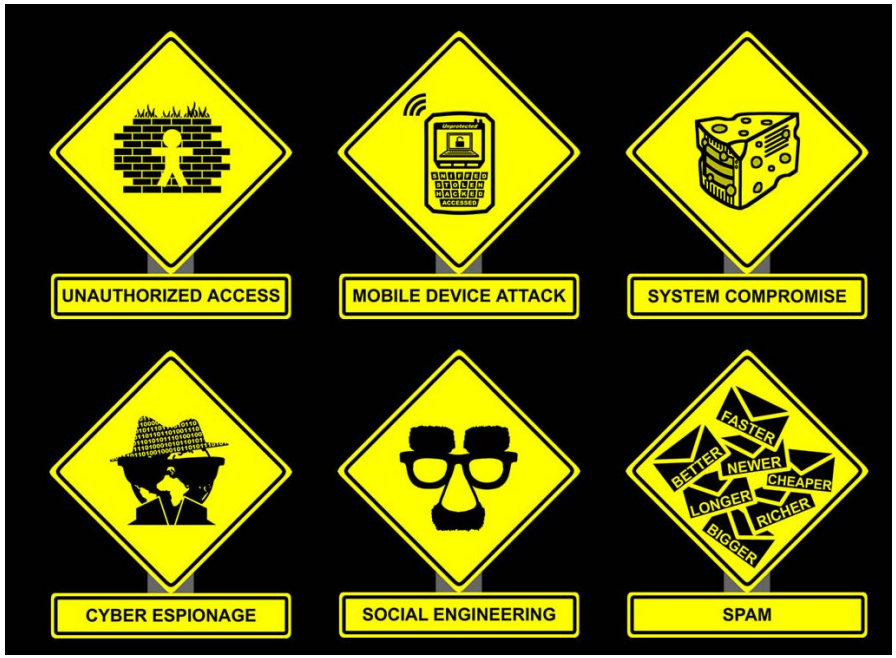
- Адекватность существующей (текущей) модели угроз – экономическая целесообразность
- Архитектурно заложенный «запас прочности» под будущие угрозы – защита инвестиций
- Переоценка роли дублирования (многократного резервирования), и его влияния на надежность в случае кибератак
- «Эшелонированность обороны», отступление на заранее подготовленные позиции: заранее определенная допустимая деградация части функций
- Распределенность защитных мер и их ассиметричная реализация
- Правильный учет «человеческого фактора»

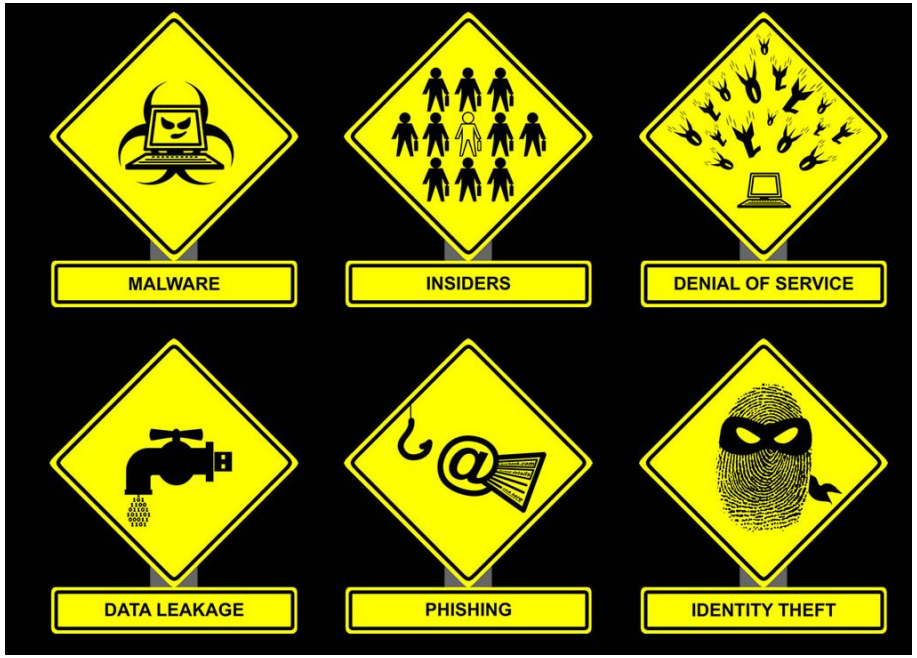
Человеческий фактор

берем за основу методологию TQM и создаем
на этой основе Total Security Management (**TSM**).
Вместо «кружков качества» будут «группы безопасности» и т.п.

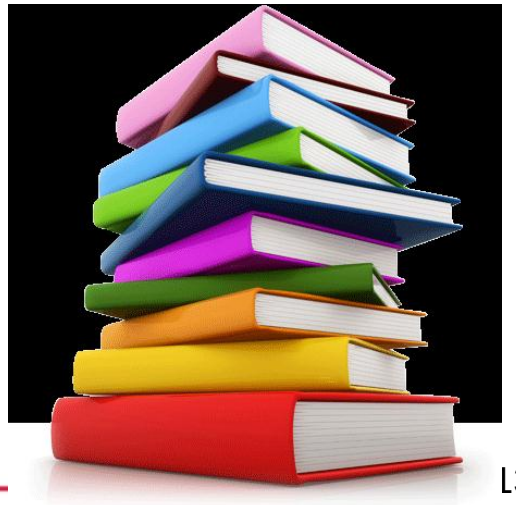
- Популяризация знаний ИБ, регулярное обучение – (хороший старт «игра» ЛК)
- Вовлеченность и стимулирование «правильного поведения» через идею TSM
- Включение собственного персонала в модель нарушителя – увы, «враг не только снаружи»
- Тройной контроль и запрет нежелательного поведения*:
  - через распорядительную документацию;
  - объективный контроль исполнения;
  - использование программно-аппаратных средств.

