Метрики безопасности

для оценки уровня защищенности компьютерных сетей на основе построения графов атак

И. В. Котенко, *д. т. н., профессор, руководитель научно-исследовательской группы компьютерной безопасности*
ivkote@comsec.spb.ru
М. В. Степашкин, *научный сотрудник*
stepashkin@comsec.spb.ru
СПИИРАН

Один из подходов к вычислению метрик безопасности и определению общего уровня защищенности компьютерных сетей может основываться на тщательном анализе возможных действий злоумышленников, направленных на реализацию различных угроз нарушения безопасности, и построении графов этих действий. В статье развивается подход к анализу защищенности компьютерных сетей на основе построения общих графов атак, и предлагается соответствующая система метрик безопасности. Общий граф атак описывает всевозможные варианты реализации нарушителем атакующих действий. Предполагается, что такие графы строятся на основе моделирования действий нарушителя с учетом параметров конфигурации компьютерной сети и правил реализуемой политики безопасности, а также целей, уровня знаний и разнообразия местоположения нарушителя, что позволяет исследовать действия как внешнего, так и внутреннего злоумышленника. В статье описывается методика анализа защищенности компьютерных сетей, базирующаяся на предложенной системе метрик безопасности. Представляется разработанная система анализа защищенности, реализующая предложенный подход, и на тестовом примере демонстрируется ее работа.

Введение

Нарушение информационной безопасности компьютерных сетей может быть вызвано множеством различных причин: наличием уязвимостей в операционных системах и приложениях, реализацией неправильной политики безопасности, неверной конфигурацией аппаратного и программного обеспечения, ошибками, допущенными при настройке механизмов защиты, и т. д. Таким образом, при проектировании и эксплуатации компьютерных сетей перед проектировщиком и (или) администратором сети (безопасности) возникает следующая задача: проверить, обеспечивают ли заданная политика безопасности, планируемые для применения или уже используемые параметры конфигурации сети и механизмы защиты необходимый уровень защищенности, характеризующийся заданной системой метрик безопасности.

Кроме того, на этапе эксплуатации компьютерных сетей довольно часто происходят изменения в их конфигурации и составе используемого программного и аппаратного обеспечения, поэтому необходимо постоянно производить мониторинг сети, анализ имеющихся уязвимостей и оценку уровня защищенности.

Данная работа посвящена *развитию подхода к анализу защищенности компьютерных сетей на основе построения общих графов атак и разработке системы метрик безопасности, используемой для оценки уровня защищенности компьютерных сетей на различных этапах их жизненного цикла, включая этап проектирования и эксплуатации.*

Методика анализа защищенности компьютерных сетей, использующая предлагаемую систему метрик безопасности, подразумевает реализацию комплекса следующих действий:

- построения графов возможных атакующих действий, выполняемых из различных точек сети и направленных на реализацию различных угроз безопасности с учетом квалификации нарушителя;
- определения уязвимостей и «узких мест» в защите (наиболее критич-

ных компонентов компьютерной сети);
- вычисления метрик безопасности и определения общего уровня защищенности;
- сопоставления полученных метрик с требованиями и выработки рекомендаций по усилению защищенности.

На основе предложенных в работе моделей, методик и системы метрик безопасности разработана система анализа защищенности (САЗ). *Основной целью разработки САЗ* было создание исследовательского инструментария для экспресс-анализа защищенности сложных компьютерных сетей с учетом не только их конфигурации (топологии, используемого программного и аппаратного обеспечения, используемых средств защиты), но и реализуемой в них политики безопасности.

Релевантные работы

В настоящий момент существует множество работ, посвященных разработке систем анализа защищенности и метрик безопасности. Источниками информации о метриках могут быть государственные научно-исследовательские организации, академические институты, индустриальные стандарты и существующие программные средства. Представим кратко лишь некоторые из них.

Для оценки возможностей систем, направленных на обеспечение информационной безопасности, должны, прежде всего, использоваться международные и национальные стандарты оценки и управления информационной безопасностью ISO 17799 (BS7799), ISO 15408 и др., стандарты аудита информационных систем и информационной безопасности CIBIT, SAC, COSO и т. п. В частности, в соответствии с международным стандартом «Общие критерии оценки безопасности информационных технологий» (ISO 15408) оценка безопасности базируется на моделях системы безопасности, состоящих из перечисленных в стандарте функций. В ISO 15408 содержится ряд предопределенных моделей (так называемых профилей), описывающих стандартные модули системы безопасности. С их помощью можно не создавать модели распространенных средств защиты самостоятельно, а пользоваться уже готовыми наборами описаний, целей, функций и требований к этим средствам. Простым примером профилей может служить модель межсетевого экрана или СУБД.

В [1–3] излагаются возможные методики анализа рисков для оценки степени защищенности компьютерных систем. В [4] показана взаимосвязь задач анализа защищенности и обнаружения вторжений с задачей управления рисками, даны обзоры основных стандартов в области защиты информации и управления рисками, инструментальных средств для анализа рисков. Работа [5] посвящена процессу анализа защищенности корпоративных автоматизированных систем. В ней приведен обзор средств анализа защищенности (сетевых сканеров, средств контроля защищенности системного уровня, анализа параметров защиты), рассмотрена типовая методика анализа защищенности, эффективность которой подтверждена практикой. В [6] раскрываются современные концепции управления рисками, их реализация на практике, инструментальные средства управления рисками.

