Ю. К. Язов, *доктор технических наук, профессор*
А. О. Авсентьев, *кандидат технических наук*
А. П. Панфилов
В. Н. Пржегорлинский, *кандидат технических наук, доцент*

СОСТАВНЫЕ СЕТИ ПЕТРИ — МАРКОВА НА ОСНОВЕ ПОЛУМАРКОВСКИХ ПРОЦЕССОВ И ИХ ПРИМЕНЕНИЕ ПРИ МОДЕЛИРОВАНИИ ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

COMPOSITE PETRI — MARKOV NETWORKS BASED ON SEMI-MARKOV PROCESSES AND THEIR APPLICATION IN MODELING THE DYNAMICS OF INFORMATION SECURITY THREATS IN INFORMATION SYSTEMS

Цель статьи состоит в изложении алгоритмов расчета временных характеристик срабатывания логических переходов с пропозициональной логикой при моделировании угроз безопасности информации в информационных системах с применением аппарата составных сетей Петри — Маркова на основе полумарковских процессов.

Показаны достоинства и недостатки применения в составных сетях Петри — Маркова полумарковских процессов по сравнению с марковскими процессами. Приведены правила построения составной сети Петри — Маркова.

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

Приведены примеры расчета математического ожидания и вероятности срабатывания переходов в составных сетях Петри — Маркова на основе полумарковских процессов при моделировании угроз безопасности информации в информационных системах.

The purpose of the article is to present algorithms for calculating the time characteristics of triggering logical transitions with propositional logic in modeling information security threats in information systems using the Petri — Markov composite network apparatus based on semi-Markov processes.

The advantages and disadvantages of using semi-Markov processes in composite Petri — Markov networks in comparison with Markov processes are shown. The rules for constructing a composite Petri-Markov network are given.

Analytical relations are obtained for calculating the probabilistic-temporal characteristics of the processes of triggering logical transitions with a propositional logic of triggering such as «AND», «OR», «AND-OR», «AND-NOT», «OR-NOT» in the case of the presence of permissive and forbidding arcs in these transitions with deterministic and the random time of permission or prohibition, respectively.

Examples of calculating the mathematical expectation and probability of transitions in composite Petri-Markov networks based on semi-Markov processes in modeling information security threats in information systems are given.

Введение. Аппарат составных сетей Петри — Маркова (ССПМ) был предложен в [1] для моделирования динамики реализации угроз безопасности информации в информационных системах и развит в [2]. В отличие от аппарата сетей Петри позволяет оценивать вероятностно-временные характеристики процесса их реализации, а в отличии от традици-

онного аппарата сетей Петри — Маркова [3] — учитывать не только параллельность выполняемых парциальных процессов, но и наличие различных логических условий их реализации. Вместе с тем одновременно было показано, что в основе ССПМ могут лежать как марковские, так и полумарковские процессы. Однако если для случая применения в ССПМ марковских процессов были получены аналитические соотношения для расчета вероятностно-временных характеристик срабатывания логических переходов с пропозициональной логикой типа «И», «ИЛИ», «И-ИЛИ», «И-НЕ», «ИЛИ-НЕ», то для случая применения полумарковских процессов такие соотношения отсутствовали.

Данная статья посвящена разработке аналитических соотношений, позволяющих рассчитывать вероятностно-временные характеристики срабатывания логических переходов ССПМ, построенных на основе парциальных полумарковских процессов.

1. Правила построения составных сетей Петри — Маркова на основе полумарковских процессов. Аппарат традиционных сетей Петри — Маркова (СПМ) был предложен в [3] в интересах моделирования процессов в теории надежности систем, при этом СПМ рассматривается как множество позиций сети Петри, моделирующих состояния рассматриваемого процесса, и множество ее переходов, моделирующих условия перехода процесса из состояния в состояние. В традиционной СПМ срабатывание переходов определяется только наличием в позициях, инцидентных переходу, маркеров и, в случае наличия управляющих дуг (например, ингибиторных), маркеров в позициях, инцидентных таким дугам. Это обусловливает то, что в таких сетях крайне сложно, а чаще практически невозможно, моделировать динамику выполнения целого ряда логических условий, таких как условия «И-НЕ», «ИЛИ-НЕ», «И-ИЛИ» и др., которые часто встречаются в моделях реализации угроз безопасности информации в информационных системах. При этом сложность состоит не в определении логических правил (что достаточно просто записывается в соответствии с математической логикой), а в определении аналитических соотношений для расчета времен срабатывания таких переходов. В частности, в [3] показано, каким образом можно рассчитать время ожидания завершения второй процедуры в составе моделируемого процесса после завершения первой, если процесс завершается после окончания второй процедуры. Однако для других условий формулы для расчета временных характеристик отсутствуют.

Кроме того, весьма сложно моделировать циклические процедуры с заранее установленными правилами их завершения или дальнейшего продолжения выполнения процесса.

С учетом изложенного моделирующие возможности классического аппарата СПМ применительно к решению задач аналитического моделирования процессов реализации угроз безопасности информации оказываются ограниченными.

Для расширения моделирующих возможностей традиционных СПМ предложено использовать [3—6]:

- окрашивание позиций, маркеров и переходов СПМ (применение раскрашенных или «цветных» СПМ);
- формирование так называемых иерархических сетей, в которые вложены другие, возможно, также иерархические сети;
- приоритеты срабатывания переходов, при этом если несколько переходов являются разрешенными, то срабатывает тот из них, который имеет наивысший приоритет [4];
- логические запреты на выполнение переходов с использованием ингибиторых (сдерживающих) дуг (по аналогии с классическими сетями Петри [5]) или специальных ограничений на срабатывание переходов;
- изменяемую структуру, в которой кратность дуг не является постоянной, при этом в самомодифицируемых сетях кратность дуги может либо задаваться натуральным числом, либо определяться количеством маркеров, находящихся во входных позициях некоторого перехода;
- временные сети, в которых переходам ставятся в соответствие их времена срабатывания, либо позициям ставятся в соответствие времена нахождения маркеров в позициях (по сути, временные сети предшествовали СПМ).