Например. Запрет использования 3G модемов и Wi-Fi контролируется сканерами, а в серверных помещениях «дублируется» глушителями сигнала.





НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ VS УГРОЗЫ

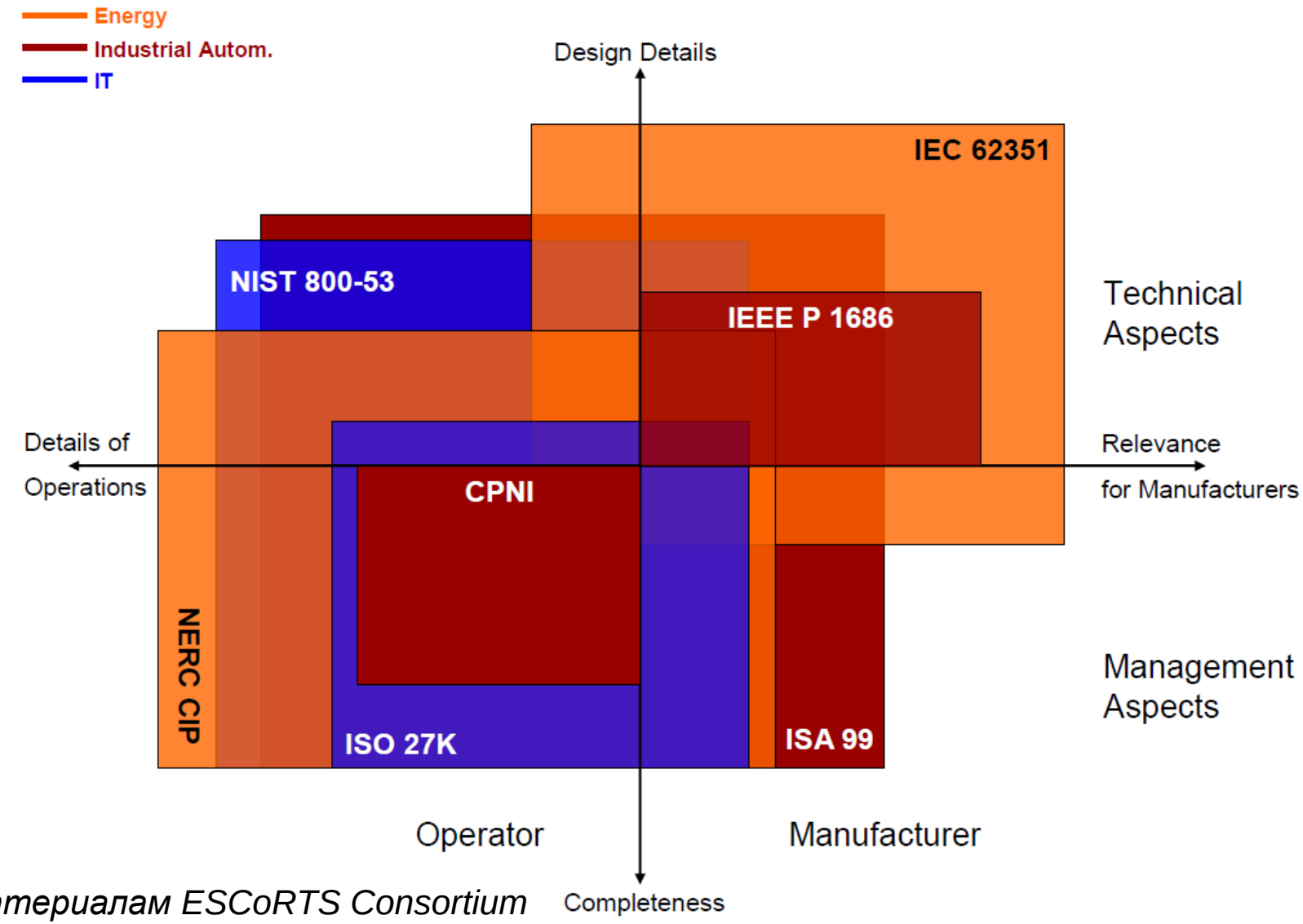


Стандарты и мировой опыт

- **NERC-CIP** (США и Азия);
- **CPNI** (Великобритания);
- **BDEW White Paper** (Германия, Европа);
- **ISA-62443 (International Society of Automation);**
- **IEC 62351**
- **NIST Special Publications 800 series** (США);
- **ISO 27000 series** (международные)
- **Ausgrid** (корпоративный, Австралия)

– Это только источники!
Каждый источник содержит десятки документов.

