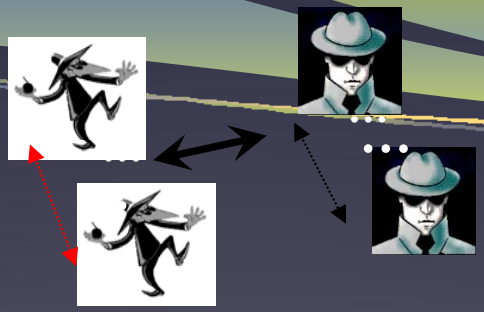


# Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами

***Котенко Игорь Витальевич**, д.т.н., профессор, лаборатория проблем компьютерной безопасности, СПИИРАН,*

***Новикова Евгения Сергеевна**, к.т.н., СПбГЭТУ «ЛЭТИ»,*

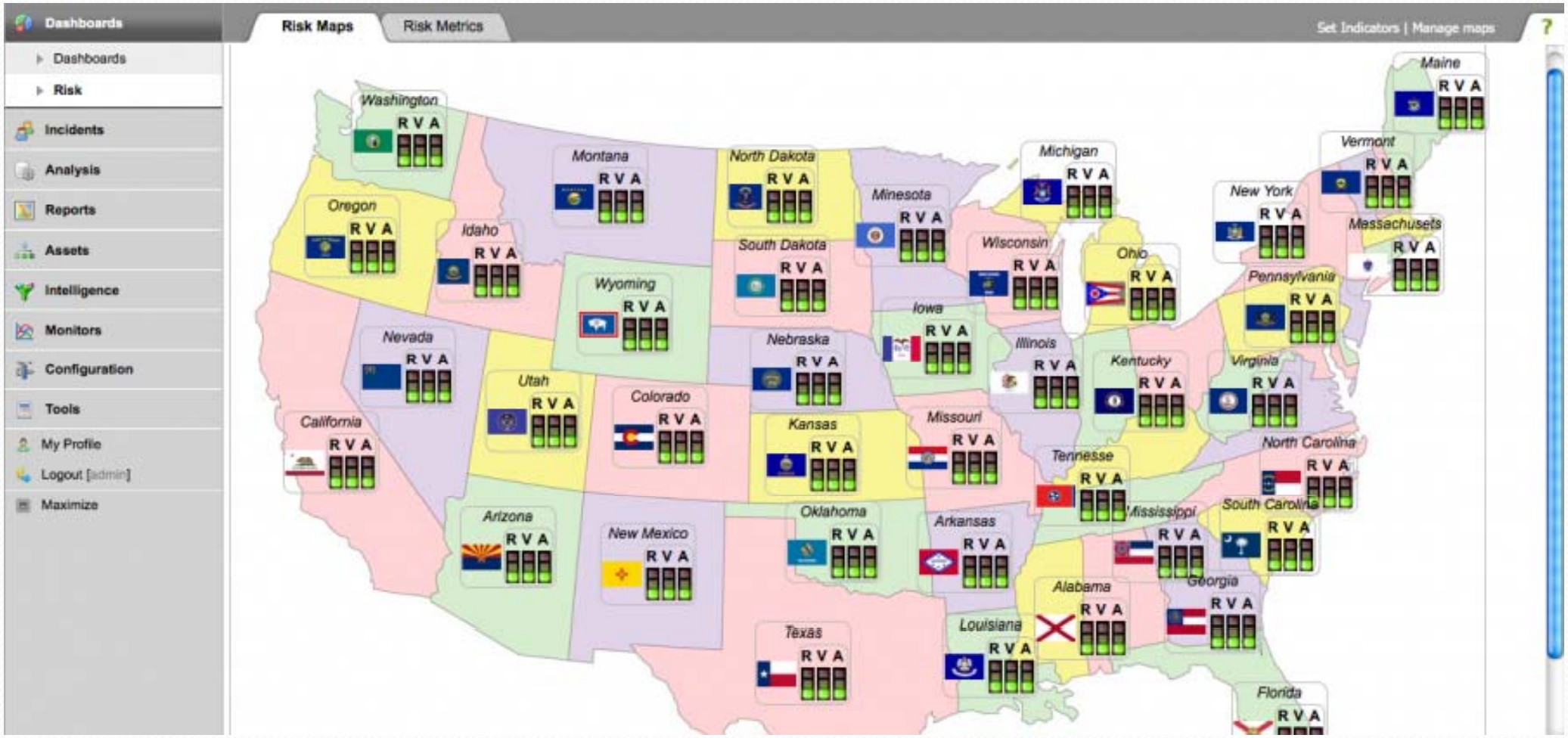
***Архипов Юрий Анатольевич**, ЗАО «НПП «ТЕЛДА»*

**РусКрипто'2015, 17-21 марта 2015 г.**

# План доклада

- Введение
- Релевантные работы
- Визуальная модель
- Метрики защищенности
- Реализация
- Эксперименты
- Заключение

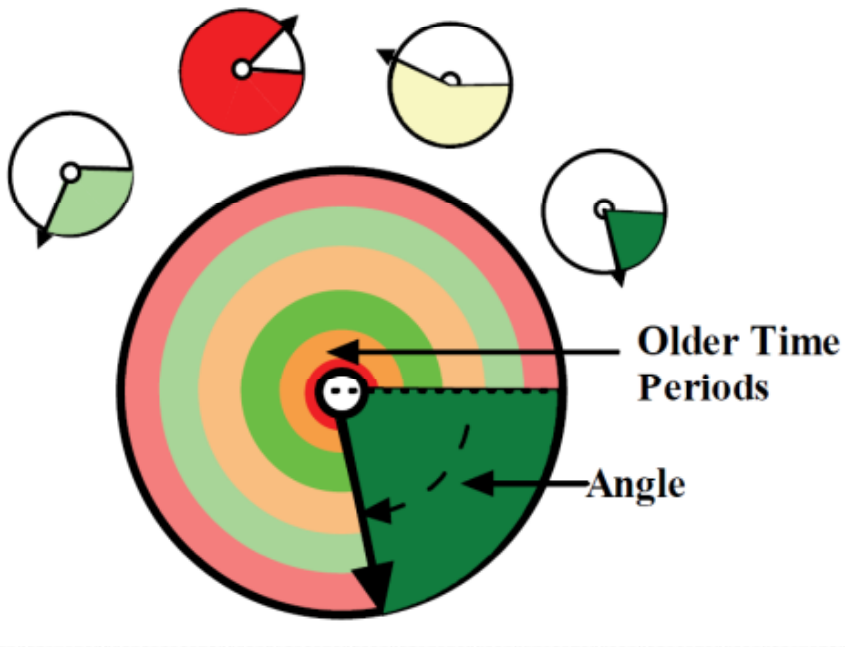
# OSSIM: карта рисков




**Карта рисков** отображает информацию о состоянии риска (R), уязвимостей (V) и доступности (A) каждого сетевого объекта, расположенного на карте в виде светофоров

