

СОСТАВНЫЕ СЕТИ ПЕТРИ-МАРКОВА СО СПЕЦИАЛЬНЫМИ УСЛОВИЯМИ ПОСТРОЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Язов Ю. К.¹, Панфилов А. П.²

DOI: 10.21681/2311-3456-2024-2-53-65

Цель исследования состоит в расширении аппарата составных сетей Петри-Маркова в интересах обеспечения возможности моделирования разрешений, запретов и приоритетов срабатывания логических переходов с учетом фактора времени при моделировании угроз безопасности информации в информационных системах.

Методами проведения исследования являются математический аппарат теории вероятностей, теории марковских и полумарковских процессов, теории случайных потоков событий и математический аппарат составных сетей Петри-Маркова.

В результате исследования показана необходимость расширения аппарата составных сетей Петри-Маркова за счет использования ингибиторных дуг и установления приоритетов в таких сетях в интересах введения логических условий, касающихся запретов, разрешений и приоритетов срабатывания переходов в сетях, моделирующих процессы реализации угроз безопасности информации в информационных системах.

Получены аналитические соотношения для расчета вероятностно-временных характеристики процессов срабатывания логических переходов с пропозициональной логикой срабатывания типа «И», «ИЛИ», «И-НЕ», «ИЛИ-НЕ», «И-ИЛИ», «XOR» в случае наличия в этих переходах разрешающих и запрещающих дуг при детерминированном и случайном времени разрешения или запрета соответственно.

Показано, каким образом вводятся и выполняются приоритеты срабатывания переходов в составных сетях Петри-Маркова, построенных на основе марковских и полумарковских процессов. Получены аналитические соотношения для расчета вероятностно-временных характеристик срабатывания переходов с приоритетами.

Приведены примеры расчета математического ожидания и вероятности срабатывания переходов в составных сетях Петри-Маркова с ингибиторными дугами со случайным и детерминированным временами запрета (разрешения) и с приоритетами.

Научная новизна статьи состоит в том, что в ней впервые предложены и описаны приемы введения в составные сети Петри-Маркова запретов и разрешений на срабатывание переходов в этих сетях, а также установления приоритетов на такие срабатывания, что существенно расширяет возможности моделирования процессов реализации угроз безопасности информации в информационных системах.

Ключевые слова: информационная система, процесс, вероятность, модель, логический переход, логическое условие, ингибиторная дуга, приоритет.

COMPOSITE PETRI-MARKOV NETWORKS WITH SPECIAL CONSTRUCTION CONDITIONS FOR MODELING INFORMATION SECURITY THREATS

Yazov Yu. K.³, Panfilov A. P.⁴

The goal of article: is to extend the apparatus of composite Petri–Markov networks in the interests of providing the possibility of modeling permissions, prohibitions and priorities to actuate logical transitions taking into account the time factor in modeling of information security threats in information systems.

- 1 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail: yazoff_1946@mail.ru
- 2 Панфилов Андрей Павлович, начальник отдела Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail: panfilov@gniii.ru
- 3 Yuri K. Yazov, Dr.Sc., Professor, Chief Researcher of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russian Federation. E-mail: yazoff_1946@mail.ru
- 4 Andrey P. Panfilov, Head of Department of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russian Federation. E-mail: panfilov@gniii.ru

The method of research: is the mathematical apparatus of probability theory, the theory of Markov and Semi-Markov processes, the theory of random streams of events and the mathematical apparatus of composite Petri–Markov networks.

The result of the research: the research shows the necessity of extending the apparatus of composite Petri–Markov networks by using inhibitory arcs and setting priorities in such networks in order to introduce logical conditions concerning prohibitions, permissions and priorities of triggering transitions in networks modeling processes of implementing information security threats in information systems.

Analytical relationships were obtained to calculate the probabilistic-temporary characteristics of triggering processes of logic with propositional logic of triggering of the type «AND», «OR», «AND-NOT», «OR-NOT», «AND-OR», «GOOD» in these transitions at random and deterministic times of permission or prohibition respectively.

It is shown how the priorities of triggering transitions in composite Petri-Markov networks are introduced and implemented, based on Markov and semi-Markov processes. Analytical relations were obtained to calculate the probabilistic-temporary characteristics of triggering transitions with priorities.

Examples of calculation of mathematical expectation and probability of triggering transitions in composite Petri-Markov networks with inhibitory arcs with random and deterministic times of prohibition (permission) and with priorities are given.

Scientific novelty: for the first time, this article offers and describes the methods of introduction in composite Petri-Markov networks of prohibitions and permissions to actuate transitions in these networks, and to establish priorities on such triggering, that essentially extends possibilities in modeling processes of implementing information security threats in information systems.

Keywords: information system, process, probability, model, logical transition, logical condition, inhibitory arc, priority.

Введение

Аппарат составных сетей Петри-Маркова (ССПМ) был предложен в [1] для моделирования динамики реализации угроз безопасности информации в информационных системах (ИС) и, в отличие от аппарата сетей Петри, позволяет оценивать вероятностно-временные характеристики процесса их реализации, а в отличие от традиционного аппарата сетей Петри-Маркова⁵, учитывать не только параллельность выполняемых парциальных процессов, но и наличие различных логических условий их реализации. Возможности этого аппарата постоянно расширяются, например, за счет использования в нем нечетких оценок вероятностно-временных характеристик процессов реализации угроз в ИС при наличии неопределенности сведений о них [2, 3], использования предикатов для задания логических условий [4–8] и т.д. Вместе с тем еще в конце прошлого века в целом ряде работ⁶ и в последние годы были предложены многочисленные расширения как аппарата сетей Петри, так и традиционного аппарата сетей Петри-Маркова, касающиеся использования раскрашенных (цветных) сетей [9, 10], введения приоритетов для дуг и переходов, создания так называемых самомодифицируемых и иерархических сетей Петри [10–12], применения нечетких сетей [13, 14],

использования ингибиторных дуг [15] и т.д. Введение таких расширений для аппарата ССПМ существенно повышает возможности моделирования, в частности, позволяет корректно вводить дополнительные условия срабатывания ССПМ, которые могут иметь место в процессах реализации угроз безопасности информации в ИС. Однако, при этом необходимо определить, каким образом рассчитывать вероятностно-временные характеристики срабатывания ССПМ, построенных на основе марковских и полумарковских процессов [1, 2] и модифицированных с применением указанных расширений.

Данная статья посвящена разработке аналитических соотношений, позволяющих рассчитывать вероятностно-временные характеристики срабатывания логических переходов ССПМ, в которых, во-первых, применяются ингибиторные дуги, а, во-вторых, устанавливаются приоритеты срабатывания переходов.

1. Составные сети Петри-Маркова с ингибиторными дугами

Ингибиторные дуги впервые были введены Аджервалой и Флинном⁷ для проверки сетей Петри на нулевую разметку. Ингибиторная дуга в традиционном понимании соединяет входную позицию, имеющую нулевую разметку, с переходом, в который помимо нее входит обычная дуга. При этом, если ингибиторная дуга является разрешающей, то данный

5 Игнатъев, В. М. Сети Петри-Маркова/ В. М. Игнатъев, Е. В. Ларкин. –Тула: ТулГУ, 1994, 163 с.

6 Например, изложенные в работе: Котов, В. Е. Сети Петри/ В. Е. Котов. – М.: Издательство «Наука», Главная редакция физико-математической литературы, 1984.

7 Agerwala T., Flynn M. Comments on capabilities, limitations and «correctness» of Petri nets. – In: Proc. of First Annual Symposium on Computer Architecture. New York, 1973, p. 81–86.

переход может сработать только в случае, если в позиции, из которой исходит ингибиторная дуга, появится метка (фишка) (рисунок 1).

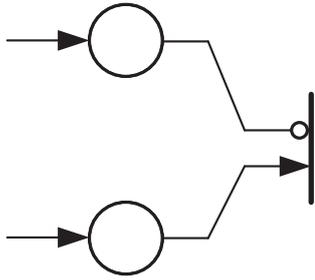


Рисунок 1. Пример сети Петри с ингибиторной дугой

Если же ингибиторная дуга является запрещающей, то переход не сработает после появления метки в позиции, инцидентной ингибиторной дуге.

