RTSoft
средства и системы автоматизации

Сценарии оптимизации затрат на мероприятия по обеспечению кибер-безопасности

Павел Васильевич Литвинов

RUGRIDS ELECTRO

«Панельная дискуссия
«Кибербезопасность: от угроз к возможностям»

октябрь, 2015

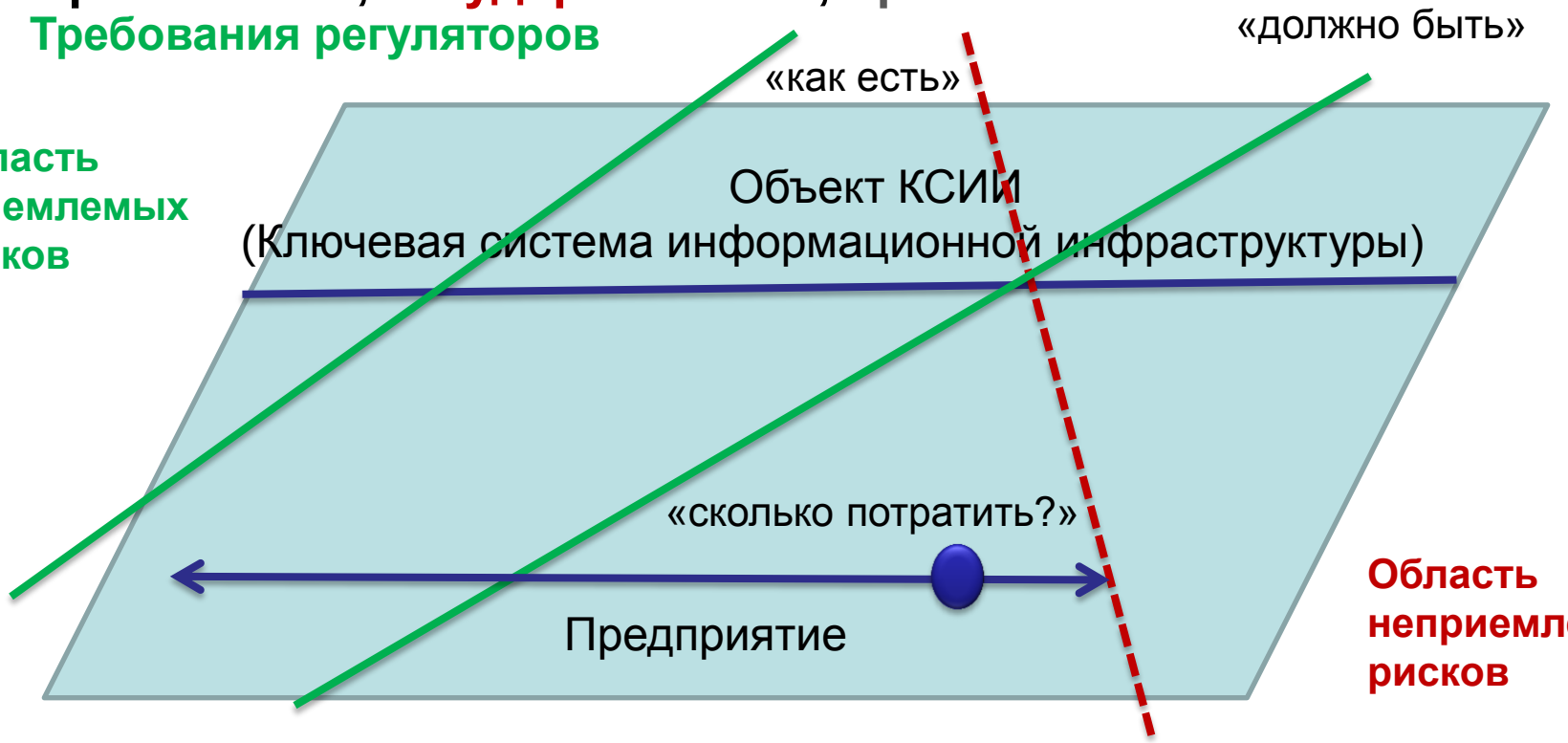
Оптимизационная задача – сложная функция от:

- Начальных (граничных) условий
  - масштаб организации (задачи)
  - наличие требований регуляторов
- Точки зрения
  - специалист по ИБ
  - руководитель
  - собственник
- Стратегии (сценария)
  - «оптимизация»
  - «новое строительство»
  - «выживание»

Осуществлять контроль + рассматривать альтернативы + проводить компенсационные мероприятия

Сколько тратить на безопасность?

- Регуляторы – **ФСТЭК**, **Ростехнадзор**, **ФСБ, МО**, **МВД, Минюст, … (~ 17!)**
- Безопасность – **информационная**, **технологическая**, **физическая**, **государственная**, **правовая**



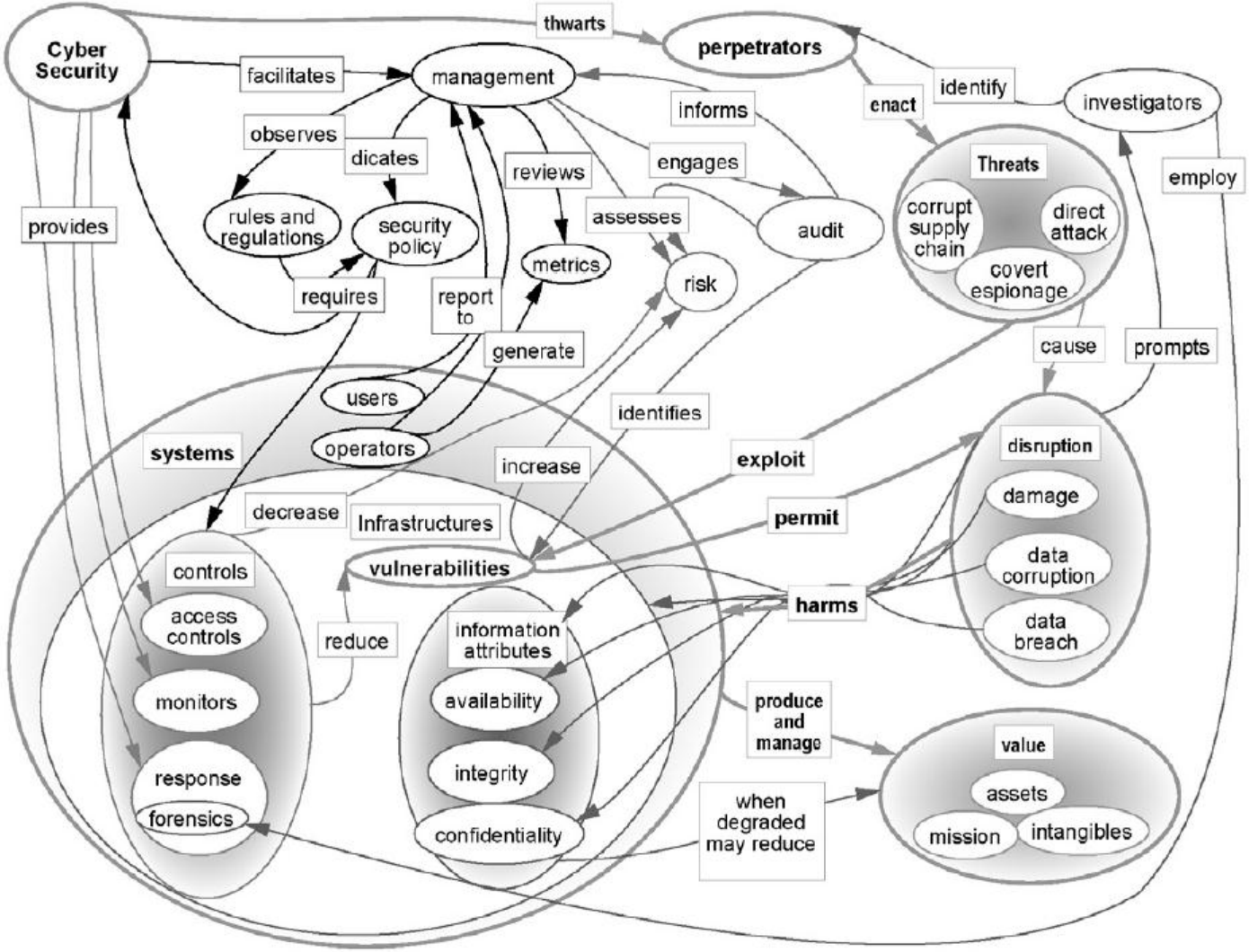
Вкладывать средства в безопасность – выгодно, чтобы не попасть в зону неприемлемых рисков!

