УДК 517.9

К.М. Сагиндыков, Г. Мусайф

Казахский университет экономики, финансов и международной торговли, Астана
(E-mail: ksagin@mail.ru)

Использование сети Петри для оценки систем защиты информации

В статье рассмотрено использование сети Петри для оценки систем защиты информации. В качестве исходной информации для метода оценки средств защиты информации информационных систем использована продукционная модель, представляющая собой набор разделенных на секции и подсекции продукционных правил.

Ключевые слова: продукционная система, множество, количество позиций, сеть.

В качестве исходной информации для метода оценки средств защиты информации информационных систем (СЗИ ИС) используется продукционная модель, представляющая собой набор разделенных на секции и подсекции продукционных правил [1, 2]. В общем виде правила продукции (ПП) представляются как кортеж [3]:

$$PR = \langle S, N, F, A \Rightarrow C, W \rangle, \tag{1}$$

где N - номер или имя правила; S - сфера применения данного правила; F - предусловие применения (условие активизации), содержащее информацию об истинности и приоритетности данного правила; $A \Rightarrow C$ - ядро ПП; W - постусловие.

Ядра могут быть детерминированные и недетерминированные, в зависимости от вида A и C. В детерминированных ядрах правая часть ядра выполняется обязательно, а в недетерминированных ядрах - с определенной вероятностью. В работе используются только ПП с детерминированными ядрами

$$\text{«если A, то C» или «если A, то } C_1 \text{ иначе } C_2\text{»}, \tag{2}$$

где A, C, C_1, C_2 — логические выражения.

Кроме того, консеквента и постусловия W продукции могут быть представлены в виде

$$\text{«если A, то C - результат W»}. \tag{3}$$

Правила, используемые в описываемой модели для описания исходной экспертной информации, должны удовлетворять следующим требованиям:

- правила должны быть детерминированными (однозначными или альтернативными);
- порядок выполнения правил должен быть заранее определен;
- выражения антецедентов A и консеквентов C должны допускать представление в виде логических последовательностей в терминах двузначной логики;
- в выражениях A могут использоваться только переменные D и вспомогательные переменные V, а в выражениях C - как переменные D и V, так и выходные переменные K.

Традиционная схема разрешения конфликтов, когда запрещается одновременное исполнение нескольких правил, т.е. когда на каждом шаге функционирования продукционная система (ПС) выбирает только одно правило, является неэффективной, так как в этом случае возникают неоправданные задержки или запрещения применения «вытесненных» неконфликтных операций, которые могут быть использованы одновременно с оставшимися.

Для упрощения ПС и уменьшения числа правил применяется их объединение. В ПС возможно наличие конфликтов правил. Существуют различные методы разрешения конфликтов:

- дополнение ПС набором метаправил, корректирующих работу процедуры в подобных случаях;

- запрет на изменение управляющих воздействий, по поводу которых возникает конфликт, с выдачей сообщения оператору;

- запрет одновременного исполнения нескольких правил.

В предлагается метод разрешения конфликтов путем добавления метаправил вида: если применимы правила $R_i...R_j$, то вытеснить $R_k...R_l$.

Однако такой подход может не выявить все возможные конфликты. Поэтому предлагается использование метода запрета на изменение управляющих воздействий, по поводу которых возник конфликт.

Для реализации этого метода предлагается метод коррекции ПС путем попарного сравнения правил. Этот метод является наиболее простым с точки зрения применения и менее требовательным к аппаратным и программным ресурсам при автоматическом расчете по сравнению с другими методами.