# Метафора представления метрик защищенности на основе циферблата [Erbacher, 2012]

- Каждая метрика представляется с использованием циферблата, и ее значение "усиливается" цветом, чтобы сделать боле быстрым восприятие. Наружное кольцо соответствует более позднему (текущему) значению
- Набор метрик представляется с помощью множества различных циферблатов (cyber command gauge cluster ) для поддержки принятия контрмер и выполнения других задач защиты информации

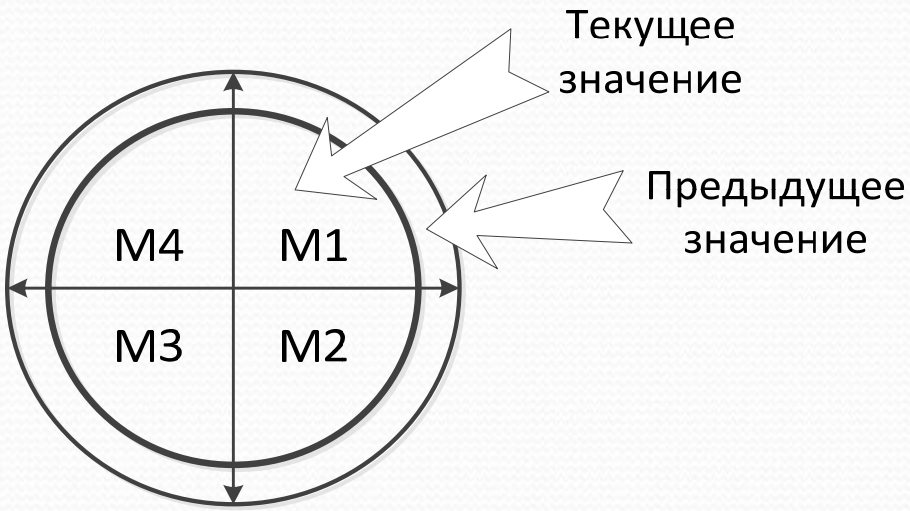


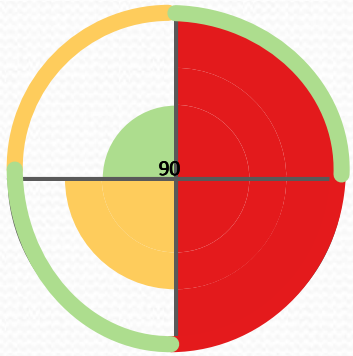
# Модель оперативного индикатора доверия [Matuszak et al., 2013]

- В одном индикаторе отображается три типа доверия, цвет используется для задания значения доверия
- Эти параметры представляются в виде части наружного кольца круга. Круг в центре обозначает общее доверие, рассчитываемое как взвешенная сумма других видов доверия

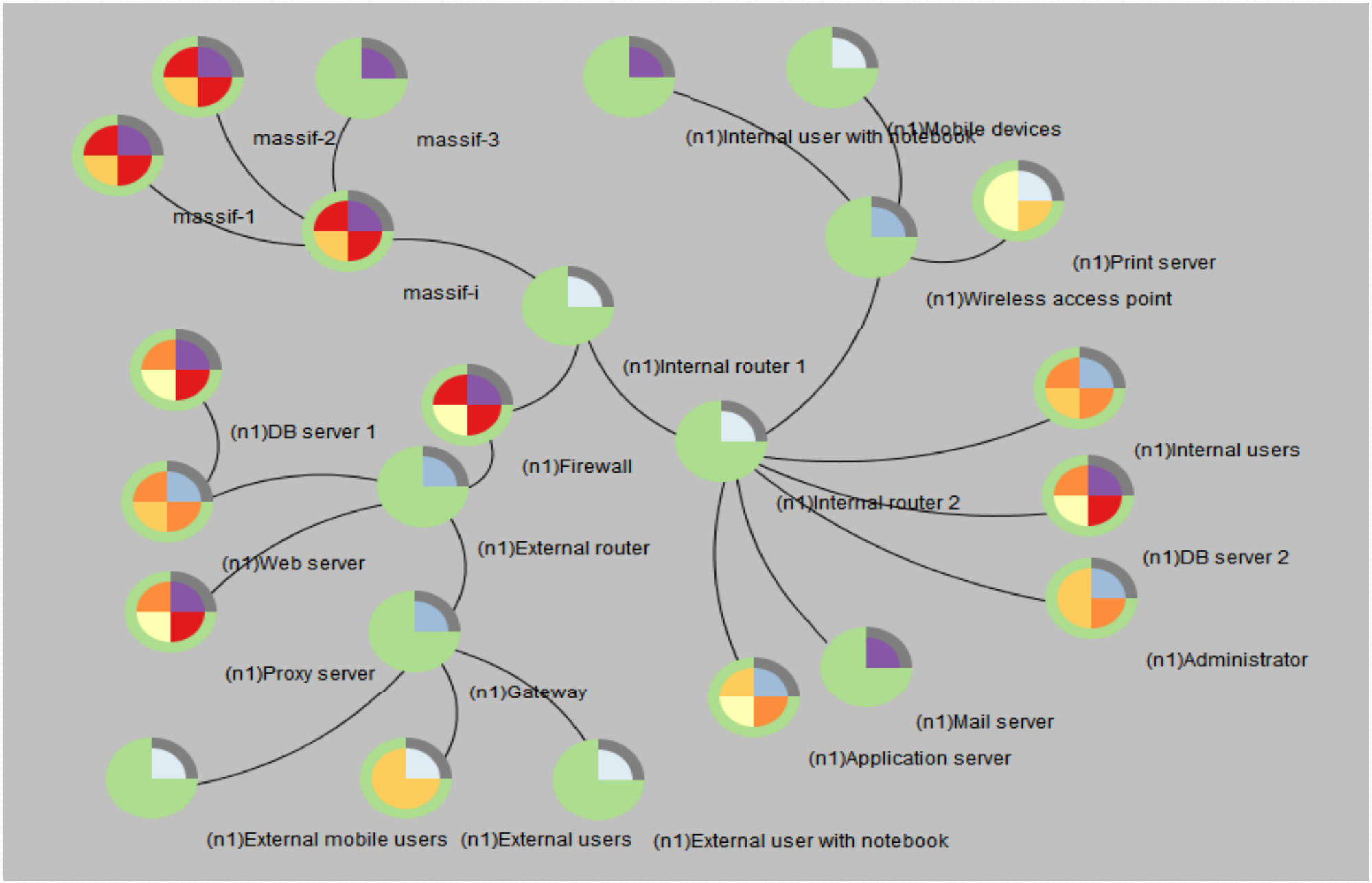
# Предлагаемое представление метрик защищенности

- Для предоставления пользователям возможности анализировать несколько метрик предложена модель визуализации (глиф) на основе кругов, способная отображать предыдущие значения метрик
- Круг разделяется на n секторов, которые отображают значения n метрик. Внешние кольца представляют предыдущие значения
- Для отображения критичности значения используется цвет
- Модификация этой модели – от критичности значения метрики зависит радиус сектора

