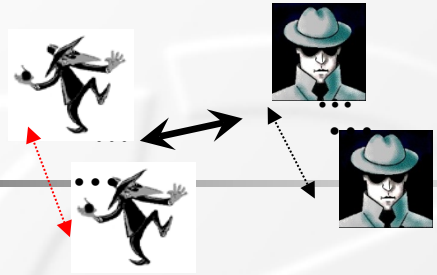


Проактивное управление информацией и событиями безопасности в сетях NGN

Котенко И.В., д.т.н., профессор
Саенко И.Б., д.т.н., профессор
Чечулин А.А., к.т.н.

Лаборатория проблем компьютерной безопасности
Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)

Семинар ITU, 23-25 июня 2014 г., г. Санкт-Петербург

План доклада

- **Введение**
- Концепция построения системы проактивного управления информацией и событиями безопасности
- Сервисы аналитического моделирования
- Сервисы анализа защищенности
- Сервисы визуализации
- Заключение

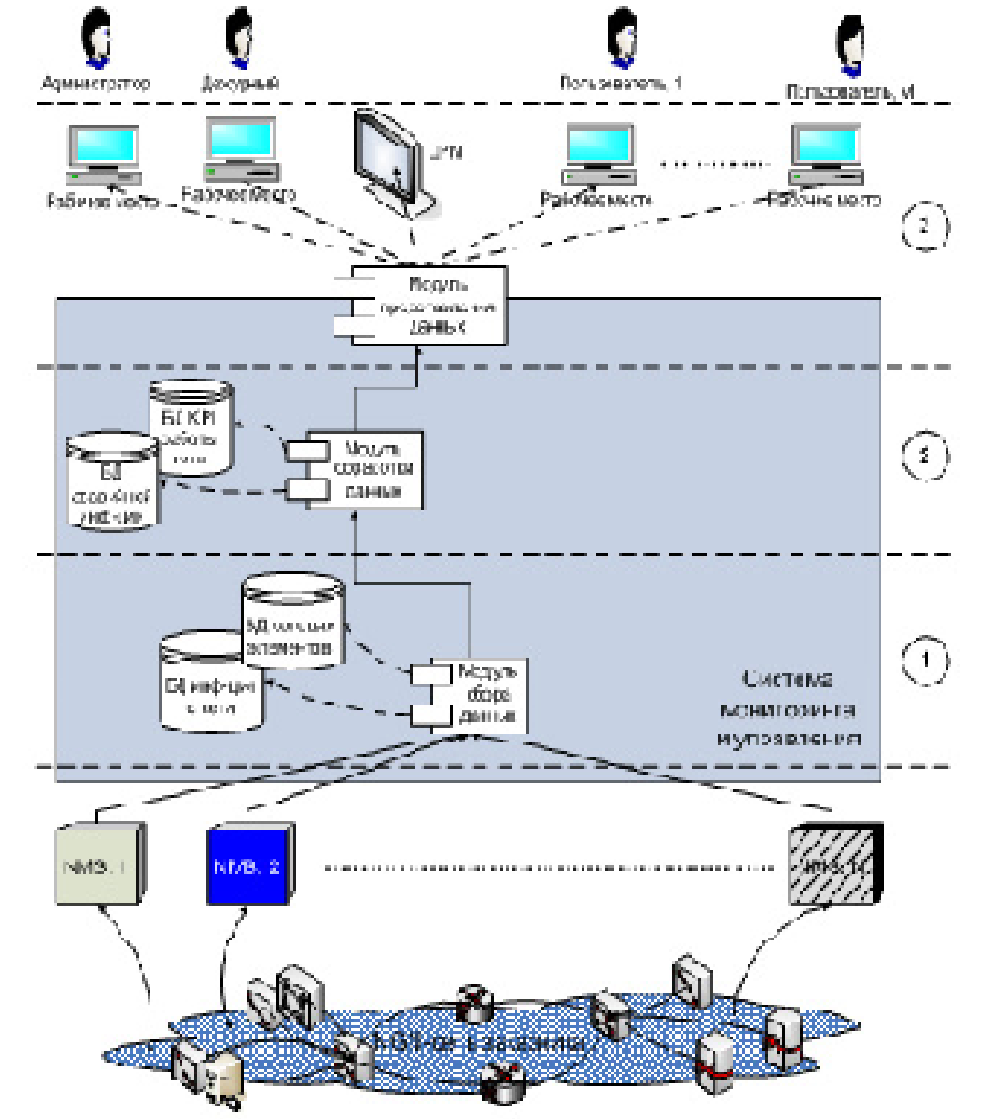
Тенденции развития средств реализации атак на сети NGN

- В настоящее время мы являемся свидетелями новой фазы противостояния (“гонки вооружений”) в компьютерных сетях между системами нападения и защиты
- Важными особенностями этого противостояния является
  - повышение уровня автоматизации, мощности, изощренности и масштабности этих систем
  - использование концепции “постоянных изощренных угроз” (“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.)
  - пример: Stuxnet -> Duqu -> Flame -> Gauss -> Red October -> …

Обобщенная структура системы защиты сетей NGN

Средства интеллектуального управления защитой			
Оценка состояний	Формирование вариантов управления	Адаптация	
Средства проактивной защиты			
Анализ защищенности	Обнаружение атак	Противодействие атакам	
Традиционные средства защиты			
Шифрование	Управление доступом	Контроль целостности	Регистрация и учет

NGN как объект мониторинга и управления безопасностью*



Примечания

Модель мониторинга и управления:

1 – уровень сбора данных

2 – уровень обработки и хранения данных

3 – уровень представления и использования данных

KPI - показатели работы сети

NMS – системы (внешние) управления сетью

АРМ – центральное рабочее место

---

* Чижиков Д. Мультисервисные сети следующего поколения: потребности рынка, принципы, мониторинг // http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html

Требования к NGN

- “**мультисервисность**”, под которой понимается независимость технологий предоставления услуг от транспортных технологий;
- “**широкополосность**”, под которой понимается возможность гибкого и динамического изменения скорости передачи информации в широком диапазоне в зависимости от текущих потребностей пользователя;
- “**мультимедийность**”, под которой понимается способность сети передавать многокомпонентную информацию (речь, данные, видео, аудио и др.) с необходимой синхронизацией этих компонент в реальном времени и использованием сложных конфигураций соединений;
- “**интеллектуальность**”, под которой понимается возможность управления услугой, вызовом и соединением со стороны пользователя или поставщика услуг;
- “**инвариантность доступа**”, под которой понимается возможность организации доступа к услугам независимо от используемой технологии;
- “**многооператорность**”, под которой понимается возможность участия нескольких операторов в процессе предоставления услуги и разделение их ответственности в соответствии с их областью деятельности.

Фундаментальные свойства NGN

- Поддержка **большого набора услуг**, приложений и механизмов поблочного построения услуг (включая услуги в реальном времени/ потоковую передачу/ услуги, предоставляемые не в режиме реального времени и мультимедиа-услуги).
- Отделение процесса предоставления услуги от самой сети и обеспечение о**ткрытых интерфейсов**, разделение функций управления от возможностей транспортной среды, вызова/сеанса и приложения/услуги, что позволяет услугам и сетям развиваться независимо друг от друга.
- **Взаимодействие** с унаследованными сетями по открытым интерфейсам.
- **Пакетный перенос**.
- **Широкополосный доступ** с обеспечением качества из конца в конец и «прозрачности».
- **Обобщенная мобильность**.
- **Открытый доступ пользователей** к различным сервис-провайдерам.
- **Различные схемы идентификации**, которые могут быть реализованы с использованием IP-адресации в целях маршрутизации по IP-сетям.
- **Унифицированные** характеристики услуги в понимании пользователя.
- **Конвергенция** услуг между сетями фиксированной и подвижной связи.
- **Совместимость** со всеми требованиями в области регулирования отрасли, например, экстренной связи, **безопасности, защищенности** и т.п.

Факторы необходимость внедрения интеллектуальных средств защиты в NGN

- многообразие возможных угроз безопасности (видов атак);
- 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 «редких» атак;
- необходимость проактивной защиты информации (основанной на способности предвидеть намерения и поведения атакующего)
- и прочее

План доклада

- Введение
- **Концепция построения системы проактивного управления информацией и событиями безопасности**
- Сервисы аналитического моделирования
- Сервисы анализа защищенности
- Сервисы визуализации
- Заключение

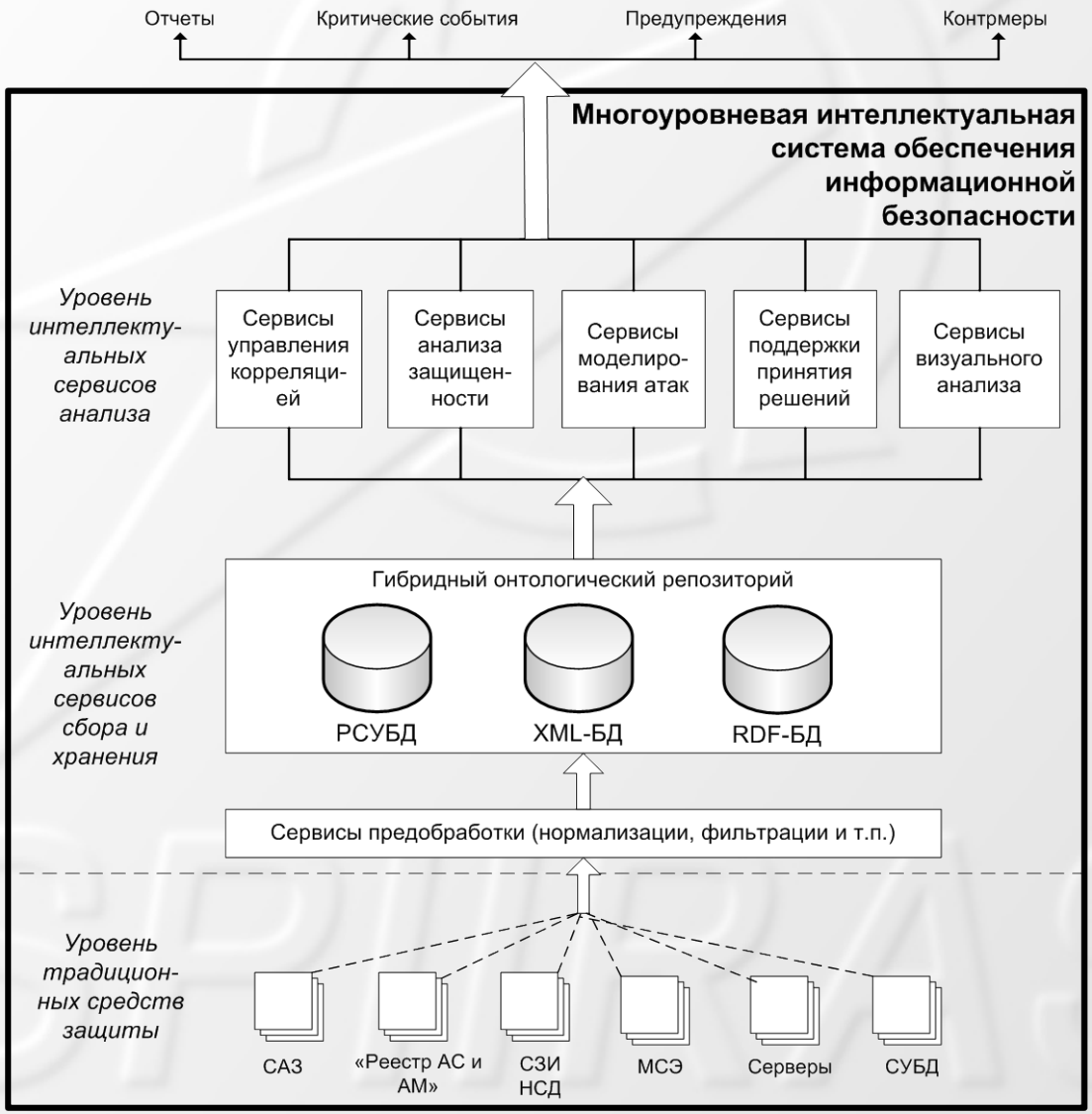
Понятие «интеллектуального сервиса защиты информации»

Интеллектуальный сервис защиты информации – это совокупность средств и механизмов защиты информации, основанных на применении методов и моделей ИИ и связанных общностью реализуемых функций защиты.

