Международная научная школа: «Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах»

Лекция: Технологии мониторинга и управления инцидентами нового поколения для защиты информации в критически важных инфраструктурах

Котенко И.В.

д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности

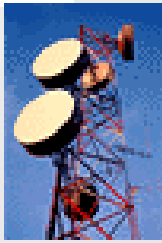
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)

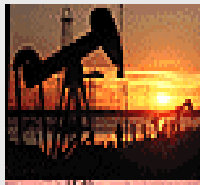
IM&CTCPA-2015, Санкт-Петербург, СПИИРАН, 26–28 ноября 2015 г.

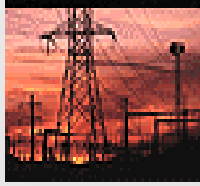
Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
- Заключение

Место и роль информационной безопасности







- Информационная безопасность в условиях глобальной информатизации общества рассматривается сегодня как одна из основных компонент национальной безопасности, определяющая все другие ее составляющие: экономическую, оборонную, социальную, экологическую и т.д.
- Информация, информационно-телекоммуникационные технологии, информационные ресурсы определяют дальнейшее развитие экономики, оборонного комплекса, социальной сферы, науки и других сфер человеческой деятельности
- С увеличением эффективности информационных технологий все более острой становится проблема обеспечения защиты информации и построения информационно-безопасных вычислительных систем

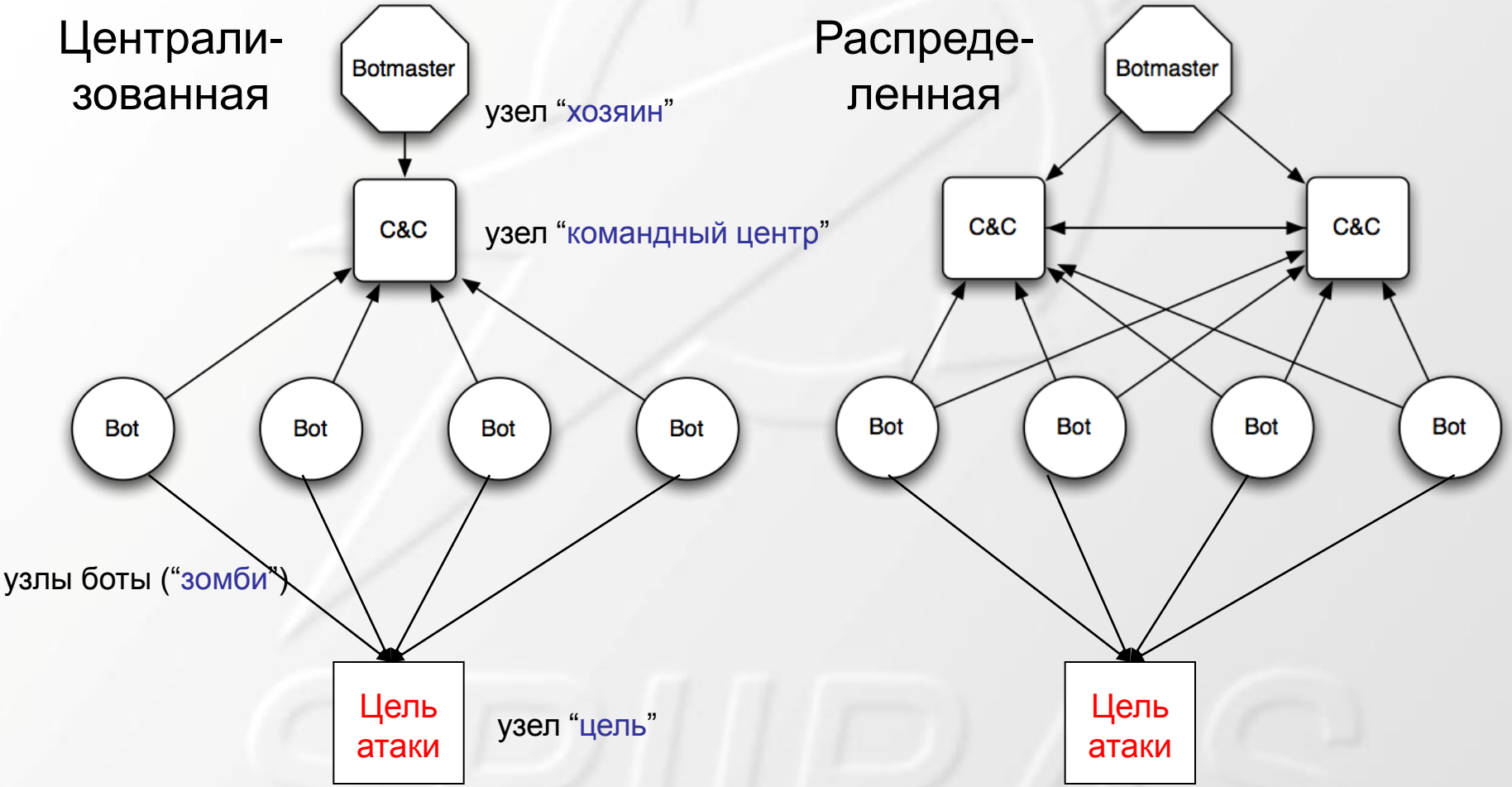
Тенденции развития средств реализации компьютерных атак

- В настоящее время мы являемся свидетелями новой фазы “гонки вооружений” между системами нападения и защиты
- Важными особенностями этого противостояния является
  - повышение уровня автоматизации, мощности, изощренности и масштабности этих систем
  - использование концепции “постоянных изощренных угроз” (APT, целевых атак) (“Изощренный” - обладание полным спектром методов разведки и компрометации. “Постоянный” - предпочтение некоторой определенной цели, постоянный мониторинг и взаимодействие с объектом атаки для достижения) и комплексной многоуровневой защиты;
  - профессиональная разработка кибероружия и средств защиты, увеличение количества субъектов (включая отдельные группы злоумышленников, корпорации и страны), осуществляющих его разработку и совершенствование.)
  - Примеры: Stuxnet -> Duqu -> Flame -> Gauss -> Red October -> Elderwood (Flamer против США) -> Duke (MiniDuke, CosmicDuke, OnionDuke. CozyDuke, ...), Naikon, Grabit, Duqu 2.0, Simda ... -> …

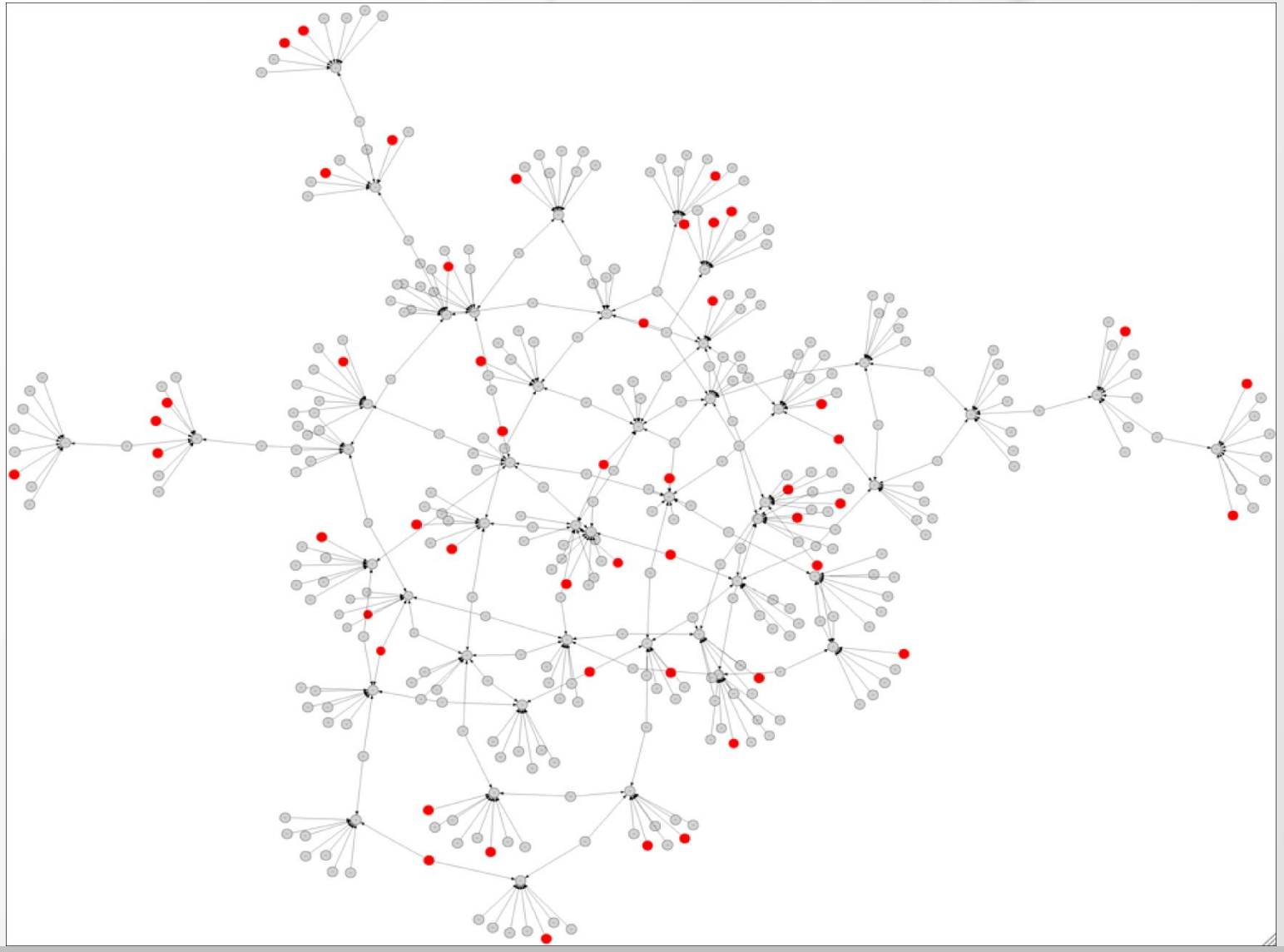
Ключевые особенности современного вредоносного ПО

- **гибкая система управления**, позволяющая минимизировать риски обнаружения и противодействия (в том числе отсутствие единого центра управления создаваемой бот-сетью — используется принцип организации, заложенный в файлообменных сетях, где каждый узел хранит информацию только о нескольких соседних и обменивается с ними командной информацией)
- **поэтапная схема инфицирования**, позволяющая до последнего момента (например, до непосредственного запуска) считать модули потенциально опасного приложения неопасными
- **модульность обновлений**, обеспечивающая возможность функциональной и структурной вариативности вплоть до формирования смешанных вредоносных программ
- **эффективные механизмы сокрытия** своего присутствия на пораженном хосте (в том числе, в активной фазе функционирования)
- **наличие активных механизмов противодействия** средствам антивирусной защиты (предполагается, что в дальнейшем усилится борьба между вирусами и антивирусами, в которой каждая сторона будет использовать методы противника)
- использование **стойких криптоалгоритмов** для взаимодействия
- использование концепции «**облачных вычислений**» …

Централизованная и распределенная структуры бот-сетей



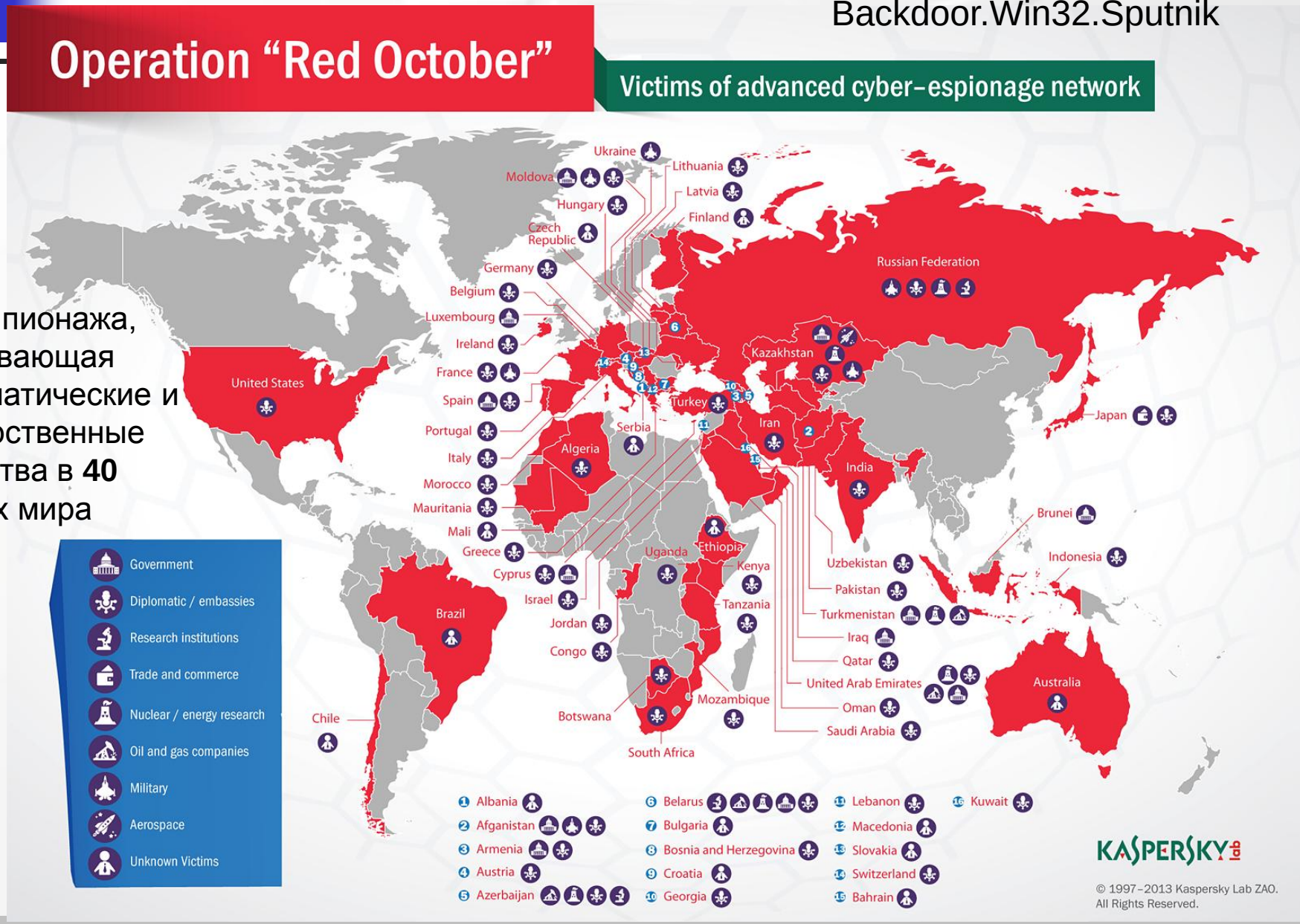
Пример топологии P2P бот-сети



Сеть кибершпионажа Red October (1/2)

Backdoor.Win32.Sputnik

Сеть кибершпионажа, охватывающая дипломатические и государственные ведомства в **40** странах мира



Сеть кибершпионажа Red October (2/2)

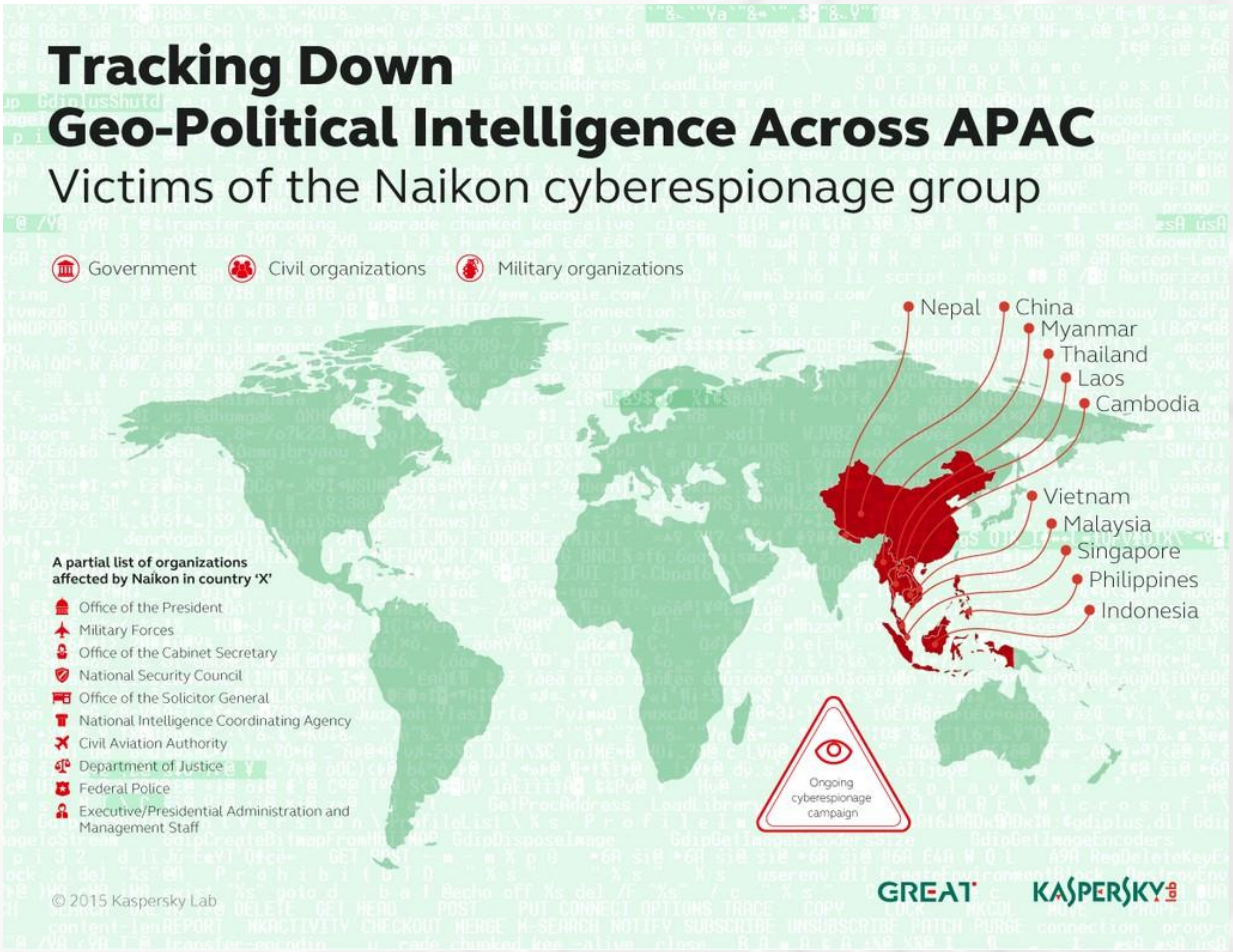
Отличительные особенности:

- **Модуль восстановления**, позволяющий преступникам «воскрешать» заражённые машины. Модуль встраивается как плагин в Adobe Reader и Microsoft Office и обеспечивает атакующим повторный доступ к системе в случае, если основная вредоносная программа была детектирована и удалена или если произошло обновление системы.
- **Усовершенствованные криптографические шпионские модули, предназначенные для кражи информации**, в том числе из различных криптографических систем, например, из Acid Cryptofiler, которая используется с 2011 года для защиты информации в таких организациях, как НАТО, Европейский Союз, Европарламент и Еврокомиссия.
- **Возможность инфицирования мобильных устройств**: Помимо заражения традиционных рабочих станций это вредоносное ПО способно красть данные с мобильных устройств, в частности смартфонов. Также злоумышленники могли красть информацию о конфигурации с сетевого промышленного оборудования (маршрутизаторы, коммутационные устройства) и удалённые файлы с внешних USB-накопителей.

