УДК 004.056.5

Е.С. Новикова, И.В. Котенко

АНАЛИЗ МЕХАНИЗМОВ ВИЗУАЛИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Новикова Е.С., Котенко И.В. **Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях.**
Аннотация. Для контроля и оценки состояния защищенности информационной системы необходимо постоянно отслеживать и анализировать данные, поступающие от различных сенсоров безопасности. В большинстве случаев эти данные имеют текстовый формат, поэтому для их анализа используются различные методики визуализации. В настоящей работе рассмотрены основные способы графического представления данных для выявления подозрительной деятельности в информационной системе, обнаружения аномалий в сетевом трафике и анализа защищенности сети.
Ключевые слова: визуализация событий безопасности, анализ сетевого трафика, визуализация графов атак, автоматизированные системы управления событиями безопасности.

Novikova E.S., Kotenko I.V. **Analysis of the Visualization Techniques used for Information Security in the Computer Networks**
Abstract. To monitor the state of the information system it is necessary to track constantly and analyze data received from different security sensors. In the majority of cases this information has textual format, therefore different visualization techniques are used for data analysis. The paper presents the results of the survey on the modern techniques in security visualization.
Keywords: security event visualization, network traffic analysis, attack graph visualization, security event and information management systems.

1. Введение. Методики визуализации широко используются для решения различных аналитических задач. В первую очередь, это связано с особенностями зрительного восприятия человеком графической информации, человеческий мозг является одновременно точным и мощным инструментом по распознаванию общих тенденций или отклонений в характере анализируемой информации, выявлению связей между различными наборами данных. Кроме того, современные информационные системы характеризуются большим объемом обрабатываемых данных, и визуализация помогает справиться с возрастающей сложностью анализируемых данных, поскольку с помощью различных графических атрибутов, таких как цвет, форма, размер, относительное расположение на изображении, можно одновременно передать различные аспекты анализируемой информации [28].

Для анализа защищенности информационной системы необходимо анализировать конфигурационные файлы и логи различных устройств и приложений, таких как маршрутизаторы, системы обна-

ружения вторжений атак, межсетевые экраны и т. д. Поскольку большая часть этих данных имеет текстовый формат, визуализация является важным и эффективным инструментом обработки данных [3-5]. Графическое представление данных позволяет выявить подозрительную активность в сети, ошибки конфигурации устройств и программ. В настоящей работе рассматриваются различные способы представления данных для мониторинга периметра сети, анализа логов систем обнаружения вторжений, обнаружения внутреннего нарушителя и представления результатов моделирования атак.

Статья структурирована следующим образом. Во втором разделе рассматриваются наиболее часто используемые механизмы визуализации на примере автоматизированных систем управления событиями безопасности (АСУСБ) [1-2]. В следующих секциях представляются результаты различных исследований в области визуализации информации: способы графического представления данных для мониторинга периметра сети описываются в третьем разделе, а способы графического представления данных для анализа защищенности сети – в четвертом. В пятой секции предлагается архитектура подсистемы визуализации для АСУСБ, позволяющая легко расширять функциональность системы и использовать различные технологии визуализации для реализации различных графических элементов.

2. Механизмы визуализации в системах управления событиями безопасности. Авторами статьи были исследованы различные методики визуализации событий безопасности в современных АСУСБ, в том числе в системах OSSIM [33], ArcSight [32], QRadar SIEM [34]. Задачей АСУСБ является формирование общего представления о состоянии безопасности информационной системы организации, оперативное реагирование на возникающие угрозы и поддержка принятия решений по обеспечению безопасности [1, 2]. Подсистема визуализации АСУСБ должна предоставлять пользователю удобный интерфейс для решения следующих задач:

- мониторинг данных в режиме реального времени (сетевой трафик, сетевые сервисы, доступность хостов);
- работа с репозиторием событий безопасности (исторический анализ, формирование отчетов);
- создание, редактирование правил для модулей анализа рисков, корреляции событий, моделирования атак;
- представление результатов моделирования атак, анализа рисков;
- управление событиями безопасности;

- управление ресурсами контролируемой сети, источниками данных для системы и пользователями системы.

Анализ показал, что большинство АСУСБ реализуют схожий набор функций по графическому представлению данных. Так для отображения статистической информации о состоянии сети используются гистограммы, круговые диаграммы, линейные графики, карты деревьев. Например, наиболее активные хосты-источники/приемники и наиболее часто используемые сервисы представляются в виде гистограммы или круговой диаграммы, карты деревьев применяются для оценки распределения протоколов в сетевом трафика на хостах, а для выявления информационных потоков – графы вида “источник-сообщение-приемник”. Такое визуальное представление информации позволяет пользователю системы эффективно контролировать периметр сети, легко выявлять различные инфраструктурные атаки (DDOS-атаки, сетевые черви и т. д.) [10, 21].

Кроме того, АСУСБ предоставляют пользователю возможность отслеживать информацию, связанную с задачей принятия решений по обеспечению безопасности, например, представлять варианты решений по реагированию на инциденты безопасности, отображать результаты работы сканеров уязвимостей и оценки рисков [32-34]. Для этого обычно применяются следующие модели представления данных:

- гистограмма или круговая диаграмма, с помощью которой выявляются наиболее уязвимые хосты;
- карта деревьев, которая позволяет не только отобразить критичные узлы, но и оценить уровень их критичности для информационной системы;
- географические карты, с помощью которых формируется общее видение о системе в целом с учетом географического расположения ее отдельных компонентов.

В АСУСБ информация группируется по панелям управления, которые, исходя из их назначения, можно подразделить на оперативные, тактические и стратегические. Такой способ организации информации позволяет специалисту быстро найти нужные данные и эффективно решить поставленную перед ним задачу в рамках заданного временного горизонта. Обычно на одной панели управления задаются как графические, так и текстовые (таблицы, текстовые списки) элементы. Благодаря этому пользователь имеет возможность проанализировать информацию с разных сторон и получить более точную оценку состояния системы.

На рис. 1 представлена панель управления системы OSSIM, отображающая отчет о выявленных уязвимостях в системе, в том числе наиболее уязвимые хосты, наиболее уязвимые службы и степень серьезности обнаруженных уязвимостей. Опираясь на эту информацию, администратор безопасности сети может принять решение о коррекции плана мероприятий по обеспечению безопасности системы, обновлению или замене используемого программного обеспечения и т.д.

