ОЦЕНКА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ГРАФОВ АТАК И КАЧЕСТВЕННЫХ МЕТРИК ЗАЩИЩЕННОСТИ

И. В. Котенко, М. В. Степашкин, В. С. Богданов

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<ivkote@comsec.spb.ru>, <stepashkin@comsec.spb.ru>,
<bogdanov@comsec.spb.ru>

УДК 681.3

Котенко И. В., Степашкин М. В., Богданов В. С. **Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности** // Труды СПИИРАН. Вып. 3, т. 2. — СПб.: Наука, 2006.

Аннотация. *В работе предлагается подход к анализу защищенности компьютерных сетей, предназначенный для использования как на этапах их проектирования, так и эксплуатации. Подход базируется на автоматической генерации общего графа атак и использовании качественных метрик защищенности. Граф отражает возможные распределенные сценарии атак с учетом конфигурации сети, реализуемой политики безопасности, а также местоположения, целей, уровня знаний и стратегий нарушителя. Рассмотрены общая архитектура предлагаемой системы анализа защищенности, основные понятия общего графа атак, используемые таксономии метрик защищенности, правила их расчета, а также методика оценки общего уровня защищенности. Предложенные метрики защищенности позволяют оценивать защищенность компьютерной сети с различной степенью детализации и с учетом различных аспектов. Представлено описание реализованного программного прототипа и рассмотрены примеры его использования для экспресс-анализа защищенности тестовой компьютерной сети.* — Библ. 38 назв.

UDC 681.3

Kotenko I. V., Stepashkin M. V., Bogdanov V. S. **Evaluating Security of Computer Networks based on Attack Graphs and Qualitative Security Metrics** // SPIIRAS Proceedings. Issue 3, vol. 2. — SPb.: Nauka, 2006.

Abstract. *Approach to computer network security analysis for using both at design and operation stages is suggested. This approach is based on generating common attack graph and using qualitative security metrics. The graph represents possible scenarios of distributed attacks taking into account network configuration, security policy, malefactor's location, knowledge level and strategy. The general architecture of the security analysis system proposed, the main concepts of common attack graph, used security metrics taxonomies, metrics calculation rules and general security level evaluation procedure are considered. The suggested security metrics allow to evaluate computer network security level with different detailing level and taking into account different aspects. The implemented software prototype is described, and examples of using the prototype for express-analysis of computer network security level are considered.* — Bibl. 38 items.

1. Введение

Нарушение информационной безопасности компьютерных сетей может быть вызвано множеством различных причин: наличием уязвимостей в операционных системах и приложениях; неверной конфигурацией аппаратного и программного обеспечения; ошибками, допущенными при настройке контроля доступа; наличием уязвимых или легко атакуемых сервисов и т.д.

Используя комбинации имеющихся уязвимостей и недостатков в конфигурации сети и применяемой политике безопасности, нарушители (как внешние, так и внутренние), в зависимости от своих целей, могут реализовать различные стратегии нападения. Эти стратегии могут быть направлены на разные крити-

ческие ресурсы сети и включать разнообразные цепочки атакующих действий. В рамках этих цепочек может осуществляться пошаговая компрометация различных хостов и реализация различных угроз безопасности.

Поэтому при проектировании и эксплуатации компьютерных сетей перед проектировщиком и (или) администратором сети возникает задача проверки того, обеспечивают ли планируемые для применения или уже используемые параметры конфигурации сети и механизмы защиты необходимый уровень защищенности. Кроме того, на этапе эксплуатации компьютерных сетей довольно часто происходят изменения в ее конфигурации и составе используемого программного и аппаратного обеспечения, поэтому необходимо постоянно производить мониторинг сети, анализ имеющихся уязвимостей и оценку уровня защищенности. На этапе проектирования основными исходными данными для анализа защищенности выступают спецификации проектируемой сети и политики безопасности, а на этапе эксплуатации — параметры реальной сети.

Возросшая сложность компьютерных сетей и механизмов защиты, увеличение количества уязвимостей и потенциальных ошибок в их использовании, а также возможностей нарушителей по реализации атак обуславливает необходимость разработки мощных автоматизированных средств (систем) анализа защищенности [17, 26]. Эти системы призваны выполнять задачи по обнаружению и исправлению ошибок в конфигурации сети и используемой политике безопасности, выявлению возможных трасс атакующих действий различных категорий нарушителей, определению критичных сетевых ресурсов и выбору адекватной угрозам политики безопасности, которая задействует наиболее подходящие в заданных условиях защитные механизмы.

На этапе проектирования могут использоваться различные методы анализа защищенности и определения общего уровня защищенности, например, базирующиеся на основе количественных и качественных методик анализа риска, в том числе на основе математического аппарата теории вероятностей, байесовских сетей, теории возможностей, нечетких множеств и т.п. [1, 2]. Перспективным направлением в оценке уровня защищенности являются подходы, основанные на построении представления возможных действий нарушителей в виде деревьев или графов атак и последующей проверки свойств этого дерева (графа) на базе использования различных методов, например, методов верификации на модели (model checking), а также вычисления на базе данного представления разнообразных метрик защищенности.

*На этапе эксплуатации к*омпьютерных систем используются пассивные и активные методы анализа уязвимостей. Пассивные методы реализуются на основе анализа журналов регистрации событий, настроек программного и аппаратного обеспечения и т.п. Активные методы сводятся к «тестированию сетей на проникновение», выполняемого путем реализации различных атакующих действий. Пассивные методы не позволяют оценить возможные трассы проникновения нарушителей, а активные не всегда могут быть применены, так как приводят к нарушению работоспособности отдельных сервисов или системы в целом. Комбинирование пассивного метода (для получения соответствующих данных о текущей конфигурации и реализуемой политике безопасности), процедур построения графов атак и автоматического вывода и проверки (анализа) свойств построенного графа позволяет частично решить две указанные проблемы.

Данная работа посвящена разработке архитектуры, моделей и прототипов системы анализа защищенности (САЗ), базирующейся на формировании графа

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

атак и вычислении разнообразных метрик защищенности на основе комбинирования качественных методик анализа риска. Предлагаемый подход подразумевает реализацию комплекса следующих функций: (1) построение графов возможных атакующих действий, выполняемых из различных точек сети и направленных на реализацию различных угроз безопасности с учетом квалификации нарушителя; (2) определение уязвимостей и «узких мест» в защите (наиболее критичных компонентов компьютерной сети); (3) вычисление различных метрик защищенности и определение общего уровня защищенности; (4) сопоставление полученных метрик с требованиями и выработка рекомендаций по усилению защищенности.

Работа организована следующим образом. В разделе 2 представлен краткий обзор близких по тематике работ и основные положения предлагаемого подхода. В разделе 3 описана обобщенная архитектура предлагаемой САЗ. В разделе 4 дается определение основных понятий и процедур, применяемых при формировании графа атак и вычислении метрик защищенности. В разделе 5 представлена модель определения уровня защищенности, в том числе заданы используемые таксономии и примеры метрик защищенности, правила их расчета и методика оценки общего уровня защищенности. В разделе 6 дано описание реализации программного прототипа и примеры его использования для экспресс-анализа защищенности тестовой компьютерной сети. В заключении приведены основные результаты работы и обозначены направления дальнейших исследований.

2. Релевантные работы и сущность предлагаемого подхода

В настоящее время существует много работ, раскрывающих различные подходы к анализу защищенности [1–4, 5, 7, 8, 10–16, 18–20, 25, 27–29, 31–36, 37, 38]. Например, в приведенных ниже работах используются различные способы представления сценариев атак и построения графов (деревьев) атак для анализа защищенности: деревья атак [32], формальные грамматики [10], раскрашенные сети Петри [15], метод анализа изменения состояний [4], причинно-следственная модель атак [5], описательные модели сети и злоумышленников [38], структурированное описание на базе деревьев [8], использование и создание графов атак для анализа уязвимостей [12], объектно-ориентированное дискретное событийное моделирование [3], модели, основанные на знаниях [33] и т.д. В [1, 2] излагаются возможные методики анализа рисков для оценки степени защищенности компьютерных систем. В [13, 14] предлагается методика анализа графов атак, рассматривается использование метода верификации на модели (model checking), байесовского и вероятностного анализа, описывается генерация событий, возникающих при реализации атак, исследование их влияния на заданную спецификацию сети и отображение полученных результатов на сценарных графах. В работе [16] предлагается метод оценки уровня защищенности на основе теории игр. В этой работе авторы рассматривают взаимодействие между злоумышленником и администратором как вероятностную игру с двумя игроками и предлагают модель данной игры.