Вместе с тем все эти расширения не позволяют аналитически описывать дина-

мику процессов реализации угроз, применяются в основном для имитационного моделирования и могут рассматриваться лишь как одно из направлений модификации СПМ.

Пусть СПМ состоит из нескольких подпроцессов — парциальных марковских или полумарковских процессов, при этом переход от одного парциального процесса к другому осуществляется только при выполнении определенных логических условий. Для того чтобы отделить подпроцессы, завершающиеся логическими условиями, от других подпроцессов, вводятся переходы, срабатывающие при определенной логике наступления событий. В связи с этим сеть Петри — Маркова разбиваются на участки, что и обусловило то, что такие СПМ в [2] названы составными сетями Петри — Маркова (ССПМ). Таким образом, в ССПМ используются как простые, так и логические переходы.

Так же, как сети Петри и традиционные СПМ, составные сети представляются в виде графа (рисунок 1).

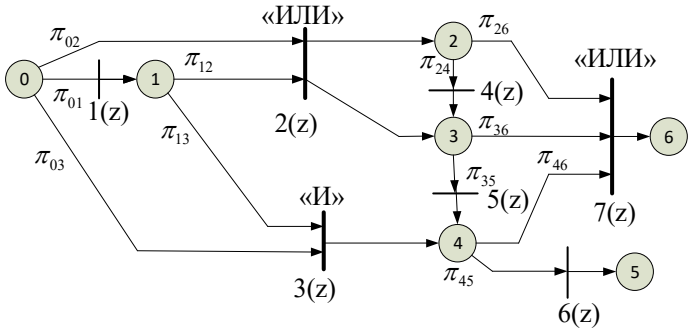

Рис. 1. Пример графа составной сети Петри — Маркова на основе парциальных полумарковских процессов с логическими условиями «И» и «ИЛИ»

На графе ССПМ принято, что, во-первых, переходы обозначаются жирной чертой и номером с буквой *z*, а позиции — кружком и просто нумеруются, во-вторых, в индексах функций и параметров первая буква означает номер состояния, из которого исходит дуга, а вторая — номер перехода, в который она входит, при двузначных цифрах в индексах применяется разделяющая запятая.

Основными их отличиями от традиционных СПМ являются следующие:

- традиционные СПМ, как было отмечено ранее, являются сетями, в которых переходы обязательно срабатывают, если для каждой входящей в переход дуги имеется не менее одного маркера, однако в ССПМ для перехода может быть определена любая логика срабатывания: пропозициональная[1] или логика предикатов [7], в соответствии с которой недостаточно, чтобы логический переход срабатывал, если для каждой входящей в него дуги имелся маркер во входящей позиции, но должны выполняться и иные заданные для логического перехода логические условия (например, условие, когда переход срабатывает, если по одной дуге парциальный процесс подошел к переходу, а по другим дугам парциальные процессы запоздали);

- на каждом из участков ССПМ, соединяемых между собой логическими переходами, моделируемый процесс может быть как марковским, так и полумарковским. Важной особенностью полумарковского процесса является наличие разветвления моделируемого процесса при выходе его из хотя бы одного из состояний;

- расчет вероятностно-временных характеристик осуществляется по каждому участку и по каждому логическому переходу, а затем путем свертки [6] рассчитывается время и вероятность срабатывания ССПМ в целом.

Порядок построения ССПМ состоит в следующем:

- определяются начальное, промежуточные и конечные состояния, в которых может находиться моделируемый процесс реализации угрозы по мере выполнения дей-

[1] К пропозициональной логике (лат. *propositio* — «высказывание») относятся логики «И», «ИЛИ», «И-ИЛИ» и т. п.

ствий, определенных в функциональной модели, и таким образом формируется перечень позиций ССПМ;

- определяются логические переходы, к которым относятся все переходы, срабатывающие при определенных логических условиях. Указывается место каждого логического перехода (после каких состояний процесса должен выполняться переход) и логика его срабатывания;

- определяются для каждого участка ССПМ между начальным состоянием и первым логическим переходом, между логическими переходами и, наконец, между последним логическим переходом и конечным состоянием все простые переходы;

- для каждого простого и логического перехода формируются входные и выходные дуги, соединяющие переход с инцидентными входными и выходными позициями ССПМ;

- осуществляется разметка ССПМ путем помещения маркера (фишки) в начальную позицию (или начальные позиции, если их несколько).

При построении графа для ССПМ необходимо выполнять следующие правила:

- если две или большее количество дуг входят в переход, то этот переход является логическим, несколько дуг не могут входить в простой переход;

- если из позиции выходит более одной дуги, то моделируемый процесс относится к полумарковскому и для этой позиции необходимо определить вероятности того, что парциальный процесс начнет перемещаться по каждой из дуг. Если из позиции выходит только одна дуга, то моделируемый процесс относится к марковскому;

- количество дуг, выходящих из перехода, определяется составом и содержанием моделируемых действий, при количестве выходящих дуг две и более, по сути, имеет место разветвление процесса после перехода с перемещением подпроцессов к разным позициям, при этом осуществляется размножение маркера и по всем исходящим из перехода дугам маркеры (по каждому маркеру на дугу) перемещаются в инцидентные позиции мгновенно;

- каждая дуга должна выходить или из позиции и входить в переход, или из перехода и входить в позицию, не допускаются ситуации, чтобы дуга выходила из позиции и входила в позицию или выходила из перехода и входила в переход (то есть в ССПМ не может быть две подряд позиции или два подряд перехода);

- как правило, граф ССПМ, моделирующий процесс реализации угрозы, имеет одну начальную и одну конечную позицию, при этом начальная разметка сети сводится к помещению маркера в начальную позицию, однако граф ССПМ может иметь несколько начальных позиций, при этом, во-первых, начальная разметка сети сводится к помещению маркера во все начальные позиции, во-вторых, проводится синхронизация начала выполнения парциальных процессов с каждой начальной позиции, в том числе с возможными задержками относительно самого раннего парциального процесса;