В отличие от обычной дуги ингибиторная заканчивается кружком. Ингибиторная дуга может быть использована аналогичным образом в ССПМ, то есть для разрешения или запрещения срабатывания инцидентного ей перехода. Время появления условия срабатывания перехода (прихода метки по ингибиторной дуге) может быть как случайным, так и неслучайным (детерминированным). Ингибиторная дуга может применяться и в простых, и в логических переходах ССПМ. Однако в простых переходах при детерминированном времени появления условия срабатывания перехода вероятность срабатывания будет равна вероятности того, что по обычной дуге процесс подойдет к простому переходу после получения им по ингибиторной дуге разрешения на срабатывание, если эта ингибиторная дуга является разрешающей, или до поступления запрета на срабатывание перехода, если ингибиторная дуга является запрещающей. Расчет таких вероятностей не представляет никакой сложности. Если ингибиторная дуга является разрешающей и время разрешения определяется детерминированной величиной t_0 , то вероятность срабатывания перехода при экспоненциальном приближении [1, 10] рассчитывается по формуле:

$$P(t) = \begin{cases} 1 - \exp\left[-(t - t_0)/\bar{\tau}\right], & \text{если } t > t_0, \\ 0, & \text{если } t \leq t_0, \end{cases} \quad (1)$$

где $\bar{\tau}$ – математическое ожидание времени поступления на простой переход парциального потока.

Если ингибиторная дуга является запрещающей, и время запрета определяется детерминированной величиной t_0 , то вероятность срабатывания перехода рассчитывается по формуле:

$$P(t) = \begin{cases} 1 - \exp\left[-t/\bar{\tau}\right], & \text{если } t \leq t_0, \\ 0, & \text{если } t > t_0, \end{cases} \quad (2)$$

При случайном времени разрешения t_0 простой переход сработает, если случайная величина τ поступления потока на переход будет больше случайного времени поступления метки по ингибиторной дуге t_0 . Тогда для расчета используется усредненная по времени вероятность [1, 2]:

$$\overline{P(t_0 < \tau)} = \int_0^\infty P(t_0 < \tau) f_0(t_0) dt_0 = \bar{t}_0 / (\bar{t}_0 + \bar{\tau}). \quad (3)$$

С этой усредненной по времени вероятностью парциальный поток, входящий в переход, будет прореживаться, и математическое ожидание времени того, что рассматриваемый простой переход с разрешающей ингибиторной дугой сработает, рассчитывается из соотношения:

$$\bar{\tau}^{(p)} = \bar{\tau} \cdot \left(1 + \bar{\tau}/t_0\right). \quad (4)$$

Вероятность срабатывания перехода с логикой «И» с разрешающей ингибиторной дугой при экспоненциальном приближении рассчитывается следующим образом:

$$P_\wedge(t) = 1 - \exp\left(-t/\tau_\wedge^{(p)}\right). \quad (5)$$

Для логических переходов для расчета вероятностно-временных характеристик используется аналогичный подход.

Пусть имеет место логический переход с логикой «И» и разрешающей его срабатывание с момента времени t_0 ингибиторной дугой (рисунок 2), при этом время t_0 может быть детерминированным или случайным.

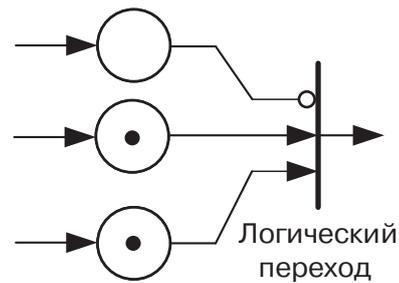


Рисунок 2. Пример логического перехода, на который поступают два входящих потока и имеется ингибиторная дуга

Вероятностно-временные характеристики срабатывания такого логического перехода «И» при двух входящих обычных дугах (двух входящих парциальных потоках) определяются следующим образом. При детерминированном поступлении метки по разрешающей ингибиторной дуге вероятность того, что ко времени t_0 оба парциальных потока событий поступят на логический переход и при этом время

поступления обоих потоков будет меньше t_0 , определяется из соотношения:

$$P_{\wedge}^{(p)}(t) = \begin{cases} P_1(t-t_0) \cdot P_2(t-t_0), & \text{если } t > t_0, \\ 0, & \text{если } t \leq t_0, \end{cases} \quad (6)$$

где $P_1(t-t_0)$, $P_2(t-t_0)$ – вероятности того, что парциальные процессы по первой и второй дуге соответственно поступят на переход после времени t_0 и в течение времени $t-t_0$.

При пуассоновских входящих парциальных потоках поток срабатываний перехода «И» очень близок к пуассоновскому и при детерминированном поступлении метки по разрешающей ингибиторной дуге вероятность срабатывания перехода определяется по формуле:

$$P_{\wedge}^{(p)}(t) = \begin{cases} 1 - \exp\left[-(t-t_0)/\bar{\tau}_{\wedge}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases} \quad (7)$$

где $\bar{\tau}_{\wedge}$ – математическое ожидание времени прихода на логический переход как первого, так и второго парциального процесса (соответствует срабатыванию логического перехода с логикой «И» [1]),

$$\bar{\tau}_{\wedge} = \frac{\bar{\tau}_1^2 + \bar{\tau}_1 \cdot \bar{\tau}_2 + \bar{\tau}_2^2}{\bar{\tau}_1 + \bar{\tau}_2}. \quad (8)$$

Если метка по разрешающей ингибиторной дуге поступает в случайное время t_0 , то по аналогии с соотношениями (3) и (4) сначала рассчитывается усредненная по времени вероятность того, что время прихода к логическому переходу двух парциальных потоков будет больше времени прихода метки по разрешающей ингибиторной дуге:

$$\overline{P(t_0 < \tau_{\wedge})} = \int_0^{\infty} P(t_0 < \tau_{\wedge}) f_0(t_0) dt_0 = \bar{t}_0 / (\bar{t}_0 + \bar{\tau}_{\wedge}). \quad (9)$$

С этой вероятностью входящий в переход поток, определяемый логическим условием «И» (когда поступил на переход и первый, и второй поток), будет прожигаться, и математическое ожидание времени того, что рассматриваемый логический переход срабатывает для разрешающей ингибиторной дуги, рассчитывается по формуле [1, 2]:

$$\bar{\tau}_{\wedge}^{(p)} = \bar{\tau}_{\wedge} \cdot \left(1 + \bar{\tau}_{\wedge} / \bar{t}_0\right). \quad (10)$$

В этом случае для расчета вероятности срабатывания перехода с логикой «И» с ингибиторной дугой при случайном времени поступления метки по ней может быть использовано соотношение:

$$P_{\wedge}^{(p)}(t) = 1 - \exp\left(-t / \bar{\tau}_{\wedge}^{(p)}\right). \quad (11)$$

Таковыми же рассуждениями можно показать, что если ингибиторная дуга является запрещающей, то при детерминированном времени поступления метки по ней:

$$P_{\wedge}^{(s)}(t) = \begin{cases} 1 - \exp\left[-t / \bar{\tau}_{\wedge}\right] & \text{нпу } t \leq t_0; \\ 0 & \text{нпу } t > t_0, \end{cases} \quad (12)$$

где $\bar{\tau}_{\wedge}$ рассчитывается по формуле (8).

При случайном времени поступления метки по запрещающей ингибиторной дуге:

$$P_{\wedge}(t) = 1 - \exp\left(-t / \bar{\tau}_{\wedge}^{(s)}\right). \quad (13)$$

где $\bar{\tau}_{\wedge}^{(s)}$ – математическое ожидание времени срабатывания логического перехода с логикой «И» при поступлении запрета на его срабатывание в случайный момент времени t_0 ,

$$\bar{\tau}_{\wedge}^{(s)} = \bar{t}_0 \cdot \left(1 + \bar{t}_0 / \bar{\tau}_{\wedge}\right). \quad (14)$$

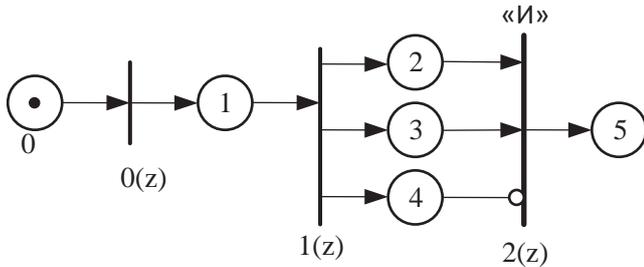
Аналогично выводятся соотношения для расчета вероятностно-временных характеристик для других переходов с ингибиторными дугами. Формулы для расчета вероятностей срабатывания логического перехода для широко встречающихся в практике моделирования динамики реализации угроз безопасности информации пропозициональных логик при пуассоновских входящих потоках приведены в таблице 1.