Одним из методов разрешения конфликтов является представление структуры ПС в виде иерархической сети с дальнейшим анализом сети Петри известными способами. На структурном уровне сеть Петри представляет собой двудольный ориентированный граф, включающий в себя вершины двух типов: позиции (p) и переходы (t). Позиции обозначаются как p_i, а переходы - t_j. Позиции и переходы соединены направленными дугами f_k, каждая из которых имеет свой вес w_k. Дуги также можно разделить на два типа: дуги, направленные от позиции к переходам, (p-t), и дуги, направленные от переходов к позициям (t-p). Исходя из этого, сеть Петри может быть формально представлена как совокупность множеств

$$N = (P, T, G, \Omega), \tag{4}$$

где $P = p_1, p_2...p_n$ - множество всех позиций (n - количество позиций); $T = t_1, t_2 \dots t_m$ - множество переходов (m - количество переходов), $G = (G_{p-t}, G_{t-p})$ - множество дуг сети; $G_{p-t} = (p \times t)$, $G_{t-p} = (t \times p)$-множества дуг, ведущих соответственно от переходов к позициям и от позиций к переходам; $\Omega = \omega_1, \omega_2...\omega_k$ - множество весов дуг (k - количество дуг).

Каждая позиция может быть маркирована, т.е. содержать некоторое число фишек. Если обозначить числа фишек, находящихся в i-й позиции p_1, как m_1, то маркировка всей сети будет выглядеть таким образом: $M = m_1, m_2...m_n$. Тогда полное определение сети Петри, включая данные о начальной маркировке, можно записать в виде

$$PN = (N, M_n), \tag{5}$$

где M_0 - начальная маркировка сети.

При оценке СЗИ АС и описании правил продукции с помощью сети Петри переходы интерпретируют собой логические предложения, соответствующие выполнению оценочных действий, входные позиции - оценки, выходные позиции - результат выполнения действий [1].

Формирование сети происходит следующим образом. Сначала формируется сеть верхнего уровня. Каждая секция правил представляется в виде перехода сетей Петри (СП), имеющего входные и выходные позиции. Затем аналогично проводится формирование подсетей нижнего уровня. Каждой секции правил ПС соответствует своя подсеть. Для этого сначала каждому правилу ставится в соответствие своя подсеть, переходу ставится в соответствие логическое выражение консеквента. Если в правилах доопределен результат его выполнения, то выходные позиции перехода будут соответствовать логическим переменным, входящим в выражение результата. Далее подсети правил объединяются в подсети секций путем определении порядка выполнения

подсетей правил и слиянии позиций, соответствующих одинаковым логическим переменным. Полученная таким образом сеть является иерархической, что позволяет уменьшить число ее состояний. Эта сеть используется для выявления параллельных процессов с целью описания каждой параллельной ветви в виде некоторого субавтомата. Для последовательных правил применяется следующий подход. Например, фокусирующему правилу вида

ЕСЛИ D_1 включен И D_2 включен, И D_3, ТО $K_1 = 0$ и $K_2 = 1$, РЕЗУЛЬТАТ: D_1 выключается, будет соответствовать подсеть, изображенная на с рисунке 1.

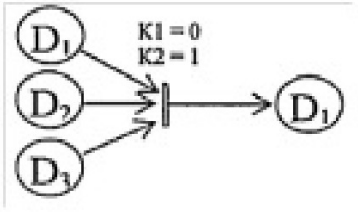

Рисунок 1. Фокусирующая подсеть

Здесь каждая входная переменная представляется в подсети одной или несколькими позициями. Данные позиции соединены друг с другом параллельно, имея общий выходной переход. Если антецедент не является дизъюнкцией нескольких термов, то в подсети, соответствующей правилу, имеет место только один переход, помеченный логическим выражением консеквента. Выходными позициями этого перехода являются позиции, соответствующие переменным, перечисленным в выражении результата [2].

Результирующая подсеть Петри получается путем объединения этих подсетей (рис. 2,г).