- в ССПМ, наряду с одной конечной позицией, могут иметь место тупиковые позиции, в которых развитие процесса прекращается, для того чтобы показать, где может остановиться процесс, не достигнув конечной позиции;

- если граф ССПМ имеет цикл, то должно вводиться логическое условие выполнения цикла (например, касающееся установленного количества повторов), однако в пропозициональной логике таких логических условий нет, поэтому для введения нужного условия применяются предикаты [7];

- в сети могут применяться кратные дуги, но тогда, во-первых, в состоянии, из которого они исходят, должно находиться или накапливаться такое же или большее количество маркеров (фишек) и, во-вторых, переходы, в которые входят кратные дуги, являются логическими и для них должны быть определены соответствующие правила срабатывания;

- целесообразно сокращать количество состояний и переходов в ССПМ, проводя их объединение (агрегирование) там, где это не приводит к некорректному моделированию процесса;

- в ССПМ должна быть установлена начальная разметка сети.

2. Порядок расчета вероятностно-временных характеристик срабатывания составной сети Петри — Маркова на основе полумарковских процессов. Полумар-

ковские процессы (ПМП) представляют собой обобщение достаточно хорошо изученных в теории вероятностей марковских процессов. Они введены в 1954—1955 гг. независимо П. Леви, В. Смитом и Л. Такачем и сегодня достаточно широко и успешно используются в теории надежности и теории массового обслуживания.

В соответствии с [8, 9] суть ПМП сводится к следующему.

Пусть в начальный момент времени $t = 0$ моделируемый процесс находится в состоянии $i, i \in I$, в течение некоторого случайного времени θ_{0j}, зависящего от того, в какое состояние будет переходить процесс, после чего процесс мгновенно переходит в состояние $j, j \in I$. При этом время θ_{0j} — случайная величина с *произвольной* функцией распределения $F_{0j}(x)$, а переход процесса из состояния i в состояние j происходит с вероятностью $\pi_{ij} \geq 0$ и для любого i выполняется условие $\sum_{i \in J} \pi_{ij} = 1$. Если затем из состояния j процесс переходит в состояние $k, k \in I,$ то в состоянии j процесс пребывает случайное время θ_{jk}, имеющее произвольное распределение $F_{jk}(x)$ и т. д. (рис. 2).

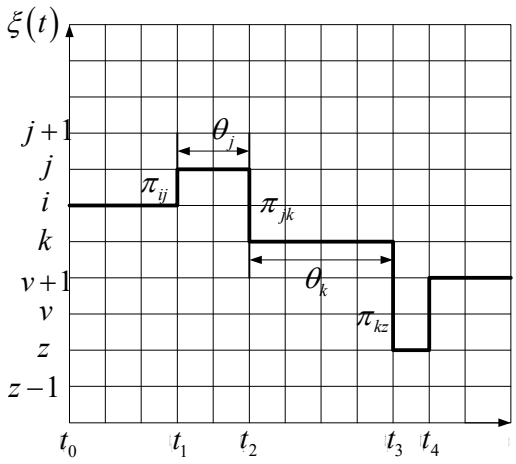

Рис. 2. Графическое представление полумарковского процесса

ПМП является скачкообразным случайным процессом, при этом распределение времени пребывания ПМП в каждом состоянии не обязательно является показательным, что отличает полумарковский процесс от марковского [8]. Для ПМП характерно то, что процесс мгновенных вероятностных переходов представляет собой вложенную цепь Маркова. В соответствии с теорией полумарковских процессов [8, 9] для расчета вероятностно-временных характеристик полумарковского процесса в случае отсутствия логических переходов составляется система интегро-дифференциальных уравнений вида

$$F_{ij}(x) = \sum_{k \in I} \int_0^x q'_{ik}(t) \cdot F_{kj}(x - t) \cdot dt,\ k, i, j \in I, t > 0 \tag{1}$$

где I — общее количество состояний процесса;

$q'_{ik}(t)$ — производная от функции — элемента полумарковской матрицы, при этом варианты представления такой матрицы могут быть, например, следующие:

$$q_{ij}(x) = \pi_{ij}, x \geq 0, \sum_{j \in I} \pi_{ij} = 1,\ i, j \in I; \tag{2}$$

$$q_{ij}(x) = \pi_{ij}(1 - e^{-\lambda_i \cdot x}), x \geq 0, \sum_{j \in I} \pi_{ij} = 1,\ i, j \in I; \lambda_i > 0; \tag{3}$$

Если из состояния i в состояние j процесс может переместиться только по одной траектории (нет разветвления), то $\pi_{ij} = 1$ и $q_{ij}(x) \equiv F_{ij}(x)$.

В случае если $q_{ij}(x) = \pi_{ij}, x \geq 0$, производная $q'_{ik}(t)$ равна δ-функции [10].

Если определить время пребывания в состоянии i при условии, что после его окончания процесс перейдет в состояние j через θ_{ij}, то переходные вероятности π_{ij} вычисляются по формуле:

$$\pi_{ij} = \theta_{ij} \Big/ \sum_{j \in I} \theta_{ij}, i, j \in I \tag{4}$$

Необходимо отметить, что вероятности π_{ij} срабатывания вложенной марковской цепи определяют то, что моделируемому процессу «разрешено» перемещаться из *i*-й позиции в *j*-й переход, при этом перемещения по марковской цепи не зависят от времени и не влияют на временные характеристики перемещения моделируемого процесса из позиции в переход.

Для ССПМ составляются интегро-дифференциальные уравнения для каждого парциального процесса. В частности, для ССПМ, представленной графом, приведенным на рисунке 1, составляются интегро-дифференциальные уравнения для парциальных полумарковских процессов:

1) между нулевым состоянием и переходом 2z с охватом состояния 1;
2) между нулевым состоянием и переходом 3z с охватом состояний 1;
3) между состоянием 2 и переходом 7z с охватом состояния 3;
4) между состоянием 3 и переходом 7z с охватом состояния 4;
5) между состоянием 4 и переходом 6z.