Основное отличие предлагаемого в данной работе подхода от рассмотренных заключается в использовании построенного общего графа атак для определения семейства различных показателей (метрик) защищенности, задействуемых для качественного анализа заданной конфигурации сети и реализуемой политики безопасности. Система анализа защищенности, использующая пред-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ложенный подход, предназначена для функционирования на различных этапах жизненного цикла компьютерной сети, включая этапы проектирования и эксплуатации. На этапе проектирования САЗ оперирует с моделью анализируемой компьютерной сети, которая базируется на заданной спецификации компьютерной сети и реализуемой политики безопасности. На этапе эксплуатации САЗ взаимодействует с реальной компьютерной сетью. В результате анализа защищенности определяются уязвимости, строятся трассы (графы) возможных атак, выявляются «узкие места» в компьютерной сети, и вычисляются различные метрики защищенности, которые могут быть использованы для оценки общего уровня защищенности компьютерной сети (системы), а также уровня защищенности ее компонентов. Полученные результаты обеспечивают выработку обоснованных рекомендаций по устранению выявленных узких мест и усилению защищенности системы. На основе данных рекомендаций пользователь вносит изменения в конфигурацию реальной сети или в ее модель, а затем, если необходимо, повторяет процесс анализа уязвимостей и оценки уровня защищенности. Таким образом, обеспечивается требуемый уровень защищенности компьютерной сети (системы) на всех этапах ее жизненного цикла.

3. Архитектура системы анализа защищенности

Обобщенная архитектура САЗ представлена рис. 1.

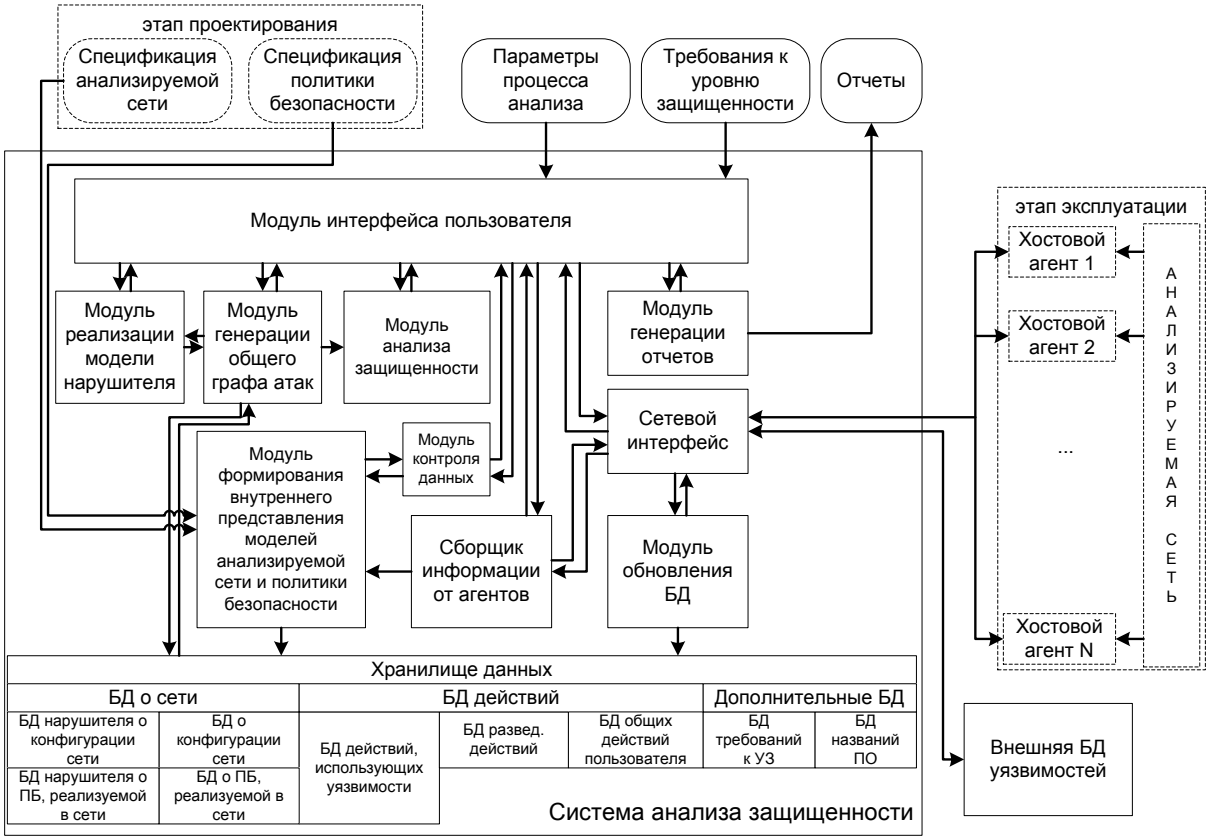

Рис. 1. Обобщенная архитектура системы анализа защищенности.

Модуль интерфейса пользователя позволяет пользователю управлять работой всех компонентов системы, задавать входные данные, просматривать отчеты по анализу защищенности и т.п. *Хостовые агенты* служат для пассив-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ного сбора информации. На основе полученных агентами данных строится модель анализируемой компьютерной сети на этапе ее эксплуатации. Например, хостовые агенты могут производить анализ конфигурационных файлов операционной системы и других программных компонент. *Сетевой интерфейс* обеспечивает взаимодействие САЗ с внешней средой: обращение к внешним базам данных уязвимостей за обновлениями; связь с агентами сбора информации. *Сборщик информации* взаимодействует с агентами и получает от них различную информацию, связанную с конфигурацией анализируемой компьютерной сети и реализуемой политикой безопасности.

Модуль формирования внутреннего представления анализируемой сети и политики безопасности преобразует данные об анализируемой сети и реализуемой политике безопасности, получаемые от сборщика информации (на этапе эксплуатации сети) или задаваемые пользователем на специализированных языках SDL (System Description Language) и SPL (Security Policy Language) (на этапе проектирования) во внутреннее представление. Вводимые в САЗ спецификации системы и политики безопасности должны описывать компоненты защищаемой системы (сети) с необходимой степенью детализации – должно быть задано используемое программное обеспечение (в виде названий программных продуктов и их версий). Если требуемых для анализа уровня защищенности данных не достаточно (например, пользователь не определил версию используемого сетевого сервиса), система должна предложить пользователю ввести необходимую информацию на основе базы данных программного обеспечения. Для обнаружения некорректных или недоопределенных данных, которые необходимы для анализа защищенности, служит *модуль контроля данных.* Например, пользователь может допустить ошибку в названии сервиса или указать, что на сервере открыт 21 порт, но не определить, какое приложение обрабатывает поступающие на данный порт запросы. Для устранения возникающих при вводе спецификаций модуль контроля обеспечивает пользователю выбор необходимых данных, используя базу названий программного обеспечения (ПО).

Хранилище данных состоит из следующих групп баз данных (БД): (1) группа баз данных о сети и реализуемой в ней политике безопасности; (2) группа баз данных действий; (3) группа дополнительных баз данных.

Группа баз данных о сети состоит из четырех баз: (1) *БД о конфигурации анализируемой компьютерной сети (КС)*; (2) *БД о реализуемой в КС политике безопасности (ПБ)*; (3) *БД нарушителя о конфигурации анализируемой КС* и (4) *БД нарушителя о реализуемой в КС политике безопасности*. Структурно данные БД попарно (базы о конфигурации и базы о политике безопасности) совпадают и содержат сведения об архитектуре и конкретных параметрах компьютерной сети (например, тип и версию ОС, список открытых портов и т.п.) и правилах, описывающих ее функционирование. Первая БД о конфигурации анализируемой КС фактически является внутренним представлением спецификации анализируемой сети, которая используется для формирования результата атакующих действий при построении общего графа атак. БД нарушителя о конфигурации КС является внутренним представлением спецификации анализируемой сети так, как ее представляет себе нарушитель, т.е. как результат реализации последовательности атакующих действий. БД о реализуемой политике безопасности содержит общие правила функционирования сети, например, «локальный пользователь хоста h не может запускать приложение A». На основе информации из БД нарушителя о реализуемой в сети ПБ становится

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

возможным планирование последовательности выполняемых нарушителем действий (например, согласно политике безопасности, доступ к файлу F разрешен только локальным администраторам, поэтому для чтения данного файла нарушителю необходимо получить требуемые права, т.е. реализовать определенную последовательность действий).

