УДК 004.056

МЕТОД ФОРМАЛИЗАЦИИ ПРОЦЕССА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВИРТУАЛИЗАЦИИ, ОСНОВАННЫЙ НА МАТЕМАТИЧЕСКОМ АППАРАТЕ СЕТЕЙ ПЕТРИ

Ю.К. Язов, А.Л. Сердечный, А.В. Бабурин

В статье указаны ограничения классического аппарата сетей Петри применительно к моделированию стохастических процессов, проходящих в системах с изменяющимися составом элементов и структурой. Предложено расширение аппарата теории сетей Петри, позволяющее осуществить математическое моделирование процесса несанкционированного доступа в информационных системах, построенных с использованием средств виртуализации

Ключевые слова: несанкционированный доступ, математическое моделирование, сети Петри

Имитационное моделирование представляется наиболее перспективным направлением исследования процесса несанкционированного доступа в информационных системах, построенных с использованием средств виртуализации (ИССВ), по ряду причин, основными из которых являются:

- высокая сложность построения аналитических моделей для таких информационных систем (ИС);
- достаточный уровень развития вычислительной техники для выполнения расчётов многокомпонентных имитационных моделей.

Для построения имитационных моделей могут использоваться разнообразные методы, такие как метод дискретно-событийного моделирования, основанный на аппарате теории массового обслуживания, метод моделирования системной динамики с использованием дифференциальных моделей, метод агентного моделирования, позволяющий на основе знания алгоритмов работы аппаратного обеспечения вычислительной сети, протоколов сетевого взаимодействия, предполагаемого поведения элементов системы и др. выявить законы функционирования самой системы, что представляет наибольший интерес для имитационного моделирования процесса несанкционированного доступа в ИССВ.

В агентном моделировании могут быть использованы методы формализации, основанные на теории сетей Петри, темпоральной логике, теории конечных аппаратов, теории игр, модели акторов и др. [1]. Однако каждый из этих методов по разным причинам (отсутствия учета статистики, временного фактора, вариаций структуры моделируемой системы и т.п.) не может быть непосредственно использован при моделировании процессов НСД.

В настоящей статье предлагается метод формализации, основанный на расширении аппарата теории сетей Петри, который может быть положен в основу агентного моделирования процесса НСД в ИССВ.

Основная идея моделирования процесса НСД в ИССВ сетью Петри заключается в том, что позиции сети Петри моделируют состояния компонент ИССВ, переходы – действия, выполняемые такими компонентами, а маркеры – сетевые пакеты или сообщения, при помощи которых осуществляется взаимодействие всех компонент. Однако процесс НСД в ИССВ представляет собой ***стохастический*** процесс, проходящий в системе с ***изменяющимся составом и структурой***. По этой причине классическая модель сетей Петри [2], не позволяет в полной мере отразить все особенности такого процесса.

Язов Юрий Константинович –ВГТУ, д-р техн. наук, профессор,
Сердечный Алексей Леонидович – ФАУ «ГНИИИ ПТЗИ ФСТЭК России», e-mail: alex-voronezh@mail.ru
Бабурин Александр Вильямович – ВГТУ, д-р техн наук, глав. науч. сотрудник, e-mail: mnac @comch.ru

Известны следующие расширения классических сетей Петри, позволяющие преодолеть некоторые из указанных ограничений:

- введение модульного принципа построения сети (иерархические сети Петри), позволяющего упростить восприятие формализованного описания моделируемого процесса, представив его более простыми иерархически-вложенными подпроцессами [3, 4];

- использование сложных маркеров и использование предикатов для позиций и переходов (цветные и предикатные сети Петри), позволяющих организовать обмен сведениями между компонентами моделируемого процесса, что решает задачу моделирования сетевых пакетов и сообщений при помощи маркеров сетей Петри [3];

- введение вероятностных характеристик (сети Петри-Маркова), позволяющих отразить случайный характер некоторых подпроцессов [5, 6];

- задание функций времени для позиций и переходов (временные сети Петри), позволяющих учесть временной фактор в процессе ведения НСД [5, 6].

Предлагаемый метод формализации включает указанные расширения, позволяет моделировать процессы, происходящие в системах с изменяющимися составом и структурой, и обеспечивает возможность выполнения операций над сетями Петри (далее по тексту «самоорганизующаяся сеть Петри» - ССП). Описание метода формализации включает:

- формальное описание элементов ССП;
- определение операций над ССП;
- задание правил выполнения ССП.