При этом полагается (как и для всех сетей Петри — Маркова [4]), что процесс выходит из перехода мгновенно, а из состояния — за ограниченное случайное время.

На практике, как отмечалось, в одной сети могут иметь место как полумарковские, так и марковские парциальные процессы. Пример такого процесса, включающего в себя как марковские, так и полумарковские парциальные процессы, приведен на рисунке 3.

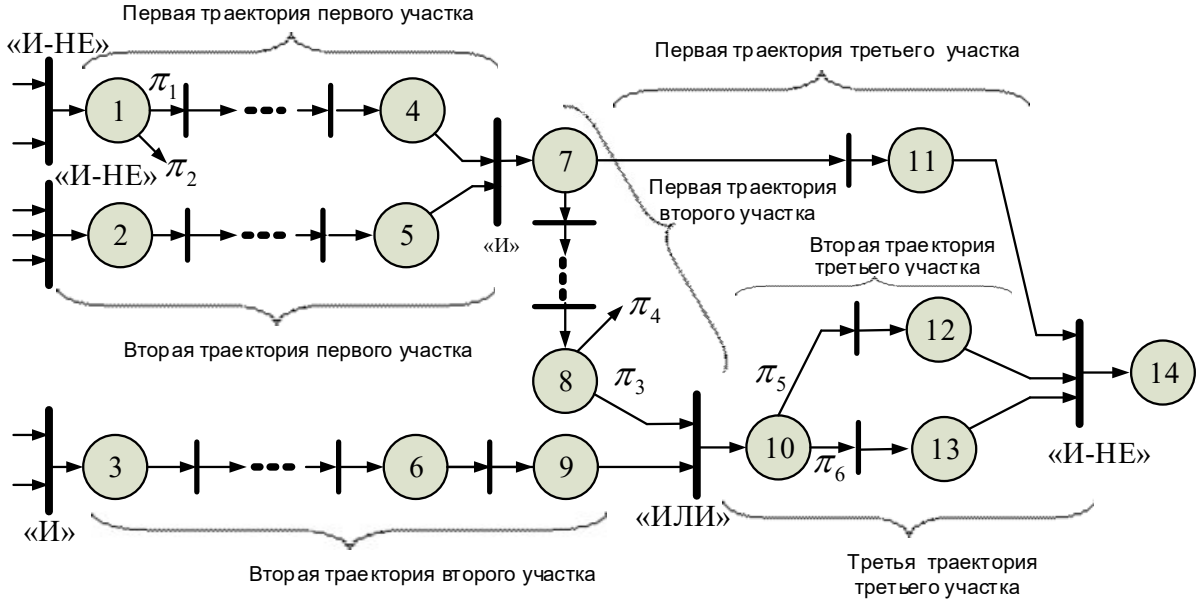

Рис. 3. Пример разбиения на участки и траектории фрагмента сети Петри — Маркова, построенной на основе полумарковских процессов

Приведенная ССПМ разбита на участки между логическими переходами, каждый из которых может иметь более одной траектории перемещения. На рисунке первые траектории первого и второго участка и весь третий участок соответствуют полумарковским парциальным процессами, а остальные траектории — марковским процессам.

Пусть на участке h, завершающемся логическим переходом с некоторой логикой, имеется несколько траекторий и на этот переход с других участков не подходит ни одна дуга (например, две траектории первого участка на рисунке 3).

Для такого участка плотность вероятности времени прохождения процесса из начальной позиции с номером 1 в логический переход с номером J представляет собой свертку функций распределения времен перемещения из каждой позиции в инцидентный ей переход, то есть

$$f_{1,J}^{(h)}(t) = f_{1,1}^{(h)}(t) * f_{2,2}^{(h)}(t) * \ldots * f_{J,J}^{(h)}(t), \tag{5}$$

где $f_{j,j}^{(h)}(t)$ — плотность вероятности для времени перемещения процесса из j-й позиции на траектории h в следующий за ней (инцидентный ей) j-й переход;

*— операция свертки [35],

$$f_{k,m}^{(h)}(t) * f_{s,r}^{(h)}(t) = \int_0^{\infty} f_{k,m}^{(h)}(x-y) \cdot f_{s,r}^{(h)}(y) dy \tag{6}$$

При этом предельная вероятность достижения перехода, то есть вероятность π_{iJ} перемещения по вложенной цепи Маркова из i-й позиции в конечный J-й переход, определяется произведением

$$\pi_{1J} = \prod_{j=1}^{J} \pi_{ij} \tag{7}$$

Так как случайные времена перемещения из позиций в переходы являются статистически независимыми, то математическое ожидание суммарного времени перемещения процесса из начальной позиции траектории в конечный переход определяется простым суммированием математических ожиданий времен ($\overline{\tau_{i,J}^{(h)}}$) перемещения процесса из каждой позиции в каждый переход по данной траектории:

$$\overline{\tau_{i,J}^{(h)}} = \sum_{j=1}^{J} \overline{\tau_{i,j}^{(h)}} \tag{8}$$

Если к логическому переходу на данном участке подходят дуги с других участков, то для них тоже вычисляется время и предельная вероятность перемещения процесса по этим дугам. Аналогичным образом рассчитываются средние времена перемещения по другим участкам.

Для определения вероятностно-временных характеристик (времени и вероятности срабатывания ССПМ) необходимо рассчитать вероятностно-временные характеристики не только перемещения каждого парциального процесса по соответствующему участку, но и срабатывания каждого логического перехода.

3. Алгоритмы расчета вероятностно-временных характеристик срабатывания логических переходов в составной сети Петри — Маркова, построенной на основе полумарковских процессов. Ниже рассматриваются нашедшие наиболее широкое применение при моделировании динамики реализации угроз безопасности информации в информационных системах логические переходы типа «И», «ИЛИ», «И-ИЛИ», «И-НЕ» и «ИЛИ-НЕ».