«Правило» 30%

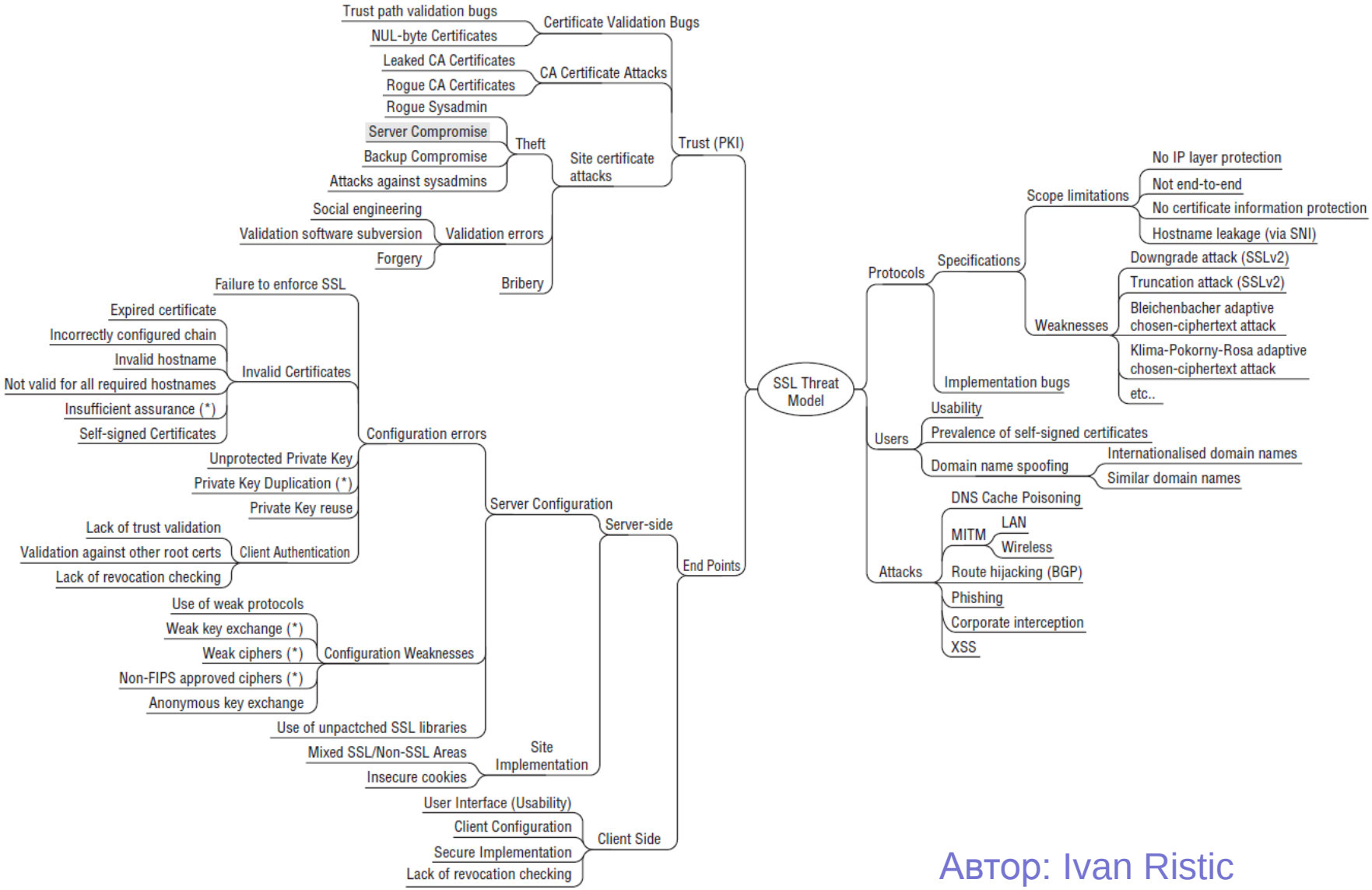
Объективные сложности

- Определение вероятности события
  - События редкие или их не было – статистика не работает
  - Даже одно событие может изменить мир, технологии и т.п.
- Расчет ущерба
  - много сценариев развития аварии с разной вероятностью
  - требуются глубокие знания технологии
  - трудно учесть взаимное влияние
- Требования регуляторов
  - не гармонизированы
  - недостаточно конкретны
  - оторваны от технологической специфики
  - не полны (не всегда актуальны текущим угрозам)
- Трудно определить Return on Investment

