УДК 004.056.53

А.А. Чечулин

МЕТОДИКА ОПЕРАТИВНОГО ПОСТРОЕНИЯ, МОДИФИКАЦИИ И АНАЛИЗА ДЕРЕВЬЕВ АТАК

Чечулин А.А. **Методика оперативного построения, модификации и анализа деревьев атак.**

Аннотация. Применение методик моделирования сетевых атак является перспективным направлением в области защиты информации. В статье рассматривается подход к аналитическому моделированию сетевых атак на основе деревьев атак. Новизна предлагаемой методики заключается в возможности ее применения в системах, работающих в режиме близком к реальному времени. В статье рассмотрены основные модели предметной области и элементы алгоритмов формирования и модификации деревьев атак.

Ключевые слова: деревья атак: анализ защищенности: модель компьютерной сети: нарушителя и атакующих действий.

Chechulin A.A. **Technique of rapid construction, modification and analysis of attack trees.**

Abstract. Application of modeling techniques of network attacks is a promising task in information security. This paper describes an approach to analytical modeling of network-based attacks trees. The novelty of the proposed method lays in the possibility of its application for systems operating in near real time mode. The paper describes the main domain models and algorithms of attack trees construction and modification.

Keywords: attack trees, security evaluation, models of networks, malefactors and attack actions.

1. Введение. Обеспечение безопасности информации компьютерных сетей в настоящее время является одной из приоритетных задач, решаемых органами государственного, регионального и местного управления во всех развитых государствах мира. Значимость решения данной задачи обусловлена существенным влиянием, которое указывают результаты ее решения в целом на национальную безопасность страны [1].

Защита информации в компьютерных сетях обладает несомненной спецификой, обусловленной как разнообразием угроз безопасности информации, так и широтой требований, предъявляемых к уровню безопасности информации. К числу угроз безопасности информации в компьютерных сетях можно отнести как угрозы со стороны вредоносных программ и неопытных пользователей, так и целенаправленные атаки со стороны подготовленных злоумышленников, которые могут иметь поддержку со стороны внешних государственных организаций.

Применение традиционных средств и систем защиты информации, основанных на анализе событий безопасности для защиты информации в компьютерных сетях, в силу специфики угроз и повышен-

ных требований безопасности информации является недостаточным [1–3]. Одним из актуальных направлений решения этой проблемы является совершенствование сервисов защиты информации, в первую очередь, сервисов, которые осуществляют интегральную оценку состояния сети, управление защитой и адаптацию политик безопасности и компонентов системы защиты информации.

Хотя в существующих работах задача построения и анализа деревьев атак в достаточной степени исследована, проблема повышения эффективности этих механизмов и возможности их автоматической работы в рамках систем защиты информации в соответствии с текущей сетевой обстановкой, остается не до конца решенной.

Таким образом, задача исследования заключается в разработке:

1. моделей предметной области, а именно: сети, атак, уязвимостей, нарушителя и деревьев атак;
2. алгоритмов оперативного построения, модификации и анализа деревьев атак;
3. методики оперативной оценки защищенности компьютерной сети на основе анализа деревьев атак.

Реализация данной методики в системах моделирования атак должна позволять не только повышать уровень защищенности сети, но и удовлетворять всем нефункциональным требованиям, таким как своевременность, обоснованность и ресурсопотребление.

2. Анализ современной литературы. Во многих работах рассматриваются различные подходы к моделированию атак с учетом различных классов атак. В данном разделе будет кратко проанализировано текущее состояние исследований в следующих областях: (1) отображения сценариев атак; (2) злоумышленников; (3) спецификации платформ, уязвимостей, оценок уязвимостей, атак, конфигураций и возможных контрмер; (4) генерации графов атак.

В данном разделе из всего множества существующих работ проанализированы только основные, ввиду ограничений по объему тезиса.

