УДК 004.056

МОДЕЛИРОВАНИЕ ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ АППАРАТА СЕТЕЙ ПЕТРИ-МАРКОВА

В.В. Текунов, Ю.К. Язов

Отмечаются широкие возможности моделирования динамики реализации угроз безопасности информации с учетом наличия логических условий и параллелизма с использованием аппарата сетей Петри-Маркова. Дается краткая характеристика указанного аппарата, приводятся основные соотношения для расчета времен срабатывания логических условий в сети Петри-Маркова с логикой «И», «ИЛИ», «И-НЕ», «ИЛИ-НЕ». Приводятся соотношения для расчета показателя эффективности защиты информации в виде относительного времени реализации угроз без мер и с применением мер защиты.

Ключевые слова: моделирование, угрозы безопасности информации

Наличие параллелизма в процессах реализации угроз безопасности информации в информационных (ИС) и информационно-телекоммуникационных системах (ИТКС), а также логических условий, при которых такая реализация возможна, приводят к необходимости использования для моделирования аппарата сетей Петри-Маркова (СПМ) [1]. Наиболее полно применение этого аппарата для моделирования угроз безопасности информации в ИС и ИТКС описано в работах [2, 3]. Вместе с тем в них не показан порядок расчета времени срабатывания некоторых встречающихся в практике логических переходов (например, с логиками «И-НЕ», «ИЛИ-НЕ» и др.), когда вероятности срабатывания переходов не относятся к функциям распределения вероятностей. Отсутствие соотношений для таких расчетов не позволяет моделировать многие процессы реализации угроз и учитывать при оценке эффективности защиты информации фактор времени. В данной статье приводятся соотношения для расчета времени срабатывания указанных логических переходов в СПМ.

В общем случае СПМ – это множество $\Psi = \{\Pi, M\}$, где Π – сеть Петри, которая представляет собой двудольный граф вида:

$$\Pi = \{A, Z, O_A(Z), O_Z(A)\}, \quad (1)$$

где A, Z – множество позиций и переходов сети Петри, моделирующих динамику рассматриваемого процесса;

$O_A(Z)$ – входная функция переходов (выходная функция позиций), отображающая множество A во множество Z;

$O_Z(A)$ – входная функция позиций (выходная функция переходов), отображающая множество Z во множество A.

Динамика реализации угроз моделируется перемещением метки из начального состояния в конечное по сети Петри и описывается множеством $M = \{P, Q(t), Y\}$, где P – вектор вероятностей, описывающих возможность появления состояния процесса в начальный момент времени, $Q(t)$ – полумарковская матрица, характеризующая временные и стохастические параметры модели, Y – матрица логических условий, элементы которой определены в виде логической функции L с условиями срабатывания каждого логического перехода по полушагам, осуществляемым из состояний в рассматриваемый переход, при этом полушаг из позиции с номером $i(a)$ в переход с номером $j(z)$ обозначен как $S_{i(a),j(z)}$, a - означает принадлежность к позиции,

Текунов Василий Васильевич – ФАУ «ГНИИИ ПТЗИ ФСТЭК России», старший научный сотрудник, 8 (920) 401-93-70

Язов Юрий Константинович – ФАУ «ГНИИИ ПТЗИ ФСТЭК России», главный научный сотрудник, д-р техн. наук, профессор, 8 (903) 651-42-69

$$\upsilon_{i(a),j(z)} = \begin{cases} L[s_{1(a),j(z)},\ldots,s_{i(a),j(z)},\ldots s_{K(a),j(z)}], \text{ если } a_{i(a)} \in O_A(z_{j(z)}); \\ 0, \qquad \text{если } a_{i(a)} \notin O_A(z_{j(z)}). \end{cases} \quad (2)$$

а z - к переходу (далее полагается, что первый индекс определяет позицию, а второй – переход, и буквы a и z не указываются).

Полумарковская матрица представляет собой произведение матрицы вероятностей переходов $\{\pi_{ij}\}$ и матрицы плотностей вероятностей времен пребывания процесса в каждом i-м состоянии $\{f_{ij}(t)\}$, если считать, что сам переход происходит мгновенно, то есть:

$$Q(t) = \{\pi_{ij} \cdot f_{ij}(t)\}. \quad (3)$$

Таким образом, процесс реализации угрозы представляет собой последовательность перемещений, реализуемых в виде полушагов по СПМ, при этом СПМ пребывает в каждом состоянии некоторое случайное время, определенное соответствующей этому состоянию плотностью распределения вероятности для случайного времени пребывания, и затем выполняется полушаг и проверка логических условий переключения сети в следующее состояние. Последовательность состояний СПМ называется траекторией моделируемого процесса. Аналитическое описание процесса осуществляется, как и для обычных полумарковских процессов, в виде интегральных уравнений по траекториям перемещений из начального состояния в конечное.