Современные АСУСБ позволяют гибко настраивать панели управления с учетом специфических требований пользователя, благодаря этому также повышается эффективность работы пользователя.

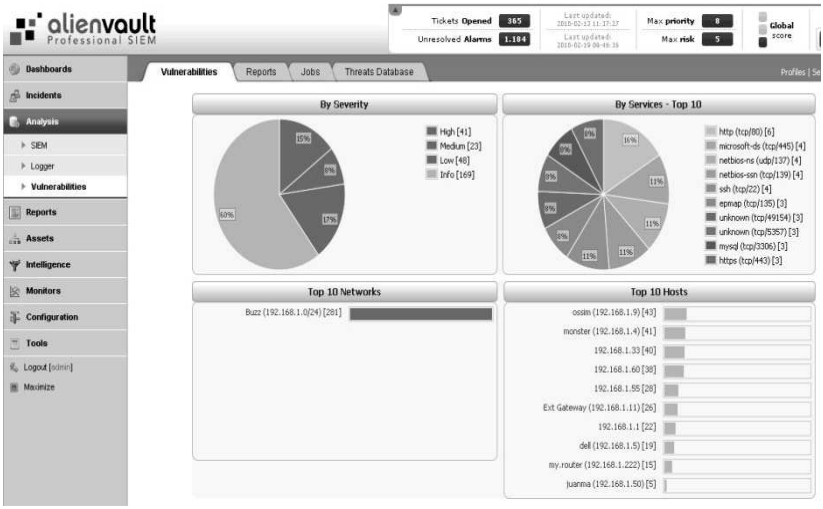

Рис. 1. Панель управления уязвимостями OSSIM.

3. Способы графического представления данных для мониторинга периметра сети.

Рассмотрим наиболее интересные решения по визуализации, предложенные для анализа сетевого трафика.

В работе [16] предлагается инструмент NVisionIP, который позволяет пользователю оценить трафик в локальной сети. Для этого используется график рассеивания, по оси *x* которого откладываются имеющиеся в сети подсети, а по оси *y* - адреса хостов внутри этих подсетей. Таким образом, каждая точка графика задает определенный IP-адрес, цвет точки кодирует число уникальных портов, используемых данным хостом. NVisionIP предоставляет пользователю возможность

фильтровать потоки, комбинируя значения IP-адресов, портов, протоколов, а также проводить сравнительный анализ трафика, проходящего по различным портам выбранных узлов, получать более детальную информацию о состоянии каждого хоста, представленную в виде гистограмм и линейных графиков.

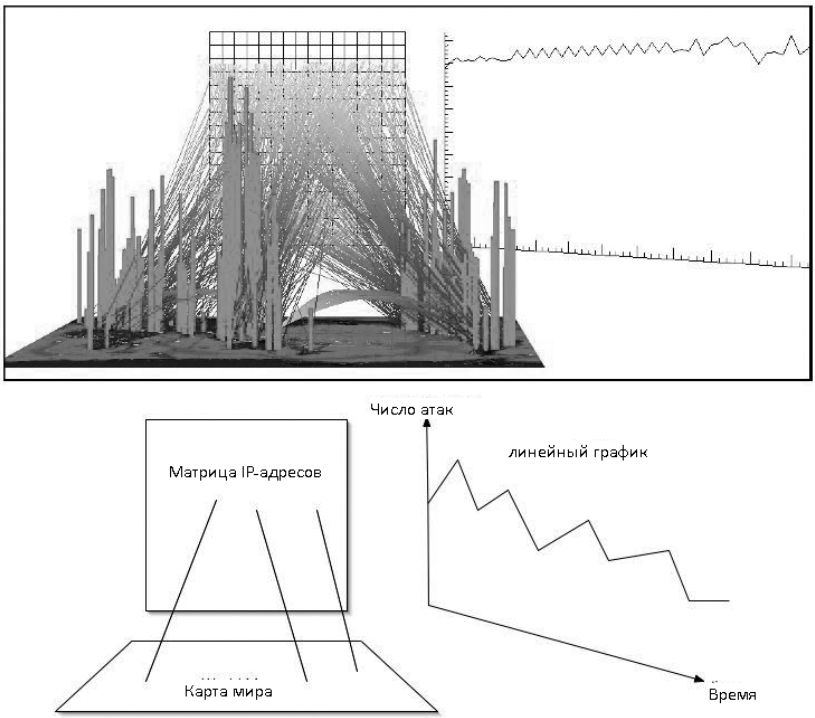

Рис. 2. Схематическое представление информации о сетевом трафике, реализованное в инструменте STARMINE.

В [26] также используется двухмерное представление IP-адресов и строится так называемая матрица IP-адресов: по вертикали откладываются старшие биты IP-адресов, по горизонтали – младшие. С помощью цвета кодируется тип инцидента безопасности, выявленный на определенном хосте. Позже авторы доработали это представление, добавив третье измерение – географическую карту. Благодаря этому два вида – логический и географический – объединяются в один, что позволяет увидеть развитие сетевых атак не только во времени, но

и в пространстве (рис. 2). Данный подход был реализован в инструменте STARMINE [14].

В [22] график рассеивания был адаптирован для контроля состояния портов сетевых приложений. В отличие от [26] каждая точка графика в данном случае обозначает определенный порт. С помощью цвета могут быть закодированы различные характеристики информационного потока, проходящего через заданный порт, например, тип протокола, число сессий, число уникальных адресов получателей/отправителей. Для каждого порта может быть получена дополнительная информация, которая отображается в дополнительном окне в виде линейных графиков, характеризующих изменение состояния порта во времени. В [6, 17] для представления информации об информационных потоках используется 3-х мерный график рассеивания, по осям которого могут откладываться значения локального IP-адреса, глобального IP-адреса, номер портов источников или приемников пакетов (рис. 3).

