УДК 681.3.06 (075.8)

ВИЗУАЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

И. В. Котенко,
доктор техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности
Е. С. Новикова,
канд. техн. наук, старший научный сотрудник
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Исследуются методики визуального анализа защищенности компьютерных сетей. Описывается компонент визуализации системы оценки защищенности компьютерной сети, отличающийся от других систем тем, что позволяет графически представлять как отчеты сканеров уязвимостей, так и результаты моделирования атак, благодаря чему пользователь системы может соотнести потенциальные причины нарушения безопасности с возможными последствиями их эксплуатации злоумышленником.

Ключевые слова *— визуализация событий безопасности, оценка защищенности, политики безопасности, графы атак, карты деревьев.*

Введение

Методики визуального анализа данных позволяют эффективно исследовать данные большого объема и извлекать новые знания из массива неоднородных, зашумленных данных. Основная идея визуальной аналитики заключается в объединении особенностей зрительного восприятия человеком информации и мощностей электронной обработки данных, в результате чего возможно создание высокоинтерактивного программного обеспечения, позволяющего пользователю погрузиться в данные, лучше понимать результаты алгоритмов их обработки и вести процесс исследования в наиболее перспективном направлении [1].

Методики визуального анализа широко используются для анализа безопасности информационной системы. В настоящее время большая часть существующих решений предназначена для эффективного контроля периметра сети [2, 3]. Имеются различные инструменты для анализа состояния всей сети в целом, мониторинга портов и определения различных паттернов сканирования портов, выявления аномалий в «сетевом поведении» пользователя, в то время как вопросы визуализации данных об уровне защищенности компьютерной сети, поддержки принятия решений проработаны в меньшей степени [2, 3].

В настоящей работе представлены модели и методики визуального анализа, реализованные в системе оценки защищенности компьютерных сетей [4–6], которая позволяет графически определить наиболее уязвимые места информационной системы, сформировать шаблоны атак в зависимости от начальных условий атак и на основе полученных данных соответствующим образом скорректировать план мероприятий по обеспечению безопасности системы. Главным отличием представляемой системы является возможность визуально анализировать потенциальные причины в контексте возможных последствий их эксплуатации.

Методики визуализации для анализа защищенности компьютерных сетей

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, систему SpiralView, предназначенную для поддержки принятия решений системным администратором, успешно можно применять для мониторинга сетевого трафика [7], поскольку в ней используется визуализация событий безопасности, регистрируемых различными датчиками безопасности, в том числе и системными утилитами, фиксирующими действия пользователей и при-

ложений, в режиме реального времени. Для графического представления информации используется подход, предложенный в работе [8]: события располагаются на окружностях, радиус которых является шкалой времени (рис. 1).

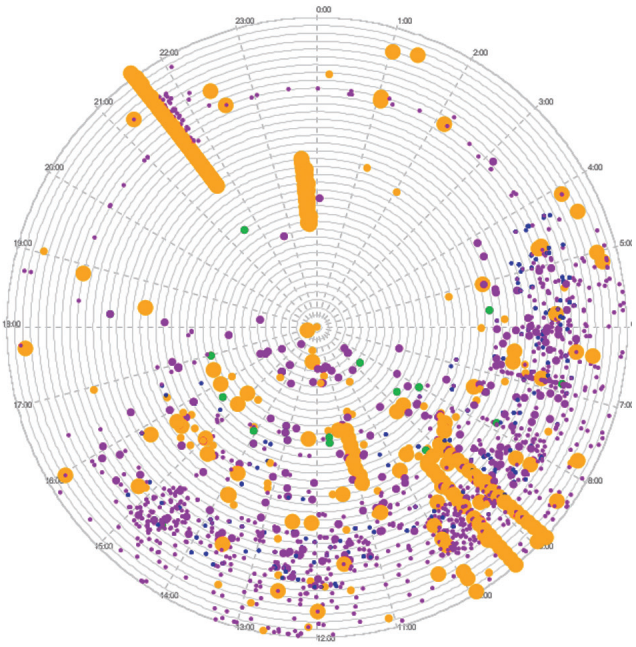
Тип событий маркируется цветом, и пользователь имеет возможность отфильтровать или выделить цветом данные в соответствии с заданными им условиями. Однако такая модель визуализации информации не представляется удобной для оценки корректности используемых в системе политик безопасности, поскольку помогает оператору выявить небезопасные элементы системы, но для понимания причин их появления требуется выполнение дополнительного анализа.

