

# Нормативное обеспечение кибербезопасности



Декабрь 2014

Вопросы и предложения

# Управление ожиданиями

## ➤ Не будет

- истории вируса Stuxnet (как впрочем и других)
- описания продукта «серебряная пуля»
- предложения «универсального решения»
- выводы в конце ☹



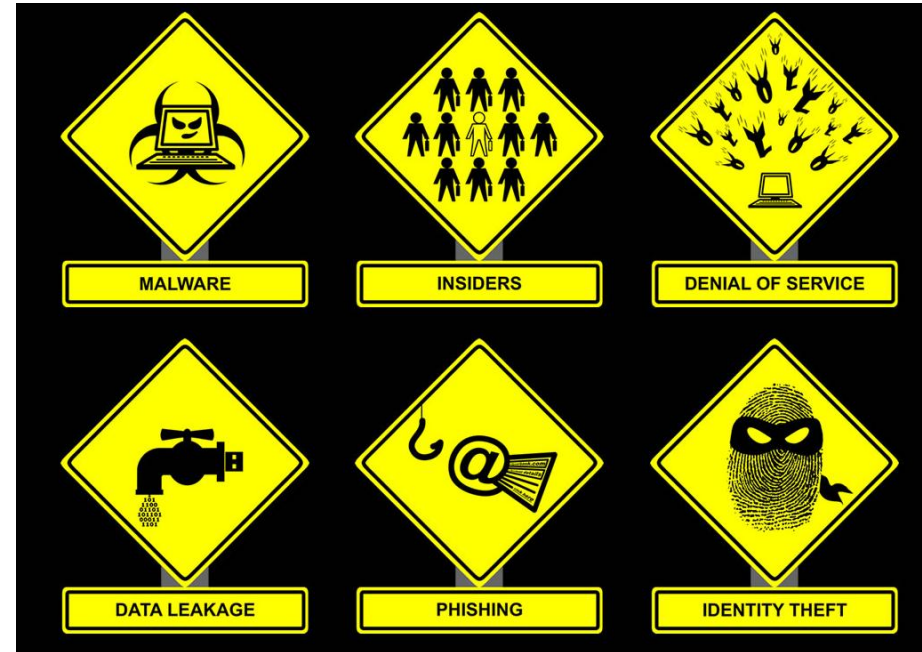
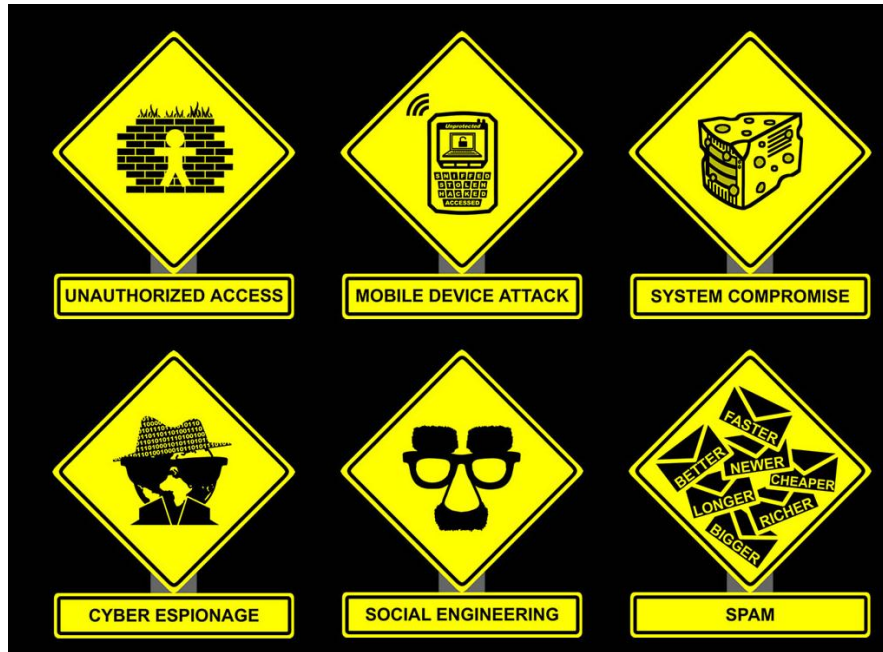
## ➤ Будет