CozyDuke

- Атака проводится с использованием ряда технологий, таких как шифрование, защита от обнаружения антивирусными программами и др.
- Для получения плацдарма для атаки используются методы социальной инженерии.
- Первый вариант - письма содержат ссылку на взломанные сайты с ZIP-архивом, который содержит самораспаковывающийся RAR-архив, который устанавливает вредоносное ПО, показывая пустой PDF-файл в качестве приманки. Второй вариант – отправка в качестве вложений к письмам флеш-видео, содержащих исполняемый вредоносный код.

Naikon



- Пользователь получает письмо с вложением документа Word. Это исполняемый файл с двойным расширением или с именем, созданным с помощью приема Right-to-Left Override для маскировки расширения файла.
- Если пользователь откроет файл, тот устанавливается шпионское ПО и выводится на экран текст документа – подсадной утки, так чтобы не возникло подозрений.
- Главный модуль Naikon представляет собой утилиту удаленного администрирования (48 команд).

Hellsing

- эта группировка стала объектом целевого фишинга со стороны Naikon и нанесла ответный удар!
- Получив электронное сообщение, адресаты просили отправителя подтвердить авторство адресной рассылки. Они получили ответ атакующего, но вложение открывать не стали.
- Вместо этого через некоторое время они отправляли письмо обратно атакующим с вредоносной программой.

Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
- Заключение

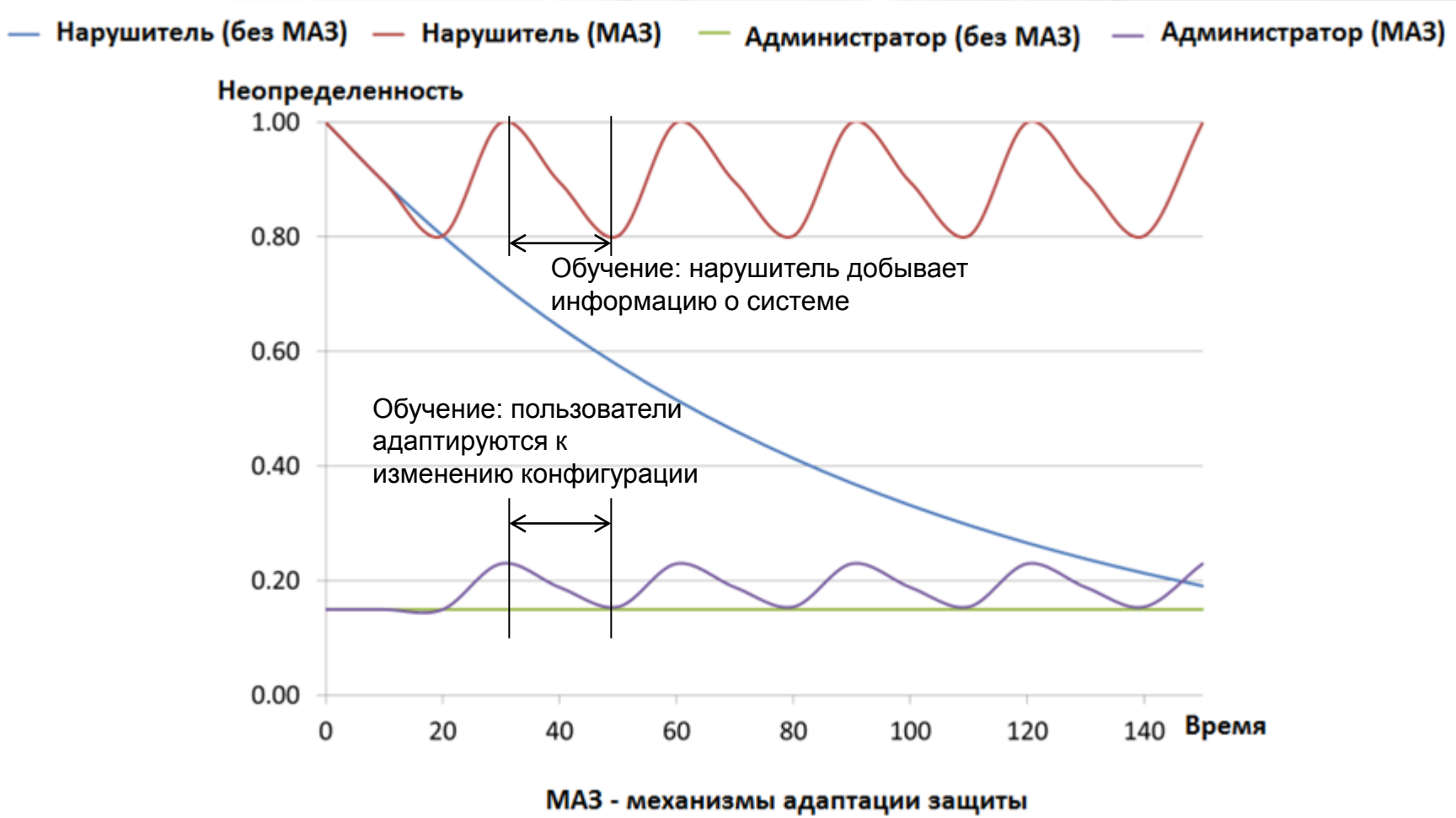
Используемые в настоящее время механизмы защиты - статичны

- Используемые в настоящее время механизмы защиты – реализуются медленно
  - Выполнение патчей, тестирование, эпизодические тесты на проникновение, мониторинг событий безопасности, основанный на принятии решения администратора
- Нарушители извлекают большую пользу из этой ситуации
  - Они могут непрерывно и систематически исследовать целевые хосты и сети с уверенностью, что их конфигурация будет изменяться медленно или совсем не изменяться
  - Они обладают достаточным временем для создания необходимых эксплоитов и тщательного планирования атак
- Кроме того, при успешной реализации атаки, нарушители могут длительное время выполнять необходимые действия на скомпрометированных хостах и сетях
  - Хосты, сети, программное обеспечение и сервисы не реконфигурируются и не изменяются, за исключением запланированных процедур технического обслуживания и регламента

Необходимость внедрения интеллектуальных адаптивных средств защиты

- многообразие возможных угроз безопасности (видов атак на информационную инфраструктуру);
- высокая критичность последствий реализации угроз информационной безопасности
- большая ответственность за выработку и реализацию контрмер по обеспечению информационной безопасности;
- ограниченность времени на принятие решений по защите информации (реальный масштаб времени или близкий к нему);
- большой масштаб объекта защиты информации;
- неполнота и противоречивость исходных данных;
- необходимость обнаружения целевых атак;
- необходимость проактивной адаптивной защиты информации (основанной на способности предвидеть намерения и поведения атакующего)

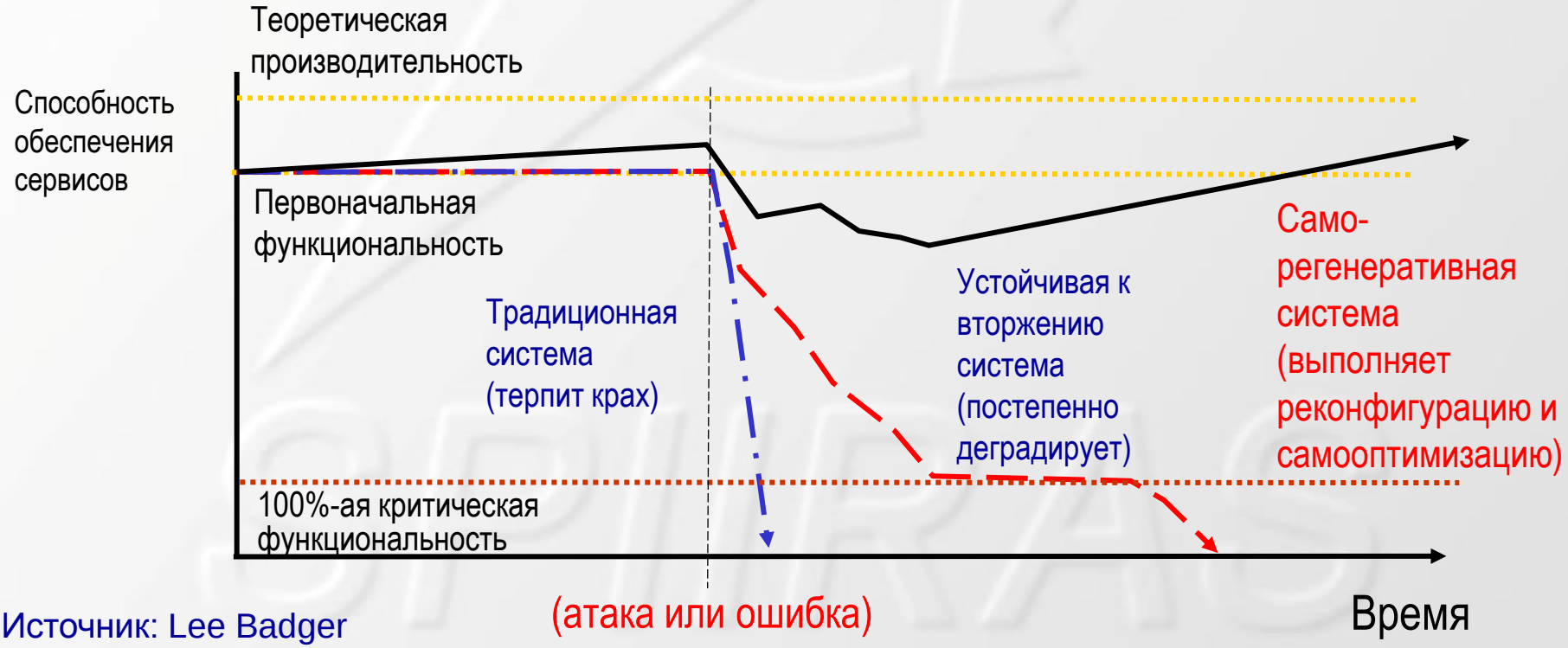
Неопределенность знаний нарушителя и администратора защиты



Источник: Sushil Jajodia

Саморегенеративные системы

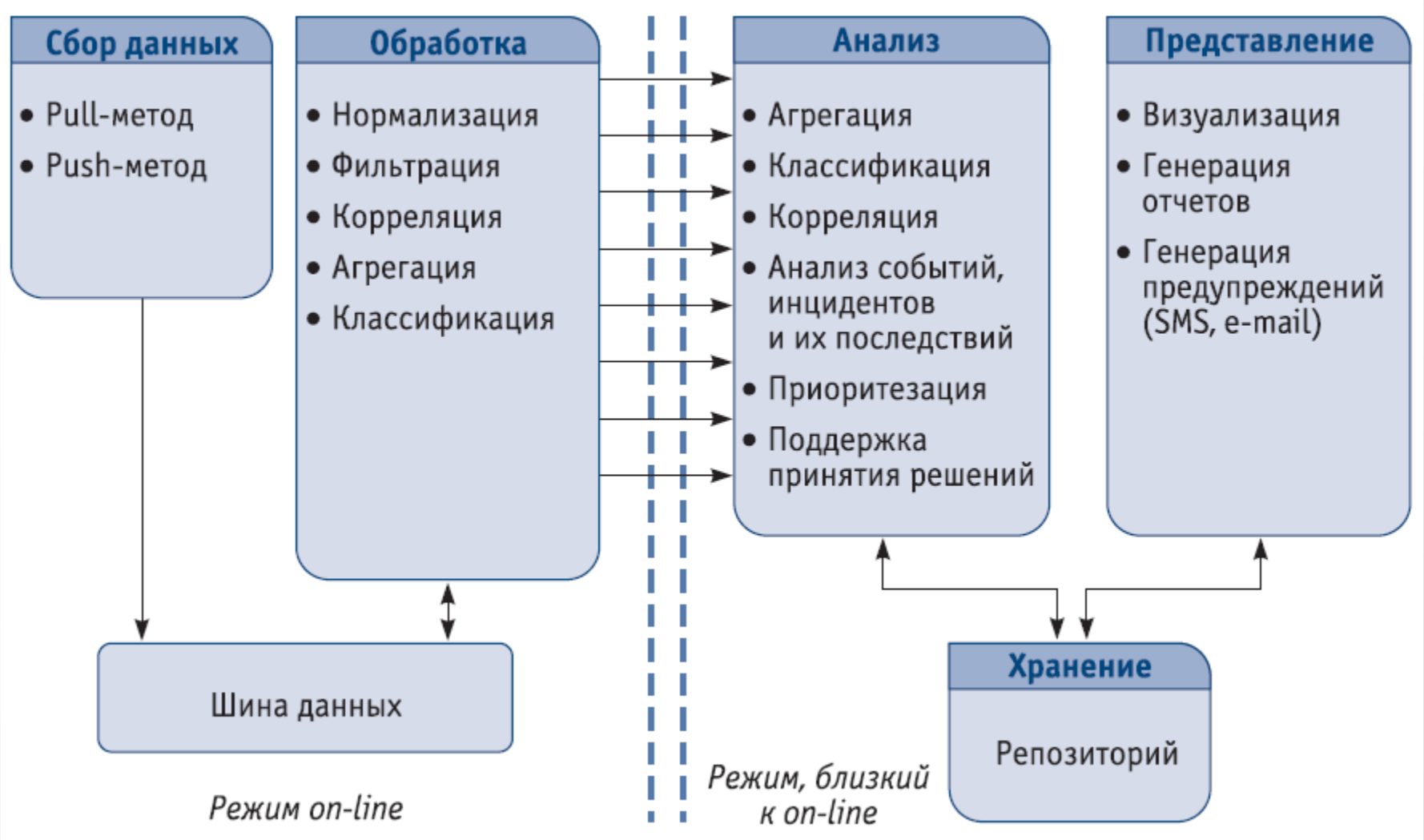
- Обеспечить 100% критических функций в течение всего времени функционирования в условиях реализации атак.
- Обнаруживать собственные уязвимости для повышения живучести в процессе функционирования.
- Восстанавливать сервисы после атаки.



Источник: Lee Badger

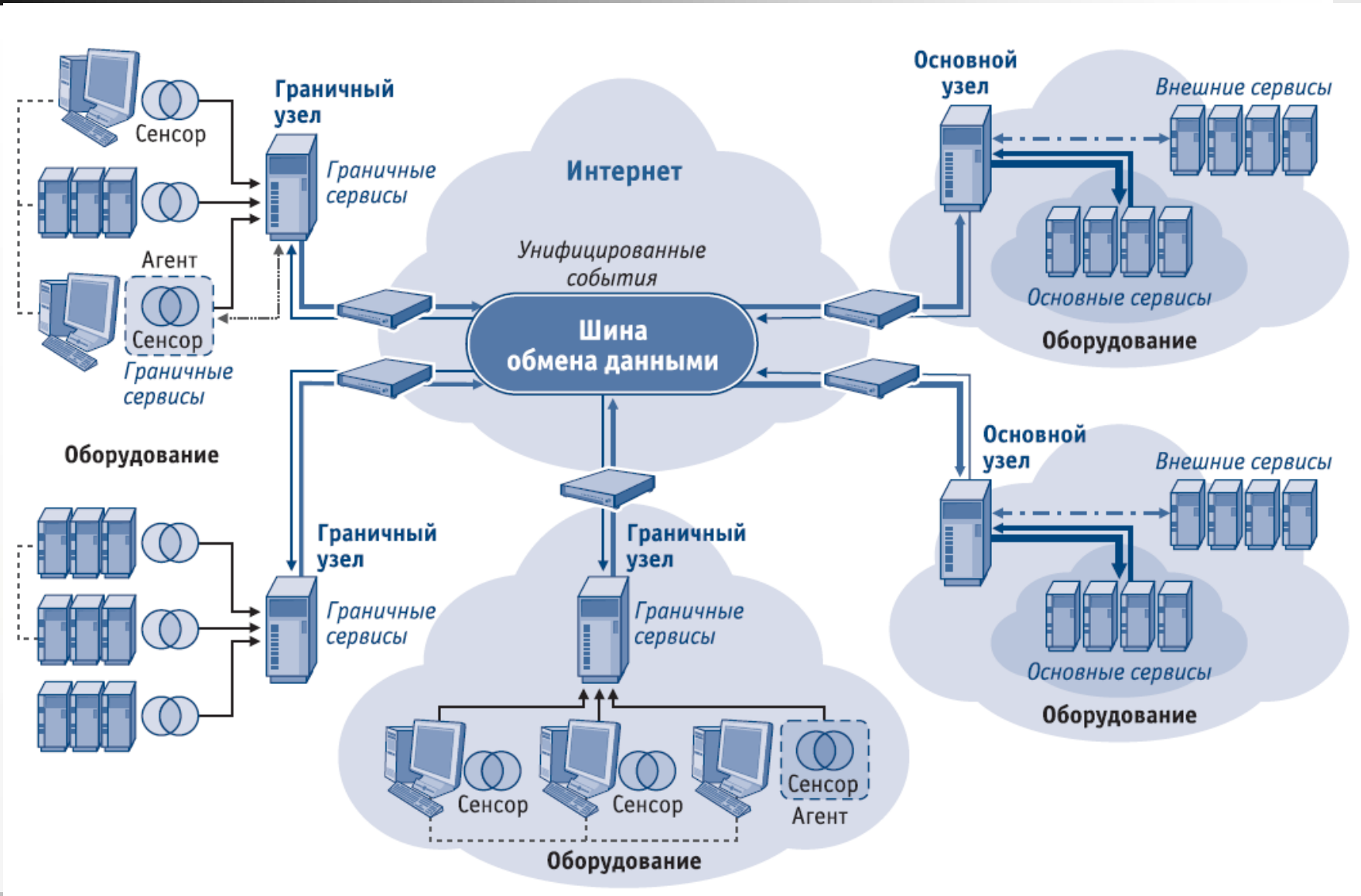
Иерархия механизмов обработки информации