Группа баз данных действий состоит из следующих баз: (1) БД действий, использующих уязвимости; (2) БД разведывательных действий; (3) БД общих действий пользователя. *БД действий, использующих уязвимости* (в отличие от других баз данной группы) строится на основе внешней базы данных уязвимостей. Атакующие действия в данной базе делятся на следующие группы: (1) действия, направленные на получение прав локального пользователя; (2) действия, направленные на получение прав администратора; (3) действия, направленные на нарушение конфиденциальности, (4) целостности и (5) доступности. Примерами действий, содержащихся в данной базе, являются используемые в тестовом примере действия «ServU-local-priv-esc», «Utilman» и др. *БД разведывательных действий* содержит действия, направленные на удаленное получение информации о хосте или сети. Описание разведывательных действий не содержится во внешних базах уязвимостей. Информацию о методах и средствах реализации нарушителем разведывательных действий можно получить лишь экспертным путем. Примерами действий, входящих в данную базу, являются следующие действия из тестового примера: (1) «Nmap-OS», (2) «Ping» и т.д. *База данных общих действий пользователя* содержит информацию о возможных действиях пользователя, выполняемых в соответствии с имеющимися у него полномочиями. К таким действиям могут относиться, например, подготовительные действия для выполнения атакующих действий, а также такие действия, как «чтение файла», «копирование файла», «удаление файла», «удаление каталога» и т.п., которые возможно использовать для реализации угроз на нарушение конфиденциальности, целостности и доступности объектов. Для каждого атакующего действия в БД хранится условие успешной реализации данного действия (например, версия уязвимого программного обеспечения) и результат его воздействия на объект атаки (например, аварийное прекращение работы сетевого сервиса).

Группа дополнительных БД состоит из следующих баз: (1) БД требований к уровню защищенности и (2) БД названий ПО. *БД требований к уровню защищенности* содержит предопределенные экспертным способом наборы значений метрик защищенности, каждый из которых соответствует требованиям к системам определенного класса защищенности, регламентируемым международными стандартами и другими нормативными документами. *База данных названий ПО* используется модулем контроля данных для выявления ошибок в используемой спецификации компьютерной сети и формирования рекомендуемых для использования программных средств, в случае отсутствия в спецификации необходимых для анализа защищенности данных.

Модуль обновления БД скачивает открытые базы данных уязвимостей (например, OSVDB – open source vulnerability database [24]) и транслирует их в базу данных атакующих действий. *Модуль генерации общего графа атак* производит построение графа атак, моделируя возможные действия нарушителя в анализируемой компьютерной сети, используя информацию о доступных действиях различных типов (атакующих, разведывательных, общих), конфигурации сети и используемой политике безопасности. Во время формирования графа атак данный модуль расставляет в вершинах метрики защищенности элемен-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

тарных объектов, на базе которых модуль анализа общего графа атак рассчитывает метрики составных объектов. *Модуль реализации модели нарушителя* обеспечивает определение первоначального положения нарушителя, уровня знаний и умений, первичные знания об анализируемой компьютерной сети. Уровень знаний и умений определяет используемый нарушителем набор действий. *Модуль анализа защищенности* формирует множество составных объектов общего графа атак (трасс, угроз), производит расчет метрик защищенности, относящиеся к данным объектам, производит качественную оценку общего уровня защищенности компьютерной сети, сравнивает полученные результаты с требованиями, определенными пользователем (если требования были заданы), выявляет «слабые места» в безопасности и формирует рекомендации по повышению общего уровня защищенности компьютерных сетей. *Модуль генерации отчетов* отображает пользователю информацию об обнаруженных уязвимостях в используемом программном и аппаратном обеспечении, «слабые места», рекомендации по повышению уровня защищенности анализируемой компьютерной сети.

4. Общий граф атак

Общий граф атак описывает всевозможные варианты реализации атакующих действий нарушителем с учетом его первоначального положения, уровня знаний и умений, первоначальной конфигурации компьютерной сети и реализуемой в ней политики безопасности.

Все *объекты графа атак* можно подразделить на базовые (элементарные) объекты и составные. Вершины графа задаются с использованием базовых объектов. Для формирования различных последовательностей действий нарушителя базовые объекты связываются на графе атак с помощью дуг. Составные объекты графа строятся на основе объединения элементарных объектов с помощью дуг. К *элементарным объектам* общего графа атак относятся объекты, принадлежащие к типам «хост» и «атакующее действие». *Множество объектов «хосты»* включает все обнаруженные нарушителем и атакуемые им сетевые компьютеры (хосты). *Множество объектов «атакующие действия»* состоит из всех различимых элементарных действий нарушителя.

Атакующие действия разделены на следующие классы: (1) действия по получению информации о сети (хосте), т.е. разведывательные действия; (2) подготовительные действия (в рамках уже имеющихся у нарушителя полномочий), служащие для создания условий реализации атакующих действий последующих классов; (3) действия, направленные на нарушение конфиденциальности; (4) действия, направленные на нарушение целостности; (5) действия, направленные на нарушение доступности; (6) действия, приводящие к получению нарушителем прав локального пользователя; (7) действия, приводящие к получению нарушителем прав администратора.

Все атакующие действия можно разделить также на две группы: (1) действия, использующие различные уязвимости программного и аппаратного обеспечения, например, «NTP_LINUX_ROOT» (использует уязвимость в сервисе NTP ОС Linux и позволяет нарушителю получить права администратора на атакуемом хосте); (2) обычные действия легитимного пользователя системы (в том числе действия по использованию утилит получения информации о хосте или сети), такие как «удаление файла», «остановка сервиса ОС» и т.п.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

К составным объектам отнесем объекты типов «трасса», «угроза» и «граф». *Трасса атаки* — это совокупность связанных вершин общего графа атак (хостов и атакующих действий), первая из которых представляет хост, соответствующий первоначальному положению нарушителя, а последняя не имеет исходящих дуг. Под *угрозой* будем понимать множество различных трасс атак, имеющих одинаковые начальную и конечную вершины.

Разделение атакующих действий по заданным выше классам, позволяет *классифицировать угрозы* следующим образом: (1) *основные угрозы* — угрозы нарушения конфиденциальности, угрозы нарушения целостности, угрозы нарушения доступности;(2) *дополнительные угрозы* — угрозы получения информации о сети (хосте), угрозы получения нарушителем прав локального пользователя, угрозы получения нарушителем прав администратора.

В общем случае, при успешной реализации нарушителем разведывательных действий, не происходит нарушения конфиденциальности, целостности и доступности информационных ресурсов. Однако, возможно нарушение конфиденциальности, например, в том случае, если политикой безопасности установлено, что информация о топологии внутренней сети является закрытой. При успешном получении нарушителем прав локального пользователя, возможности выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности, или на получение прав администратора увеличиваются, так, например, он может нарушить конфиденциальность, целостность и доступность некоторой совокупности объектов хоста, имея только права пользователя. При успешном получении прав администратора на хосте нарушитель может полностью нарушить конфиденциальность, целостность, доступность всех объектов данного хоста.

В направлении роста степени сложности все объекты графа атак можно упорядочить следующим образом (стрелка показывает направление увеличения вложенности объектов): *хосты, атакующие действия → трассы атак → угрозы → общий граф атак*.

Алгоритм формирования общего графа атак основан на реализации следующей последовательности действий: (1) реализация действий по перемещению нарушителя с одного хоста на другой, (2) реализация разведывательных действий по определению живых хостов, (3) реализация сценариев (множества действий) разведки для каждого обнаруженного хоста и (4) реализация атакующих действий, использующих уязвимости программного и аппаратного обеспечения и общих действий пользователя.