Вероятность и плотность распределения времени перемещения из состояния i в переход j по траектории h определяется из соотношений (4) и (5).

$$\pi_{i,j}(h) = \prod_{d_h=1}^{D_h} \pi_{i+d_h,r+d_h}(h); \quad (4)$$

$$f_{i,j}(h,t) = f_{i,r}(h,t) * f_{i+1_h,r+1_h}(h,t) * \ldots * f_{i+d_h,r+d_h}(h,t) * \ldots * f_{i+D_h,r+D_h}(h,t), \quad (5)$$

где $f_{i+d_h,r+d_h}(h,t)$ – плотность вероятности времени перемещения по d_h полушагам по траектории h;

* – операция свертки [4].

Вероятность перемещения процесса из начального состояния i в переход j по траектории h определяется на основе решения системы интегральных уравнений обычного вида [5]:

$$\Phi_{ij}(h,t) = \pi_{ik} \cdot \int_0^t f_{ik}(h,\tau) \cdot \Phi_{kj}(h,t-\tau) \cdot d\tau \quad (6)$$

Так как в СПМ имеются переходы с логическими условиями, то СПМ разбивается на участки, соответствующие перемещениям (рис. 1) из начального состояния до первого логического перехода, между логическими переходами и после последнего логического перехода до конечного состояния.

Для каждого такого участка на основе решения системы интегральных уравнений рассчитывается вероятность перехода из начального участка траектории в конечный. Если по данной траектории имеются еще переходы с логическими условиями, то для них изложенная процедура повторяется.

Вероятность $\Phi_{i,j}(h,t)$, если j - номер последнего перехода, является, по сути, вероятностью реализации угрозы по траектории h. Если имеет место несколько траекторий, то вероятность реализации угрозы рассчитывается по формуле:

$$\Phi_{ij}(t) = 1 - \prod_{h \in H} [1 - \Phi_{ij}(h,t)], \quad (7)$$

где H - множество всех непересекающихся траекторий, по которым возможно перемещение процесса из начального в конечное состояние.

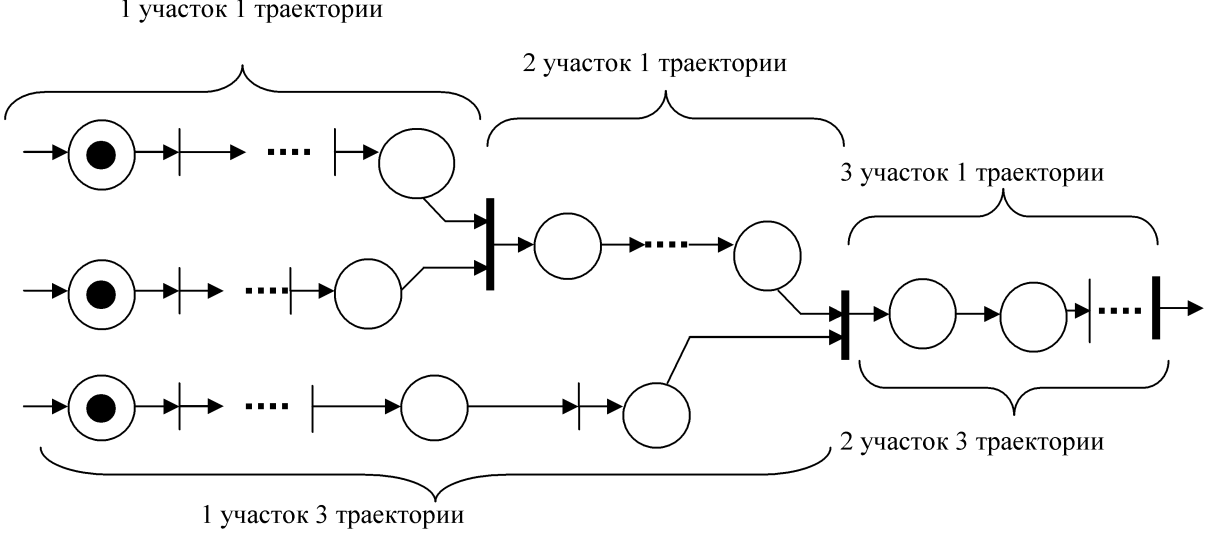


Рис. 1. Пример разбиения траекторий сети Петри-Маркова на участки

Как показано в [3], с весьма незначительными ошибками можно применять пуассоновское приближение для расчета вероятностей $\Phi_{ij}(h,t)$. Математическое ожидание времени срабатывания логического перехода может быть рассчитано обычным путем, если вероятность срабатывания перехода является функцией распределения. В частности для переходов «И» и «ИЛИ» соотношения для расчета указанных вероятностей и соответствующим им плотностей вероятностей имеют вид (8) и (9).