Функциональная модель взаимодействия механизмов обработки информации



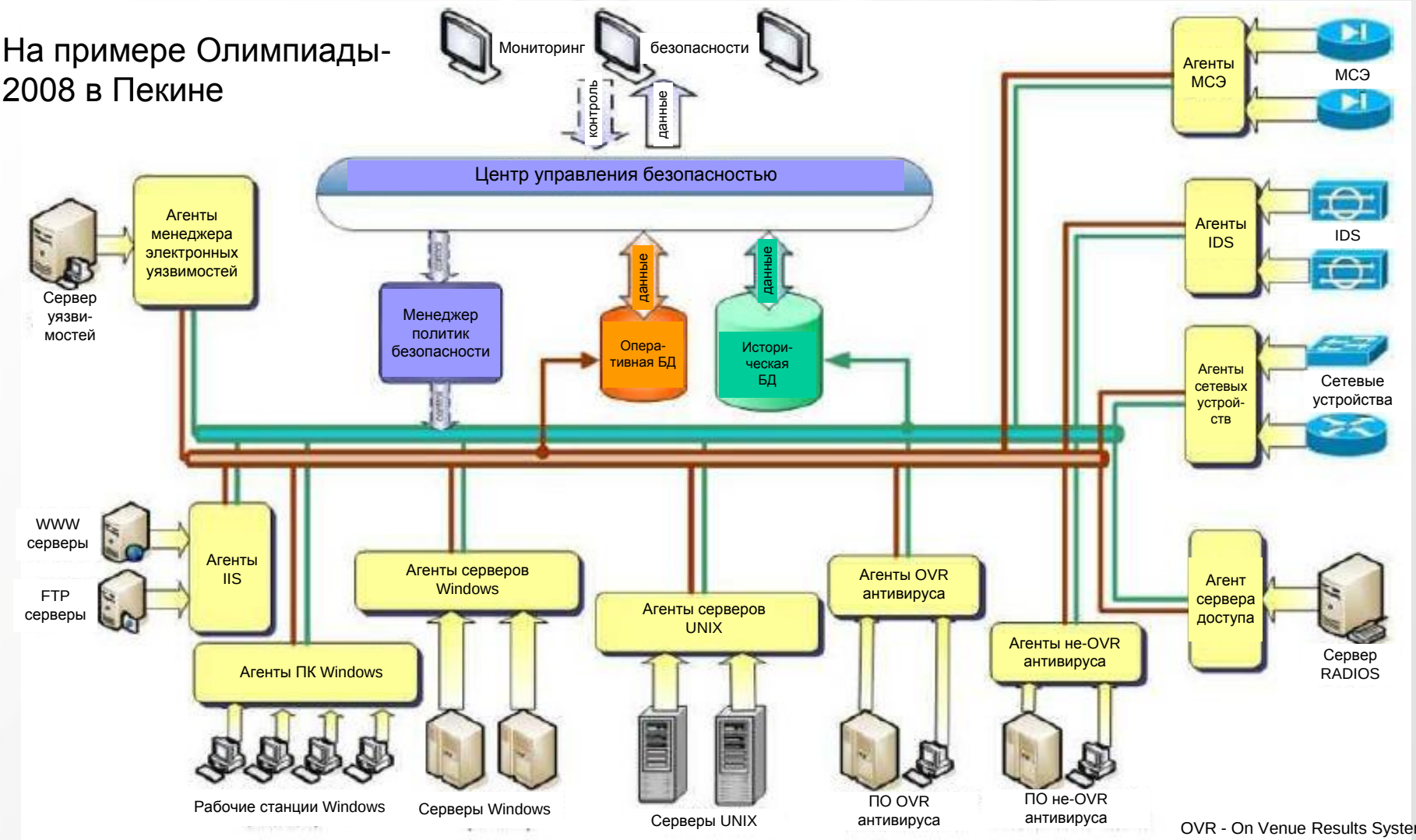
Уровни обработки информации

Обобщенная архитектура системы мониторинга и управления безопасностью



Сценарий 1. Инфраструктура проведения Олимпийских игр

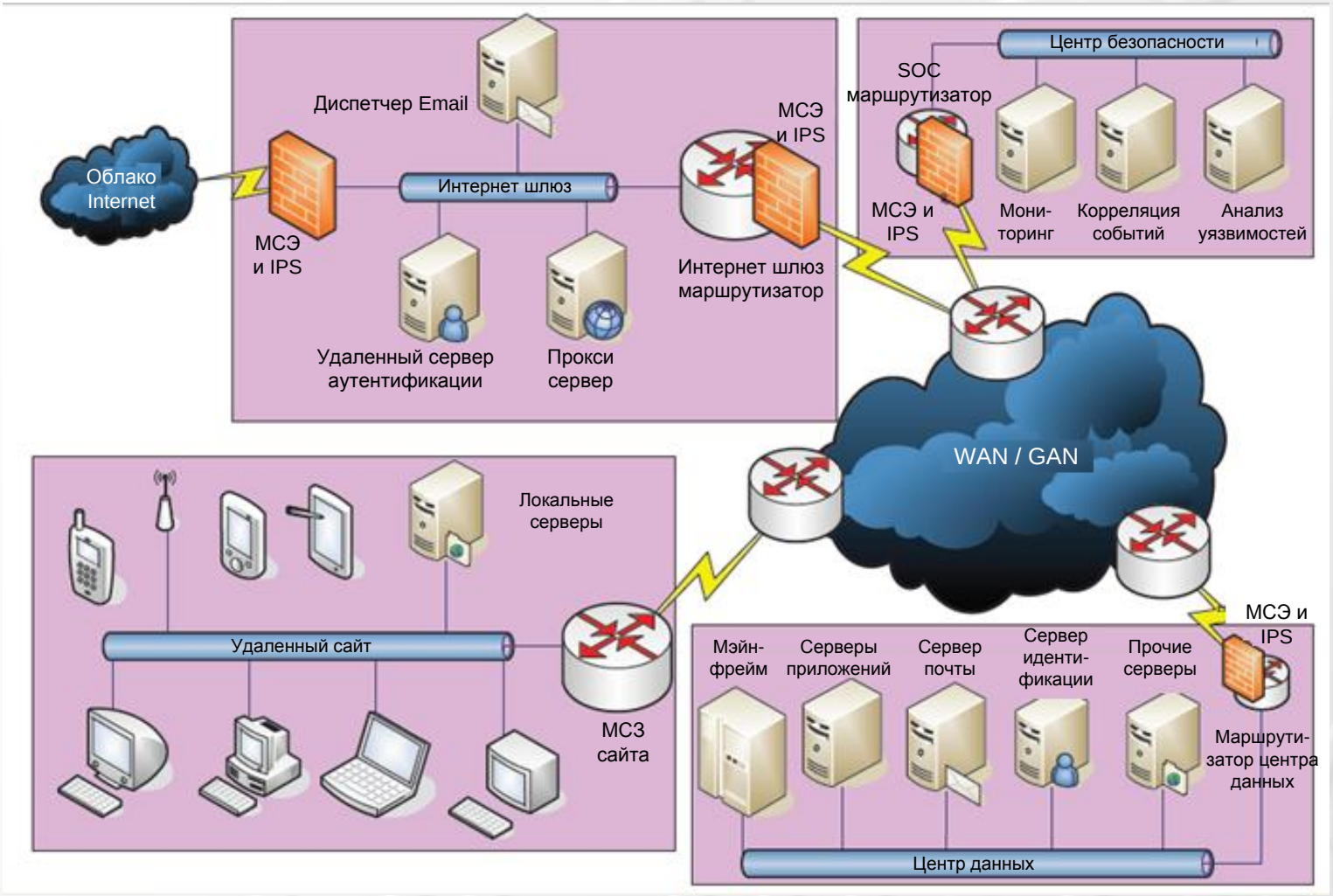
На примере Олимпиады-2008 в Пекине



OVR - On Venue Results Systems

Размерность: **20 000** типов событий безопасности; **10 000 000** пред./день; **40 000** компонентов; **35 000** пользователей

Сценарий 2. Инфраструктура сервисов управления предприятием



Проблема:

1) Противостояние массовым атакам

2) Низкая достоверность исходных данных

3) Неадекватные механизмы аварийного восстановления

Вклад: совершенствование механизмов корреляции событий на основе повышения эффективности управления событиями и данными безопасности

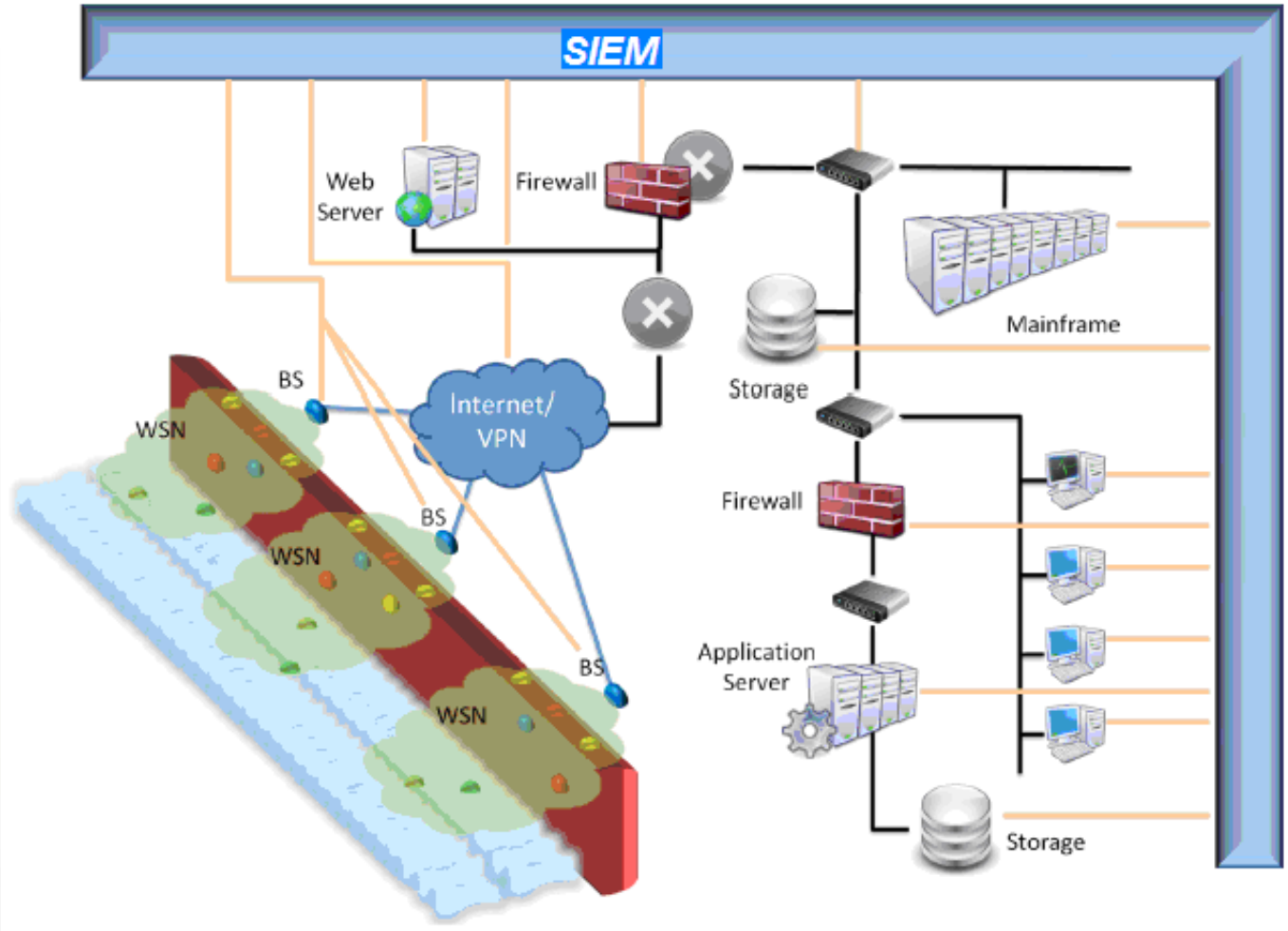
Сценарий 3. “Мобильные деньги”

Проблема: сервис подвержен риску отмывания денег и другим видам мошенничества.

Задача: защитить сервис от попыток мошенничества с помощью их обнаружения и принятия соответствующих контрмер.

Вклад: корреляция событий на разных уровнях и между уровнями

Сценарий 4. Управление процессами в критической инфраструктуре (Дамба)



Проблема:

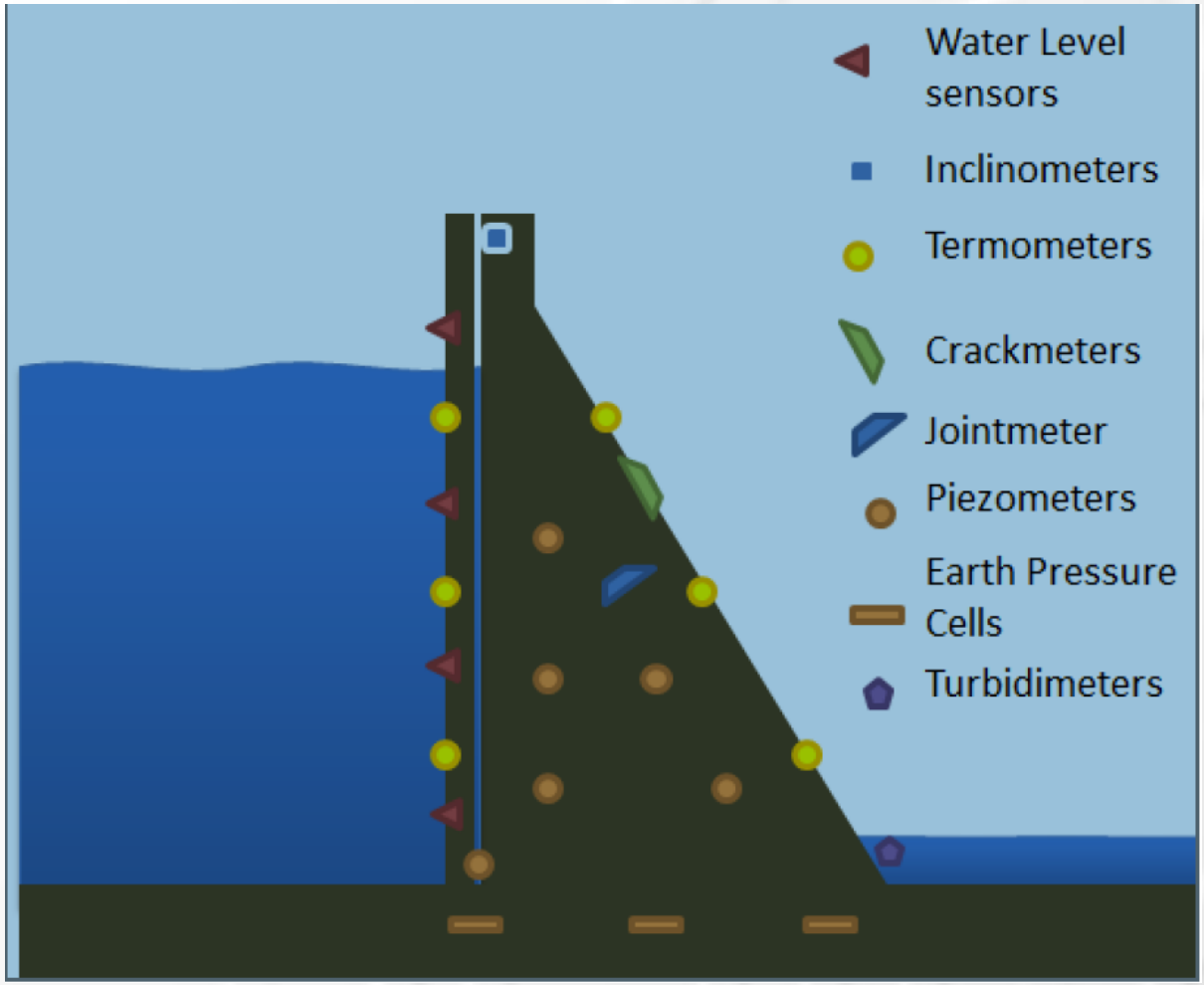
1) распознать реальные угрозы на основе множества предупреждений

2) Надежность источников данных

Задача: контроль важнейших объектов критической инфраструктуры (на примере плотины)

Вклад: на основе корреляции событий иметь полное представление обо всех потенциально критических событиях безопасности

Датчики и сенсоры для сценария 4



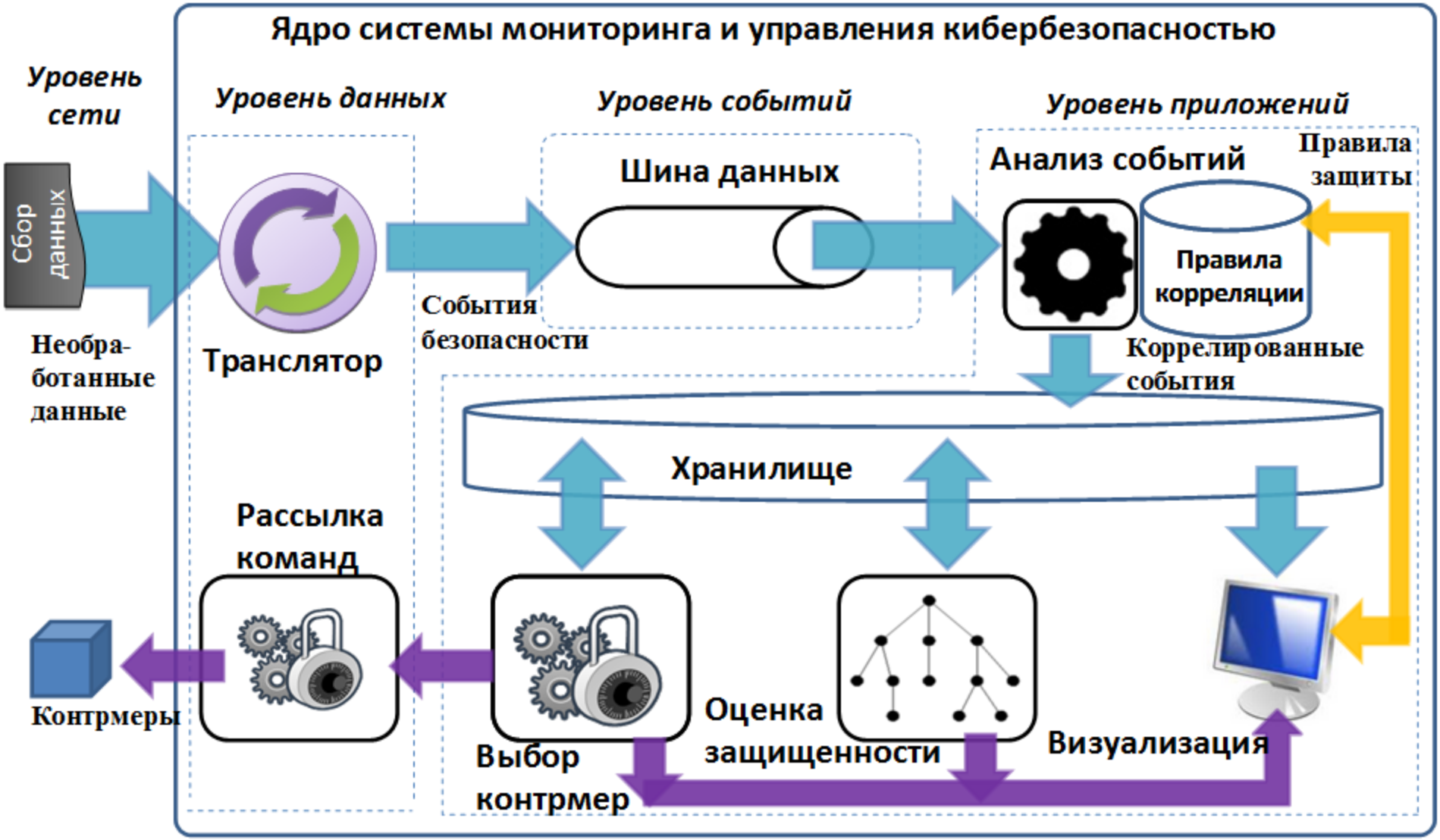
Постоянно контролируемые параметры:

1) физическая структура плотины является стабильной, т.е. она не собирается падать в ближайшее время;
2) нет утечки в настоящее время;
3) вода чистая (в частности, не загрязняется, а также не была отравлена);
4) вода ниже предопределенного уровня безопасности;
5) открытость шлюзов;
6) метеорологические данные (температура, давление, влажность, ветер, дождь);
7) вибрация плотины.