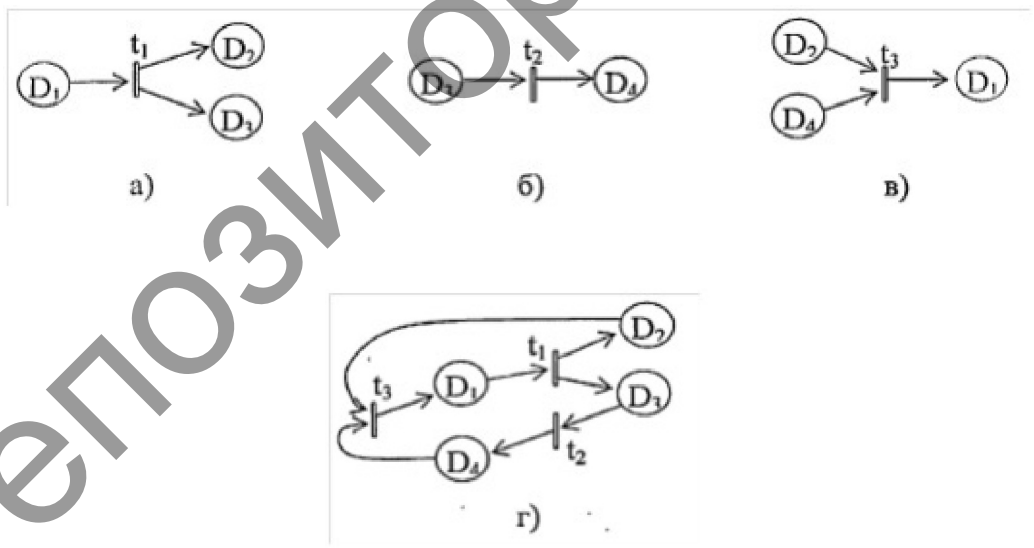

Рисунок 2. Результирующая подсеть

В получаемых сетях возможно появление параллельных ветвей и, следовательно, одновременно срабатываемых переходов (правил).

Во всех случаях, когда набор правил представляется набором простых правил, т.е. правил, в которых в <выражения> входят только операции «И» и «НЕ», количество переходов синтезируемой подсети равно количеству правил, а сама подсеть относится к классу маркированных графов.

Более сложные сети получаются, если в состав выражения входит операция «ИЛИ», т.е. имеют место А-правила, например:

ЕСЛИ<выражение 11> ИЛИ <выражение 12> ИЛИ...

ТО<выражение 21> ИЛИ <выражение 22> ИЛИ

РЕЗУЛЬТАТ <выражение 31> ИЛИ <выражение 32> ИЛИ. Рассмотрим отдельно 4 случая:

1. Элементарное правило (простое или разветвляющееся).

В этом случае мы имеем альтернативные управляющие действия. Однако, если все они имеют один и тот же результат, то на структуру подсети это не повлияет. Подсеть будет иметь такой же вид, как и в случае с простым МГ-правилом, только переходу будет соответствовать не конкретное действие, а несколько альтернативных действий.

2. Фокусирующее А-правило: ЕСЛИ <выражение 11> ИЛИ <выражение 12> ИЛИ..., ТО <выражение 2>, РЕЗУЛЬТАТ<выражение 3>.

Сеть Петри в этом случае имеет вид, изображенный на рисунке 3, т.е. кроме того, можно оптимизировать подсеть, то есть убрать позицию-условие p10. (рис. 4).

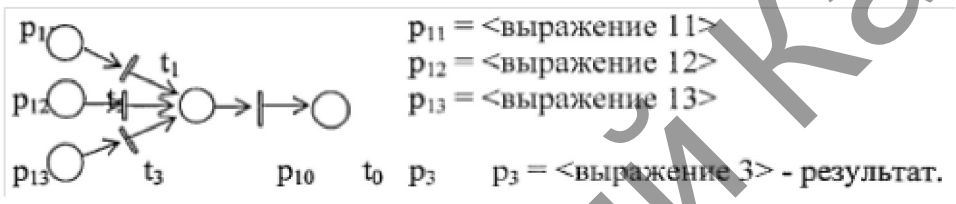

Рисунок 3. Вид фокусирующего А-правила

Или, если оптимизировать подсеть, то есть убрать позицию-условие p_{10} «в соответствии с рисунком 4»

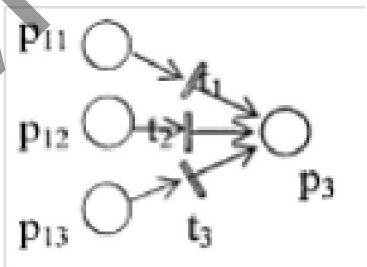

Рисунок 4. Оптимизированная подсеть

В этом случае всем переходам $t_1, t_2, t_3, ...$ будет соответствовать одно и то же действие, описанное в выражении 2.

