

**Язов Юрий Константинович;**  
доктор технических наук; профессор;  
**Соловьев Сергей Вениаминович;**  
**Тарелкин Михаил Андреевич**

**ПРИМЕНЕНИЕ СОСТАВНЫХ СЕТЕЙ ПЕТРИ-МАРКОВА  
ПРИ МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ  
УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

**APPLICATIONS OF COMPOSITE PETRI-MARKOV NETS  
IN MATHEMATICAL MODELING  
INFO SECURITY THREATS**

*Приводятся результаты мониторинга сведений об атаках и инцидентах на объектах российской инфраструктуры в этом году и отмечается не только возрастание интенсивности атак, но и существенное расширение спектра угроз в информационной сфере. Указывается на важность аналитического моделирования процессов реализации угроз с учетом фактора времени при их анализе в интересах обоснования мер и средств защиты от них. Приводится сравнительная характеристика аппаратов сетей Петри, марковских и полумарковских процессов, традиционных и составных сетей Петри-Маркова. Указываются преимущества аппарата составных сетей Петри-Маркова, позволяющего учесть как фактор времени и параллельность выполнения парциальных процессов при реализации угроз, так и наличие логических условий выполнения этих процессов. Приводятся соотношения для расчета вероятностей реализации угроз при наличии логических условий с пропозициональной логикой выполнения «И», «ИЛИ», «И-ИЛИ», «И-НЕ», «ИЛИ-НЕ». Показывается возможность экспоненциального приближения для плотностей распределения времени реализации угроз безопасности информации в информационных системах.*

*The results of monitoring information about attacks and incidents on Russian infrastructure facilities this year are given and not only an increase in the intensity of attacks is noted, but also a significant expansion of the range of threats in the information sphere. The importance of analytical modeling of the processes of implementation of threats, taking into account the time factor in their analysis in the interests of justifying measures and means of protection against them, is pointed out. Comparative characteristics of apparatuses of Petri nets, Markov and semi-Markov processes, traditional and composite Petri-Markov nets are given. The advantages of the apparatus of composite Petri-Markov networks are indicated, which allow taking into account both the time*

*factor and the parallelism of the execution of partial processes in the implementation of threats, as well as the presence of logical conditions for the execution of these processes. Ratios are given for calculating the probabilities of threats realization in the presence of logical conditions with the propositional logic of execution "AND", "OR", "AND-OR", "AND-NOT", "OR-NOT". The possibility of exponential approximation for the distribution densities of the time of implementation of information security threats in information systems is shown.*

В начале 60-х годов 20-го века немецким математиком **Карлом Петри** был предложен метод описания и анализа дискретных параллельных процессов для моделирования асинхронных информационных потоков в системах преобразования данных [1]. В 80-х годах прошлого века теория сетей Петри интенсивно развивалась. Появились многочисленные подклассы сетей Петри [2], такие как временные сети Петри, в которых переходы обладают весом, определяющим продолжительность или задержку срабатывания переходов из состояния в состояние, стохастические сети Петри со случайными задержками срабатывания, цветные сети с различными типами позиций и переходов, обозначаемых цветами, иерархические сети и т.д. Вместе с тем, аппарат сетей Петри, являясь развитием аппарата конечных автоматов, в основном был ориентирован на имитационное моделирование. В частности, с его использованием разрабатывались в нашем институте имитационные модели процесса функционирования ложных информационных систем в виртуальной среде. Для аналитического моделирования он оказался неприемлем, да и логические условия выполнения моделируемых процессов невозможно было моделировать с его использованием.

Для учета вероятностно-временных характеристик моделируемых процессов, параллельности выполнения процедур в ходе реализации таких процессов в интересах решения задач математического моделирования отказов/восстановлений в рамках теории надежности учеными Тульского государственного университета еще в 90-х годах прошлого века был предложен аппарат сетей Петри-Маркова [3].