- оценка текущего состояния вопроса с нормативным обеспечением
- предложения по следующим шагам
- сценарии повышения безопасности для обсуждения
- основное в начале ☺

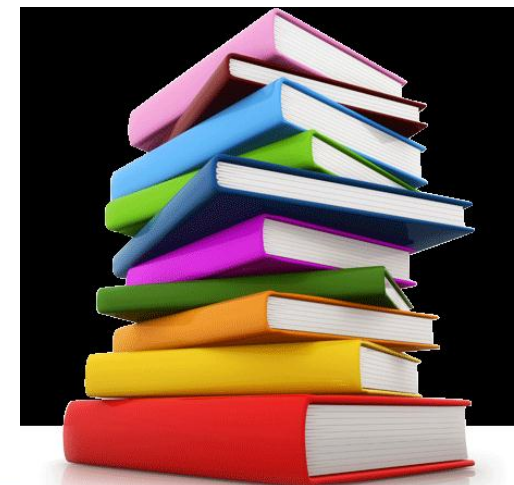


# Тезисы

- 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.)
- Российская нормативная база продолжает расти и совершенствоваться, но не хватает документов «прямого действия» с учетом отраслевой специфики
- Ситуация меняется быстрее, чем мы на нее реагируем



# НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ VS УГРОЗЫ



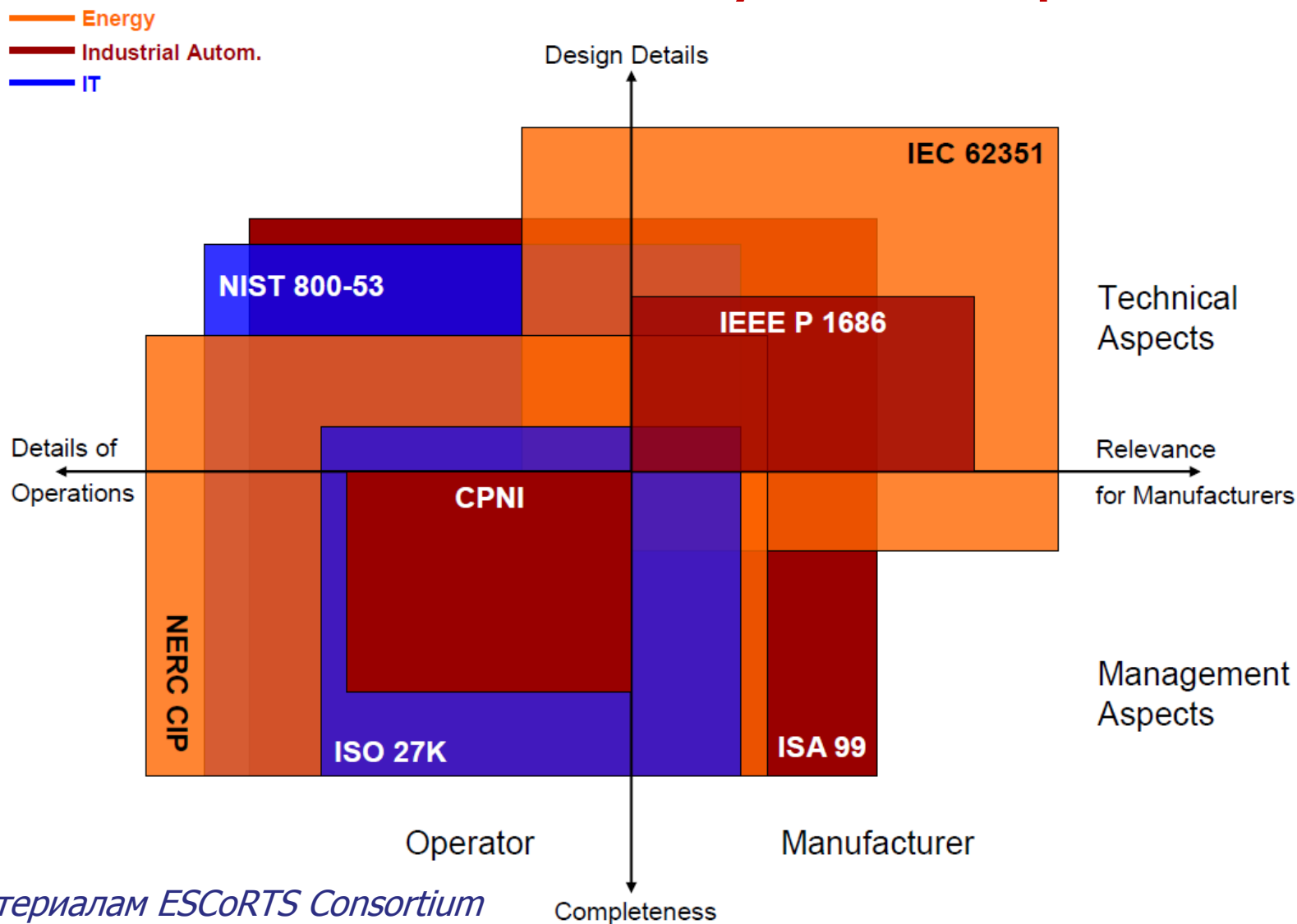
# Стандарты и мировой опыт

- **NERC-CIP** (США и Азия)
- **CPNI** (Великобритания)
- **BDEW White Paper** (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

# Правовая база в России

- Федеральный закон Российской Федерации от 21 июля 2011 г. № 256-ФЗ "О безопасности объектов топливно-энергетического комплекса"