Новые возможности следующего поколения систем мониторинга и управления кибербезопасностью

- межуровневая корреляция событий безопасности, поступающих из различных неоднородных источников
- адаптивная высоко масштабируемая обработка событий, обеспечивающая управление большими объемами данных о безопасности в реальном или близком к реальному времени
- прогностический анализ безопасности, позволяющий осуществлять проактивное обнаружение и предотвращение атак путем принятия соответствующих контрмер
- высокая доступность и отказоустойчивость сбора данных о событиях безопасности и доведения решений в условиях территориально-распределенного характера построения защищаемой инфраструктуры и активного вредоносного и/или непреднамеренного воздействия на каналы связи
- Выработка контрмер в реальном времени

Представление системы мониторинга и управления кибербезопасностью



Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
- Заключение

Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
  - Сервисы аналитического моделирования
  - Сервисы анализа защищенности
  - Сервисы визуализации
- Заключение

Основные причины использования моделей атак

- Вычисление возможных последовательностей (трасс) атак, и упреждающее определение целей безопасности, которые с наибольшей вероятностью станут мишенью для нарушителя
- Корреляция последовательностей событий безопасности, т.к. они относятся к определенным действиям внутри модели атак
- Определение показателей защищенности
- Определение соответствующих наборов контрмер, т.е. действий, предпринимаемых системой, чтобы разрушить непрерывную последовательность действий атакующего
- Динамическое вычисление воздействия атак и контрмер: атак - когда они нарушают политику безопасности, и контрмер - когда они изменяют конфигурацию системы

Базовые работы по моделированию атак для анализа механизмов защиты (1/2)

- Проверка на модели (C.Ramakrishnan и R.Sekar, R.Ritchey и P.Ammann, O.Sheyner, S.Jha и J.Wing – SMV, NuSMV, SPIN). Требуют определить гипотезу (состояние системы), нарушение которой проверяется методом model checking
- Экспертные системы (M.Danforth – Java Expert System Shell). Правила – выполнение атакующих действий, факты – состояния системы. Атаки в виде предусловия/постусловия
- Логический подход (X.Ou, W.Boyer, M.McQueen – Datalog language). Граф состоит из вершин вывода и вершин фактов. Модель сети – множество высказываний Datalog, атаки – правила Datalog
- Графы атак. Например C.Philips и L.Swiler строят граф: вершины – состояния системы, дуги – переходы [Ortalo et al., 1999; Ritchey&Ammann, 2000; Sheyner et al., 2002; Rieke, 2004; Noel&Jajodia, 2005; Lippmann&Ingols, 2006; …]

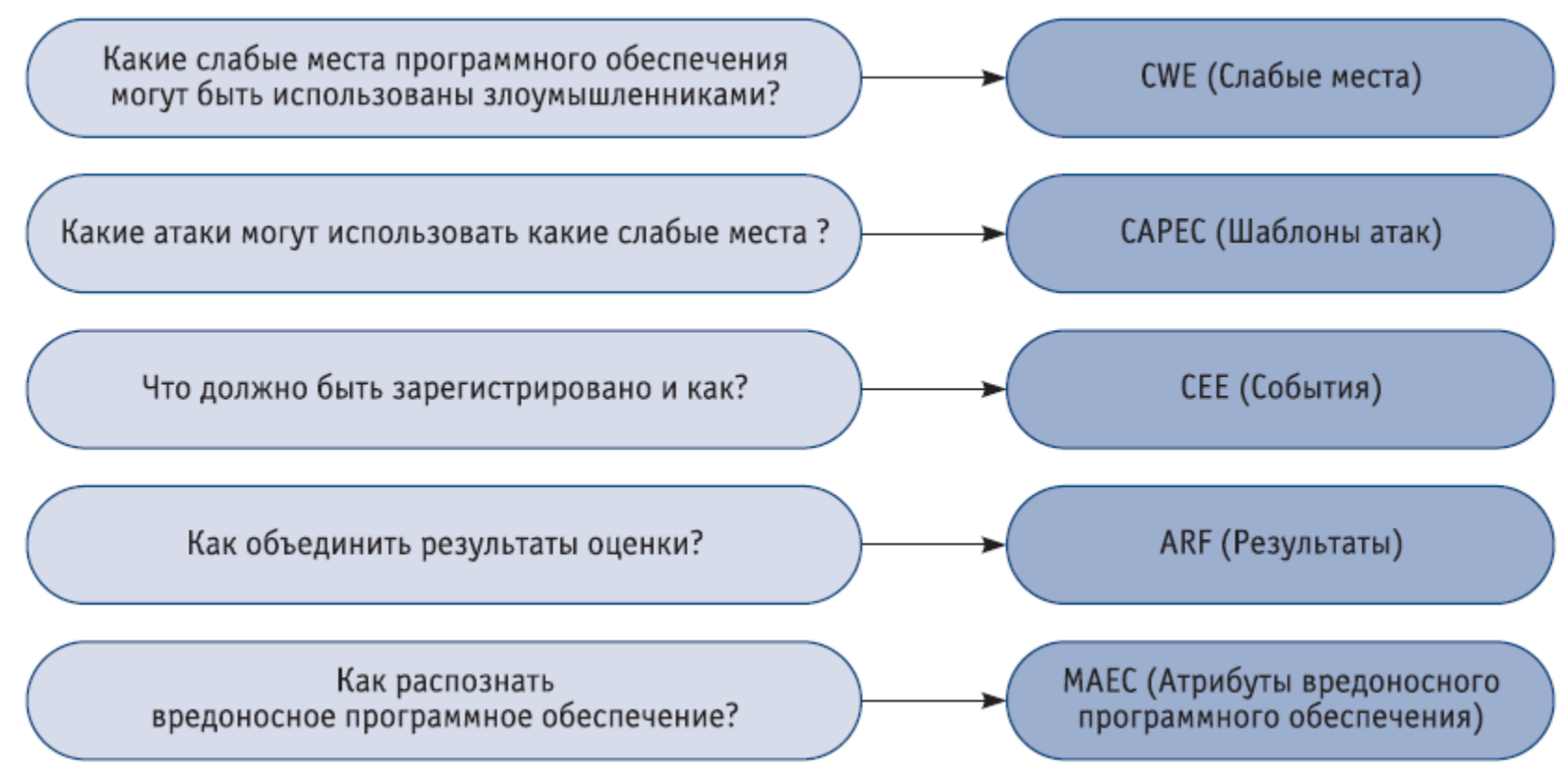
Базовые работы по моделированию атак для анализа механизмов защиты (2/2)

- Представление сценариев атак и моделей нарушителей [Schneier, 1999; Dawkins et al., 2002; Shepard et al., 2005; …]
- Спецификация платформ, уязвимостей, оценок уязвимостей, атак, слабостей и конфигураций [NVD; OSVDB; CVE; CVSS; CPE; CCE; CWE; CAPEC; …]
- Показатели защищенности [Mell et al., 2007; Jaquith, 2007; Herrmann, 2007; Jansen, 2009; …]
- Комбинирование графов зависимостей сервисов и графов атак [Kheir et al., 2009; Kheir et al., 2010; …]
- Представление атак нулевого дня [Ingols et al., 2009; Wang et al., 2010; …]
- Моделирование контрмер [Kheir et al., 2010; …]

Примеры используемых стандартов (1/2)

Какие информационные системы используются на предприятии?	CPE (Платформы)
О каких уязвимостях необходимо позаботиться?	CVE (Уязвимости)
О каких уязвимостях необходимо позаботиться НЕМЕДЛЕННО?	CVSS (Система оценки)
Как сформировать наиболее защищенную конфигурацию системы?	CCE (Конфигурации)
Как определяется политика защищенных конфигураций?	XCCDF (Контрольные списки конфигураций)
Как убедиться, что системы удовлетворяют политике?	OVAL (Язык оценки)
Как убедиться, что работа систем удовлетворяет политике?	OCIL (Язык взаимодействия)

Примеры используемых стандартов (2/2)



Общий подход к моделированию атак и анализу защищенности

Модуль хранения данных

Внешние источники

Спецификация системы
Хосты, политики безопасности, сетевая топология

Оператор
Требования к безопасности, модель нарушителя

Генерация модели атак

Уязвимости нулевого дня, известные уязвимости

Топологический анализ уязвимостей

Зависимости сервисов

Анализ атак

Стохастическое моделирование

Показатели защищенности
Возможные последствия атак, эффективность контрмер

Слабые места сети

Поддержка принятия решений

Генерация возможных контрмер

Выбор контрмер

Формирование отчета

Оценка контрмер

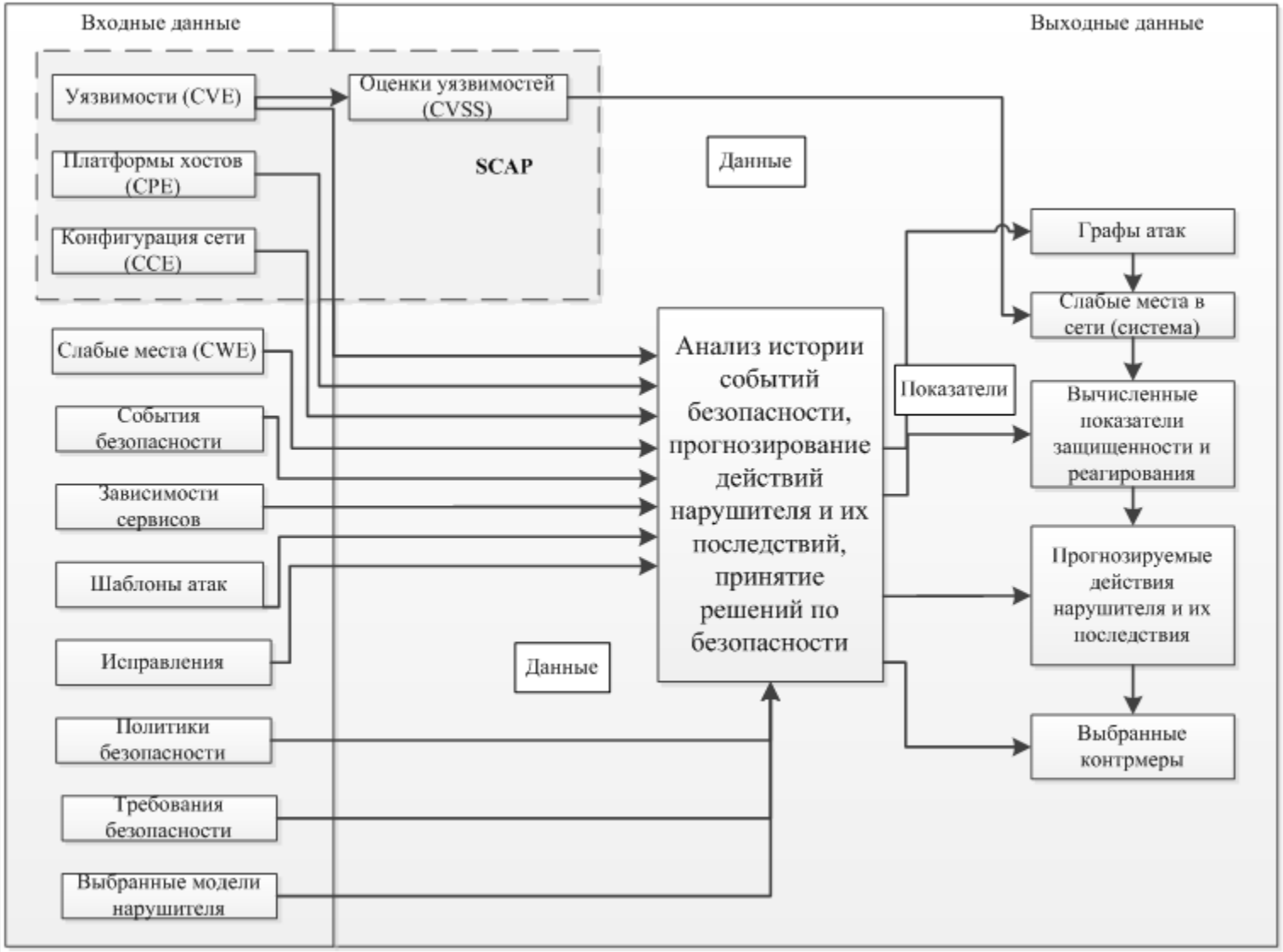
Особенности предлагаемых решений (1/2)

- Использование репозитория безопасности (содержащего данные о конфигурации системы, моделях нарушителя, уязвимостях, атаках, оценках, контрмерах и др.)
- Эффективные методики генерации графов атак и зависимостей сервисов, базирующиеся на методиках топологического анализа уязвимостей (TVA), которые формируют потенциальные последовательности использования уязвимостей для построения графов атак
- Учет как известных, так и новых атак, основанных на уязвимостях 0-го дня
- Применение anytime-алгоритмов для обеспечения близкого к реальному времени генерации подграфов атак и процедур анализа защищенности (anytime-алгоритм - итерационный вычислительный алгоритм, который способен выдать наилучшее на данный момент решение)

Особенности предлагаемых решений (2/2)

- Комбинированное использование графов атак и графов зависимостей сервисов
- Вычисление комплекса разнообразных показателей защищенности, включая следующие показатели:
  - уровень защищенности,
  - уровень воздействия и потенциал атаки,
  - уровень навыков нарушителя,
  - эффективность контрмер,
  - степень побочных потерь при реализации контрмер и др.
- Стохастическое аналитическое моделирование и интерактивная поддержка принятия решений для выбора предпочтительных решений по безопасности на основе определения предпочтений относительно различных типов целей и требований (рисков, стоимости, выигрыша) и установления компромиссов между высокоуровневыми целями защиты информации

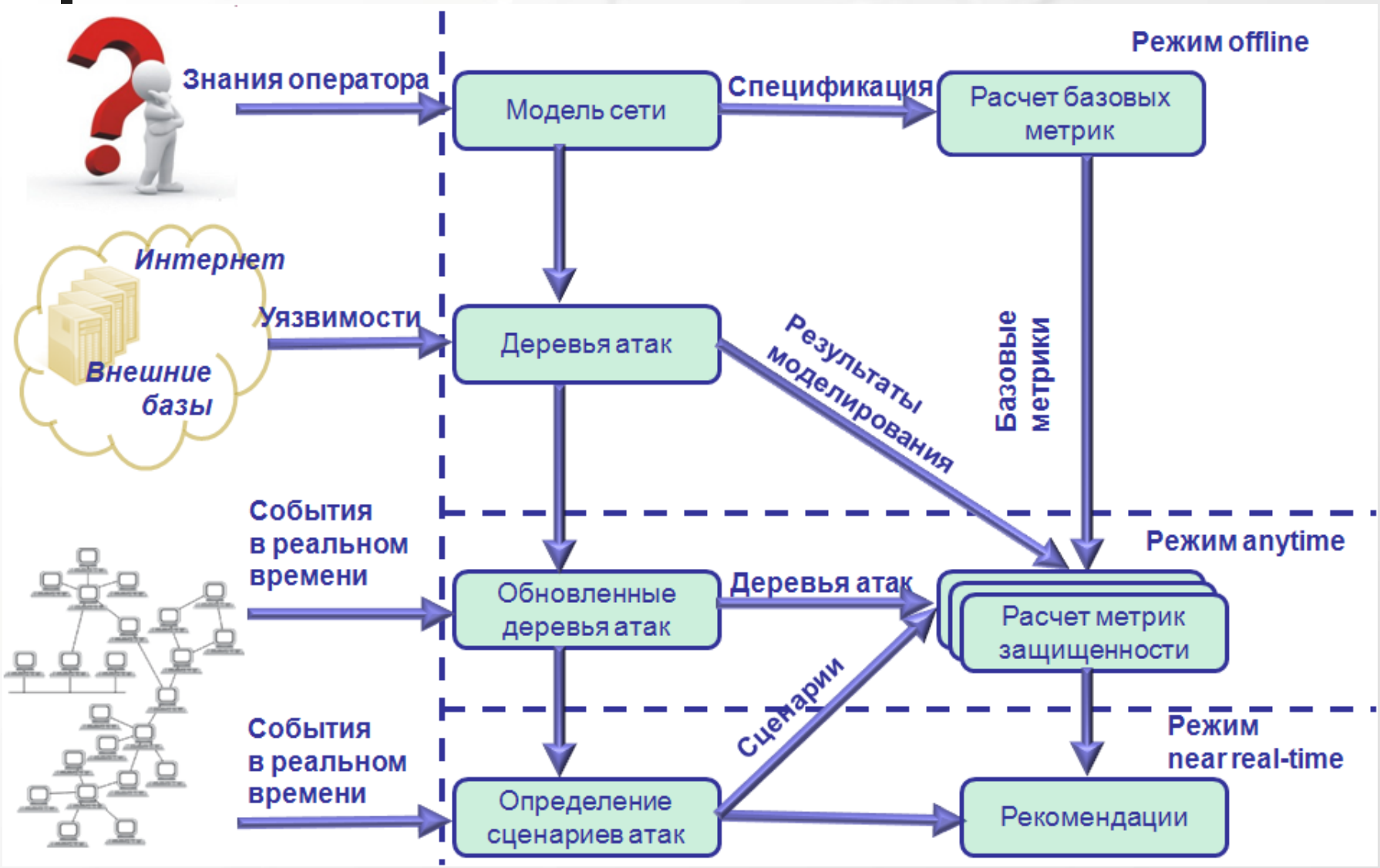
Входные и выходные данные системы оценки защищенности



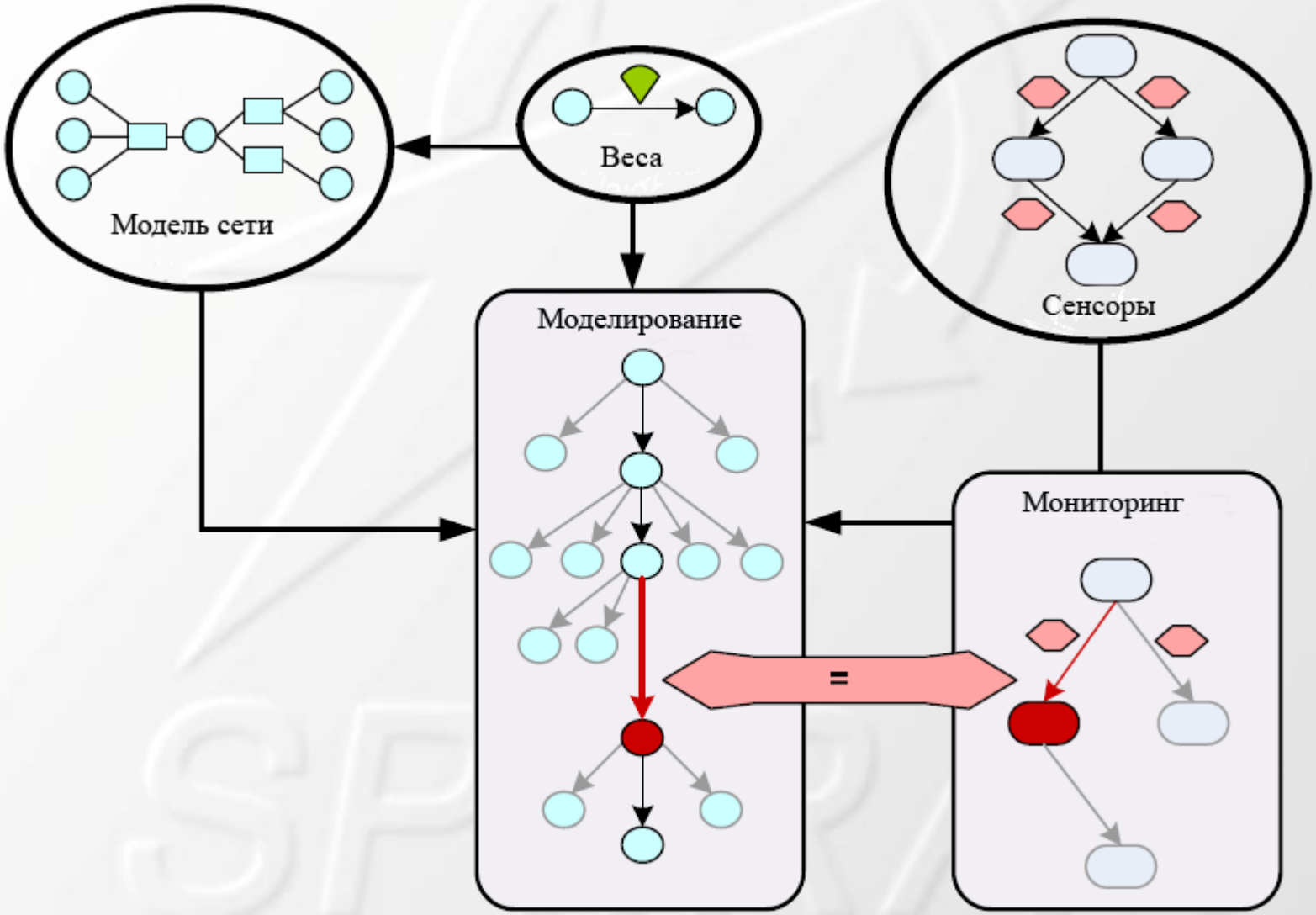
Этапы работы системы моделирования

- **Этап разработки и ввода в эксплуатацию (не real-time)**
  - Определение слабых мест в сети
  - Формирование базовых графов атак
  - Расчет метрик безопасности защищаемой сети
  - Формирование списка наиболее опасных уязвимостей нулевого дня
- **Этап эксплуатации (near real-time)**
  - Обновление хранимых графов атак для соответствия изменениям, происходящим в сети
  - Оценка возможных мероприятий по увеличению уровня защиты
  - Предсказание действий нарушителя
  - Обратный анализ действий нарушителя