Для визуального анализа политик безопасности межсетевых экранов Тран и др. [9] разработали инструмент PolicyVis, который отображает правила межсетевого экрана в виде прямоугольников. Положение и геометрия прямоугольника определяются тремя полями правила, выбираемыми пользователем. Цветом кодируется статус трафика (зеленый — разрешенный трафик, красный — блокируемый трафик). Благодаря такому представлению пользователь может легко выявить различные аномалии в политике безопасности (избыточность, затенение, обобщение, корреляцию), о которых свидетельствуют пересекающиеся прямоугольники.

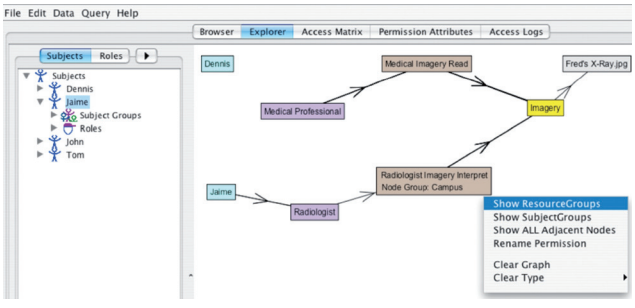
Мансманн и др. [10] для визуализации политик безопасности адаптировали модель визуализации «солнечные лучи» (Sunburst), которая позволяет компактно графически представлять иерархическую структуру. Корневой элемент структуры помещается в центр в виде круга, а элементы каждого уровня иерархии рекурсивно отображаются на соответствующие сегменты кольца. Для использования данной модели визуализации авторы разработали правила преобразования политики безопасности в иерархическую структуру. Согласно им, первый уровень после корневого узла состоит из названий различных списков контроля доступа, второй уровень содержит описания прав доступа («разрешить» или «запретить»), на третьем уровне располагаются названия протоколов («tcp», «ip», «udp» и т. д.), за которыми следуют IP-адреса получателей и отправителей.

Интересные результаты можно получить при представлении списков доступа пользователей к ресурсам в виде связных графов, вершины которых соответствуют пользователям/группам пользователей и информационным ресурсам, а ребра обозначают возможность получения доступа к объекту [11, 12]. Цветом обычно обозначаются роли пользователя/группы пользователей. Например, инструмент RubaViz [12] использует два графических представления правил доступа к ресурсам: матричное и в виде графа. Пример графа, соответствующего правилам доступа, представлен на рис. 2 [12]. Р. Марти [11] показал, что такое графическое представление в сочетании с алгоритмами кластеризации и компоновки графа, учитывающими его семантику, позволяет сформировать как стандартные модели поведения пользователей, так и отклонения от них.

Хайнтцман и др. [13] предложили представлять права доступа к файловым ресурсам в стандартной иерархической файловой системе в виде карты деревьев, вложенные прямоугольники которой соответствуют файлам и папкам. С помощью цвета кодируются их разрешения, т. е. узел карты деревьев, соответствующий заданной папке или файлу, изображается зеленым, красным или серым, если разрешения к нему слабее, сильнее или равны базовому значению соответственно, которое может принимать следующие значения: «нет доступа», «чтение», «чтение и запись» и «полный доступ». Кроме того, узлы карты дерева



■ *Рис. 1.* Модель визуализации политик безопасности



■ *Рис. 2.* Представление правил доступа к ресурсам в виде графа

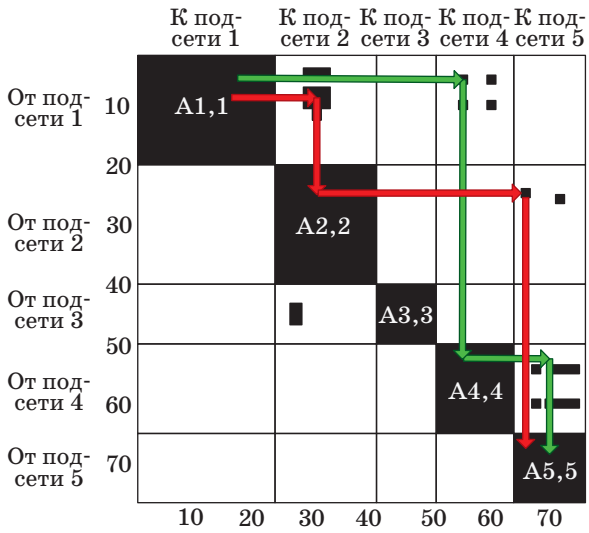
выделяются оранжевой рамкой, если имеет место нарушение разрешений родительского узла.