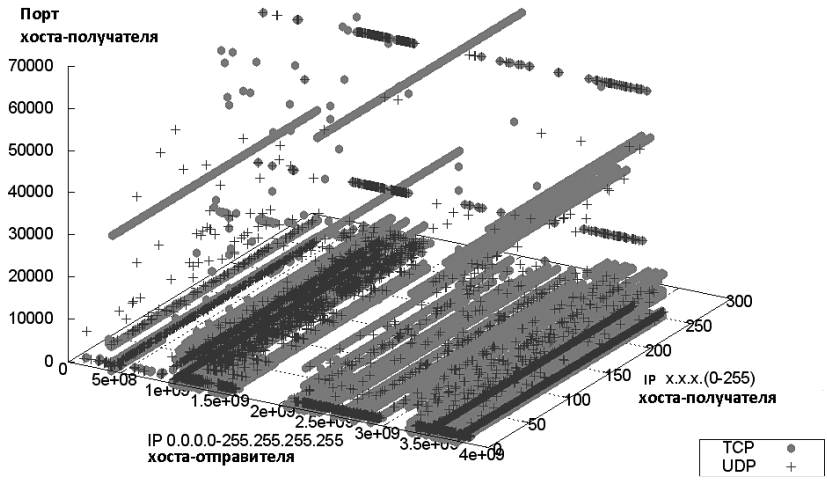

Рис. 3. Визуализация сетевого трафика, предложенная в [6].

Благодаря такому представлению информации легко выявить атаки типа “сканирование портов”. В [6] предложены специальные правила фильтрации, позволяющие более точным образом выявлять аномальные информационные потоки.

В [10, 18] для выявления аномалий в сетевом трафике, характерных для DDOS-атак и сетевых червей, используется граф на параллельных координатах, входными данными для которого является информация, поступающая от межсетевых экранов. В качестве осей могут быть использованы номера портов локального хоста, IP-адрес внешней сети [18] (рис. 4) или порт назначение пакета [10]. Каждый пакет кодируется определенным символом, цвет, размер и форма которого отражает определенные характеристики пакета, такие как его размер, статус (заблокирован/пропущен). Имеется также возможность контролировать отдельные порты.

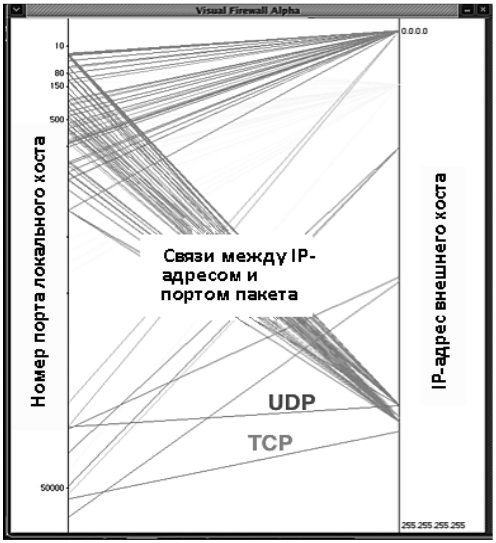

Рис. 4. Графическое представление логов межсетевого экрана с помощью графа на параллельных координатах [18].

Подобный подход реализован в системе VisFlowConnect [30], в котором для отражения информационных потоков используется граф с тремя параллельными осями. Центральная вертикальная ось представляет IP-адреса локальной сети, по левой вертикальной оси откладываются IP-адреса пакетов, передаваемых в исследуемую локальную сеть, в по правой - IP-адреса приемников. VisFlowConnect имеет удобную панель управления для просмотра сетевого трафика во времени, также реализована возможность фильтрации пакетов по номеру порта,

протоколу, размеру, что позволяет аналитику исключить из анализа ненужную информацию.

В [15] для анализа сетевого трафика используется динамически меняющий во времени 3D-граф на параллельных координатах, по осям которого откладываются IP-адреса. Авторы в стандартной 3-х мерной системе координат вместо одной оси вводят две параллельные, которые соответствуют IP-адресу источника и номеру порта приемника (рис. 5), на остальных двух осях откладываются время и размер пакета соответственно. Цветом кодируется тип протокола пакета, а яркостью цвета – время его создания.

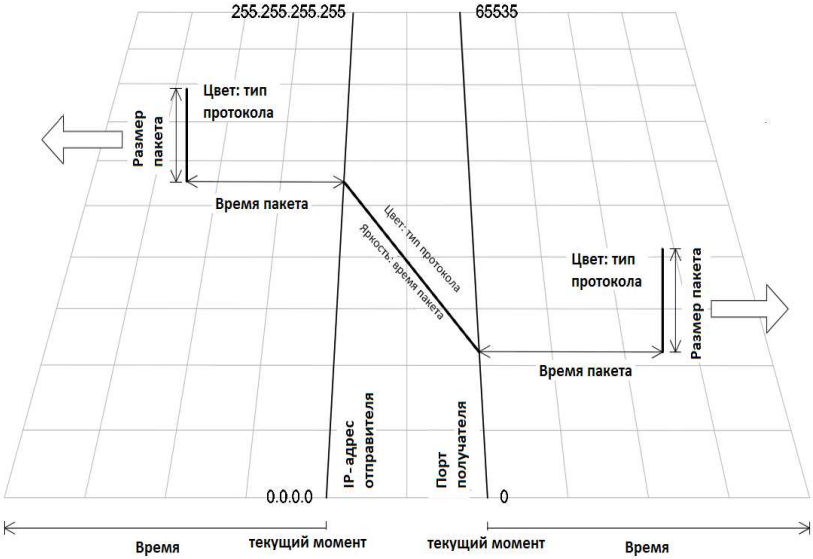

Рис. 5. 3D-визуализация сетевого трафика.

Интересный подход к представлению информации о сетевых потоках между хостами предложен в [20]. Авторы предлагают две графические модели представления, в основе первой лежит карта деревьев (treemap), вторая использует методики, основанные на графах. В первой модели узлы локальной сети представляются в виде вложенных прямоугольников (карты деревьев), а внешние узлы – в виде точек расположенных по периметру карты, кривые отражают сетевые потоки между локальными и глобальными узлами (рис. 6). Число отображаемых внешних узлов может быть изменено пользователем. С помощью

цвета элементов карты деревьев можно закодировать различные характеристики узла, а с помощью толщины линии передаются характеристики сетевого трафика, такие как число переданных пакетов, байт, число потоков и т.д. Если первая модель в большей степени акцентирует внимание пользователя на состоянии локальной сети, то вторая модель, отражает структурные особенности связей между хостами различных подсетей, например, выявляет группу взаимосвязанных хостов. Цвет вершин графа обозначает, является узел источником или приемником информационного потока.