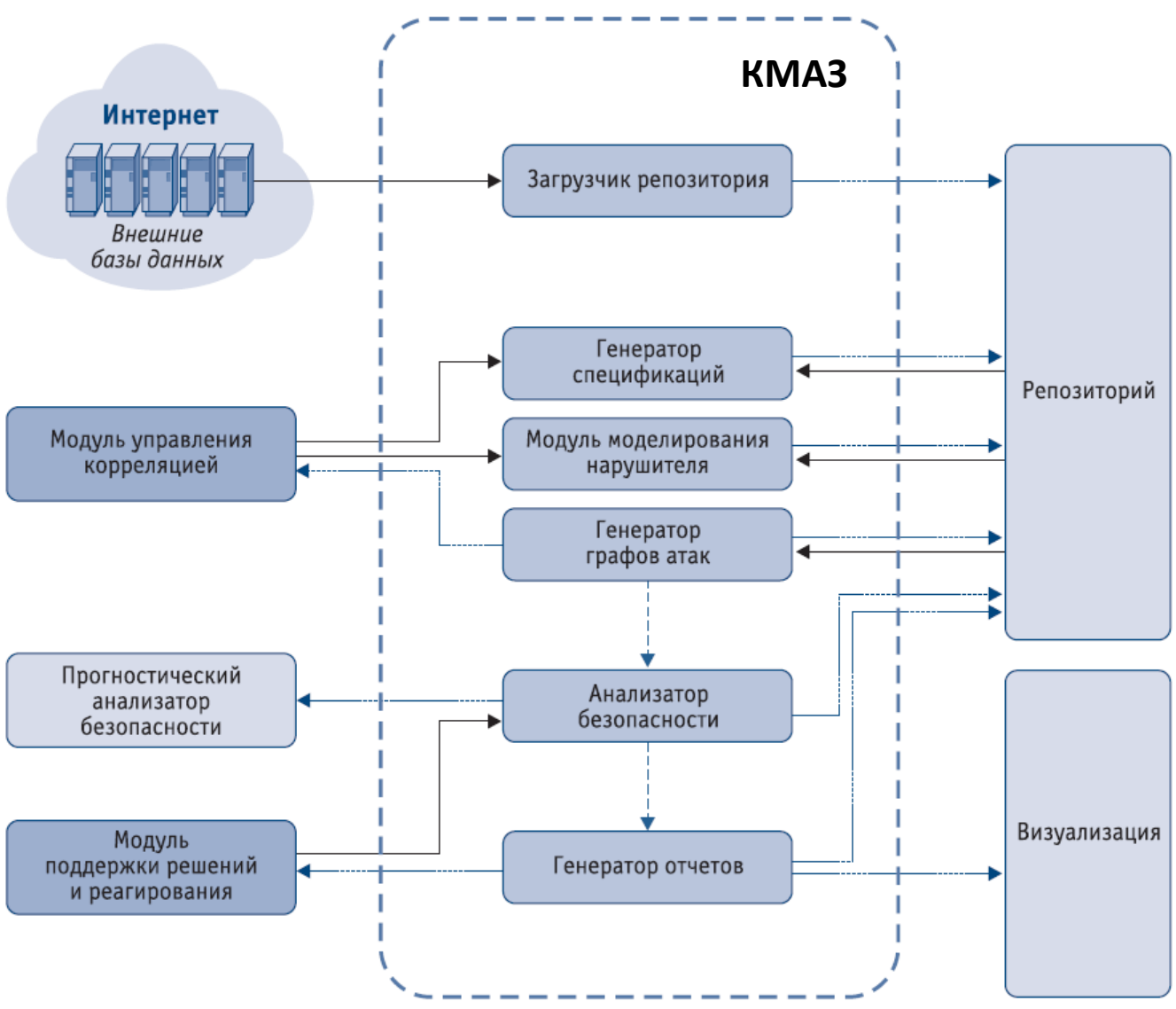
Режимы работы



Анализ событий



Архитектура компонента аналитического моделирования



Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
  - Сервисы аналитического моделирования
  - Сервисы анализа защищенности
  - Сервисы визуализации
- Заключение

Уровни оценки защищенности

Показатели CVSS (Common Vulnerability Security Scoring)

Показатели базовой оценки
(Base Metrics)

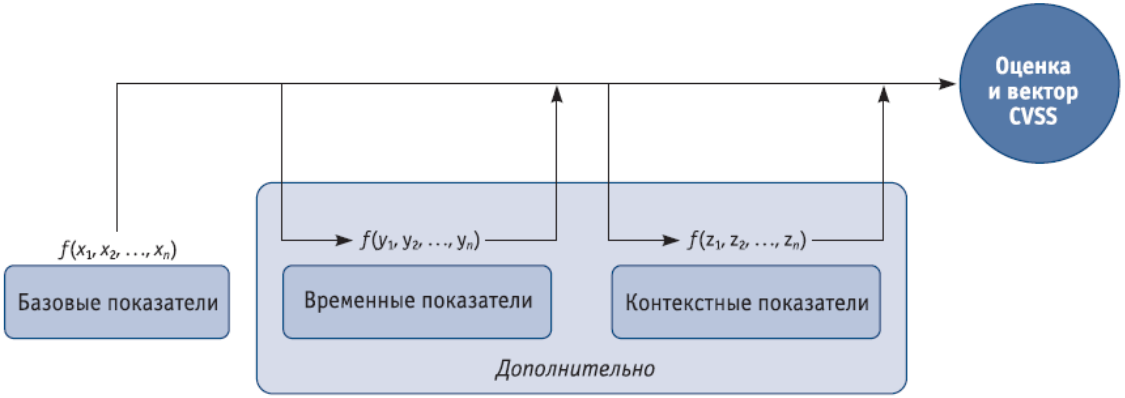
- Вектор доступа (AccessVector)
- Влияние на конфиден-циальность (ConfImpact)
- Сложность доступа (AccessComplexity)
- Влияние на целостность (IntegImpact)
- Аутентификация (Authentication)
- Влияние на доступность (AvailImpact)

Показатели временной оценки
(Temporal Metrics)

- Возможность использования (Exploitability)
- Уровень исправления (Remediation Level)
- Достоверность отчета (ReportConfidence)

Показатели контекстной оценки
(Environmental Metrics)

- Вероятность косвенного ущерба (CollateralDamage)
- Требование конфиден-циальности (ConfReq)
- Плотность целей (TargetDistribution)
- Требование целостности (IntegReq)
- Требование доступности (AvailReq)



- http://www.first.org/cvss/
- CVSS v.3. - March 15th, 2013

Показатели защищенности (1/3)

1. **Показатели топологии** **[Mayer, 2007; Mell et al., 2007; CIS, 2009]**
   - Показатели, характеризующие хосты и их связность: *Критичность хоста (ущерб для бизнеса от потери хоста), Незащищенность (определяется достижимостью хоста и простотой использования его уязвимостей), Ценность для бизнеса (то же, что и Критичность), Риск (определяется на основе Незащищенности и Ценности для бизнеса) и Нисходящий риск (кумулятивный риск, проходящий через все хосты, атакуемые с данного хоста).*
   - Топологические характеристики с точки зрения приложений: *Количество приложений, Процент критичных приложений.*
   - Топологические характеристики, учитывающие информацию об уязвимостях: *Процент систем без известных критичных уязвимостей, Среднее время на устранение уязвимости, Количество известных уязвимостей.*
   - Топологические характеристики, учитывающие информацию об атаках: *Критичность уязвимости и Сложность доступа уязвимости, позволяющие вычислить Вероятность атаки.*

Показатели защищенности (2/3)

2. Показатели нарушителя

[Kanoun et al., 2008; Dantu et al., 2009; Olsson, 2009]:

Уровень навыков нарушителя (Attacker Skill Level), определяемый на основе вероятностей и исторических данных (статический подход) и (или) на основе событий, происходящих в системе (динамический подход).

[Wheeler& Larson, 2003; Hunker et al., 2008; Blakely, 2012]:

атрибуты нарушителя (Attack attribution) - имя, инструменты, географическое положение, мотивы.

3. Показатели атаки и контрмер

[Kanoun et al., 2009; Stakhanova et al., 2007; Wu et al., 2007]:

Потенциал атаки (Attack potentiality) показывает, как близко находится нарушитель к своей цели.

Влияние (ущерб от) атаки (Attack impact) – может быть определен для каждого узла на графе атак статически или динамически на основе зависимостей сервисов.

[Toth&Kruegel, 2002; Balepin et al., 2003; Jahnke, 2009; Kheir, 2010; Kheir et al., 2010; Kheir&Viinikka, 2011; D4.3.1, 2011]:

показатели, связанные с контрмерами - *Эффективность реагирования, Выигрыш при реагировании, Побочные потери при реагировании.*

Показатели защищенности (3/3)

4. Интегральные показатели

[Howard et al., 2003; Manadhata&Wing, 2004; Manadhata et al., 2007; Manadhata&Wing, 2010]: *Поверхность атаки (Attack Surface)* определяется на основе отношения потенциала разрушений к затратам.

[**Kotenko&Stepashkin, 2006-1; Dantu et al., 2009; Poolsappasit et al., 2012**]: *Уровень риска (Risk Level).*

5. Анализ стоимости-выигрыша [Hoo, 2000; Kheir et al., 2010; AlienVault, 2011; D5.2.1, 2012]

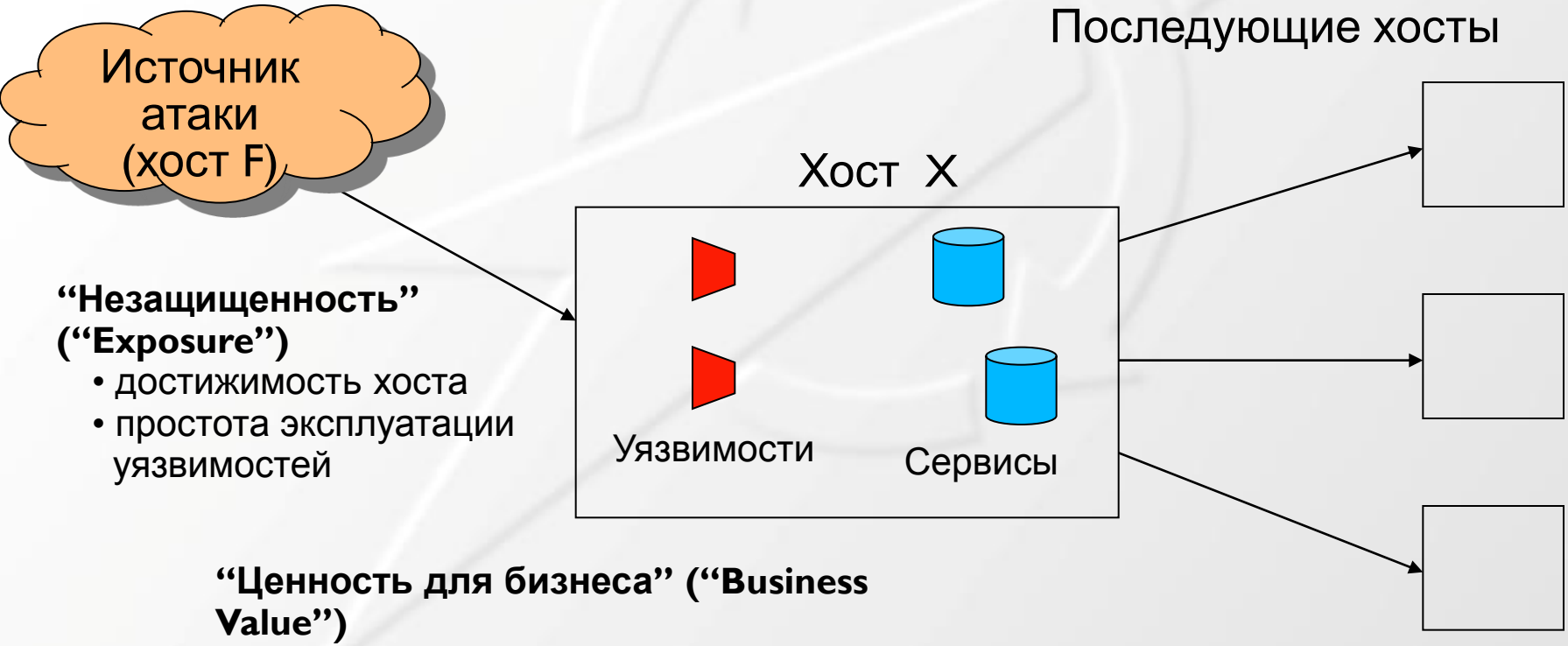
Общий выигрыш и *Ожидаемые годовые потери* (*Annual Loss Expectancy), Возврат инвестиций от реагирования на атаку (Return-On-Response-Investment* (*RORI*) index).

6. Анализ уязвимостей нулевого дня [Ahmed et al., 2008; Ingols et al., 2009; Wang et al., 2010]

Вероятностная мера уязвимости (Probabilistic Vulnerability Measure), показывающая насколько вероятно возникновение уязвимости нулевого за определенный период времени.

k-безопасность нулевого дня (*k-zero day safety)* - показатель, определяющий устойчивость сети к уязвимостям нулевого дня.

Примеры показателей, характеризующих хосты и их связность



“Незащищенность” (“Exposure”)
- достижимость хоста
- простота эксплуатации уязвимостей

“Ценность для бизнеса” (“Business Value”)
- ущерб для бизнеса от потери хоста

“Риск” (“Risk”)
- Exposure X Business Value

Нисходящий риск (“Downstream Risk”)
- кумулятивный риск для всех хостов, атакуемых с данного хоста

[Mayer, 2007]

Уровень навыков нарушителя (Attacker Skill Level, ASL)

- **ASL** – это значимый индикатор возможности нарушителя по выполнению определенных сценариев реализации атаки и достижения его целей.
- **Оценка ASL возможна на основе** отслеживания доступных сообщений и предупреждений об отдельных шагах реализации атаки и включает отслеживание действий нарушителя по графу атак.
- **Упрощенный подход** к оценке ASL - назначение уровня сложности *каждому элементарному шагу атаки*.
  - Когда некоторое предупреждение соответствует определенной атаке, ожидаемому ASL нарушителя может быть присвоено заданное связанное значение сложности.
  - Этот подход не учитывает различные факторы риска, например то, что нарушитель мог реализовать шаг атаки случайно.
- **Более развитый подход** - назначение уровней сложности определенным *последовательностям атак, являющимся комбинациями элементарных атакующих действий*.
  - Это требует способности обнаруживать соответствие нескольким условиям, но приведет к снижению влияния различных факторов риска.

Влияние (ущерб от) атаки (Attack impact, AI) (1/2)

- **Статический подход:**
  - **AI** статически устанавливается как *атрибут каждого элементарного узла* в графе атак.
  - **Влияние на систему в случае успеха атаки** соответствует агрегации статических показателей влияния, назначенных каждому успешно скомпрометированному узлу графа атак.
  - Это неявно означает, что **влияние атаки одинаково, независимо от текущей конфигурации системы**.
  - В то же время, влияние атаки является динамическим показателем, который должен модифицироваться вследствие изменения конфигурации целевой системы.
  - Использование существующих графов атак, без возможности дальнейшего расширения, требует **ручного обновления этих влияний**.
  - Этот подход доказал свою жизнеспособность только **для небольших систем**, где ручное обновление показателей влияния выполнимо.

Влияние (ущерб от) атаки (Attack impact, AI) (2/2)

- **Динамический подход на основе моделей зависимостей сервисов:**
  - **Графы атак** позволяют отслеживать последовательность атакующих действий, пока нарушитель продвигается дальше в целевой системе.
  - **Модели зависимостей сервисов** позволяют отслеживать развитие влияний атаки, в то время как нарушитель получает все больше привилегий.
  - **Когда нарушитель реализует атаки**, он приобретает дополнительные отношения доверия и функциональные отношения, выражаемые в **модели зависимостей сервисов**, и, таким образом, увеличивает влияние на систему.
  - **Изменение конфигурации сервисов** ведет к изменению реализованных отношений, которые могут иметь прямое воздействие на показатели влияния атаки.

Методики вычисления показателей защищенности

1. **Статическая методика экспресс оценки уровня защищенности**

   Методика, определяющая общий уровень защищенности системы на основе учета возможности реализации угроз и их последствий для системы.

2. **Методика, учитывающая события безопасности, происходящие в системе**

   Ориентирована на работу в реальном времени, когда текущее положение атакующего и его перемещение в сети может отслеживаться, но существуют жесткие ограничения на время вычислений.

3. **Методика, основанная на анализе исторических данных**

   При вычислении вероятности и потенциала атаки используются данные о предыдущих инцидентах.

Методики вычисления показателей защищенности

1. **Статическая методика экспресс оценки уровня защищенности**

   Методика, определяющая общий уровень защищенности системы на основе учета возможности реализации угроз и их последствий для системы.