Связи между сущностями образуют гиперкуб

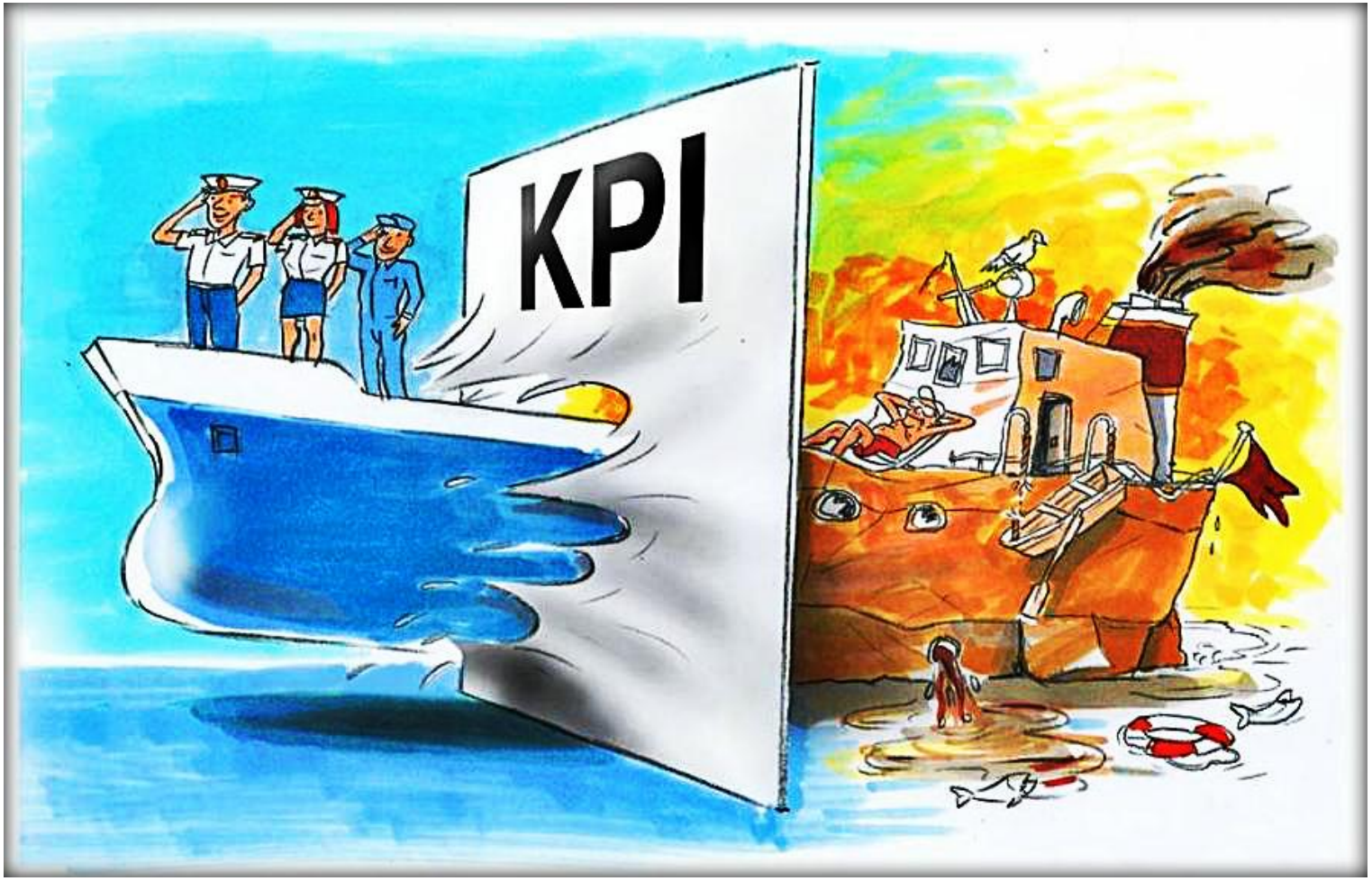


Пример: mind map диаграмма угроз для SSL



Автор: Ivan Ristic

Контроль и KPI



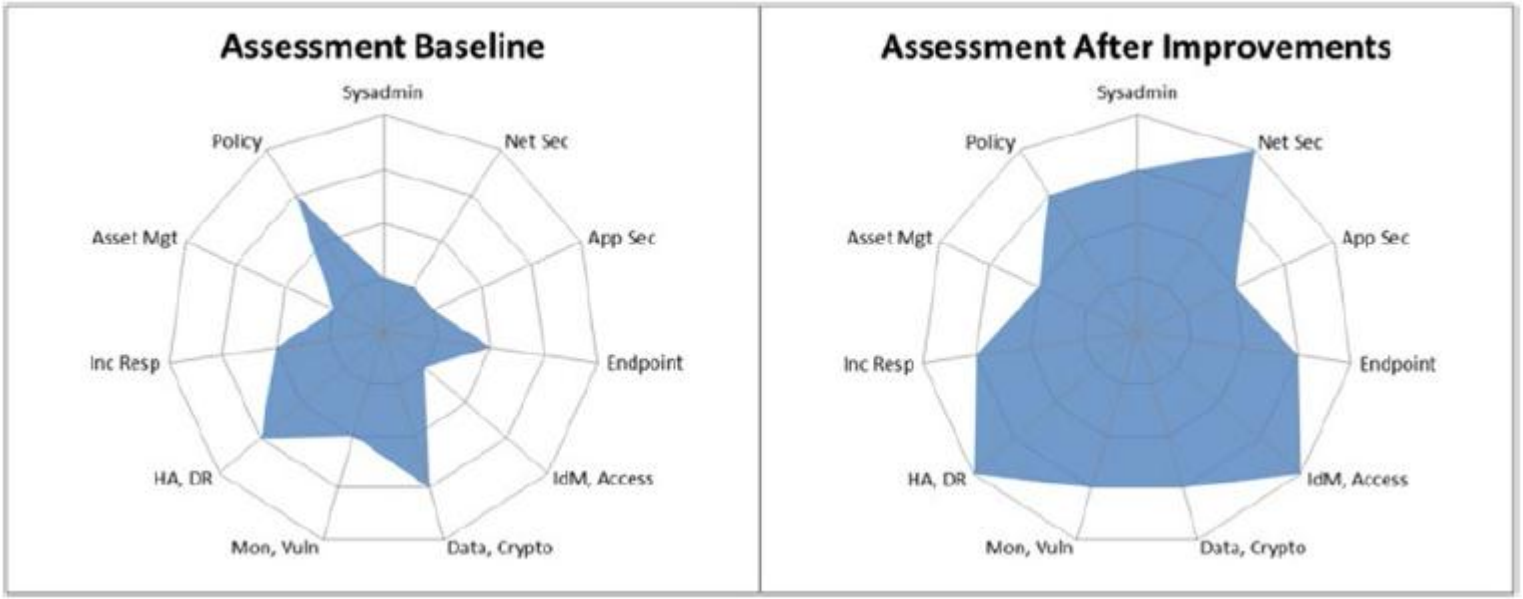
Сегментация для планирования и контроля

1шаг - оценка масштаба: 10; 100; 1000; 10 000 – метрика м.б. комплексной (компьютеры, люди, телекоммуникационное оборудование, ПО, серверы…)

- 2 шаг – сегментация мероприятий по обеспечению ИБ
  - Системное администрирования (SA)
  - Сетевая безопасность (NS)
  - Безопасность приложений (AS)
  - Безопасность рабочих станций, серверов и устройств (ESDS)
  - Идентификация, аутентификация и управление доступом (IAAM)
  - Защита данных и криптография (DPC)
  - Мониторинг, управление исправлениями (MVPM)
  - Аварийное восстановление, и физическая защита (HADRPP)
  - Реагирования на инциденты (IR)
  - Управление активами и поставками (AMSC)
  - Политики безопасности, аудит и обучение персонала (PAET)