Соотношения между стандартами



** По материалам ESCoRTS Consortium*

Статья 217.1. УК РФ

- Статья 217.1. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса

(введена Федеральным законом от 21.07.2011 N 257-ФЗ)

- 1. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса, если это деяние повлекло по неосторожности причинение тяжкого вреда здоровью человека или причинение крупного ущерба, - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо **ограничением свободы на срок до трех лет**, либо лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
- 2. То же деяние, повлекшее по неосторожности смерть человека, - наказывается лишением свободы на срок **до пяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
- 3. Деяние, предусмотренное частью первой настоящей статьи, повлекшее по неосторожности смерть двух или более лиц, - наказывается лишением свободы на срок до **семи лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Примечание. Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает один миллион рублей.

Субъект специальный - **руководитель объекта топливно-энергетического комплекса**, на котором лежит обязанность соблюдать правила, которые являются обязательными для обеспечения безопасности объектов топливно-энергетического комплекса и его антитеррористической защищенности.

Статья 217.2. УК РФ

Заведомо ложное заключение экспертизы промышленной безопасности

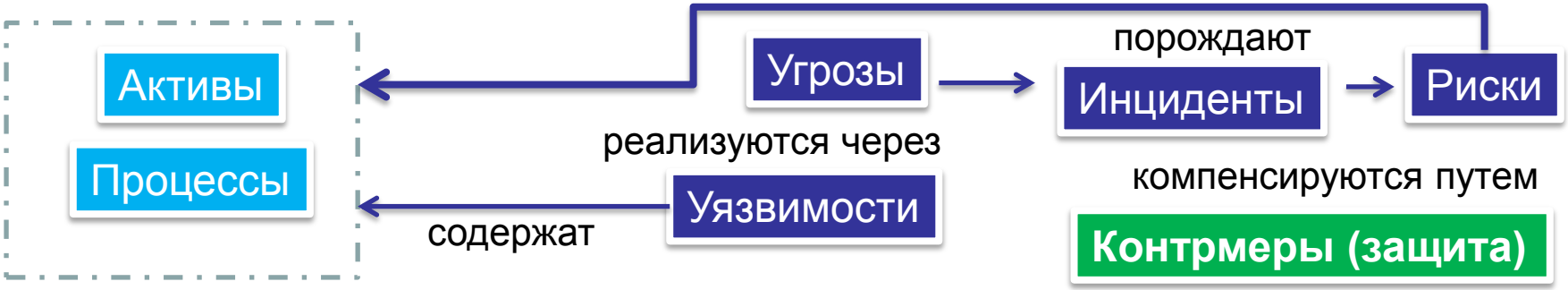
(введена Федеральным законом от 02.07.2013 N 186-ФЗ)

- 1. Дача экспертом в области промышленной безопасности заведомо ложного заключения экспертизы промышленной безопасности, если это могло повлечь смерть человека либо повлекло причинение крупного ущерба, - наказывается штрафом в размере до **двухсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до шести месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо без такового.
- 2. То же деяние, повлекшее по неосторожности причинение тяжкого вреда здоровью или смерть человека, - наказывается лишением свободы на срок **до пяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
- 3. Деяние, предусмотренное частью первой настоящей статьи, повлекшее по неосторожности смерть двух и более лиц, - наказывается лишением свободы на срок до **семи лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от одного года до трех лет или без такового.