- Федеральный закон Российской Федерации от 21 июля 2011 г. N 257 - ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности объектов топливно-энергетического комплекса"
- Постановление Правительства Российской Федерации от 22 декабря 2011 г. № 1107 "О порядке формирования и ведения реестра объектов топливно-энергетического комплекса"
- Постановление Правительства Российской Федерации от 5 мая 2012 г. № 460 "Об утверждении Правил актуализации паспорта безопасности объекта топливно-энергетического комплекса"
- Постановление Правительства Российской Федерации от 5 мая 2012 г. № 459 "Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса"
- Постановление Правительства Российской Федерации от 21 мая 2007 г. № 304 г. Москва "О классификации чрезвычайных ситуаций природного и техногенного характера"

Без претензии на полноту!

# 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

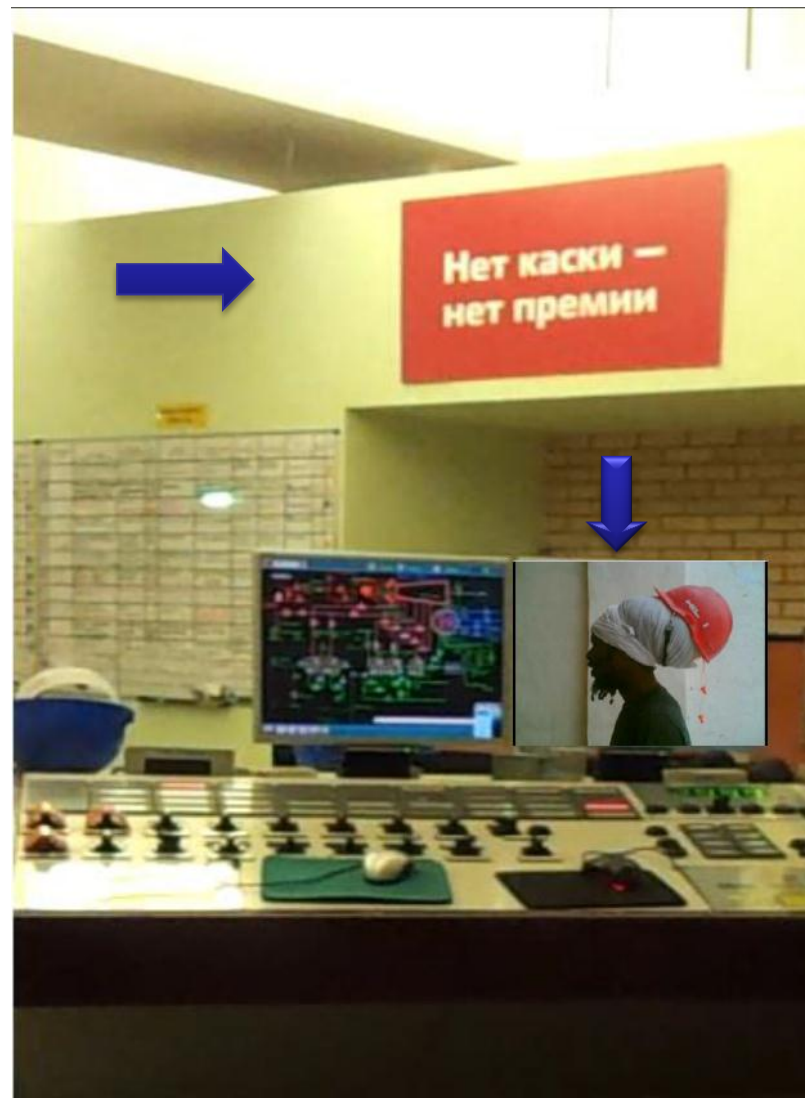
## Заведомо ложное заключение экспертизы промышленной безопасности