Первоначальное положение нарушителя четко определено. *Перемещение нарушителя с текущего хоста на атакуемый хост* осуществляется при получении нарушителем на атакуемом хосте прав локального пользователя или администратора в следующих случаях: (1) если существует возможность реализации атакующих действий, использующих уязвимости ПО и АО и требующих у нарушителя наличия прав локального пользователя на атакуемом хосте; (2) если переход на атакуемый хост открывает нарушителю доступ к другому сегменту сети; (3) если переход на атакуемый хост позволяет нарушителю использовать отношения доверия. Примером *разведывательного действия по определению живых хостов* является действие, эмулирующее работу утилиты «ping». Примеры *разведывательных действий*, на основе которых формируется множество сценариев разведки, приведены *в* разделе 6. После реализации каждого сценария из множества сценариев разведки производится проверка условий выполнения *атакующих действий, использующих уязвимости про-*

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

граммного и аппаратного обеспечения и общих действий пользователя. При успешной реализации атакующих действий данной группы, приводящих к получению нарушителем прав локального пользователя или администратора на атакованном хосте, осуществляется проверка необходимости перехода нарушителя на данный хост. В случае реализации перехода, вышеописанная последовательность действий повторяется для нового положения нарушителя.

5. Модель оценки уровня защищенности

Модель оценки уровня защищенности охватывает систему различных метрик защищенности (МЗ) и правил (формул), используемых для их расчета. Определение значений отдельных метрик и общая оценка уровня защищенности анализируемой компьютерной сети может производиться несколькими способами. Существует *два подхода к оценке уровня защищенности*: (1) качественная экспресс оценка защищенности компьютерной сети на основе качественных методик анализа рисков и (2) количественное вычисление уровня защищенности компьютерной сети (на основе математического аппарата теории вероятностей, байесовских сетей, теории возможностей, нечетких множеств и т.п.). Данный подход позволяет обеспечить большую точность оценки, но требует и большего количества используемых данных и выполняемых вычислений. В данной работе рассматривается первый подход — качественная экспресс оценка защищенности компьютерной сети на основе качественных методик анализа рисков.

Множество всех МЗ строится на основе сгенерированного общего графа атак. МЗ могут характеризовать защищенность как базовых, так и составных объектов графа атак. Проведем классификацию используемых метрик защищенности по трем признакам: (1) по разделению объектов общего графа атак на базовые и составные; (2) в соответствии с порядком вычислений; (3) в соответствии с тем, используются ли метрики для определения общего уровня защищенности анализируемой компьютерной сети.

В соответствие с разделением объектов общего графа атак на базовые и составные, множество всех метрик защищенности можно подразделить на следующие группы: (1) МЗ, формируемые по элементарным объектам (МЗ по хостам, МЗ по атакующим действиям); (2) МЗ, формируемые по составным объектам (МЗ по трассам атак, МЗ по угрозам, МЗ по общему графу атак).

В соответствии с порядком вычислений все МЗ можно разделить на две группы: (1) первичные и (2) вторичные. Первичные МЗ получаются непосредственно из общего графа атак, вторичные — рассчитываются с использованием первичных. Для расчета вторичных метрик защищенности множество метрик, рассчитываемых на основе общего графа атак, необходимо дополнить метриками, рассчитываемыми по заданной конфигурации анализируемой компьютерной сети.

В соответствии с тем, используются ли метрики для определения общего уровня защищенности анализируемой компьютерной сети, выделим основные и вспомогательные метрики. *Основные метрики* непосредственно используются для получения качественной оценки уровня защищенности анализируемой компьютерной сети. *Вспомогательные* метрики служат для построения «детальной картины», описывающей защищенность сети, требуемой, например, для выявления «узких мест» в защите и выработки рекомендаций по повышению защищенности.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В качестве основных определим следующие метрики: критичность хоста h ($\mathrm{Criticality}(h)$); уровень критичности атакующего действия a ($\mathrm{Severity}(a)$); размер ущерба, вызванного реализацией атакующего действия с учетом уровня критичности атакуемого хоста ($\mathrm{Mortality}(a,h)$); размер ущерба при реализации трассы S и угрозы T ($\mathrm{Mortality}(S)$ и $\mathrm{Mortality}(T)$); «сложность в доступе» для атакующего действия, трассы и угрозы ($\mathrm{AccessComplexity}(a)$, $\mathrm{AccessComplexity}(S)$, $\mathrm{AccessComplexity}(T)$); степень возможности реализации угрозы T ($\mathrm{Realization}(T)$); уровень риска угрозы T ($\mathrm{RiskLevel}(T)$); уровень защищенности анализируемой компьютерной сети (*SecurityLevel*).

Некоторые основные метрики защищенности (например, $\mathrm{Severity}(a)$) и значительная часть вспомогательных метрик рассчитываются на базе подхода *Common Vulnerability Scoring System* (CVSS) [6].

Индексы CVSS разделены на три основные группы: (1) базовые; (2) временные и (3) связанные с окружением. Базовые индексы определяют *критичность* уязвимости (атакующего действия, реализующего данную уязвимость). Временные индексы определяют *актуальность* уязвимости *в заданный момент времени*. Индексы, связанные с рабочим окружением, должны использоваться организациями для расстановки приоритетов при планировании действий по устранению уязвимостей. Индексы CVSS для атакующих действий, использующих различные уязвимости программного и аппаратного обеспечения, могут быть взяты непосредственно из внешних баз данных уязвимостей. Например, индексы для «SYN flood», могут быть получены из базы NVD [22].

Рассмотрим методику экспресс оценки общего уровня защищенности анализируемой компьютерной сети. Предлагаемая методика базируется на использовании оценки серьезности (критичности) атакующего действия, рассчитываемой на основе обобщенного уровня критичности атакующего действия CVSS, и методике анализа рисков FRAP («Facilitated Risk Analysis Process») [9].

Предложенный подход к получению качественной экспресс оценки защищенности компьютерной сети на основе качественных методик анализа рисков состоит из следующих этапов: (1) вычисление метрик защищенности базовых и составных объектов общего графа атак ($\mathrm{Criticality}$, $\mathrm{Severity}$, $\mathrm{AccessComplexity}$, $\mathrm{Realization}$); (2) получение качественных оценок уровня риска для всех угроз ($\mathrm{RiskLevel}$); (3) оценка уровня защищенности анализируемой компьютерной сети (*SecurityLevel*) на основе полученных оценок уровней риска всех угроз.

Размер ущерба, вызванного успешной реализацией атакующего действия, находится в зависимости от (1) критичности атакуемого хоста и (2) общего уровня критичности атакующего действия. Данную величину обозначим $\mathrm{Mortality}(a,h)$.

Критичность хоста определяется проектировщиком (администратором) анализируемой компьютерной сети по своему усмотрению по трехуровневой шкале (High, Medium, Low), исходя из назначения данного хоста и выполняемых им функций. При назначении уровня критичности хоста он может руководствоваться значениями, представленными в табл. 1.

Максимальный уровень критичности установлен для хостов, неверное функционирование (или полное прекращение функционирования) которых приводят к невозможности использования ресурсов сети. Далее в сторону умень-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

шения уровня критичности идут рабочие сервера, функционирование которых (каждого по отдельности) является очень важной составляющей успешной работы организации. Минимальным уровнем критичности обладают персональные рабочие станции, нарушения в работе которых незначительно влияют на процессы функционирования организации в целом.

Таблица 1

Определение критичности хоста

Критичность хоста	**Тип хоста**
High	DNS сервер, корпоративный маршрутизатор, контроллер домена; серверы и рабочие станции, обрабатывающие критическую информацию
Medium	web-, mail- и ftp-серверы, межсетевые экраны
Low	Персональные рабочие станции

Критичность атакующего действия рассчитывается с использованием обобщенной оценки критичности атакующего действия ($\text{BaseScore}(a)$) CVSS следующим образом [23]:

$$\text{Severity}(a) = \begin{cases} \textit{Low}, \ \text{BaseScore}(a) \in [0.0, 3.9] \\ \textit{Medium}, \ \text{BaseScore}(a) \in [4.0, 6.9] \\ \textit{High}, \ \text{BaseScore}(a) \in [7.0, 10.0] \end{cases}.$$

Размер ущерба, вызванного успешной реализацией атакующего действия с учетом уровня критичности атакуемого хоста, рассчитывается согласно табл. 2.

Таблица 2

Определение размера ущерба, вызванного успешной реализацией атакующего действия

Критичность хоста	**Уровень критичности атакующего действия**		
	High	**Medium**	**Low**
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Размер ущерба для хоста h с учетом его критичности, вызванного успешной реализацией угрозы, определяется ее последним атакующим действием: $\text{Mortality}(T) = \text{Mortality}(a_T, h_T)$, где a_T — последнее атакующее действие в угрозе, h_T — хост, на который направлено действие a_T.