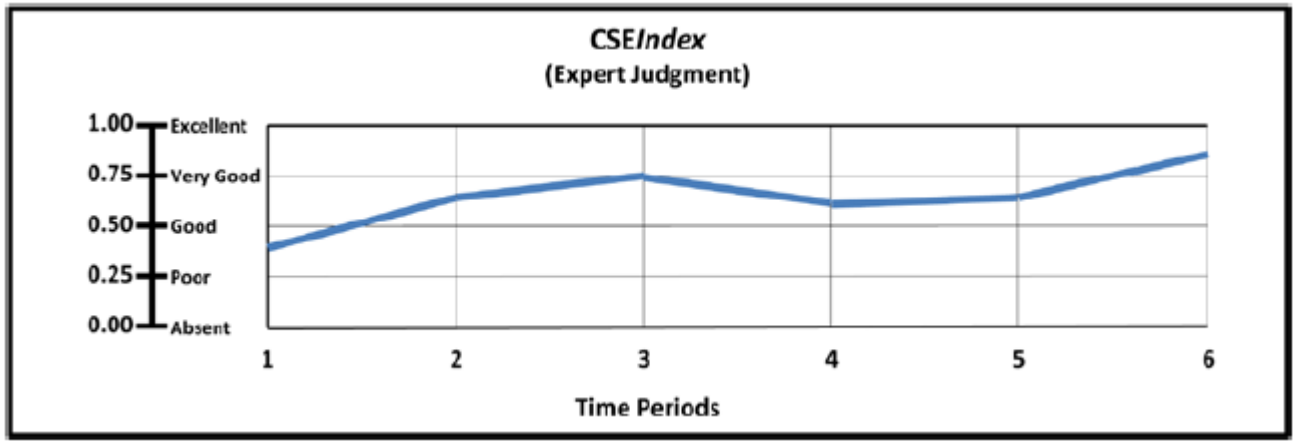
В каждом сегменте есть разделы и вопросы, позволяющие сделать для экспертную оценки

Расчет метрик и представление результата



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

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



Альтернативные варианты

Типизация нарушителей

- **«Любитель»**
  - Частное лицо, пытающееся найти возможности и технологии взлома SCADA систем, имеющих интерфейсы в Интернет с помощью известных уязвимостей, найденных с использованием поисковой системы «Shodan»
- **«Инсайдер»** (в том числе «без злого умысла»)
  - недовольный сотрудник или обслуживающий персонал собственной или сторонних организаций (поставщики, партнеры, наладчики), имеющий права доступа и знающий тонкости эксплуатации систем и способы хранения конфиденциальных данных
- **«Враг»**
  - Преступные группировки и иностранные правительства (Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War и т.п.)

[Мотивация] x [Ресурс] x [Знания, опыт] x [Информированность]

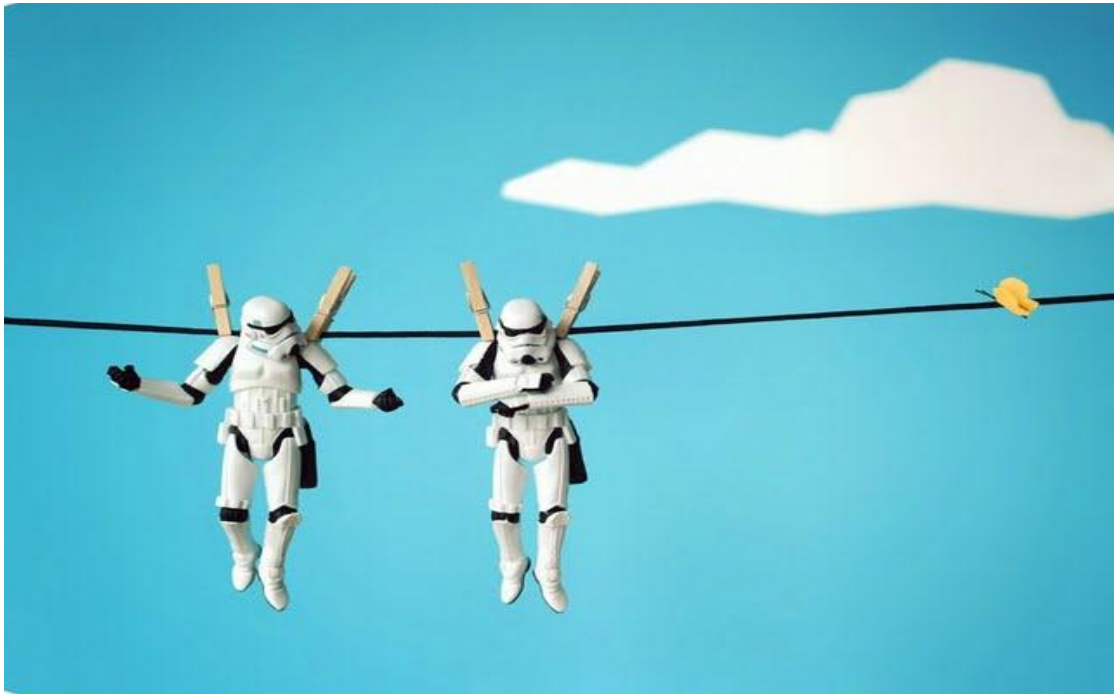
Сценарии оптимизации

- Принятие рисков
  - в модель угроз включаем только критические риски
- Принцип Парето
  - (в каждом направлении выполняем только «дешевые шаги»)
- «Чуть лучше, чем у других»
  («не надо уметь бегать быстрее, чем медведь гризли…»)
- «Не моя война»
  - Вы не можете и (не должны!) самостоятельно противостоять таким угрозам как Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War – расставляем Honeypots/Honeynets/Honeytokens для **обоснованного** обращения за помощью
- «Чужой бюджет» (времени и денег)
  - обучение, IT – инфраструктура, модернизация … и т.п.
  - согласование с планами работ других подразделений