При всем богатстве идей, заложенных в этот новый аппарат, он не позволяет учитывать логические условия выполнения моделируемого процесса с пропозициональной логикой, такой как логики «И», «ИЛИ», «И-ИЛИ», «И-НЕ» и т.д., что очень часто имеет место в процессах реализации угроз безопасности информации в информационных системах. Необходимость моделирования процессов реализации угроз стала понятной еще в начале этого века. Поэтому в ГНИИИ ПТЗИ ФСТЭК России тогда было предложено существенное расширение этого аппарата.

Сегодня это оказывается еще более актуальным, так как интенсивность процессов реализации угроз постоянно возрастает, количество атак сегодня весьма внушительно, что видно из рис. 1, где отражены результа-

ты мониторинга сведений об атаках и инцидентах на объектах российской инфраструктуры в этом году.

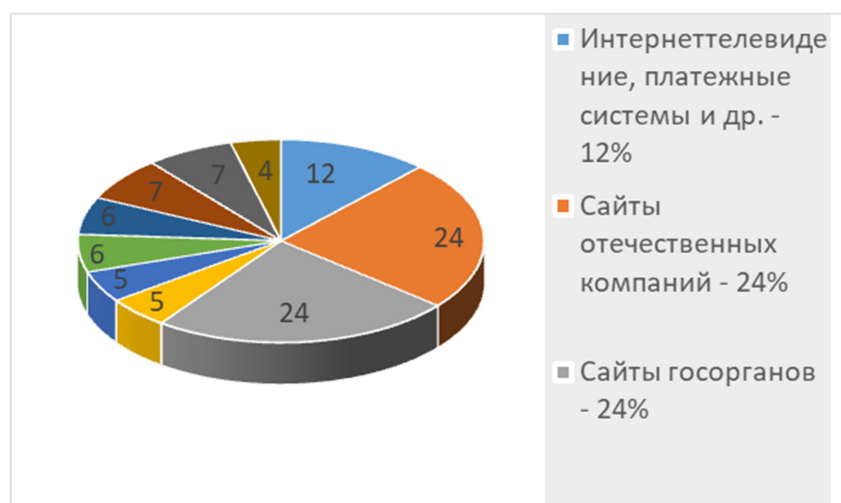


Рис. 1 – Результаты мониторинга сведений об атаках и инцидентах на объектах российской инфраструктуры с 26 февраля по 7 июля 2022 г.

Но важно еще и то, что спектр угроз существенно расширяется. При этом корректная оценки возможности реализации угроз, выявления приемлемых мер защиты и оценка их эффективности практически невозможна без математического моделирования процессов реализации угроз, что обусловлено целым рядом факторов, к основным из которых относятся:

- необходимость перехода от качественных экспертных процедур анализа угроз безопасности информации к количественным в интересах предотвращения атак и возникновения инцидентов безопасности;

- необходимость переход к количественным оценкам эффективности защиты информации и повышение тем самым обоснованности требований к мерам и средствам защиты;

- перспективы разработки экспертных систем в интересах совершенствования организации и ведения защиты информации на объектах информатизации;

- необходимость учета фактора времени при оценке возможностей реализации угроз безопасности информации, при обосновании эффективности мер защиты и применения систем защиты и др.

Среди них следует подчеркнуть необходимость учета фактора времени, особенно в случаях, когда необходимо обосновать меры защиты, направленные на опережение процессов реализации угроз сетевых атак.

Сегодня атаки реализуются не только на сетевом, системном и прикладном, но и на микропрограммном системно-технических уровнях. Как правило сетевая атака представляет собой многоэтапный процесс. Напри-

мер, сетевые атаки на системном и прикладном уровнях реализуются чаще всего в четыре этапа, показанных на рис. 3, при этом не для всех этапов требуется моделирование динамики процесса, а в основном для этапов вторжения и выполнения несанкционированных действий.