В [2] предложена модель вторжений на основе раскрашенных сетей Петри. Каждая сигнатура вторжения выражается как шаблон, который отображает отношение между событиями и их контекстом. Обозначения начального и конечного состояний и пути между ними определяют набор последовательностей событий. Шаблоны вторжений имеют предшествующие условия и последующие действия, связанные с ними.

В [3] была разработана методика анализа перехода состояний для моделирования вторжений, основанных на хостах. Эта статья описы-

вает компьютерное вторжение как последовательность действий, выполняемых атакующим для компрометации безопасности компьютерной системы. Атаки описываются с помощью диаграмм перехода состояний. Описание атаки имеет “безопасное” исходное состояние, ноль или больше переходных состояний, и (по крайней мере) одно “скомпрометированное” конечное состояние. Состояния характеризуются значениями утверждений, описывающих аспекты состояния безопасности (владение файлом, идентификация пользователя, авторизация пользователя).

Подход к моделированию вторжений в последовательной и параллельной формах был предложен в [4]. Эта статья предлагает алгоритм по преобразованию последовательного скрипта вторжения в набор параллельных скриптов, имитирующих вторжение.

Статья [5], описывающая систему обнаружения вторжений NetSTAT, предлагает формальные модели как сети, так и атак. Эти модели дают возможность определить, “какие сетевые события должны отслеживаться и где они могут отслеживаться”. Подход NetSTAT расширяет методику анализа перехода состояний [2] для основанного на сети обнаружения вторжения, чтобы отображать сценарии атак в сетях.

В [6] была предложена простая модель сетевой безопасности “Причинно-следственная модель атаки и защиты информационной системы”. Она состоит из модели сети, отображаемой узлами и связями, причинно-следственной модели, характеристических функций и псевдослучайного генератора чисел. Тем не менее, отображение кибератак и защиты, основанное на причинно-следственной модели, очень упрощенное.

В [7] представлены наглядные модели сети и возможностей, целей и способа действий атакующего. Эти модели используются для определения устройств, которые будут скомпрометированы с наибольшей вероятностью. Для предсказания поведения атакующего используются экономические принципы (использующие компромисс “выгода – затраты”).

В [8–11] атаки описываются и моделируются в структурированной, основанной на деревьях форме.

В [8] представлена высокоуровневая концептуальная модель атак, основанная на намерениях нарушителя (стратегии атаки). Широкомасштабное распределенное обнаружение вторжения сравнивается с задачей военного управления. Статья определяет намерения вторжения как дерево целей. Конечная цель вторжения соответствует корне-

вому узлу. Узлы нижних уровней отображают альтернативные или упорядоченные подцели в достижении верхнего узла/цели. Конечные узлы (листья) – подцели. Они могут подкрепляться событиями, сгенерированными в различных средах.

Статья [9] также предлагает формальный подход для описания компьютерных атак. Этот подход называется “Деревья атак”. В деревьях атак используются узлы “И” и “ИЛИ”. Узлы ИЛИ – альтернативы. Узлы И отображают различные шаги на пути к одной цели. Работа, более детально рассматривающая так называемый основанный на “деревьях” подход, предложена в [10]. Эта статья описывает методы представления атак в форме деревьев атак.

Модель оценки жизнеспособности сетевых систем при воздействии сетевых инцидентов была представлена в [12]. Модель состоит из трех подмоделей. Первая отражает выполнение атак или инцидентов. Вторая определяет влияние атаки на систему в зависимости от типа атаки и завершенности системы защиты. Третья оценивает жизнеспособность системы.

Статья [13] предлагает методологию моделирования кибер-атак, основанную на схеме SES/MB (буквальный перевод структура системных сущностей, основанная на модели), формализме дискретного моделирования событий DEVS и объектно-ориентированного представления знаний на основе фреймов. Эта методология позволяет классифицировать угрозы, определять механизмы реализации атак и оценивать механизмы защиты.