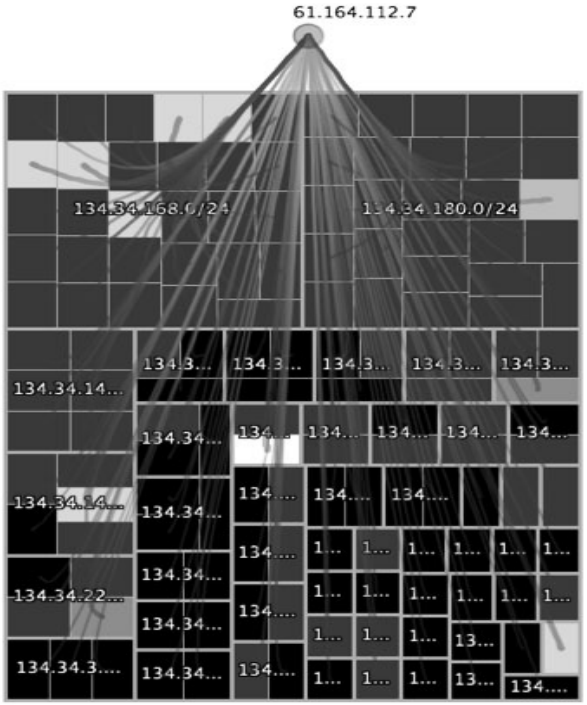

Рис. 6. Визуализация информационных потоков между внешним узлом и узлами локальной сети, предложенная в [20].

В [23] предложена система визуализации, которая позволяет выявлять взаимосвязи между различными сетевыми сканированиями портов. Для этого используется граф, узел которого соответствует одному сканированию, а расстояние между ними определяется специ-

альной величиной – показателем подобия, вычисляемый специальным образом для каждой пары сканирований (рис. 7). Цветом узла обозначается порт, который исследовался при сканировании.

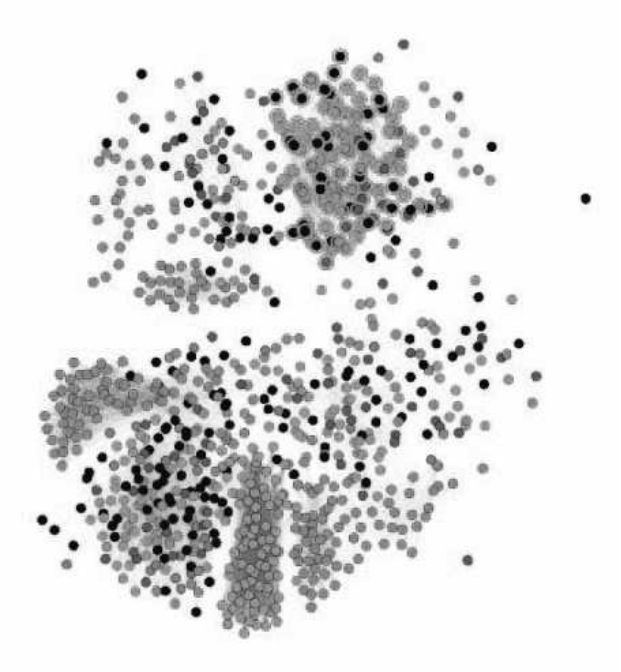

Рис. 7. Граф сканирований.

В [19] предлагается графическая модель поведения хоста, основанная на анализе его сетевого трафика. Вводится специальная система координат, представляющая собой набор узлов, расположенных по окружности и соответствующих различным сетевым службам. Положение хоста вычисляется специальным образом с учетом распределения трафика по используемым им сетевым службам (рис. 8). Такой подход к визуализации сетевого трафика позволяет легко выявлять любые аномалии в сетевом трафике, анализируя отклонения в “поведении” хоста.

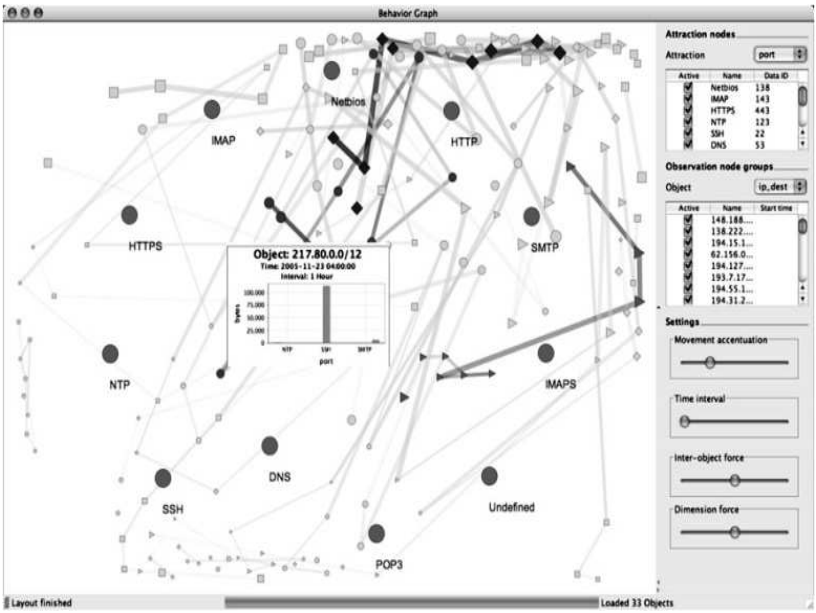

Рис. 8. Метафорическое представление “поведения” хоста, основанное на анализе распределение сетевых служб в его трафике.

Оригинальный способ представления событий безопасности, генерируемых системой обнаружения вторжений, предложен в [11]. IP-адреса локальной сети располагаются по окружности заданного радиуса. IP-адреса внешней сети располагаются сверху или снизу от окружности в зависимости от того, на какой части (верхней или нижней) полуокружности располагается связанный с ним локальный IP-адрес, номера портов располагаются по такому же принципу, только справа или слева от окружности. Такое расположение условных обозначений хостов в сети позволяет уменьшить беспорядочное пересечение линий, связывающие локальные и внешние хосты. Для того, чтобы отразить динамику появления различных событий безопасности во времени, авторы используют окружности разного радиуса: внешние кольца соответствуют наиболее поздним событиям, а внутренние – более ранним. Позже этот подход был усовершенствован в [12], чтобы пользователь имел возможность проанализировать, где, когда и какой тип события безопасности произошел. Для этого внутри окружности схематически отображается структура сети, окружность разбита на дуги,

соответствующие различным типа событиям безопасности, а длина окружности обозначает временной интервал (рис. 9).