Принципы планирования защиты

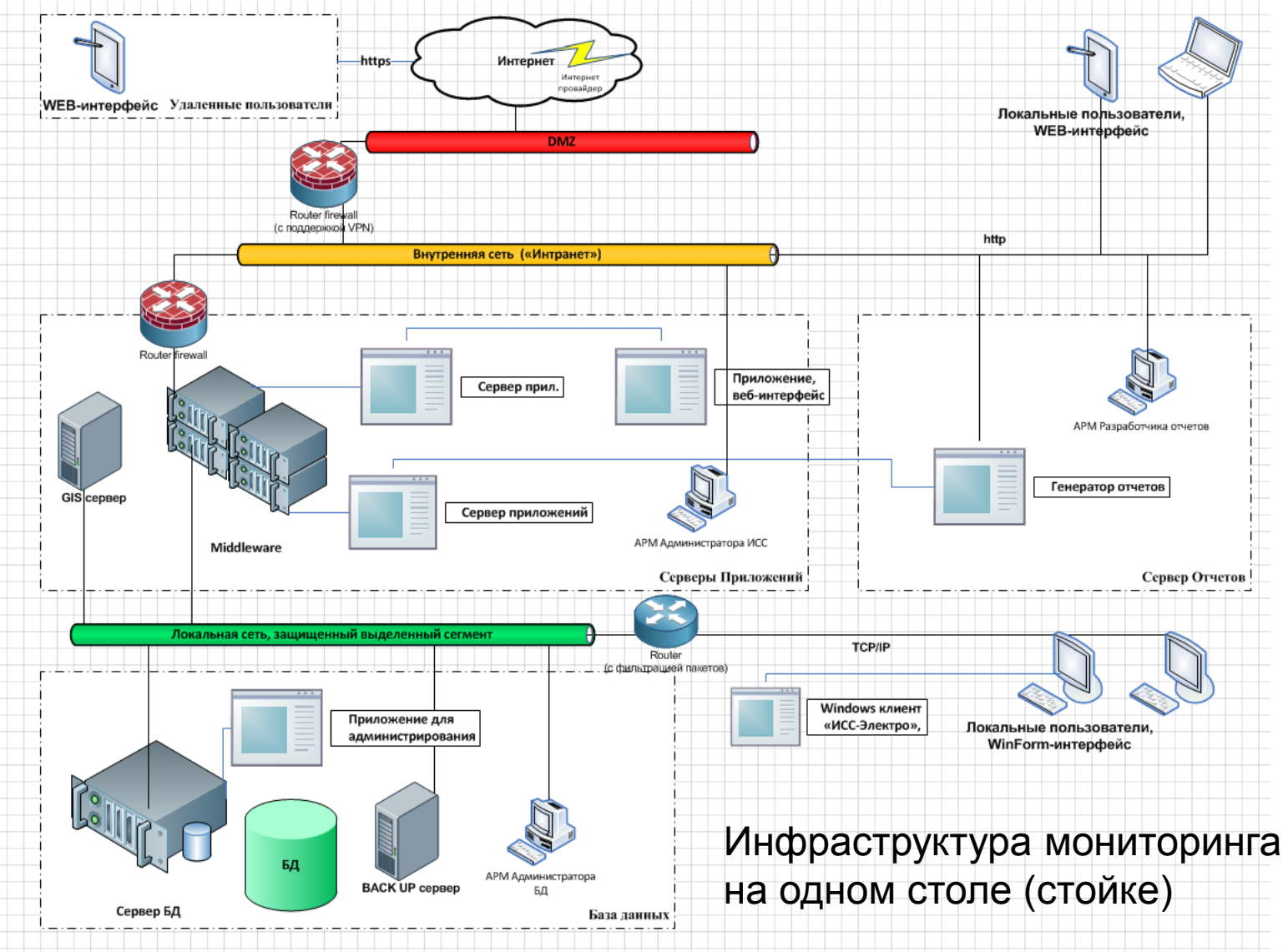
- Адекватность существующей (текущей) модели угроз – экономическая целесообразность
- Архитектурно заложенный «запас прочности» под будущие угрозы – защита инвестиций
- Переоценка роли дублирования (многократного резервирования), и его влияния на надежность в случае кибератак
- «Эшелонированность обороны»,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

Кто виноват? или когда нет SIEM…



- «Собрать» из open source компонентов
  - **включить запись логов (**где только возможно)
  - использовать Microsoft Log Parser для записи существенной информацию в БД по расписанию
  - для аналитики и визуализации использовать язык и библиотеки R
  - ….

«Свой огород»



Инфраструктура мониторинга ИБ на одном столе (стойке)

Технологическое видеонаблюдение

ИДЕЯ – технологическое видеонаблюдение позволяет получить альтернативный поток данных объекта управления. Его целесообразно использовать, когда есть основания не доверять телеметрической информации или ее поток прерван.

- Фактическое состояние оборудования механизмов и органов управления до и после выполнения операции
- Отсутствие людей вблизи исполнительных механизмов (дополнительная безопасность)
- Использование камер в инфракрасном диапазоне – температурное наблюдение
  позволяет в автоматическом режиме диагностировать, как технологические нарушение (перегрев, неравномерный нагрев и т.п.), так и появление людей

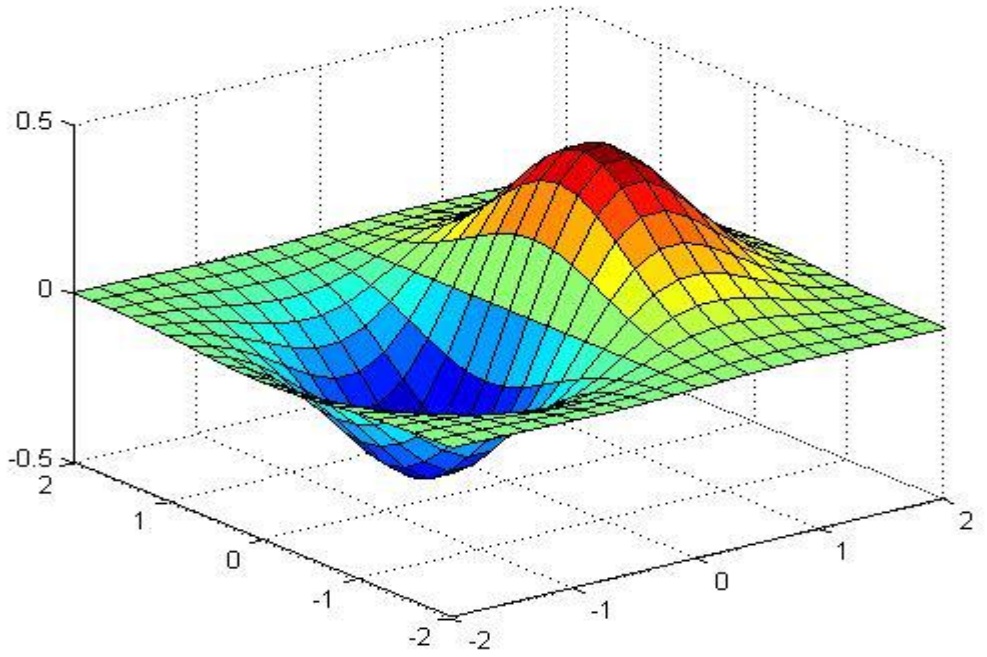
Человеческий фактор

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 «игры» Лаборатории Касперского)
- 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.