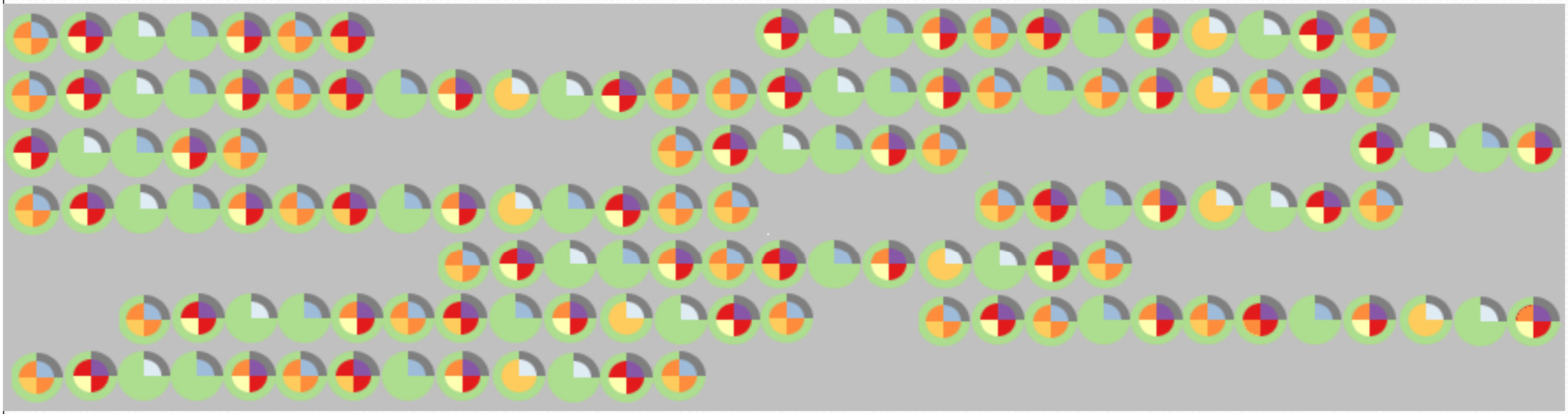


# Отображение глифов на топологии сети

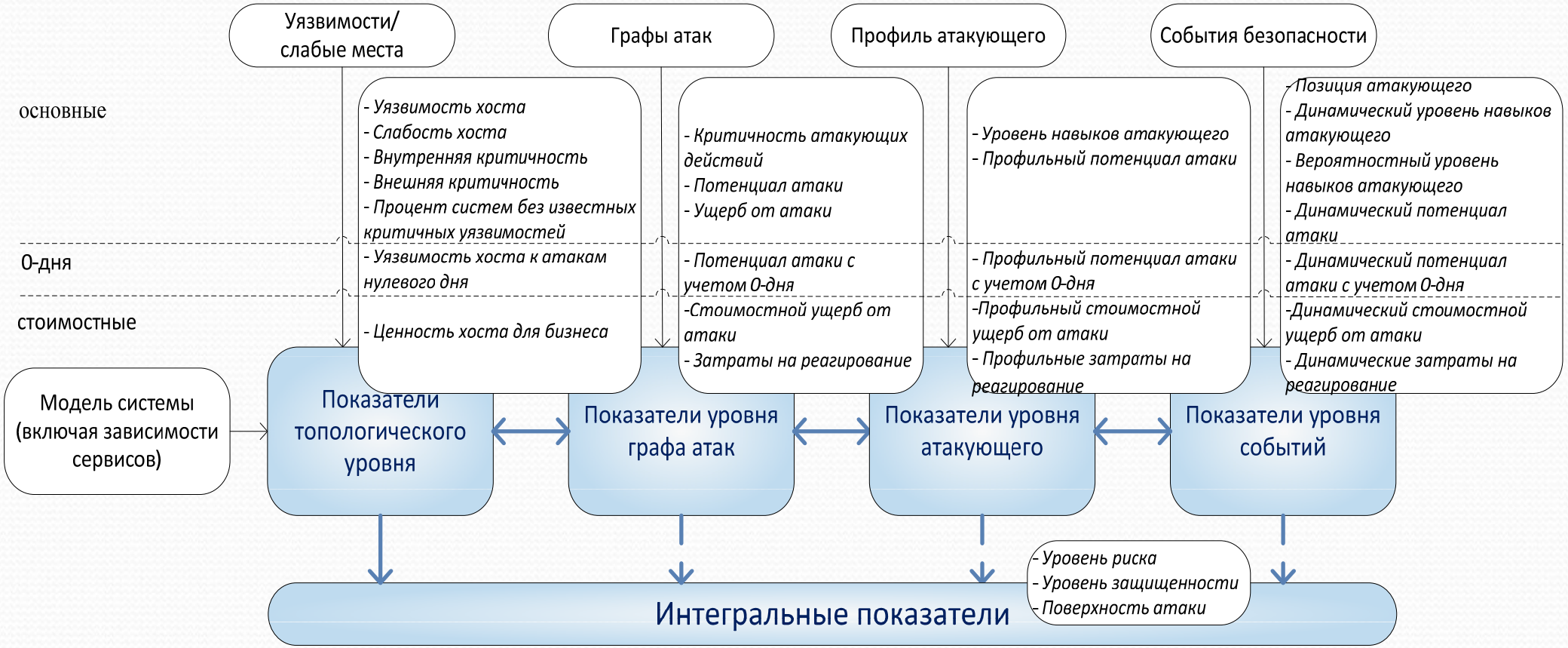


# Представление больших сетей в виде матрицы глифов



- подсети расположены на оси ординат, а отдельные хосты расположены на оси абсцисс
- для поддержки навигации и анализа данных обеспечиваются функции зуммирования или специальных механизмов масштабирования, таких как волшебный объектив (magic lens) или рыбий глаз (fisheye)