Пусть имеет место логический переход «И» и к нему подходят две траектории, по которым перемещаются два парциальных процесса с индексами 1и 2 (рис. 4).

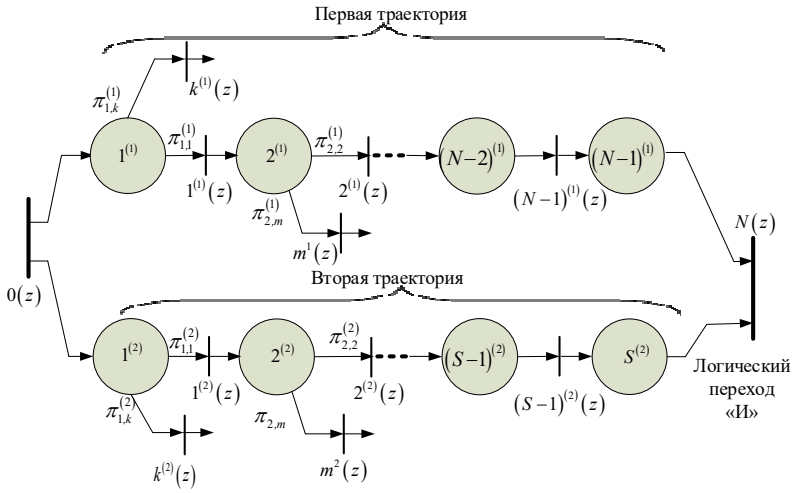

Рис. 4. Траектории перемещения процесса к логическому переходу «И»

Вероятность того, что переход сработает за время t с учетом вероятностей перемещений по вложенной марковской цепи, определяется из соотношения

$$P_{\wedge}(t) = \prod_{\substack{j=1^{(1)},\\ k=1^{(1)},\\ j\neq k}}^{J^{(1)}} \pi_{jk}^{(1)} \cdot \prod_{\substack{j=1^{(2)},\\ k=1^{(2)},\\ j\neq k}}^{J^{(2)}} \pi_{jk}^{(2)} \cdot P_{tr1}(t) \cdot P_{tr2}(t) \tag{9}$$

где верхние индексы соответствуют номеру траектории на графе ССПМ;

$P_{tr1}(t), P_{tr2}(t)$ — вероятности перемещения парциальных процессов за время *t* по первой и второй траектории соответственно, рассчитываемые в общем случае следующим образом:

$$P_{tr1}(t) = \gamma\left(\frac{t}{=}, n_1\right);\ P_{tr2}(t) = \gamma\left(\frac{t}{=}, n_2\right) \tag{10}$$

$\gamma\left\{\frac{t}{=}, n_1\right\}, \gamma\left\{\frac{t}{=}, n_2\right\}$ — неполные гамма-функции [9] со средними значениями времени появления парциальных потоков на простых переходах $\overline{\tau}_1, \overline{\tau}_2$ и параметрами формы n_1 и n_2 (соответствующих количеству простых переходов) для первой и второй траектории соответственно.

В [2] было показано, что случайное время срабатывания парциальных процессов распределено по закону, весьма близкому к экспоненциальному. В этом случае формула (9) преобразуется к виду

$$P_{\wedge}(t) = \prod_{\substack{j=1^{(1)},\\ k=1^{(1)},\\ j\neq k}}^{J^{(1)}} \pi_{jk}^{(1)} \cdot \prod_{\substack{j=1^{(2)},\\ k=1^{(2)},\\ j\neq k}}^{J^{(2)}} \pi_{jk}^{(2)} \cdot \left(1 - e^{-\frac{t}{\overline{\tau_{tr1}}}}\right) \cdot \left(1 - e^{-\frac{t}{\overline{\tau_{tr2}}}}\right) \qquad (11)$$

где $\overline{\tau_{tr1}} = \overline{\tau_1} \cdot n_1$ и $\overline{\tau_{tr2}} = \overline{\tau_2} \cdot n_2$.

Вместо этой формулы для практических расчетов можно использовать экспоненциальную зависимость вероятности срабатывания логического перехода «И» от математического ожидания времени срабатывания этого перехода. Соответствующие соотношения для расчета приведены в таблице.

Аналогичным образом рассчитываются вероятностно-временные характеристики срабатывания переходов «ИЛИ» и «И-ИЛИ» (см. таблицу).

Соотношения для расчета математических ожиданий времен и вероятностей срабатывания логических переходов для составных сетей Петри — Маркова