Пример 1. Пусть имеет место угроза несанкционированного запуска приложения. Стандартно запуск приложения осуществляется, во-первых, при условии наличия соответствующей команды пользователя, во-вторых, при готовности необходимых исходных данных для работы приложения, в-третьих, при отсутствии занятости приложения другим пользователем. Для парирования этой угрозы проводится аутентификация пользователя, а также проверка данных для работы приложения на отклонение от нормативных значений и проверка занятости приложения. Граф фрагмента ССПМ, моделирующей процесс реализации угрозы с применением разрешающих ингибиторных дуг, приведен на рисунке 3.

Ингибиторная дуга является разрешающей со случайным временем выдачи разрешения на запуск приложения, имеющим математическое ожидание \bar{t}_0 .

В соответствии с формулой (6) время срабатывания перехода «И» рассчитывается следующим образом:

$$\bar{\tau}_{\wedge}^{(2)} = \bar{t}_0 \cdot \left[1 + \frac{(\bar{\tau}_1 + \bar{\tau}_2) \cdot \bar{t}_0}{\left(\bar{\tau}_1^2 + \bar{\tau}_1 \cdot \bar{\tau}_2 + \bar{\tau}_2^2\right)}\right], \quad (15)$$



- 0 – нарушитель сделал запрос на работу с приложением;
- 1 – операционная система активизировала подсистему защиты для аутентификации пользователя (нарушителя), проверки с помощью подсистемы противоаварийной защиты необходимых данных на отклонение от нормативных значений и занятости приложения;
- 2 – подсистема защиты запустила процесс аутентификации лица, запросившего приложение;
- 3 – подсистема противоаварийной защиты запустила процесс проверки данных на отклонение от нормативных значений;
- 4 – операционная система запустила проверку занятости приложения;
- 5 – атака реализована;
- 0(z) – запрос на работу с приложением обрабатывается операционной системой;
- 1(z) – передача команд на аутентификацию, проверку данных и занятости приложения;
- 2(z) – принятие решения на запуск приложения по поступившему запросу.

Рисунок 3. Граф фрагмента составной сети Петри-Маркова, моделирующей атаку несанкционированного запуска приложения, с разрешающей ингибиторной дугой

а математическое ожидание времени реализации угрозы – по формуле⁸:

$$\bar{\tau}_u^{(3M)} = \bar{\tau}_{00} + \bar{\tau}_{11} + \bar{\tau}_{\wedge}^{(2)}. \quad (16)$$

Пусть $\bar{\tau}_{00} = \bar{\tau}_{11} = \bar{\tau}_{22} = \bar{\tau}_{32} \approx \bar{\tau}$.

$$\text{Тогда } \bar{\tau}_u^{(3M)} = \bar{\tau}_{00} + \bar{\tau}_{11} + \bar{\tau}_{\wedge}^{(2)} = 2 \cdot \bar{\tau} + \bar{t}_0 \cdot \left(1 + \frac{2 \cdot \bar{t}_0}{3 \cdot \bar{\tau}}\right).$$

Зависимость вероятности реализации угрозы $P_u^{(3M)}(t)$ (срабатывания ССПМ) от времени и параметра приведена на рисунке 4.

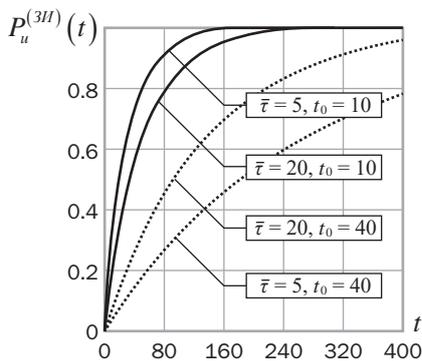


Рисунок 4 – Зависимость вероятности реализации угрозы от времени и математического ожидания времени поступления на переход метки ингибиторной дуги

8 В ССПМ принято, что время перемещения из позиции в переход является конечным и случайным, а из перехода в позицию – мгновенным, при этом используется простая индексация: первым указывается в индексе номер позиции, вторым – номер перехода. Если необходимо указать, что номер относится к переходу, то, как и в традиционных сетях Петри-Маркова, используется число с буквой z в скобках (например, 2(z)).

По рисунку видно, что значение вероятности реализации угрозы в значительной мере зависит от отношения времен $\bar{t}_0 / \bar{\tau}$, при этом с увеличением этого отношения, то есть с увеличением времени выдачи разрешения на запуск приложения, вероятность реализации угрозы существенно снижается.

2. Составные сети Петри-Маркова с приоритетами

Для дальнейшего развития аппарата традиционных сетей Петри-Маркова⁹ было предложено по аналогии с сетями Петри¹⁰ ввести приоритеты срабатывания переходов. Введение приоритетов вполне возможно и для аппарата ССПМ. Сложность заключается в получении аналитических соотношений для расчета вероятностно-временных характеристик такой сети. Приоритеты устанавливаются для переходов, последовательность срабатывания которых обуславливает процесс реализации угрозы. На практике, как правило, бывают только два перехода, один из которых имеет больший приоритет срабатывания. Если необходимо установить приоритеты для многих переходов ССПМ, взаимосвязанных логикой выполнения моделируемого процесса, то предпочтительны два варианта введения приоритетов. Первый вариант состоит в том, что приоритеты вводятся попарно. Например, если связанными логикой выполнения процесса оказываются три перехода $i(z)$, $j(z)$ и $k(z)$, то устанавливаются приоритеты:

$pr_{i(z), j(z)}$, указывающий, что переход $i(z)$ имеет приоритет срабатывания перед переходом $j(z)$;

$pr_{j(z), k(z)}$, указывающий, что переход $j(z)$ имеет приоритет срабатывания перед переходом $k(z)$.

В результате сначала срабатывает переход $i(z)$, затем $j(z)$, а последним – $k(z)$.

Второй вариант состоит в том, что вводится ограниченное множество натуральных чисел, определяющее общее количество назначаемых приоритетов для таких переходов и определяющих порядок их срабатывания. Каждому переходу, для которого устанавливается приоритет, присваивается соответствующее натуральное число, и таким образом формируется множество $M_{pr} = \{pr_{i(z)}\}$, в котором, например, $pr_{i(z)} = 1$, что означает, что переход имеет высший приоритет и срабатывает первым. Например, для четырех переходов $i(z)$, $j(z)$, $k(z)$, $m(z)$ могут быть назначены следующие значения $pr_{i(z)} = 1$, $pr_{j(z)} = 2$, $pr_{k(z)} = 3$, $pr_{m(z)} = 4$.

Это означает, что первым срабатывает переход $i(z)$, а затем по порядку переходы $j(z)$, $k(z)$ и $m(z)$.

Приоритеты могут вводиться в ССПМ, которые построены как на основе марковских, так и полумарковских процессов. При этом могут устанавливаться

9 См. книгу: Игнатъев, В. М. Сети Петри-Маркова / В. М. Игнатъев, Е. В. Ларкин. – Тула: ТулГУ, 1994, 163 с.