*(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.

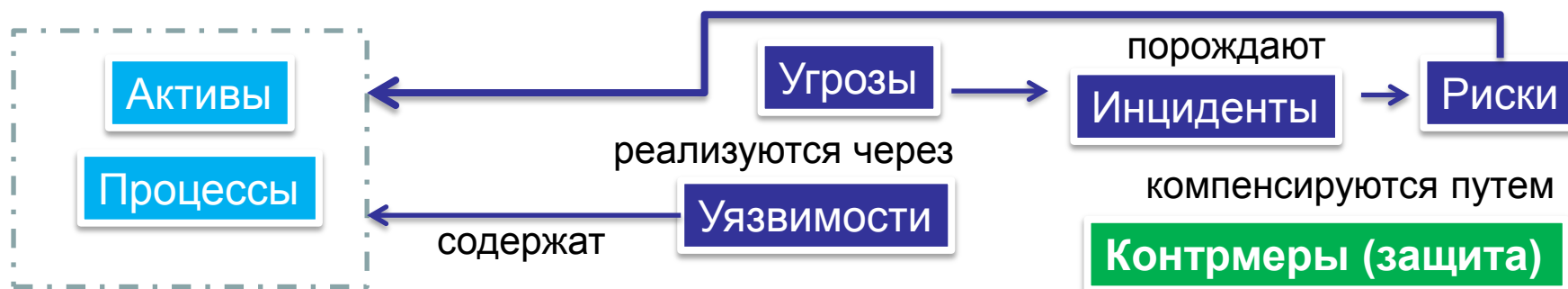
# Нормативная база в России

- ГОСТ 0043-003-2012 по аттестации объектов информатизации (**ДСП**)
- **ФСК** СТО 56947007-29.240.01.169-2014 «Обеспечение информационной безопасности на стадиях жизненного цикла информационных и технологических систем» - (**новый**)
- **ФСТЭК** «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»  
(Зарегистрирован Минюстом 30-06-2014)
- **ФСБ** – ждем новостей ...



# ВЫЗОВЫ

- Классические способы обеспечения надежности путем резервирования не работают против кибер-атак
- Импортозамещение
- Мероприятия по обеспечению ИБ могут влиять на нормальное функционирование системы
- Нежелательность (невозможность) проведения тестов на проникновение



# Сопоставление угроз мерам защиты

The screenshot displays the RTSoft IAS application interface, which is used for mapping threats to security measures. The interface is divided into three main sections:

- Left Pane (Tree View):** Displays the 'ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ (ГОСТ Р 51275-2006)' (Factors affecting information, GOST R 51275-2006). The tree structure includes:
  - Объективные факторы (Objective factors)
    - Внутренние факторы (Internal factors)
      - 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 (External factors)
      - Явления техногенного характера
      - Природные явления, стихийные бедствия
  - Субъективные факторы (Subjective factors)
    - Внутренние факторы (Internal factors)
      - Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:
      - Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:
      - 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 обеспечения;
      - хищения носителя защищаемой информации;
      - нарушения функционирования ТС обработки информации.
    - Недостатки организационного обеспечения защиты информации при:
    - Ошибки обслуживающего персонала ОИ при:
  - Внешние факторы (External factors)
    - Доступ к защищаемой информации с применением технических средств:
      - разведки;
      - система информации.
    - Несанкционированный доступ к защищаемой информации путем:
    - Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки;
    - 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 электромагнитным воздействием.
- Central Pane:** Displays the 'ГОСТ Р 51275-2006' (GOST R 51275-2006) standard, specifically the 'Защита информации' (Information protection) section, which defines the 'ОБЪЕКТ ИНФОРМАТИЗАЦИИ, ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ' (Object of informatization, factors affecting information).
- Right Pane (Tree View):** Displays the 'Состав мер защиты информации' (Composition of security measures for information). The tree structure includes:
  - Состав мер защиты информации (Composition of security measures for information)
    - 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 установок обновлений программного обеспечения, включая обновление программ
      - 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 (ОЦП)
    - X. Обеспечение доступности (ОДП)
    - 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 технически
      - Организация контролируемой зоны, в пределах которой постоянно размещаются стационарн
      - Размещение устройств вывода (отображения) информации, исключающее ее несанкционир
      - 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 (ППН)
      - Разработка правил и процедур (политик) планирования мероприятий по обеспечению защит
      - 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 автоматизированн
    - XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
      - Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденн
      - 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