В [7] проведен анализ вопросов, стоящих перед исследователями в области метрик безопасности. Автор утверждает, что существует необходимость в разработке интегрированной среды для формирования метрик, определяя их цель, значение, единицы измерения, диапазон принимаемых значений и формируя таксономии. В [8] предложен подход, основанный на понятии сложности по Колмогорову, которая определяет исправность системы обеспечения безопасности. Так как сложность является фундаментальной характеристикой информации, то данный подход может быть применен без знания детальной спецификации анализируемой системы. Работы [9, 10] посвящены разработке руководства по метрикам безопасности информационных систем. Данное руководство может быть использовано организациями для оценки адекватности используемых методов и средств защиты информации. Авторами предлагается подход для разработки собственных метрик безопасности. Представлены примеры метрик и их таксономия. В [11] рассмотрена таксономия метрик безопасности, которая может быть использована исследователями для разработки собственных метрик. Предложенная таксономия основана на представлении авторов о разделении метрик безопасности на следующие классы: (1) объективные/субъективные; (2) качественные/количественные; (3) статические/динамические; (4) абсолютные/относительные; (5) прямые/косвенные. Авторы выделяют две основные группы метрик: организационные и помогающие оценить возможности продукта или системы в области обеспечения безопасности. Первая группа содержит, допустим, метрики, связанные с персоналом, задействованным в обеспечении безопасности. Вторая – включает, например, метрики, связанные с количеством технических объектов и систем (аппаратных или программных), способных выполнять функции по защите информации.

В научных исследованиях используются различные способы представления сценариев атак и построения графов (деревьев) атак для анализа защищенности: деревья атак [12], формальные грамматики [13], раскрашенные сети Петри [14], метод анализа изменения состояний [15], причинно-следственная модель атак [16], описательные модели сети и злоумышленников [17], структурированное описание на базе деревьев [18], использование и создание графов атак для анализа уязвимостей [19], объектно-ориентированное дискретное событийное моделирование [20], модели, основанные на знаниях [21] и т. д. В [22, 23] 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 спе-

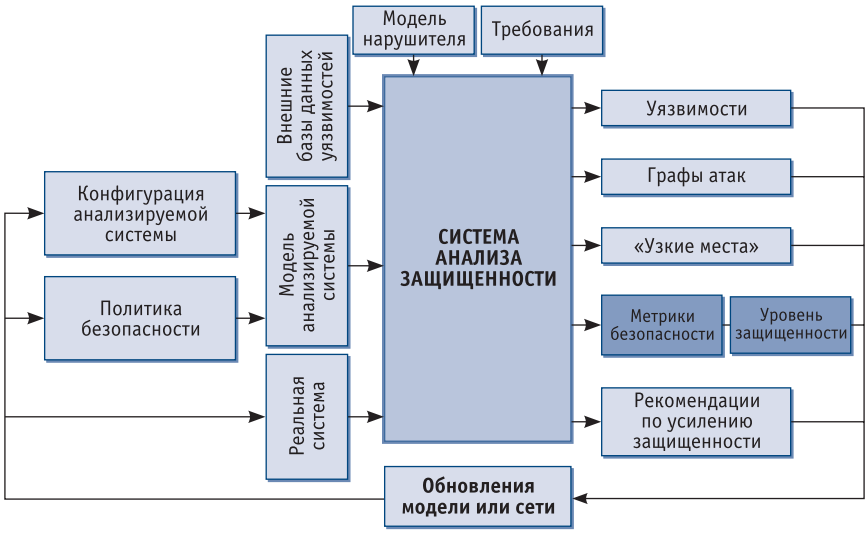

Рис. 1. ***Обобщенное представление входных и выходных данных для системы анализа защищенности***

цификацию сети и отображение полученных результатов на сценарных графах. В работе [24] 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.

Сущность предлагаемого подхода

Основное отличие предлагаемого в данной работе подхода 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 (САЗ), использующая предложенный подход, предназначена для функционирования на различных этапах жизненного цикла компьютерной сети, включая этапы проектирования и эксплуатации. Обобщенное представление входных и выходных данных для данной системы приведено на рис. 1. 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) и 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.

Предлагаемый в данной работе подход к анализу защищенности компьютерных сетей базируется, в том числе, на указанных выше работах, но обладает следующими *особенностями*:

- использованием для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях, в том числе моделей нарушителя, сценариев атак, формирования графа атак, расчета метрик безопасности и определения общего уровня защищенности;
- учетом разнообразия местоположения, целей и уровня знаний нарушителя;
- использованием при построении общего графа атак не только параметров конфигурации компьютерной сети, но и правил реализуемой политики безопасности;
- учетом как собственно атакующих действий (по использованию уязвимостей), так и разрешенных действий пользователя, имеющего определенные полномочия, и действий по сетевой разведке;
- возможностью исследования различных угроз безопасности для различных ресурсов сети;
- возможностью определения «узких мест» (хостов, ответственных за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации);
- возможностью задания запросов к системе вида «что если» (например, как повлияет на защищенность изменение определенного параметра конфигурации сети, правила политики безопасности);
- применением для построения графа атак актуализированных баз данных об уязвимостях (например, OSVDB [25]);
- использованием для расчета части первичных метрик подхода CVSS [26];
- применением для вычисления метрик безопасности качественных методик анализа риска (в частности, модифицированной методики оценки серьезности сетевой атаки SANS/GIAC и методики FRAP [27]).