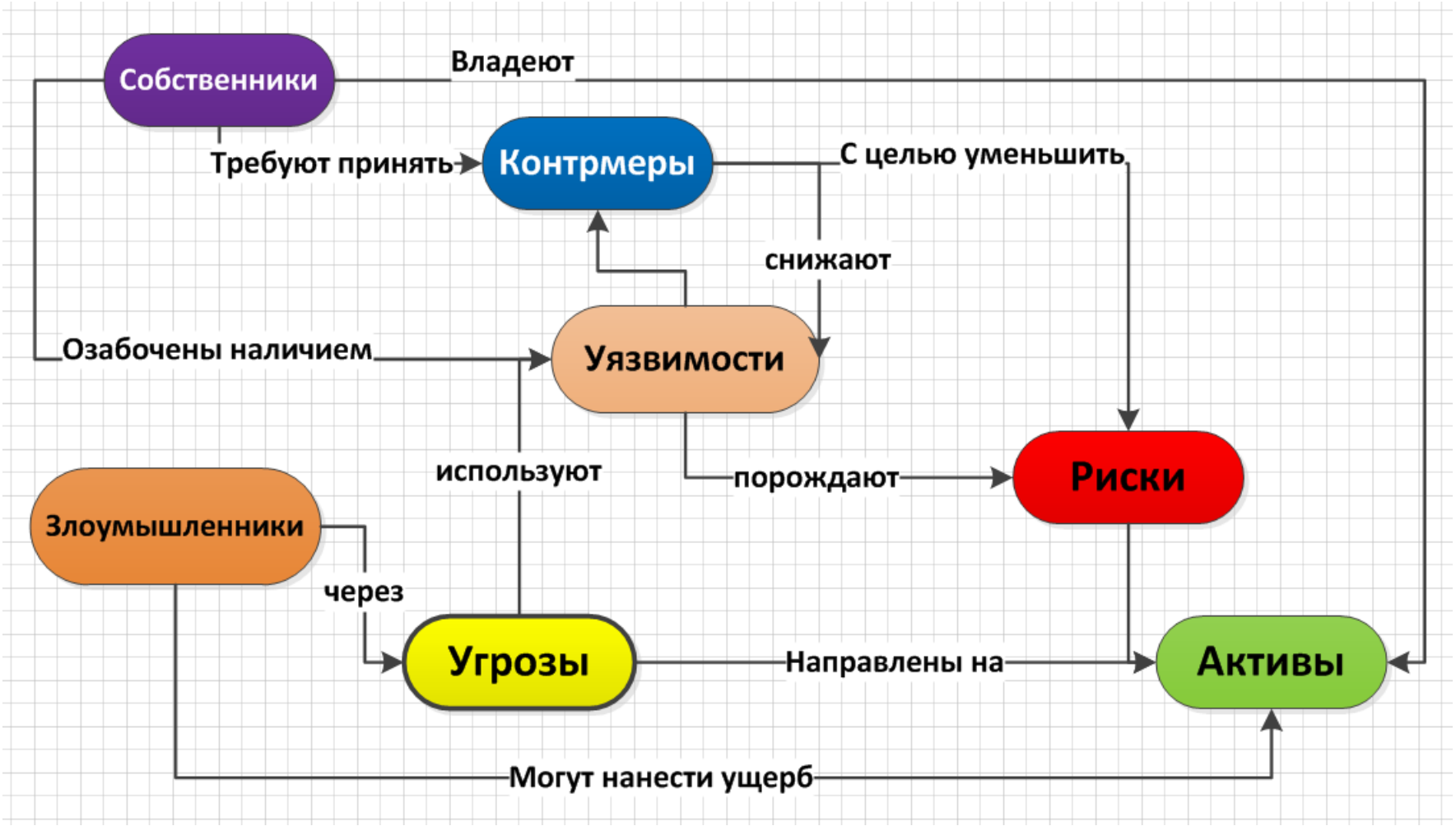
**Например. Запрет использования 3G модемов и Wi-Fi контролируется, а в серверных помещениях «дублируется» глушителями сигнала.*