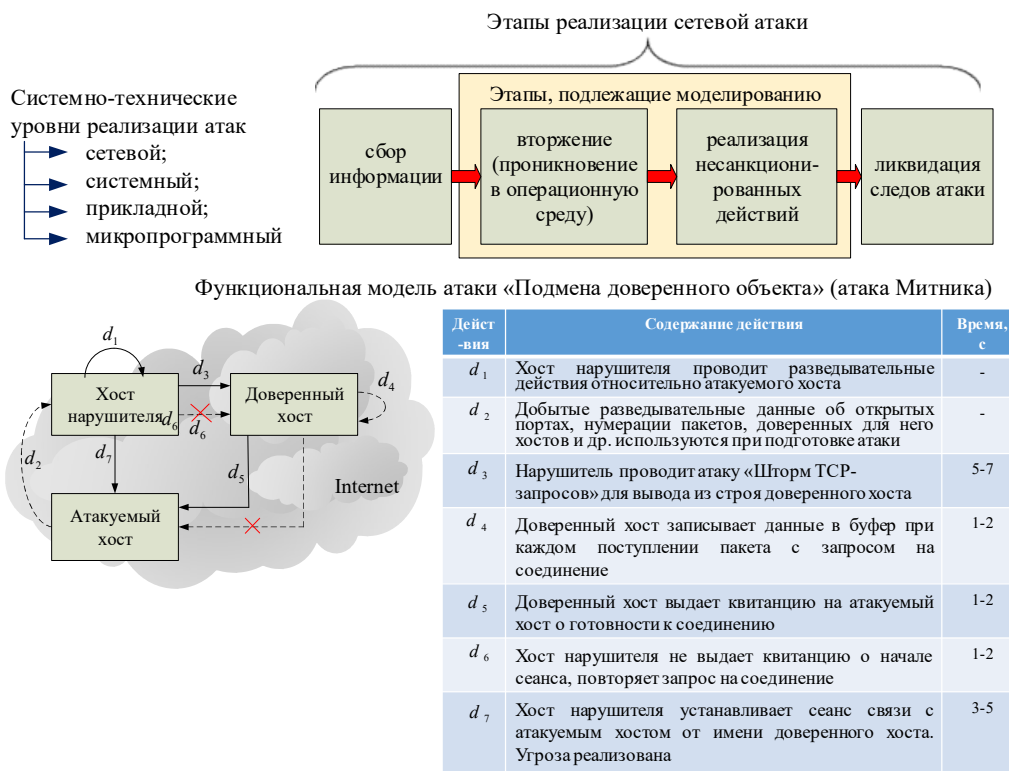


Рис. 2 – Этапы реализации сетевой атаки и пример функциональной модели атаки «Подмена доверенного объекта»

Кроме того, для разработки математической модели необходимо иметь соответствующие описания атак с указанием времен выполнения действий как нападающей, так и защищающейся стороны, если применяются меры защиты. А это значит, что нужно разработать для каждой атаки ее функциональную модель, содержащую не только описание действий, их взаимосвязь и последовательность выполнения, но и временные характеристики выполнения. Пример такой модели атаки «Подмена доверенного объекта» приведен на рис. 2.

Если имеется функциональная модель атаки, то далее необходимо определить, какой аппарат пригоден для математического моделирования этой атаки с учетом динамики ее реализации. Для этого наиболее часто используются аппараты марковских, полумарковских процессов и составных сетей Петри-Маркова на основе марковских и полумарковских процессов. Краткая характеристика марковских и полумарковских процессов сводится к следующему.

Основное свойство марковских процессов состоит в том, что в нем будущее процесса не зависит от прошлого, а определяется настоящим (свойство марковости) [4]. Существует 4 вида марковских процессов: цепь Маркова, дискретный марковский процесс, марковская последовательность и непрерывнозначный процесс Маркова. В практике моделирования угроз безопасности информации в основном применяются первые два. На рисунке 3 представлена для примера модель процесса инфицирования файла на основе марковской цепи с соотношением для расчета вероятности такого инфицирования за  $k$  шагов.