10 См. книгу: Котов, В. Е. Сети Петри / В. Е. Котов. – М.: Издательство «Наука», Главная редакция физико-математической литературы, 1984

Таблица 1

Формулы для расчета вероятностно-временных характеристик срабатывания логических переходов с разрешающей или запрещающей ингибиторной дугой

1	2	3	4	5
Тип пропозициональной логики срабатывания перехода	Математическое ожидание времени срабатывания логического перехода при отсутствии ингибиторной дуги	Тип ингибиторной дуги	Математическое ожидание времени срабатывания логического перехода при наличии ингибиторной дуги	Вероятность срабатывания логического перехода за время t
1	2	3	4	5
Логика «И» для двух дуг ($1 \wedge 2$): переход срабатывает, если по обеим дугам парциальные процессы поступили на переход	$\overline{\tau_{\wedge}^{(2)}} = \frac{\overline{\tau_1}^{-2} + \overline{\tau_1} \cdot \overline{\tau_2} + \overline{\tau_2}^{-2}}{\overline{\tau_1} + \overline{\tau_2}}$	Разрешающая для детерминированного значения t_0	$\overline{\tau_{\wedge}^{(раз)}} = \overline{\tau_{\wedge}^{(2)}}$ ТОЛЬКО ДЛЯ $t > t_0$	$P_{\wedge}^{(2)}(t) = \begin{cases} 1 - \exp\left[-\frac{(t-t_0) \cdot (\overline{\tau_1} + \overline{\tau_2})}{\overline{\tau_1} + \overline{\tau_1} \cdot \overline{\tau_2} + \overline{\tau_2}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$
Логика «ИЛИ» для двух дуг ($1 \vee 2$): переход срабатывает, если хотя бы по одной из дуг парциальные процессы поступили на переход	$\overline{\tau_{\vee}^{(2)}} = \frac{\overline{\tau_1} \cdot \overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}}$	Разрешающая для детерминированного значения t_0	$\overline{\tau_{\vee}^{(раз)}} = \overline{\tau_{\vee}^{(2)}} \cdot \left[1 + \frac{t_0}{\overline{\tau_{\vee}^{(2)}}}\right]$ ТОЛЬКО ДЛЯ $t > t_0$	$P_{\vee}^{(2)}(t) = \begin{cases} 1 - \exp\left[-(t-t_0)/\overline{\tau_{\vee}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$
Логика «И-НЕ» для двух дуг ($1 \neg 2$): переход срабатывает, если по первой дуге парциальный процесс поступил на переход, а по второй нет	$\overline{\tau_{\wedge\neg}^{(2)}} = \overline{\tau_1} \cdot \left(1 + \frac{\overline{\tau_2}}{\tau_2}\right)$	Запрещающая для детерминированного значения t_0	$\overline{\tau_{\wedge\neg}^{(раз)}} = \overline{\tau_{\wedge\neg}^{(2)}}$ ТОЛЬКО ДЛЯ $t \leq t_0$	$P_{\wedge\neg}^{(2)}(t) = \begin{cases} 1 - \exp\left[-(t-t_0)/\overline{\tau_{\wedge\neg}^{(2)}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$

1	2	3	4	5
<p>Логика «И-НЕ» для трех дуг $((1 \wedge 2) \neg 3)$; переход срабатывает, если парциальные процессы поступили на переход по первой и второй дуге, а по третьей нет</p>	$\overline{\tau_{\wedge}^{(3)}} = \overline{\tau_{\wedge}^{(2)}} \cdot \left(1 + \frac{\overline{\tau_{\wedge}^{(1)}}}{\tau_3} \right)$ $\overline{\tau_{\vee}^{(3)}} = \overline{\tau_1 + \tau_2 + \tau_3} = \overline{\tau_1} \cdot \overline{\tau_2} \cdot \overline{\tau_3}$ <p>где $\overline{\tau_{\wedge}^{(2)}} = \overline{\tau_1 + \tau_2 + \tau_3} = \overline{\tau_1} \cdot \overline{\tau_2} \cdot \overline{\tau_3}$</p>	<p>Разрешающая после детерминированного значения t_0</p>	$\overline{\tau_{\wedge}^{(pres)}} = \overline{\tau_{\wedge}^{(3)}} \text{ ТОЛЬКО ДЛЯ } t > t_0$ $\overline{\tau_{\wedge}^{(sum)}} = \overline{\tau_{\wedge}^{(3)}} \cdot \left(1 + \frac{\overline{\tau_{\wedge}^{(1)}}}{t_0} \right)$	$P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left[-(t - t_0)/\overline{\tau_{\wedge}^{(3)}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$ $P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\wedge}^{(3)}}\right) \\ 0, & \text{если } t > t_0, \end{cases}$ $P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\wedge}^{(3)}}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0, \end{cases}$
<p>Логика «И-ИЛИ» для трех дуг $((1 \wedge 2) \vee 3)$; переход срабатывает, если или по первой и второй дугам парциальные процессы поступили на переход, или парциальный процесс поступил по третьей дуге</p>	$\overline{\tau_{\wedge}^{(3)}} = \left(\frac{\overline{\tau_1} \cdot \tau_3}{\tau_1 + \tau_3} + \frac{\overline{\tau_2} \cdot \tau_3}{\tau_2 + \tau_3} - \frac{\overline{\tau_1} \cdot \tau_2 \cdot \tau_3}{\tau_1 \cdot \tau_2 + \tau_1 \cdot \tau_3 + \tau_2 \cdot \tau_3} \right)$	<p>Разрешающая для детерминированного значения t_0</p>	$\overline{\tau_{\wedge}^{(pres)}} = \overline{\tau_{\wedge}^{(3)}} \text{ ТОЛЬКО ДЛЯ } t > t_0$ $\overline{\tau_{\wedge}^{(sum)}} = \overline{\tau_{\wedge}^{(3)}} \cdot \left(1 + \frac{\overline{\tau_{\wedge}^{(1)}}}{t_0} \right)$	$P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left[-(t - t_0)/\overline{\tau_{\wedge}^{(3)}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$ $P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\wedge}^{(3)}}\right) \\ 0, & \text{если } t > t_0, \end{cases}$ $P_{\wedge}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\wedge}^{(3)}}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0, \end{cases}$
<p>Логика «ИЛИ-И» для трех дуг $((1 \vee 2) \wedge 3)$; переход срабатывает, если по первой или второй дуге парциальные процессы поступили на переход, и парциальный процесс поступил по третьей дуге</p>	$\overline{\tau_{\vee}^{(3)}} = \tau_3 + \frac{\overline{\tau_1} \cdot \tau_2}{\tau_1 + \tau_2} - \frac{\overline{\tau_1} \cdot \tau_2 \cdot \tau_3}{\tau_1 \cdot \tau_2 + \tau_1 \cdot \tau_3 + \tau_2 \cdot \tau_3}$	<p>Разрешающая после детерминированного значения t_0</p>	$\overline{\tau_{\vee}^{(pres)}} = \overline{\tau_{\vee}^{(3)}} \text{ ТОЛЬКО ДЛЯ } t > t_0$ $\overline{\tau_{\vee}^{(sum)}} = \overline{\tau_{\vee}^{(3)}} \cdot \left(1 + \frac{\overline{\tau_{\vee}^{(1)}}}{t_0} \right)$	$P_{\vee}^{(3)}(t) = \begin{cases} 1 - \exp\left[-(t - t_0)/\overline{\tau_{\vee}^{(3)}}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$ $P_{\vee}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\vee}^{(3)}}\right) \\ 0, & \text{если } t > t_0, \end{cases}$ $P_{\vee}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\overline{\tau_{\vee}^{(3)}}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0, \end{cases}$

1	2	3	4	5
Логика «ИЛИ-НЕ» для трех дуг $(1 \vee 2) \neg 3$: переход срабатывает, если по первой или второй дуге парциальные процессы поступили на переход, и парциальный процесс поступил по третьей дуге	$\tau_{\vee_1}^{(3)} = \tau_{\vee_1}^{(2)} \cdot \left(1 + \frac{\tau_3^{(2)}}{\tau_3} \right)$ $\tau_{\vee_1}^{(sum)} = \tau_1 + \tau_2 + \tau_3$ <p>где $\tau_{\vee_1}^{(i)}$</p>	Разрешающая после детерминированного значения t_0	$\tau_{\vee_1}^{(sum)} = \tau_{\vee_1}^{(3)}$ ТОЛЬКО ДЛЯ $t > t_0$	$P_{\vee_1}^{(3)}(t) = \begin{cases} 1 - \exp\left[-(t-t_0)/\tau_{\vee_1}^{(3)}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$
Логика («XOR») эксклюзивного выбора для ДВУХ ДУГ $(1 \oplus 2)$: переход срабатывает, если парциальный поток поступил только по первой дуге, а по второй нет или только по второй дуге, а по первой нет	$\tau_{\oplus}^{(2)} = \frac{\tau_1 + \tau_2}{2}$	Разрешающая после детерминированного значения t_0	$\tau_{\oplus}^{(sum)} = \tau_1 + \tau_2$ ТОЛЬКО ДЛЯ $t > t_0$	$P_{\oplus}^{(2)}(t) = \begin{cases} 1 - \exp\left[-(t-t_0)/\tau_{\oplus}^{(sum)}\right], & \text{если } t > t_0; \\ 0, & \text{если } t \leq t_0, \end{cases}$
		Запрещающая после детерминированного значения t_0	$\tau_{\vee_1}^{(sum)} = \tau_{\vee_1}^{(3)} \cdot \left[1 + \frac{\tau_3^{(3)}}{t_0} \right]$	$P_{\vee_1}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\tau_{\vee_1}^{(3)}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0 \end{cases}$
		Запрещающая после детерминированного значения t_0	$\tau_{\oplus}^{(sum)} = \tau_1 + \tau_2$ ТОЛЬКО ДЛЯ $t \leq t_0$	$P_{\oplus}^{(2)}(t) = \begin{cases} 1 - \exp\left(-t/\tau_{\oplus}^{(sum)}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0 \end{cases}$
		Разрешающая после детерминированного значения t_0	$\tau_{\oplus}^{(sum)} = \tau_1 + \tau_2 \cdot \left[1 + \frac{2 \cdot t_0}{\tau_1 + \tau_2} \right]$	$P_{\oplus}^{(2)}(t) = \begin{cases} 1 - \exp\left(-t/\tau_{\oplus}^{(sum)}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0 \end{cases}$
		Запрещающая после детерминированного значения t_0	$\tau_{\oplus}^{(sum)} = \tau_1 + \tau_2 \cdot \left[1 + \frac{\tau_1 + \tau_2}{2 \cdot t_0} \right]$	$P_{\oplus}^{(3)}(t) = \begin{cases} 1 - \exp\left(-t/\tau_{\oplus}^{(sum)}\right), & \text{если } t \leq t_0; \\ 0, & \text{если } t > t_0 \end{cases}$