Общий граф атак и его формирование

Определение предлагаемых в данной работе метрик безопасности основано на использовании общего графа атак, который описывает всевозможные варианты реализации нарушителем атакующих действий с учетом его первоначального местоположения, уровня знаний и умений, первоначальной конфигура-

ции компьютерной сети и реализуемой в ней политики безопасности. На основе общего графа атак производится анализ защищенности компьютерной сети, определение «узких мест», формируются рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности.

Все *объекты графа атак* можно подразделить на базовые 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 базовых объектов с помощью дуг. К *базовым 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:

- разведывательные действия (то есть направленные на получение информации о сети (хосте);
- подготовительные действия (в рамках уже имеющихся у нарушителя полномочий), служащие для создания условий реализации атакующих действий последующих классов;
- действия, направленные на нарушение конфиденциальности;
- действия, направленные на нарушение целостности;
- действия, направленные на нарушение доступности;
- действия, приводящие к получению нарушителем прав локального пользователя;
- действия, приводящие к получению нарушителем прав администратора.

Все атакующие действия можно разделить также на две группы:

- 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);
- 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.

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. *Граф* объединяет все возможные трассы атак.

Разделение атакующих действий по заданным выше классам позволяет *классифицировать угрозы* следующим образом:

- *основные угрозы* – угрозы нарушения конфиденциальности, целостности и доступности;
- *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. Например, он может реализовать эти угрозы для некоторой совокупности объектов хоста, имея только права пользователя. При успешном получении прав администратора на хосте злоумышленник 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 моделировании действий нарушителя и осуществления следующей последовательности его действий:

- реализация действий по перемещению нарушителя с одного хоста на другой;
- реализация разведывательных действий по определению живых хостов;
- реализация сценариев (множества действий) разведки для каждого обнаруженного хоста;
- реализация атакующих действий, использующих уязвимости программного и аппаратного обеспечения, а также общих действий пользователя.

Метрики безопасности

На основе сформированного общего графа атак можно построить множество различных метрик безопасности и произвести оценку общего уровня защищенности компьютерной сети. Метрики могут характеризовать защищенность как базовых, так и составных объектов графа атак, включая и защищенность всей компьютерной сети.

Проведем классификацию используемых метрик безопасности по трем признакам:

- по разделению объектов общего графа атак на базовые и составные;
- в соответствии с порядком вычислений;
- в соответствии с тем, используются ли метрики для определения общего уровня защищенности анализируемой компьютерной сети.

В соответствии *с разделением объектов общего графа атак на базовые*

и составные множество всех метрик можно подразделить на следующие группы:

- формируемые по элементарным объектам (хосты и атакующие действия);
- формируемые по составным объектам (трассы атак, угрозы и общий граф атак).

В соответствии *с порядком вычислений* все метрики можно разделить на две группы: первичные и вторичные. Первичные метрики получаются непосредственно из общего графа атак, вторичные – рассчитываются с использованием первичных. Для расчета вторичных метрик безопасности множество метрик, вычисляемых на основе общего графа атак, необходимо дополнить метриками, определяемыми по заданной конфигурации анализируемой компьютерной сети.

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

В качестве *основных* определим следующие метрики:

- критичность хоста h (*Criticality*(h));
- уровень критичности атакующего действия a (*Severity*(a));
- размер ущерба, вызванного реализацией атакующего действия a с учетом уровня критичности атакуемого хоста h (*Mortality*(a,h));
- размер ущерба при реализации трассы S и угрозы T (*Mortality* (S) и *Mortality* (T));
- «сложность доступа» для атакующего действия a, трассы S и угрозы T (*AccessComplexity*(a), *AccessComplexity*(S), *AccessComplexity*(T));
- степень возможности реализации угрозы T (*Realization*(T));
- уровень риска угрозы T (*RiskLevel*);
- уровень защищенности компьютерной сети (*SecurityLevel*).

На данный момент исследований определено более 150 метрик безопасности различного уровня общности. В табл. 1 представлены некоторые примеры используемых метрик, основные из которых выделены серым цветом.

Некоторые основные метрики безопасности (например, *Severity*(a)) и значительная часть вспомогательных метрик рассчитываются на базе подхода *Common Vulnerability Scoring System* (*CVSS*) [26].

Индексы CVSS разделены на три основные группы: базовые, временные и 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 атакующего действия SYN flood могут быть получены из базы NVD [28].