Размер ущерба $\text{Mortality}(T)$ при реализации угрозы T можно охарактеризовать следующим образом: High — остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли; Medium — кратковременное прерывание работы критических процессов или систем, которое приводит к ограниченным финансовым потерям в одном бизнес-подразделении; Low — перерыв в работе, не вызывающий ощутимых финансовых потерь.

Однако, возможна ситуация, когда нарушителем во время реализации угрозы был нанесен гораздо бо́льший ущерб компьютерной сети, чем рассчитанный по последнему атакующему действию. Для учета данной ситуации необхо-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

димо ввести метрики максимального размера ущерба при реализации трассы S и угрозы T, рассчитываемые по следующим формулам:

$$\text{Mortality}^{\max}(S) = \max_i\left(\text{Mortality}(a_i, h_i)\right),\ i \in [1, N_S],\ a_i \in S,$$

$$\text{Mortality}^{\max}(T) = \max_i\left(\text{Mortality}(S_i)\right),\ i \in [1, N_T],\ S_i \in T,$$

где N_S — длина трассы (количество атакующих действий в трассе); N_T — количество трасс, реализующих угрозу T.

Для получения качественной оценки уровня риска угрозы необходимо оценить степень возможности ее реализации ($\text{Realization}(T)$) и воспользоваться методикой FRAP с использованием полученного ранее размера ущерба при реализации угрозы ($\text{Mortality}(T)$).

Для определения степени возможности реализации угрозы T воспользуемся индексом CVSS «сложность в доступе» из множества базовых индексов CVSS, задаваемых для каждого атакующего действия в графе атак. Возможными значениями данного индекса являются: (1) High — существуют условия на доступ, например, специфические временные рамки, специфические обстоятельства (специфическая конфигурация сервиса), взаимодействие с атакуемым человеком); (2) Low — нет специфических условий на доступ, т.е. использование уязвимости возможно всегда.

Тогда индекс «сложность в доступе» для трассы атак S будет вычисляться по следующей формуле:

$$\text{AccessComplexity}(S) = \begin{cases} High, \exists k \in [1,N]\ \text{AccessComplexity}(a_k) = High \\ Low, \forall k \in [1,N]\ \text{AccessComplexity}(a_k) = Low \end{cases},\ S = \{a_i\}_{i=1}^{N}$$

где S — сценарий (трасса) атаки; N — длина трассы (количество действий).

Расчет данного индекса для угрозы (совокупности различных трасс, имеющих одинаковые первую и последнюю вершины) производится по следующей формуле:

$$\text{AccessComplexity}(T) = \begin{cases} Low, \exists k \in [1,N_S]\ \ \text{AccessComplexity}(S_k) = Low \\ High, \forall k \in [1,N_S]\ \ \text{AccessComplexity}(S_k) = High \end{cases}$$

где $T = \{S_k\}_{k=1}^{N_S}$ — угроза; N_S — количество различных трасс, реализующих угрозу T; $S_k = \{a_i\}_{i=1}^{N_k}$ — трасса атаки; N_k — количество действий в трассе.

Тогда степень возможности реализации угрозы T будет рассчитываться по следующей формуле:

$$\text{Realization}(T) = \begin{cases} High, \text{AccessComplexity}(T) = Low \\ Low, \text{AccessComplexity}(T) = High \end{cases}.$$

Оценка уровня риска угрозы получается в соответствие с правилом, задаваемым матрицей рисков (табл. 3).

Полученная оценка уровня риска может интерпретироваться следующим образом: **уровень А** — связанные с риском действия (например, внедрение новых средств защиты информации или устранение уязвимостей) должны быть выполнены немедленно и в обязательном порядке; **уровень В** — связанные с

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

риском действия должны быть предприняты; **уровень C** — требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо); **уровень D** — никаких действий в данный момент предпринимать не требуется.

Таблица 3

Матрица оценки уровня риска угрозы

Степень возможности реализации угрозы	**Уровень серьезности (критичности) угрозы**		
	High	Medium	Low
High	**A**	**B**	**C**
Low	**B**	**C**	**D**

Исходя из полученных качественных оценок уровня риска для всех угроз, определим уровень защищенности анализируемой компьютерной сети следующим образом:

$$SecurityLevel = \begin{cases} Green, \forall i \in [1, N_T] \ \text{RiskLevel}(T_i) = D \\ Yellow, \forall i \in [1, N_T] \ \text{RiskLevel}(T_i) \le C \\ Orange, \forall i \in [1, N_T] \ \text{RiskLevel}(T_i) \le B \\ Red, \exists i \in [1, N_T] \ \text{RiskLevel}(T_i) = A \end{cases},$$

где $D < C < B < A$; N_T — количество всех угроз.

6. Программный прототип и его функционирование на тестовом примере

Для проведения экспериментов была специфицирована и реализована тестовая компьютерная сеть. На рис. 3 представлена структура тестовой компьютерной сети, используемой для проведения экспериментов в задаче анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации. Тестовая компьютерная сеть состоит из трех подсетей: части глобальной сети Интернет с IP адресами 195.19.200.*; демилитаризованной зоны (ДМЗ) с IP адресами 192.168.0.*; локальной вычислительной сети с IP адресами 10.0.0.*.

Для демонстрации предложенного подхода был реализован программный прототип системы анализа защищенности. Прототип реализован на языке программирования Java с использованием объектно-ориентированного подхода.

Рассмотрим функционирование программного прототипа САЗ компьютерных сетей на этапе проектирования на тестовых примерах. Первый пример отражает анализ защищенности компьютерной сети, в которой присутствует ряд уязвимостей в используемом программном обеспечении и реализуемой политики безопасности. Второй пример соответствует той же компьютерной сети после реализации рекомендаций по повышению уровня защищенности.

Раскроем ряд понятий, используемых в описании функционирования программного прототипа. Описание компьютерной сети, заданное на специализированном языке System Description Language (SDL), позволяет определить топологию сети (множество хостов и сетевых концентраторов), информацию о функционирующих операционных системах на хостах сети, информацию о настройках стека протоколов TCP/IP, информацию о сервисах и т.п. Описание по-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

литики безопасности, заданное на специализированном языке Policy Description Language (PDL), позволяет определить правила фильтрации сетевого трафика, отношения доверия и т.п. *Правила фильтрации* сетевого трафика задаются в виде набора таблиц [21]. В задаче анализа защищенности компьютерных сетей нас будут интересовать правила перенаправления портов («port forwarding»), задаваемые таблицами PREROUTING и FORWARD.

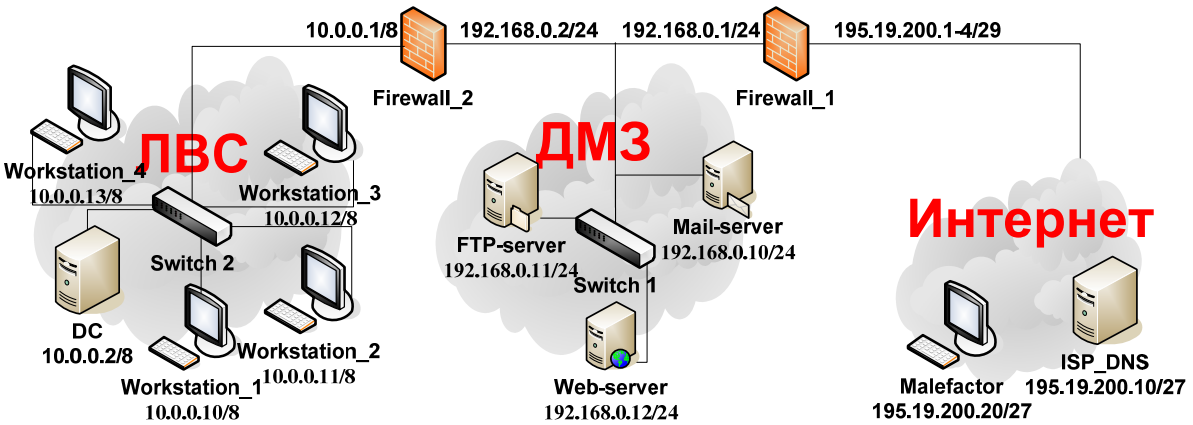

Рис. 3. Структура тестовой компьютерной сети.