Примеры интеллектуальных сервисов защиты информации:

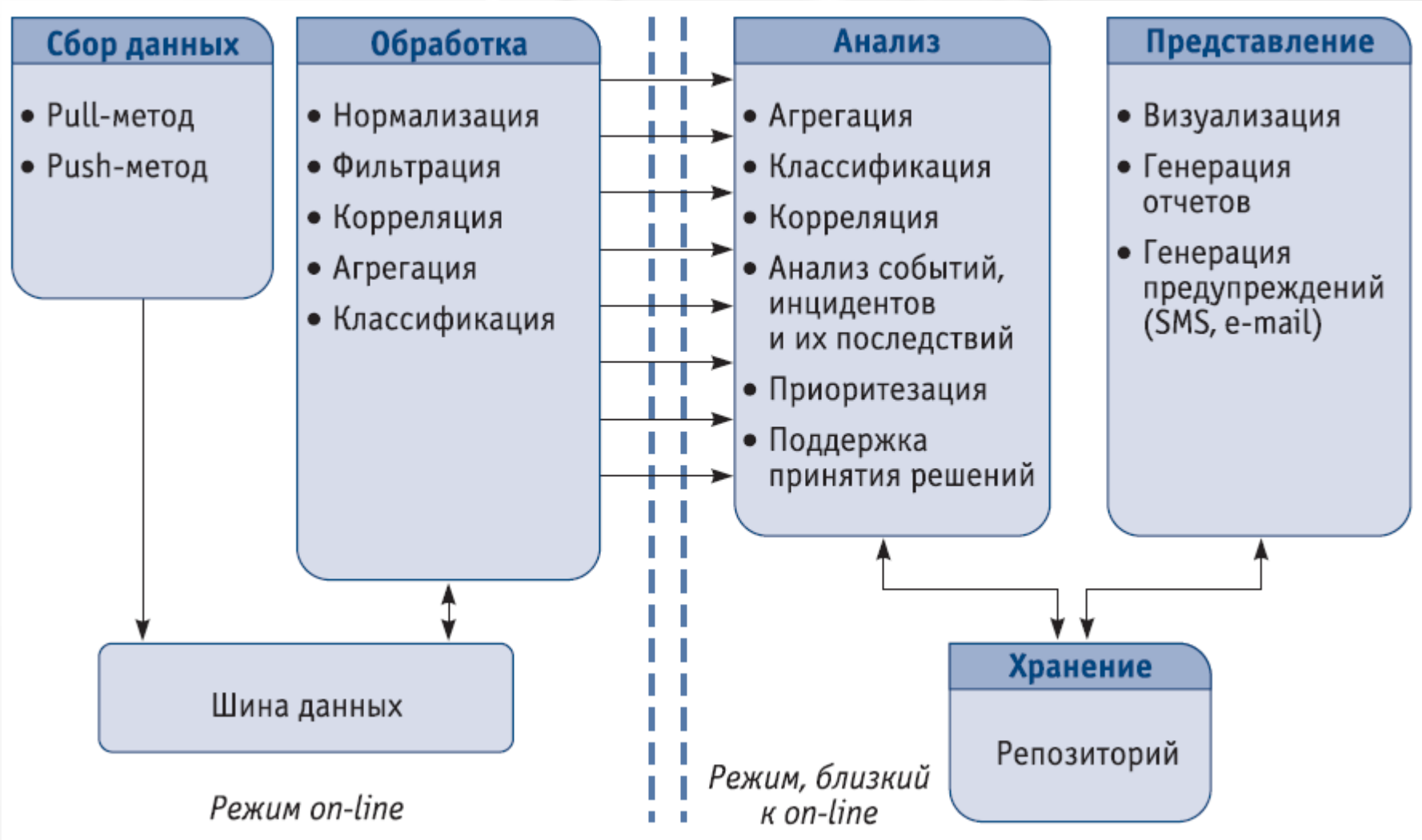
- **сбора и предварительной обработки** информации о состоянии инфраструктуры, угрозах безопасности, шаблонах атак, инцидентах и пр.;
- **хранения** информации о безопасности;
- **аналитической обработки** информации о безопасности (анализа защищенности, моделирования атак, принятия решений и т.д.) ;
- **отображения** информации (визуального анализа)

Архитектура системы проактивного управления информацией и событиями безопасности в NGN



Иерархия механизмов обработки информации

Функциональная модель



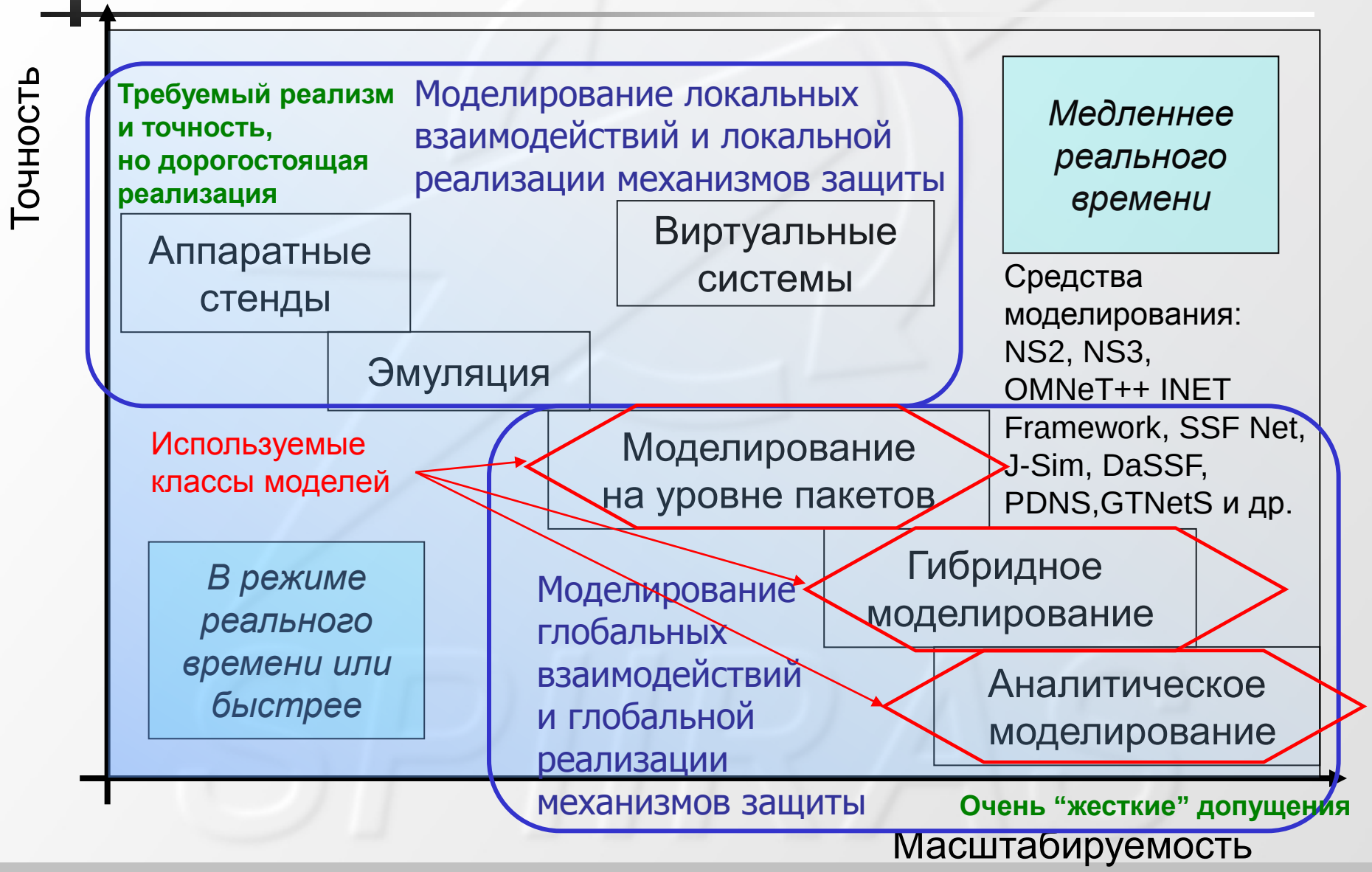
План доклада

- Введение
- Концепция построения системы интеллектуальных сервисов защиты информации
- **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

Спектр используемых моделей



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

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

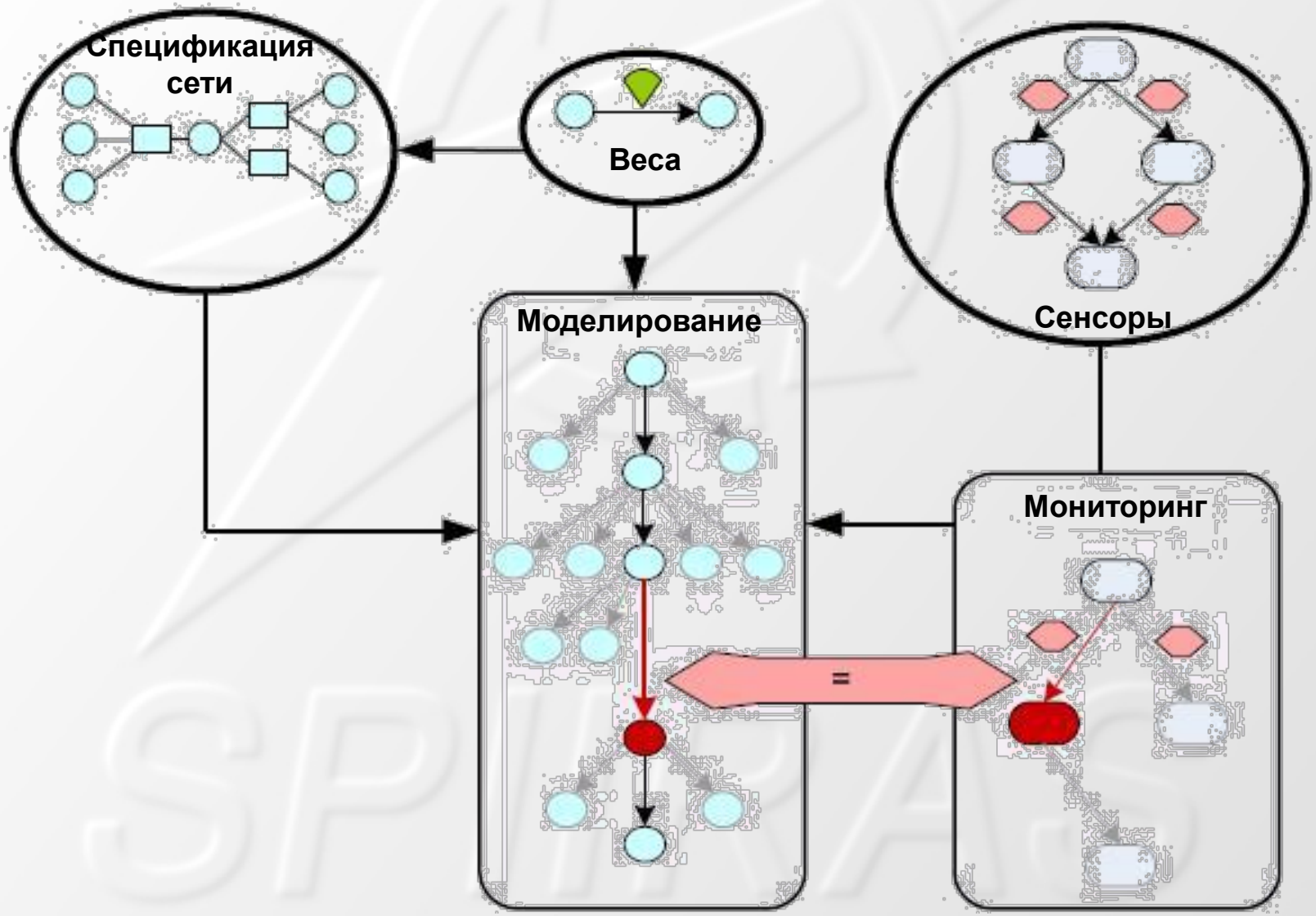
Входные данные (1/2)

Данные	Формат	Источник
Данные о программном и аппаратном обеспечении хостов	CPE (Common Platform Enumeration, http://cve.mitre.org/)	знания оператора и данные от средств сбора информации
Топология сети	XML	знания оператора и данные от средств сбора информации
Графы зависимостей сервисов	XML	знания оператора и данные от средств сбора информации
Возможные контрмеры	CRE (Common Remediation Enumeration)	знания оператора и данные из Интернет
Политики безопасности и настройки ПО	CCE (Common Configuration Enumeration, http://cce.mitre.org/)	знания оператора и данные от средств сбора информации