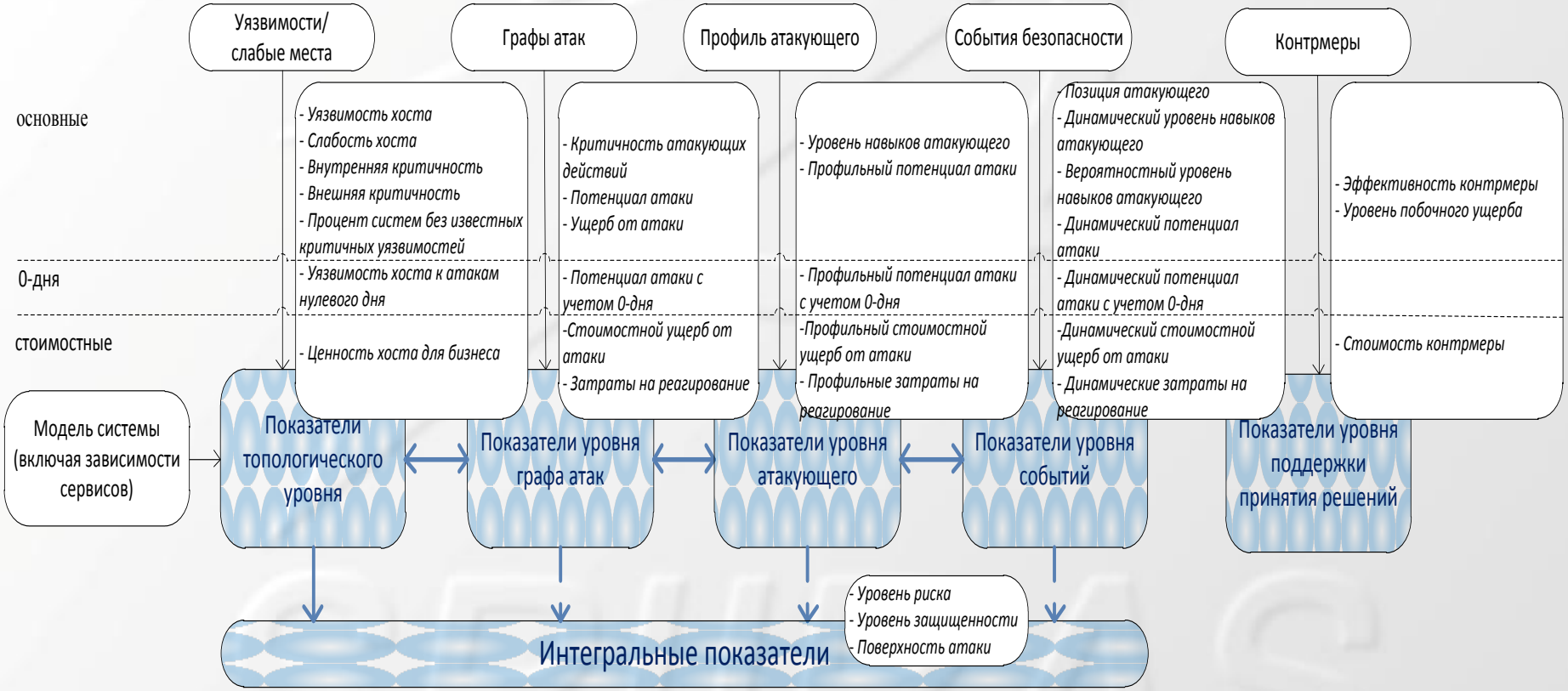
2. **Методика, учитывающая события безопасности, происходящие в системе**

   Ориентирована на работу в реальном времени, когда текущее положение атакующего и его перемещение в сети может отслеживаться, но существуют жесткие ограничения на время вычислений.

3. **Методика, основанная на анализе исторических данных**

   При вычислении вероятности и потенциала атаки используются данные о предыдущих инцидентах.

Расширенная таксономия показателей защищенности



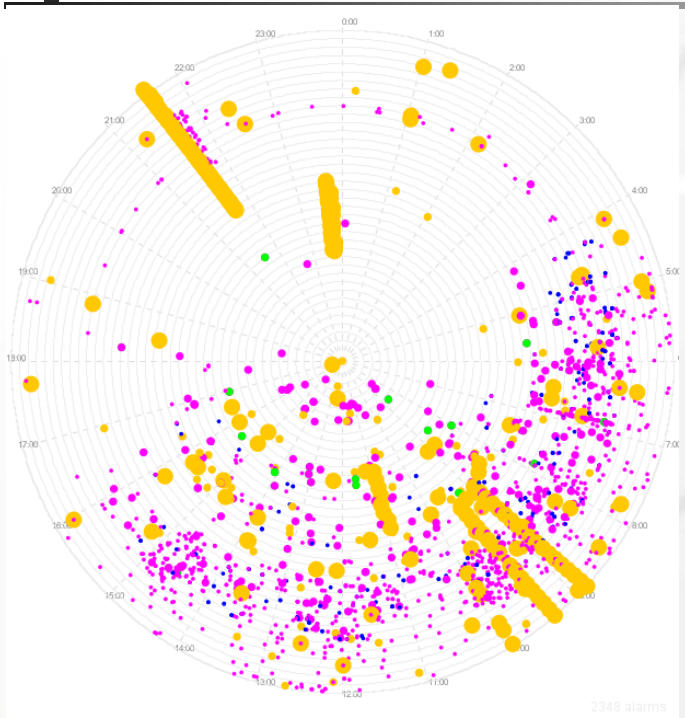
Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
  - Сервисы аналитического моделирования
  - Сервисы анализа защищенности
  - Сервисы визуализации
- Заключение

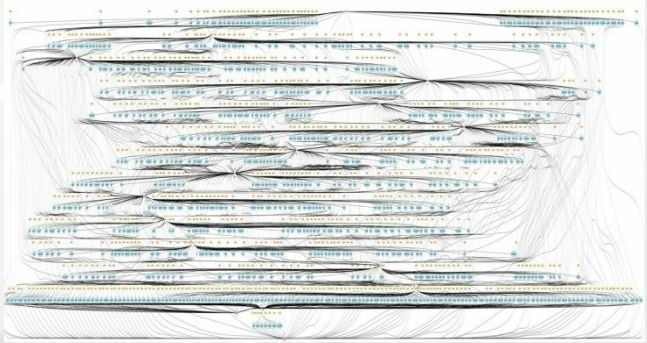
Модели визуализации данных и их применение

- Мониторинг периметра сети:
  - круговая диаграмма, представляющая наиболее активные хосты-приемники и хосты-получатели
  - гистограмма наиболее часто используемых сервисов
  - граф коммуникаций, отражающих потоки между хостами
  - карта деревьев (treemap), отражающая частоту использования портов различными хостами
  - графы вида «отправитель-сообщение-получатель» и т.д.
- Контроль деятельности пользователей:
  - графы вида «пользователь-деятельность» и «пользователь-сервер»
  - гистограмма, отражающая число документов, просмотренных пользователям
- Отображение уровня защищенности:
  - круговая диаграмма, отражающая наиболее уязвимые хосты
  - карты деревьев, отражающие наиболее уязвимые хосты
  - географические карты, отражающие расположение хостов с указанием оценок рисков, доступности и уязвимости хостов

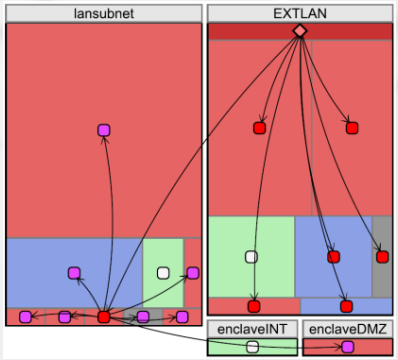
Модели визуализации для представления событий и анализа защищенности

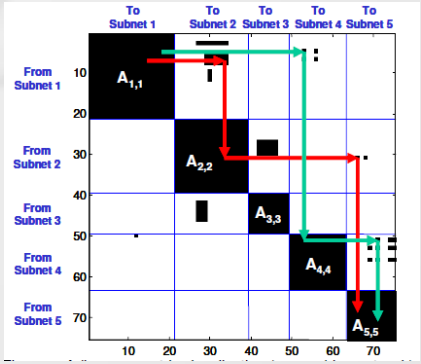


Представление событий в SpiralView [1]



Визуализация атак на основе графов [2]





Альтернативные представления атак [3, 4]

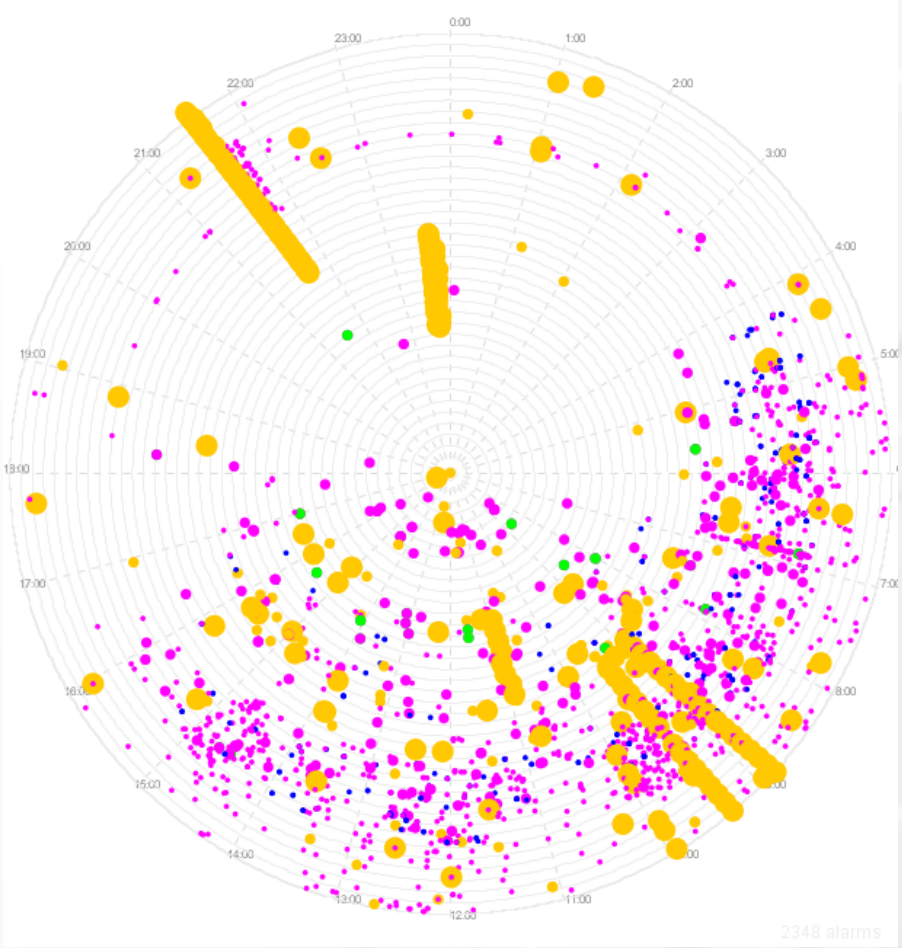
[1] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. In Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007. pp.139-146.

[2] Noel S.. Managing attack graph complexity through visual hierarchical aggregation. In Proceedings of ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04), NY., ACM press, 2004, pp.109-118.

[3] Williams L., Lippmann R., Ingols K. An Interactive Attack Graph Cascade and Reachability Display. In Proceedings of the Workshop on Visualization for Computer Security, Sacramento, California, USA, 2008. Springer, Heidelberg. pp. 221-236.

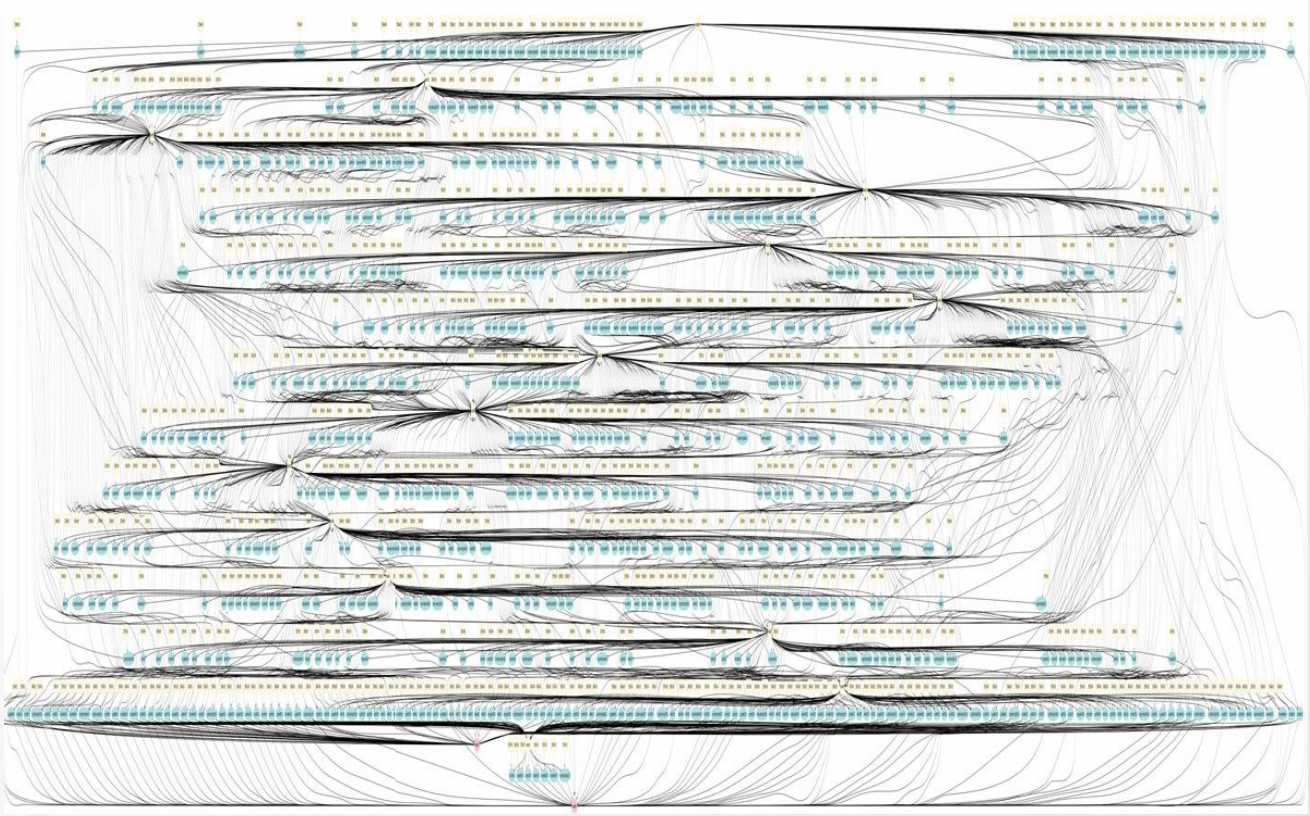
[4] Noel S., Jajodia S. Understanding complex network attack graphs through clustered adjacency matrices. In Proceedings of the 21st Annual Computer Security Applications Conference, 2005, pp.160-169.

Спиральное представление событий безопасности [Bertini et al., 2007]



- Используется для мониторинга событий безопасности, регистрируемых различными датчиками безопасности
- В графической модели используется временная шкала. Для обозначения k суток или месяцев применяется шкала, состоящая из k окружностей разного радиуса. Окружности разделены на 24 части, обозначающие часы в сутках. Самые ранние события в виде точек располагаются на внутренней окружности, а самые поздние - на внешней.
- Цвет точки обозначает тип события, а размер точки - уровень его критичности.
- Для анализа событий реализован механизм фильтрации, масштабирования и выделения событий цветом в зависимости от заданных пользователем условий.

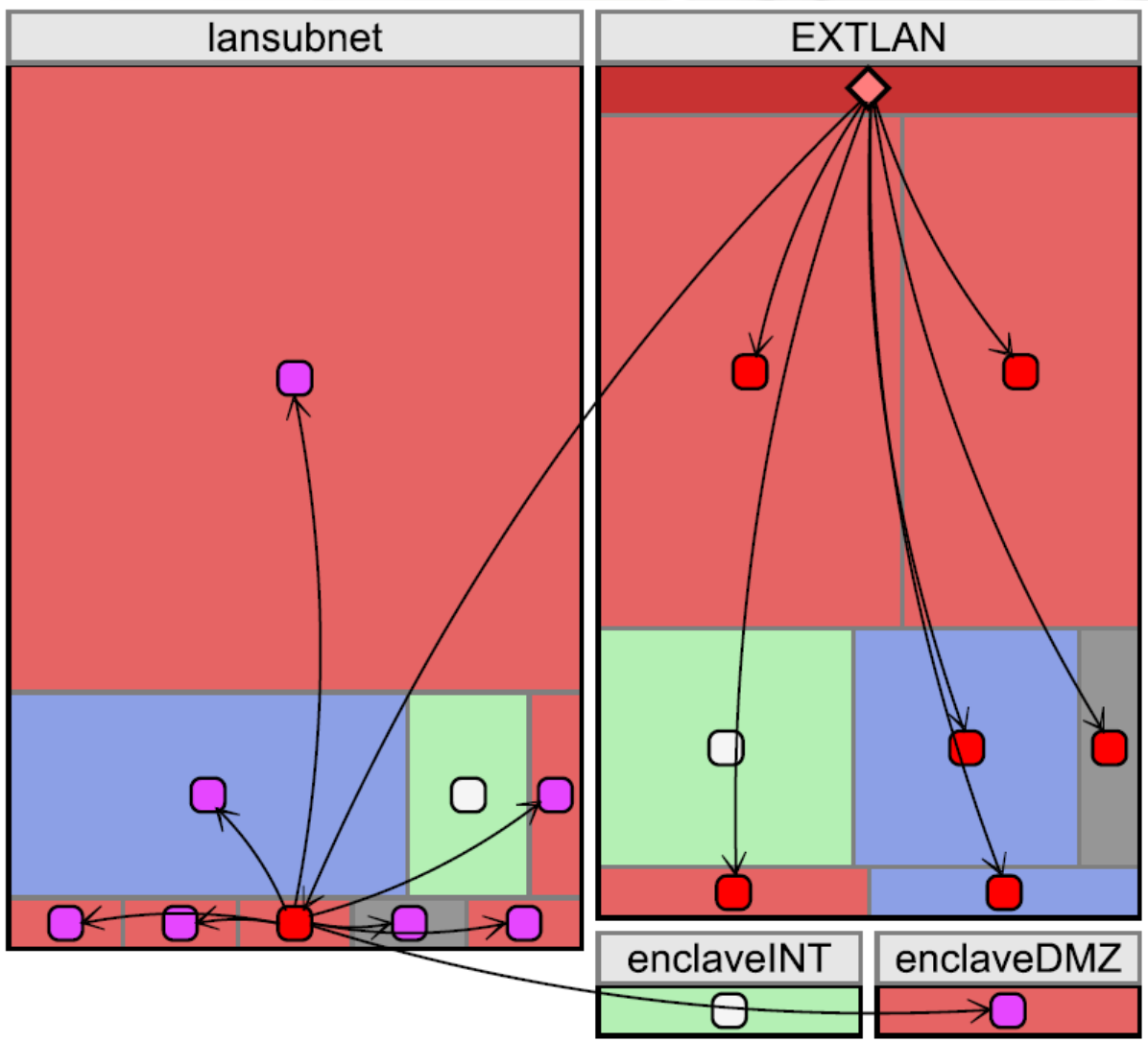
Визуализация атак на основе графов [Noel, 2004]



Исследуется проблема уменьшения сложности графов атак на основе визуального иерархического агрегирования. Предложено свертывать непересекающиеся подграфы графа атак в одиночные вершины графа.

Операция агрегирования - рекурсивна в соответствии с иерархией агрегирования. На каждом уровне агрегирования устанавливаются правила, которые основаны либо на общих атрибутах элементов графа атак, либо связности графа атак.