БЕЗОПАСНОСТЬ КАК АКТИВ

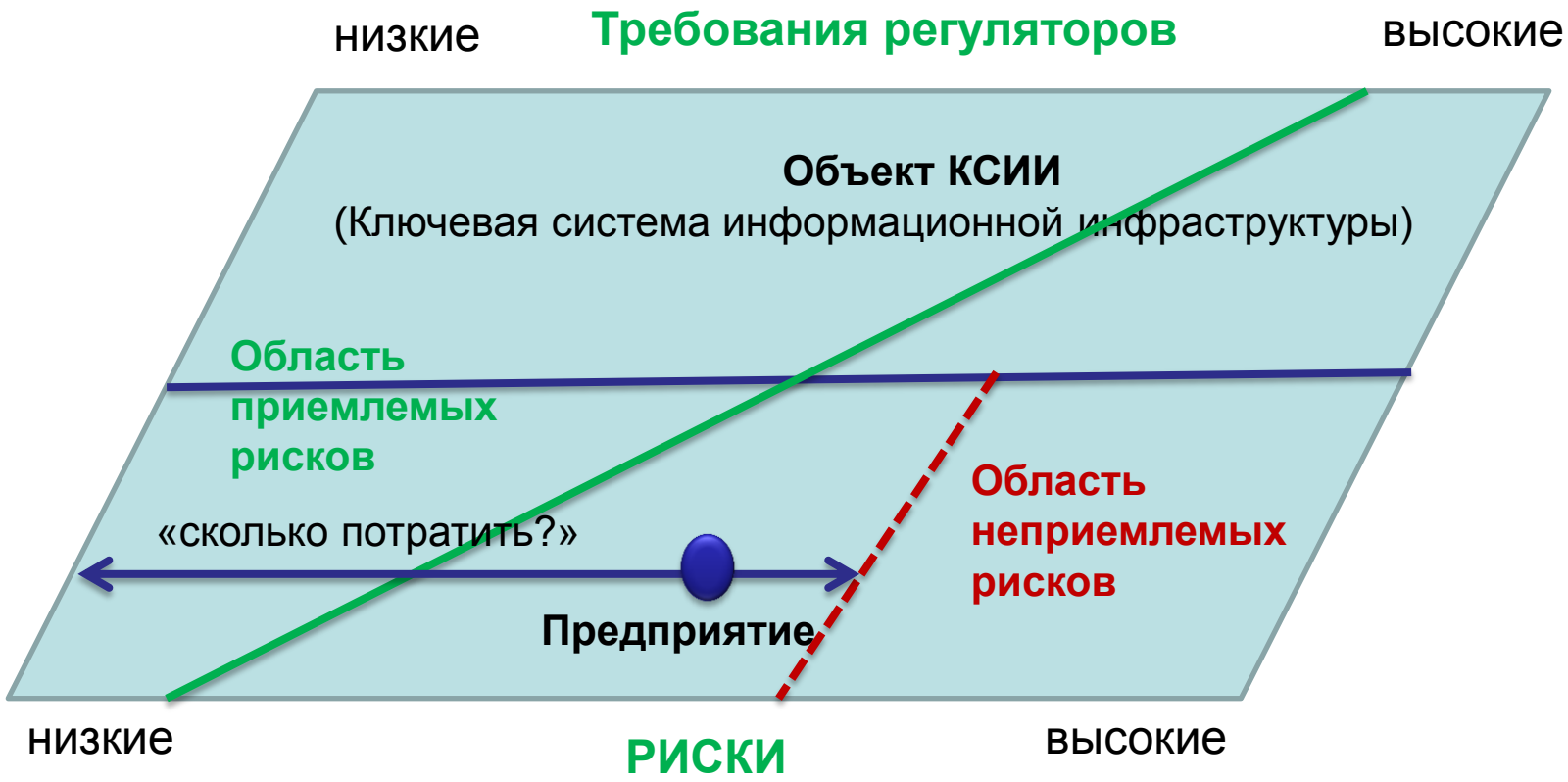
Вызовы

- Классические способы обеспечения надежности путем резервирования не эффективны против кибер-атак;
- Импортозамещение;
- Мероприятия по обеспечению ИБ могут влиять на нормальное функционирование системы;
- Нежелательность (невозможность) проведения тестов на проникновение;
- Необходимость соблюдать режим ДСП и разумную конфиденциальность.



Сколько тратить на безопасность?

- Регуляторы – **ФСТЭК**, **Ростехнадзор**, **ФСБ, МО**, **МВД, Минюст**
- Безопасность – **информационная**, **технологическая**, **физическая**, **государственная**, **правовая**

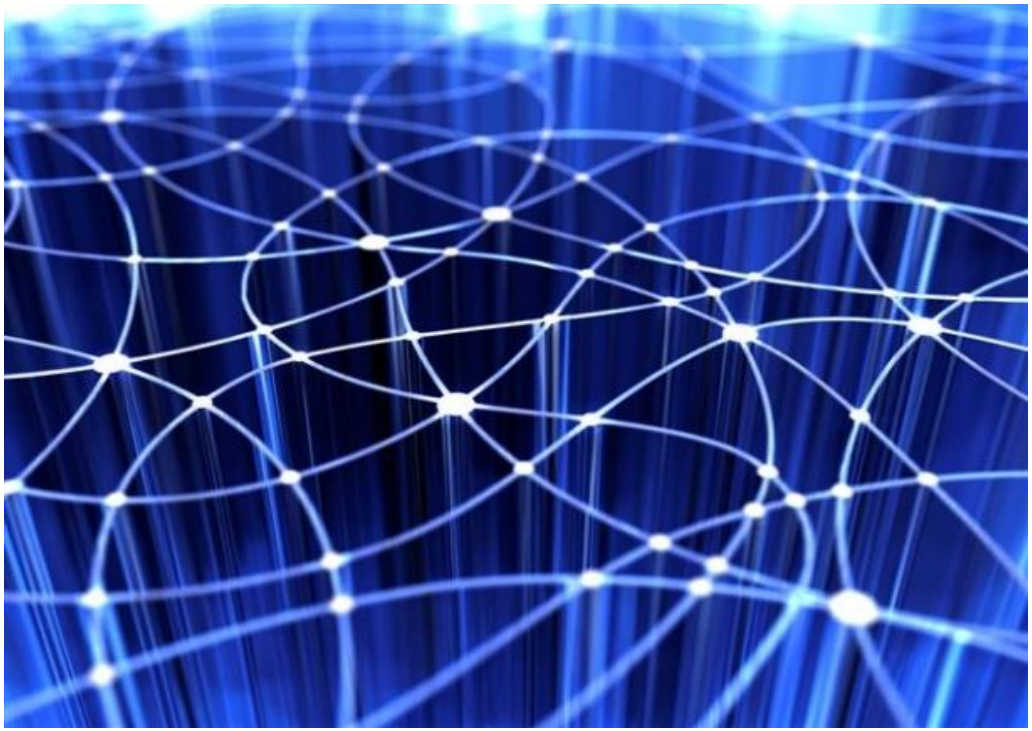


Вкладывать средства в безопасность – выгодно, чтобы не попасть в зону неприемлемых рисков!

Забота о «зоопарке»

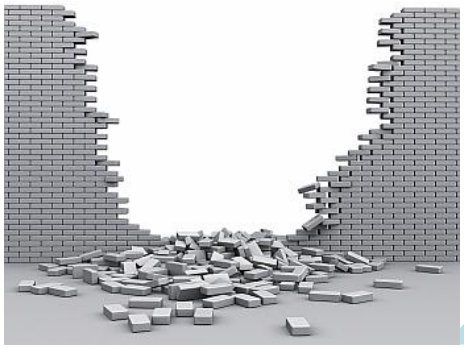
- АСУ ТП, РЗА, ПА
- ЦУС (SCADA, DMS, EMS)
- АИИС КУЭ
- СККЭ
- Оперативно-ситуационный центр
- …

- Защита инвестиций
  (у каждого решения есть свой жизненный цикл, сроки окупаемости и оно тщательно выбиралось в свое время)
- Непрерывность операционной деятельности
- Ассиметричные, разнородные, частично дублирующие друг друга и слабо связанные решения – затрудняют выполнение и потенциально способны уменьшить последствия кибератак.