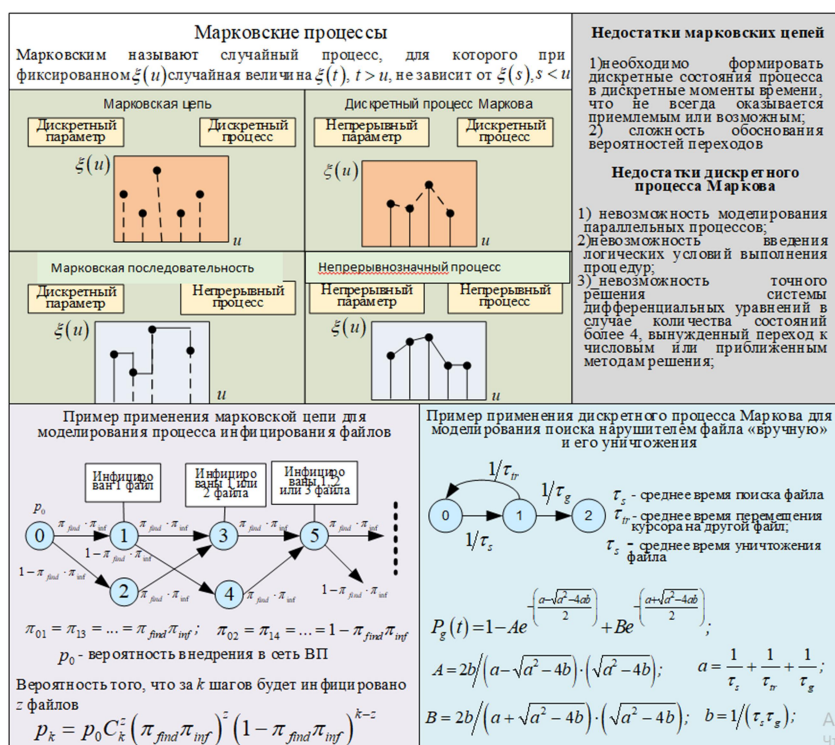


Рис. 3 – Марковские процессы и возможности их использования для моделирования угроз

На рис. 3 представлена также модель поиска нарушителем файла «вручную» и его уничтожение с использованием штатной программы операционной системы, а также формула для расчета вероятности реализации угрозы. Основные недостатки марковских цепей и дискретного процесса Маркова приведены на этом же рисунке.

Рассматривая особенности моделирования с использованием традиционного аппарата сетей Петри-Маркова, необходимо отметить следующее. Как и сеть Петри, сеть Петри-Маркова является ориентированным графом с состояниями, нумерованными с буквой «а», и переходами, нумерованными с буквой «z» (рис. 4). В таких сетях перемещения процесса из состояния в переход считаются конечными во времени и случайными, а перемещения из перехода в состояние – мгновенными.

