УДК 004.7

РАЗРАБОТКА НЕЧЕТКИХ ЛИНГВИСТИЧЕСКИХ МОДЕЛЕЙ СЕТЕВЫХ АТАК ДЛЯ АНАЛИЗА РИСКОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В. О. Шапорин, д. т. н. Н. Б. Копытчук, к. ф.-м. н. П. М. Тишин, к. т. н. Р. О. Шапорин

Одесский национальный политехнический университет
Украина, г. Одесса
shaporin_onpu@inbox.ru, knb47@mail.ru, tik88@mail.ru, shaporin@ics.opu.ua

Рассмотрены методы построения моделей рисков вторжений в компьютерные сети в условиях неопределенности с использованием математического аппарата нечеткой логики и анализ данных моделей в терминах рисков для информационной системы. В качестве инструмента анализа рисков используется метод Coras.

Ключевые слова: безопасность компьютерных сетей, нечеткая логика, лингвистические переменные, анализ рисков, модели сетевых атак.

Использование сетевых технологий как инструмента бизнеса, обучения, хранения информации, управления процессами и т. п. обуславливает необходимость обеспечения безопасности подобных систем. Известные и активно используемые сигнатурные и поведенческие методы определения атак характеризуются вероятностной оценкой параметров протекающих процессов либо сравнением некоторого формализованного описания атаки с соответствующим шаблоном, что в условиях современных технологий не всегда приемлемо с точки зрения конечного результата.

Для повышения степени достоверности результатов оценки риска возникновения атаки или определения уже начавшегося вторжения, целесообразно задействовать аппарат нечеткой логики и базы знаний.

В данной работе предлагается использовать метод Coras, который широко используется при анализе и прогнозировании рисков в информационных системах (ИС) [1]. Терминология Coras позволяет описать все составляющие угрозы для информационной системы, а именно:

– актив (Asset) – набор ресурсов системы, подверженных угрозе;

– преднамеренная угроза (deliberate threat) – действия злоумышленников, приводящие к возникновению риску проведения атаки;

– сценарий угрозы (threat scenario) – последовательность действий, определяющая процесс протекания атаки;

– техногенная угроза (non-human threat) – случайные факторы, приводящие к возникновению угрозы;

– нежелательный инцидент (unwanted incident) – событие, возникающее в результате выполнения сценария угрозы.

Построение диаграмм, входящих в метод Coras, формирует систему анализа риска, которая описывает отношения между объектами Coras. Таким образом, входными переменными для анализа системы являются параметры данных объектов и отношения между ними. Выходные параметры – активы, которые подвержены риску. В терминах безопасности сетевой инфраструктуры в качестве защищаемых активов выступают:

– степень доступности ресурсов ИС;

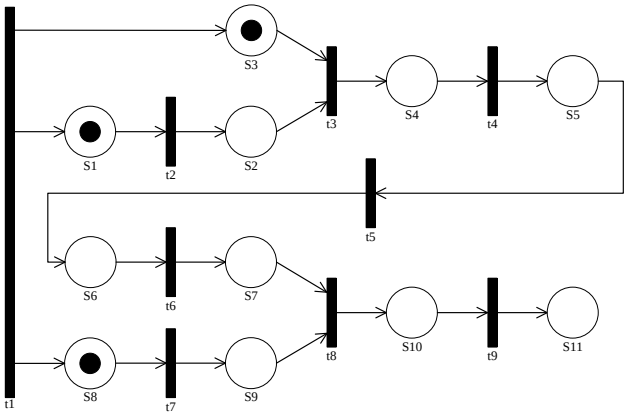
– степень конфиденциальности ресурсов ИС;

– степень целостности ресурсов ИС.

Сценарий угрозы описывается последовательностью состояний системы в процессе реализации атаки. В данной работе предполагается, что каждое состояние описывается некоторой нечеткой величиной либо закономерностью с нечетко заданными параметрами.

Для формулирования зависимостей свойств объектов и отношений, входящих в диаграмму угроз, от параметров процессов, протекающих в реальной сетевой инфраструктуре, в работе используется аппарат сетей Петри–Маркова. При построении сети Петри–Маркова этапам атаки соответствует определенное состояние сети S_i, а переходы t_j между состояниями описывают условия начала следующего этапа атаки [2].

Независимо от своего типа, любая атака несет угрозу минимум одному активу информационной системы. Однако, при более глубоком анализе результатов выполнения вторжений, можно отметить, что каждая атака непосредственно или косвенно причиняет ущерб всем трем активам с определенной степенью достоверности. Также следует отметить, что большинство сетевых атак имеют взаимосвязь между собой. Так, например, атака «подмена доверенного объекта» требует перезагрузки легального хоста сети принудительно или самостоятельно. Модель сети Петри—Маркова для такой атаки представлена на рисунке.



Модель атаки «подмена доверенного объекта»
и предшествующая ей атака «отказ в обслуживании»

В данной модели состояния S1–S5 соответствуют атаке «отказ в обслуживании», все последующие состояния реализуют подмену доверенного объекта. С точки зрения анализа рисков, можно рассматривать эти модели по отдельности или в единой системе. Начальное состояние t_1 (начальная задержка срабатывания сети) можно заменить атакой «сканирование сети», атаку «отказ в обслуживании» можно заменить нечеткой случайной величиной самопроизвольной перезагрузки хоста, т .е. комбинировать возможные взаимосвязи между различными сценариями угроз.

Таким образом, используя методологию Coras, дополненную аппаратом нечеткой дескриптивной логики, можно оценивать риски в ИС, формулируя нечеткие предложения, которые иллюстрируют нечеткий вывод о состоянии ИС в конкретный момент времени с точностью и прозрачностью, которые выше, чем вероятностная оценка.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Копытчук Н. Б. Тишин П. М., Ботнарь К. В., Цюрупа М. В. Разработка формализованного языка анализа рисков на основе дескрипционной логики // Электротехнические и компьютерные системы.– 2011.– № 02(78).– С. 103–108.

2. Радько Н. М., Скоболев И. О. Риск-модели ИТКС при реализации угроз удаленного и непосредственного доступа. – Москва: РадиоСофт, 2010.

N. B. Kopitchuk, P. M. Tishin, R. O. Shaporin, V. O. Shaporin

Development of fuzzy linguistic models of network attacks for risk analysis in distributed information systems.

In this work the authors consider the methods of developing fuzzy linguistic models of network attacks for risk analysis in distributed information systems. The Coras method is used for risk analysis.

Keywords: *computer system security, fuzzy logic, linguistic variables, risk analysis, network attack models.*