Концепция доверенного телеуправления

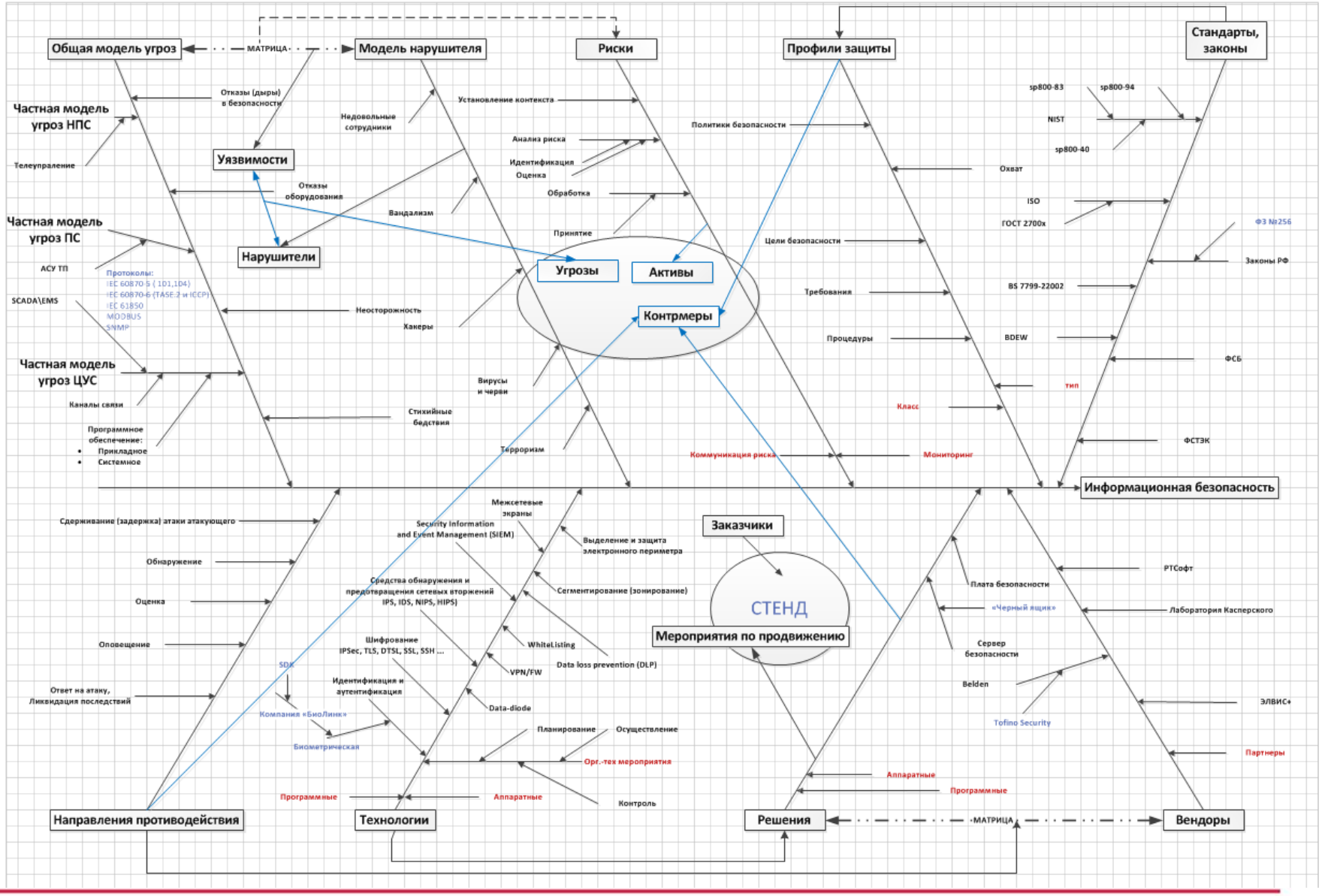


МОДЕЛИРОВАНИЕ

Концептуальная модель архитектуры безопасности



Онтологическая модель

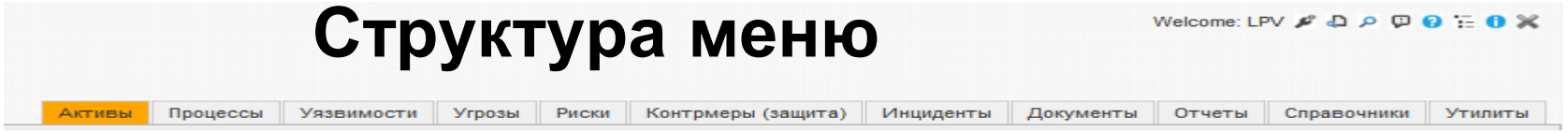


ПО «Моделирования и поддержки жизненного цикла решений по обеспечению безопасности» (ISLS)

Основными целями разработки и применения ISLS являются:

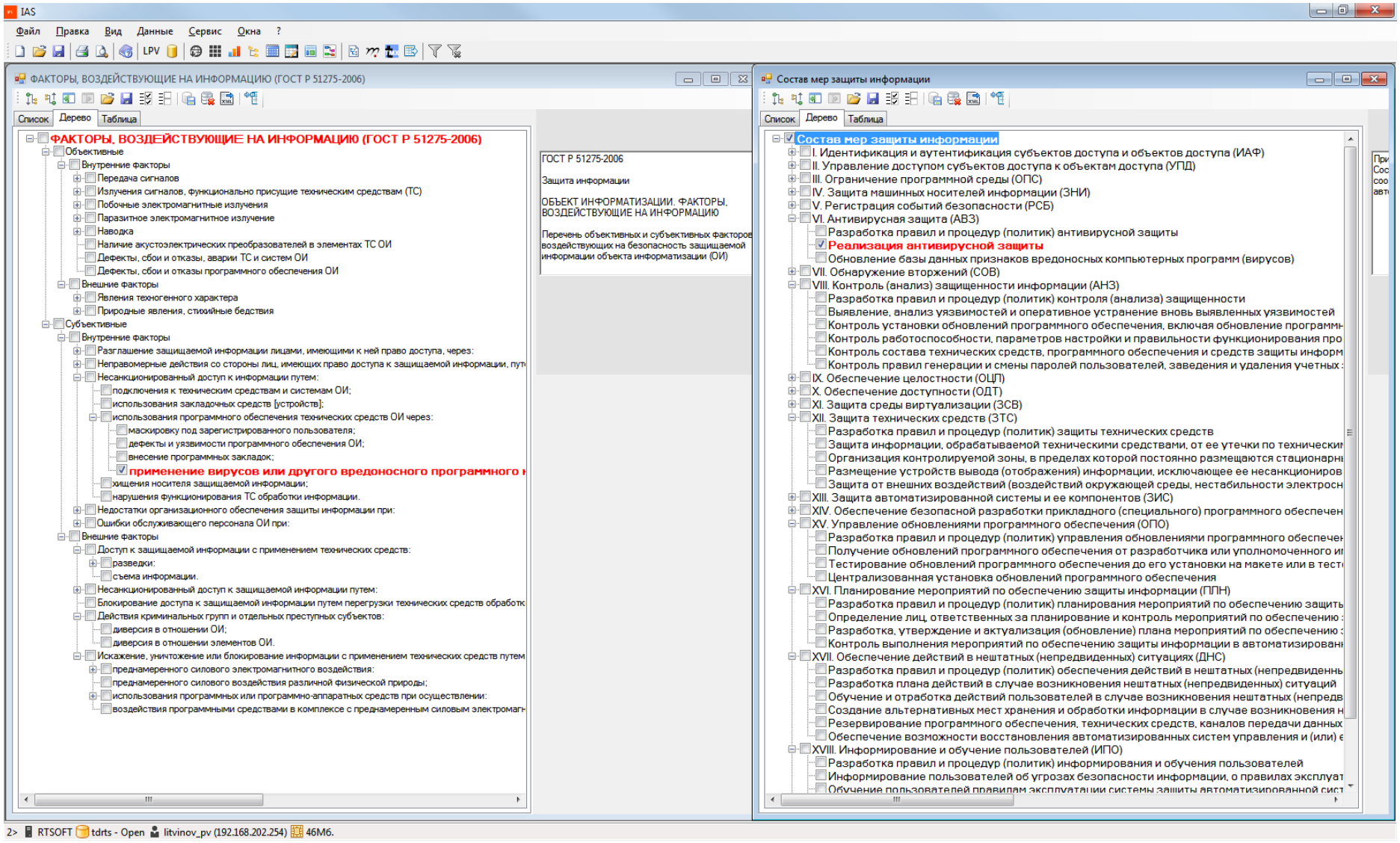
- реализация комплексного подхода к разным граням обеспечения безопасности: физической, информационной, технологической и т.д. Все составляющие необходимо развивать пропорционально, поскольку атака может быть проведена через самое слабое звено;
- системный подход к моделированию и прогнозированию. Безопасность системы, это в общем случае, сложная и нелинейная функция от состояния ее компонентов;
- определение необходимой достаточности и экономической целесообразности – оптимизация затрат на безопасность путем расчета рисков, при наличии статистических данных или моделирования рисков для новых видов угроз;
- непрерывная адаптация моделей и генерируемых на их основе документов, под меняющиеся угрозы и условия внешней и внутренней среды;
- обеспечение онтологической связности – прогнозирование через моделирование прямых и косвенных последствий событий и принимаемых решений и отдаваемых команд;
- конвергенции технологий и услуг – с целью дополнительного резервирования или исключения не рационального дублирования;
- проектирование эшелонированных мероприятий и решений по защите и активному противодействию угрозам.