В работе [14] описывается гибкая расширяемая модель компьютерных атак, язык для определения модели, и их использование в приложениях по безопасности, таких как анализ уязвимостей, обнаружение вторжений и генерация атак.

В [15] предлагается модель данных для системы обнаружения вторжений, называемую M2D2, которая использует четыре информационных типа: информация о характеристиках отслеживаемой информационной системы, информация об уязвимостях, информация о продуктах безопасности, используемых для проверки, и информация о наблюдаемых событиях.

В настоящей работе, были использованы подходы, описанные в публикациях из данного раздела. Новизна предложенного подхода, заключается в применении принципов моделирования атак для анализа событий, происходящих в реальном времени.

3. Основные модели предметной области. В качестве базиса для построения моделей (объекта защиты, уязвимостей, атак и т.д.) ис-

пользуется набор стандартов, на основе которых будут описываться элементы модели. Для представления данных, связанных с информационной безопасностью, предлагается использовать комплект взаимосвязанных стандартов разработанных корпорацией MITRE и национальным институтом стандартов США. Данные стандарты позволят создать единое, обновляемое и согласованное хранилище данных, необходимое для построения и анализа сценариев атак (в виде графов или деревьев атак).

Модель защищаемой сети задается следующим образом:

Network=<Hosts, Links, Service dependencies>, где Hosts – список описаний хостов, Links – список связей между хостами, Service dependencies – зависимости сервисов.

Модель хостов задается следующим образом:

Host = <Platform, Security>, где Platform – определяет программно-аппаратную платформу хоста, а Security, в свою очередь, включает в себя списки пользователей и их прав (в том числе, права атакующего, если он является внутренним нарушителем), характеристики информации, хранящейся на хосте с точки зрения конфиденциальности, целостности и доступности, и описание политик безопасности систем защиты информации, ограничивающих список доступных к проведению атак. Описание платформы хоста включает в себя Software и Hardware – списки, соответственно, программного и аппаратного обеспечения на языке CPE, а так же, Operation system – версия операционной системы на языке CPE.

Модель связей между хостами задается следующим образом:

Links = <Physical Links{<Host, Host, Bandwidth, Attacks>, <Host, Host, Bandwidth, Attacks>,…}, Virtual Links{<Host, Host, Type, Attacks>, <Host, Host, Type, Attacks >,…}. В данном описании выделяются два основных типа связей – физические и виртуальные. Для данных типов связей определяется, какие именно хосты связаны между собой (и, соответственно, могут атаковать друг друга), а также, возможные атаки на саму связь (например, нарушение конфиденциальности передаваемой информации или нарушение функциональных зависимостей). Так же для физических связей определяется пропускная способность, на основе которой можно определить интенсивность трафика, которая может привести к блокировке канала (атаки на истощение ресурсов).

Модель зависимостей сервисов задается следующим образом:

Service dependencies = {<<Host, Software>, <Host, Software>, Type, Attacks>, <<Host, Software>, <Host, Software>, Type, Attacks>, …}, где

пара <Host, Software> представляет собой определенное приложение на некотором хосте, которое участвует в зависимости, Type – тип зависимости (зависимость доверия, функционирования и т.д.), а Attacks определяет возможные атаки, которые можно провести через эти отношения зависимости.

4. Методика построения и модификации деревьев атак. Деревья атак предоставляют собой подходящий инструмент для решения множества проблем, связанных с безопасностью, включая корреляцию и предотвращение вторжений и реакцию на них [21,22]. Тем не менее, методики использующие деревья атак для построения моделей, описанные в большинстве существующих исследований, имеют строгие ограничения. Существует множество исследований, в которых описаны подходы, позволяющие построить деревья атак, но, при этом, процесс обновления этих деревьев в соответствии с изменениями в защищаемой сети либо не рассматривается, или происходит за счет полной перестройки деревьев [16,17]. Исходя из этого, важным направлением исследований становятся способы формирования деревьев атак таким образом, чтобы задача обновления и анализа элементов этого дерева была максимально простой и требовала минимальное время и ресурсы. Для решения этой задачи в данной работе предлагается модель деревьев потенциальных атак. Для данной модели наиболее важными параметрами являются: возможности нарушителя, влияние и вероятность атаки.