Методика экспресс-оценки общего уровня защищенности

Предлагаемая методика экспресс-оценки общего уровня защищенности компьютерной сети базируется на использовании оценки серьезности (критичности) атакующего действия, рассчитываемой на основе обобщенного уровня критичности атакующего действия CVSS, и применении некоторых процедур методики анализа рисков FRAP (Facilitated Risk Analysis Process) [27]. Данная методика не претендует на охват всех возможных аспектов, влияющих на защищенность компьютерной сети, не позволяет оценивать стоимостные показатели решений по безопасности, но учитывает основные аспекты, влияющие на возможность компрометации сети со стороны злоумышленников. В настоящее время ведутся исследования по расширению возможностей данной методики.

Разработанная методика оценки защищенности включает следующие этапы:

- вычисление метрик безопасности базовых и составных объектов общего графа атак (*Criticality*, *Severity*, *AccessComplexity*, *Realization*);
- получение качественных оценок уровня риска для всех угроз (*RiskLevel*);
- 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 критичности атакуемого хоста и общего уровня критичности атакующего действия. Данную величину обозначим *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. 2.

Максимальный уровень критичности установлен для хостов, неверное функционирование (или полное прекращение функционирования) которых приводит к невозможности использования ресурсов сети. Далее в сторону уменьшения уровня критичности идут рабочие серверы, функционирование которых (каждого по отдельности) является очень важной составляющей успешной работы организации. Минимальным уровнем критичности обладают персональные рабочие станции, нарушения в работе которых весьма незначительно влияют на процессы функционирования организации в целом.

Критичность атакующего действия рассчитывается с использованием обобщенной оценки кри-

Табл. 1. ***Примеры метрик безопасности***

Обозначение (формула)	Описание
Метрики, определяемые непосредственно на основе конфигурации сети	
N^H, N^{FH}, N^{LH}, N^{WH}, N^{HA}, N^{HF}, N^{HIDS}	Количество хостов (*H*), межсетевых экранов (*FH*), хостов под управлением ОС семейства Linux (*LH*), Microsoft Windows (*WH*), хостов, на которых используются антивирусные программные средства (*HA*), персональные средства фильтрации сетевого трафика (*HF*), хостовые системы обнаружения вторжений (*HIDS*)
Метрики хостов	
Criticality(*h*)	Критичность хоста *h*
Метрики атакующих действий	
Severity(*a*)	Уровень критичности атакующего действия *a*
Mortality(*a*)	Размер ущерба, вызванного реализацией атакующего действия *a* с учетом уровня критичности хоста *h*
AccessComplexity(*a*)	«Сложность доступа» атакующего действия *a* (индекс CVSS [26])
V^{VI}, V^{VI_C}, V^{VI_I}, V^{VI_A}, V^{VAC}	Индексы CVSS «Базовая оценка» (BaseScore), «Воздействие на конфиденциальность» (Confidentiality Impact (*C*)), «Воздействие на целостность» (Integrity Impact (*I*)), «Воздействие на доступность» (Availability Impact (*A*)), «Сложность в доступе» (Access Complexity) (*AC*) атакующего действия [26]
Метрики трасс атак	
N_R^{VH}, $N_R^{VH_U}$, $N_R^{VH_R}$	Количество различных уязвимых хостов в трассе (длина трассы, выражаемая в количестве уязвимых хостов), количество хостов, на которых нарушителем получены права локального пользователя (*U*) и администратора (*R*)
N_R^V	Количество различных атакующих действий в трассе (длина трассы, выражаемая в количестве атакующих действий)
V_R^{diff}	Множество различных атакующих действий в трассе
$V_R^{V_{AC}} = max_{V_R^{diff}}\{V^{V_{AC}}\}$	Наивысшая сложность в доступе, требуемой для реализации всех атакующих действий трассы
Mortality(*S*), $Mortality^{max}(S)$	Размер ущерба и максимальный размер ущерба при реализации трассы *S*
AccessComplexity(*S*)	Индекс «сложность доступа» трассы
Метрики угроз безопасности	
$N_T^{VHmin} = min\{N_{R_i}^{VH}\}$, $R_i \in T$	Минимальное количество различных уязвимых хостов, используемых при реализации угрозы *T*
N_T^R	Количество различных трасс, приводящих к реализации угрозы *T*
Mortality(*T*), $Mortality^{max}(T)$	Размер и максимальный размер ущерба при реализации угрозы *T*
AccessComplexity(*T*)	Индекс «сложность доступа» угрозы *T*
Realization(*T*)	Степень возможности реализации угрозы *T*
RiskLevel(*T*)	Уровень риска угрозы *T*
Метрики общего графа атак	
1) По хостам	
N_G^{VH}, $N_G^{VH_U}$, $N_G^{VH_R}$	Количество различных уязвимых хостов на графе, количество хостов, на которых нарушителем получены права локального пользователя (*U*) и администратора (*R*)
2) По атакующим действиям	
N_G^V, V_G^{diff}	Количество и множество различных атакующих действий на графе
$V_G^{VI} = \sum_{V_G^{diff}} V^{VI} / N_G^V$	Средняя базовая оценка по всем различным атакующим действиям графа
3) По трассам	
N_G^R, $N_G^{R^C}$, $N_G^{R^I}$, $N_G^{R^A}$	Общее количество трасс атак на графе, количество трасс, приводящих к нарушению конфиденциальности (*C*), целостности (*I*) и доступности (*A*)
4) По угрозам	
N_G^T, $N_G^{T^C}$, $N_G^{T^I}$, $N_G^{T^A}$	Общее количество угроз на графе, количество угроз, приводящих к нарушению конфиденциальности (*C*), целостности (*I*) и доступности (*A*)
5) Комбинированные (интегральные)	
A_G^{RH}	Массив количества трасс, проходящих через каждый хост общего графа атак
SecurityLevel	Интегральная метрика «Уровень защищенности анализируемой компьютерной сети». Является основной результирующей метрикой