## Чего не хватает?

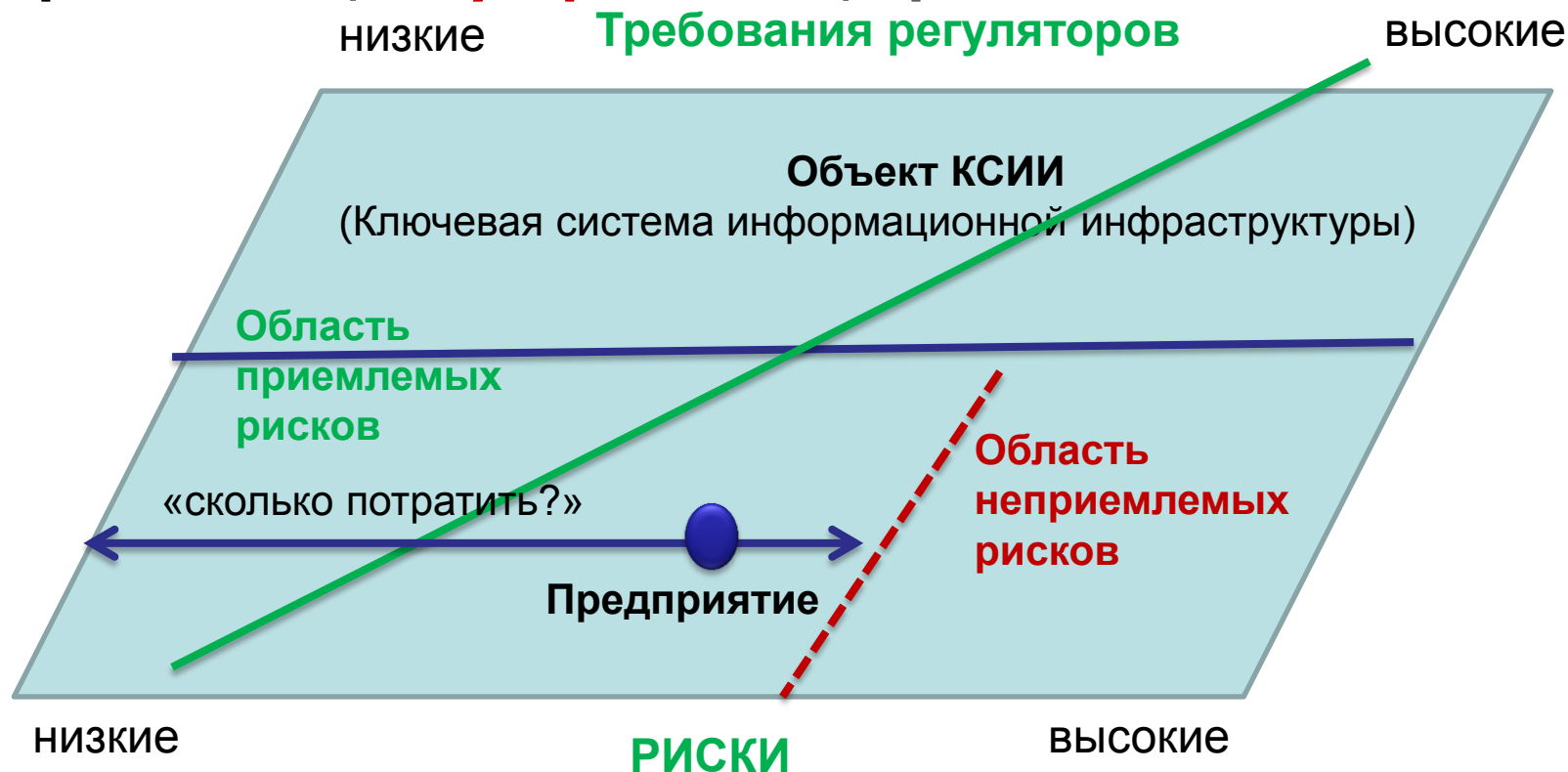
- Научности – нужна помощь научного сообщества
- Уверенности, основанной на результатах тестирования – требуется организация полигонов для испытаний
- Оперативности внесения изменений – должна работать «обратная связь», уточняющая модели угроз, нарушителей и т.п. по реальным инцидентам
- Информированности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