Для добавления потенциальной атаки в граф атак должны быть выполнены 3 условия: (1) защищаемая система должна иметь уязвимости; (2) нарушитель должен обладать необходимыми знаниями и ресурсами для осуществления атакующих действий; (3) выполнение атаки продвигает нарушителя к выполнению его цели. Первое условие определяется полностью свойствами защищаемой системы, второе формируется за счет свойств как системы, так и модели нарушителя, третье же, в свою очередь, определяется целями нарушителя.

На этапе подготовки к построению деревьев атак, для каждого хоста строится 3-х мерная матрица по следующим данным:

1. класс атак (attack action class) – сбор данных, подготовительные действия, повышение привилегий, выполнение цели атаки;
2. необходимый тип доступа (access type) – удаленный источник без прав доступа, удаленный пользователь системы, локальный пользователь системы, администратор;
3. уровень знаний нарушителя (malefactor knowledge level) – типы уязвимостей, которые нарушитель может реализовывать.

В результате, для каждого хоста формируется набор кортежей (Attack Action Class, Access type, Knowledge Level, Vulnerability), для каждого из кортежей, в свою очередь, формируется список конкретных атак и уязвимостей, реализуемых этими атаками. Общий список уязвимостей составляется на основе описания программно-аппаратного обеспечения хоста на языке CPE и таких открытых баз уязвимостей, как NVD.

Модель уязвимостей задается следующим образом:

Vulnerability=<Software, Complexity, Access type, Required rights, Result>, где Software определяет, в каком именно программном обеспечении (или при какой комбинации установленного программного обеспечения) появляется возможность реализации данной уязвимости, Complextity определяет уровень знаний нарушителя, необходимый для реализации этой уязвимости, Access type и Required rights определяют необходимый тип доступа и права, без которых нарушитель не сможет использовать данную уязвимость. Параметр Result определяет, что именно получит нарушитель (повышение привилегий, нарушение конфиденциальности, целостности или доступности) в результате реализации данной уязвимости.

В формируемый для конкретного нарушителя список условий, необходимых для добавления потенциальной атаки в дерево атак, входит необходимое условие - нарушитель должен обладать необходимыми знаниями и ресурсами для осуществления атакующих действий, чтобы выполнение этой атаки, продвигало его к выполнению его цели.

Соответственно, модель нарушителя определяет ограничения нарушителя по выбору потенциально возможных атакующих действий из общего множества. В качестве ограничений выступают:

1. знания нарушителя, ограничивающие сложность уязвимостей, которые нарушитель может использовать (данная характеристика также определяет список уязвимостей нулевого дня, известных нарушителю);

2. начальное расположение нарушителя в защищаемой сети, определяющее список доступных атакующему хостов на основе модели защищаемой компьютерной сети (существует два основных типа нарушителя в соответствии с данным параметром–внешний и внутренний нарушитель);

3. начальные права нарушителя, ограничивающие множество атак на основе требуемых условий для реализации атакующих действий (например, некоторые атаки могут быть осуществлены только при наличии у нарушителя прав обычного пользователя).

Таким образом, модель нарушителя задается кортежем из трех элементов:

Malefactor = <Knowledge, Starting point, Base rights>, где Knowledge – знания нарушителя, Starting point – элементы модели защищаемой сети, к которым нарушитель имеет доступ с самого начала, Base rights – начальные права на нарушителя в защищаемой сети.

Модель знаний нарушителя задается следующим образом:

Knowledge=<Knowledge level, Known vulnerabilities, 0-day vulnerabilities>, где Knowledge level – уровень знаний нарушителя определяется как высокий/низкий/отсутствующий, Known vulnerabilities – список известных нарушителю общедоступных уязвимостей и 0-day vulnerabilities – список известных нарушителю уязвимостей нулевого дня.