тичности атакующего действия ($BaseScore(a)$) CVSS следующим образом [29]:

$$Severity(a) = \begin{cases} Low, BaseScore(a) \in [0.0, 3.9] \\ Medium, BaseScore(a) \in [4.0, 6.9] \\ High, BaseScore(a) \in [7.0, 10.9] \end{cases}.$$

Размер ущерба, вызванного успешной реализацией атакующего действия с учетом уровня критичности атакуемого хоста, рассчитывается согласно табл. 3.

Размер ущерба для хоста h с учетом его критичности, вызванного успешной реализацией угрозы, определяется ее последним атакующим действием в одной из трасс реализации угрозы:

$$Mortality(T) = Mortality(a_T, h_T),$$

где a_T – последнее атакующее действие в угрозе, h_T – хост, на который направлено действие a_T. Размер ущерба $Mortality(T)$ 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 ущерб компьютерной сети, нанесенный нарушителем во время реализации угрозы, гораздо больше рассчитанного по последнему атакующему действию. Для учета данной ситуации необходимо ввести метрики максимального размера ущерба при реализации трассы S и угрозы T, рассчитываемые по следующим формулам:

$$Mortality^{max}(S) = max_i(Mortality(a_i, h_i)),$$
$$i \in [1, N_S],\ a_i \in S,$$
$$Mortality^{max}(T) = max_i(Mortality(S_i)),$$
$$i \in [1, N_T],\ S_i \in T,$$

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 ($Realization(T)$) и воспользоваться методикой FRAP [27] с использованием полученного ранее размера ущерба при реализации угрозы ($Mortality(T)$).

Для определения степени возможности реализации угрозы T воспользуемся индексом CVSS «сложность доступа» из множества базовых индексов CVSS, задаваемых для каждого атакующего действия в графе атак. Возможными значениями данного индекса являются:

- High – существуют условия доступа, например, специфические временные рамки, специфические обстоятельства (специфическая конфигурация сервиса), взаимодействие с атакуемым человеком);
- Low – нет специфических условий доступа, то есть использование уязвимости возможно всегда.

Тогда индекс «*сложность доступа*» *для трассы атак S* будет вычисляться по следующей формуле:

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

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:

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

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:

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

Уровень риска угрозы оценивается в соответствии с табл. 4.

Полученная оценка уровня риска может интерпретироваться следующим образом:

- уровень A – действия, связанные с риском (например, внедрение новых средств защиты информации или устранение уязвимостей), должны быть выполнены немедленно и в обязательном порядке;
- уровень B – действия, связанные с риском, должны быть предприняты;
- уровень C – требуется мониторинг ситуации, непосредственных мер по противодействию угрозе принимать, возможно, не надо;
- уровень D – никаких действий в данный момент предпринимать не требуется.

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

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

где $D < C < B < A$; N_T – количество всех угроз. Предполагается использование четырех уровней защищенности системы, их можно упорядочить по возрастанию уровня защищенности следующим образом: красный (Red), оранжевый (Orange), желтый (Yellow) и зеленый (Green).

Система анализа защищенности

Предложенный поход по построению общего графа атак, определению семейства различных метрик и вычислению общего уровня защищенности был реализован в разработанной системе анализа защищенности (САЗ). Структура этой системы представлена на рис. 2.

На этапе проектирования САЗ оперирует с моделью анализируемой компьютерной сети (системы), которая базируется на заданных спецификациях последней и политики безопасности, которые описываются с использованием специализированных языков, основанных на XML. На этапе эксплуатации для построения модели анализируемой сети используется подсистема сбора информации об анализируемой компьютерной сети.

Кратко рассмотрим функции основных модулей. *NetworkModel Initialization* преобразует информацию о конфигурации сети и реализуемой в ней политике безопасности, задаваемых пользователем во внутреннее представление. *DataControl* используется для обнаружения некорректно заданных данных или отсутствия необходимых сведений для процесса анализа защищенности данных. Например, пользователь может ввести ошибочное имя сервиса или указать, что порт 21 открыт, но не определить, какое приложение обрабатывает поступающие на данный порт запросы. *GraphBuilder* строит общий граф атак, эмулируя действия нарушителя в анализируемой компьютерной сети. Для этого используется информация о доступных атакующих действиях различных типов, о конфигурации сети и реализуемой в ней политике безопасности. Данный модуль расставляет в вершинах графа метрики защищенности базовых объектов, на основе которых *GraphAnalyzer* рассчитывает метрики составных объектов. *Хранилище данных* состоит из групп баз данных (БД) и баз знаний (БЗ), определяющих конфигурацию анализируемой компьютерной сети и политику безопасности (*NetworkModel*), а также атакующие действия (*Attacks*). *Network Interface* преобразует XML-спецификации уязвимостей из OSVDB [25] во внутренний формат. *InformCollector* служит для сбора информации, поступающей от хостовых агентов и ее передачи компонентам САЗ.