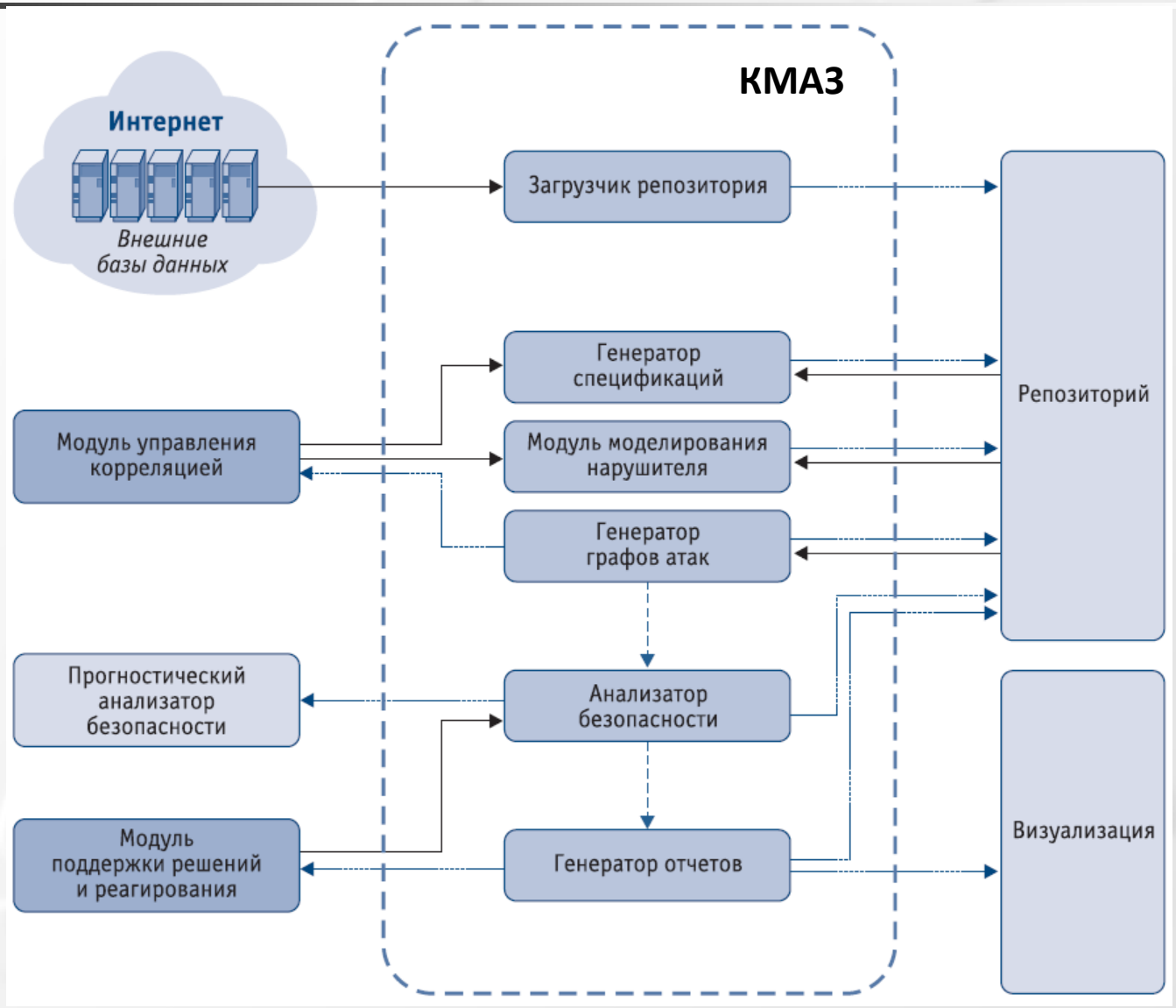
Входные данные (2/2)

Данные	Формат	Источник
Требования к безопасности	XML (требуемый уровень защищенности, ценность информации на хостах)	знания оператора, предварительно заданные данные
Уязвимости	CVE (Common Vulnerabilities and Exposures, http://cve.mitre.org/)	National Vulnerability Database Version 2.2, http://nvd.nist.gov/download.cfm)
Данные о шаблонах атак	CAPEC (Common Attack Pattern Enumeration and Classification, http://capec.mitre.org/)	данные из Интернет и знания оператора
Модель нарушителя	XML	знания оператора, предварительно заданные данные
Метрики безопасности	CVSS (Common Vulnerability Scoring System)	National Vulnerability Database

Анализ событий безопасности



Архитектура компонента аналитического моделирования



План доклада

- Введение
- Концепция построения системы интеллектуальных сервисов защиты информации
- Сервисы аналитического моделирования
- **Сервисы анализа защищенности**
- Сервисы визуализации
- Заключение

Уровни оценки защищенности

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.

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.

Методика экспресс оценки уровня защищенности

- Объединяет качественный и количественный подходы к оценке показателей защищенности и позволяет определить общий уровень защищенности.
- Риск определяется как результат возможности/вероятности угрозы и последствий ее реализации для системы.
- Используется CVSS (для определения критичности атакующих действий) и методику FRAP (Facilitated Risk Analysis Process) .

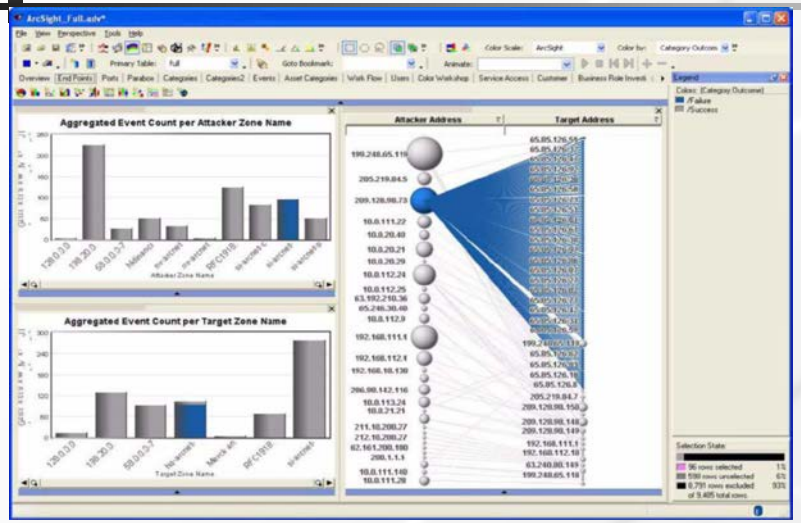
План доклада

- Введение
- Концепция построения системы интеллектуальных сервисов защиты информации
- Сервисы аналитического моделирования
- Сервисы анализа защищенности
- **Сервисы визуализации**
- Заключение

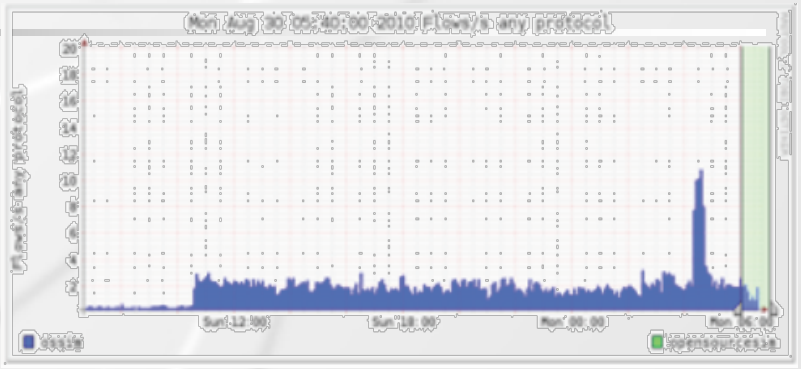
Модели представления данных и их применение