Логическое условие	Вероятность срабатывания логического перехода	Соотношение для расчета математического ожидания времени срабатывания перехода при экспоненциальных распределениях	Формула для расчета вероятности срабатывания логического перехода при экспоненциальном приближении
$1 \wedge 2$ («И») (переход срабатывает, когда оба парциальных процесса подошли к переходу)	$P_{\wedge}(t) = \pi_{tr1} \cdot \pi_{tr2} \cdot P_{tr1}(t) \cdot P_{tr1}(t)$, $\pi_{tr1} = \prod_{\substack{j=\overline{1,f^{(1)}}, \\ k=\overline{1,f^{(1)}}, \\ j \neq k}} \pi_{jk}^{(1)}$; $\pi_{tr2} = \prod_{\substack{j=\overline{1,f^{(2)}}, \\ k=\overline{1,f^{(2)}}, \\ j \neq k}} \pi_{jk}^{(2)}$	$\overline{\tau_{\wedge}} = \frac{\overline{\tau_1}^2 + \overline{\tau_1} \cdot \overline{\tau_2} + \overline{\tau_2}^2}{\overline{\tau_1} + \overline{\tau_2}}$	$P_{\wedge}(t) = \pi_{tr1} \cdot \pi_{tr2} \cdot \left(1 - e^{-\frac{t}{\overline{\tau_{\wedge}}}}\right)$
$1 \vee 2$ («ИЛИ») (переход срабатывает, когда хотя бы один из парциальных процессов подошел к переходу)	$P_{\vee}(t) = 1 - \left[1 - \pi_{tr1} \cdot P_{tr1}(t)\right] \cdot \left[1 - \pi_{tr2} \cdot P_{tr1}(t)\right]$	$\overline{\tau_{\vee}} = \frac{\overline{\tau_1} \cdot \overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}}$	$P_{\vee}(t) \approx \left[1 - (1 - \pi_{tr1}) \cdot (1 - \pi_{tr2})\right] \cdot \left[1 - e^{-\frac{t}{\overline{\tau_{\vee}}}}\right]$
$(1 \wedge 2) \vee 3$ («И-ИЛИ») (переход срабатывает, когда первые два парциальных процесса подошли к переходу или третий)	$P_{\wedge\vee}(t) = 1 - \left[1 - \pi_{tr1} \cdot \pi_{tr2} \cdot P_{tr1}(t) \cdot P_{tr2}(t)\right] \times \left[1 - \pi_{tr3} \cdot P_{tr3}(t)\right]$	$\overline{\tau_{\wedge\vee}} = \overline{\tau_1} + \overline{\tau_2} - \frac{\overline{\tau_1} \cdot \overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}} - \frac{\overline{\tau_3}^2 \overline{\tau_1}}{\left(\overline{\tau_1} + \overline{\tau_3}\right)^2} - \frac{\overline{\tau_3}^2 \overline{\tau_2}}{\left(\overline{\tau_2} + \overline{\tau_3}\right)^2} + \frac{\overline{\tau_1} \cdot \overline{\tau_2} \cdot \overline{\tau_3}}{\overline{\tau_1} \cdot \overline{\tau_2} + \overline{\tau_1} \cdot \overline{\tau_3} + \overline{\tau_2} \cdot \overline{\tau_3}}$	$\hat{P}_{\wedge\vee}(t) = \left[1 - (1 - \pi_{tr1} \cdot \pi_{tr2}) \cdot (1 - \pi_{tr3})\right] \cdot \left(1 - e^{-\frac{t}{\tau_{max}}}\right)$
$1 \neg 2$ «И-НЕ»[8] (переход срабатывает, когда первый парциальный процесс подошел к переходу, а второй нет)	$P_{\wedge\neg}(t) = \pi_{tr1} \cdot P_{tr1}(t) \cdot \left\{\begin{array}{l} 1 - \left[1 - (1 - \pi_{tr2}) \cdot P_{tr2}(t)\right] \times \\ \times \left[1 - \pi_{tr2} \cdot (1 - P_{tr2}(t))\right] \end{array}\right.$	$\overline{\tau_{\wedge\neg}} = \overline{\tau_1} \cdot \left(1 + \frac{\overline{\tau_1}}{\overline{\tau_2}}\right)$	$P_{\wedge\neg}(t) \approx \pi_{tr1} \cdot (1 - \pi_{tr2}) \cdot \left(1 - e^{-\frac{t}{\overline{\tau_{\wedge\neg}}}}\right)$
$(1 \vee 2) \neg 3$ («ИЛИ-НЕ») (переход срабатывает, когда первый или второй парциальные процессы подошли к переходу, а третий нет)	$P_{\vee\neg}(t) = \left[1 - \left(1 - \pi_{tr1} \cdot P_{tr1}(t)\right) \cdot \left(1 - \pi_{tr2} \cdot P_{tr2}(t)\right] \times \left\{1 - \left[1 - (1 - \pi_{tr3}) \cdot P_{tr3}(t)\right] \cdot \left[1 - \pi_{tr3} \cdot (1 - P_{tr3}(t))\right.\right.$	$\overline{\tau_{\vee\neg}} = \overline{\tau_{\vee}^{(1,2)}} \cdot \left(1 + \frac{\overline{\tau_{\vee}^{(1,2)}}}{\overline{\tau_3}}\right)$, где $\overline{\tau_{\vee}^{(1,2)}} = \frac{\overline{\tau_1} \cdot \overline{\tau_2}}{\overline{\tau_1} + \overline{\tau_2}}$	$P_{\vee\neg}(t) \approx \left[1 - (1 - \pi_{tr1})(1 - \pi_{tr2})\right] \cdot (1 - \pi_{tr3}) \times \times \left(1 - e^{-\frac{t}{\overline{\tau_{\vee\neg}}}}\right)$

Для переходов с логиками «И-НЕ» и «ИЛИ-НЕ», как показано в [2], расчет должен проводиться по-другому — на основе теории рекуррентного прореживания потоков [11], так как вероятности срабатывания таких переходов не являются функциями распределения, поскольку и в нуле, и на бесконечности они равны нулю, и по ним не-

возможно рассчитать математические ожидания и дисперсии. В [1, 2] получены формулы для ССПМ, построенных на основе марковских процессов, а в таблице 1 с учетом этих формул приведены соотношения для ССПМ на основе полумарковских процессов, в которые введены вероятности переходов для вложенных марковских цепей.

Наконец, следует отметить, что при построении СПМ на основе составных полумарковских процессов появляется возможность расчета вероятности реализации угрозы при альтернативных вариантах развития моделируемого процесса (рис. 5).

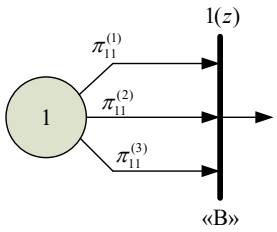

Рис. 5. Фрагмент сети Петри — Маркова с альтернативными вариантами развития моделируемого процесса

В этом случае или для каждого варианта строится своя СПМ, или на графе СПМ с альтернативными вариантами вводится дополнительный логический переход «Выбор» («В»), при поступлении на который процесса с вероятностями $\pi_{ij}^{(h)}, h = \overline{1,H}, \sum_h \pi_{ij}^{(h)} = 1$ осуществляется выбор одной из альтернатив и далее для нее проводится расчет, затем выбираются другие альтернативы и по ним также проводятся расчеты.

В результате расчета получаются альтернативные результаты, которые затем могут быть свернуты с вероятностями $\pi_{ij}^{(h)}$ в один результирующий показатель оценки возможности реализации угрозы.