Главное окно графического интерфейса САЗ (рис. 3) разделено на четыре части:

- меню, предназначенное для управления работой прототипа;
- верхняя область рабочей части окна с закладками Analyzed Network Model – представление модели анализируемой компьютерной сети, Malefactor's Network Model – представление модели анализируемой компьютерной сети так, как ее представляет себе нарушитель на данном этапе формирования общего графа атак, General Attack Graph – представление общего графа атак;
- нижняя область рабочей части окна с закладками: Log – журнал работы, Vulnerabilities – список уязвимых хостов и обнаруженных уязвимостей, Metrics – метрики безопасности, Requirements – перечень заданных пользователем требований, Reports – отчеты (рекомендации по повышению уровня защищенности, действия по устранению обнаруженных уязвимостей и т. п.);
- область кнопок управления.

Табл. 2. ***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

Табл. 3. ***Определение размера ущерба при реализации атакующего действия***

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

Табл. 4. ***Матрица оценки уровня риска угрозы***

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

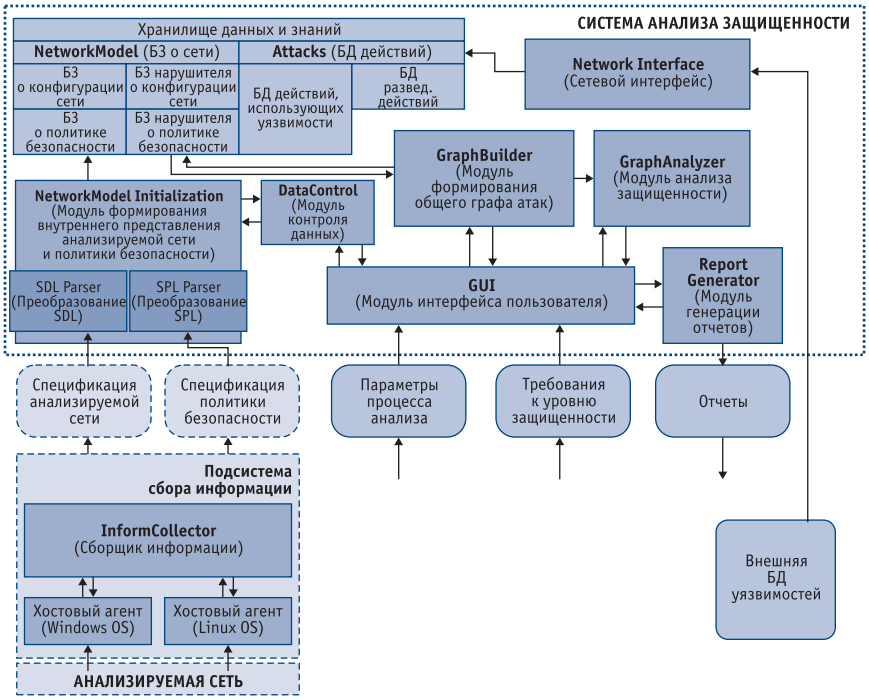

Рис. 2. ***Структура системы анализа защищенности***

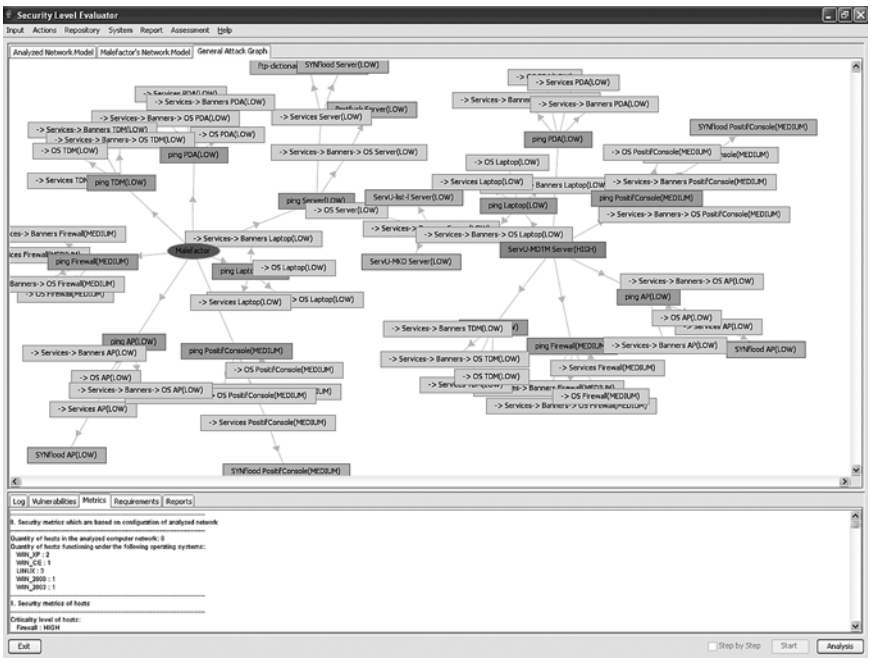

Рис. 3. ***Графический интерфейс пользователя системы анализа защищенности***

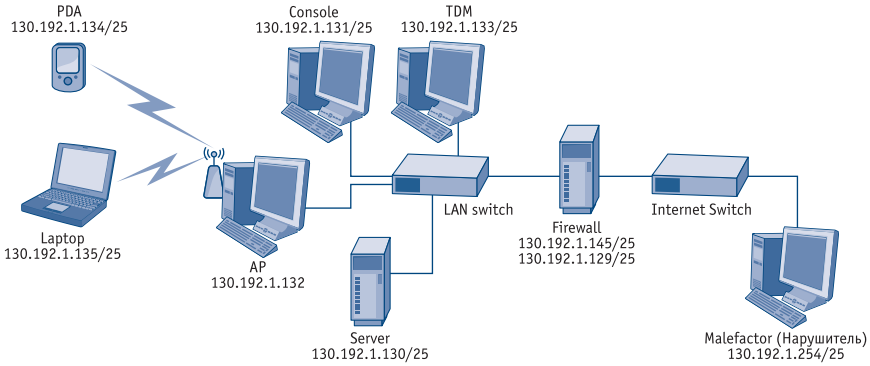

Рис. 4. ***Структура тестовой компьютерной сети***

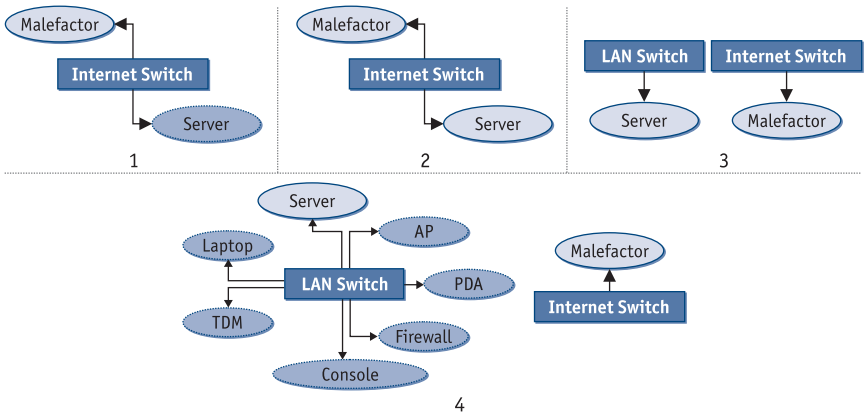

Рис. 5. ***Изменение представлений нарушителя об атакуемой компьютерной сети***

Перейдем к рассмотрению работы системы анализа защищенности на тестовой компьютерной сети, структура которой представлена на рис. 4.