Для логики «И»:

$$\Phi_{\cap}(t) = \prod_{i=1}^{I} \Phi_{ij}(t) \quad \text{и}$$

$$f_{\cap}(t) = \sum_{i=1}^{I} f_{ij}(t) \cdot \frac{\prod_{i \in I} \Phi_{ij}(t)}{\Phi_{ij}(t)} \qquad (8)$$

Для логики «ИЛИ»:

$$\Phi_{\cup}(t) = 1 - \prod_{i=1}^{I} (1 - \Phi_{ij}(t)) \quad \text{и}$$

$$f_{\cup}(t) = \sum_{i=1}^{I} f_{ij}(t) \frac{\prod_{i=1}^{I} [1 - \Phi_{ij}(t)]}{1 - \Phi_{ij}(t)}, \qquad (9)$$

где I – количество входящих дуг в переход j.

Зная плотности распределения, нетрудно вычислить математические ожидания (табл. 1).

По-иному, поскольку результирующая вероятность срабатывания перехода не является функцией распределения, рассчитывается время срабатывания перехода, если в логическом условии присутствует условие «НЕ». Пусть имеет место переход с логикой «И-НЕ», с двумя входящими дугами, одна из которых соответствует условию «НЕ». При этом время перемещения по первой дуге распределено по экспоненциальному закону $f_1(t) = ae^{-at}$, а по второй дуге - по закону $f_2(t) = be^{-bt}$. Рассмотрим случайную величину $y=\tau_1/\tau_2$. Если $y<1$ к моменту времени t, то переход сработает. Плотность вероятности величины y в соответствии с [4] определяется следующим образом:

$$f_{\cap \not\subset}(y) = \frac{ab}{(b + ay)^2}. \qquad (10)$$

Характерно, что математическое ожидание для такой плотности вероятности бесконечно. Вероятность того, что будет выполняться условие $y<1$, определяется из соотношения:

$$P(y<1) = \int_0^1 f_{\cap \not\subset}(y)dy = \frac{a}{b+a} \quad \text{или}$$

Табл. 1

Соотношения для определения среднего времени срабатывания переходов с различными логическими условиями

Логическое условие	Общее соотношение для расчета математического ожидания времени срабатывания перехода	Соотношение для расчета математического ожидания времени срабатывания перехода для различного количества входящих дуг	Обозначения
«И» (процесс реализуется по всем входящим в переход дугам)	$\overline{\tau_u} = \int_0^{\infty} t \cdot \sum_{i=1}^{I} \frac{1}{\overline{\tau_i}} e^{-t \cdot \frac{1}{\overline{\tau_i}}} \cdot \prod_{j \neq i} (1 - e^{-t \cdot \frac{1}{\overline{\tau_j}}}) dt$	Для двух дуг: … $\overline{\tau_u} = \frac{\overline{\tau_1}^2 + \overline{\tau_1}\,\overline{\tau_2} + \overline{\tau_2}^2}{(\overline{\tau_1} + \overline{\tau_2})}$ …… Для трех дуг: $\overline{\tau_u} = \overline{\tau_1} + \overline{\tau_2} + \overline{\tau_3} + \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}} - \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}}} - \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_3}}} - \frac{1}{\frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}}$	$\overline{\tau_i}$ - средняя продолжительность срабатывания перехода по i-й дуге; I - количество входящих дуг в переходе, соответствует условию «И»; J - количество входящих дуг в переходе, по которым процесс не должен выполняться (соответствующих условию «НЕ»);
«И-НЕ» (время перемещения метки к переходу по всем дугам, соответствующим условию «И», меньше времен перемещенияпо дугам, соответствующим условию «НЕ»	$\overline{\tau_u} = \overline{\tau_I} \cdot (1 + \frac{\overline{\tau_J}}{\overline{\tau_J}})$ где $\overline{\tau_I}$ определяется по формулам для логического перехода «И» применительно к дугам соответствующим условию «И»; где $\overline{\tau_J}$ определяется по формулам для логического перехода «ИЛИ» применительно к дугам соответствующим условию «НЕ»	Для двух дуг, вторая из которых соответствует условию «НЕ» $\overline{\tau_u} = \overline{\tau_1} \cdot (1 + \frac{\overline{\tau_1}}{\overline{\tau_2}})$; Для трех дуг, первая и вторая из которых соответствует условию «И», а третья – условию «НЕ» $\overline{\tau_u} = \frac{\overline{\tau_1}^2 + \overline{\tau_1}\,\overline{\tau_2} + \overline{\tau_2}^2}{(\overline{\tau_1} + \overline{\tau_2})} \cdot (1 + \frac{\overline{\tau_1}^2 + \overline{\tau_1}\,\overline{\tau_2} + \overline{\tau_2}^2}{(\overline{\tau_1} + \overline{\tau_2}) \cdot \overline{\tau_3}})$	
«ИЛИ» (процесс реализуется хотя бы по одной из входящих дуг)	$\overline{\tau_u} = \frac{I}{\sum_{i=1}^{I} \frac{1}{\overline{\tau_i}}}$	Для двух дуг: $\overline{\tau_u} = \frac{\overline{\tau_1} \cdot \overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}}$ Для трех дуг: $\overline{\tau_u} = \frac{1}{\frac{1}{\overline{\tau_1}} + \frac{1}{\overline{\tau_2}} + \frac{1}{\overline{\tau_3}}}$	
«ИЛИ-НЕ» (процесс реализуется хотя бы по одной	$\overline{\tau_u} = \overline{\tau_I} \cdot (1 + \frac{\overline{\tau_J}}{\overline{\tau_J}})$	Для трех дуг, первая и вторая из которых соответствуют условию «ИЛИ», третья – условию «НЕ»	