# Классификация метрик защищенности



# Подсистема визуализации VisSecAnalyzer: цели и задачи

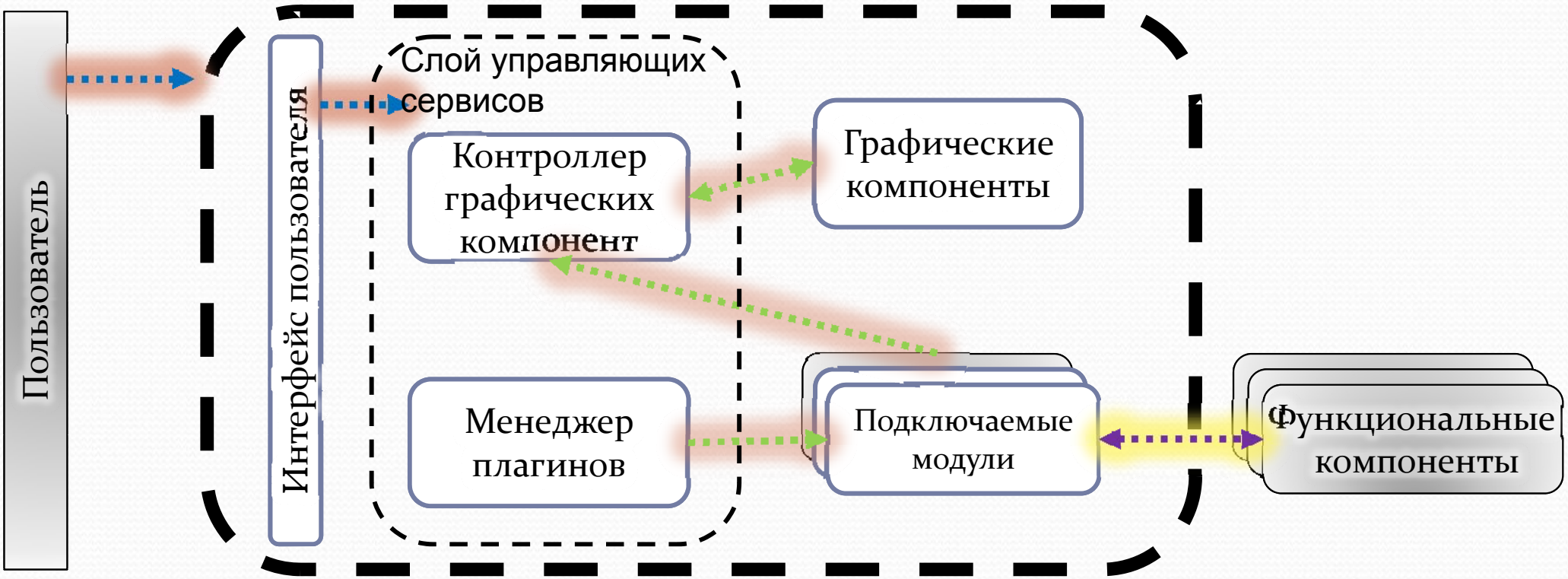
**VisSecAnalyzer - подсистема визуализации для SIEM-компонентов, включая систему моделирования атак и оценивания защищенности (AMSEC)**

**Задачи VisSecAnalyzer:**

- Визуализация графов атак , сгенерированных AMSEC
- Визуализация метрик защищенности, вычисленных AMSEC
- Конфигурирование сетей и хостов сети
- Загрузка и сохранение конфигурации сети из/в файл или базу данных