Будем считать, что *хост 1 доверяет хосту 2*, если любому пользователю хоста 1, прошедшему процесс аутентификации, при обращении к хосту 2 имеет те же полномочия, что и на хосте 1. Например, пусть хост Firewall_1 доверяет хосту FTP_SERVER и пусть на хосте FTP_SERVER существует пользователь Tigra с правами локального пользователя USER. Тогда, если пользователь Tigra прошел аутентификацию на хосте FTP_SERVER, то при обращении к хосту Firewall_1 он будет также иметь права локального пользователя.

В таблице 4 представлены условные обозначения элементов, используемых на общем графе атак.

Таблица 4

Условные обозначения используемых на общем графе атак элементов

Действие нарушителя	описывает реализацию одного атакующего действия нарушителя
Конечное действие нарушителя	обозначает конечное действие нарушителя (не имеющее дальнейшего развития)
Положение нарушителя ПРАВА	служит для обозначения положения нарушителя (хост) и его прав на данном хосте
Атакуемый хост (критичность)	служит для обозначения атакуемых хостов и их уровня критичности

На графе используются следующие обозначения: (1) у хостов в скобках указан их уровень критичности; (2) для атакующих действий указан вектор, состоящий из следующих компонентов: уровень критичности атакующего действия и индекс CVSS «сложность в доступе».

Пример 1. Входными данными для примера 1 являются: (1) топология сети, сервисы, ОС и т.п. соответствуют описанию тестовой компьютерной сети; (2) правила перенаправления портов для хоста Firewall_1 приведены в табл. 5; (3) Firewall_1 и Firewall_2 доверяют всем хостам из ДМЗ; (4) нарушитель нахо-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

дится во внешней сети на хосте Malefactor и обладает на нем правами администратора; (5) в задании на анализ защищенности указано, что необходимо оценить все типы угроз (на нарушение целостности, доступности, конфиденциальности); (6) в задании на анализ защищенности указано, что необходимо провести анализ всех хостов ДМЗ и ЛВС; (7) пользователь в качестве требований к анализируемой сети указал, что данная сеть должна иметь уровень защищенности лучше, чем Orange (предполагается использование четырех уровней защищенности системы, их можно упорядочить по возрастанию уровня защищенности следующим образом: красный (Red), оранжевый (Orange), желтый (Yellow) и зеленый (Green)).

Таблица 5

Правила перенаправления портов для хоста Firewall_1

Комментарий	**Destination (целевой хост)**		**Forward to… (перенаправить на…)**	
	IP	**Port**	**IP**	**Port**
Web_server	195.19.200.3	80	192.168.0.12	80
FTP_server	195.19.200.2	21	192.168.0.11	21
MAIL_server POP3	195.19.200.4	110	192.168.0.10	110
MAIL_server SMTP	195.19.200.4	25	192.168.0.10	25
MAIL_server RDC	195.19.200.4	3389	192.168.0.10	3389

На рис. 4 представлен общий граф атак, соответствующий вышеописанным входным данным. Кратко рассмотрим построение данного графа атак.

Нарушитель, находясь на хосте Malefactor, реализует атаку «Ping Hosts», позволяющую определить живые хосты. Согласно заданному описанию анализируемой компьютерной сети, результатом выполнения данного действия является получение нарушителем информации о четырех хостах (FTP_server, Web_server, Mail_server и Firewall_1) с IP-адресами 195.19.200.1–4 (реально это один хост Firewall_1, однако этого нарушитель не знает). Далее нарушитель производит анализ каждого хоста отдельно.

Рассмотрим подробнее анализ хоста с IP-адресом 195.19.200.2. Согласно информации из базы данных разведывательных действий нарушителю доступны четыре сценария разведки: (1) «Nmap serv» (определение множества открытых портов); (2) «Nmap OS» (определение типа и версии ОС); (3) «Nmap serv»+«Banner» (определение множества открытых портов и идентификация сервисов); (4) «Nmap serv»+«Banner»+«Nmap OS». После реализации каждого из сценариев разведки (в представленной последовательности) нарушитель производит проверку, удовлетворяет ли полученная о хосте информация условиям выполнения атакующих действий, использующих уязвимости. Действия, использующие уязвимости, которые уже были отображены на графе после одного из сценариев разведки, не отображаются повторно после последующих сценариев. Это реализовано для того, чтобы избежать излишнего загромождения графа. Например, атакующее действие «SYN flood» может быть реализовано сразу же после первого сценария разведки («Nmap serv»). Оно может быть реализовано также после третьего и четвертого сценариев. Однако после данных сценариев на графе атак не отображается действие «SYN flood». Результатом действия «NMap serv» для хоста с IP-адресом 195.19.200.2 является перечень открытых портов на хосте FTP_server (открытый порт один — 21), так как согласно таблице перенаправления портов входящие соединения на адрес 195.19.200.2:21 (где 21 — порт назначения) перенаправляются на 192.168.0.11:21. Таким образом, нарушитель определяет наличие одного от-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

крытого порта, который может быть атакован с использованием атакующего действия «SYN flood». Информация, полученная нарушителем после реализации второго сценария разведки («Nmap OS»), не позволяет реализовать какое-либо атакующее действие, использующее уязвимости. Реализовав третий сценарий разведки, нарушитель может использовать три действий, использующих уязвимости: (1) подбор пароля («FTP dict»); (2) атака на отказ в обслуживании («ServU-MKD»); (3) атака по повышению привилегий («ServU-MDTM»). Первые два действия являются конечными. Выполнив третье действие, нарушитель получает права администратора, что дает ему всю информацию о хосте FTP_server. Получение прав администратора позволяет нарушителю осуществить переход на данный хост для последующей реализации атакующих действий, направленных на другие хосты.