Карты деревьев широко применяются для анализа выявленных уязвимостей в компьютерных сетях [11, 14]. Например, веб-приложение Nv [14] представляет отчеты сканера уязвимостей Nessus [15] в виде карт деревьев и гистограмм. Помимо графической интерпретации результатов одного сканирования инструмент позволяет оценить прогресс в устранении обнаруженных уязвимостей, показывая, какие уязвимости были устранены, какие остались неразрешенными и какие новые уязвимости появились в системе. В инструменте используется семантическая цветовая схема, в рамках которой устраненные уязвимости обозначаются зеленым цветом, новым уязвимостям соответствует красный цвет, а оранжевым обозначаются уязвимости, находящиеся в работе.

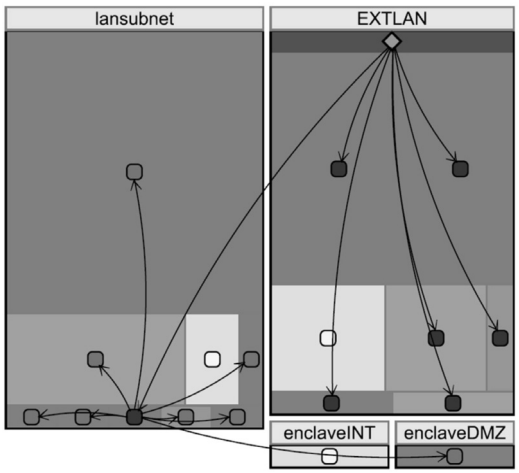
Графы атак являются одним из способов анализа защищенности сети. Графы атак — важный инструмент для оценивания уровня защищенности сети и выявления потенциальных путей проникновения в систему злоумышленником [4–6, 16]. Естественным представлением результатов моделирования атак являются сами графы. Вершинами 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. Однако, как показано в работе [17], сложность графа атак квадратично зависит от числа хостов в анализируемой сети, поэтому в большинстве случаев традиционное представление графов нечитаемо из-за большого количества узлов и связей между ними.

Для анализа возможных шагов злоумышленника предлагается [17] использовать матрицы смежности, которые являются альтернативным способом представления графов. Ненулевой элемент матрицы a_{ij} обозначает дугу между i-й и j-й вершинами графа атак (рис. 3). 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.

В работе [18] 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. 4) [18]. Этот подход



■ ***Рис. 3.*** Представление графа атак в виде матрицы смежности



■ ***Рис. 4.*** Представление графов атак в виде карты деревьев

реализован в системе Navigator [19]. Пользователь имеет возможность располагать карты деревьев в произвольном порядке, чтобы получить интуитивно понятный вид топологии исследуемой сети. Кроме того, инструмент позволяет проводить эксперименты вида «что-если», благодаря этому администратор сети может оценить необходимость установки различных патчей, изменения правил межсетевых экранов и т. д.

Модели и методики визуального анализа, применяемые в системе оценки защищенности компьютерной сети

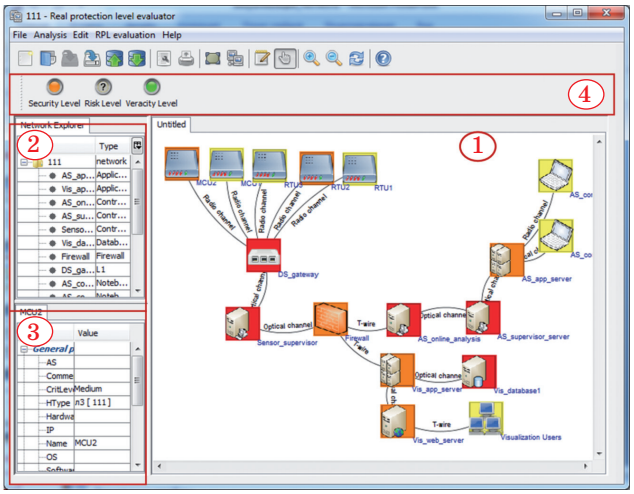
Система оценки защищенности компьютерной сети позволяет оценить уровень ее защищенности, основываясь на результатах аналитического

и динамического моделирования атак и расчета метрик безопасности [4–6]. Графический интерфейс пользователя предоставляет оператору системы возможности по конфигурированию исходных данных и представлению результатов моделирования атак в графическом виде.