- 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

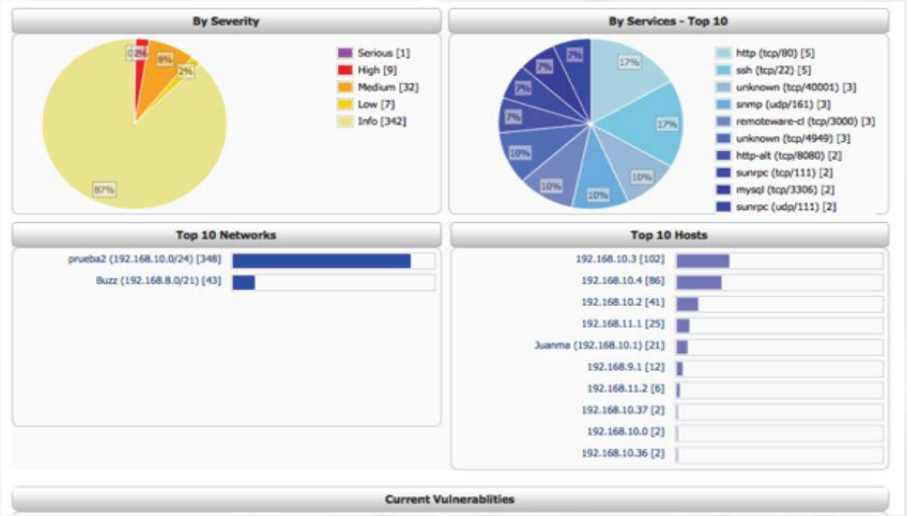
Модели визуализации в SIEM-системах



Arcsight: обнаружение атак



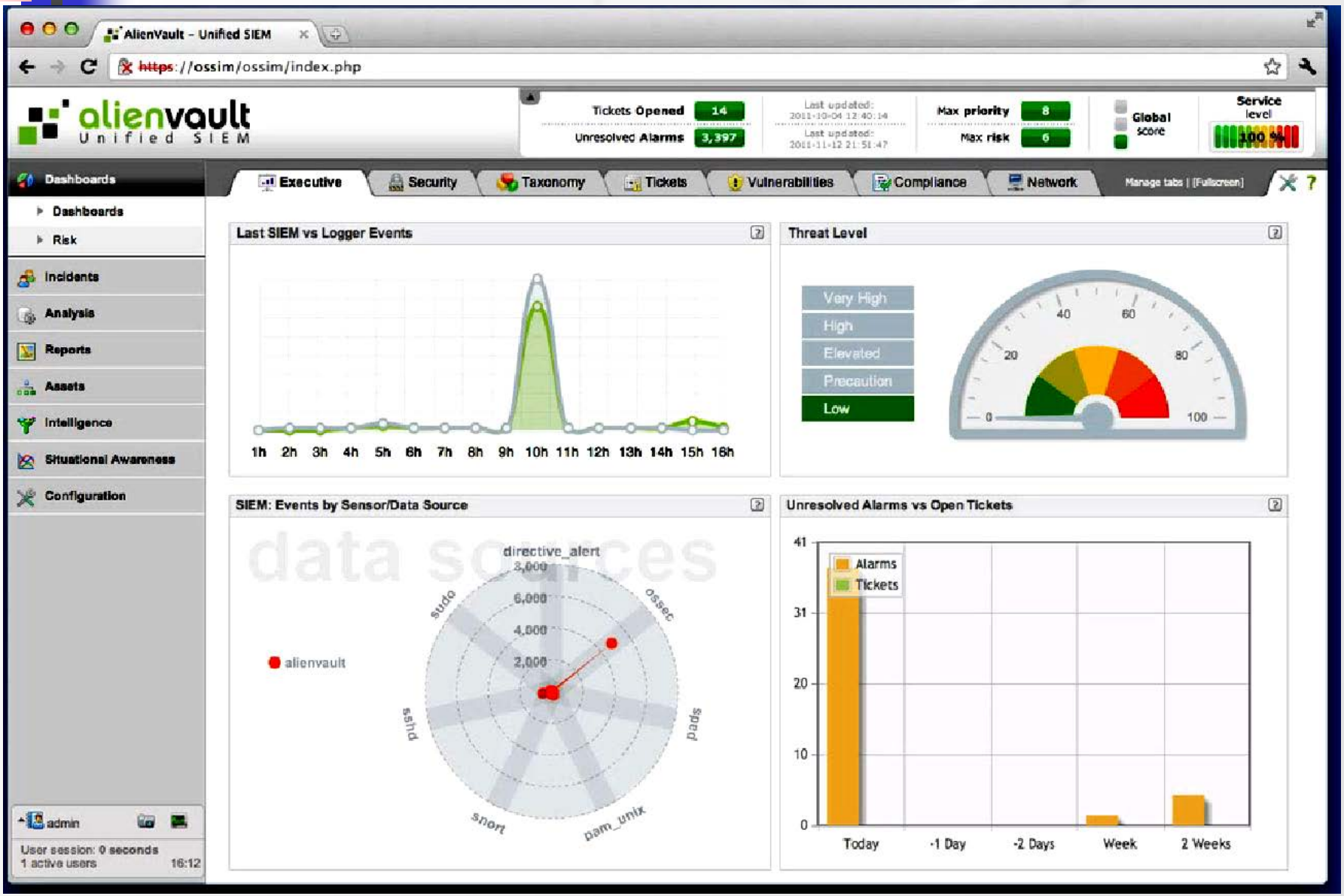
OSSIM: визуализация сетевого трафика



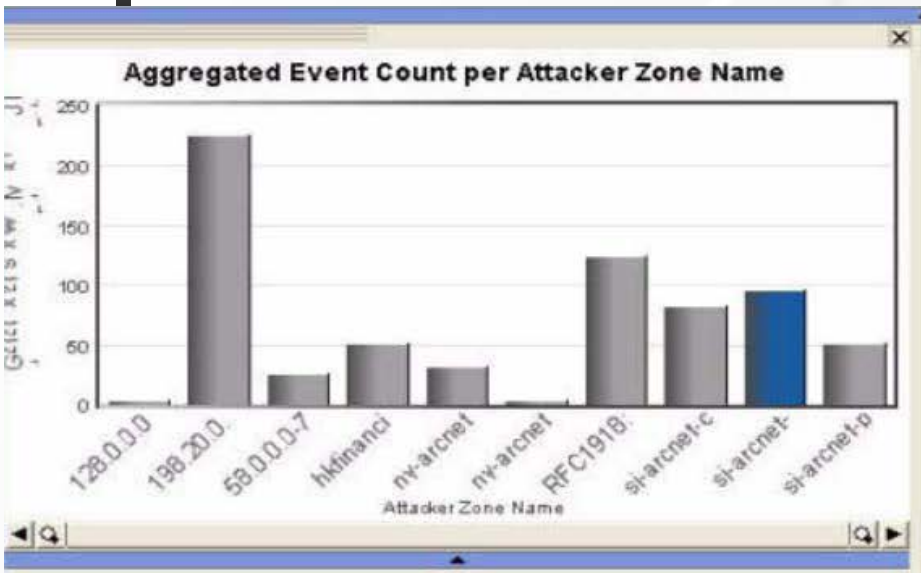
OSSIM: отчет об уязвимостях

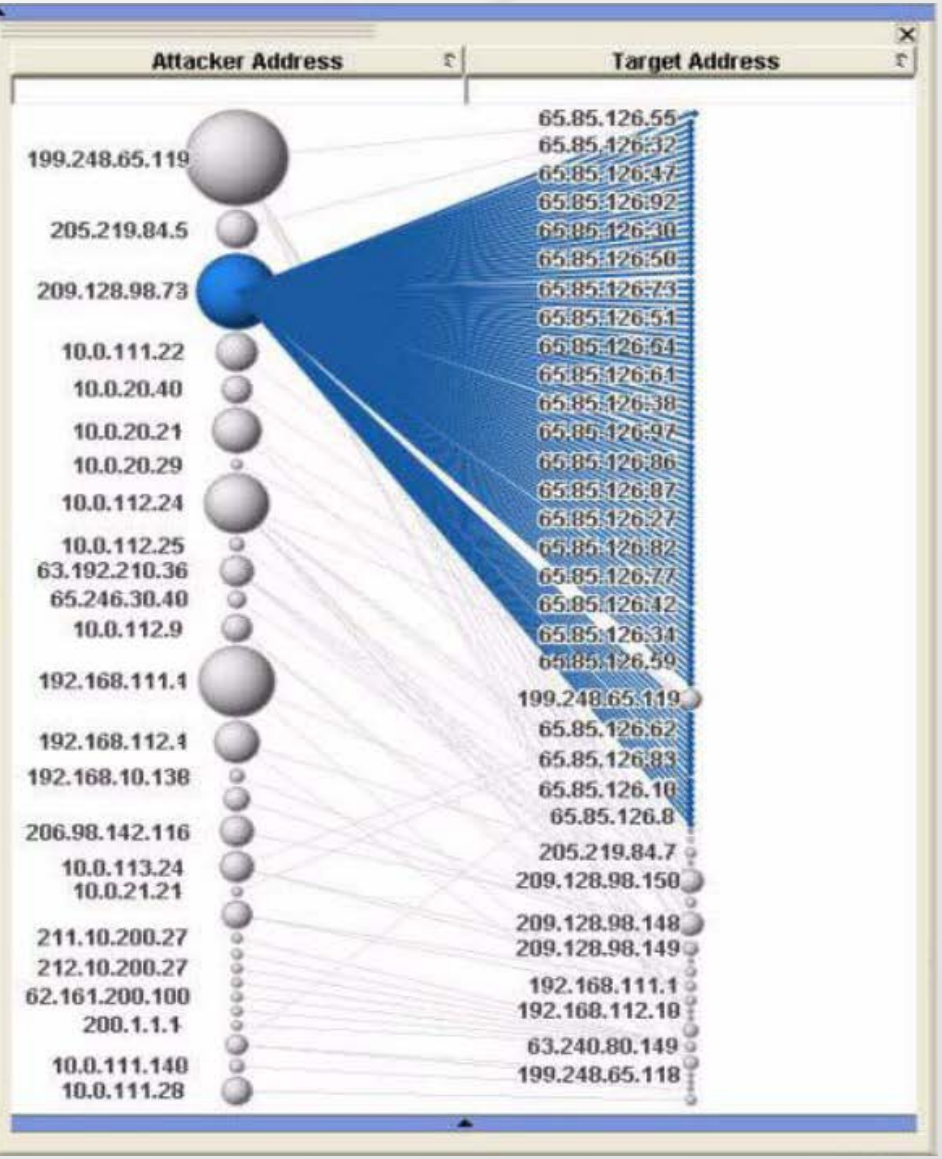
TSIEM: представление правил доступа

(1) OSSIM: панель управления

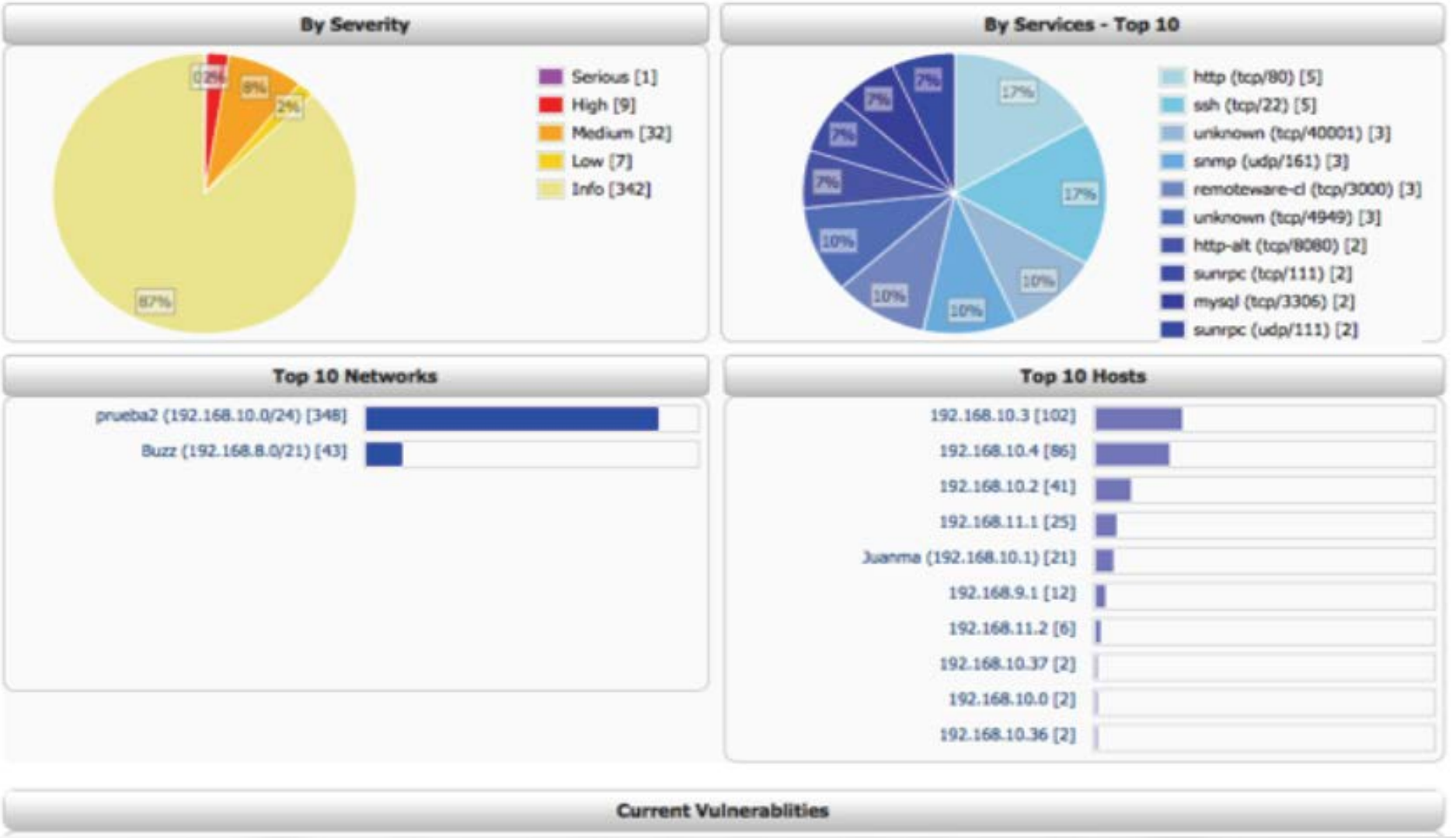


(2) Arcsight: панель анализа атак



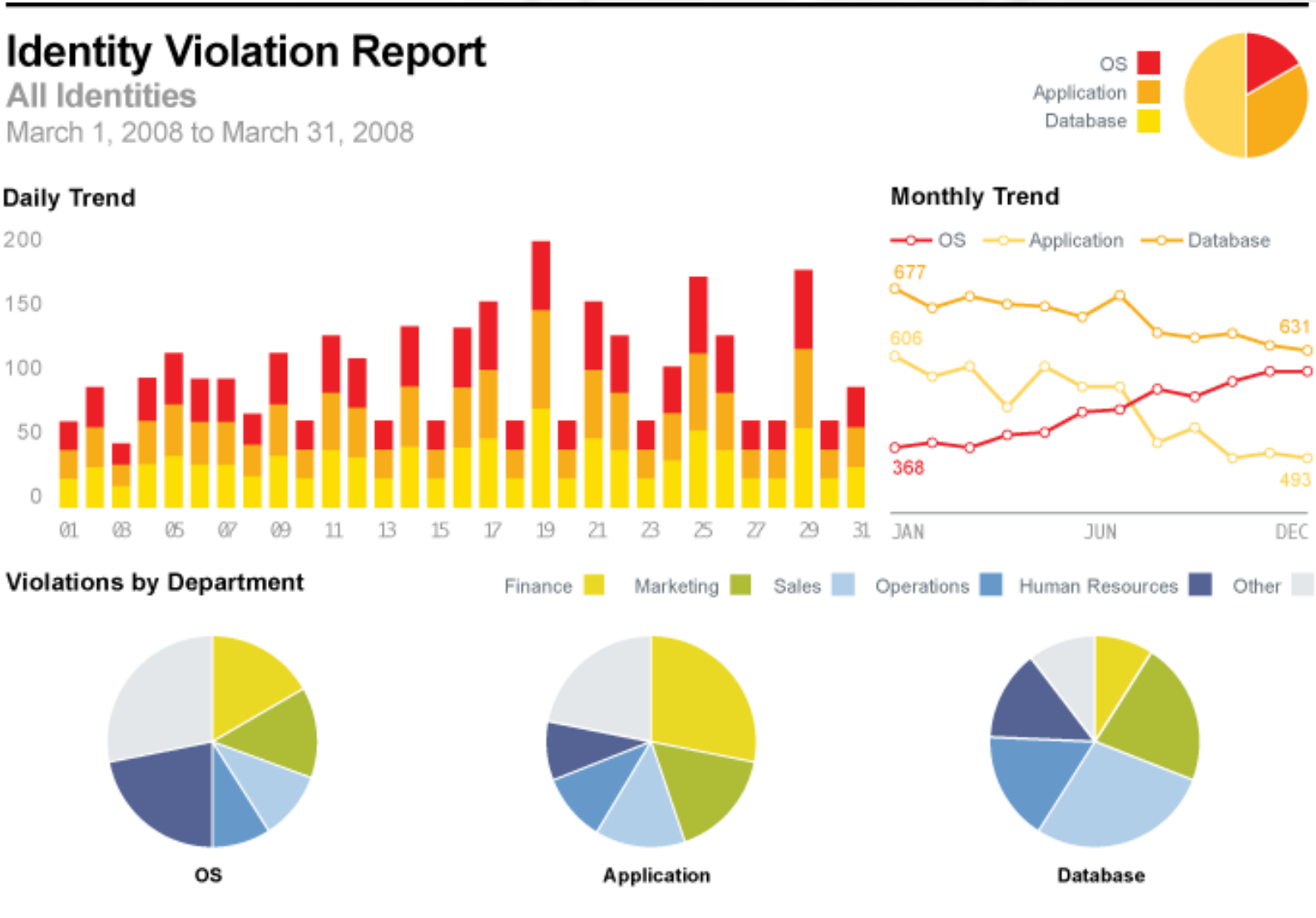


(3) OSSIM: отчет об уязвимостях

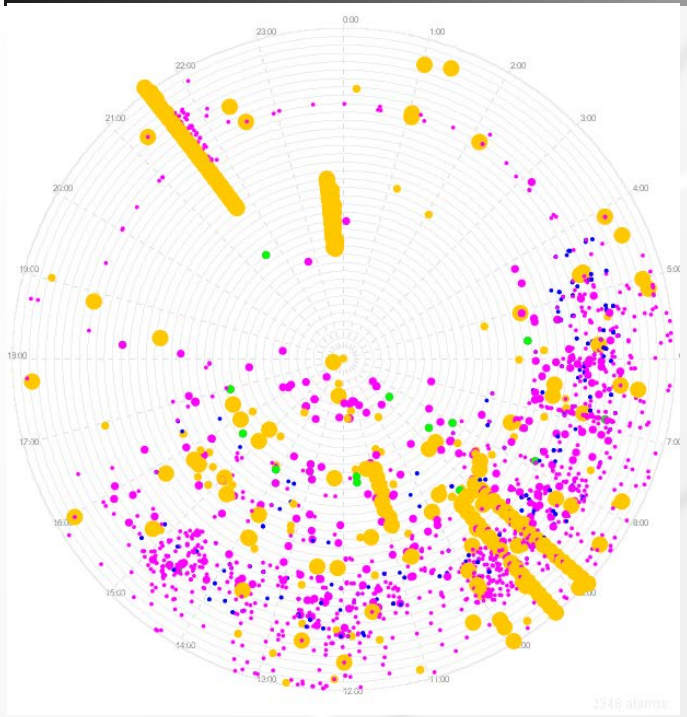


(4) TSIEM: представление правил доступа

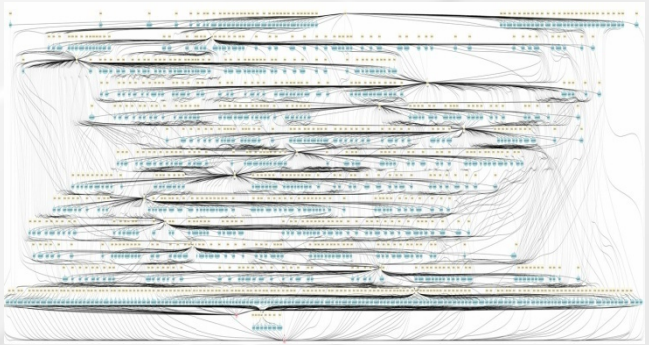
(5) NetIQ Sentinel: отчет о нарушениях политики безопасности



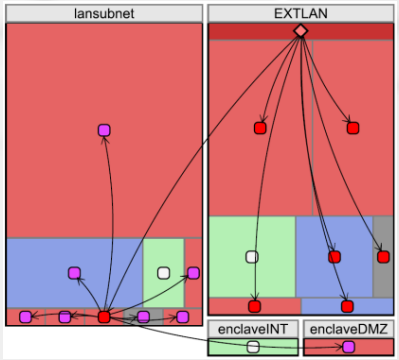