ПРАКТИКА

Декомпозиция задачи импортозамещения



Сейчас

Санкции потеря поставок или поддержки

Ждать

Завтра

Безопасность

Не доверяем

(кибер-безопасность)

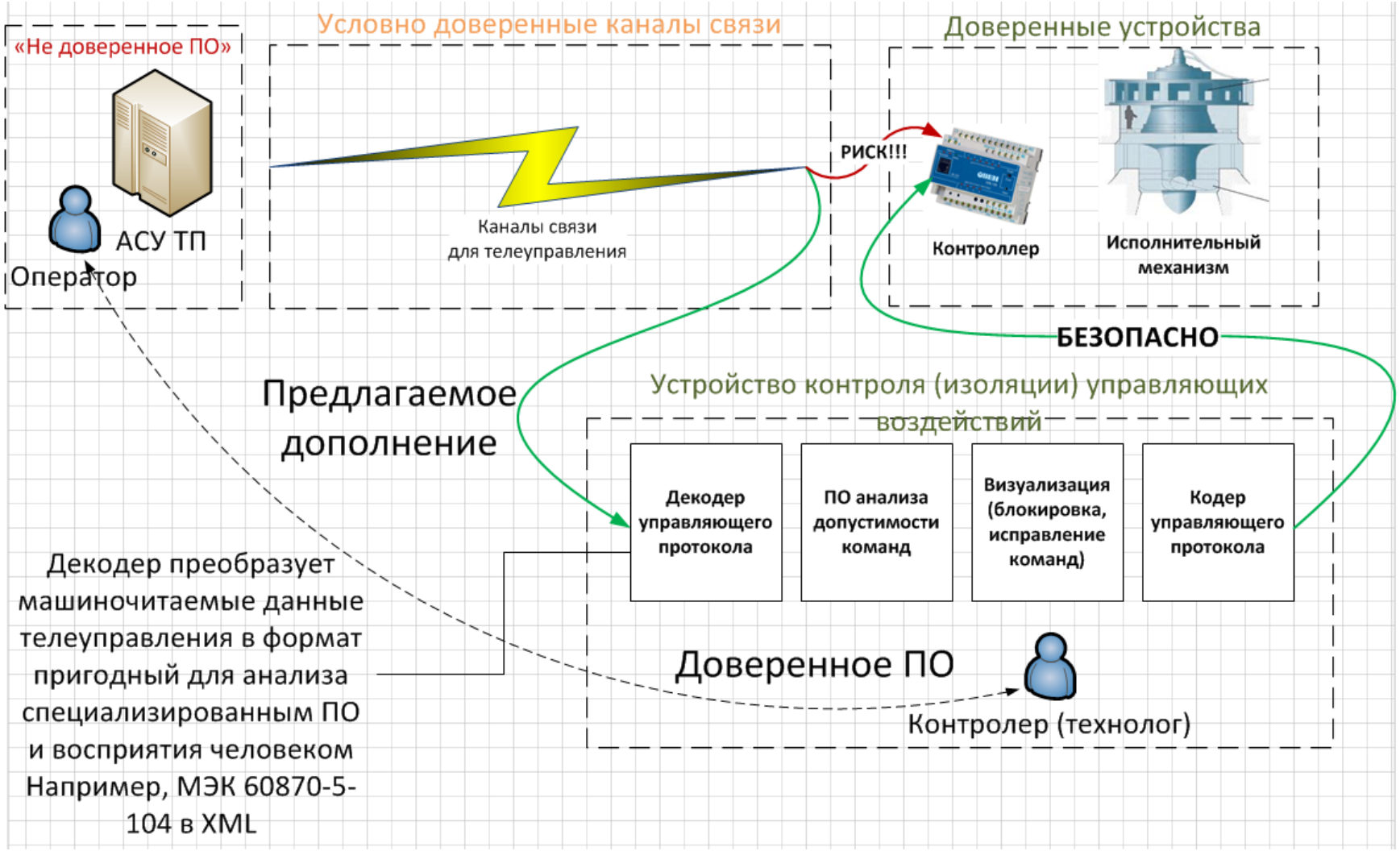
Всегда

Экономика

Не выгодно

Конкурентное решение

Концепция доверенного телеуправления