Главное окно системы разделено на четыре функциональных вида (рис. 5).

Главный вид *1* представляет топологию исследуемой сети в виде графа, в то время как вид *2* отражает иерархическую структуру, показывая домены или группы хостов. Пользователь может добавлять и удалять узлы компьютерной сети. Пиктограммы оборудования являются настраиваемыми, поэтому пользователь может задать иконку для обозначения типа сетевого объекта. Фон пиктограммы используется для отображения значений метрик безопасности, вычисленных в результате работы системы оценки защищенности компьютерной сети. Пользователь может выбрать метрику из предопределенного списка {Уровень критичности, Уровень риска, Ущерб, Число уязвимых приложений}. Краткая информация по каждому хосту также доступна в виде всплывающей подсказки, которая появляется при наведении указателя мышки пользователем на объект сети. Свойства узлов сети задаются при помощи редактора свойств *3*, причем пользователь может сконфигурировать каждый узел сети и саму сеть в целом. Он может задать как значения заранее определенных свойств, таких как IP-адрес, тип хоста (веб-сервер, файловый сервер, роутер и т. д.), установленное программное и аппаратное обеспечение, так и определить собственные свойства хостов.

Панель управления *4* используется для отображения значений метрик защищенности: она отображает уровень защищенности анализируемой сети, уровень рисков, уровень достоверности информации. Такое расположение информации об исследуемой сети позволяет оценить ее состояние в целом, и пользователь имеет возможность проанализировать результаты оценки защищенности сети в контексте исходной информации, которая доступна в разнообразных видах, расположенных на одной панели управления.



■ *Рис. 5.* Главное окно системы анализа защищенности компьютерной сети

Для представления компьютерных сетей большого размера используется обычное геометрическое и семантическое масштабирование. Применение механизмов семантического масштабирования позволяет проводить агрегирование узлов графа, исходя из значений свойств узла (принадлежность к рабочей группе, домену и т. д.). Агрегирование узлов происходит в интерактивном режиме: пользователь может свернуть/развернуть часть сети, выбирая соответствующий пункт контекстного меню выбранного узла сети.

Отличительной особенностью разрабатываемой системы является возможность визуально анализировать отчеты сканеров уязвимости и графов атак одновременно; таким образом, пользователь системы может оценить потенциальные причины нарушения безопасности в компьютерной сети и возможные последствия их эксплуатации злоумышленником.

Выявленные уязвимости оцениваются при помощи метрик, определенных системой CVSS [20]. Статистическая информация по выявленным уязвимостям представляется с помощью простых графических моделей, применяющих секторные и пузырьковые диаграммы.

Например, секторные диаграммы используются для отображения распределения уязвимостей с учетом их критичности (Severity), сложности реализации (Access Complexity), уровня ущерба (Mortality) для одного хоста и для всей сети в целом. При этом пользователь может выбрать сектор диаграммы и, нажав на него мышью, получить перечень уязвимостей, попавших в заданную категорию. Информация о наиболее часто встречаемых уязвимостях в системе и наиболее уязвимых хостах также представляется в виде секторной диаграммы.

Пузырьковые диаграммы используются для анализа сложности реализации и критичности уязвимостей, выявленных на одном хосте, т. е. пользователь имеет возможности оценить число наиболее критичных уязвимостей в контексте сложности их эксплуатации.

Поскольку указанные метрики могут принимать ограниченное число значений: {Высокий, Средний, Низкий} для показателя критичности и {Высокий, Низкий} для сложности их эксплуатации, — то число комбинаций этих значений равно шести, благодаря чему генерируемое изображение не перегружено и легко читается поль-

зователем. Размер пузырька определяется числом уязвимостей, принадлежащих заданной категории, а цвет определяется комбинацией этих двух метрик: чем выше уровень критичности и ниже уровень сложности эксплуатации уязвимости, тем насыщенней и ярче красный цвет.