- Загрузка отчетов об уязвимостях, сформированных сканерами уязвимостей
- Реализация экспериментов “что-если” для оценки последствий эксплуатации уязвимостей

# Архитектура подсистемы визуализации VisSecAnalyzer

- Компонент SIEM-системы
- Функциональная расширяемость
- Гибкая связь между компонентами
- Независимая разработка модулей



# Графический интерфейс VizSecAnalyzer

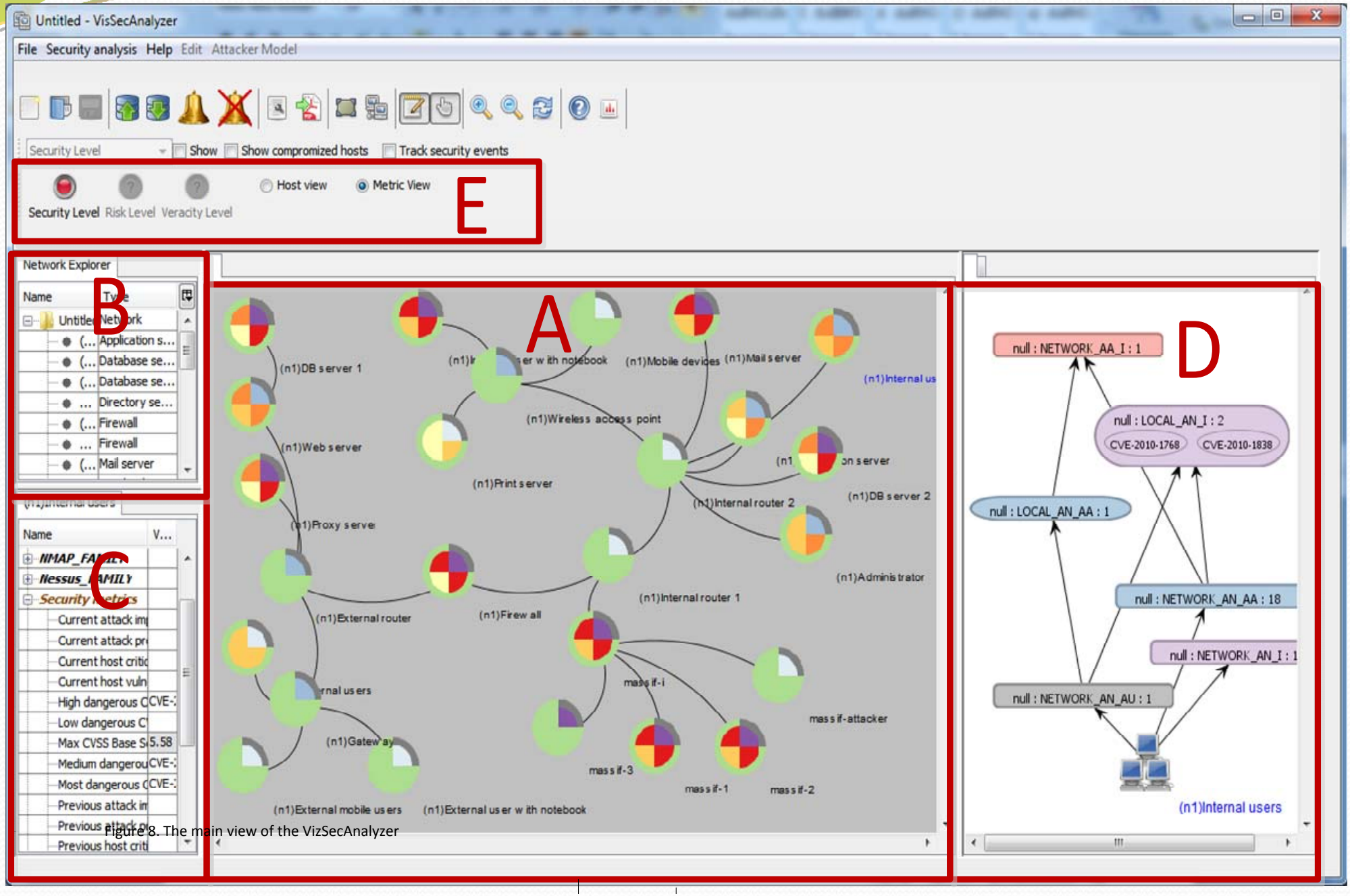
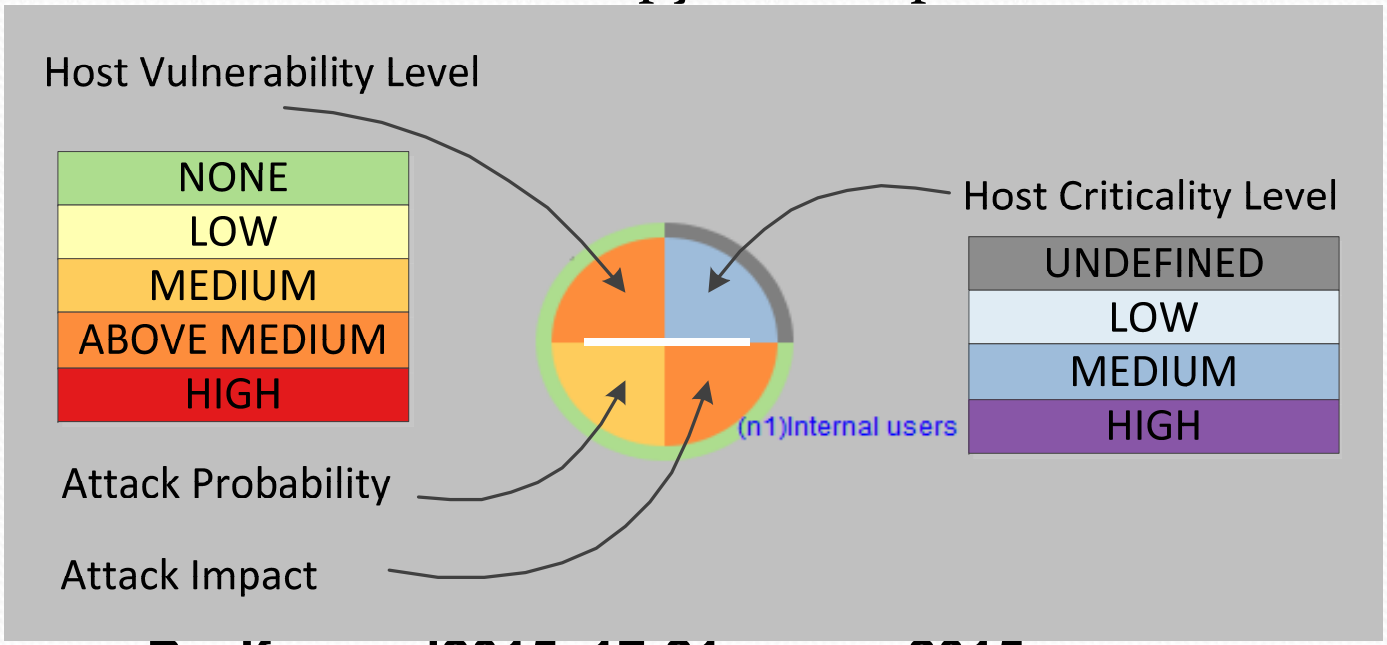