приоритеты как для логических, так и для простых переходов.

Пусть ССПМ с приоритетами построена на основе марковских процессов. На рисунке 5 показан фрагмент такой ССПМ, в которой логический переход 2(z) имеет приоритет срабатывания перед для логическим переходом 1(z).

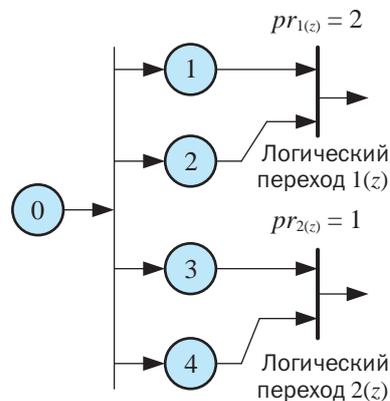


Рисунок 5. Фрагмент составной сети Петри-Маркова с приоритетами на основе марковского процесса

Динамика срабатывания переходов ССПМ с приоритетами определяется, по сути, опережением прихода парциального процесса к переходу с более высоким приоритетом по сравнению с приходом парциального процесса к переходу с меньшим приоритетом. При этом полагается, что если событие парциального процесса на переходе произошло раньше, чем событие на переходе, то оно теряется.

Рассмотрим случаи, когда оба логических перехода имеют логики срабатывания: а) «И», б) «ИЛИ», в) .переход 1(z) логику «И», а переход 2(z) логику «ИЛИ». При этом при любой логике переход сработает, если случайное время поступления процесса к переходу окажется меньше времени поступления парциального процесса на переход.

В случае а) математические ожидания времен срабатывания логических переходов с логикой «И» при отсутствии приоритетов определяются из соотношений:

$$\tau_{1z} = \frac{\tau_{11} + \tau_{11} \cdot \tau_{21} + \tau_{21}}{\tau_{11} + \tau_{21}},$$

$$\tau_{2z} = \frac{\tau_{32} + \tau_{33} \cdot \tau_{42} + \tau_{42}}{\tau_{32} + \tau_{42}}, \tag{17}$$

то есть парциальные потоки поступили на оба перехода, при учете приоритета математическое ожидание времени срабатывания второго перехода останется прежним, а первого перехода будет определяться по аналогии с формулой (9) путем прореживания потока срабатываний этого перехода с вероятностью:

$$P_{np} = \overline{\tau_{1(z)}} / (\overline{\tau_{1(z)}} + \overline{\tau_{2(z)}}), \quad (18)$$

Тогда формулы для расчета математических ожиданий срабатывания переходов имеют вид:

$$\begin{aligned} \overline{\tau_{1z}^{(pr)}} &= \frac{\overline{\tau_{2z}}}{P_{np}} = \overline{\tau_{2z}} \cdot \left[1 + \frac{\overline{\tau_{2z}} \cdot (\overline{\tau_{11}} + \overline{\tau_{21}})}{\overline{\tau_{11}}^2 + \overline{\tau_{11}} \cdot \overline{\tau_{21}} + \overline{\tau_{21}}^2} \right], \\ \overline{\tau_{2z}^{(pr)}} &= \overline{\tau_{2z}} = \frac{\overline{\tau_{32}}^2 + \overline{\tau_{33}} \cdot \overline{\tau_{42}} + \overline{\tau_{42}}^2}{\overline{\tau_{32}} + \overline{\tau_{42}}} \end{aligned} \quad (19)$$

В случае б) математические ожидания времени срабатывания логических переходов с логикой «ИЛИ» при отсутствии приоритетов определяются из соотношений:

$$\overline{\tau_{1z}} = \frac{\overline{\tau_{11}} \cdot \overline{\tau_{21}}}{\overline{\tau_{11}} + \overline{\tau_{21}}}, \quad \overline{\tau_{2z}} = \frac{\overline{\tau_{33}} \cdot \overline{\tau_{42}}}{\overline{\tau_{32}} + \overline{\tau_{42}}}, \quad (20)$$

а при наличии приоритетов расчет проводится по формулам:

$$\begin{aligned} \overline{\tau_{1z}^{(pr)}} &= \overline{\tau_{2z}} \cdot \left[1 + \frac{\overline{\tau_{2z}} \cdot (\overline{\tau_{11}} + \overline{\tau_{21}})}{\overline{\tau_{11}} \cdot \overline{\tau_{21}}} \right], \\ \overline{\tau_{2z}^{(pr)}} &= \overline{\tau_{2z}} = \frac{\overline{\tau_{33}} \cdot \overline{\tau_{42}}}{\overline{\tau_{32}} + \overline{\tau_{42}}} \end{aligned} \quad (21)$$

Аналогично для случая в):

$$\begin{aligned} \overline{\tau_{1z}^{(pr)}} &= \overline{\tau_{2z}} \cdot \left[1 + \frac{\overline{\tau_{2z}} \cdot (\overline{\tau_{11}} + \overline{\tau_{21}})}{\overline{\tau_{11}}^2 + \overline{\tau_{11}} \cdot \overline{\tau_{21}} + \overline{\tau_{21}}^2} \right], \\ \overline{\tau_{2z}^{(pr)}} &= \overline{\tau_{2z}} = \frac{\overline{\tau_{32}}^2 + \overline{\tau_{33}} \cdot \overline{\tau_{42}} + \overline{\tau_{42}}^2}{\overline{\tau_{32}} + \overline{\tau_{42}}} \end{aligned} \quad (22)$$

Пример 2. Пусть для фрагмента ССПМ, показанного на рисунке 5, известны математические ожидания времен перемещения парциальных процессов из позиций в переходы, то есть величины $\overline{\tau_{11}}$, $\overline{\tau_{21}}$, $\overline{\tau_{32}}$ и $\overline{\tau_{42}}$. Рассчитанные при этих значениях указанных величин зависимости от времени вероятностей срабатывания переходов приведены на рисунке 6 в случае, когда переход 1z имеет логику «И» (сплошная линия), а переход 2z – логику «ИЛИ» (пунктирная линия).

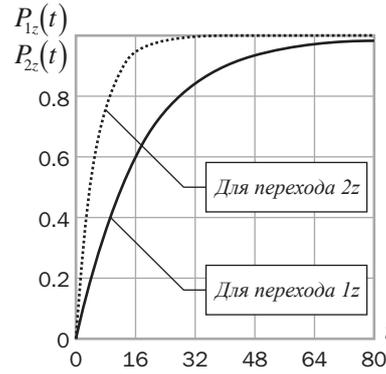


Рисунок 6. Зависимости от времени вероятностей срабатывания логических переходов для фрагмента составной сети, приведенной на рисунке 5

Рассмотрим случай, когда ССПМ построена на основе полумарковских процессов. На рисунке 7 показан фрагмент ССПМ с приоритетами с одним логическим переходом (1z), имеющим меньший приоритет ($pr_1 = 2$), и одним простым переходом (2z) с большим приоритетом ($pr_2 = 1$). Динамика срабатывания переходов ССПМ с приоритетами определяется, по сути, опережением прихода парциального процесса к переходу с более высоким приоритетом по сравнению с приходом этого же или другого парциального процесса к переходу с меньшим приоритетом.