Данные графические модели представления просты и понятны пользователю, кроме того, могут быть использованы в отчетной документации любого уровня. Однако они не подходят для представления данных большого объема, так как оптимальное число различных категорий данных, отображаемых с их помощью, равно 10–15 [11]. Для формирования общего представления о выявленных уязвимостях в системе используются карты деревьев, каждый вложенный прямоугольник которых обозначает узел сети. Используя такие атрибуты, как размер прямоугольника и его цвет, можно закодировать атрибуты анализируемого объекта. Например, на рис. 6 размер прямоугольников определяется уровнем критичности узла, назначаемым пользователем. Таким образом, наиболее важные с точки зрения пользователя узлы более заметны. Цвет используется для обозначения критичности выявленных на хосте уязвимостей. Так, красный цвет соответствует высокому уровню критичности, а желтый — низкому уровню.

Такой подход позволяет определить или изменить план мероприятий для повышения уровня защищенности компьютерных сетей, например график обновлений и замены программного обеспечения. Для того чтобы позволить пользователю работать с крупномасштабными сетями, предусмотрен гибкий механизм масштабирования, позволяющий отображать выбранную часть (домен, рабочую группу) карты деревьев, определяемую иерархией сети.

Следует отметить, что для представления результатов анализа уязвимостей мы используем семантическую цветовую схему при представлении значений метрик — от желтого к красному. Зеленые цвета в отчетах об уязвимостях не используются, так как они обычно применяются для обозначения нормальных (безопасных) значений показателей, а любая уязвимость потенциально несет угрозу для безопасности системы.

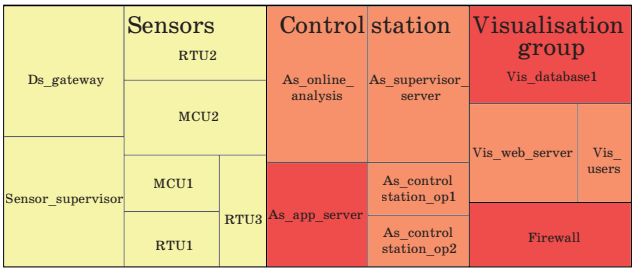
Для представления результатов моделирования атак используются графы. Каждый узел графа соответствует определенному атакующему действию, а их порядок отражает последовательность действий, выполняемых злоумышленником: узлы, расположенные на одном уровне, обозначают действия, которые могут быть выполнены одновременно или независимо друг от друга, а узлы, расположенные на разных уровнях, обозначают действия, которые выполняются в определенной последовательности.

В системе используются условные обозначения (таблица). Для обозначения типа действия применяются одновременно цвет и форма пиктограммы, благодаря этому с помощью цвета могут быть закодированы характеристики, вычисленные для каждого действия.

Графы атак позволяют изучить развитие атаки в анализируемой компьютерной сети, отслеживая действия нарушителя. Однако исследования показали, что графы атак могут обладать высокой степенью связности и быть чрезвычайно сложными, что значительно затрудняет их применение на практике [17]. В целях упрощения и повышения эффективности процесса их анализа были разработаны следующие способы взаимодействия с графическим представлением графов атак.

Геометрическое масштабирование. Позволяет пользователю сфокусироваться на определенных частях графа и уменьшить уровень связности графа. Расстояние между узлами графа может быть динамически изменено с помощью колесика мыши.

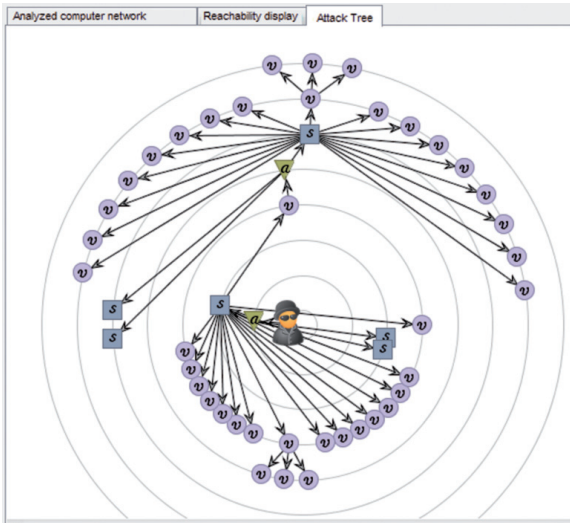
Настройка компоновки графа. В настоящее время в системе поддерживаются два алгоритма компоновки графа — древовидный и радиальный. Радиальное расположение графа более компактно и позволяет пользователю увидеть граф атак целиком (рис. 7). Такое расположение полезно при использовании цветовой кодировки значений метрик, ассоциированных с узлами графа, благодаря чему пользователь может получить представление о сложности выполняемой атаки. Древовидная компоновка графа удобна при изучении последовательности действий атакующего.