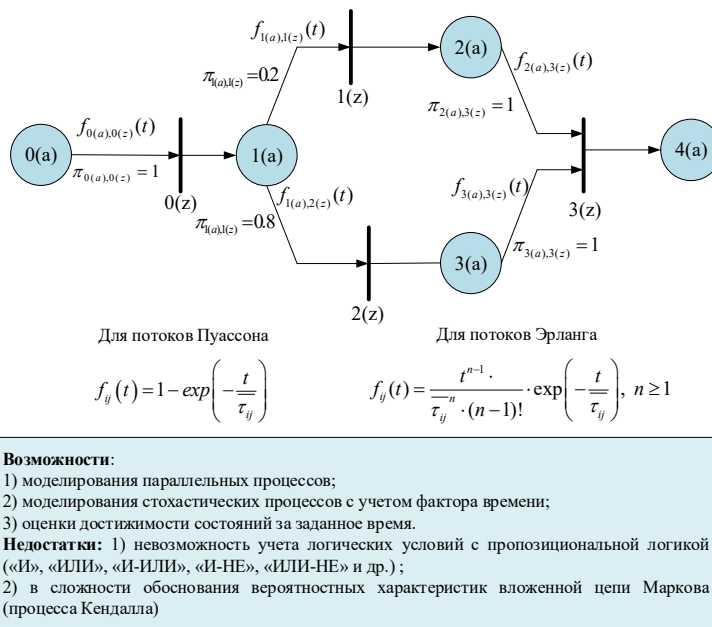


Рис. 4 – Возможности и недостатки традиционных сетей Петри-Маркова

При этом случайные времена перемещения из состояния в переход характеризуются соответствующими плотностями вероятностей. Это может быть экспоненциальное распределение, то есть поток событий является пуассоновским, или в виде распределения Эрланга с параметром потока Эрланга, равным целому числу  $n$ . Кроме того, срабатывание каждого перехода сети характеризуется соответствующей вероятностью переходов. Совокупность этих вероятностей определяет так называемую вложенную цепь Маркова (процесс Кендалла) [5]. На переходы могут накладываться логические условия их срабатывания, однако в традиционных сетях эти условия не являются статистическими и связываются с логической функцией, принимающей значение 1, если переход разрешается, или 0, если переход запрещается, помимо условия, определяемого вероятностью срабатывания перехода для вложенной цепи Маркова. Таким образом, это не позволяет учитывать случайные времена срабатывания переходов, для которых может иметь место пропозициональная логика («И», «ИЛИ» и т.д.). Возможности и основные недостатки таких сетей приведены на рис. 4.

Все это привело к необходимости модификации традиционного аппарата сетей Петри-Маркова и перехода к составным сетям [6]. Составная сеть Петри-Маркова – это сеть, состоящая из нескольких участков, каждый из которых находится или между первым простым и первым логическим переходом, или между логическими переходами, а также после последнего логического перехода. На каждом участке определяются возможные траектории, по которым может развиваться процесс в соответствии с предварительно разработанной функциональной моделью (рис. 5).



Следует отметить, что если траектория не имеет разветвления, то математическое ожидание времени выполнения процесса по этой траектории является суммой математических ожиданий времен перемещения подпроцесса из состояний в переходы, независимо от законов распределения, которым подчиняются распределения суммируемых случайных времен (верхний рисунок справа). В случае марковского составного процесса получается достаточно простая формула для расчета вероятности того, что за заданное время процесс перейдет в конечное состояние, то есть угрозы окажется реализованной.

В случае, когда составной процесс является полумарковским (характерным признаком этого является его разветвление, то есть из состояния выходят несколько дуг),