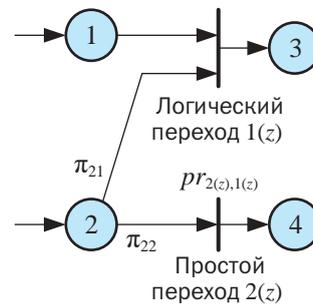


Рисунок 7. Фрагмент составной сети Петри-Маркова с приоритетами на основе полумарковского процесса

Вероятностно-временные характеристики срабатывания переходов с приоритетами, как и ранее, существенно зависят от структуры ССПМ. Найдем аналитические соотношения для их расчета применительно к фрагменту сети, показанному на рисунке 7, в которой имеется один логический переход с одной из двух наиболее распространенных логик срабатывания – «И» и «ИЛИ» и простой переход.

Рассмотрим сначала случай, когда имеет место логический переход с логикой «И», который для рассматриваемого фрагмента ССПМ имеет меньший приоритет, чем простой переход.

Логический переход работает, если случайное время перемещения процесса к простому переходу τ_{22}

окажется меньше времени поступления парциальных процессов на переход с логикой «И» по дугам $1 \rightarrow 1$ и $2 \rightarrow 1$. То есть сначала сработает простой переход с математическим ожиданием времени срабатывания, равным $\bar{\tau}_{22}$, а после него сработает логический переход с логикой «И». Тогда по аналогии с формулой для расчета математическое ожидание времени срабатывания перехода с логикой «И» с разрешающей ингибиторной дугой (см. таблицу 1) в данном случае расчет проводится по формуле:

$$\bar{\tau}_{\wedge}^{(pr)} = \bar{\tau}_{22} \cdot \left[1 + \frac{(\bar{\tau}_{11} + \bar{\tau}_{21}) \cdot \bar{\tau}_{22}}{\bar{\tau}_{11} + \bar{\tau}_{11} \cdot \bar{\tau}_{21} + \bar{\tau}_{21}} \right], \quad (23)$$

Если имеет место логический переход с логикой «ИЛИ», то математическое ожидание времени его срабатывания рассчитывается следующим образом:

$$\bar{\tau}_{\vee}^{(pr)} = \bar{\tau}_{22} \cdot \left[1 + \frac{(\bar{\tau}_{11} + \bar{\tau}_{21}) \cdot \bar{\tau}_{22}}{\bar{\tau}_{11} \cdot \bar{\tau}_{21}} \right]. \quad (24)$$

Для расчета вероятностей срабатывания переходов за время t необходимо учитывать вероятности перехода процесса по вложенной марковской цепи π_{21} и π_{22} («разрешающих» перемещение процесса из позиции 2 в переходы 1 и 2 соответственно). При экспоненциальном приближении вероятности срабатывания переходов определяются по формулам:

$$P_{\wedge}(t) = \pi_{21} \cdot \left(1 - e^{-\frac{t}{\bar{\tau}_{\wedge}^{(pr)}}} \right); \quad P_{\vee}(t) = \pi_{21} \cdot \left(1 - e^{-\frac{t}{\bar{\tau}_{\vee}^{(pr)}}} \right); \quad (25)$$

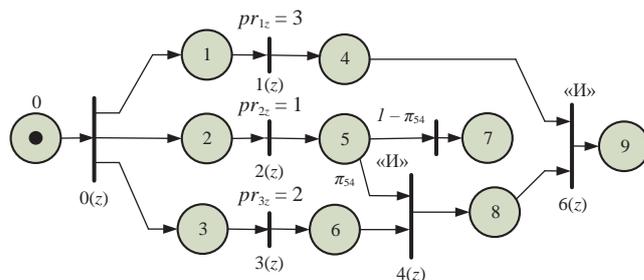
$$P(t) = \pi_{22} \cdot \left(1 - e^{-\frac{t}{\bar{\tau}_{22}}} \right),$$

при этом $\pi_{21} + \pi_{22} = 1$.

Аналогично находятся аналитические соотношения для расчета математических ожиданий времен срабатывания переходов с приоритетами и другими сочетаниями логик (таблица 2).

Пример 3. Нарушитель пытается реализовать атаку «Подмена доверенного объекта». Действия, которые выполняются в ходе атаки и граф ССПМ, моделирующей эту атаку, приведены на рисунке 8. Известны математические ожидания времен перемещения парциальных процессов из позиций в переходы, то есть величины $\bar{\tau}_{00}$, $\bar{\tau}_{11}$, $\bar{\tau}_{33}$, $\bar{\tau}_{46}$, $\bar{\tau}_{54}$, $\bar{\tau}_{55}$, $\bar{\tau}_{64}$, и $\bar{\tau}_{86}$, а также вероятность π_{54} , «разрешающая» перемещение по вложенной цепи Маркова основного процесса из состояния 5 в логический переход 4(z).

Результаты расчета вероятности реализации угрозы атаки «Подмена доверенного объекта» сводятся к следующему. Математические ожидания времен



- 0 – нарушитель и атакуемый компьютер функционируют в сети общего пользования;
- 1 – нарушитель в готовности к организации связи с атакуемым хостом;
- 2 – нарушитель в готовности к подбору (прогнозу) номеров ответных пакетов и порта взаимодействия атакуемого и доверенного хостов;
- 3 – нарушитель в ожидании получения данных о доверенном хосте для проведения атаки «Шторм TCP-запросов» на хост доверенного пользователя;
- 4 – нарушитель установил соединение с атакуемым хостом от имени доверенного объекта;
- 5 – нарушитель начал атаку «Анализ трафика» для выявления порта взаимодействия и нумерации пакетов трафика атакуемого хоста при его взаимодействии с доверенным хостом;
- 6 – нарушитель в готовности к проведению атаки «Шторм TCP-запросов» на хост доверенного объекта;
- 7 – атака сорвалась с вероятностью из-за неправильного определения порта взаимодействия или номера пакета подтверждения соединения или из-за срыва подавления доверенного хоста в результате «шторма TCP-запросов»;
- 8 – созданы условия для завершения атаки проникновения в операционную среду атакуемого хоста;
- 9 – осуществлен НСД к атакуемому хосту от имени доверенного пользователя, атака реализована;
- 0(z) – подготовка к проведению атаки;
- 1(z) – передача запроса на соединение с атакуемым хостом от имени доверенного хоста;
- 2(z) – подбор (прогноз) порта взаимодействия и номера пакета подтверждения соединения;
- 3(z) – проведение атаки «шторма TCP-запросов» с целью нарушения функционирования доверенного хоста;
- 4(z) – логический переход «И», срабатывающий, если нарушителю с вероятностью удалось подобрать номера ответного пакета и порта взаимодействия и функционирование доверенного хоста нарушено;
- 5(z) – нарушителю с вероятностью не удалось подобрать номера ответного пакета и порта взаимодействия;
- 6(z) – логический переход «И», срабатывающий, если созданы условия для проникновения в операционную среду атакуемого хоста и установлена связь с ним от имени доверенного объекта.