Логическое условие	Общее соотношение для расчета математического ожидания времени срабатывания перехода	Соотношение для расчета математического ожидания времени срабатывания перехода для различного количества входящих дуг	Обозначения
дуге, входящей в условие «или», при этом метки по дугам, входящим в условие «НЕ» не подошли к логическому переходу)	где $\overline{\tau}_I$ определяется по формуле для логического перехода «ИЛИ» применительно к дугам соответствующим условию «ИЛИ» (индекс *I*); $\overline{\tau}_J$ определяется по формулам для логического перехода «И» применительно к дугам соответствующим условию «НЕ» (индекс *J*)	$$\overline{\tau}_u = \frac{\overline{\tau}_1 \cdot \overline{\tau}_2}{\overline{\tau}_1 + \overline{\tau}_2} \cdot \left(1 + \frac{\overline{\tau}_1 \cdot \overline{\tau}_2}{(\overline{\tau}_1 + \overline{\tau}_2) \cdot \overline{\tau}_3}\right)$$	
«И-ИЛИ» ((процесс реализуется по одной группе лугслогикой «И» или по другой группе дуг с логикой «И»)	$$\overline{\tau}_u = \int_0^\infty t \cdot \left\{ \begin{array}{l} \sum_{i=1}^{I} \frac{1}{\overline{\tau}_i} e^{-t \cdot \frac{1}{\overline{\tau}_i}} \cdot \prod_{k \neq i}^{I} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_k}}) + \\ \sum_{j=1}^{J} \frac{1}{\overline{\tau}_j} e^{-t \cdot \frac{1}{\overline{\tau}_j}} \cdot \prod_{k \neq i}^{J} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_k}}) + \\ \sum_{i=1}^{I} \frac{1}{\overline{\tau}_i} e^{-t \cdot \frac{1}{\overline{\tau}_i}} \cdot \prod_{k \neq i}^{I} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_k}}) \cdot \prod_{j=1}^{J} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_j}}) + \\ \sum_{j=1}^{J} \frac{1}{\overline{\tau}_j} e^{-t \cdot \frac{1}{\overline{\tau}_j}} \cdot \prod_{k \neq j}^{J} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_k}}) \cdot \prod_{i=1}^{I} (1 - e^{-t \cdot \frac{1}{\overline{\tau}_i}}) \end{array} \right\} dt$$ Для трех дуг (первая и вторая или третья) $$\overline{\tau}_u = \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_3}} + \frac{1}{\frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3}} - \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3}}$$ Для четырех дуг (первая и вторая или третья и четвертая) $$\overline{\tau}_u = \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_3}} + \frac{1}{\frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3}} + \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_4}} + \frac{1}{\frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_4}} - \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3}} - \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_4}} - \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_3} + \frac{1}{\overline{\tau}_4}} - \frac{1}{\frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3} + \frac{1}{\overline{\tau}_4}} + \frac{1}{\frac{1}{\overline{\tau}_1} + \frac{1}{\overline{\tau}_2} + \frac{1}{\overline{\tau}_3} + \frac{1}{\overline{\tau}_4}}$$	I – количество входящих дуг первой группы в переходе, соответствующих условию «И»; J – количество входящих дуг второй группы в переходе, соответствующих условию «И»

$$P(\tau_1 < \tau_2) = \frac{\tau_2}{\tau_1 + \tau_2}. \quad (11)$$

Тогда для двух дуг среднее время срабатывания рассматриваемого логического перехода может быть определено как:

$$\overline{\tau_{пер}} \approx \frac{\overline{\tau_1}}{P(\tau_1 < \tau_2)} = \overline{\tau_1} \cdot \left(1 + \frac{\overline{\tau_1}}{\overline{\tau_2}}\right). \quad (12)$$

Аналогичным образом определяется время срабатывания перехода с логикой «ИЛИ-НЕ». Формулы для расчета времени срабатывания наиболее широко встречаемых логических переходов «ИЛИ», «И», «И-НЕ», «ИЛИ-НЕ» приведены в табл. 1.

Для проверки соответствия результатов расчетов по выведенным соотношениям реальным временам срабатывания логических переходов была разработана специальная программа экспериментальных исследований, с помощью которой было определено, что абсолютное отклонение расчетных значений от экспериментальных составило в среднем:

для перехода с логикой «И» около 3,3%;

для перехода с логикой «ИЛИ» менее 2,7%;

для перехода с логикой «И-НЕ» менее 3,7%;

для перехода с логикой «ИЛИ-НЕ» менее 11%;

для перехода с логикой «И-ИЛИ» менее 1%.