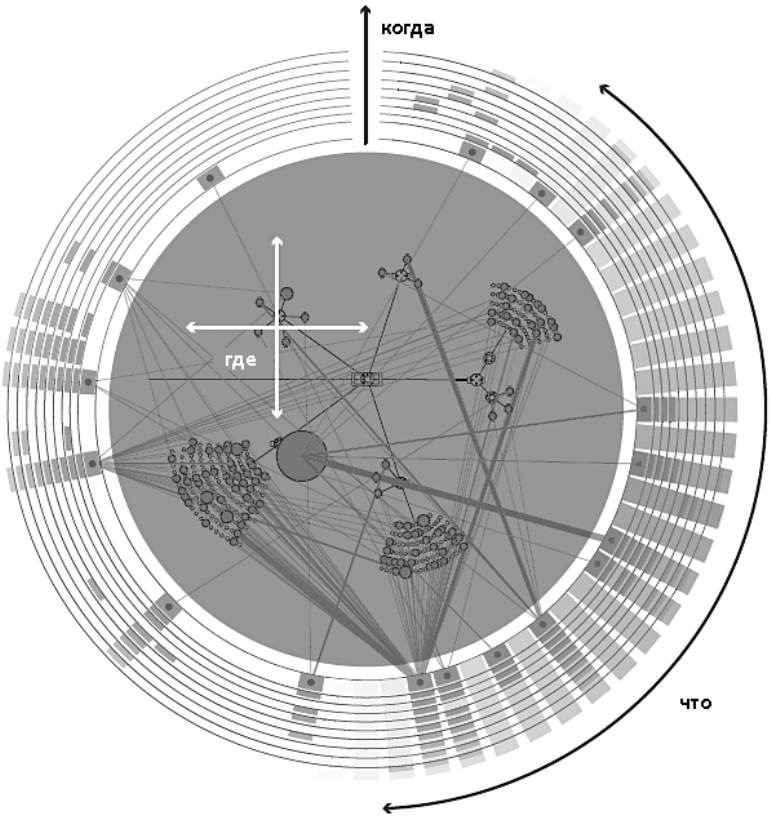

Рис. 9. Визуализация логов системы обнаружения атак [12].

4. Способы графического представления данных для анализа защищенности сети. Механизмы визуализации, предназначенные для анализа защищенности сети и поддержки принятия решений администратором сети, представлены в научных работах не столь широко. Кроме того, иногда сложно провести четкую границу между инструментами визуализации, исходя из области их применения.

Так, например, в [7] представлена система SpiralView, которая может быть использована для мониторинга сетевого трафика, однако

ее основное назначение – это поддержка принятия решений администратором сети. Данная система помогает оценить корректность используемых политик безопасности на основе визуализации событий безопасности, регистрируемых различными датчиками безопасности, включая системные утилиты, фиксирующие действия пользователей и приложений.

В SpiralView для графического представления информации, используется подход, предложенный в [11]: события располагаются на окружностях, радиус которых является шкалой времени. Тип событий маркируется цветом, и пользователь имеет возможность отфильтровать или выделить цветом данные в соответствии с заданными им условиями.

Графы атак являются важным инструментом для оценивания уровня защищенности сети и выявления потенциальных путей проникновения в систему злоумышленником. Естественным представлением результатов моделирования атак являются сами графы [13, 24]. Вершинами графа являются различные хосты сети и уязвимости, эксплуатируемые злоумышленником по мере продвижения от одной скомпрометированной машины к другой, а дуги отражают порядок выполнения действия атакующего (рис. 10).

Однако, как показано в [24], сложность графа атак квадратично зависит от числа хостов в анализируемой сети, поэтому в большинстве случае традиционное представление графов является нечитаемым из-за большого количества узлов и связей между ними.

В [13, 24] предложены различные методики упрощения визуального представления графов атак за счет агрегирования узлов в один, исходя из их связности или общности определенных свойств.

Для анализа возможных шагов злоумышленника в [25] предлагается использовать матрицы смежности, которые являются альтернативным способом представления графов. Ненулевой элемент матрицы a_{ij} обозначает дугу между i-ой и j-ой вершинами графа атак. Ряды и столбцы матрицы могут быть упорядочены любым образом, при этом структура графа атак остается неизменной. С помощью такого графического представления уменьшается сложность анализируемых данных, кроме того, можно пошагово отследить развитие атаки, выделить определенные шаблоны атак и классифицировать их в зависимости от исходных условий.

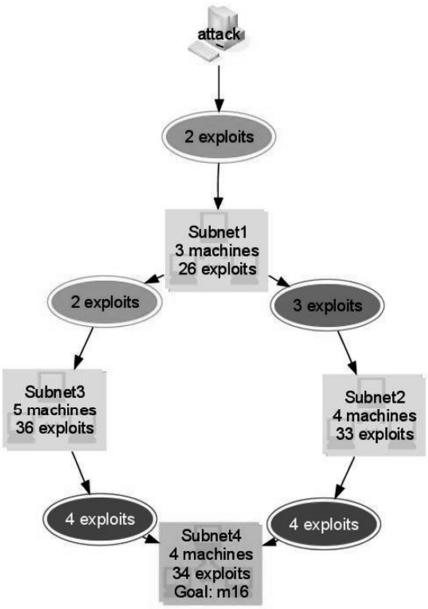

Рис. 10. Графическое представление графа атак.

В [29] предложен способ представления графов атак, который позволяет спроецировать результаты моделирования атаки на физическую топологию сети. Каждая подсеть представляется в виде карты деревьев, вложенные прямоугольники которой символизируют узлы, с помощью цвета кодируются различные атрибуты узлов, а размер пропорционален числу скомпрометированных узлов в подсети (рис. 11). Этот подход реализован в системе Navigator [9]. Пользователь имеет возможность располагать карты деревьев в произвольном порядке для того, чтобы получить интуитивно понятный вид топологии исследуемой сети. Кроме того, инструмент позволяет эксперименты вида “если - что”, благодаря этому администратор сети имеет возможность оценить необходимость установки различных патчей, изменения правил файерволов и т.д.