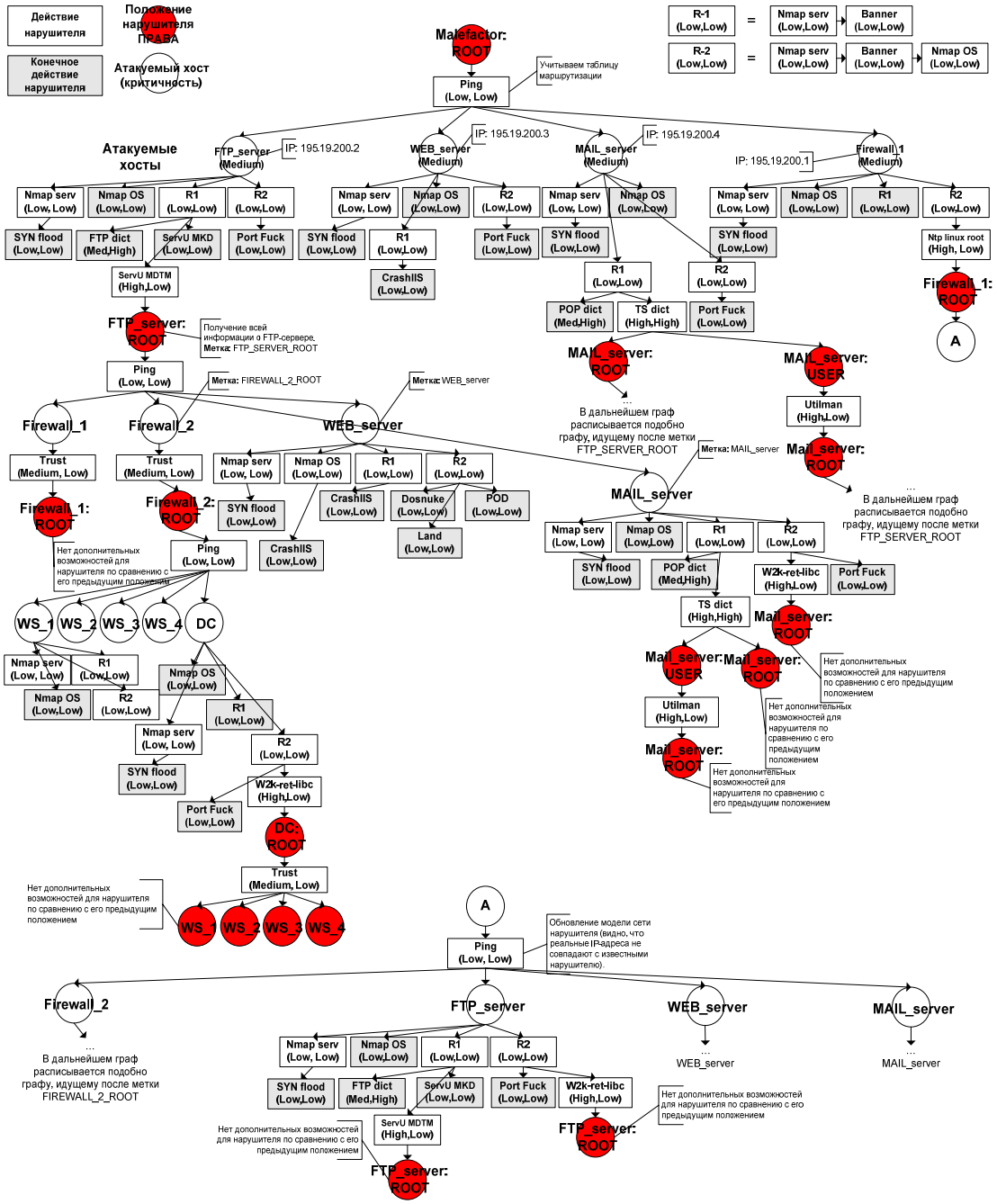

Рис. 4. Общий граф атак для примера 1.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Получив информацию о FTP_server'е, нарушитель обнаруживает, что реальный IP-адрес хоста (192.168.0.11) не совпадает с тем, который «знал» нарушитель (195.19.200.2). Следовательно, в анализируемой сети реализуется перенаправление портов, а значит, нарушитель попал в другую сеть. Этот факт является решающим фактором при решении вопроса об изменении положения нарушителя с текущего хоста (Malefactor) на захваченный (FTP_server). Изменив положение, нарушитель реализует действие «Ping Hosts» и обнаруживает в сети четыре хоста, которые последовательно анализируются по вышеприведенной схеме. Кроме того, учитываются отношения доверия, задаваемые политикой безопасности, которые позволяют сразу же получить права администратора для хостов Firewall_1 и Firewall_2. Дальнейшее построение общего графа атак производится аналогичным образом.

В результате проведенного анализа защищенности компьютерной сети были получены следующие данные: (1) общее количество хостов в сети: $N^H = 11$; (2) общее количество различных уязвимых хостов: $N_G^{VH} = 11$; (3) $N_G^{VH} / N^H = 1$; (4) слабые места в сети (по количеству проходящих через данные вершины трасс атак): Firewall_1, FTP_server, …; (5) критические уязвимости: NTP_LINUX_ROOT, Serv-U MDTM, …; (6) на графе существуют трассы, а следовательно и угрозы с $\text{Mortality}^{\max}(T) = High$ (например, трасса Malefactor-Ping-FTP_server(Nobody)-Nmap serv-Banner-ServU MDTM-FTP_server(Root)…) и с $\text{Realization}(T) = High$. Следовательно $SecurityLevel = Red$. Данный уровень защищенности компьютерной сети не удовлетворяет заданным пользователем требованиям (лучше, чем Orange) и требует немедленных действий по устранению обнаруженных уязвимостей программного обеспечения, слабых мест реализуемой политики безопасности.

Пример 2. Входными данными для примера 2 являются: (1) топология сети, сервисы, ОС и т.п. соответствуют описанию тестовой компьютерной сети, за исключением: (а) на хосте Firewall_1 уязвимый сервис ntp обновлен на последнюю версию, т.е. известных уязвимостей нет; (б) на хосте Ftp-server уязвимый сервис Serv-u обновлен на последнюю версию; (в) на хостах Ftp-server и Mail-server обновлена ОС; (г) на хосте Web-server обновлена ОС и IIS на последние версии; (д) правила перенаправления портов для хоста Firewall_1 приведены в табл. 6 (отличие с примером 1 заключается в отключении возможности внешним пользователям использовать сервис Microsoft Remote Desktop Connection); (2) Firewall_1 и Firewall_2 доверяют всем хостам из ДМЗ; (3) пользователи ftp-сервиса не имеют учетных записей на сервере; (4) нарушитель находится во внешней сети на хосте Malefactor и обладает на нем правами администратора; (5) политикой безопасности установлены правила, делающие невозможным подбор пароля к предоставляемым сетевым сервисам (ftp, pop3), т.е. установлены ограничения на количество неверных вводов пароля, после которых учетная запись блокируется; (6) для межсетевых экранов Firewall_1 и Firewall_2, серверов демилитаризованной зоны администратором установлен уровень критичности Medium; (7) в задании на анализ защищенности указано, что необходимо оценить все типы угроз (на нарушение целостности, доступности, конфиденциальности); (8) в задании на анализ защищенности указано, что необходимо провести анализ всех хостов ДМЗ и ЛВС.

На рис. 5 представлен общий граф атак, соответствующий вышеописанным входным данным.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В результате проведенного анализа защищенности компьютерной сети были получены следующие данные: (1) общее количество хостов в сети: $N^H = 11$; (2) общее количество различных уязвимых хостов: $N_G^{VH} = 4$; (3) $N_G^{VH} / N^H = 0.36$; (4) для всех трасс $\text{Severity}(S) = Low$. Тогда, для всех угроз $\text{Severity}(T) = Low$; (5) для всех угроз степень возможности их реализации $\text{Realization}(T) = High$; (6) следовательно $SecurityLevel = Yellow$. Данный уровень защищенности компьютерной сети не предполагает введение дополнительных средств защиты информации, а требует проведение мониторинга.

Таблица 6

Правила перенаправления портов для хоста Firewall_1

Комментарий	Destination (целевой хост)		Forward to… (перенаправить на…)	
	IP	Port	IP	Port
Web_server	195.19.200.3	80	192.168.0.12	80
FTP_server	195.19.200.2	21	192.168.0.11	21
MAIL_server POP3	195.19.200.4	110	192.168.0.10	110
MAIL_server SMTP	195.19.200.4	25	192.168.0.10	25

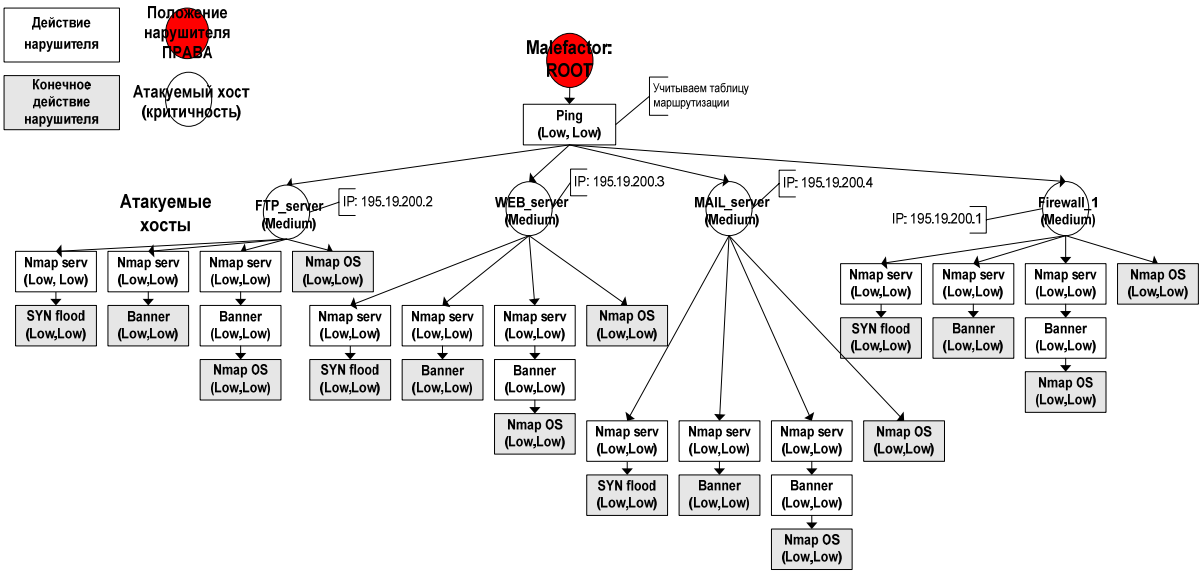

Рис. 5. Общий граф атак для примера 2.

7. Заключение

В работе предложен подход к анализу уязвимостей и оценке уровня защищенности компьютерных сетей, предназначенный для реализации на различных этапах жизненного цикла компьютерных сетей, основанный на генерации графов атак и вычислении различных метрик защищенности.