Таким образом, результаты эксперимента подтвердили правильность теоретических расчетов.

Рассмотрим пример применения данного аппарата для моделирования динамики реализации угроз безопасности информации.

Пример. Пусть в ИС, имеющей выход в сеть общего пользования, существует угроза хищения информации, хранимой на сервере базы данных в составе ИС. Угроза реализуется путем инфицирования файлового сервера ИС вредоносной программой. Рассмотрим случай, когда в ИС отсутствуют средства антивирусной защиты. СПМ, моделирующая процесс хищения информации, для этого случая приведена на рис. 2.

В этой сети, должны выполняться условия:

$$\sum_{n=1}^{N} \pi_n = 1, \quad \sum_{n=N+1}^{2N} \pi_n = 1. \quad (13)$$

Если все порты равнозначны, то $\pi_n = \frac{1}{N}$.

Среднее время реализации угрозы определяется следующим образом:

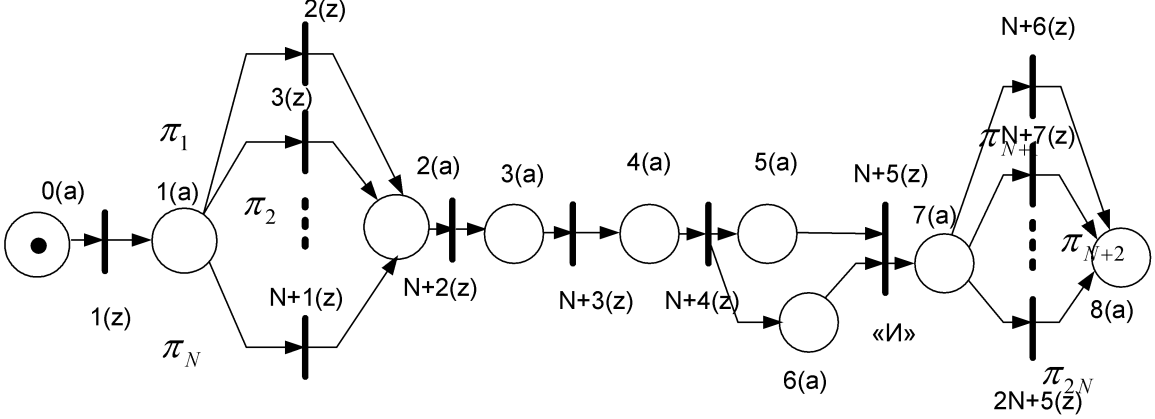
$$\overline{\tau_u} = \overline{\tau_{0,N+4}} + \frac{\overline{\tau_{5,N+5}}^2 + \overline{\tau_{5,N+5}} \cdot \overline{\tau_{6,N+5}} + \overline{\tau_{6,N+5}}^2}{\overline{\tau_{5,N+5}} + \overline{\tau_{6,N+5}}} + \frac{1}{\sum_{n=N+6}^{2N+5} \frac{\pi_n}{\overline{\tau_{7,n}}}}; \quad (14)$$

$$\overline{\tau_{0,N+4}} = \overline{\tau_{0,1}} + \frac{1}{\sum_{n=2}^{N+1} \frac{\pi_n}{\overline{\tau_{1,n}}}} + \overline{\tau_{2,N+2}} + \overline{\tau_{3,N+3}} + \overline{\tau_{4,N+4}}. \quad (15)$$

где $\overline{\tau_{0,N+4}}$ – среднее время срабатывания перехода *N+4(z),* которое определяется по формуле (15). Если не имеет значения, какой из портов выбирается для атаки, и это не влияет на время ее реализации, то:

Рассмотрим случай, когда для защиты от вредоносных программ установлены антивирусные средства

$$\overline{\tau_{0,N+4}} = \overline{\tau_{0,1}} + \overline{\tau_{1,n}} + \overline{\tau_{2,N+2}} + \overline{\tau_{3,N+3}} + \overline{\tau_{4,N+4}}; \quad (16)$$