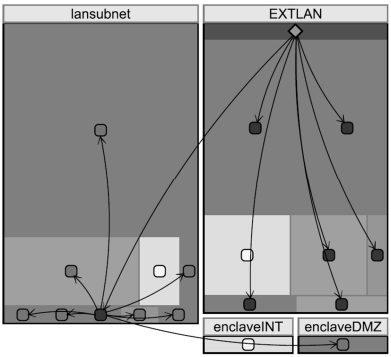

Рис. 11. Представление графа атак в виде карты деревьев.

5. Подсистема визуализации для АСУСБ. Анализ существующих инструментов визуализации информации о защищенности компьютерной сети показал, что их эффективность в первую очередь определяется используемыми в них моделями графического представления данных. Модель представления сильно зависит как от решаемой задачи, так и от типа входных данных [28]. Поскольку информация о безопасности информационной системы разнообразна по своему характеру, и исходные данные могут быть числовыми, интервальными, категориями и т.д., то для ее представления может быть успешно использовано большинство графических форм: гистограммы, круговые диаграммы, линейные графики, графы и т.д., что подтверждается их использованием в современных АСУСБ. Они просты как для реализации, так и для понимания в силу своего широкого применения для представления информации в различных областях общественной деятельности человека (финансовой, экономической, образовательной, медицинской и т.д.). Для представления взаимосвязей между различными характеристиками объектов используются графы на параллельных координатах (способ представления *n*-мерного пространства, в котором оси располагаются параллельно друг другу, а точка представляется в виде ломаной линии), графики рассеивания и матрицы являются оптимальным представлением данных в двухмерном пространстве. Для представления иерархических связей между данными применяются карты деревьев, с помощью которых объекты представляются в виде вложенных прямоугольников, площадь и цвет которых отражают определенные свойства анализируемых объектов [21].

Кроме того, важным моментом в визуализации является интерактивность генерируемого изображения, поскольку данные о событиях

безопасности характеризуются большим объемом, и при их графическом представлении может быть получена “нечитаемая” картинка с перекрывающими друг друга иконками и линиями.

В [27] сформулирован общий принцип работы пользователя с интерактивным графическим изображением для анализа данных: “общий вид – приближение, фильтрация – детали по требованию”, который реализован в большинстве современных инструментов визуализации.

Исходя из проведенного исследования средств визуализации, можно выделить следующие механизмы взаимодействия:

- масштабирование (изменение размеров генерируемого изображения и/или увеличение детализации картинки);
- фильтрация (выборка определенных значений, параметров, согласно определенному критерию);
- сортировка и агрегирование данных, в т.ч. при расположении объектов на картинке;
- использование различных графических эффектов (цвет, размытие и т.д.) для подсветки выбранных параметров;
- получение доступа к исходным данным, представляемым в текстовом или графическом виде («детали по требованию»).

Третьим важным составляющим эффективного представления данных является применение принципов зрительного восприятия человеком при проектировании графических элементов. Использование визуальных эффектов (цвет, размытие и т.д.), расположение элементов относительно друг друга способствует выявлению общих или отличающихся характеристик в группе анализируемых объектов. Таким образом, при проектировании инструмента визуализации необходимо учитывать конечную задачу графического представления данных (например, выявление DDoS-атак); возможность активного взаимодействия пользователя с системой; особенности зрительного восприятия информации человеком.

В рамках проекта MASSIF [35] разрабатывается АСУСБ нового поколения, которая характеризуется расширенными возможностями по анализу защищенности информационной системы, более эффективным механизмом выявления событий безопасности и т.д.

Подсистема визуализации АСУСБ не только предоставляет графический интерфейс пользователя для работы с различными функциональными модулями, но и объединяет их в единую систему. Следовательно, при ее проектировании необходимо учитывать возможность расширения функциональности системы, в т.ч. и для графического представления данных.

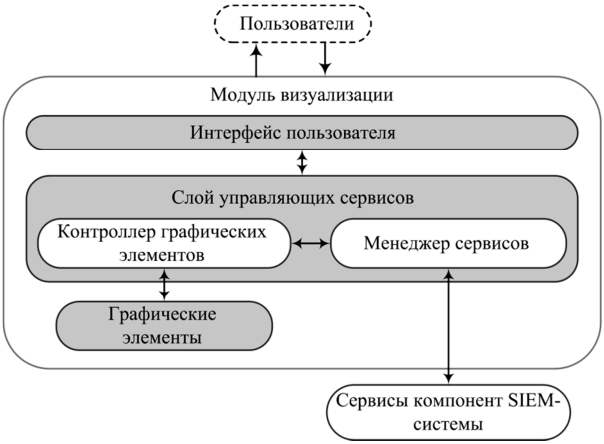

Рис. 12. Архитектура подсистемы визуализации.

В основе разработанной архитектуры подсистемы визуализации лежит сервис-ориентированный подход. Благодаря этому требование функциональной расширяемости компонента легко выполняется. Кроме того, он хорошо согласуется моделью графических систем “данные → отображение → вид ↔ управление” [8, 30].

Архитектура подсистемы визуализации состоит из трех уровней:

- пользовательский интерфейс,
- управляющие сервисы и
- графические элементы.

На рис. 12 представлено схематичное изображение предложенной архитектуры. Стрелками обозначены потоки данных между ее элементами. Выделение пользовательского интерфейса в отдельный уровень позволяет поддерживать разработку различных видов графических интерфейсов, начиная от простой командной строки, заканчивая сложным многооконным интерфейсом с различными панелями управления. Предполагается, что данные, которые необходимо представить графически, передаются соответствующему сервису, который возвращает готовый результат для отображения в форме приложения. Такой механизм взаимодействия позволяет скрыть детали, кто инициировал процесс визуализации – пользователь или функциональный сервис, что позволяет рассматривать уровень управляющих сервисов как движок визуализации.

Исходя из выполняемых им функций, можно выделить две основные группы сервисов – *контроллер графических элементов* и *менеджер сервисов*. Контроллер графических элементов предоставляет стандартный интерфейс по работе с потоками визуализации: создание и остановка графического потока, который реализуется на уровне графических элементов. Менеджер сервисов компонент SIEM-системы обеспечивает подключение сервисов, реализующих функциональность различных компонент SIEM-системы. Такое решение позволяет вести разработку компонент различными организациями, независимо друг от друга, что является очевидным достоинством при выполнении совместного исследовательского проекта.