Во время построения общего графа атак происходят следующие основные изменения в представлении нарушителя об атакуемой сети (рис. 5):

- после реализации атаки ping (с учетом таблицы маршрутизации трафика) нарушитель узнает о существовании хоста Server;
- нарушитель реализует атаку, использующую уязвимость в ftp-сервисе и позволяющую получить права локального администратора;
- нарушитель использует полученные права на хосте Server для сбора всей доступной информации, анализируя которую злоумышленник понимает, что используется перенаправление портов (port forwarding) и хост Server подключен к другому сетевому концентратору (следовательно, нарушителю выгодно «перейти» на хост Server, поскольку такой переход открывает ему доступ в другой сегмент сети);
- перейдя на Server, нарушитель реализует атаку ping и узнает о существовании множества других хостов, которые он последовательно пытается атаковать.

Общий граф атак для тестовой компьютерной сети представлен на рис. 6.

Основными результатами процесса анализа защищенности являются:

- множество обнаруженных уязвимостей (например, уязвимость ServU-MDTM на рис. 6);
- множество метрик безопасности (например, количество трасс атак, проходящих через хост Server);
- отчет о состоянии основных аспектов безопасности и рекомендации по повышению уровня защищенности.

В результате анализа защищенности для тестовой компьютерной сети был получен красный уровень защищенности. Дальнейшими действиями пользователя должны стать устранение обнаруженных уязвимостей и «узких мест» (обновление конфигурации сети и реализуемой политики защищенности) и повторный анализ защищенности сети, заданной обновленными спецификациями.