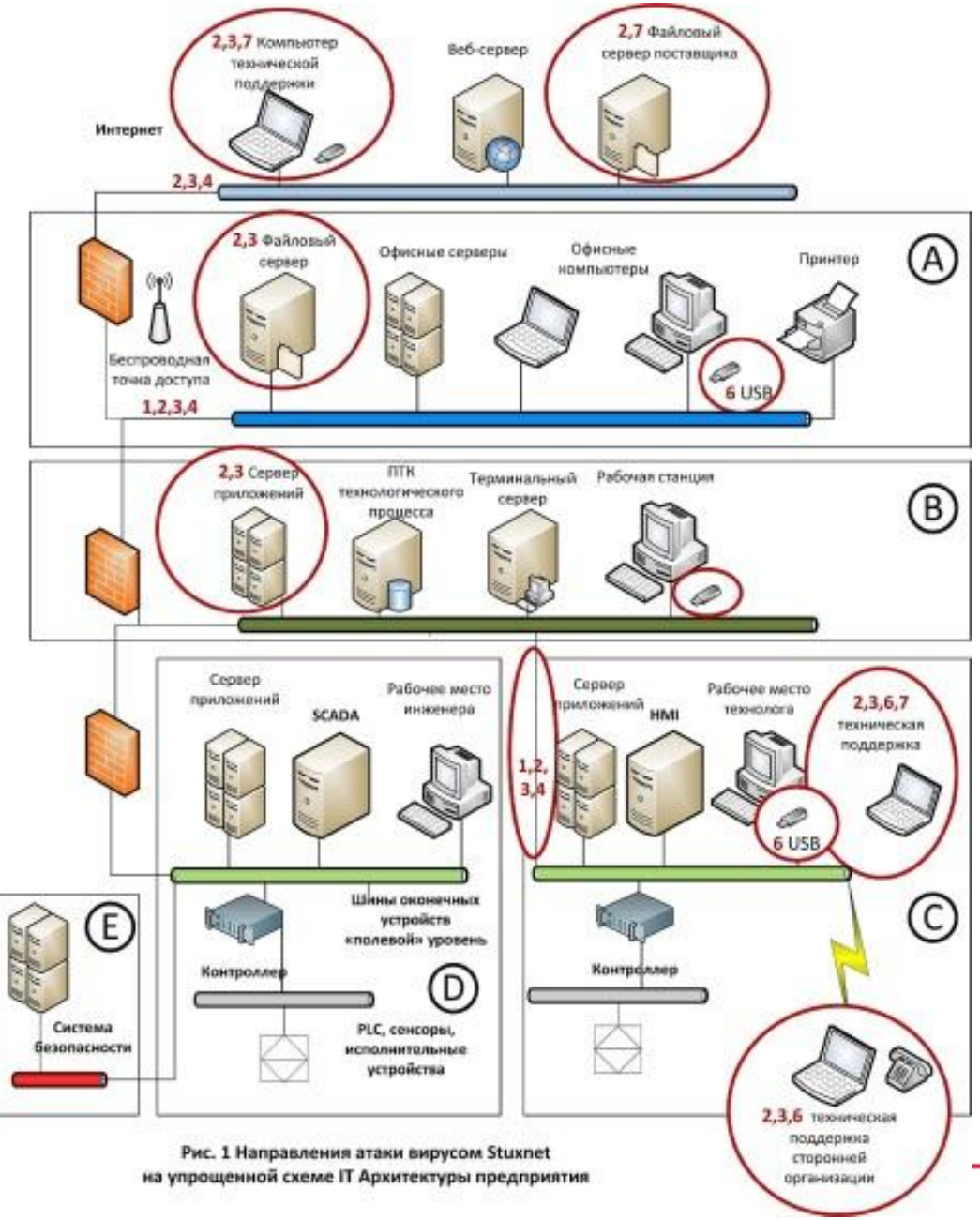


Рис. 1 Направления атаки вирусом Stuxnet на упрощенной схеме IT Архитектуры предприятия

Сегментация технологической сети

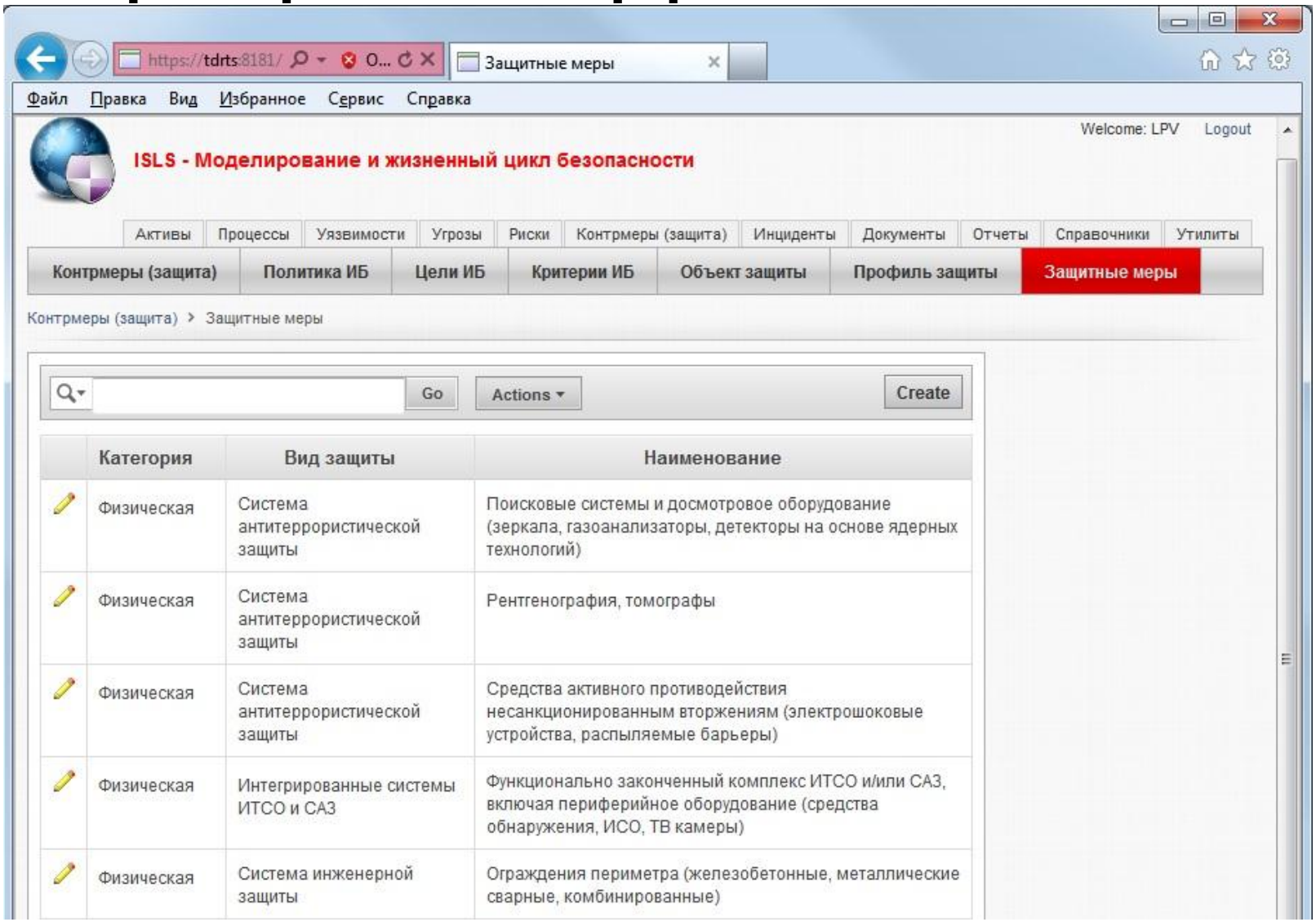
- WAN
- DMZ
- «Офисная»
- Технологическая
- Объектовая х кол-во
- Безопасности