Уровень графических элементов включает библиотеку необходимых графических примитивов – графов, лепестковых диаграмм, гистограмм, карт деревьев, географических карт и т.д. Графические элементы реализуют обработку входных данных, их отображение и взаимодействие пользователя непосредственно с входными данными. Предложенный подход позволяет для разработки графических элементов использовать различные технологии визуализации, например, Java3D, Flash, SVG и т.д.

6. Заключение. На основе существующих работ в статье сделан обзор методов визуализации, применяемых для анализа событий безопасности. В частности рассмотрены способы графического представления сетевого трафика и уровня защищенности сети на примере визуализации графов атак и политики безопасности.

В статье показано, что эффективность использования средств визуализации определяется моделью представления, выбранной для решения конкретной задачи по обеспечению защиты компьютерной сети и возможностью активного взаимодействия пользователя с графической подсистемой и принятие во внимание особенностей зрительного восприятия информации человеком.

Предложена архитектура подсистемы визуализации АСУСБ, создаваемой в рамках проекта MASSIF [35], которая учитывает вышеперечисленные результаты проведенного исследования и позволяет легко расширять функциональность приложения. Кроме того, она позволяет использовать различные технологии для графического представления данных.

Дальнейшая работа связана с разработкой программного прототипа и проведением различных экспериментов с ним.

Литература

1. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012.
2. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012.
3. *Новикова Е.С., Котенко И.В.* Механизмы визуализации в SIEM-системах // Системы высокой доступности, № , 2012. С.91-99.
4. *Новикова Е.С., Чечулин А.А., Котенко И.В.* Технологии визуализации для противодействия компьютерным атакам в системах управления информационной безопасностью // Санкт-Петербургский научный форум «Наука и общество». 7-ая Петербургская встреча нобелевских лауреатов. Тезисы докладов. Санкт-Петербург. 2012.
5. *Чечулин А.А., Котенко И.В., Новикова Е.С., Дойникова Е.В.* Моделирование атак и механизмов защиты в системах управления информацией и событиями безопасности // Международная конференция “Информационные технологии в управлении” (ИТУ–2012). 09–11 октября 2012 г., Труды конференции. Санкт-Петербург, 2012.
6. *Ansaleh M., Barrera D., Oorshot P.C. van.* Improving Security Visualization with Exposure Map Filtering // Proceedings of the 2008 Annual Computer Security Applications Conference (ACSAC’08). IEEE Computer Society 2008 P. 205-214.
7. *Bertini E., Hertzog P., Lalanne D.* SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms // Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007. P.139-146.
8. *Chi E.H.* A Taxonomy of Visualization Techniques Using the Data State Reference Model // IEEE Symposium on Information Visualization, 2000. P.69-75.
9. *Chu M., Ingols K., Lippmann R., Webster S., Boyer S.* Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR // Proceedings of the Seventh International Symposium on Visualization for Cyber Security , Ontario, Canada. P. 22-33.
10. *Conti G.* Security Data Visualization. No Starch Press, San Francisco, CA, USA, 2007.
11. *Erbacher R. F., Christensen K., Sundberg A.* Designing Visualization Capabilities for IDS Challenges // Proceedings of the IEEE Workshops on Visualization for Computer Security (VizSEC '05). 2005, IEEE C/S, Washington DC, USA. P. 15.
12. *Foresti S., Agutter J., Livnat Y., Moon S., Erbacher R.* Visual Correlation of Network Alerts // IEEE Comput. Graph. Appl., vol. 26, n. 2. P. 48-59.
13. Homer J., Varikuti A., Ou X., McQueen M. A. Improving Attack Graph Visualization Through Data Reduction and Attack Grouping // Proceedings of the VizSEC 2008 Workshop on Visualization for Computer Security. Springer-Verlag, Berlin, Heidelberg, 2008. P. 68–79.
14. *Hideshima Y., Koike H.* STARMINE: a Visualization System For Cyber Attacks // Proceedings of the Asia Pacific Symposium on Information Visualisation. Tokyo, Japan, 2006. Vol. 243. P. 131-138.
15. *Krasser S., Conti G., Grizzard J., Gribshaw J., Owen H.* Real-time and forensic network data analysis using animated and coordinated visualization // Proceedings of the 2005 IEEE Workshop on Information Assurance. IEEE Press, 2005. P. 42-49.
16. *Lakkaraju K., Yurcik W., Lee A.J.* NVisionIP: Netflow visualizations of system state for security situational awareness // Proceedings of the ACM workshop on visualization and data mining for computer security (VizSEC/DMSEC ’04). New York, NY, USA, 2004. P.65–72