0(a) – начальное состояние, когда ИС функционирует, включены файловый сервер и сервер базы данных;
1(a) – инициирован (нарушителем или вредоносной программой) процесс выявления открытых портов, по которым может быть получен доступ к файловому серверу ИС;
2(a) – получен удаленный доступ по одному из *N* портов к файловому серверу ИС;
3(a) – файловый сервер инфицирован вредоносной программой;
4(a) – активирована вредоносная программа на файловом сервере, запрос на нужную информацию с файлового сервера поступил на сервер базы данных;
5(a) – вредоносная программа на файловом сервере готова к приему и распаковке пакетов, поступающих с сервера базы данных;
6(a) – сервер базы данных начал подготовку к передаче нужной нарушителю информации на файловый сервер;
7(a) – похищенная информация записана в выбранные участки постоянной памяти;
8(a) – похищенная информация передана по одному из *N* портов на компьютер нарушителя в составе внешней сети, угроза реализована;
1(z) – подготовка действий по поиску открытых портов на рабочих станциях ИС;
2(z) – N+1(z) – выявляются открытые порты в ИС;
N+2(z) – вредоносная программа перемещается (записывается) на файловый сервер;
N+3(z) – активация вредоносной программы и передача запроса на подлежащую похищению информацию с файлового сервера на сервер базы данных;
N+4(z) – нужная нарушителю информация передается на файловый сервер;
N+5(z)–нужная нарушителю информация поступает на файловый сервер и перехватывается вредоносной программой, копируется и записывается в выбранные участки постоянной памяти;
N+6(z) - 2N+5(z) – нужная нарушителю информация передается на компьютер нарушителя во внешней сети по одному из открытых портов (не обязательно по тому, по которому был инфицирован файловый сервер);

π_i – вероятность того, что выявлен *i*-й порт, или вероятность того, что выбран *i*-й порт для передачи похищенной информации во внешнюю сеть

Рис. 2. Сеть Петри-Маркова, моделирующая процесс реализации угрозы хищения информации с сервера базы данных путем внедрение вредоносной программы на файловый сервер

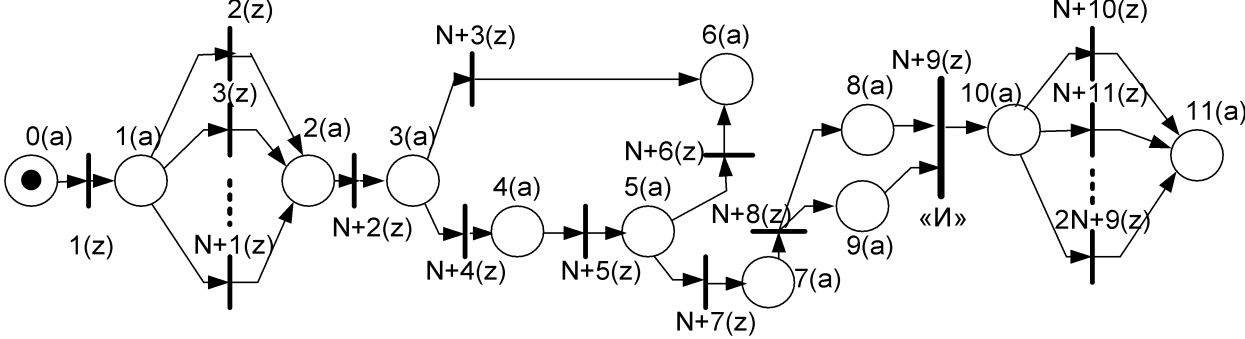
на периметре ИС и на файловом сервере. При этом другие меры защиты не рассматриваются.

СПМ, моделирующая процесс реализации угрозы хищения информации путем внедрение вредоносной программы на файловый сервер при использовании для защиты антивирусных средств, приведена на рис. 3.

Для этой сети должны выполняться условия (17) и (18).

$$\sum_{i=1}^{N}\pi_i = 1, \pi_{N+1} + \pi_{N+2} = 1, \pi_{N+3} + \pi_{N+4} = 1, \sum_{i=N+5}^{2N+5}\pi_i = 1 \ ; \qquad (17)$$

$$\sum_{i=1}^{N}\pi_i = 1, \pi_{N+1} + \pi_{N+2} = 1, \pi_{N+3} + \pi_{N+4} = 1, \sum_{i=N+5}^{2N+5}\pi_i = 1 \ . \qquad (18)$$



0(a) – начальное состояние, когда ИС функционирует;

1(a) – инициирован (нарушителем или вредоносной программой) процесс выявления открытых портов, по которым может быть получен доступ к файловому серверу;

2(a) – на антивирусное средство в составе межсетевого экрана или прокси-сервера ИС поступило инфицированное сообщение из внешней сети;

3(a) – запущен антивирусный сканер, начата проверка сообщения;

4(a) – с вероятностью π_{N+1} антивирусным средством в составе межсетевого экрана (прокси-сервера) пропущена вредоносная программа, получен доступ к файловому серверу;

5(a) – на файловый сервер поступило инфицированное сообщение и начата его проверка собственным антивирусным средством;

6(a) – с вероятностью π_{N+2} антивирусным средством в составе межсетевого экрана (прокси-сервера) или с вероятностью π_{N+4} антивирусным средством в составе файлового сервера выявлено наличие вредоносной программы, сообщение блокировано, атака сорвана;

7(a) – на файловом сервере с вероятностью π_{N+3} пропущена вредоносная программа, файловый сервер инфицирован вредоносной программой, вредоносная программа активирована и запрос на нужную информацию с файлового сервера поступил на сервер базы данных;