+

- Поставщик ПО
- Техническая поддержка, обновления
- и т.п.

Горизонтально + вертикально!

Пример web-интерфейса пользователя



	Категория	Вид защиты	Наименование
	Физическая	Система антитеррористической защиты	Поисковые системы и досмотровое оборудование (зеркала, газоанализаторы, детекторы на основе ядерных технологий)
	Физическая	Система антитеррористической защиты	Рентгенография, томографы
	Физическая	Система антитеррористической защиты	Средства активного противодействия несанкционированным вторжениям (электрошоковые устройства, распыляемые барьеры)
	Физическая	Интегрированные системы ИТСО и САЗ	Функционально законченный комплекс ИТСО и/или САЗ, включая периферийное оборудование (средства обнаружения, ИСО, ТВ камеры)
	Физическая	Система инженерной защиты	Ограждения периметра (железобетонные, металлические сварные, комбинированные)

Структура меню

Welcome: LPV

Активы | Процессы | Уязвимости | Угрозы | Риски | Контрмеры (защита) | Инциденты | Документы | Отчеты | Справочники | Утилиты

Активы: Организационная модель | Объекты защиты | Классификатор активов | Реестр активов

Процессы: Классификатор процессов | Бизнес-процессы | Технологические процессы | Процессы ИТ | Матрица ответственности | Процессы менеджмента ИБ | Процедуры ИБ | Аудит ИБ

Уязвимости: Классификатор уязвимостей | Форма регистрации выявленной уязвимости

Угрозы: Классификатор угроз | Классификатор нарушителей | Реестр угроз

Риски: Классификатор рисков | Мониторинг рисков | Оценки рисков | Анализ рисков | Коммуникация рисков

Контрмеры (защита): Политика ИБ | Цели ИБ | Критерии ИБ | Объект защиты | Профиль защиты | Защитные меры