Представление графа атак в виде карты деревьев [Williams et al., 2008]



- Каждая подсеть представляется в виде карты деревьев, вложенные прямоугольники - узлы, с помощью цвета кодируются различные атрибуты узлов, а размер пропорционален числу скомпрометированных узлов в подсети
- Режимы взаимодействия с картами деревьев:
  (1) оценка достижимости узлов в результате атаки;
  (2) отображение кратчайших путей атакующего между узлами.
- Возможность экспериментов “что, если”

Визуализация в Security Risk Manager (RedSeal): представление шагов атаки (1/2)

Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

File Edit View Tools Help

Home | Risk | Threats | Inventory | Reports

Confidence

Subnet Attribute Mapping

Exposure

Business Value

Related Tasks

Configure Patch Frequency

Configure Applications

Network Path Explorer

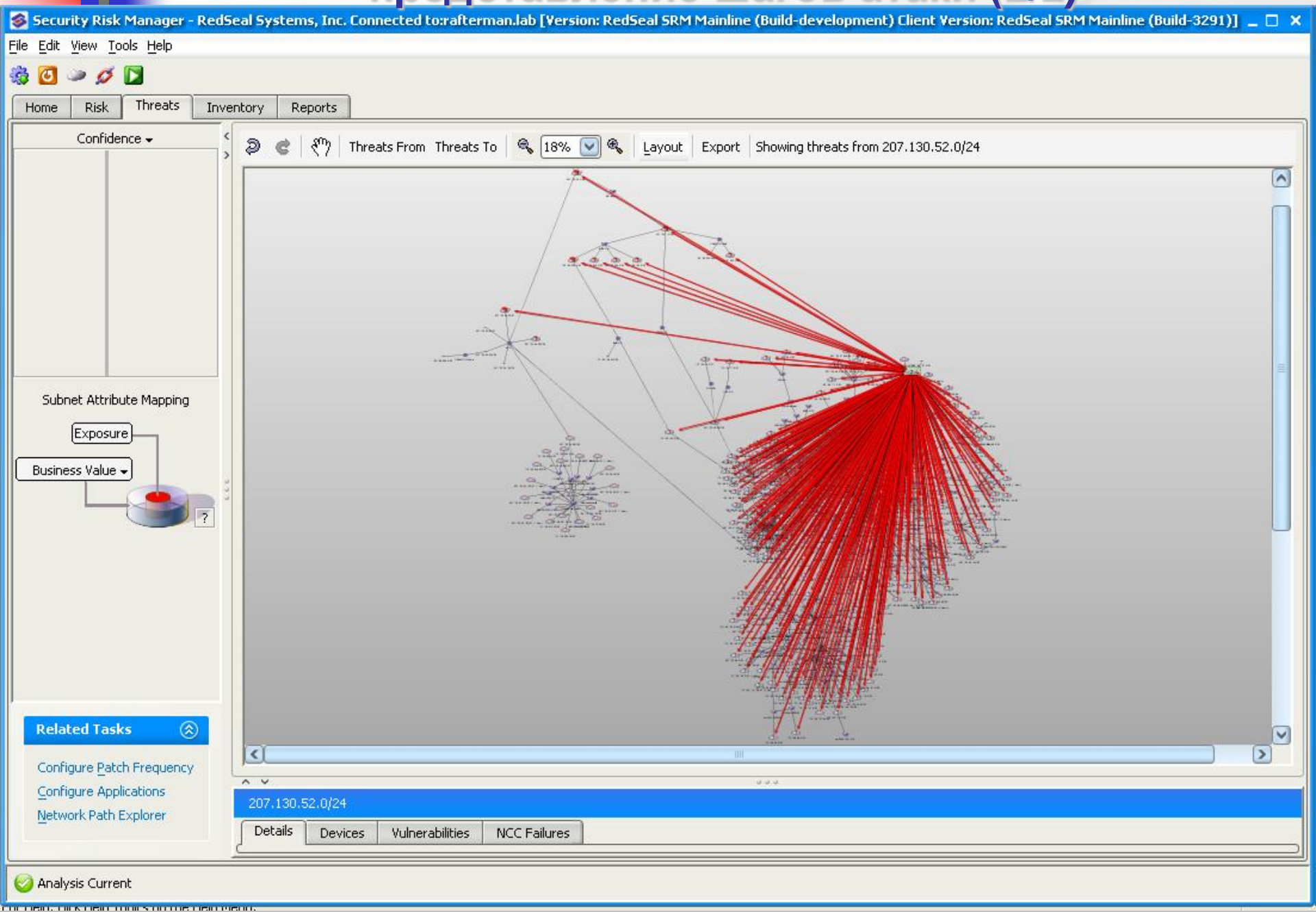
Threats From Threats To 21% Layout Export Showing threats from 207.130.95.208/28

207.130.95.208/28

Details | Devices | Vulnerabilities | NCC Failures

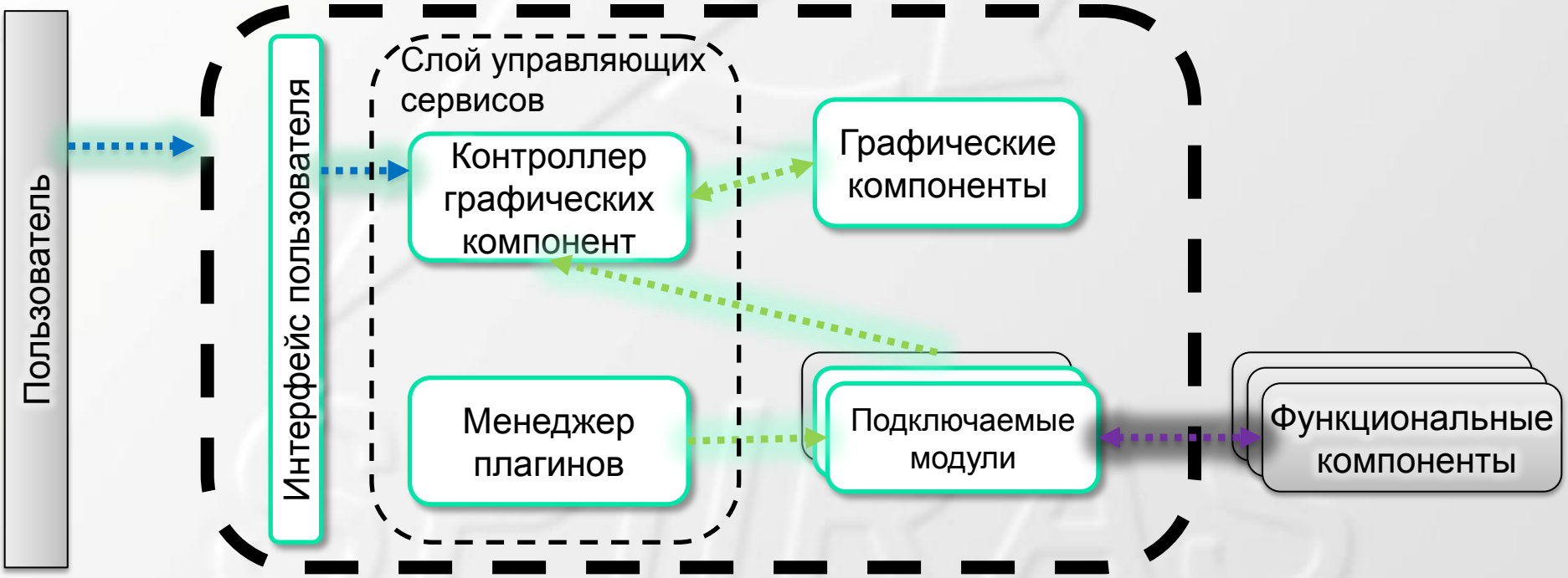
Analysis Current

Визуализация в Security Risk Manager (RedSeal): представление шагов атаки (2/2)



Архитектура подсистемы визуализации

- Функциональная расширяемость
- Гибкая связь между компонентами
- Независимая разработка модулей



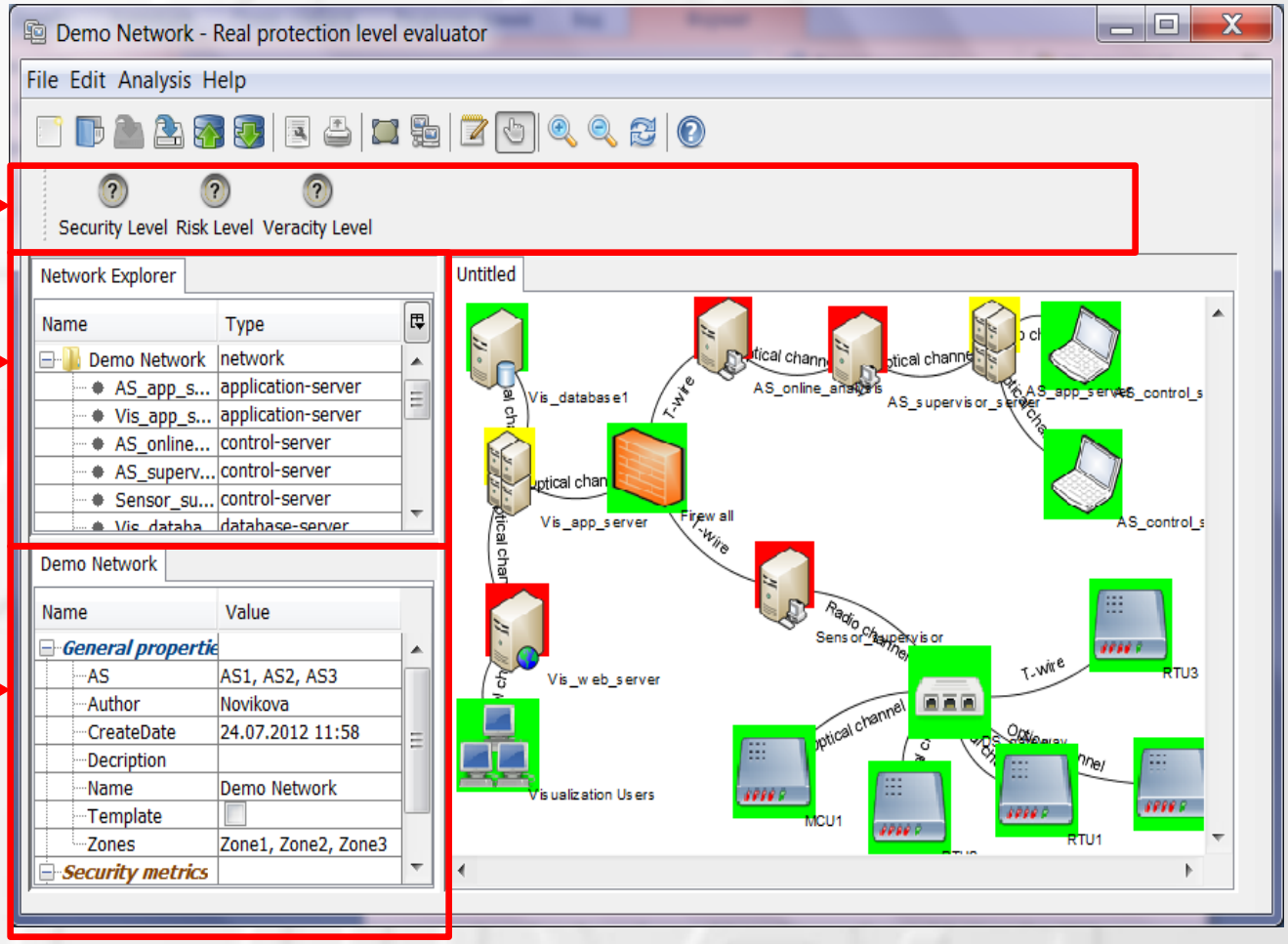
Графический интерфейс модуля моделирования атак и оценки защищенности

Главное окно

Основные метрики

Редактор структуры сети

Редактор свойств объектов сети



Java Universal Network/Graph Framework, http://jung.sourceforge.net/

Графический интерфейс модуля моделирования атак и оценки защищенности

Информационные окна

WIN-L2B1S0L1QBA

Name	Value
General properties	
AS	
Comment	
CritLevel	
HType	Неизвестный тип
Hardware	
IP	10.10.37.4
Name	WIN-L2B1S0L1QBA
OS	
Software	
Veracity	Not specified
Zones	
MaxPatrol propertie	
MaxPatrolHardware	Номер процессора = 0, Производитель = Genuine
MaxPatrolOS	Windows 2008 R2 ServerEnterprise (x64)
MaxPatrolSoftware	Microsoft Internet Explorer 8.0, Microsoft Windows
Security metrics	
Vulnerabilities	227
User-defined proper	

Data

Номер процессора = 0, Производитель = GenuineIntel, Семейство процессора = 6, Название модели = Intel(R) Xeon(R) CPU X54...
Размер физической памяти = 2147016704 bytes
Производитель = Phoenix Technologies LTD, Версия = PhoenixBIOS 4.0 Release 6.0, Дата выпуска = 2011.07.12
Производитель = Intel Corporation, Модель = 440BX Desktop Reference Platform, Версия = None, Серийный номер = None
Название = VMware Virtual disk SCSI Disk Device, Размер = 107372805120 bytes, Тип интерфейса = SCSI, Количество цилиндров = 130...
Название модели = Сетевое подключение Intel(R) PRO/1000 MT, Производитель = Intel, Тип интерфейса = Ethernet 802.3, MAC-адр...

OK Cancel

Data

Microsoft Internet Explorer 8.0
Microsoft Windows MDAC N/A
Microsoft .NET Framework 2.0 SP2
Microsoft XML Core Services 6.0
Microsoft JScript N/A
Microsoft Windows Remote Access Connection Manager N/A
Microsoft Pragmatic General Multicast 6.1
Microsoft Updates 2008 SP0
Microsoft Windows Windows 2008 R2 ServerEnterprise (x64)

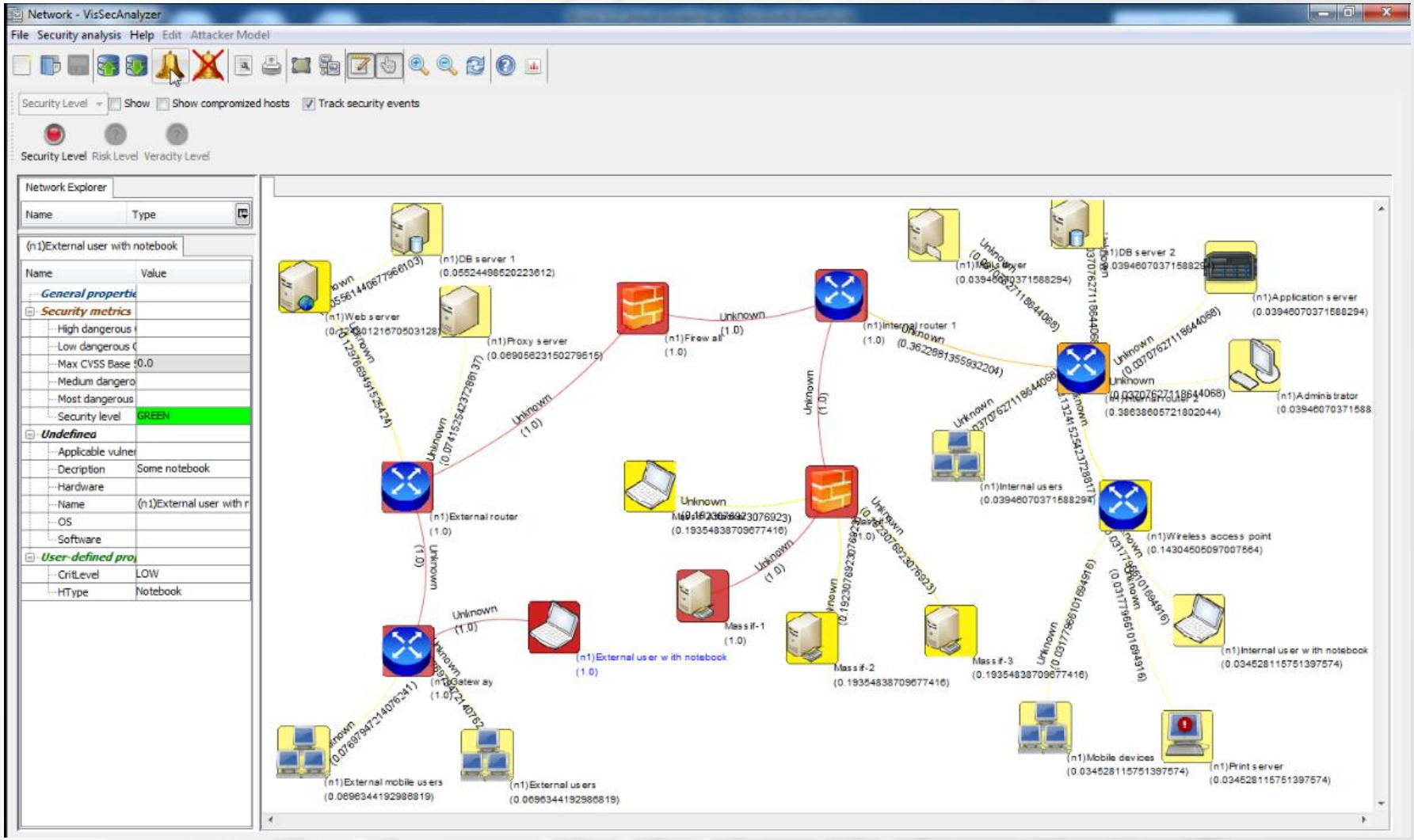
OK Cancel

Vulnerability List

id	title	short ...	description	counter...	links	CVSS	CVE
412389	Уязвимость работы с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2009-3671
412391	Ошибка при работе с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2009-3673
412442	Ошибка при работе с не...	Уязвим...	Уязвимость, которая позволяет...	Использу...	MS (M...	9.3	CVE-2010-0490
412444	Ошибка при работе с па...	Уязвим...	Уязвимость, которая позволяет...	Использу...	MS (M...	9.3	CVE-2010-0492
412486	Междоменное разглаше...	Уязвим...	Уязвимость, которая позволяет...	Использу...	MS (M...	9.3	CVE-2010-0255
412488	Ошибка при работе с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-1259
412489	Ошибка при работе с па...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-1260
412490	Ошибка при работе с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-1261
412491	Ошибка при работе с па...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-1262
412533	Ошибка при работе с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-2556
412535	Ошибка при работе с па...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-2558
412536	Ошибка при работе с не...	Уязвим...	Уязвимость, позволяющая удал...	Использу...	MS (M...	9.3	CVE-2010-2559

OK

Анализ событий



Элементы графического интерфейса компонента

Метрики безопасности – семафор

Security Level

Not defined

Green (Network is secured)

Yellow (Low Criticality)

Orange (Medium Criticality)

Red (High Criticality)