8(a) – вредоносная программа на файловом сервере, она готова к приему запрошенной информации;

9(a) – сервер базы данных передал информацию на файловый сервер;

10(a) – похищенная информация записана в выбранные участки постоянной памяти;

11(a) – похищенная информация передана по одному из *N* портов на компьютер нарушителя в составе внешней сети, угроза реализована;

1(z) – подготовка действий по поиску открытых портов на рабочих станциях ИС;

2(z) – N+1(z) – выявляются открытые порты в ИС;

N+2(z) – сообщение с вредоносной программой поступает на межсетевой экран (прокси-сервер), записывается в буфер и подается команда на запуск антивирусного сканера;

N+3(z) – выявляется и блокируется вредоносная программа в межсетевом экране (прокси-сервере);

N+4(z) – сообщение с вредоносной программой передается на файловый сервер;

N+5(z) – осуществляется проверка сообщения собственным антивирусным сканером файлового сервера;

N+6(z) – с вероятностью π_{N+4} вредоносная программа обнаруживается и блокируется;

N+7(z) – с вероятностью π_{N+3} сообщение с вредоносной программой записывается на файловый сервере;

N+8(z) – активация вредоносной программы и передача запроса на передачу нужной информации на сервер базы данных;

N+9(z) – похищаемая информация поступает на файловый сервер и считывается вредоносной программой;

N+10(z)- 2N+9(z) – похищенная информация передается во внешнюю сеть на компьютер нарушителя по одному из открытых портов (не обязательно по тому, по которому был инфицирован файловый сервер)

Рис. 3. Сеть Петри-Маркова, моделирующая процесс реализации угрозы хищения информации с сервера базы данных путем внедрение вредоносной программы на файловый сервер при наличии антивирусных средств защиты

Среднее время реализации угрозы хищения УП путем внедрение вредоносной программы на файловый сервер при использовании для защиты антивирусных средств с учетом формул табл. 1 определяется из соотношения (19).

$$\overline{\tau_u} = \overline{\tau_{0,N+9}} + \frac{1}{\sum_{n=N+10}^{2N+9} \frac{\pi_n}{\overline{\tau_{10,n}}}} \quad ; \qquad (19)$$

$$\overline{\tau_{0,N+9}} = \overline{\tau_{0,N+8}} + \frac{\overline{\tau_{8,N+9}}^2 + \overline{\tau_{8,N+9}} \cdot \overline{\tau_{9,N+9}} + \overline{\tau_{9,N+9}}^2}{\overline{\tau_{8,N+9}} + \overline{\tau_{9,N+9}}} \quad ; \qquad (20)$$

$$\overline{\tau_{0,N+8}} = \overline{\tau_{0,1}} + \frac{1}{\sum_{n=2}^{N+1} \frac{\pi_n}{\overline{\tau_{1,n}}}} + \overline{\tau_{2,N+2}} + \frac{1}{\pi_{N+1}} \overline{\tau_{3,N+4}} + \overline{\tau_{4,N+5}} + \frac{1}{\pi_{N+3}} \overline{\tau_{5,N+7}} + \overline{\tau_{7,N+8}} \; . \qquad (21)$$

Если не имеет значения, какой из портов выбирается для атаки, и это не влияет на время ее реализации, то среднее время реализации угрозы может быть рассчитано из соотношений (22) и (23).

$$\overline{\tau_u} = \overline{\tau_{0,N+9}} + \overline{\tau_{10,n}} \quad ; \qquad (22)$$

$$\overline{\tau_{0,N+9}} = \overline{\tau_{0,1}} + \overline{\tau_{1,n}} + \overline{\tau_{2,N+2}} + \frac{1}{\pi_{N+1}} \overline{\tau_{3,N+4}} + \overline{\tau_{4,N+5}} + \frac{1}{\pi_{N+3}} \overline{\tau_{5,N+7}} + \overline{\tau_{7,N+8}} + \frac{\overline{\tau_{8,N+9}}^2 + \overline{\tau_{8,N+9}} \cdot \overline{\tau_{9,N+9}} + \overline{\tau_{9,N+9}}^2}{\overline{\tau_{8,N+9}} + \overline{\tau_{9,N+9}}} \; , \qquad (23)$$

где n – номер выбранного с вероятностью π_n порта;

$\overline{\tau_{1,n}}, \overline{\tau_{10,n}}$ – среднее время передачи сообщений с компьютера нарушителя на файловый сервер и с файлового сервера на компьютер нарушителя по n-му порту соответственно.

Эффективность применения антивирусных средств может оцениваться по относительному показателю:

$$\eta_{отн} = 1 - \frac{\overline{\tau_u^{(0)}}}{\overline{\tau_u^{(ЗИ)}}}, \; \overline{\tau_u^{(ЗИ)}} \geq \overline{\tau_u^{(0)}} \; , \qquad (24)$$

где $\overline{\tau_u^{(0)}}$ и $\overline{\tau_u^{(ЗИ)}}$ - времена реализации угрозы без применения и с применением средств защиты соответственно.