Модель начальных прав задается следующим образом:

Base rights = {<Host, Rights>1, <Host, Rights>2, ... , <Host, Rights>n}, где n-количество хостов, а Host – это элемент модели компьютерной сети, а Rights это уровень прав нарушителя.

Для определения целей нарушителя в предлагаемую модель вводится список действий, к выполнению которых будет стремиться нарушитель (например, это может быть компрометация определенного хоста, кража конфиденциальной информации из базы данных и т.д). Модель нарушителя, обладающего целью, определяется следующим образом:

Aimed Malefactor = <Malefactor, Aims>, где Malefactor представляет собой модель нарушителя, а Aims – цели нарушителя при проведении атак.

Цель (цели) нарушителя определяют, в какой момент нарушитель завершит свои атакующие действия. Данный параметр позволяет определять вероятностные характеристики при выборе потенциальных путей развития дерева атак для конкретного нарушителя.

Модель цели нарушителя задается следующим образом:

Aims={<Host, Result>,<Host, Result>,...}, где Host – это элемент модели компьютерной сети, а Result – это результат атакующего действия, являющийся отражением общей цели нарушителя, например, это может быть кража критичной информации (нарушение конфиденциальности), ее порча (нарушение целостности), приведение системы или ее компонентов в нерабочее состояние (нарушение доступности) или получение определенных прав доступа.

Модели нарушителя используются на двух этапах функционирования системы построения и анализа деревьев атак – этапах проектирования и эксплуатации:

1. на первом этапе модели нарушителей используются для построения различных деревьев атак на основе установленных характеристик (профилей нарушителей), которые выбраны администратором системы;

2. на втором этапе система позволяет распознать наиболее вероятную модель нарушителя по обнаруженной вредоносной активности внутри защищаемой сети и затем использовать эту модель для предсказания последующих шагов реального нарушителя.

Таким образом, модели нарушителей помогают определить возможные действия, используемые нарушителем и потенциальные/реальные стратегии атак. Оценка характеристик нарушителей (навыки, цели, исходный набор прав доступа, и т.д.) позволяет связать критичность атаки с профилем атакующего. Уровень навыков нарушителя и его цели могут помочь, среди других показателей, при поддержке принятия решений (например, более серьезная реакция в случае высококвалифицированного атакующего).

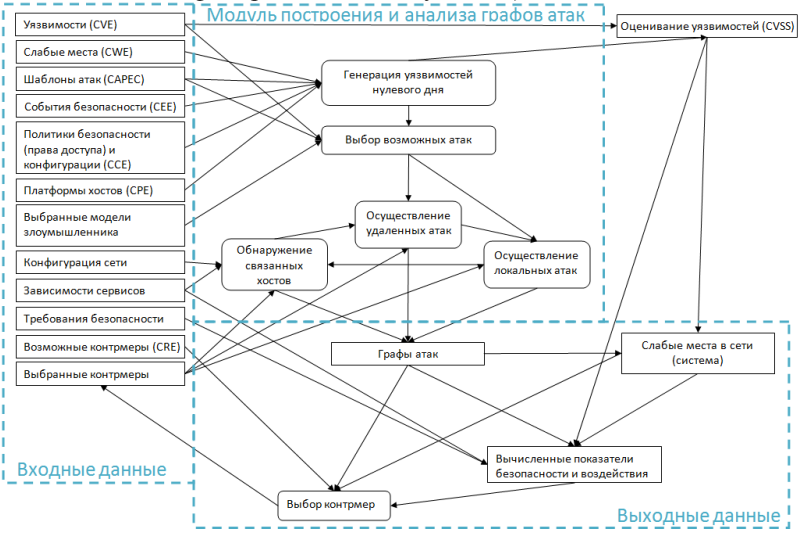

Рис. 1. Основные потоки данных.