Модели визуализации для представления событий и анализа защищенности

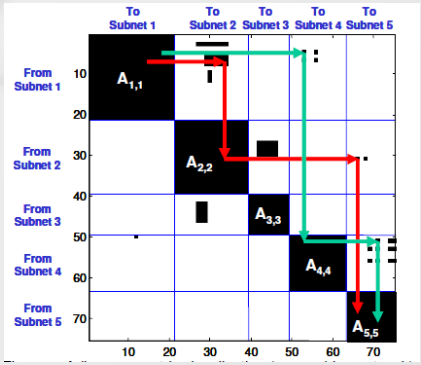


Представление событий в SpiralView [1]



Визуализация атак на основе графов [2]





Альтернативные представления атак [3, 4]

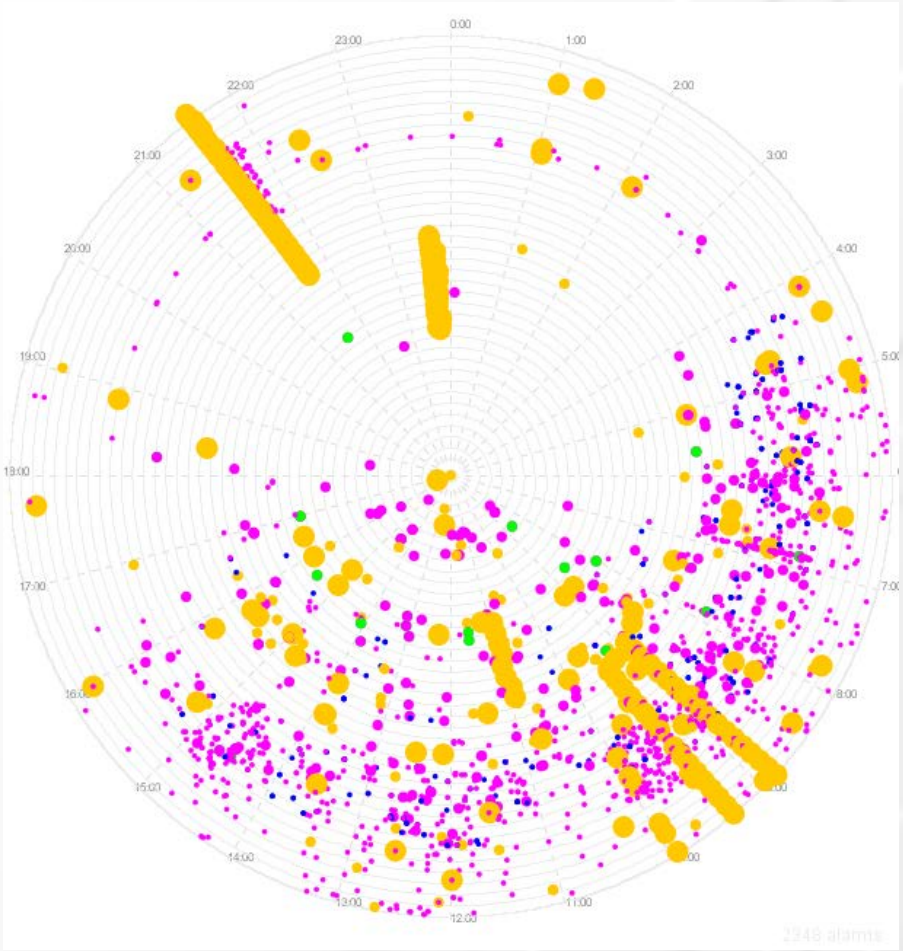
[1] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. In Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007. pp.139-146.

[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.

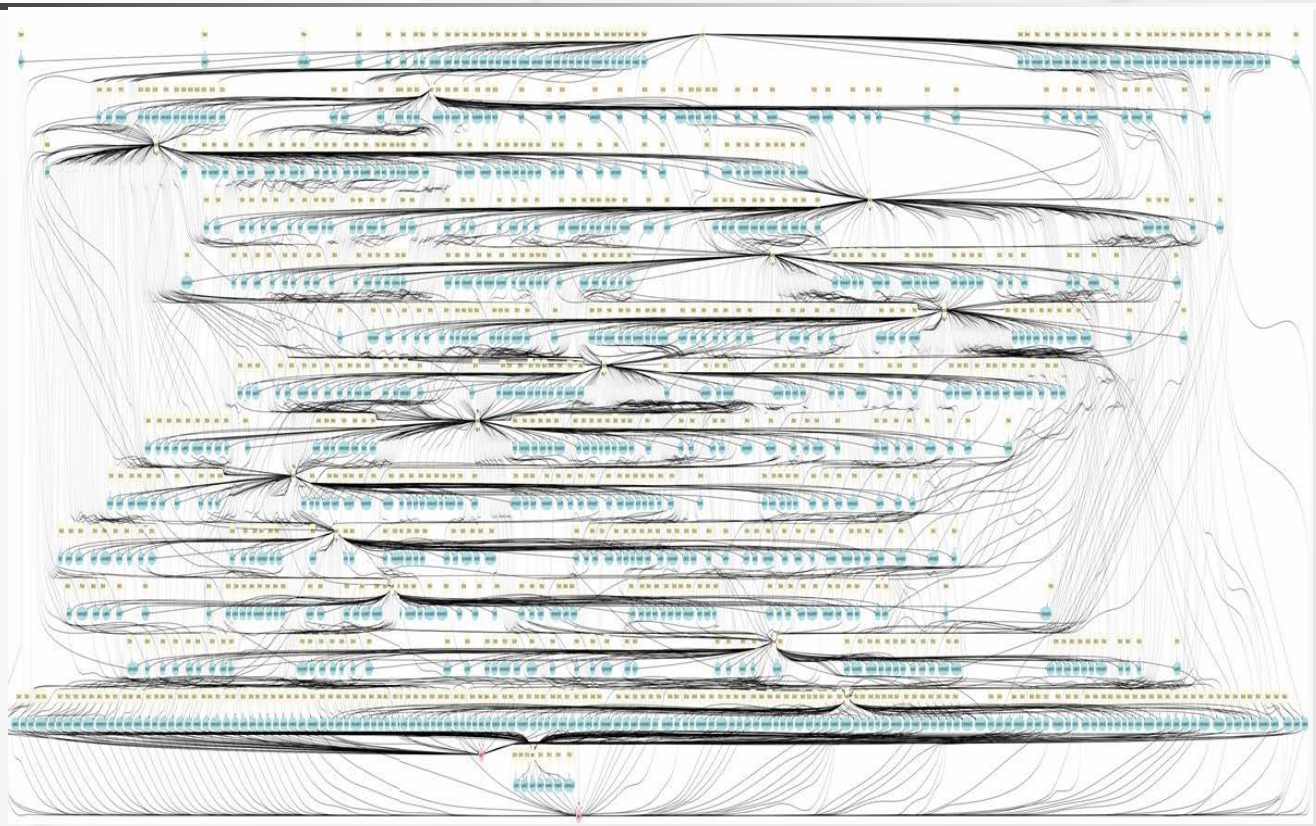
[4] Noel S., Jajodia S. Understanding complex network attack graphs through clustered adjacency matrices. In Proceedings of the 21st Annual Computer Security Applications Conference, 2005, pp.160-169.

(1) 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.