Рисунок 8 – Граф составной сети Петри-Маркова, моделирующий атаку «Подмена доверенного объекта (IP-spoofing)»

срабатывания переходов с приоритетами рассчитываются по формулам:

$$\bar{\tau}_{2(z)}^{(pr)} = \bar{\tau}_{22}; \quad \bar{\tau}_{3(z)}^{(pr)} = \bar{\tau}_{22} \cdot \left(1 + \frac{\bar{\tau}_{22}}{\bar{\tau}_{33}} \right); \quad \bar{\tau}_{1(z)}^{(pr)} = \bar{\tau}_{3(z)}^{(pr)} \cdot \left(1 + \frac{\bar{\tau}_{3(z)}^{(pr)}}{\bar{\tau}_{11}} \right), \quad (26)$$

времени срабатывания логического переход 4(z) – по формуле:

$$\bar{\tau}_{4(z)} = \frac{(\bar{\tau}_{2(z)} + \bar{\tau}_{54})^2 + (\bar{\tau}_{2(z)} + \bar{\tau}_{54}) \cdot (\bar{\tau}_{3(z)} + \bar{\tau}_{64}) + (\bar{\tau}_{3(z)} + \bar{\tau}_{64})^2}{\bar{\tau}_{2(z)} + \bar{\tau}_{54} + \bar{\tau}_{3(z)} + \bar{\tau}_{64}}, \quad (27)$$

Таблица 2

Формулы для расчета математических ожиданий времен срабатывания сочетаний двух переходов с различными приоритетами*

Тип первого перехода с большим приоритетом	Тип второго перехода с меньшим приоритетом	Математическое ожидание времени срабатывания первого перехода	Математическое ожидание времени срабатывания первого перехода	Математическое ожидание времени срабатывания обоих переходов
Простой переход	Простой переход	$\bar{\tau}_1$	$\bar{\tau}_2$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_1 \cdot \left(1 + \frac{\bar{\tau}_1}{\bar{\tau}_2}\right)$
Простой переход	Логический переход с логикой «И»	$\bar{\tau}_1$	$\bar{\tau}_{\wedge} = \frac{\bar{\tau}_{\delta 1}^{-2} + \bar{\tau}_{\delta 1} \cdot \bar{\tau}_{\delta 2} + \bar{\tau}_{\delta 2}^{-2}}{\bar{\tau}_{\delta 1} + \bar{\tau}_{\delta 2}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_1 \cdot \left(1 + \frac{\bar{\tau}_1}{\bar{\tau}_{\wedge}}\right)$
Логический переход с логикой «И»	Простой переход	$\bar{\tau}_{\wedge} = \frac{\bar{\tau}_{\delta 1}^{-2} + \bar{\tau}_{\delta 1} \cdot \bar{\tau}_{\delta 2} + \bar{\tau}_{\delta 2}^{-2}}{\bar{\tau}_{\delta 1} + \bar{\tau}_{\delta 2}}$	$\bar{\tau}_2$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge} \cdot \left(1 + \frac{\bar{\tau}_{\wedge}}{\bar{\tau}_2}\right)$
Простой переход	Логический переход с логикой «ИЛИ»	$\bar{\tau}_1$	$\bar{\tau}_v = \frac{\bar{\tau}_{\delta 1} \cdot \bar{\tau}_{\delta 2}}{\bar{\tau}_{\delta 1} + \bar{\tau}_{\delta 2}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_1 \cdot \left(1 + \frac{\bar{\tau}_1}{\bar{\tau}_v}\right)$
Логический переход с логикой «ИЛИ»	Простой переход	$\bar{\tau}_v = \frac{\bar{\tau}_{\delta 1} \cdot \bar{\tau}_{\delta 2}}{\bar{\tau}_{\delta 1} + \bar{\tau}_{\delta 2}}$	$\bar{\tau}_2$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_v \cdot \left(1 + \frac{\bar{\tau}_v}{\bar{\tau}_2}\right)$
Простой переход	Логический переход с логикой «И-НЕ»	$\bar{\tau}_1$	$\bar{\tau}_{\wedge\sim} = \bar{\tau}_{\delta 1} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}}{\bar{\tau}_{\delta 2}}\right)$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_1 \cdot \left(1 + \frac{\bar{\tau}_1}{\bar{\tau}_{\wedge\sim}}\right)$
Логический переход с логикой «И-НЕ»	Простой переход	$\bar{\tau}_{\wedge\sim} = \bar{\tau}_{\delta 1} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}}{\bar{\tau}_{\delta 2}}\right)$	$\bar{\tau}_2$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge\sim} \cdot \left(1 + \frac{\bar{\tau}_{\wedge\sim}}{\bar{\tau}_2}\right)$
Логический переход с логикой «И»	Логический переход с логикой «И»	$\bar{\tau}_{\wedge}^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)-2} + \bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)} + \bar{\tau}_{\delta 2}^{(1)-2}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_{\wedge}^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)-2} + \bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)} + \bar{\tau}_{\delta 2}^{(2)-2}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\wedge}^{(1)}}{\bar{\tau}_{\wedge}^{(2)}}\right)$
Логический переход с логикой «И»	Логический переход с логикой «ИЛИ»	$\bar{\tau}_{\wedge}^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)-2} + \bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)} + \bar{\tau}_{\delta 2}^{(1)-2}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_v^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\wedge}^{(1)}}{\bar{\tau}_v^{(2)}}\right)$
Логический переход с логикой «ИЛИ»	Логический переход с логикой «И»	$\bar{\tau}_v^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_{\wedge}^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)-2} + \bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)} + \bar{\tau}_{\delta 2}^{(2)-2}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_v^{(1)} \cdot \left(1 + \frac{\bar{\tau}_v^{(1)}}{\bar{\tau}_{\wedge}^{(2)}}\right)$
Логический переход с логикой «ИЛИ»	Логический переход с логикой «ИЛИ»	$\bar{\tau}_v^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_v^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_v^{(1)} \cdot \left(1 + \frac{\bar{\tau}_v^{(1)}}{\bar{\tau}_v^{(2)}}\right)$
Логический переход с логикой «И»	Логический переход с логикой «И-НЕ»	$\bar{\tau}_{\wedge}^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)-2} + \bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)} + \bar{\tau}_{\delta 2}^{(1)-2}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_{\wedge\sim}^{(2)} = \bar{\tau}_{\delta 1}^{(2)} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}^{(2)}}{\bar{\tau}_{\delta 2}^{(2)}}\right)$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\wedge}^{(1)}}{\bar{\tau}_{\wedge\sim}^{(2)}}\right)$
Логический переход с логикой «И-НЕ»	Логический переход с логикой «И»	$\bar{\tau}_{\wedge\sim}^{(1)} = \bar{\tau}_{\delta 1}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}^{(1)}}{\bar{\tau}_{\delta 2}^{(1)}}\right)$	$\bar{\tau}_{\wedge}^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)-2} + \bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)} + \bar{\tau}_{\delta 2}^{(2)-2}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge\sim}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\wedge\sim}^{(1)}}{\bar{\tau}_{\wedge}^{(2)}}\right)$
Логический переход с логикой «ИЛИ»	Логический переход с логикой «И-НЕ»	$\bar{\tau}_v^{(1)} = \frac{\bar{\tau}_{\delta 1}^{(1)} \cdot \bar{\tau}_{\delta 2}^{(1)}}{\bar{\tau}_{\delta 1}^{(1)} + \bar{\tau}_{\delta 2}^{(1)}}$	$\bar{\tau}_{\wedge\sim}^{(2)} = \bar{\tau}_{\delta 1}^{(2)} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}^{(2)}}{\bar{\tau}_{\delta 2}^{(2)}}\right)$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_v^{(1)} \cdot \left(1 + \frac{\bar{\tau}_v^{(1)}}{\bar{\tau}_{\wedge\sim}^{(2)}}\right)$
Логический переход с логикой «И-НЕ»	Логический переход с логикой «ИЛИ»	$\bar{\tau}_{\wedge\sim}^{(1)} = \bar{\tau}_{\delta 1}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\delta 1}^{(1)}}{\bar{\tau}_{\delta 2}^{(1)}}\right)$	$\bar{\tau}_v^{(2)} = \frac{\bar{\tau}_{\delta 1}^{(2)} \cdot \bar{\tau}_{\delta 2}^{(2)}}{\bar{\tau}_{\delta 1}^{(2)} + \bar{\tau}_{\delta 2}^{(2)}}$	$\bar{\tau}_{1\&2}^{(pr)} = \bar{\tau}_{\wedge\sim}^{(1)} \cdot \left(1 + \frac{\bar{\tau}_{\wedge\sim}^{(1)}}{\bar{\tau}_v^{(2)}}\right)$

*примечания:

1) обозначение $\bar{\tau}_{\delta 1}^{(i)}$ означает математическое ожидание времени поступления парциального процесса на первый логический переход по первой дуге, а $\bar{\tau}_{\delta 2}^{(i)}$ – по второй дуге. Соответственно $\bar{\tau}_{\delta 1}^{(i)}$ и $\bar{\tau}_{\delta 2}^{(i)}$ означает то же самое только для второго перехода;

2) для простых переходов имеет место только одна входящая дуга, поэтому обозначение $\bar{\tau}_1$ означает математическое ожидание времени поступления парциального процесса на первый простой переход, а $\bar{\tau}_2$ – на второй простой переход.