ССП представлена следующей формализованной записью $\theta = (П, \mu_0, EQ, (E), C, F)$,

где $П$ – сеть Петри, включающая соединительные дуги, описываемые множеством E (дуги, на базе которых возможно проводить операции объединения или разъединения ССП);

μ_0 – начальная маркировка ССП;

EQ – множество условий, ограничивающих возможности пребывания маркеров в позициях, хранения маркеров переходами и прохождения маркеров по дугам;

(E) – множество параметров для групп дуг ССП, определяющих правила выбора дуг при перемещении маркера в конфликтных ситуациях;

C – множество параметров, связанных с переходами ССП;

F – множество функций, характеризующих работу переходов ССП.

Графическое обозначение ССП показано на рис. 1.

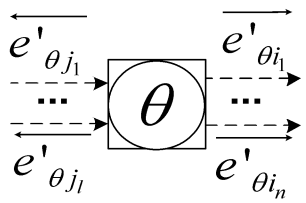

Рис. 1. Графическое обозначение расширенной сети Петри

Над ССП могут быть заданы операции: изменения значения параметра перехода, задания маркировки ССП, задания ограничений на перемещение маркеров по дугам, объединения и разъединения ССП, остановки и возобновление выполнения ССП, создание экземпляра ССП, идентичного оригиналу.

Операция изменения значения параметра перехода записывается следующим образом: $O_C(c_1) = c_2 \mid c_1, c_2 \in C$. В результате применения операции выполняется изменение параметра c_1 на значение c_2.

Операция задания маркировки расширенной сети Петри записывается следующим образом: $O_{\mu\theta}(x)$. В результате применения операции осуществится замена текущей маркировки расширенной сети Петри на маркировку, заданную аргументом x.

Операция задания ограничений на перемещение маркеров по дугам записывается следующим образом: $O_{EQ\theta}(EQ_E)$. В результате применения операции произойдёт добавление ограничений EQ_E для дуг сети θ.

Бинарные операции объединения расширенных сетей Петри включают следующие операции:

- правостороннюю операцию объединения ($\overset{\rightarrow}{\cup}$);

- левостороннюю операцию объединения ($\overset{\leftarrow}{\cup}$);

- полную операцию объединения ($\overset{\leftrightarrow}{\cup}$).

Правосторонняя операция объединения ССП записывается следующим образом: $\theta_3 = \theta_1\left(\left[\overrightarrow{E^{ij}_1}\right]_{i=1}^{j}\right) \overset{\rightarrow}{\cup} \theta_2\left(\left[\overleftarrow{E^{ij}_2}\right]_{i=1}^{j}\right)$.

В результате выполнения операции происходит слияние сетей θ_1 и θ_2 в сеть θ_3. Слияние сетей происходит за счёт слияния дуг в местах соединений, задаваемых соединительными участками $\left[\overrightarrow{E^{ij}_1}\right]$, $\left[\overleftarrow{E^{ij}_2}\right]$.

Для правосторонней операции объединения слияние дуг происходит на базе выходных соединительных дуг каждого участка $\left[\overrightarrow{E^{ij}_1}\right]_{i=1}^{j}$. В новую объединённую сеть θ_3 будут входить все дуги сетей θ_2 и θ_3, а также новообразованные при слиянии дуги. Сеть θ_3 включает все вершины и переходы сетей θ_1 и θ_2. То же самое касается и других параметров сетей θ_1 и θ_2.

Аналогично задаётся левосторонняя операция объединения, однако для неё слияние дуг происходит на базе входных соединительных дуг.

Полная операция объединения включает в себя правостороннюю и левостороннюю операции объединения.

Операция разъединения ССП записывается следующим образом: $\theta_1 = \theta_2[\overrightarrow{E}] / \theta_3[\overleftarrow{E}]$. В результате применения операции происходит разъединение сети θ_2 на θ_1 и θ_3 за счёт удаления дуг $\overrightarrow{E}$ и $\overleftarrow{E}$.

Операция остановки выполнения ССП записывается следующим образом: $O_{stop}(\theta)$. В результате применения операции такая ССП сохраняет свою маркировку, но временно (до момента запуска) не участвует в процессе, составной частью которого она является.

Операция возобновления выполнения ССП записывается следующим образом: $O_{start}(\theta)$. Операция возобновляет работу ранее остановленной расширенной сети Петри.

Операция создания экземпляра ССП, идентичного оригиналу записывается следующим образом: $\theta_1 = O_{new}(\theta_2)$. В результате применения операции создаётся ССП $\theta_1 = \theta_2$.