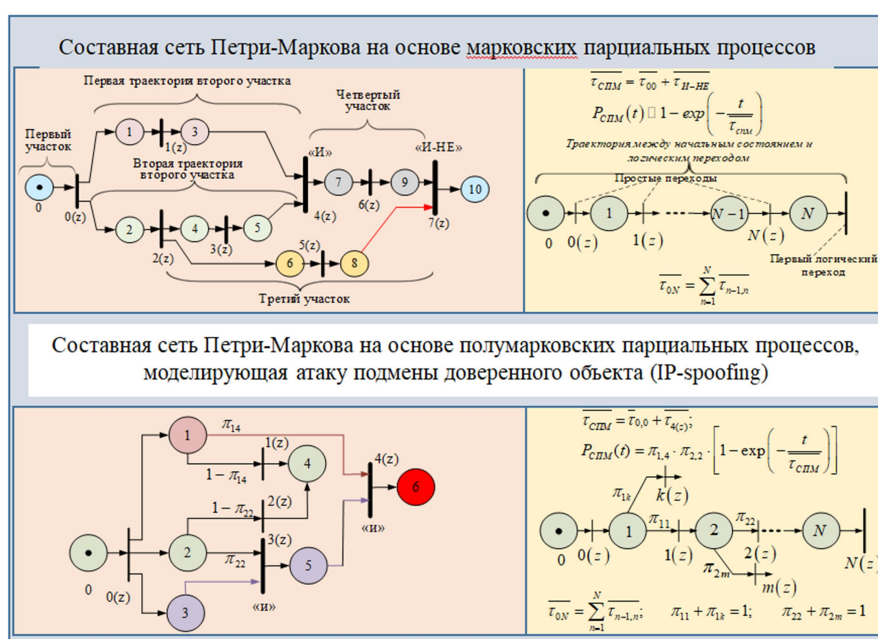


Рис. 5 – Составные сети Петри-Маркова

сначала проводится расчет математического ожидания времени срабатывания сети без учета вероятностей перехода из состояния в состояние для вложенной марковской цепи (см. рис. 5), то есть как и для марковского процесса. А затем с учетом этих вероятностей переходов определяется вероятность того, что за заданное время угроза будет реализована.

С учетом изложенного и судя по приведенным примерам необходимо уметь рассчитывать математические ожидания времен срабатывания логических переходов. Для переходов с логикой «И», «ИЛИ», «И-ИЛИ» найти аналитические соотношения для расчета оказалось достаточно просто, хоть и громоздко. Для логики «И» вероятность срабатывания перехода является произведением вероятностей того, что процесс подойдет к логическому переходу к заданному моменту времени по всем инцидентным ду-

гам. При этом вероятность является, по сути, функцией распределения времени срабатывания перехода: она равна нулю в начале процесса и единице при времени, стремящемся к бесконечности. Тогда для пуассоновских входящих потоков нетрудно получить математическое ожидание времени срабатывания перехода с логикой «И». Для эрланговских потоков математические ожидания времен наступления событий рассчитываются как произведения математического ожидания времени на параметр эрланговского потока. Поэтому результирующая формула принимает вид, показанный на рис. 6.

Для логики «ИЛИ», вероятность срабатывания перехода соответствует вероятности того, что к переходу подойдет хотя бы один из парциальных процессов, а для логики «И-ИЛИ» – вероятности того, что процесс подойдет к переходу по первой и второй дуге или по третьей. При этом вероятности срабатывания переходов также соответствуют требованиям, предъявляемым к функциям распределения случайных величин. Поэтому по аналогии с тем, как это делалось для перехода с логикой «И», находятся формулы для расчета математического ожидания времени срабатывания и этих логических переходов (см. рис. 6).



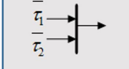
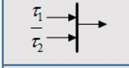
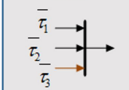
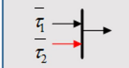
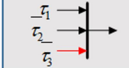
Переход «И» 	$P_I(t) = P_1(t) \cdot P_2(t); \quad f_I(t) = f_1(t) \cdot P_2(t) + f_2(t) \cdot P_1(t); \quad \overline{\tau_I} = \int_0^\infty t \cdot f_I(t) dt$ При пуассоновских потоках: $\overline{\tau_I} = \frac{\tau_1^2 + \tau_2^2 + \tau_1 \cdot \tau_2}{\tau_1 + \tau_2}$ ;      При эрланговских потоках: $\overline{\tau_I} = \frac{(\tau_1 \cdot n_1)^2 + \tau_1 \cdot n_1 \cdot \tau_2 \cdot n_2 + (\tau_2 \cdot n_2)^2}{\tau_1 \cdot n_1 + \tau_2 \cdot n_2}$
Переход «ИЛИ» 	$P_{II}(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)]; \quad f_{II}(t) = f_1(t) \cdot [1 - P_2(t)] + f_2(t) \cdot [1 - P_1(t)];$ При пуассоновских: $\overline{\tau_{II}} = \frac{\tau_1 \cdot \tau_2}{\tau_1 + \tau_2}$ ;      При эрланговских: $\overline{\tau_{II}} = \frac{\tau_1 \cdot n_1 \cdot \tau_2 \cdot n_2}{\tau_1 \cdot n_1 + \tau_2 \cdot n_2}$
Переход «И-ИЛИ» 	$P_{II-II}(t) = 1 - [1 - P_1(t) \cdot P_2(t)] \cdot [1 - P_3(t)]$ $f_{II-II}(t) = [f_1(t) \cdot P_2(t) + f_2(t) \cdot P_1(t)] \times [1 - P_3(t)] + f_3(t) \cdot [1 - P_1(t) \cdot P_2(t)]$ При пуассоновских потоках: $\overline{\tau_{II-II}} = \frac{\tau_1 \tau_2}{\tau_1 + \tau_2} + \frac{\tau_1^2 \tau_3}{(\tau_1 + \tau_3)^2} + \frac{\tau_2^2 \tau_3}{(\tau_2 + \tau_3)^2} - \frac{\tau_1 \tau_2 \tau_3}{\tau_1 \tau_2 + \tau_1 \tau_3 + \tau_2 \tau_3}$
Переход «И-НЕ» 	$P_{I-NE}(t) = P_1(t) \cdot [1 - P_2(t)]; \quad y = \tau_2 - \tau_1; \quad y > 0$ $f_{I-NE}(y) = \frac{1}{\tau_1 + \tau_2} e^{-\frac{y}{\tau_1 + \tau_2}} + \frac{1}{\tau_1 + \tau_2} \delta(y); \quad P_{y=0} = \frac{\tau_2}{\tau_1 + \tau_2}$ При пуассоновских: $\overline{\tau_{I-NE}} = \frac{\tau_1}{\tau_1 + \tau_2} \cdot \left(1 + \frac{\tau_1}{\tau_2}\right)$
Переход «ИЛИ-НЕ» 	$P_{II-NE}(t) = [1 - P_1(t)] \cdot [1 - P_2(t)] \cdot [1 - P_3(t)]$ $\overline{\tau_{II-NE}} = \tau_{12} \cdot \left(1 + \frac{\tau_{12}}{\tau_3}\right), \text{ где } \tau_{12} = \frac{\tau_1 \cdot \tau_2}{\tau_1 + \tau_2}$