Заключение

В работе рассмотрен подход к анализу защищенности компьютерных сетей на основе построения общих графов атак. В соответствии с данным подходом расчет метрик безопасности производится на основе общего графа атак, описываю-

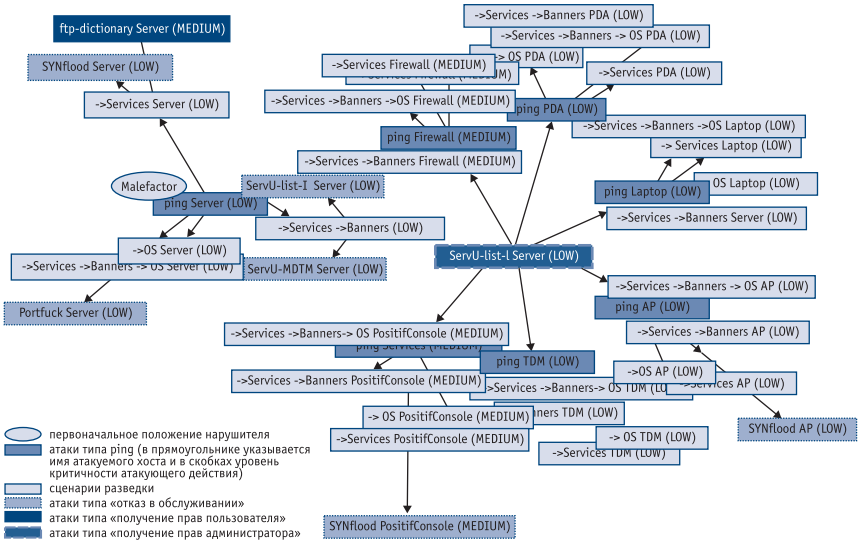

Рис. 6. ***Общий граф атак для тестовой компьютерной сети***

щего всевозможные варианты реализации атакующих действий нарушителя.

Методика оценки уровня защищенности компьютерных сетей, использующая предложенную в данной работе систему метрик безопасности, позволяет определить трассы (графы) возможных многошаговых атак, «узкие места» в компьютерной сети, на которых основываются эти атаки. Полученные результаты могут обеспечить выработку обоснованных рекомендаций по устранению выявленных уязвимостей и «слабых мест» и усилению защищенности анализируемой системы.

Предложенные в работе модели и методики (в частности, модель формирования графа атак, расчета метрик безопасности, методика экспресс оценки общего уровня защищенности компьютерных сетей) реализованы в разработанной системе анализа защищенности. Проведены эксперименты на тестовой компьютерной сети.

Направлениями дальнейших исследований являются совершенствование предложенной системы метрик безопасности и правил их вычисления, развитие функциональности системы анализа защищенности и проведение дальнейшей экспериментальной оценки предложенных решений.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 04-01-00167), программы фундаментальных исследований ОИТВС Российской Академии наук (контракт № 3.2/03) и проекта Евросоюза POSITIF (контракт IST-2002-002314). ■

ЛИТЕРАТУРА

1. Alberts C., Dorofee A. Managing Information Security Risks: The OCTAVE Approach. Addison Wesley Professional, 2002.

2. Chapman C., Ward S. Project Risk Management: Processes, Techniques and Insights. Chichester, John Wiley, 2003.

3. Peltier T. R., Peltier J., Blackley J. A. Managing a Network Vulnerability Assessment. Auerbach Publications, 2003.

4. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2004.

5. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info, № 7, 2002.

6. Симонов С. В. Технологии и инструментарий для управления рисками // JetInfo, № 2, 2003.

7. Skroch M., McHugh J., Williams JM. Information Assurance Metrics: Prophecy, Process or Pipedream // Panel Workshop. National Information Systems Security Conference (NISSC-2000). 2000.

8. Evans S., Bush S., Hershey J. Information Assurance through Kolmogorov Complexity // DARPA Information Survivability Conference and Exposition (DISCEX-H-2001). 2001.

9. Swanson M. Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication, № 800-26, 2001.

10. Swanson M., Nadya B., Sabato J., Hash J., Graffo L. Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication, № 800-55, 2003.

11. Vaughn R., Henning R., Siraj A. Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy // Proceedings of 36th Hawaii International Conference on System Sciences (HICSS-03), 2003.

12. Schneier B. Attack Trees // Dr. Dobb's Journal, Vol. 12, 1999.

13. Gorodetski V., Kotenko I. Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // Lecture Notes in Computer Science. Springer Verlag, Vol. 2516, 2002.

14. Kumar S., Spafford E. H. An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR 94 013. Purdue University, 1994.

15. 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. 1995.

16. Cohen F. Simulating Cyber Attacks, Defenses, and Consequences // IEEE Symposium on Security and Privacy, Berkeley, CA, 1999.

17. Yuill J., Wu F., Settle J., Gong F. Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks, No. 34, 2000.

18. Dawkins J., Campbell C., Hale J. Modeling network attacks: Extending the attack tree // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.

19. Iglun K., Kemmerer R. A., Porras P. A. State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, Vol. 21, No. 3. 1995.

20. 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. Springer Verlag, Vol. 2119, 2001.

21. 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.

22. Jha S., Linger R., Longstaff T., Wing J. Survivability Analysis of Network Specifications // International Conference on Dependable Systems and Networks, IEEE CS Press, 2000.

23. Jha S., Sheyner O., Wing J. Minimization and reliability analysis of attack graphs. Technical Report CMU-CS-02-109. Carnegie Mellon University, 2002.

24. Lye K., Wing J. Game Strategies in Network Security // International Journal of Information Security, February, 2005.