Выполнение операций

Процесс НСД в ИССВ можно представить в виде ССП θ_{KP} (рис. 2, а),

где $\theta_{Л}$ – модель людей, использующих ИССВ (рис. 2, б), состоящая из моделей злоумышленников $\theta_{ЗЛi}$, моделей пользователей θ_{Ui} и моделей администраторов θ_{ADi};

$\theta_{ИС}$ – модель ИССВ (рис. 3, в), состоящая из модели компьютеров, входящих в состав ИССВ $\theta_{К}$ (рис. 2, г-е), и модели сетевого оборудования $\theta_{СО}$;

$\theta_{АО}$ – модель аппаратного обеспечения оборудования ИССВ;

$\theta_{СПО}$ – модель системного программного обеспечения компьютеров ИССВ;

$\theta_{ППО}$ – модель прикладного программного обеспечения компьютеров ИССВ.

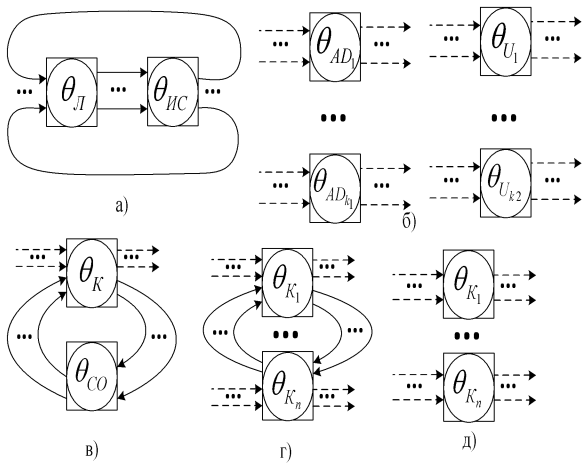

Рис. 2 – Модель процесса НСД и ИССВ

Модель НСД, разработанная с использованием предлагаемого метода, позволяет оценить временные характеристики процесса

НСД, эффективность средств защиты от НСД и др.

Таким образом, предложенные расширения аппарата теории сетей Петри позволяют преодолеть ограничения классического аппарата сетей Петри применительно к моделированию стохастических процессов, происходящих в системах с изменяющимися составом и структурой. Это дает возможность осуществлять математическое моделирование процесса НСД в ИССВ.

Литература

1. Дубинин, В. Н. Сетевые технологии проектирования и реализации распределенных вычислительных систем на программно-аппаратных платформах локальных и глобальных сетей Ethernet/Internet. – Пенза: Изд-во Пенз. гос. ун-та, 1998. – 322 с.: 160 ил.

2. Питерсон, Дж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 264 с., ил.

3. Котов, В.Е. Сети Петри. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 160 с.

4. Ломазова, И.А. Вложенные сети Петри и моделирование распределённых систем – М.: Научный Мир, 2004. – С. 208

5. Язов, Ю.К., Панфилов А.П. Моделирование динамики реализации угроз несанкционированного доступа к информации в компьютерных системах на основе аппарата сетей Петри-Маркова – Журнал «Информация и безопасность». Воронеж: Воронежский государственный технический университет, 2006. Вып. 1 – С. 117-123

6. Ларкин Е.В., Котов В.В., Котова Н.А., Соколов В.А. К вопросу о моделировании отказоустойчивых систем с помощью сетей Петри-Маркова – Журнал «Фундаментальные исследования». Пенза: Издательский Дом «Академия Естествознания», 2007. Вып. 5. – С. 5.

7. Батаронов И.Л. , Паринов А.В., Симонов К.В. Оценка и регулирование рисков обнаружение и предупреждение компьютерных атак на инновационные проекты // Информация и безопасность. 2013. Т. 16. № 2. С. 243-246.

8. Бекетнова Ю.М., Львович И.Я. Решение задачи раннего выявления рисков нарушения финансовой и информационной безопасности юридического лица в терминах теории распознавания образов // Информация и безопасность. 2013. Т. 16. № 2. С. 191-194.

9. Борисов В.И. , Радько Н.М. , Голозубов А.А. , Батаронов И.Л. , Ермилов Е.В. Вероятностные аналитические модели сетевой атаки с внедрением вредоносного программного обеспечения // Информация и безопасность. 2013. Т. 16. № 1. С. 5-30.

Воронежский государственный технический университет
Voronezh State Technical University

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю
State science research experimental institute of technical information protection problem of Federal service of technical and export control

THE PETRI NET FORMALIZATION METHOD OF UNAUTHORIZED ACCESS IN VIRTUALIZATION INFORMATION SYSTEM

Yu.K. Yazov, A.L. Serdechnyy, A.V. Baburin

The article quoted limitations of the classical apparatus of Petri nets applied to the modeling of stochastic processes taking place in systems with varying composition of elements and structure. The extension of the Petri nets, which allows to carry out mathematical modeling of unauthorized access to information systems constructed with the use of

Key words: unauthorized access, mathematical modeling, Petri nets