Пиктограммы, использующие для отображения графа атак

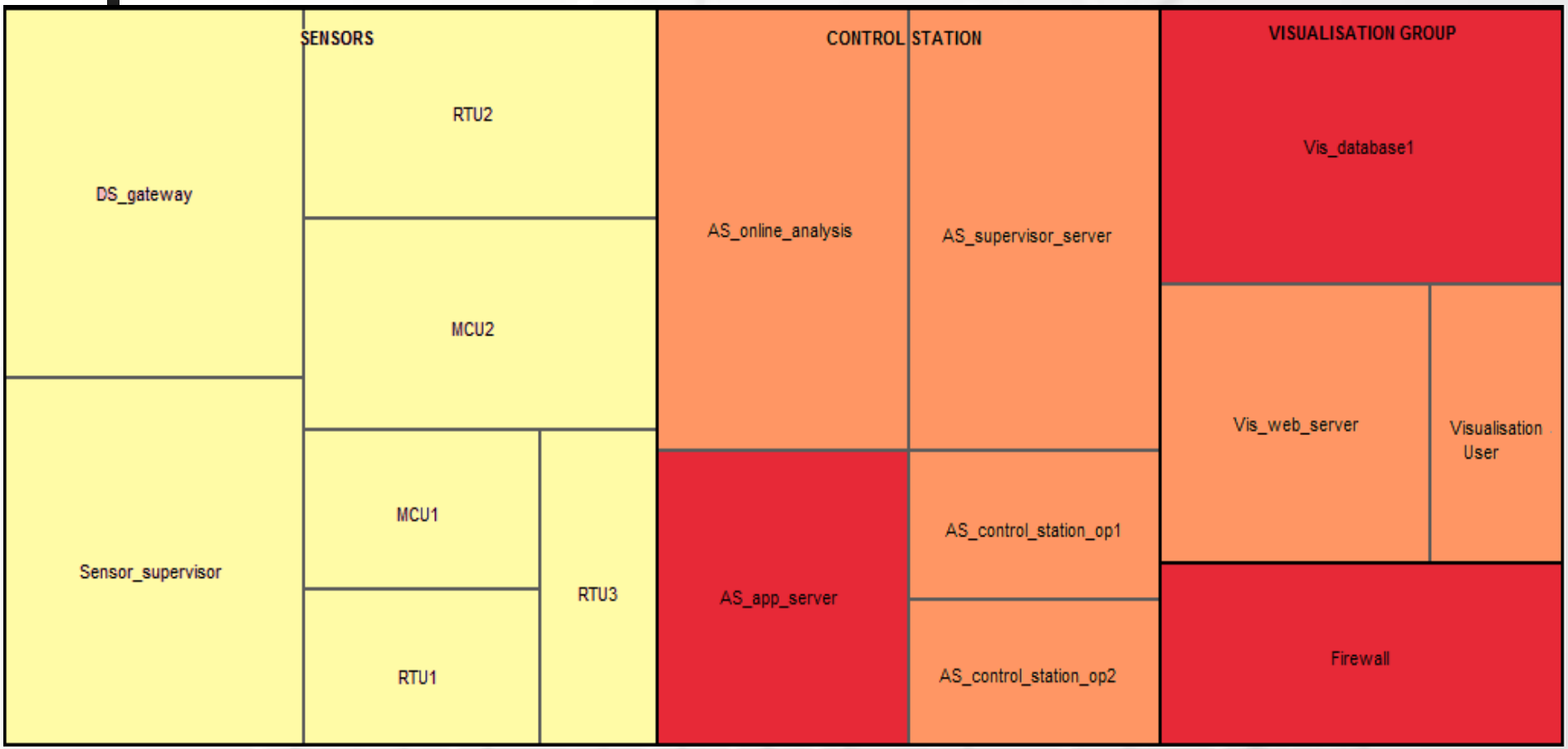
Исходное положение нарушителя

Применение атомарного действия

Применение сценария без использования уязвимости

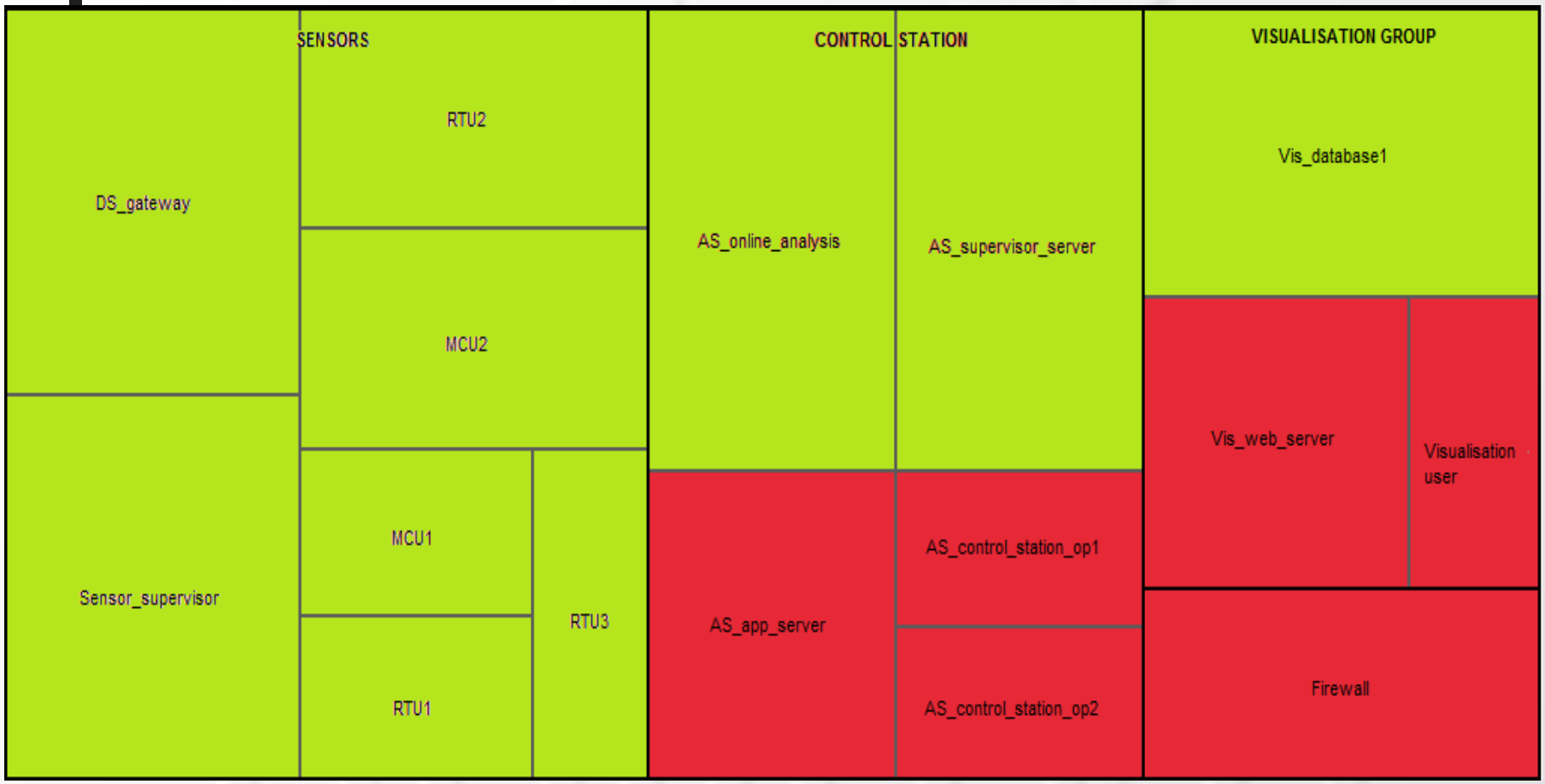
Эксплуатация уязвимости

Отчет об уязвимостях на основе карт деревьев



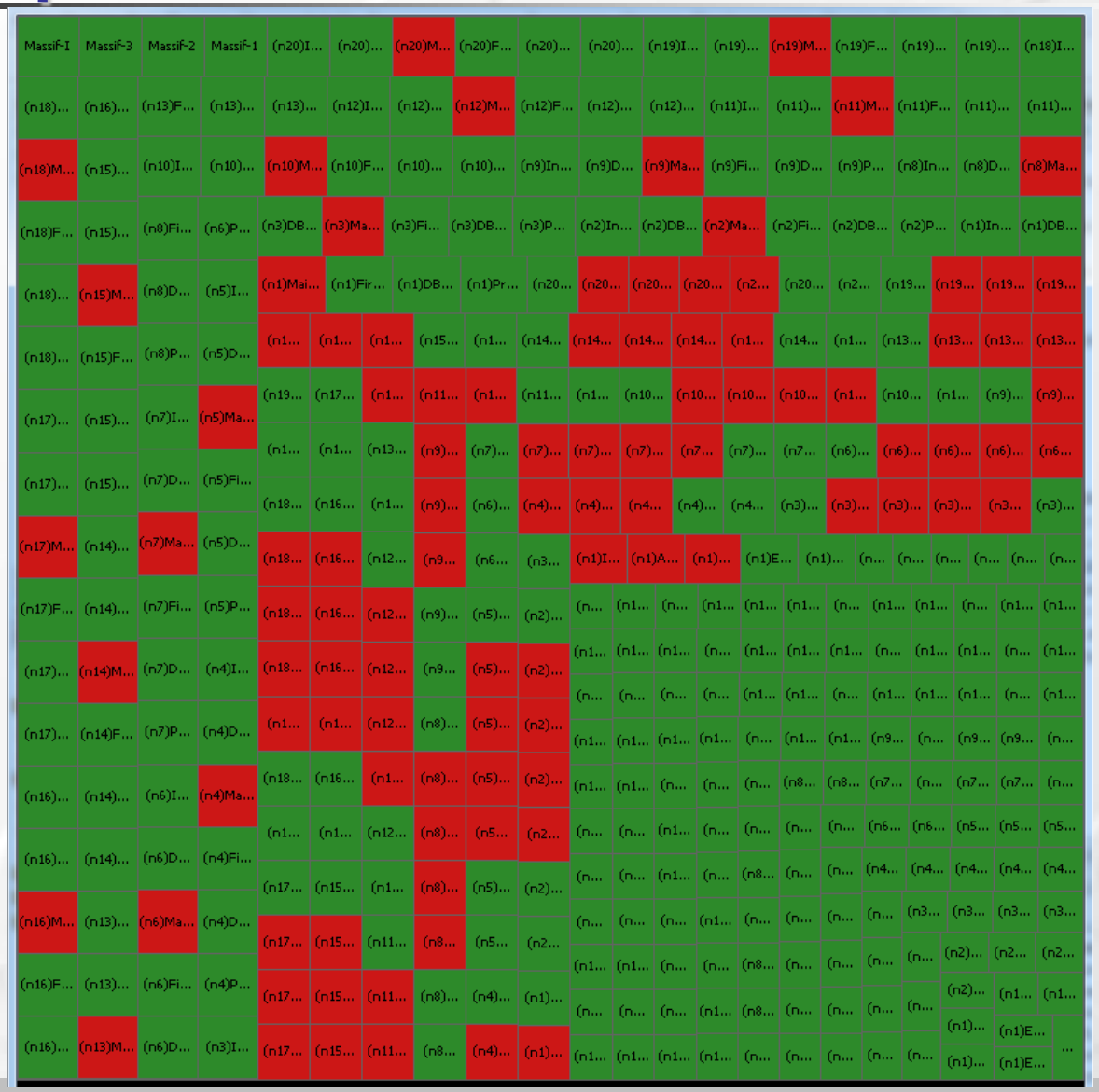
Каждый вложенный прямоугольник отображает хост. Размер прямоугольника определяется задаваемой пользователем критичностью хоста. Цвет используется для обозначения серьезности уязвимости, обнаруженной на данном хосте.

Анализ достижимости атаки на основе карт деревьев



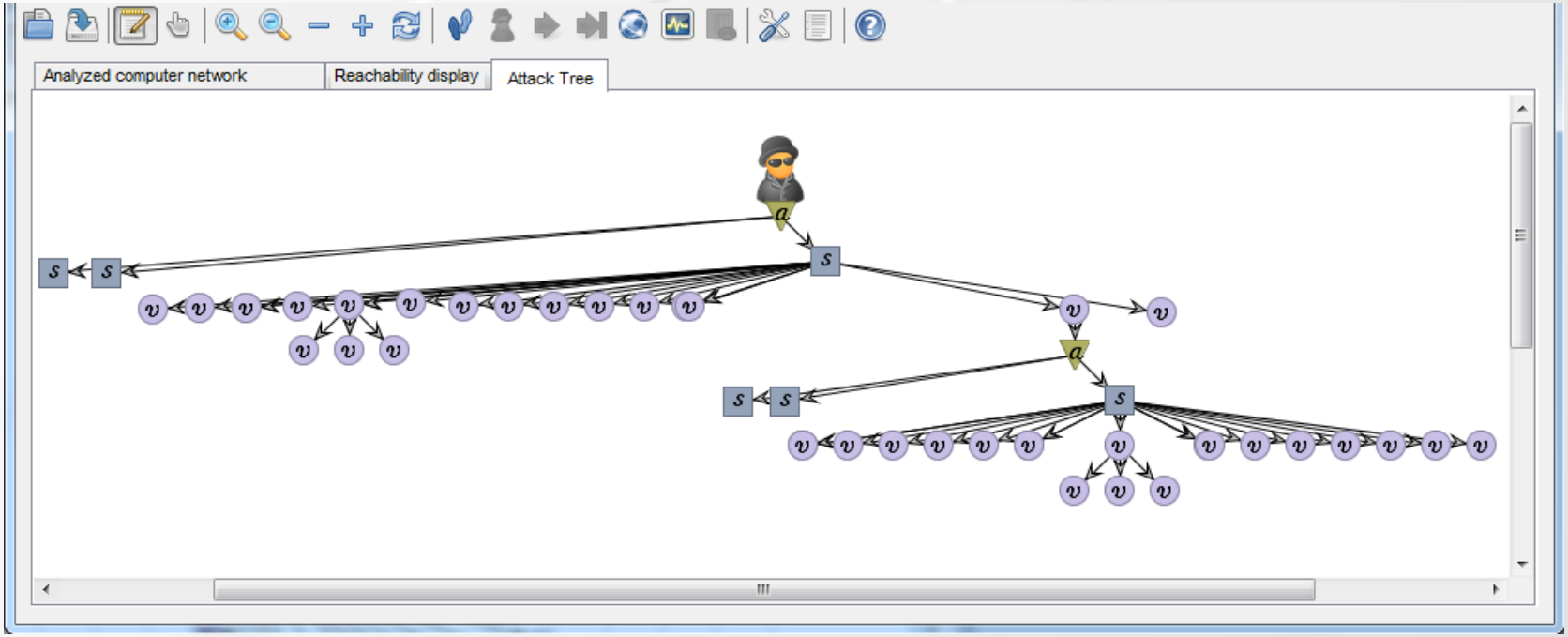
Размер вложенных прямоугольников соответствует уровню критичности, а цвет отражает состояние хоста (красный - хост достигаем нарушителем, зеленый - нарушитель не может получить доступ к хосту.

Представление скомпрометированных и защищенных узлов сети в виде карты деревьев



Представление графов атак (1/2)

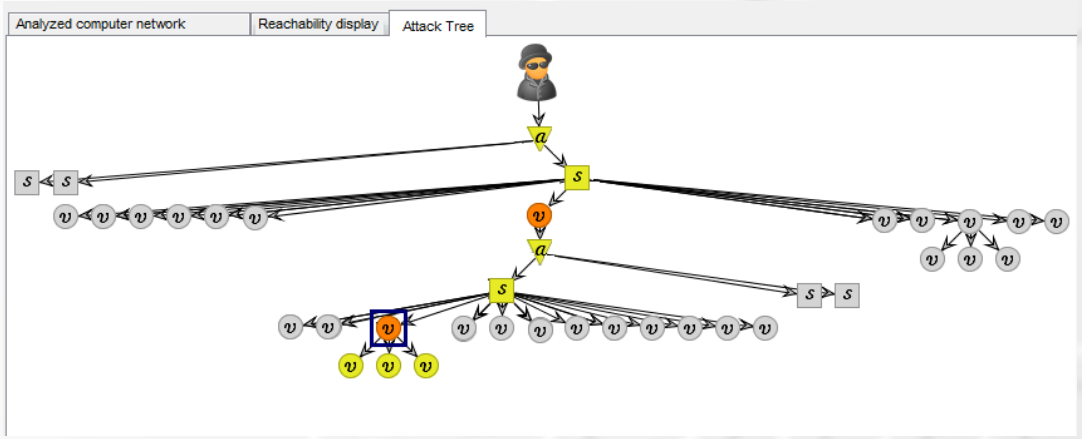
Обозначение	Описание
	Исходное положение нарушителя
	Специфическое атакующее действие
	Сценарий, не использующий уязвимости
	Атакующее действие, использующее уязвимость



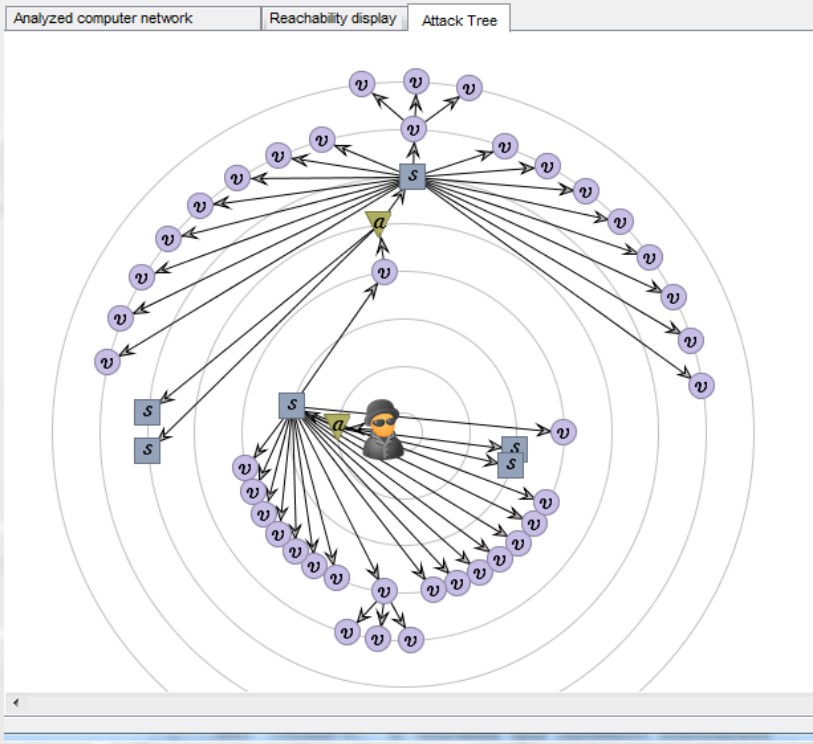
Представление графов атак (2/2)

Способы взаимодействия с графическим представлением графов атак:

- Управление представлением графа (древовидное и радиальное)
- Геометрическое масштабирование
- Семантическое масштабирование (агрегирование узлов графа)
- Детали по требованию
- Подсветка и связывание



Древовидное представление и эффект подсветки и связывания



Радиальное представление

Вопросы лекции

- Введение
- Концепция построения системы мониторинга и управления кибербезопасностью
- Сервисы аналитического моделирования, анализа защищенности и визуализации
- Заключение

Основные текущие проекты, в которых реализуются предлагаемые технологии

- Грант Российского научного фонда № 15-11-30029 « **Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах с учетом облачных сервисов и сетей Интернета вещей**», 2015-2017 гг.
- Государственный контракт № 14.604.21.0033 «**Модели, методики и программные средства разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей**». Проект Минобрнауки России в рамках Программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы», 2014-2015 гг.
- Государственный контракт № 14.604.21.0137 «**Разработка технологий интерактивной визуализации неформализованных данных разнородной структуры для использования в системах поддержки принятия решений при мониторинге и управлении информационной безопасностью информационно-телекоммуникационных систем**». Проект Минобрнауки России …, 2014-2016 гг.
- Государственный контракт № 14.604.21.0147 «**Разработка методов агрегации, нормализации, анализа и визуализации больших массивов гетерогенных структурированных, полуструктурированных и неструктурированных данных для мониторинга и управления безопасностью распределенной сети электронных потребительских устройств**». Проект Минобрнауки России …, 2014-2016 гг.

Реализованные программно-аппаратные комплексы

1. Программно-аппаратный комплекс оценки защищенности компьютерных сетей с учетом различных категорий нарушителей

1.1. Конструктор сети

1.2. Взаимодействие с о сканером сети

1.3. Оценка защищенности

2. Программно-аппаратный комплекс оценки защищенности с использованием деревьев атак

2.1. Отображение графов атак для внешнего и внутреннего нарушителя

3. Программно-аппаратный комплекс аналитического моделирования атак, оценки текущего состояния и анализа защищенности

3.1. Архитектура БД + Сервер приложений

3.2. Оценка защищенности, карты деревьев

3.3. Обработка событий и вероятности

4. Система динамического моделирования атак и механизмов защиты для проектирования и исследования защищенности компьютерных сетей

4.1. Демонстрация софта на стенде

4.2. Сценарий функционирования бот-сети

5. Комплексная система мониторинга и управления безопасностью

5.1. Общая архитектура системы

5.2. Сценарий функционирования

Контактная информация

Котенко Игорь Витальевич (СПИИРАН)
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko/

Благодарности

- Работа выполняется при финансовой поддержке РНФ (соглашение № 15-11-30029), Минобрнауки в рамках Программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (№ 14.604.21.0033, 14.604.21.0137, 14.604.21.0147) и РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417).
- Основные разработчики лаборатории проблем компьютерной безопасности СПИИРАН: И.Б.Саенко, Е.С.Новикова, А.А.Чечулин, Е.В.Дойникова, В.А.Десницкий и др.