# БЕЗОПАСНОСТЬ КАК АКТИВ

# Сколько потратить на безопасность?

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

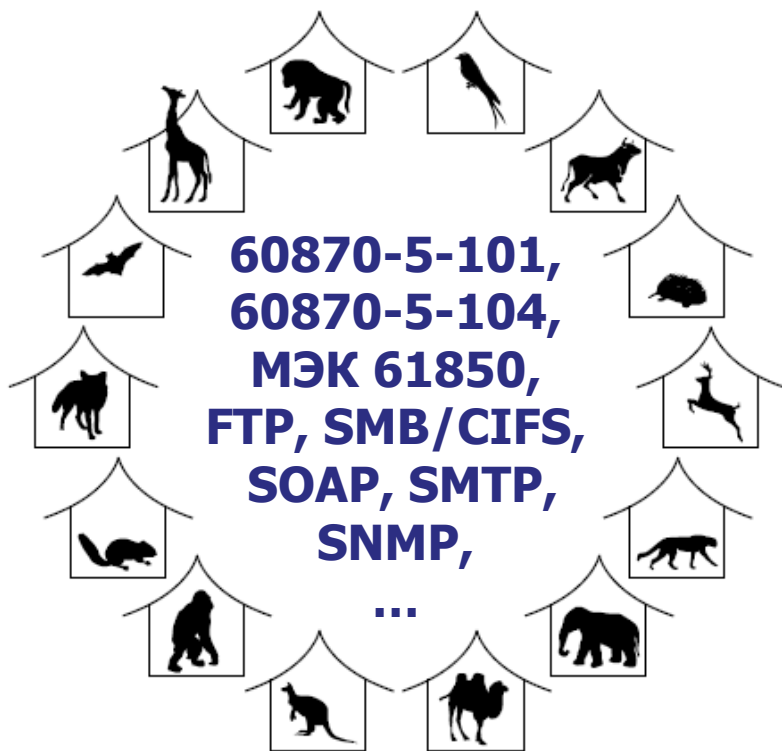


**Вкладывать средства в безопасность – выгодно,  
чтобы не попасть в зону неприемлемых рисков!**

# Принципы разработки НТД должны учитывать требования к реализации

- 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 асимметричная реализация
- Правильный учет «человеческого фактора»

# 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



# 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

*Пример. Запрет использования 3G модемов и fi-fi контролируется сканерами, а в серверных помещениях «дублируется» глушителями сигнала.*

# Предложения по решению НТС

- Создать рабочую группу с целью подготовки конкурсов *(названия тем условные)*:
- Разработка СТО на основе Приказа ФСТЭК №31
- Создание Программного комплекса Моделирования и поддержки жизненного цикла решений по обеспечению информационной безопасности (ПК МиПЖЦ ИБ) позволяющего на основе стандартов, нормативно-технической документации, архитектуры и состава испытываемой системы формализовать разработку моделей нарушителя, уязвимостей и, как следствие, частной модели угроз
- Разработка методики и стенда для проведения предварительных испытаний отдельных видов устройств, ПТК автоматизации подстанций и ПТК ЦУС на соответствие стандартам и требованиям информационной безопасности

Полигон – Аналитика – Нормативное обеспечение



# Вопросы?

## Спасибо за внимание!

Павел Васильевич Литвинов,  
начальник аналитического отдела

[litvinov\\_pv@rtsoft.msk.ru](mailto:litvinov_pv@rtsoft.msk.ru)

**ЗАО «РТСофт»**

тел.: +7 (495) 742-68-28, 967-15-05