Предлагаемый подход обладает следующими *особенностями*: (1) использование для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях, в том числе моделей злоумышленника, моделей сценариев атак, формирования графа атак, расчета метрик защищенности и определения общего уровня защищенности; (2) учет разнообразия местоположения, целей и уровня знаний нарушителя; (3) использование при построении общего графа атак не только параметров конфигурации компьютер-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ной сети, но и правил реализуемой политики безопасности; (4) учет как собственно атакующих действий (по использованию уязвимостей), так и разрешенных действий пользователя и действий по разведке; (5) возможность исследования различных угроз безопасности для различных ресурсов сети; (6) возможность определения «узких мест» (хостов, ответственных за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации); (7) возможность задания запросов к системе вида «что если», например, какова будет защищенность при изменении определенного параметра конфигурации сети, правила политики безопасности; (8) применение для построения графа атак актуализированных баз данных об уязвимостях (например, OSVDB [24]); (9) использование для расчета части первичных метрик защищенности подхода CVSS [6]; (10) применение для вычисления метрик защищенности качественных методик анализа риска (в частности, модифицированной методики оценки серьезности сетевой атаки SANS/GIAC и методики FRAP [9]).

Направлениями дальнейших исследований является совершенствование моделей компьютерных атак и оценки уровня защищенности, в частности системы метрик защищенности и правил их вычисления, развитие программного прототипа САЗ и проведение дальнейшей экспериментальной оценки предложенных решений. Работа выполнена при финансовой поддержке РФФИ (проект №04-01-00167), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314).

Литература

1. *Alberts C., Dorofee A.* Managing Information Security Risks: The OCTAVE Approach. Addison Wesley Professional, 2002. 464 p.
2. *Chapman C., Ward S.* Project Risk Management: Processes, Techniques and Insights. Chichester, John Wiley, 2003. 408 p.
3. *Chi S.-D., Park J. S., Jung K.-C., Lee J.-S.* Network Security Modeling and Cyber Attack Simulation Methodology // Lecture Notes in Computer Science. New York: Springer-Verlag, 2001. Vol. 2119. P. 320–333.
4. *Chung M., Mukherjee B., Olsson R. A., Puketza N.* Simulating Concurrent Intrusions for Testing Intrusion Detection Systems // Proceeding of the 1995 National Information Systems Security Conference. Baltimore, Maryland, October 10–13, 1995. P. 173–183.
5. *Cohen F.* Simulating Cyber Attacks, Defenses, and Consequences [Электронный ресурс] // <http: // all.net / journal / ntb / simulate / simulate.html> (по сост. на 1.03.06).
6. CVSS. Common Vulnerability Scoring System [Электронный ресурс] // <http: // www.first.org / cvss> (по состоянию на 17.03.06).
7. *Dantu R., Loper K., Kolan P.* Risk Management using Behavior based Attack Graphs // International Conference on Information Technology: Coding and Computing, 2004. P. 445–449.
8. *Dawkins J., Campbell C., Hale J.* Modeling network attacks: Extending the attack tree paradigm // In Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.
9. FRAP. Facilitated Risk Analysis Process [Электронный ресурс] // <http: // www.peltierassociates.com> (по состоянию на 17.03.06).
10. *Gorodetski V., Kotenko I.* Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // Lecture Notes in Computer Science. New York: Springer-Verlag, 2002. Vol. 2516. P. 219–238.
11. *Hariri S., Qu G., Dharmagadda T., Ramkishore M., Raghavendra C. S.* Impact Analysis of Faults and Attacks in Large-Scale Networks [Электронный ресурс] // <http: // www.ece.arizona.edu / ~hpdc / projects / nvat / j5049.pdf> (по сост. на 17.03.06).
12. *Iglun K., Kemmerer R. A., Porras P. A.* State Transition Analysis: A Rule-Based Intrusion

Detection System // IEEE Transactions on Software Engineering. 1995. Vol. 21, no. 3. P. 181–199.
13. *Jha S., Linger R., Longstaff T., Wing J.* Survivability Analysis of Network Specifications [Электронный ресурс] // <http: // www.cs.cmu.edu / ~wing / publications / Jha-Longstaff00.pdf> (по состоянию на 17.03.06).
14. *Jha S., Sheyner O., Wing J.* Minimization and reliability analysis of attack graphs. Technical Report CMU-CS-02-109. Carnegie Mellon University, 2002.
15. *Kumar S., Spafford E. H.* An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR 94 013. Purdue University, 1994.
16. *Lye K., Wing J.* Game Strategies in Network Security // International Journal of Information Security, February, 2005. P. 71–86.
17. *McNab C.* Network Security Assessment. O'Reilly Media, Inc, 2004. 396 p.
18. *Noel S., Jacobs M., Kalapa P., Jajodia S.* Multiple coordinated views for network attack graphs // IEEE Workshop on Visualization for Computer Security, 2005. P. 99–106.
19. *Noel S., Jajodia S.* Managing attack graph complexity through visual hierarchical aggregation // ACM Workshop on Visualization and Data Mining for Computer Security, 2004. P. 109–118.
20. *Noel S., Jajodia S.* Understanding complex network attack graphs through clustered adjacency matrices // Proc. 21st Annual Computer Security Conference, 2005. P. 160–169.
21. Netfilter/iptables documentation [Электронный ресурс] // <http: // www.netfilter.org / documentation> (по состоянию на 17.03.06).
22. NVD: National Vulnerability Database [Электронный ресурс] // <http: // nvd.nist.gov> (по состоянию на 17.03.06).
23. NVD-Severity. National Vulnerability Database Severity Ranking [Электронный ресурс] // <http: // nvd.nist.gov / cvss.cfm> (по состоянию на 17.03.06).
24. OSVDB: The Open Source Vulnerability Database [Электронный ресурс] // <http: // www.osvdb.org> (по состоянию на 17.03.06).
25. *Ou X., Govindavajhala S., Appel A. W.* MulVAL: A Logic-based Network Security Analyzer // 14th Usenix Security Symposium, 2005. P. 113–128.
26. *Peltier T. R., Peltier J., Blackley J. A.* Managing a Network Vulnerability Assessment. Auerbach Publications, 2003. 312 p.
27. *Rieke R.* Tool based formal Modeling, Analysis and Visualization of Enterprise Network Vulnerabilities utilizing Attack Graph Exploration // Proceeding of EICAR 2004, 2004.
28. *Ritchey R. W., Ammann P.* Using model checking to analyze network vulnerabilities // Proceedings of IEEE Computer Society Symposium on Security and Privacy, 2000. P. 156–165.
29. *Rothmaier G., Krumm H.* A Framework Based Approach for Formal Modeling and Analysis of Multi-level Attacks in Computer Networks // Lecture Notes in Computer Science. New York: Springer-Verlag, 2005. Vol. 3731. P. 247–260.
30. *Sheyner O., Haines J., Jha S., Lippmann R., Wing J. M.* Automated generation and analysis of attack graphs // Proceeding of the IEEE Symposium on Security and Privacy. 2002. P. 273–284.
31. *Sheyner O.* Scenario Graphs and Attack Graphs. CMU Computer Science Department technical report CMU-CS-04-122. Ph.D. dissertation. 2004.
32. *Schneier B.* Attack Trees // Dr. Dobb's Journal. 1999. Vol. 12. P. 21–29.
33. *Shepard B., Matuszek C., Fraser C. B., etc.* A Knowledge-based approach to network security: applying Cyc in the domain of network risk assessment // The Seventeenth Innovative Applications of Artificial Intelligence Conference (IAAI-05), 2005. P. 1563–1568.
34. *Singh S., Lyons J., Nicol D. M.* Fast Model-based Penetration Testing // Proceedings of the 2004 Winter Simulation Conference, 2004. P. 309–317.
35. *Swarup V., Jajodia S., Pamula J.* Rule-based topological vulnerability analysis // Lecture Notes in Computer Science. New York: Springer-Verlag, 2005. Vol. 3685. P. 23–37.
36. *Swiler L., Phillips C., Ellis D., Chakerian S.* Computer-attack graph generation tool // In proceedings DISCEX'01 : DARPA Information Survivability Conference & Exposition II. 2001. P. 307–321.
37. *Wing J. M.* Scenario Graphs Applied to Security [Электронный ресурс] // <http: // www.cs.cmu.edu / ~wing / publications / Wing05.pdf> (по состоянию на 17.03.2006).
38. *Yuill J., Wu F., Settle J., Gong F.* Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks. 2000. No. 34. P. 671–697.