Примеры применения ССПМ на основе полумарковских процессов при моделировании процессов реализации угроз безопасности информации в ИС приведены на рисунках 6 и 7.

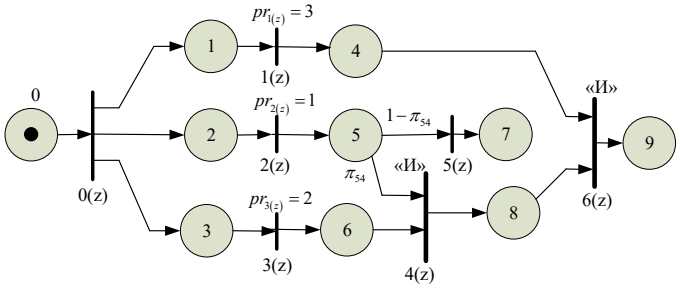

Рис. 6. Подмена доверенного объекта (IP- spoofing):

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 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 $1-\pi_{54}$ 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 π_{54} удалось подобрать номера ответного пакета и порта взаимодействия и функционирование доверенного хоста нарушено;

5(z) — нарушителю с вероятностью $1-\pi_{54}$ 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.

Соотношение для расчета среднего времени и вероятности реализации угрозы:

$$\overline{\tau_{2(z)}^{(pr)}}=\overline{\tau_{22}};\ \overline{\tau_{3(z)}^{(pr)}}=\overline{\tau_{22}}\cdot\left(1+\frac{\overline{\tau_{22}}}{\overline{\tau_{33}}}\right);\ \overline{\tau_{1(z)}^{(pr)}}=\overline{\tau_{3(z)}^{(pr)}}\cdot\left(1+\frac{\overline{\tau_{3(z)}^{(pr)}}}{\overline{\tau_{11}}}\right)$$

$$\overline{\overline{\tau_{4(z)}}}=\frac{\left(\overline{\tau_{2(z)}}+\overline{\tau_{54}}\right)^2+\left(\overline{\tau_{2(z)}}+\overline{\tau_{54}}\right)\cdot\left(\overline{\tau_{3(z)}}+\overline{\tau_{64}}\right)+\left(\overline{\tau_{3(z)}}+\overline{\tau_{64}}\right)^2}{\overline{\tau_{2(z)}}+\overline{\tau_{54}}+\overline{\tau_{3(z)}}+\overline{\tau_{64}}}$$

$$\overline{\overline{\tau_u}}=\overline{\overline{\tau_{00}}}+\frac{\left(\overline{\tau_{1(z)}^{(pr)}}+\overline{\tau_{46}}\right)^2+\left(\overline{\tau_{1(z)}^{(pr)}}+\overline{\tau_{46}}\right)\cdot\left(\overline{\tau_{4(z)}}+\overline{\tau_{86}}\right)+\left(\overline{\tau_{4(z)}}+\overline{\tau_{86}}\right)^2}{\left(\overline{\tau_{1(z)}^{(pr)}}+\overline{\tau_{46}}\right)+\left(\overline{\tau_{4(z)}}+\overline{\tau_{86}}\right)};$$

$$P_u(t)=\pi_{54}\cdot\left(1-e^{-\frac{t}{\overline{\overline{\tau_u}}}}\right)$$

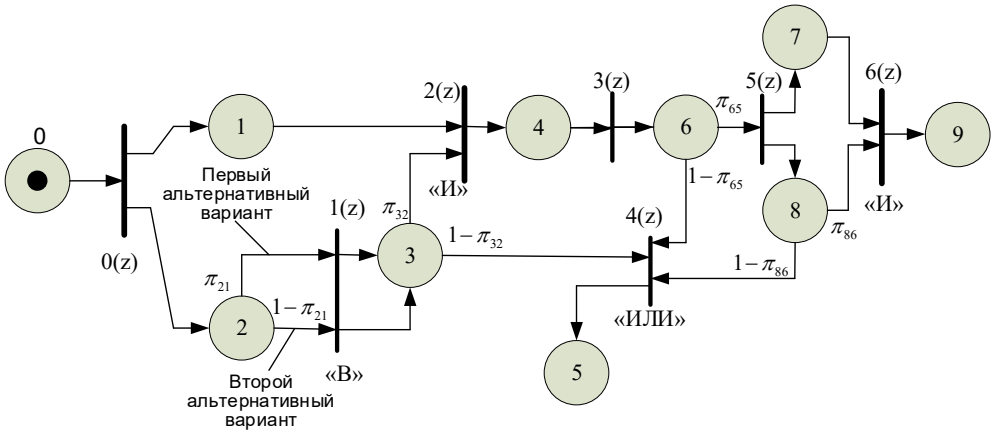

Рис. 7. Несанкционированный запуск приложения:

где 0 — нарушитель сделал запрос на соединение с атакуемым хостом;

1 — абонентом проведен запрос пароля;

2 — нарушитель, не зная пароля, решил подобрать его путем прямого перебора (первый вариант) или по специальному словарю (второй вариант);

3 — нарушитель завершил подбор пароля;

4 — пароль подобран правильно;

5 — атака сорвана;

6 — поиск приложения завершен;

7 — предпринята попытка запуска приложения;

8 — проведен анализ трафика на предмет обнаружения атаки;

9 — атака реализована;

0(z) — абонент — объект атаки запрашивает пароль;

1(z) — подбор пароля по словарю или прямым перебором (логический переход «Выбор»);

2(z) — при наличии запроса на соединение на атакуемом хосте вводится пароль доступа для нарушителя (логический переход «И»);

3(z) — получение доступа в операционную среду объекта атаки и поиск приложения;

4(z) — формирование сообщения об отказе в доступе или из-за неправильно подобранного пароля, или из-за обнаружения атаки, или из-за срыва поиска нужного приложения (логический переход «ИЛИ»);

5(z) — передача команды на запуск приложения, включение системы обнаружения вторжений на атакуемом хосте;

6(z) — запуск приложения при условии пропуска атаки.