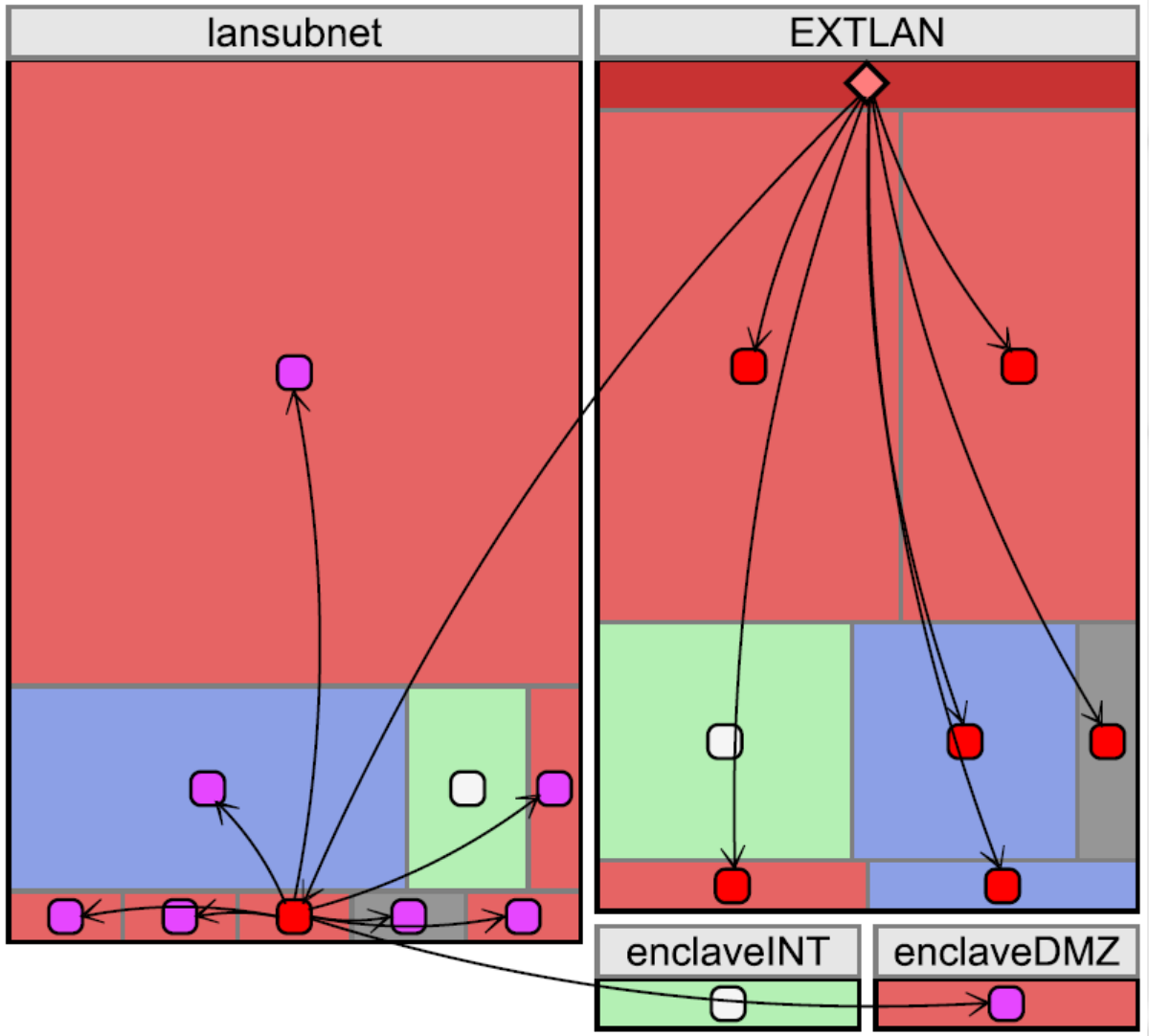
(2) Визуализация атак на основе графов [Noel, 2004]



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.

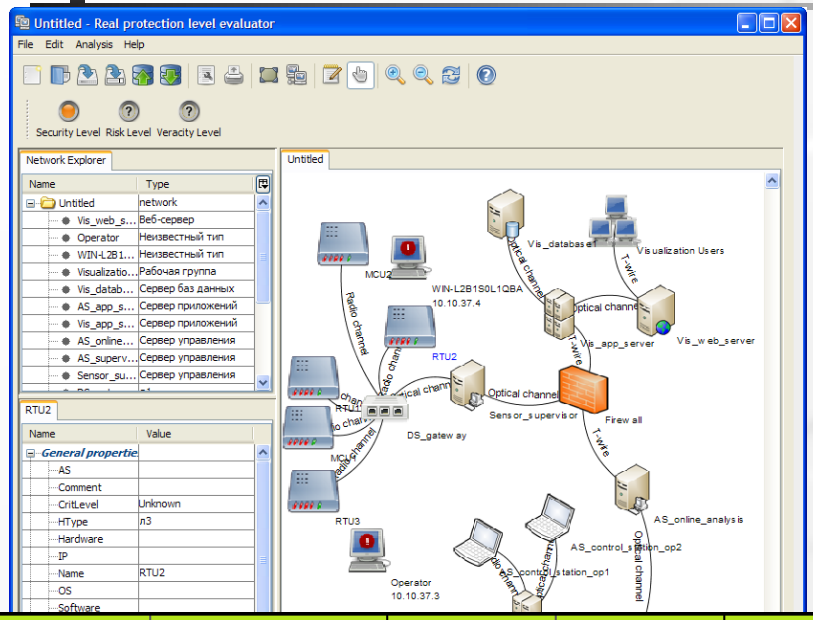
(3) Представление графа атак в виде карты деревьев [Williams et al., 2008]

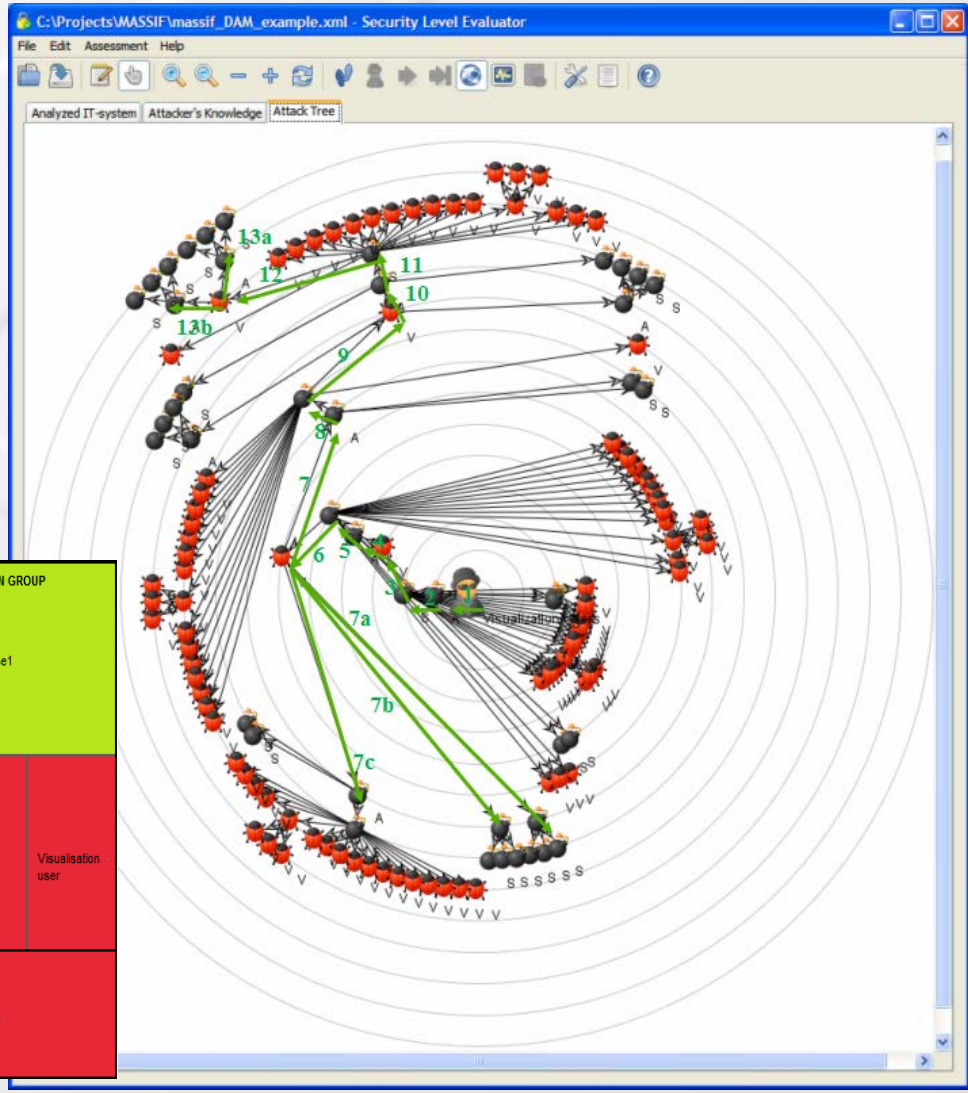


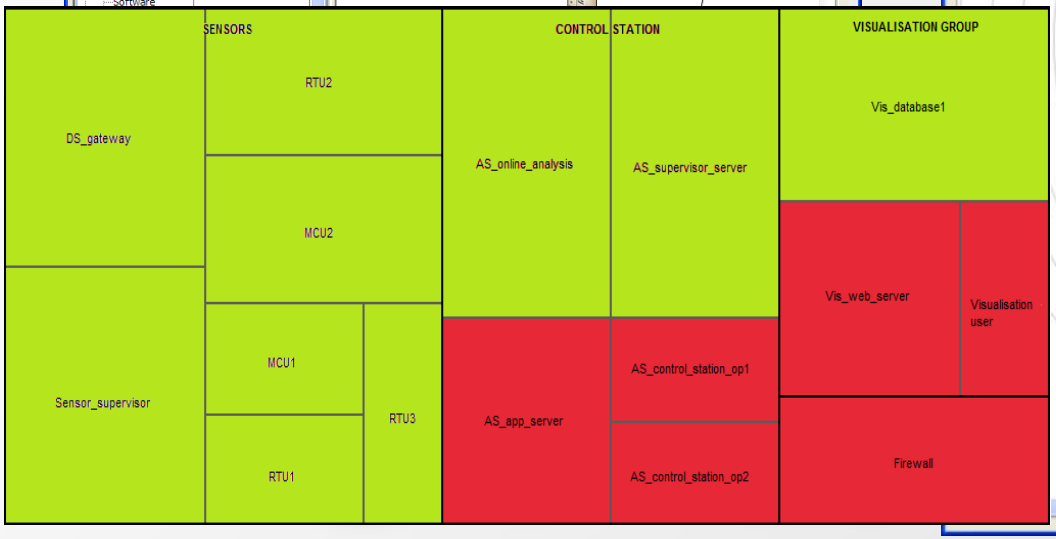
- Каждая подсеть представляется в виде карты деревьев, вложенные прямоугольники - узлы, с помощью цвета кодируются различные атрибуты узлов, а размер пропорционален числу скомпрометированных узлов в подсети
- Режимы взаимодействия с картами деревьев:
  (1) оценка достижимости узлов в результате атаки;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

Архитектура подсистемы визуализации

Примеры интерфейсов компонента моделирования и анализа защищенности







Главное окно (1/2)