Инциденты: Классификатор инцидентов | Форма регистрации инцидента

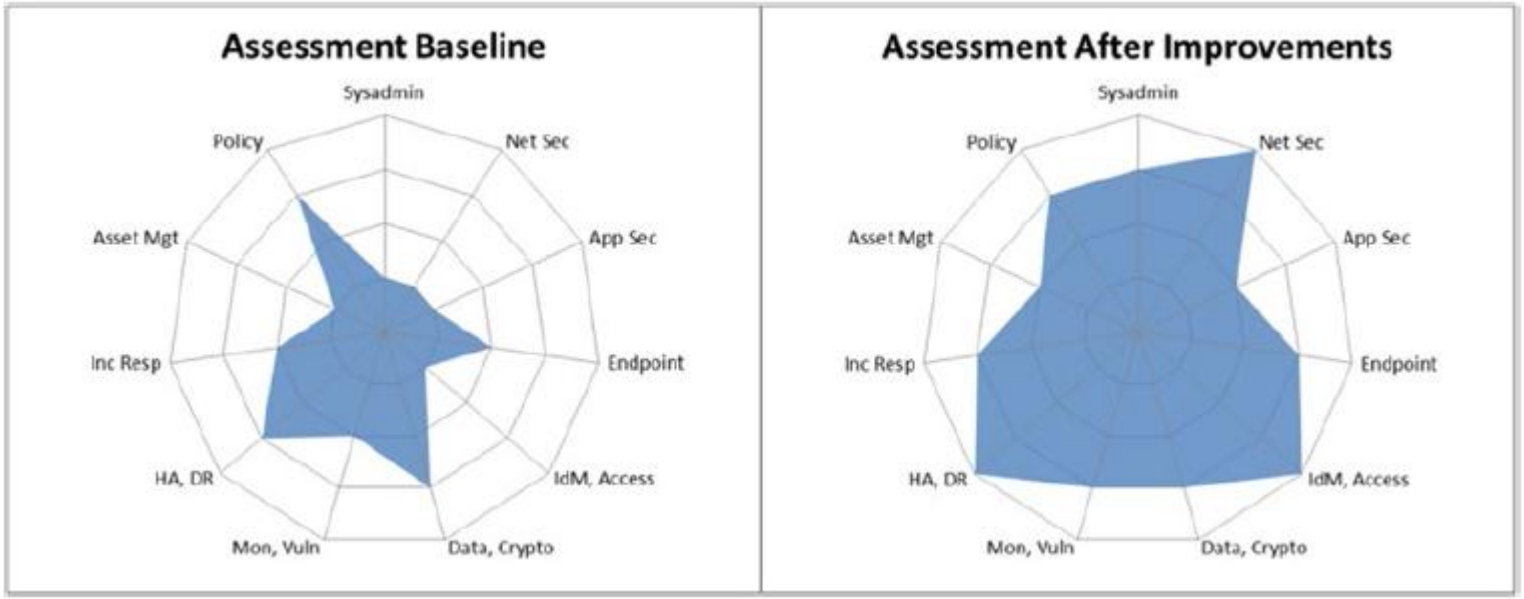
Документы: Законы | Стандарты | Инструкции

Справочники: Технологии защиты | Поставщики решений | Решения по защите | Глоссарий терминов

Утилиты: Генератор отчетов | Импорт | Экспорт | События триггеры | Уведомления

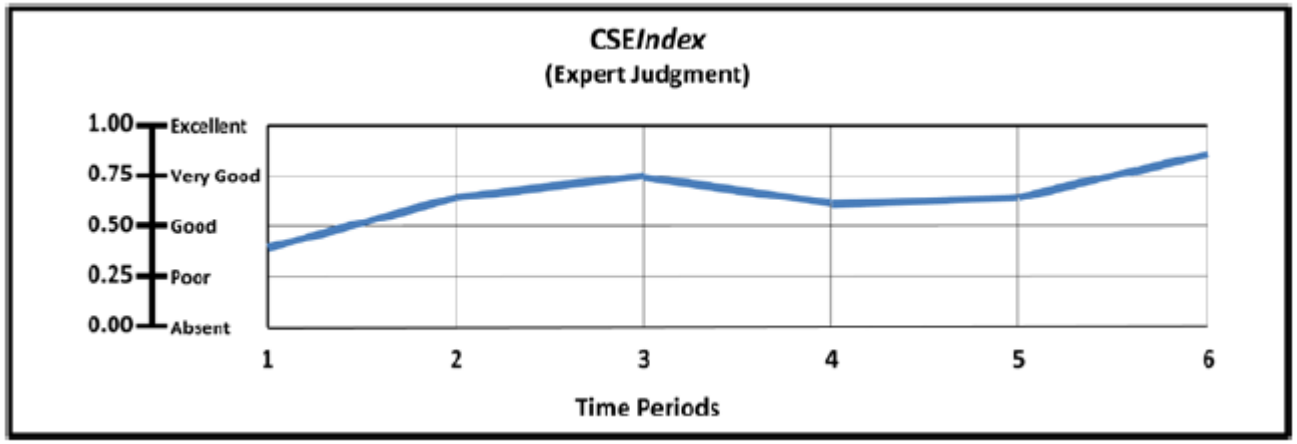
В разработке….

Расчет метрики и KPI



$$\text{OM}\,Index = \frac{\sqrt{\sum_{i=1}^{n} w_i^2 at_i^2}}{\sqrt{\sum_{i=1}^{n} w_i^2 (maximum[at_i])^2}}$$

where at_i = object attribute measurement
n = number of object attribute measurements
w_i = weighting factor for object attribute at_i
maximum $[at_i]$ = maximum value of at_i



Модель угроз – нетривиальные случаи

- Не обязательно быть целью, чтобы стать жертвой;
  Вредоносное ПО – это тоже программа

- Понимание границ возможностей и ответственности;
  Нет 100% защиты от целевой атаки
  (**общие угрозы**, «хактивисты», организованная преступность, действия разведок и иностранных спецслужб, кибер-войны)
  Honeypots/Honeynets/Honeytokens – инструмент провокаций ☺

- Во многой мудрости много печали; и кто умножает познания, умножает скорбь;
  Глубокий анализ рисков – порождает другие риски

- Импортозамещение. (отечественное ПО – тоже может содержать НДВ, уязвимости, ошибки и т.п.
  + «проблема компилятора»)

Чего не хватает?

- Научности – нужна помощь научного сообщества;
- Уверенности, основанной на результатах тестирования – требуется организация полигонов для испытаний;
- Оперативности внесения изменений – должна работать «обратная связь», уточняющая модели угроз, нарушителей и т.п. по реальным инцидентам;
- Информированности – работа над НТД должна вестись последовательно и методично с опорой на уже достигнутый уровень.

Не хватает Финансирования!

Спасибо за внимание!

Павел Литвинов,
начальник аналитического отдела

ЗАО «РТСофт»
тел. +7 (495) 742-68-28, 967-15-05