Figure 8. The main view of the VizSecAnalyzer

# Представление хоста с использованием глифа

**Схема кодирования цвета:**

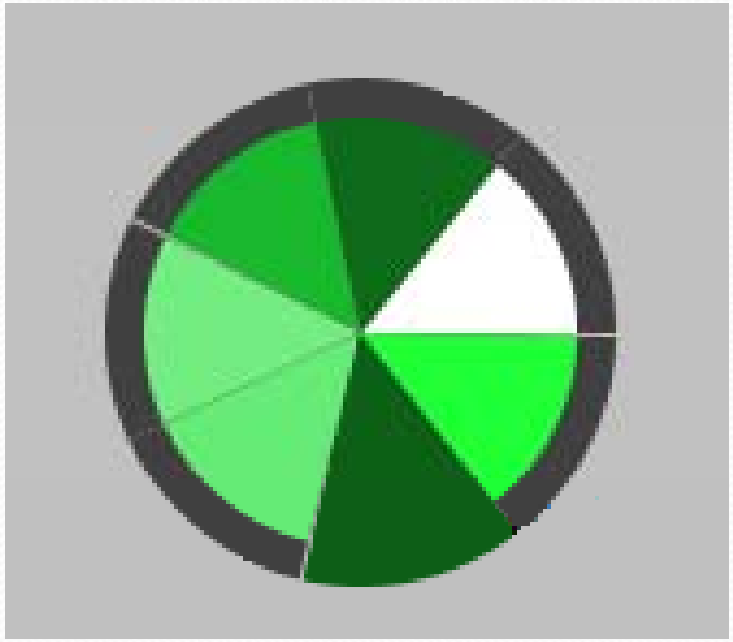
- Для рациональных и интервальных параметров определено пять интервалов, обозначенных как {None, Low, Medium, Above Medium, High}. Эти значения кодируются с использованием шкалы “желтый – красный”, за исключением значения None, которое обозначается с помощью зеленого цвета.
- Для кодирования уровня критичности хоста используется другая схема, так как эта метрика должна применяться для приоритезации действий аналитика и не предназначена для оповещения о возможной опасности, как другие метрики.



# Глиф для отображения метрик RORI

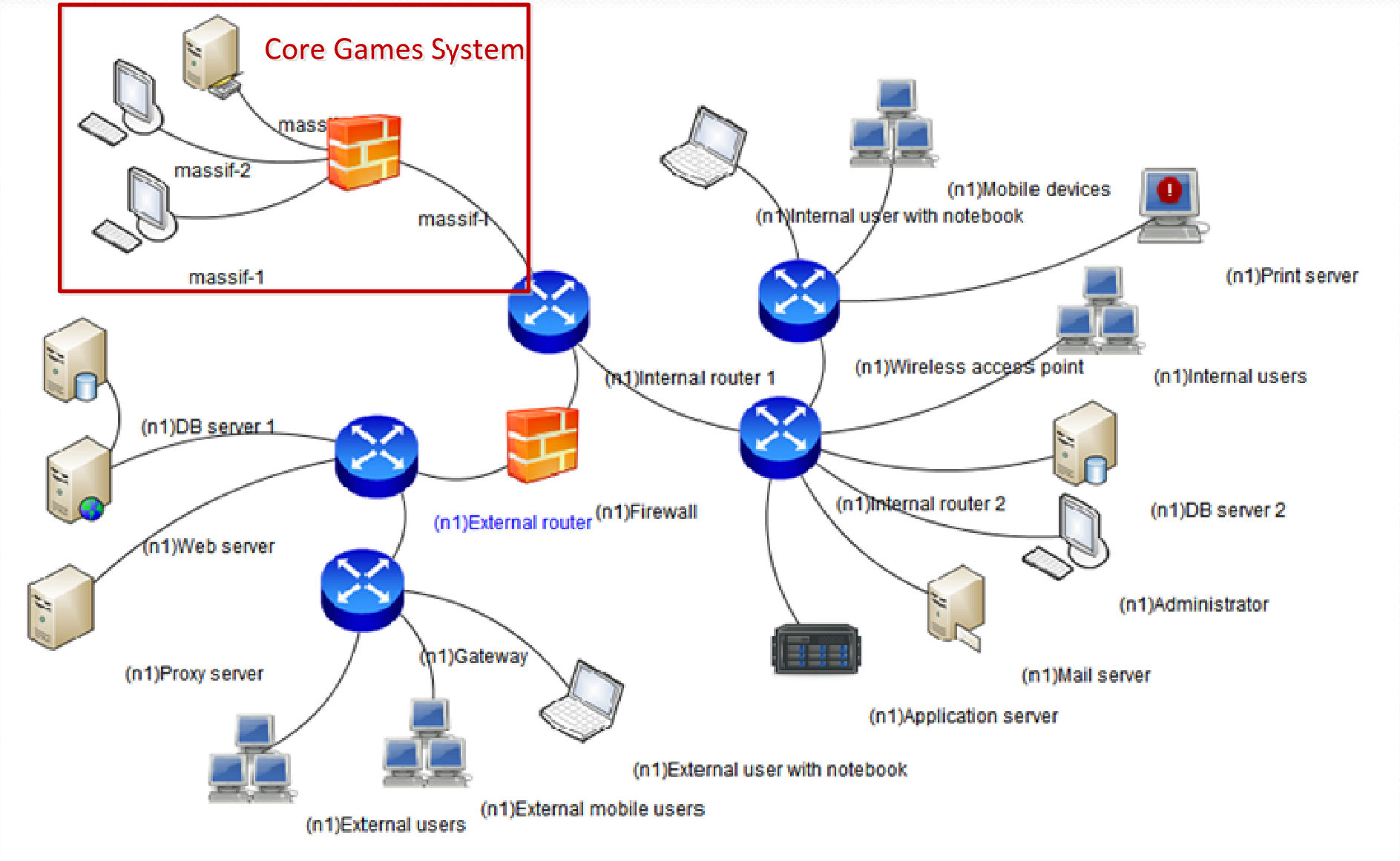
***RORI - Return On Response Investment***