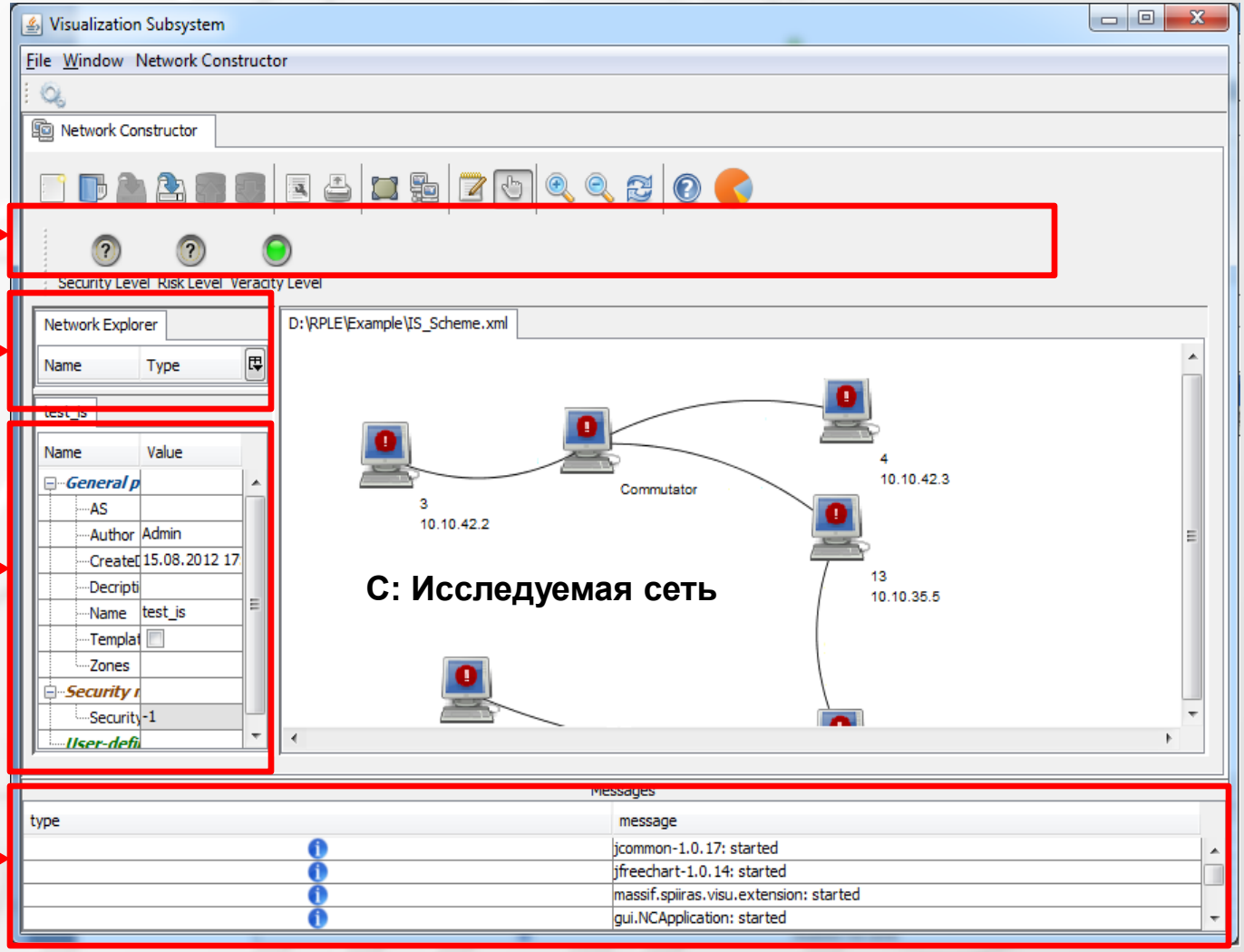
При спецификации сети

D: Network security metrics
Для быстрого доступа

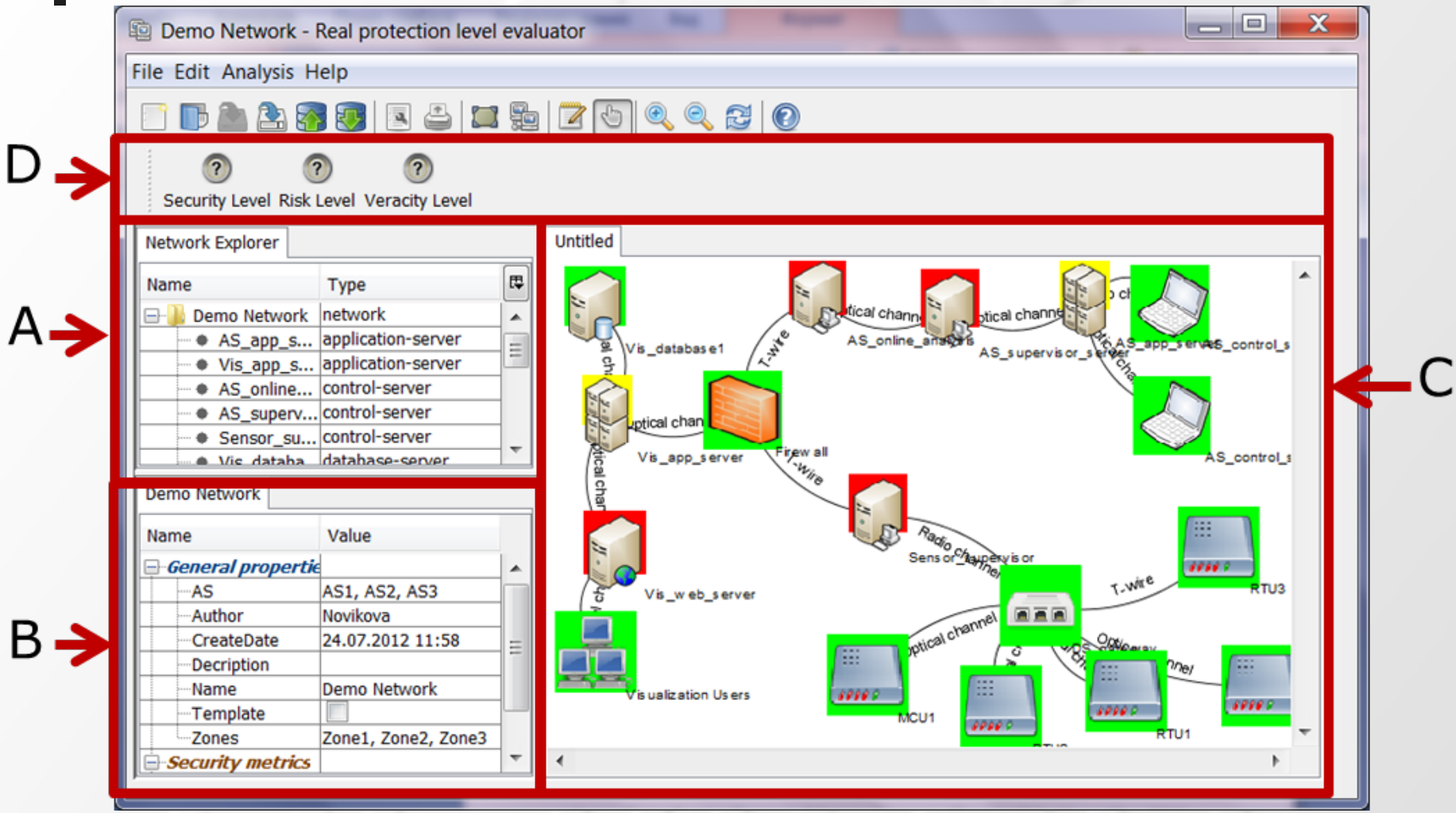
A: Network Explorer
Для быстрого просмотра сети

B: Property explorer
Для конфигурирования узлов сети

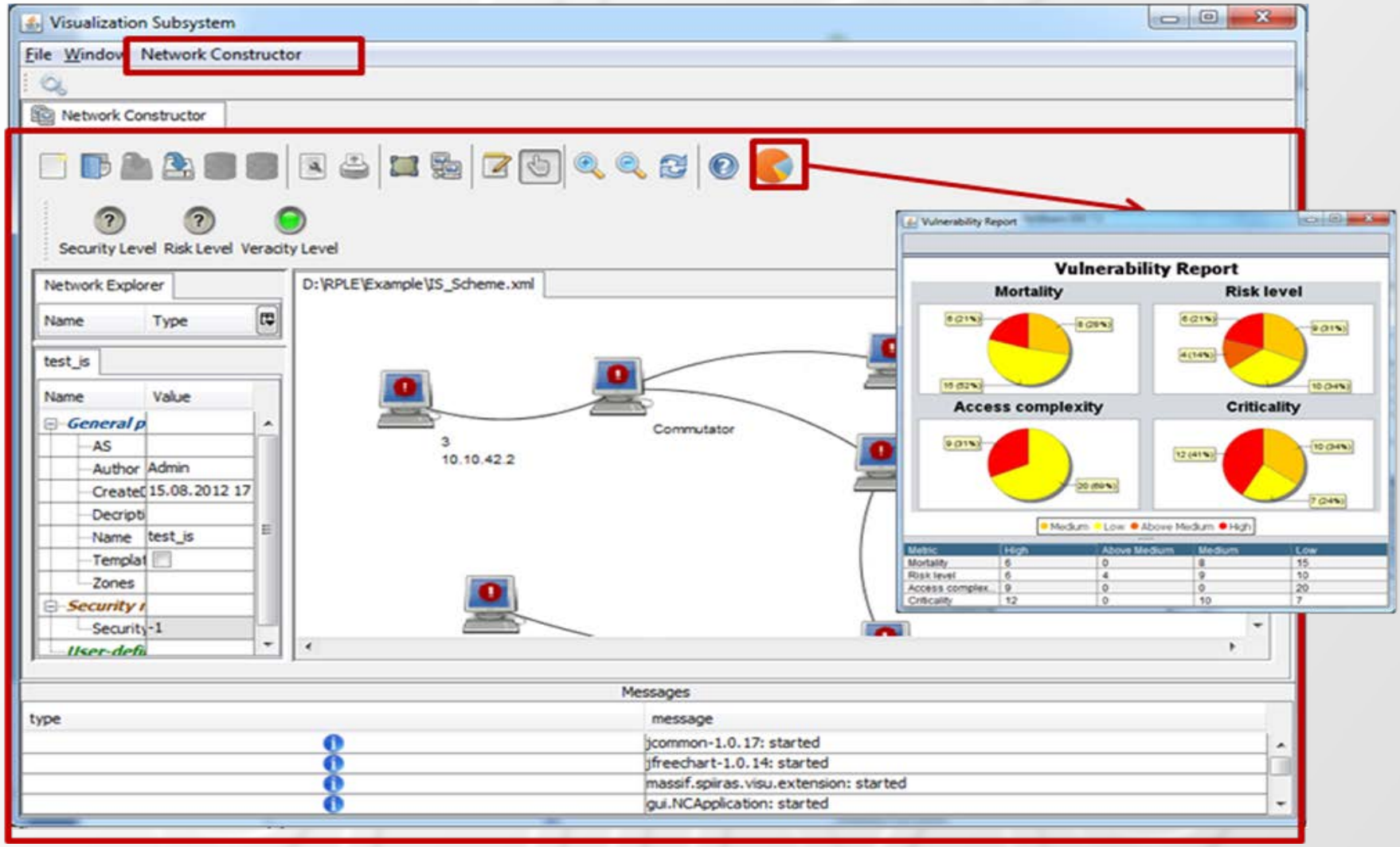
System messages



Главное окно (2/2)

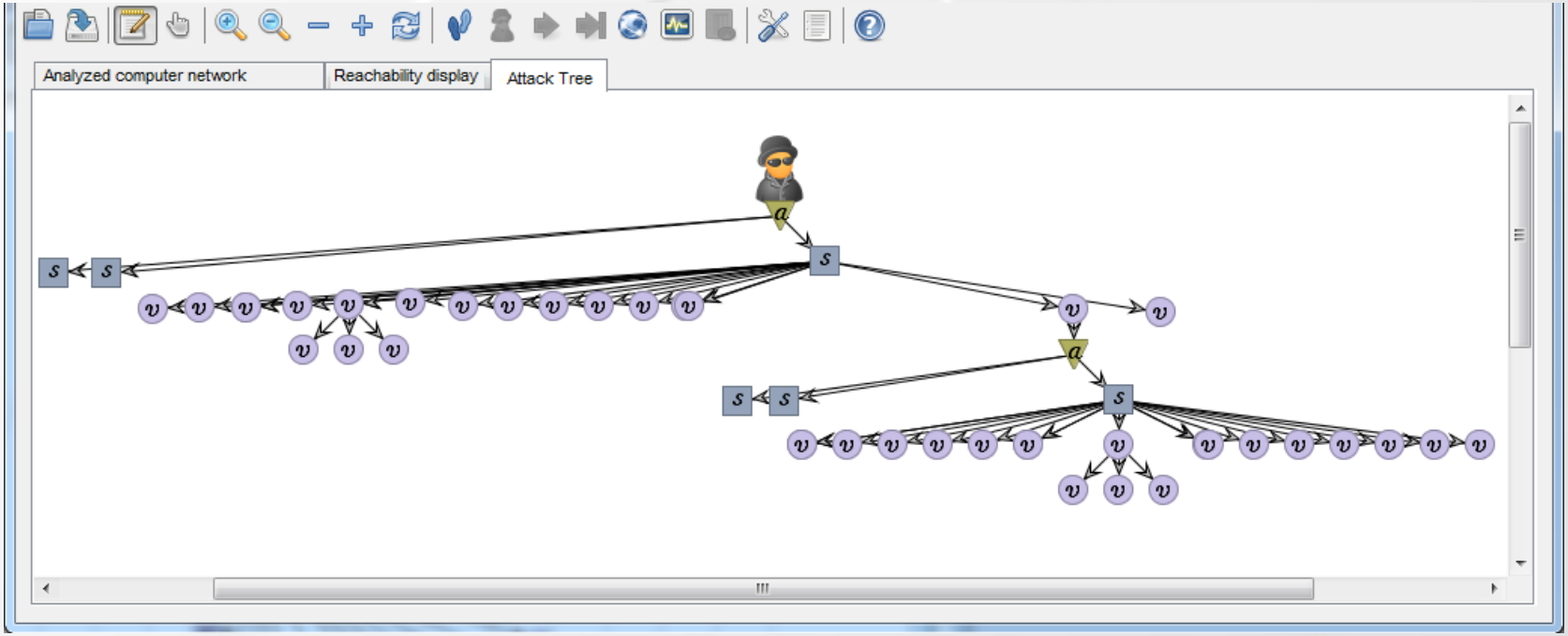


Отображение отчета об уязвимостях



Представление графов атак (1/2)