■ ***Рис. 6***. Представление результатов анализа уязвимостей в виде карты деревьев

■ Условные обозначения, используемые в системе оценки защищенности компьютерной сети

Обозначение	Описание
	Начальное положение злоумышленника
	Атомарное действие, имеющее разведывающий характер
	Сценарий, в котором не задействованы уязвимости
	Атакующее действие, использующее уязвимость



■ ***Рис. 7.*** Радиальное расположение узлов графа атак

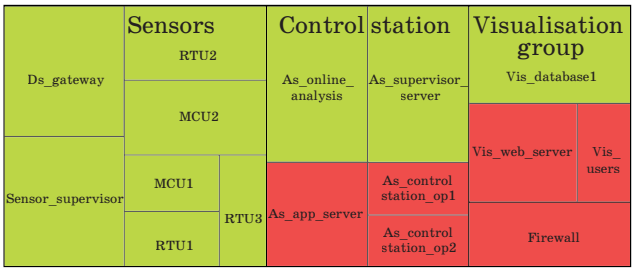
Семантическое масштабирование (агрегирование узлов графа). Для уменьшения сложности графа в системе используется механизм агрегации узлов графа, учитывающий его семантические и структурные свойства. Для формирования кластеров графа адаптирован подход, предложенный в работе [21]. В зависимости от таких свойств узла, как тип действия злоумышленника, хост, принадлежность группе/домену, вершины графа могут быть заменены на один мета-узел.

Используемые правила агрегации схематично представлены на рис. 8. Агрегирование узлов графа выполняется в интерактивном режиме. Пользователь имеет возможность определять степень агрегирования графа, задавая свойства и их последовательность применения для формирования мета-узлов.

Детали по требованию. При нажатии на узел графа мышью пользователь получает детальную информацию в отдельной вкладке окна. Эта информация включает тип атаки, хост, на котором выполняется атакующее действие, атакуемый хост, критичность хоста, описание уязвимости, вычисленные метрики безопасности (Ущерб, Уровень риска).

Подсветка и связывание. Данный визуальный эффект может быть использован для выделения пути в графе атак. При включении данного

■ ***Рис. 8.*** Иерархия правил агрегации узлов графа атак



■ ***Рис. 9.*** Представление скомпрометированных и защищенных узлов сети в виде карты деревьев

режима пользователь может выбрать узел графа, нажав на него указателем мышки, после чего все узлы, предшествующие и последующие выбранному, остаются цветными, а все остальные окрашиваются в оттенки серого.

Представление результатов моделирования атак в виде графов полезно при анализе последовательности действий злоумышленника, однако они не дают интуитивное представление о числе скомпрометированных узлов в сети. Для анализа достижимости узлов злоумышленником предлагается использовать карты деревьев, которые компактно представляют иерархическую структуру. Если, согласно результатам анализа защищенности компьютерной сети, узел может быть скомпрометирован, то соответствующий ему прямоугольник закрашивается красным цветом, в противном случае — зеленым.

На карте деревьев (рис. 9) размер прямоугольников соответствует уровню критичности узла для бизнес-процессов, а цветом обозначается состояние хоста. Поскольку при таком представлении пользователь не знает, какие уязвимости были использованы злоумышленником, он может получить данную информацию, нажав мышью на соответствующий прямоугольник карты деревьев.

Благодаря такому способу представления специалист может коррелировать выявленные уязвимости в компьютерной сети с числом потенциально скомпрометированных узлов, оценивая таким образом возможные последствия атаки.

Заключение

Анализ существующих программных решений по визуализации информации о защищенности компьютерной сети показал, что они предназначены для решения конкретной, достаточно узкой задачи, например, визуального анализа уязвимостей или моделирования атак. Для формирования полного понимания состояния защищенности системы пользователю необходимо применить нескольких таких инструментов, что может значительно усложнить работу системно-

го администратора и повлиять на ее эффективность в целом. Спроектированная авторами подсистема визуализации позволяет оценить уровень защищенности системы более полно и может быть использована как система поддержки принятия решения по планированию мероприятий по обеспечению безопасности, поскольку позволяет соотнести выявленные недостатки системы с возможными последствиями их эксплуатации и тем самым обоснованно определить наиболее критичные и требующие оперативного устранения уязвимости.