Она учитывает стоимость контрмеры, связанное с контрмерой снижение риска, ценность хоста для бизнеса и ожидаемые потери



C1 - Ничего не делать (RORI = 0.0%).
C2 - Блокирование подозрительных учетных записей (RORI = 400.36%).
C3 - Активация систем обнаружения вторжений (IDS) в стратегических местах (RORI = 308.96%).
C4 - Изменение порта (RORI = 163.64%).
C5 - Активация многофакторной аутентификации (RORI = 386.07%).
C6 - Активация правил обнаружения аномального поведения (RORI = 411.52%).
C7 - Временная деактивация учетной записи (RORI = 259.40%).

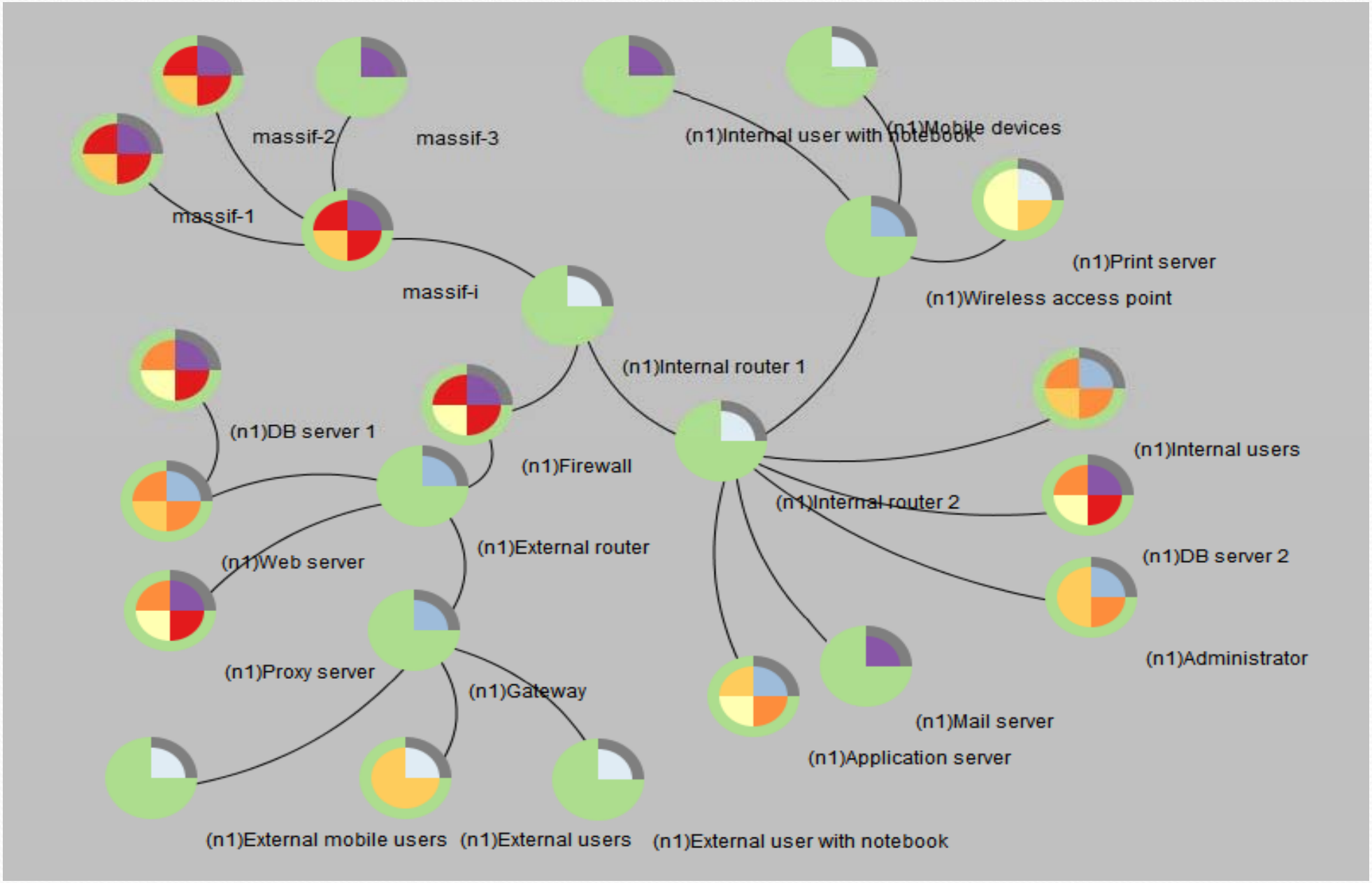
# Структура сети



# Параметры сети для экспериментов

- **massif-1 and massif-2**: Red Hat JBoss Community Application Server 5.0.1; Windows Server 2008 R2 for x64-based Systems;
- **massif-3**: NetIQ eDirectory 8.8.6.0; Novell SUSE Linux Enterprise Desktop 12ServicePack 1;
- **massif-i**: Novell Suse Linux Enterprise Desktop 11 Service Pack 1 and Citrix Ica Client For Linux 11.0;
- **(n1) Firewall**: Linux Kernel 2.6.27.33, Citrix Ica Client For Linux 11.0;
- **(n1)External mobile users**: Google Android Operating System 4.1.2;
- **(n1)External users and (n1)Internal users**: Microsoft Windows 7 64-bit; Apple iTunes 9.0.3;Microsoft Office 2007 SP1; Microsoft Internet Explorer 7;
- **(n1)Proxy server**: Linux Kernel 2.6.27.33; Gnome KDE;
- **(n1)Web server**: Windows Ftp Server 2.3.0; Windows Server 2008 for 32-bit Systems; Sun iPlanet Web Server 4.1 SP10 Enterprise;
- **(n1)DB server 1 and (n1) DB server 2**: Apache Software Foundation; Derby 10.1.3.1; phpMYAdmin 3.5.2.2; Oracle MySQL 5.5.25; Linux Kernel2.6.27.33;
- **(n1)Administrator**: VMware vCenter Server Appliance (vCSA) 5.1;Ubuntu linux 10.04; Gnome KDE;
- **(n1)Mail server**: Windows Server 2008 for 32-bit Systems; Microsoft Exchange Server 2007 Service Pack 1; Microsoft Sharepoint Server 2007 sp1x64;
- **(n1)Mobile devices**: Apple iPhone OS 4.0.

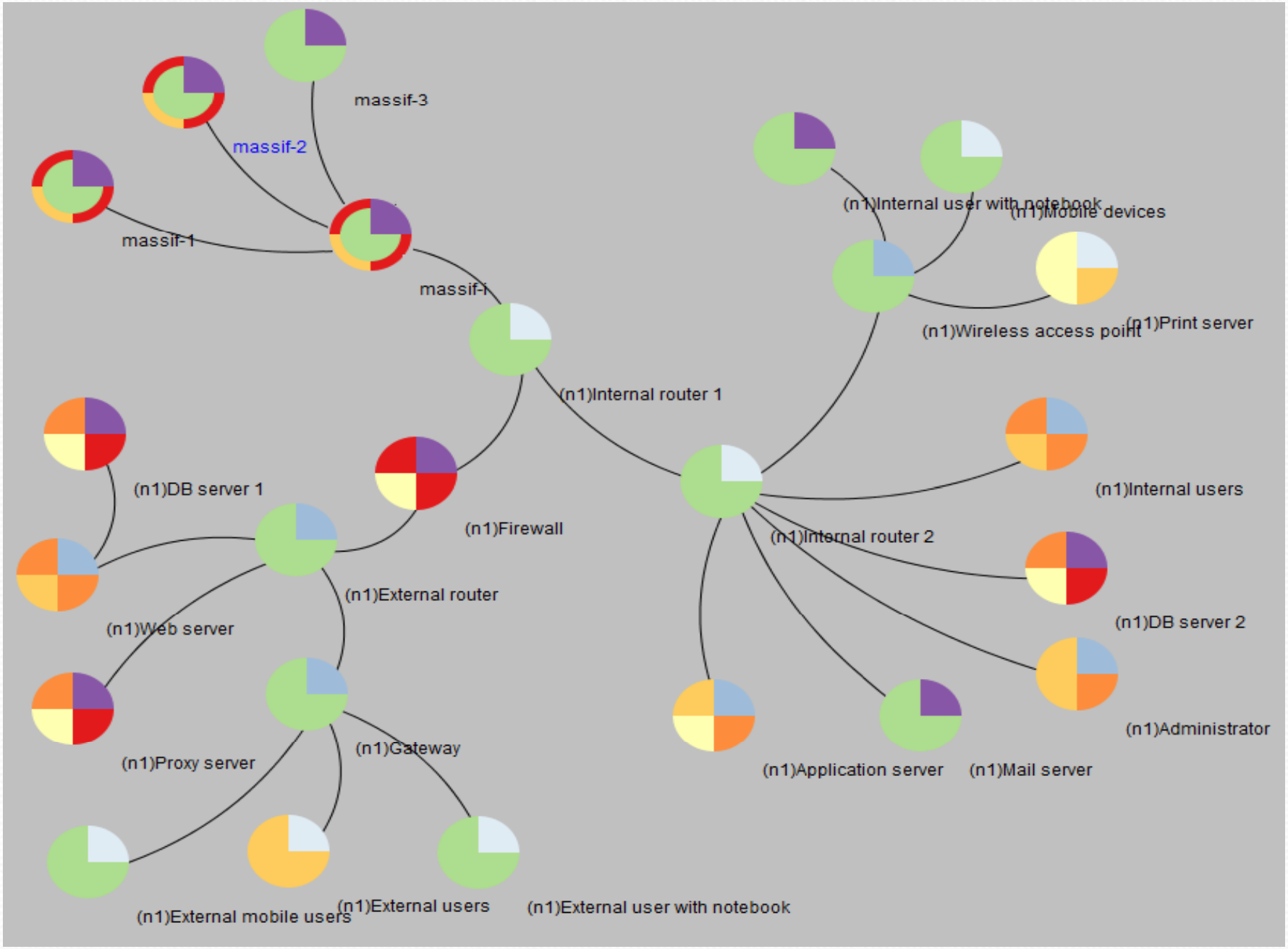
# Первоначальный уровень защищенности хостов сети