Рис. 6 – Соотношения для расчета времени срабатывания логических переходов в составных сетях Петри-Маркова

Однако для переходов с логиками «И-НЕ», «ИЛИ-НЕ» такой подход не годится, так как соответствующие вероятности не являются функциями распределения. Так, для перехода «И-НЕ» функция распределения времени его срабатывания имеет вид:  $P_{I-NE}(t) = P_1(t) \cdot [1 - P_2(t)]$ , при этом усредненная вероятность того, что при каждой попытке реализации угрозы вероятность того, что разность  $y = \tau_2 - \tau_1$  будет больше нуля, то есть по первой дуге процесс подойдет к переходу, а по второй – нет, определяется как вероятность прореживания первого потока вторым и равна отношению  $\overline{p_{y>0}} = \frac{\tau_2}{\tau_1 + \tau_2}$ , показанному на рис. 6. Там же приведена формула для расчета математического ожидания времени срабатывания перехода «И-НЕ». Аналогичным образом определяется формула для расчета математического ожидания времени срабатывания перехода «ИЛИ-НЕ».

Значения времен срабатывания логических переходов оценивались и путем имитационного моделирования, в результате сравнения их с теоретическими значениями было показано, что различия составляют единицы процентов, то есть аналитические соотношения дают весьма точные оценки.

Наконец, целесообразно остановиться еще на одном достаточно часто поднимаемом вопросе: о возможности использования экспоненциального приближения при расчетах вероятностей срабатывания составных сетей Петри-Маркова. Такое приближение резко упрощает проведение расчетов. Прежде чем рассмотреть возможность такого приближения, необходимо отметить следующее.

Еще в прошлом веке было показано в целом ряде работ (например, в [7]), что если прореживать произвольный поток событий (даже периодический), то он становится пуассоновским, то есть с экспоненциальным распределением пауз между оставшимися событиями (рис. 7).