Общая структура потоков данных системы, основанной на предлагаемой методике, делится на три группы по типу источника (рис. 1).

К первой группе относятся данные, получаемые из открытых баз данных в сети Интернет. К этой группе относятся данные об уязвимостях, слабых местах, шаблонах атак и исправлениях. Вторая группа определяется на основе данных, собранных в защищаемой сети и на основе знаний оператора системы, и включает в себя топологию сети, политики безопасности, зависимости сервисов и списки установленного программного и аппаратного обеспечения на хостах. Источником для третьей группы является оператор системы. Оператор определяет требования безопасности, предъявляемые к защищаемой системе и, выбирает наиболее вероятные модели злоумышленников. Результатом работы системы являются базовые графы атак, список слабых мест системы и рассчитанные показатели защищенности [19,20].

5. Заключение. Защита компьютерных сетей предполагает применение новейших подходов к построению средств и систем защиты информации, способных осуществлять непрерывный мониторинг защищенности на основе разнородных данных поступающих от различных сенсоров и источников в режиме времени, близком к реальному. В настоящей статье рассмотрена методика оперативного построения и анализа деревьев атак для компьютерных систем. Новизна предлагаемой методики заключается в том: что модели, алгоритмы и методика оперативного построения и анализа деревьев атак, отличаются от существующих ориентацией на работу в режиме реального (или близкого к реальному) времени. Использование данных моделей позволит построить систему, использующую анализ деревьев атак в режиме реального времени, и учитывающую большой объем разнородных входных данных.

В настоящее время продолжаются теоретические исследования способов построения графов атак, учитывающих существующие уязвимости, и уязвимостей нулевого дня, политики безопасности, зависимости сервисов и т.д., и осуществляется разработка программного прототипа подсистемы моделирования атак. В дальнейшей работе планируется: (1) расширить функциональность прототипа, добавив в него анализ атак нулевого дня и связей сервисов; (2) расширить список метрик безопасности для уточнения оценки уровня защищенности сети; (3) уточнить модель нарушителя; (4) ускорить работу прототипа, за счет оптимизации процесса построения графов атак.

Литература

1. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд, № 2, 2006. С.46–57.
2. *Kumar S., Spafford E.H.* An Application of Pattern Matching in Intrusion Detection // Technical Report CSDTR 94 013. The COAST Project. Department of Computer Sciences. Purdue University. West Lafayette, 1994.
3. *Iglun K., Kemmerer R.A., Porras P.A.* State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, 21(3), 1995.
4. *Chung M., Mukherjee B., Olsson R.* Simulating concurrent intrusions for testing intrusion detection systems // Proceedings of the 1995 National Information Security Conference, 1995. P. 173–183.
5. *Kemmerer R.A., Vigna G.* NetSTAT: A network-based intrusion detection approach // Proceedings of the 14th Annual Computer Security Applications Conference, Scottsdale, Arizona, 1998.
6. *Cohen F.* Simulating Cyber Attacks, Defenses, and Consequences // IEEE Symposium on Security and Privacy, Berkeley, CA. 1999.
7. *Yuill J., Wu F., Settle J., Gong F., Forno R., Huang M., Asbery J.* Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks, No.34, 2000.
8. *Huang M.-Y., Wicks T.M.* A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis // First International Workshop on the Recent Advances in Intrusion Detection, Raid'98, Louvain-la-Neuve, Belgium, 1998.
9. *Schneier B.* Attack Trees // Dr. Dobb's Journal, Vol.12, 1999.
10. *Moore A.P., Ellison R.J., Linger R.C.* Attack Modeling for Information Security and Survivability // Technical Note CMU/SEI-2001-TN-001. Survivable Systems, 2001.
11. *Dawkins J., Campbell C., Hale J.* Modeling network attacks: Extending the attack tree paradigm // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.
12. *Moitra S.D., Konda S.L.* A Simulation Model for Managing Survivability of Networked Information Systems // Technical Report CMU/SEI-2000-TR-020 ESC-TR-2000-020, 2000.
13. *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, Vol.2119, 2001.
14. *Templeton S. J., Levitt K.* A Requires/Provides Model for Computer Attack // Proceedings of the New Security Paradigms Workshop, 2000.
15. *Morin B., Me L., Debar H., Ducasse M.* M2d2: A formal data model for ids alert correlation // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002. Vol. 1516. P.115–137.
16. *Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В.* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии, № 1, 2009. С.37–42.
17. *Котенко И.В., Степашкин М.В.* Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.31, Москва, URSS, 2007. С.126–207.
18. *Котенко И.В., Дойникова Е.В., Чечулин А.А.* Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд, № 4, 2012. С.54-66.
19. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Про-