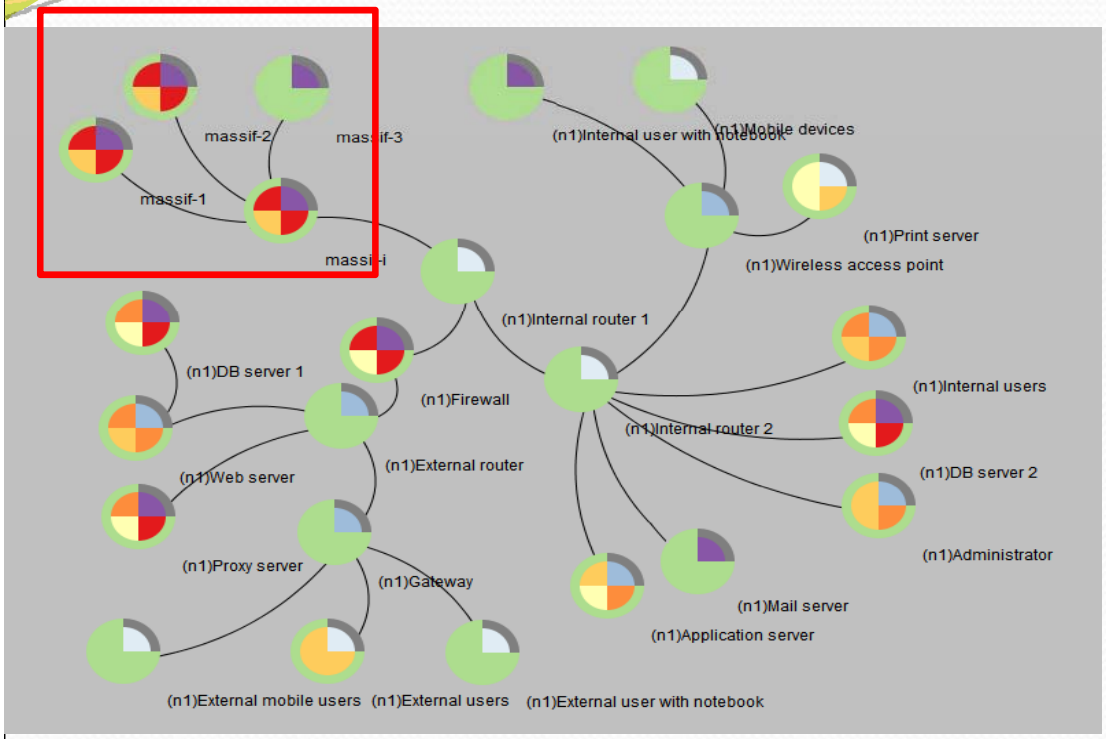
# Реконфигурация хостов

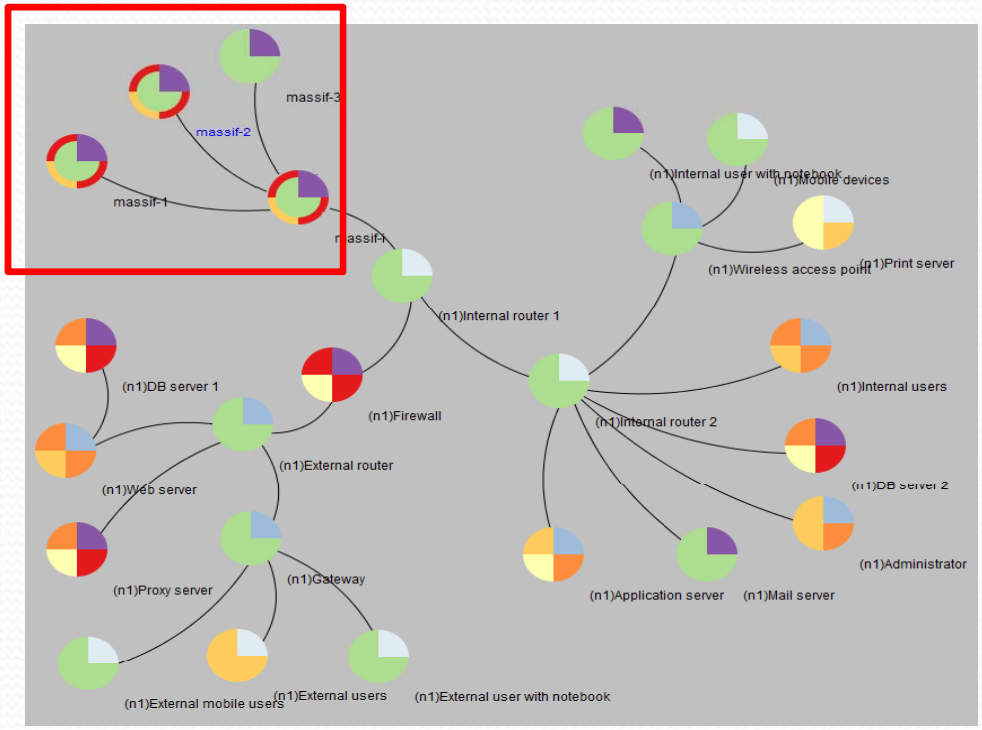
- Аналитик может нажать на интересующий глиф и получить подробную информацию об уязвимостях
- Например, для massif-1 и massif-2 уязвимости – в Windows Server 2008 R2 for x62-based systems, и возможное решение – в инсталляции соответствующего service pack для Windows Server 2008 R2 SP1 for x62-based systems
- Уязвимости, обнаруженные на файерволе massif-i связаны с Novell SUSE Linux Enterprise Desktop 11 Service Pack 1 и Citrix Ica Client For Linux 11.0, возможное решение – обновить ПО
- Аналитик может оценить необходимость этих контрмер до их реализации за счет изменения конфигурации хостов и пересчета метрик защищенности

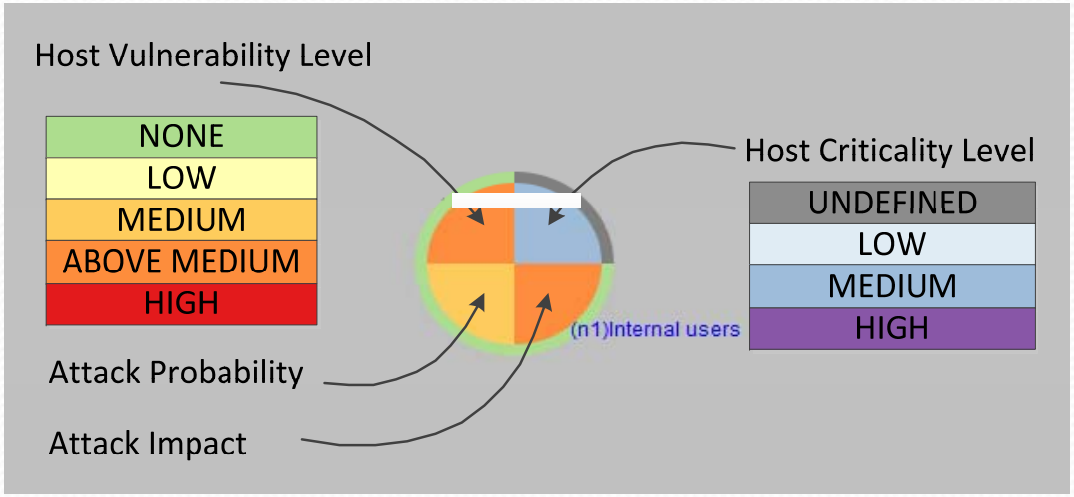
# Уровень защищенности хостов сети после реконфигурации



# Уровни защищенности хостов сети до и после реконфигурации



# Заключение

- Проанализированы методики визуализации, используемые для представления высокоуровневой информации для ситуационной осведомленности, и предложен подход к визуализации метрик защищенности, который позволяет проводить сравнительный анализ текущих и предыдущих значений
- Разработанная визуальная модель может быть использована для представления данных разных типов и обозначать как метрики низкого уровня, так и мета-метрики, такие как уровень воздействия атаки
- Для оценки эффективности предложенного подхода реализован сценарий Олимпийских Игр, в процессе выполнения которого оценивался уровень защищенности сети
- Дана положительная оценка со стороны администраторов и отмечена компактность представления метрик

# Будущие исследования

- Дальнейшая разработка и анализ предложенной визуальной модели и ее применимости для различных задач защиты информации
- Оценка эффективности предложенной подсистемы визуализации, в том числе оценка удобства работы (usability) графического пользовательского интерфейса

# Контактная информация

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

## Благодарности

- Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451), программы фундаментальных исследований ОНИТ РАН, проекта ENGENSEC программы Европейского Сообщества TEMPUS и Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0033, уникальный идентификатор соглашения RFMEFI60414X0033; соглашение № 14.604.21.0137, уникальный идентификатор соглашения RFMEFI60414X0137; соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).