Соотношение для расчета среднего времени и вероятности реализации угрозы:

$$\overline{\tau_u} = \overline{\tau_{06}} = \overline{\tau_{00}} + \overline{\tau_{2(z)}} + \overline{\tau_{6(z)}}; \overline{\tau_{2(z)}} = \frac{\overline{\tau_{12}^2} + \overline{\tau_{12}} \cdot \overline{\tau_{22}} + \overline{\tau_{22}^2}}{\overline{\tau_{12}} + \overline{\tau_{22}}};$$

$$\overline{\tau_{22}} = \overline{\tau_{21}} + \overline{\tau_{32}};$$

$$\overline{\tau_{6(z)}} = \overline{\tau_{43}} + \overline{\tau_{65}} + \frac{\overline{\tau_{76}^2} + \overline{\tau_{76}} \cdot \overline{\tau_{86}} + \overline{\tau_{86}^2}}{\overline{\tau_{76}} + \overline{\tau_{86}}};$$

$$P_u(t)=\begin{cases}\pi_{21}\cdot\pi_{32}\cdot\pi_{65}\cdot\pi_{86}\cdot(1-e^{-\frac{t}{\tau_u}})-\text{в первом варианте;}\\(1-\pi_{21})\cdot\pi_{32}\cdot\pi_{65}\cdot\pi_{86}\cdot(1-e^{-\frac{t}{\tau_u}})-\text{во втором варианте}\end{cases}$$

Заключение. Оценивая возможности применения аппарата составных СПМ на основе полумарковских процессов, необходимо отметить важность корректного задания вероятностей перемещения по вложенной цепи Маркова. Как правило, для этого приходится разрабатывать дополнительные модели, связанные с динамикой преодоления мер защиты (например, подбора пароля), успешным с некоторой вероятностью характером каких-либо действий (например, выявления открытого порта, номера пакета, внедрения вредоносной программы), своевременным обнаружением сетевой атаки или вредоносной программы и т. д. Для разработки таких моделей, в свою очередь, могут быть использованы составные СПМ на основе как марковских, так и полумарковских процессов.

ЛИТЕРАТУРА

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

2. Язов Ю. К., Анищенко А. В. Сети Петри — Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. — Воронеж : Кварта, 2020. — 173 с.

3. Игнатьев В. М., Ларкин Е. В. Сети Петри — Маркова. — Тула : ТулГТУ, 1994. — 163 с.

4. Математическая модель локальной политики безопасности с учетом структурных особенностей автоматизированной информационной системы информационного центра / В. И. Сумин, А. В. Душкин, С. В. Родин, М. А. Жукова // Математические методы и информационно-технические средства : материалы IX Всероссийской научно-практической конференции. — Краснодар : Краснодарский университет МВД России. — 2013. — С. 305—307.

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

6. Сети Петри. WF-сети. — URL: https//ru.wikipedis.org/wiki/WF-сеть.

7. Рудометкина М. Н., Спицын В. Г. Модель логической сети с предикатными операциями // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 10-3. — С. 21—26. — URL: http://applied-research.ru/ru/article/view?id=6019.

8. Сильверстов Д. С. Полумарковские процессы с дискретным множеством состояний. — М. : Советское радио, 1980.

9. Королюк В. С., Турбин А. Ф. Полумарковские процессы и их приложения. — Киев : Наукова думка, 1976.

10. Справочник по теории вероятностей и математической статистике / В. С. Королюк, Н. И. Портенко, А. В. Скороход, А. Ф. Турбин. — М. : Наука. Главная редакция физико-математической литературы, 1985. — 640 с.

11. Климов Г. П. Стохастические системы обслуживания. — М. : Наука, 1966. — 244 с.

REFERENCES

1. Yazov Yu. K. Osnovy` metodologii kolichestvennoj ocenki e`ffektivnosti zashhity` informacii v komp`yuterny`x sistemax. — Rostov-na-Donu : SKNCz VSh, 2006. — 274 s.

2. Yazov Yu. K., Anishhenko A. V. Seti Petri-Markova i ix primenenie dlya modelirovaniya processov realizacii ugroz bezopasnosti informacii v informacionny`x sistemax. — Voronezh : Kvarta, 2020. — 173 s.

3. Ignat`ev V. M., Larkin E. V. Seti Petri — Markova. — Tula : TulGTU, 1994. — 163 s.

4. Matematicheskaya model` lokal`noj politiki bezopasnosti s uchetom strukturny`x osobennostej avtomatizirovannoj informacionnoj sistemy` informacionnogo centra / V. I. Sumin, A. V. Dushkin, S. V. Rodin, M. A. Zhukova // Matematicheskie metody` i informacionno-texnicheskie sredstva : materialy` IX Vserossijskoj nauchno-prakticheskoj konferencii. — Krasnodar : Krasnodarskij universitet MVD Rossii. — 2013. — S. 305—307.

5. Kotov V. E. Seti Petri. — M. : Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury`, 1984. — 160 s.

6. Seti Petri. WF-seti. — URL: https//ru.wikipedis.org/wiki/WF-set`.

7. Rudometkina M. N., Spicyn V. G. Model` logicheskoj seti s predikatny`mi operaciyami // Mezhdunarodny`j zhurnal prikladny`x i fundamental`ny`x issledovanij. — 2014. — № 10-3. — S. 21—26. — URL: http://applied-research.ru/ru/article/view?id=6019.

8. Sil`verstov D. S. Polumarkovskie processy` s diskretny`m mnozhestvom sostoyanij. — M. : Sovetskoe radio, 1980.

9. Korolyuk V. S., Turbin A. F. Polumarkovskie processy` i ix prilozheniya. — Kiev : Naukova dumka, 1976.

10. Spravochnik po teorii veroyatnostej i matematicheskoj statistike / V. S. Korolyuk, N. I. Portenko, A. V. Skoroxod, A. F. Turbin. — M. : Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury`, 1985. — 640 s.

11. Klimov G. P. Stoxasticheskie sistemy` obsluzhivaniya. — M. : Nauka, 1966. — 244 s.