блемы информационной безопасности. Компьютерные системы. № 2, 2012. С. 57-68.
20. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. С. 27-56.
21. *Чечулин А.А.* Методика построения графов атак для систем анализа событий безопасности // XVI международная заочная научно-практическая конференция "Инновации в науке". 28 января 2013 г. Материалы конференции. Новосибирск, 2013. С.156-161. ISBN 978-5-4379-0210-3.
22. *Kotenko I., Chechulin A., Novikova E.* Attack Modelling and Security Evaluation for Security Information and Event Management. SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24–27 July 2012. P. 391-394.

Чечулин Андрей Алексеевич — научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей. Число научных публикаций — 70. chechulin@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450. Научный руководитель — И.В. Котенко.

Chechulin Andrey Alexeevich — research scientist of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, intrusion detection, analysis of the network traffic, analysis of vulnerability. The number of publications — 70. chechulin@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450. Supervisor — I.V. Kotenko.

Поддержка исследований. В публикации представлены результаты исследований, поддержанных Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ, программой фундаментальных исследований ОНИТ РАН и проектами Седьмой рамочной программы Европейского Союза *SecFutur* и *MASSIF*.

Рекомендовано лабораторией проблем компьютерной безопасности СПИИРАН.
Заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 03.03.2013.

РЕФЕРАТ

Чечулин А.А. **Методика оперативного построения, модификации и анализа деревьев атак.**

Применение аналитического моделирования атак является перспективным направлением в области защиты информации, особенно для крупных компьютерных сетей, содержащих узлы с критически важной информацией. Для эффективного использования моделирования, необходимо решение ряда задач, одна из которых связана с временными затратами на построение моделей.

В статье приводятся основные элементы предлагаемой методики, позволяющей формировать, анализировать и модифицировать модели сети и атакующих действий в режиме близком к реальному времени. Рассмотренные в статье задачи являются составными элементами общей системы управления информацией и событиями. Результатом работы системы моделирования атак могут быть следующие характеристики: (1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак); (2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак; (3) возможные последствия реализации контрмер, учитывающие зависимости сервисов.

Рассматриваемая методика реализована в виде программного прототипа и успешно используется в рамках проекта Европейского союза MASSIF.

SUMMARY

Chechulin A.A. **Efficient technique of construction, modification and analysis of attack graphs.**

The analytical attack modeling is the promising approach in the information security field, especially for large networks that contain hosts with critical information. But for effective modeling usage it is necessary to solve some problems. One of the problems is related to performance of the models construction and modification.

The paper presents the main elements of the proposed approach which allows constructing, analyzing and modifying of the network attack models in near real time. This approach can be used in Security Information and Event Management (SIEM) systems. The results of the modeling process include the following characteristics: (1) weaknesses of the network topology (hosts, through that the most number of attack routs are going), (2) the selected countermeasures that reduce the number of attack routs, and (3) the impact factor of the countermeasures, taking into account the service dependencies.

The technique is implemented as a software prototype and successfully used in the framework of the European Union project MASSIF.