17. *Lau S.* The spinning cube of potential doom // Communications of the ACM, vol. 47(6), 2004. P.24-26.
18. *Lee C.P., Trost J., Gibbs N., Beyah N., Copeland J.A.* Visual Firewall: Real-time Network Security Monitor // Proceedings of the IEEE Workshop on Visualization for Computer Security (VizSEC 05), 2005. P.129-136.
19. *Mansmann F., Meier L., Keim D.A.* Visualization of Host Behavior for Network Security // Proceedings of the Workshop on Visualization for Computer Security (VizSEC 2007), Sacramento, California, USA. P.187-202.
20. *Mansmann F., Fischer F., Keim D. A., North S. C.* Visual Support for Analyzing Network Traffic and Intrusion Detection Events using TreeMap and Graph Representations // Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology (CHiMiT '09), 2009. No. 3 P.19-28.
21. *Marty R.* Applied Security Visualization. NY:Addison Wesley Professional, 2008.
22. *McPherson J., Ma K.-L., Krystosk P., Bartoletti N., Christensen M.* PortVis: A Tool for PortBased Detection of Security Events // Proceedings of the ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04), New York, NY, USA, 2004. P.73-81.
23. *Muelder C., Chen L., Thomason R., Ma K.-L., Bartoletti T.* Intelligent Classification and Visualization of Network Scans // Proceedings of the Workshop on Visualization for Computer Security, Sacramento, California, USA, 2007. Springer, Heidelberg. P. 237-253.
24. *Noel S., Jacobs M., Kalapa P., Jajodia S.* Multiple Coordinated Views for Network Attack Graphs // Proceedings of the IEEE Workshops on Visualization for Computer Security, IEEE Computer Society, 2005. P.12.
25. *Noel S., Jajodia S.* Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices // Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05). IEEE Computer Society, 2005. P. 160-169.
26. *Ohno K., Koike H., Koizumi K.* IP Matrix: An Effective Visualization Framework for Cyber Threat Monitoring // Ninth International Conference on Information Visualization (IV05), London, England, IEEE/CS. P.678–685.
27. *Shneiderman, B.* Dynamic queries for visual information seeking. The Craft of Information Visualization: Readings and Reflections 2003, 14.
28. *Ware. C.* Information Visualization. Perception for Design 2nd Edition, Elsevier Morgan Kaufman, 2004.
29. *Williams L., Lippmann R., Ingols K.* An Interactive Attack Graph Cascade and Reachability Display // Proceedings of the Workshop on Visualization for Computer Security, Sacramento, California, USA, 2007. Springer, Heidelberg. P. 221-236.
30. *Wood J., Brodlie K.W., Seo J., Duke D.J. and Walton J.* A web services architecture for visualization // Proceedings of the IEEE Fourth International Conference on eScience, 2008. 7-12 December 2008, Indianapolis, Indiana, USA. IEEE Computer Society Press. P.1-7.
31. *Yin X., Yurcik W., Treaster M., Li Y., Lakkaraju K.* VisFlowConnect: netflow visualizations of link relationships for security situational awareness // Proceedings of the the 2004 ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04). 2004, Washington DC, USA P. 26-34.
32. ArcSight Website http://www.arcsight.com/products/products-esm/
33. OSSIM Website http://alienvault.com/products/unified-siem/siem
34. QRadar SIEM-система Website http://q1labs.com/products/qradar-siem.aspx
35. MASSIF Website. http://www.massif-project.eu/

Котенко Игорь Витальевич — д.т.н., проф.; заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений, телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Kotenko Igor Vitalievich — Prof. of Computer Science; head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, artificial intelligence, including multi-agent frameworks and systems, agent-based modeling and simulation, soft and evolutionary computing, machine learning, data mining, data and information fusion, telecommunications, including decision making and planning for telecommunication systems. The number of publications — 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Новикова Евгения Сергеевна — старший научный сотрудник научно-исследовательской группы «Защита информации в критических инфраструктурах» СПИИРАН, к.т.н. Область научных интересов: визуализация событий безопасности, протоколы аутентификации, двухключевая криптография. Число научных публикаций — 45. novikova@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Novikova Evgenia Sergeevna — Senior researcher of the scientific research group “Information Security in Critical Infrastructures” Ph.D. student of Laboratory of Computer Security Problems, SPIIRAS, PhD. Research interests: security visualization, authentication protocols, public key cryptography. The number of publications — 45. novikova @comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Поддержка исследований. Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а, 12-07-13119-офи_м_РЖД), программы фундаментальных исследований ОНИТ РАН (проект № 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

Рекомендовано СПИИРАН, лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 07.08.2012

РЕФЕРАТ

Новикова Е.С., Котенко И.В. **Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях.**

Современные информационные системы характеризуются большим объемом обрабатываемых данных, в отличие от анализа данных в текстовом виде, методики визуального анализа являются более эффективным способом обработки данных, позволяя легко выявлять общие закономерности или отклонения в характере изменения данных. В настоящей работе рассмотрены основные методики визуализации, применяемые для анализа сетевого трафика и оценки защищенности информационной системы.

В статье показано, что эффективность инструментов визуализации в первую очередь определяется способом представления данных, который должен быть выбран в соответствии с решаемой задачей. Например, карты деревьев являются оптимальным решением, если необходимо отразить иерархические связи между объектами, а графы на параллельных координатах позволяют выявить определенные зависимости между свойствами объектов.

Механизмы активного взаимодействия пользователя с генерируемым изображением также являются важной характеристикой инструмента визуализации, поскольку в большинстве случаев картинка оказывается нечитаемой из-за большого объема визуализируемых данных. Большинство современных графических инструментов реализуют общий принцип работы с данными: “общий вид – приближение, фильтрация – детали по требованию”.

Результаты анализа различных техник визуализации, применяемых для анализа безопасности сети, были учтены при проектировании системы визуализации для системы управления событиями безопасности, разрабатываемой в рамках проекта MASSIF. Предложена трехуровневая сервис-ориентированная архитектура, включающая пользовательский интерфейс, управляющие сервисы и графические элементы. Такое решение позволяет легко расширять функциональность системы, а также интегрировать различные технологии визуализации для реализации используемых графических элементов. Определены дальнейшие направления будущих исследований.

Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект № 2.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

SUMMARY

Novikova E.S., Kotenko I.V. **Analysis of the Visualization Techniques used for Information Security in the Computer Networks.**

Modern information systems are characterized by enormous volumes of the processed data, and in contrast to handling textual data visualization offers more effective way for data analysis as it helps to identify general trends or anomalies in datasets. Different visualization techniques used for traffic analysis and security level evaluation are discussed in the paper.

We have shown that the effectiveness of the security visualization tools is determined first of all by the data visual model that has to be chosen strictly according to the intended use. Thus, to represent network statistics pie chart, linear charts can be used. Treemaps are good choice to reflect hierarchical dependency between objects, while to get better understanding of the correlation between certain object properties scatterplots and parallel coordinates should be used.

The interaction is the second important issue in security visualization as it has to deal with large datasets, and thus cluttering image with the overlapping icons and connected lines can be produced. Almost all modern visualization tools implement seeking mantra “overview – filter – details on demand” in order to help data analysis.

Consideration of the human perception principles when designing graphical elements also can enforce the understanding of the information. Different graphical effects such as color, blurring, object location on the picture can help to detect similarities or differences in datasets.

The results of the visualization techniques analysis were considered when developing visualization subsystem of the SIEM system that is designed in the framework of the MASSIF FP7 project. The three-level service-oriented architecture of the visualization component is proposed. It consists of the User Interface, Control Services Middleware and Graphical elements. Such approach allows developing the scalable application and integrating different visualization technologies used to implement graphical items. Further research directions are determined.

This research is being supported by grants of the Russian Foundation of Basic Research (project #10-01-00826), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences (project #2.2), the State contract #11.519.11.4008 and by the EU as part of the SecFutur and MASSIF projects.