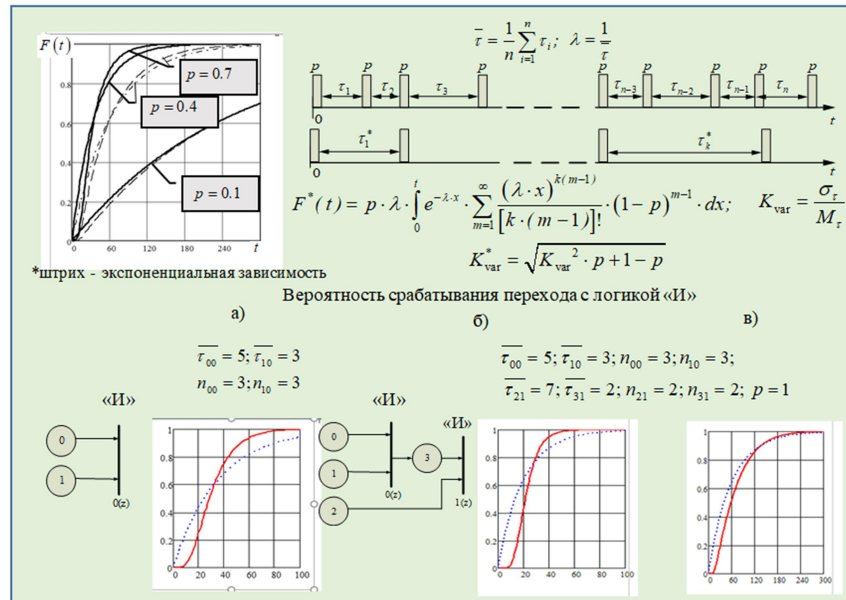


Рис. 7 – Возможность экспоненциального приближения при расчете вероятности срабатывания составной сети Петри-Маркова

Кроме того, было показано (например, в книге Тихонова «Статистическая радиотехника»), что любая плотность распределения вероятности положительно определенной случайной величины может с любой степенью точности аппроксимирована гамма-распределением, то есть распределением Эрланга, только с параметром, который может принимать не только целочисленные, но дробные значения. На рис. 7 показано полученное соотношение для расчета функции распределения для прореженного потока Эрланга и графики ее зависимости от времени и вероятности прореживания, из которого видно, что уже при вероятности прореживания меньше 0.4 поток становится близким к пуассоновскому.

Мерой приближения прореженного потока к пуассоновскому является упоминаемый в целом ряде работ (например, в [8]) коэффициент вариации – отношение среднеквадратического отклонения к математическому ожиданию. Из приведенной на рис. 7 формулы для расчета коэффициента вариации прореженного потока видно, что с уменьшением вероятности, с которой в потоке остаются события, коэффициент вариации прореженного потока стремится к единице, то есть поток становится пуассоновским.

Каждый логический переход, кроме перехода «ИЛИ», также обладает прореживающими свойствами, что иллюстрируется двумя нижними рисунками слева. Если применяются меры и средства защиты в информаци-

онной системе, которые с некоторой вероятностью снижают возможности реализации угрозы, результирующий поток, описывающий процесс реализации угрозы становится пуассоновским, то есть экспоненциальное приближение оказывается несомненно допустимым, что иллюстрируется нижним рисунком справа.

Таким образом, аппарат составных сетей Петри-Маркова является весьма перспективным для аналитического моделирования процессов реализации угроз. Конечно, в докладе изложены далеко не все его возможности. В частности, не показано, каким образом можно моделировать циклические процессы, для чего нами используется в рамках этого аппарата элементы теории предикатных операций. Так же, как и в сетях Петри, здесь могут применяться приемы раскрашивания позиций, переходов и дуг для учета приоритетов развития парциальных процессов и т.д. Тем не менее авторы надеются, что изложенное заинтересует участников конференции.

## ЛИТЕРАТУРА

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

2. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» - docs.cntd.ru [Электронный ресурс]. URL: <https://docs.cntd.ru/document/1200057516> (дата обращения: 10.11.2022).

3. Язов Ю. К., Панфилов В. В. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова // Информация и безопасность. 2006. Т. 9. № 1. С. 117-123

4. Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований по защите информации, содержащейся в информационных системах общего пользования».