3.Разветвляющееся А-правило.

Такому правилу соответствует ситуация, когда какое-либо действие имеет несколько вероятных последствий. Вид правила:

ЕСЛИ <выражение 1>, ТО <выражение 2>,

РЕЗУЛЬТАТ<выражение 31> ИЛИ выражение 32>, ИЛИ <выражение 33> ...
Этому правилу соответствует подсеть, изображенная на рисунке 5.

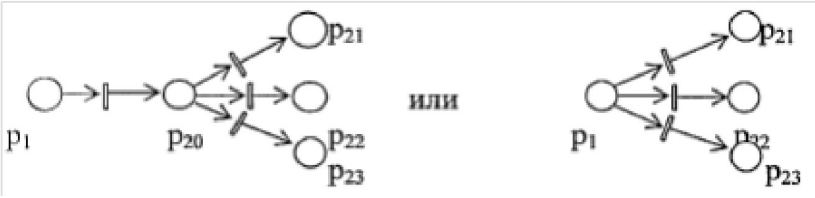

Рисунок 5. Вид фокусирующего А-правила

Здесь $p_1 =< 1 >$, $p_{21} =< 21 >$, $p_{22} =< 22 >$, $p_{23} =< 23 >$
1.ЕСЛИ<выражение 11> ИЛИ <выражение 12>ИЛИ <выражение 13> ...,
ТО <выражение 2>, РЕЗУЛЬТАТ<выражение 31> ИЛИ <выражение 32>
ИЛИ <выражение 33> ....

Далее для разрешения конфликтов используется метод запрета на изменения правил, по поводу которых возник конфликт. Предварительно представим структуру продукционной системы в виде иерархической сети Петри с дальнейшим анализом сети известными способами анализа живости.

Достоинством использования сетей Петри для разрешения конфликтов являются возможность моделирования ПС всех возможных типов с учетом возможных конфликтов между ними, высокая наглядность, возможность автоматизированного анализа, легкость перехода от одного уровня детализации описания продукционной системы к другому (за счет раскрытия/закрытия переходов)[3].

Список литературы

1 *Зегжда Д.П. и др.* Теория и практика обеспечения информационной безопасности. — М.: Яхтсмен, 2006.

2 *Зегжда Д.П., Ивашко А.М.* Как построить защищенную информационную систему. — СПб.: Мир и семья, 2007.

3 *Кобзарь М., Сидак А.* Методология оценки безопасности информационных технологий по общим критериям // Информационный бюллетень. — 2014. — № 6.

К.М.Сагиндыков, Г.Мусайф

Ақпаратты қорғау жүйесін бағалау үшін Петри желісін қолдану

Мақалада ақпаратты қорғау жүйесін бағалау үшін Петри желісін қолдану қарастырылды. Ақпараттық жүйеде ақпаратты қорғау құралы бастапқы ақпараттың сапасын бағалау әдісі үшін өнімнің моделін, бөлінген секциялар мен ішкі секциялар ұсынған өнімнің ережелерінде қолданылды.

K.M. Sagindykov, G. Mussaif

The use of Petri nets for the evaluation of information security systems

This article discusses the use of Petri nets to assess the security systems information. As initial information for the method of evaluation facilities of defence of information of the informative systems used productional model, which is a set divided into sections and subsections of production rules.

References

1 Zegzhda D.P. et.al. *The theory and practice of information security*, Moscow: Yachtsman, 2006.

2 Zegzhda D.P., Iwashko A.M. *How to build a secure information system*, Saint Petersburg: Mir i semya, 2007.

3 Kobzar M., Sidak A. *Bull. Info*, 2014, 6.