а времени реализации угрозы (с учетом времени срабатывания логического перехода $\bar{b}(z)$) – из соотношения:

$$\bar{\tau}_u = \bar{\tau}_{00} + \frac{\left(\bar{\tau}_{1(z)}^{(pr)} + \bar{\tau}_{46}\right)^2 + \left(\bar{\tau}_{1(z)}^{(pr)} + \bar{\tau}_{46}\right) \cdot \left(\bar{\tau}_{4(z)} + \bar{\tau}_{86}\right) + \left(\bar{\tau}_{4(z)} + \bar{\tau}_{86}\right)^2}{\left(\bar{\tau}_{1(z)}^{(pr)} + \bar{\tau}_{46}\right) + \left(\bar{\tau}_{4(z)} + \bar{\tau}_{86}\right)}. \quad (28)$$

Тогда вероятность реализации угрозы за время t по аналогии с формулами (21) рассчитывается следующим образом:

$$P_u(t) = \pi_{54} \cdot \left(1 - e^{-\frac{t}{\bar{\tau}_u}}\right) \quad (29)$$

Пусть $\bar{\tau}_{00} \approx \bar{\tau}_{11} \approx \bar{\tau}_{22} \approx \bar{\tau}_{33} \approx \bar{\tau}_{46} \approx \bar{\tau}_{54} \approx \bar{\tau}_{55} \approx \bar{\tau}_{64} \approx \bar{\tau}_{86} = \bar{\tau}$.

На рисунке 9 приведены графики зависимости от времени вероятности реализации угрозы, рассчитанной по формуле (29) при разных значениях математического ожидания времени $\bar{\tau}$ и вероятности π_{54} .

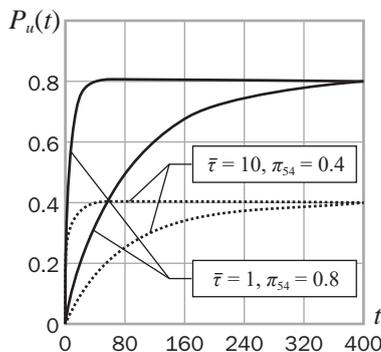


Рисунок 9. Графики зависимости от времени вероятности реализации угрозы атаки «Подмена доверенного объекта», моделируемой с применением ССПМ с приоритетами

По формулам и приведенным графикам видно следующее:

- во-первых, наличие приоритетов существенно замедляет процесс срабатывания соответствующих переходов и в целом процесс реализации угрозы безопасности информации (срабатывания ССПМ). В частности, переход $3(z)$ со вторым приоритетом срабатывает в 2 раза позже, а переход $1(z)$ – в 6 раз позже по сравнению со случаем отсутствия приоритетов;
- во-вторых, с увеличением времени срабатывания простого перехода $\bar{\tau}$ увеличивается и время срабатывания логических переходов, что приводит

к заметному снижению вероятности срабатывания ССПМ, то есть реализации угрозы в целом;

- в-третьих, на вероятность срабатывания ССПМ, построенной с использованием аппарата полумарковских процессов, существенно влияет значение вероятности перемещения моделируемого процесса по вложенной марковской цепи (в данном примере π_{54}). Это обуславливает необходимость обоснования значений таких вероятностей и построения соответствующих математических моделей для такого обоснования.

Заключение

Для расширения моделирующих возможностей аппарата составных сетей Петри-Маркова, позволяющего при моделировании процессов реализации угроз безопасности информации в ИС учитывать фактор времени, параллельность и логические условия выполнения парциальных процессов, целесообразно использовать предложенные еще для сетей Петри такие приемы, как введение запретов и разрешений срабатывания переходов на основе применения ингибиторных дуг и установления приоритетов. Однако для использования таких приемов в ССПМ необходимы аналитические соотношения для расчета вероятностно-временных характеристик срабатывания переходов с ингибиторными дугами и приоритетами.

Предложенные в статье соотношения впервые дают возможность рассчитать математические ожидания времен срабатывания как простых, так и логических переходов с различными типами пропозициональной логики срабатывания («И», «ИЛИ», «И-НЕ», «ИЛИ-НЕ» и т.д.), и вероятности такого срабатывания при применении:

- во-первых, разрешающих и запрещающих ингибиторных дуг с детерминированным и случайным временем запрета и разрешения;
- во-вторых, при установлении приоритетов на срабатывание логических и простых переходов.

Это позволяет существенно расширить моделирующие возможности аппарата составных сетей Петри-Маркова при анализе угроз безопасности информации в информационных системах без применения и в условиях применения мер защиты и тем самым повысить обоснованность выбора этих мер.

Литература

1. Язов, Ю. К. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография / Ю. К. Язов, А.В. Анищенко. – Воронеж: Кварта, 2020. – 173 с.
2. Язов, Ю. К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю. К. Язов, С.В. Соловьев. – Санкт-Петербург: Научное издание, 2023. – 258 с.
3. Соловьев, С. В. Математические модели оценки показателей качества информационного обеспечения деятельности по технической защите информации / С. В. Соловьев, Ю. К. Язов, А. А. Теплинских. – Вопросы кибербезопасности. 2023, №6 (58), с. 81–95.
4. Корнилов, С. А. Модель обслуживания заявок с приоритетами и прерыванием в звене мультисервисной сети связи / С. А. Корнилов, М. И. Торгашов. Информационные технологии. Проблемы и решения. 2021. № 2 (15). С. 65–69.
5. Лебедев, А. В. Модель случайного множественного доступа в локальной вычислительной сети с потоками различной интенсивности и приоритетов / А. В. Лебедев, П. В. Зобов. Вестник Воронежского государственного технического университета. 2019. Т. 15. № 6. С. 22–29.
6. Казыханова, Д. Р. К вопросу о необходимости расстановки приоритетов при обеспечении безопасности информации / Д. Р. Казыханова, А. А. Казыханов., Д. В. Редников. Современные научные исследования и разработки. 2018. Т. 1. № 12 (29). С. 253–254.
7. Козырь, О. Ф. Модель и алгоритм назначения приоритетов задачам, выполняемым в информационных системах / О. Ф. Козырь, Кривоносов В. А. Инженерный вестник Дона. 2020. № 7 (67). С. 224–232.
8. Макарова, О. С. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями / О. С. Макарова, С. В. Поршнева. Безопасность информационных технологий. 2020. Т. 27. № 1. С. 6–18.
9. Коган, Ю. Г. Модифицированная раскрашенная сеть Петри: метод и средство имитационного моделирования / Ю. Г. Коган, К. В. Пителинский, А. А. Щербина. Оборонный комплекс – научно-техническому прогрессу России. 2021. № 1 (149). С. 26–32.
10. Асанова, С. М. Развитие сетей Петри для разработки самоорганизующихся многокомпонентных вычислительных алгоритмов решения задач электроэнергетики / С. М. Асанова. Проблемы автоматизации и управления. 2022. № 2 (44). С. 15–21.
11. Артюхин, В. В. Расширение инструментария моделирования отказов с использованием сетей Петри / Артюхин В. В., Егоров В. М. Технологии гражданской безопасности. 2023. Т. 20. № 3 (77). С. 98–103.
12. Остроух, А. В. 079 Введение в искусственный интеллект: монография / А. В. Остроух. – Красноярск: Научно-инновационный центр, 2020. – 250 с. ISBN 978-5-907208-26-1. DOI: 10.12731/978-5-907208-26-1. <http://nkras.ru/arhiv/2020/ostroukh1.pdf>. Дата обращения 10.12.2023 г.
13. Борисов В. В., Захарченков К. В., Кутузов В. В., Мисник А. Е., Прокопенко С. А. Моделирование образовательных процессов на основе нейро-нечетких темпоральных сетей Петри // Прикладная информатика. – 2021. – № 4. – С. 35–47.
14. Прокопенко, С. А. Темпоральные нейро-нечеткие сети Петри для моделирования информационно-технологических процессов / С. А. Прокопенко, А. В. Бобряков <http://e.biblio.bru.by/bitstream/handle/1212121212/32724/104-109.pdf?sequence=1&isAllowed=y> Дата обращения 10.12.2023 г.
15. Pertsukhov, P. A. Simulating petri nets with inhibitor and reset arcs / P. A. Pertsukhov, A. A. Mitsyuk. Proceedings of the Institute for System Programming of the RAS. 2019. Т. 31. № 4. С. 151–162.