Структура меню



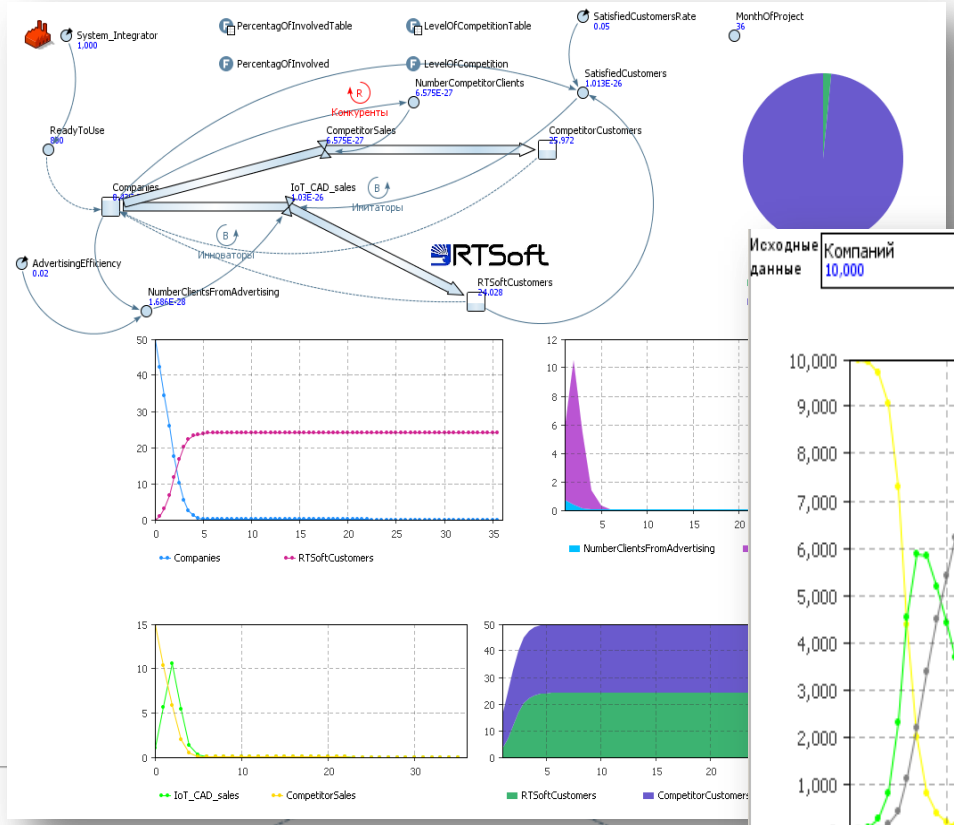
- **Активы**
  - Организационная модель
  - Объекты защиты
  - Классификатор активов
  - Реестр активов
- **Процессы**
  - Классификатор процессов
  - Бизнес-процессы
  - Технологические процессы
  - Процессы ИТ
  - Матрица ответственности
  - Процессы менеджмента ИБ
  - Процедуры ИБ
  - Аудит ИБ
- **Уязвимости**
  - 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

Интерфейс для аналитики

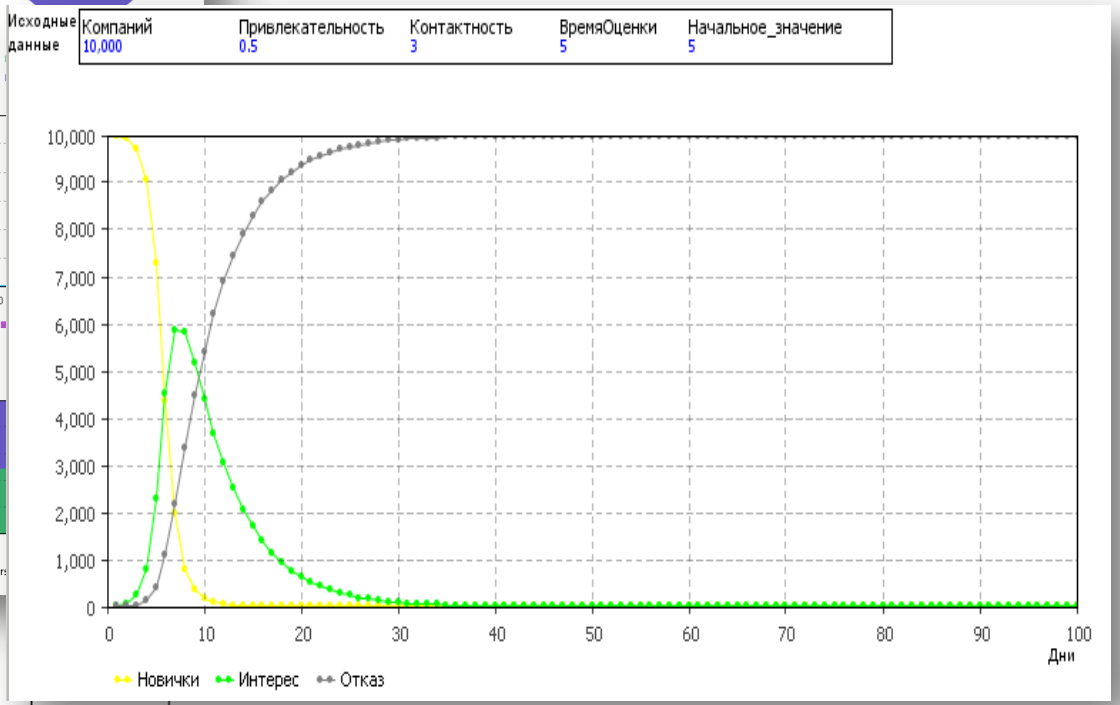


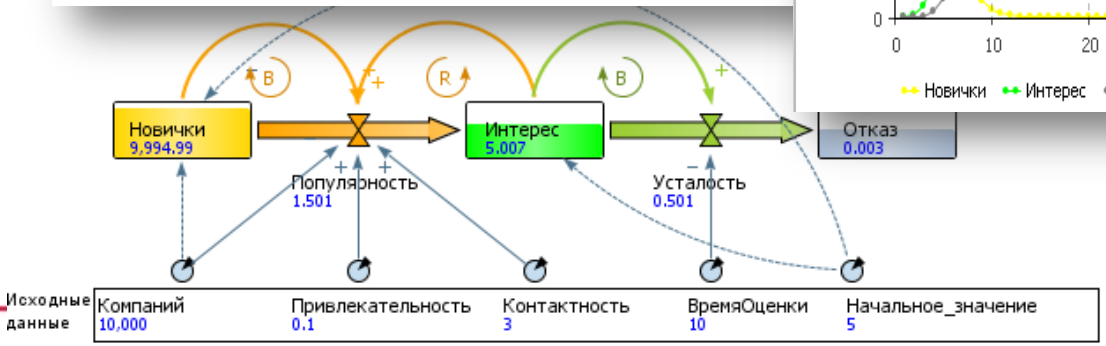
[Факторы воздействующие на информацию (ГОСТ)] x [Меры защиты (ФСТЭК)]

Моделирование



диффузионная модель BAAS





метод системной динамики – модель «эпидемии»

Поведение и взаимосвязи!

Вопросы?

Спасибо за внимание!

Павел Литвинов,
начальник аналитического отдела

litvinov_pv@rtsoft.msk.ru

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