В предположении, что все времена срабатывания переходов примерно равны $\overline{\tau}$, время анализа программ вредоносной программы - $\overline{\tau_{ВП}}$, а вероятность выбора открытого порта одинакова для всех портов, зависимость показателя эффективности от существенных параметров в графическом виде - приведены на рис. 4 и 5.

Таким образом, математическое моделирование процессов реализации угроз безопасности информации с использованием аппарата СПМ позволяет учесть фактор времени, параллелизм этих процессов, логические условия реализации угроз, оценивать эффективность защиты информации на основе сравнения времен реализации угроз без применения и с применением средств защиты и тем самым не только перейти к количественным оценкам возможности реализации угроз безопасности информации, но и значительно повысить наглядность достигаемого эффекта защиты.

Литература

1. Игнатьев В.М., Ларкин Е.В. Сети Петри-Маркова. Тула: ТулГТУ, 1994.

2. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Пособие. – Воронеж: Кварта, 2015.- 440 с.

3. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. 274 с.: ил.

4. В. Феллер. Введение в теорию вероятностей и ее приложения. Т.2. Изд-во «МИР», М.,1967.

5. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. Изд., пер. и доп. М.: Наука, Глав. ред. физ.-математ. литературы, 1987.

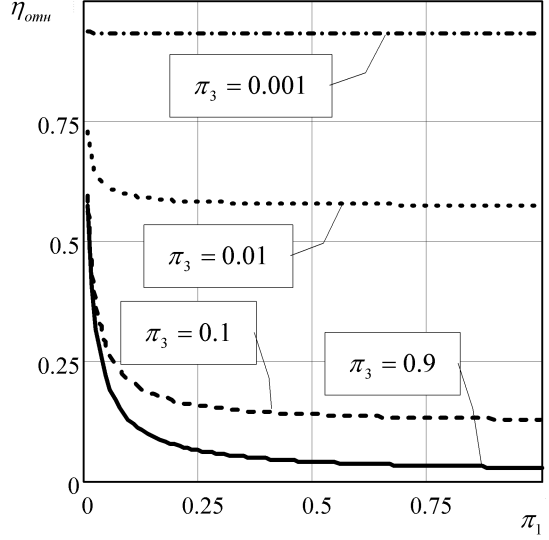


Рис. 4. Зависимости эффективности применения антивирусных средств от вероятностей пропуска вредоносных программ антивирусными средствами на периметре ИС (π_1) и в файловом сервере (π_3) при отношении $\frac{\overline{\tau_{ВП}}}{\overline{\tau}} = 0{,}1$

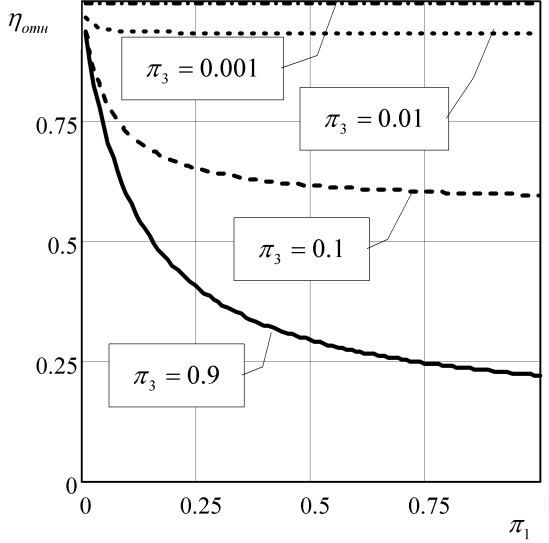


Рис. 5. Зависимости эффективности применения антивирусных средств от вероятностей пропуска вредоносных программ на периметре ИС (π_1) и в файловом сервере (π_3) при отношении $\frac{\overline{\tau_{ВП}}}{\overline{\tau}} = 1$

ФАУ «Государственный научно-исследовательский испытательный
институт проблем технической защиты информации
Федеральной службы по техническому и экспортному контролю»
State Science and Research Experimental Institute of Technical information protection problems
of Federal Service for Technical and Export Control

MODELING THE DYNAMICS OF THE IMPLEMENTATION OF INFORMATION SECURITY THREATS USING THE APPARATUS PETRI-MARKOV NETS

V.V. Tekunov, U.K. Yazov

There have been opportunities of modeling the dynamics implementation of the information security risks, taking into account the availability of logical conditions and parallelism using apparatusPetri-Markovnets. A brief description of said apparatus are the main correlation to calculate the response time of the logic conditions in the Petri-Markov network logic «AND», «OR», «AND-NOT», «NOR». It is proposed to measure the effectiveness of information security in the form of a relative time realization threats without measures and with the use of protective measures and given the calculation

Key words: modeling, information security threats