Работа выполняется при финансовой поддержке РФФИ, 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.

Литература

1. **Keim D.** et al. Visual Analytics: Definition, Process, and Challenges // Information Visualisation, LNCS 4950. Springer-Verlag, 2008. P. 154–175.
2. **Новикова Е. С., Котенко И. В.** Механизмы визуализации в SIEM-системах // Системы высокой доступности. 2012. № 2. С. 91–99.
3. **Новикова Е. С., Котенко И. В.** Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях // Тр. СПИИРАН. 2012. Вып. 4(23). С. 7–30.
4. **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 // Тр. СПИИРАН. 2012. Вып. 1(20). С. 27–56.
5. **Чечулин А. А., Котенко И. В.** Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы. 2010. № 6(49). С. 21–27.
6. **Kotenko I., Chechulin A.** Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing, Besançon, France, Nov. 20–23, 2012 / Los Alamitos, California. IEEE Computer Society, 2012. P. 94–101.
7. **Bertini E., Hertzog P., Lalanne D.** SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms // Proc. of the IEEE Symp. on Visual Analytics Science and Technology (VAST). 2007. P. 139–146.
8. **Foresti S.** et al. Visual Correlation of Network Alerts // IEEE Comput. Graph. Appl. 2006. Vol. 26. N 2. P. 48–59.
9. **Tran T., Al-Shaer E., Boutaba R.** PolicyVis: firewall security policy visualisation and inspection // Proc. of the 21st Conf. on Large Installation System Administration Conf. (LISA'07) / USENIX Association. Berkeley, CA, USA, 2007. P. 1–16.
10. **Mansmann F., Göbel T., Cheswick W.** Visual Analysis of Complex Firewall Configurations // Proc. of the 12th Intern. Workshop on Visualisation for Computer Security (VizSec'12). Seattle, WA, USA, 2012. P. 1–8.
11. **Marty R.** Applied Security Visualization. — N. Y.: Addison Wesley Professional, 2008. — 552 p.
12. **Montemayor J.** et al. Information Visualisation for Rule-based Resource Access Control // Proc. of Int. Symp. on Usable Privacy and Security (SOUPS), 2006. 2 p.
13. **Heitzmann A., Palazzi B., Papamanthou C., Tamassia R.** Effective Visualisation of File System Access-Control // Proc. of the 5th Intern. Workshop on Visualisation for Computer Security (VizSec'08). Berlin, Heidelberg: Springer-Verlag, 2008. P. 18–25.
14. **Harrison L.** et al. NV: Nessus Vulnerability Visualisation for the Web // Proc. of the 12th Intern. Workshop on Visualisation for Computer Security (VizSec'12). Seattle, WA, USA, 2012. P. 25–32.
15. **Nessus** vulnerability scanner website. http://www.tenable.com/ (дата обращения: 10.04.2013).
16. **Kotenko I., Stepashkin M.** Attack Graph based Evaluation of Network Security // Lecture Notes in Computer Science. 2006. Vol. 4237. P. 216–227.
17. **Noel S., Jacobs M., Kalapa P., Jajodia S.** Multiple Coordinated Views for Network Attack Graphs // Proc. of the IEEE Workshops on Visualization for Computer Security. IEEE Computer Society, 2005. P. 12.
18. **Williams L., Lippmann R., Ingols K.** An Interactive Attack Graph Cascade and Reachability Display // Proc. of the Workshop on Visualization for Computer Security, Sacramento, California, USA, 2007. Springer, Heidelberg. P. 221–236.
19. **Chu M.** et al. Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR // Proc. of the Seventh Intern. Symp. on Visualization for Cyber Security, Ontario, Canada. P. 22–33.
20. **Mell P., Scarfone K., Romanosky S.** A Complete Guide to the Common Vulnerability Scoring System Version 2.0 // Forum of Incident Response and Security Teams, June, 2007. P. 23.
21. **Homer J., Varikuti A., Ou X., McQueen M. A.** Improving Attack Graph Visualization Through Data Reduction and Attack Grouping // Proc. of the 5th Intern. Workshop on Visualisation for Computer Security (VizSec'08). Berlin, Heidelberg: Springer-Verlag, 2008. P. 68–79.