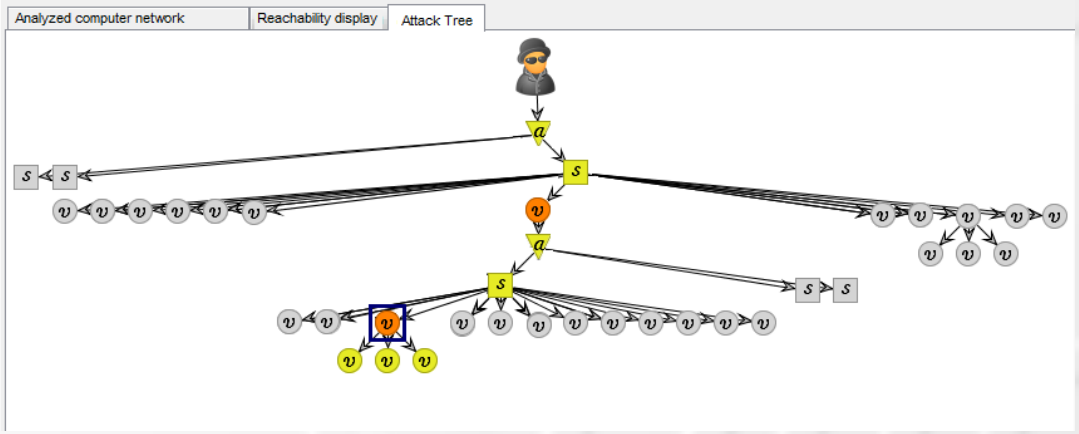
Обозначение	Описание
	Исходное положение нарушителя
	Специфическое атакующее действие
	Сценарий, не использующий уязвимости
	Атакующее действие, использующее уязвимость



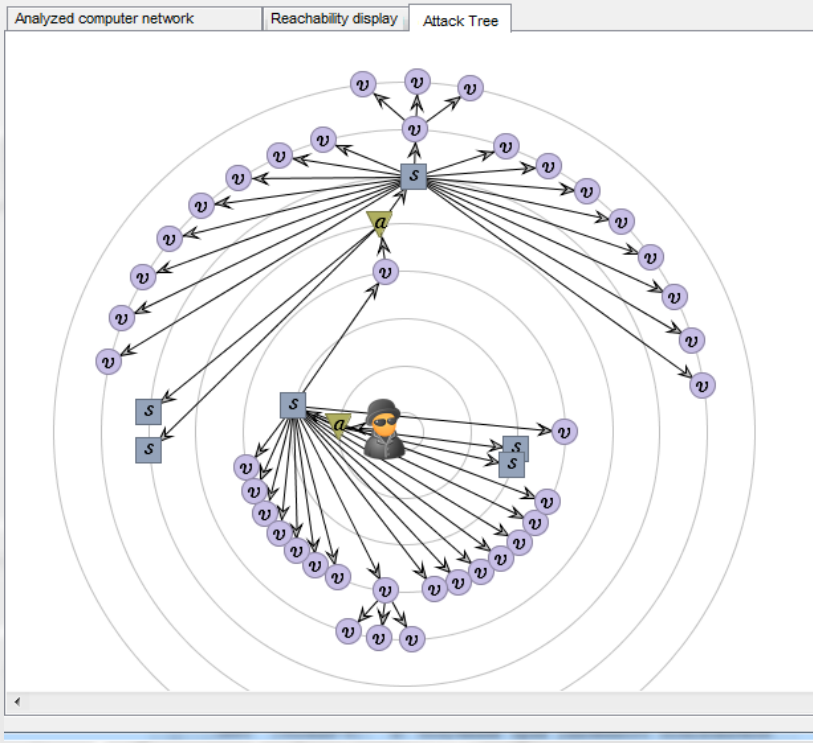
Представление графов атак (2/2)

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

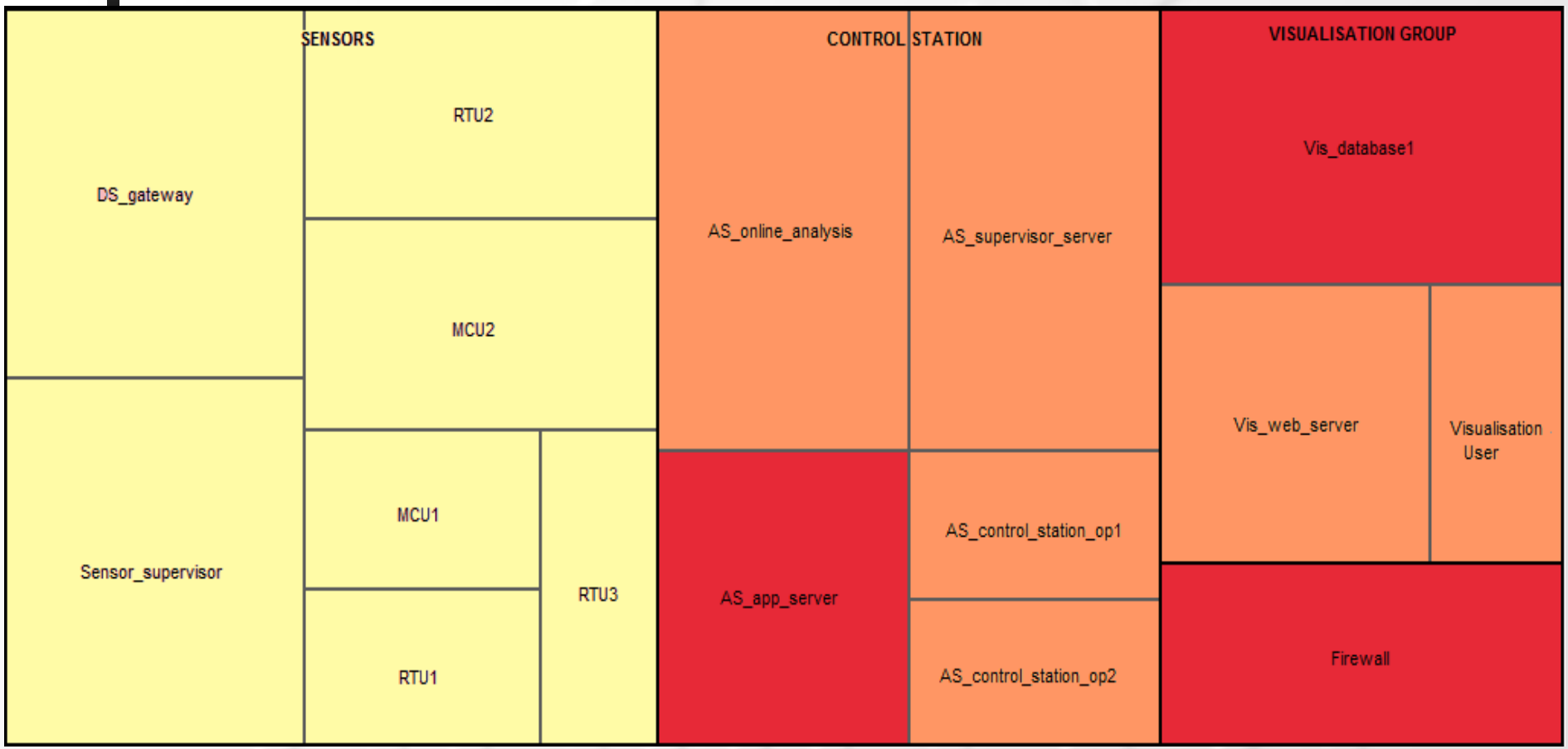


Древовидное представление и эффект подсветки и связывания



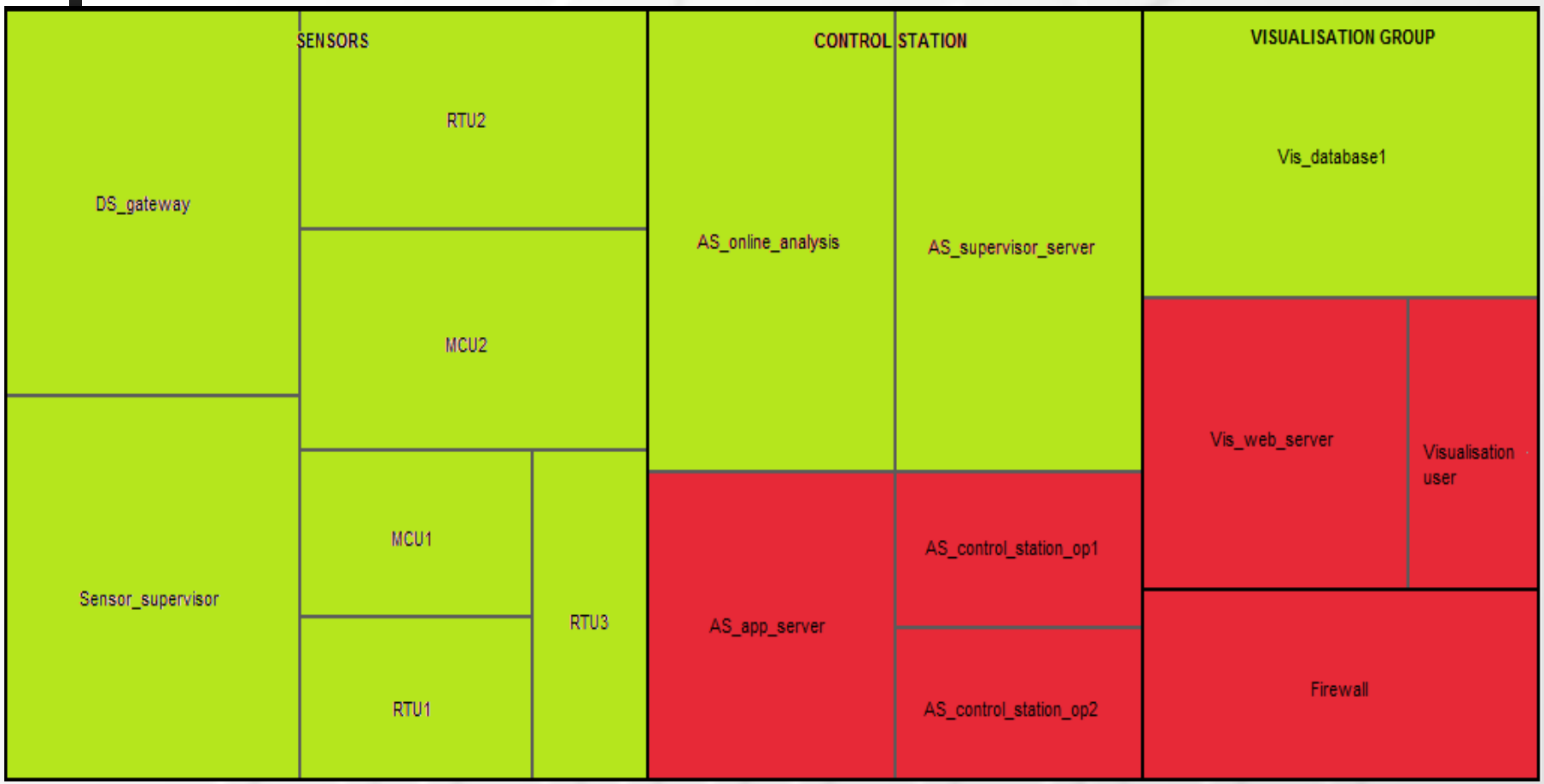
Радиальное представление

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 показателей защищенности верхнего уровня

Показатели защищенности (защищенность, риск, достоверность)

Уровень защищенности

- Не определен
- зеленый (сеть защищена)
- желтый (Low Criticality)
- оранжевый (Medium Criticality)
- красный (High Criticality)

План доклада

- Введение
- Концепция построения системы интеллектуальных сервисов защиты информации
- Сервисы аналитического моделирования
- Сервисы анализа защищенности
- Сервисы визуализации
- **Заключение**

Основные результаты работы

- Представлен подход к построению перспективных **систем проактивного управления информацией и событиями безопасности** для NGN.
- Предложена архитектура **системы проактивного управления информацией и событиями безопасности** в NGN
- Предложены методы, модели и алгоритмы, и разработаны первоначальные прототипы средств аналитического моделирования, анализа защищенности и визуализации, реализующие данный подход.

Контактная информация

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

Саенко Игорь Борисович (СПИИРАН)
ivkote@comsec.spb.ru
http://comsec.spb.ru/saenko/

Чечулин Андрей Алексеевич (СПИИРАН)
ivkote@comsec.spb.ru
http://comsec.spb.ru/saenko/

Благодарности

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и государственного контракта №14.BBB.21.0097.

РОССИЙСКАЯ АКАДЕМИЯ НАУК