Л. В. Акчурина, *кандидат технических наук*
А. Н. Бабкин, *кандидат технических наук, доцент*
С. П. Алексеенко, *кандидат физико-математических наук, доцент*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРИМЕНЕНИЯ ЦЕПЕЙ МАРКОВА И СЕТЕЙ ПЕТРИ ДЛЯ МОДЕЛИРОВАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

COMPARATIVE ANALYSIS USE OF MARKOV CIRCUITS AND PETRI NETWORKS FOR SIMULATION OF SECURE INFORMATION PROCESSES IN TELECOMMUNICATION NETWORK

В статье приводится анализ применения цепей Маркова и сетей Петри для моделирования защищенных информационных процессов в телекоммуникационных сетях. Отмечено, что сети Петри позволяют описать логику последовательности событий, переложить которую на функционирование телекоммуникационной сети в реальных условиях эксплуатации достаточно сложно из-за формализма в способе описания. В цепях Маркова переход от одного дискретного состояния к последующему совершается через заданный интервал времени, а значит, это процесс, контролируемый во времени. Опираясь на модель Маркова, можно установить момент перехода сети в новое состояние, что является существенным плюсом при моделировании защищенных информационных процессов в таких сетях.

The article provides an analysis of the use of Markov circuits and Petri networks for modeling secure information processes in telecommunications networks. It is noted that Petri networks allow describing the logic of the sequence of events, which is difficult to shift to the functioning of the telecommunications network in real operating conditions due to the formalism in the description method. In Markov circuits, the transition from one discrete state to the next is made after a given time interval, which means it is a time-controlled process. Based on the Markov model, it is possible to establish the moment of transition of the network to a new state, which is a significant plus when modeling secure information processes in such networks.

Введение. В работах [1—3] рассматривались различные задачи, целью которых был анализ возникновения информационных атак со стороны нарушителя в процессе передачи данных в телекоммуникационных сетях.

Оценивалась информационная безопасность телекоммуникационной сети как объекта информатизации на основе моделирования его функционирования с использованием цепей Маркова и сетей Петри.

Для моделей вычислялась вероятность угрозы от атаки со стороны злоумышленника.

Отметим, что по содержанию модели, построенные на основе цепей Маркова и сетей Петри, различаются и это можно наблюдать как по поставленным задачам, так и по результатам моделирования.

Цель данной статьи состоит в проведении сравнительного анализа рассматриваемых моделей, определении целесообразности применения цепей Маркова или сетей Петри в моделировании процессов передачи данных в телекоммуникационных сетях (ТКС).

Основная часть. Сети Петри — это графы, состоящие из мест (отмечаются кружком, сюда относятся состояния системы, условия) и переходов (отмечаются прямоугольниками, сюда относятся действия).

Места и переходы соединяются дугами, которые и указывают последовательность наступления событий.

Всегда место и переход чередуются, что и показывает логичность функционирования сети и последовательность наступления событий.

В «кружке» ожидаются (накапливаются) условия, необходимые для срабатывания перехода.

Переход же срабатывает, если все места до него промаркированы.

Модель, к сожалению, не привязывается ко времени. Момент срабатывания перехода зависит только от выполнения условий включения маркера.

Еще одним недостатком сети Петри является то, что после срабатывания перехода возможно не одно состояние системы, их может быть несколько, а указать приоритет состояния после перехода не представляется возможным.

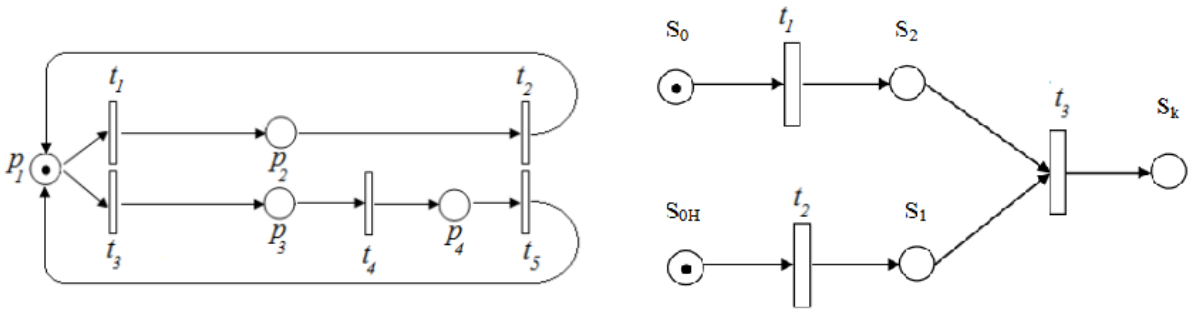
Данная неопределенность снижает возможности ее применения, так как она не является управляемой в таких переходах.

Если рассматривать задачи, связанные с анализом процессов передачи данных в телекоммуникационных сетях, то данную особенность сети Петри можно положительно использовать как возможность перехвата данных нарушителем [3].

На рис. 1, а, б представлены сети Петри, моделирующие взаимодействие авторизованного субъекта (далее — просто субъекта, например, рабочей станции пользователя ТКС) с авторизованным объектом (далее просто объектом, например, DNS-сервером).

P_1 (рис. 1, а) представляет собой начальное состояние субъекта в отношении которого планируется атака со стороны неавторизованного субъекта (далее — нарушителя), t_1 — переход, моделирующий взаимодействие субъекта и объекта, P_2 — состояние, моделирующее ответ объекта на запрос субъекта, t_2 — переход, моделирующий передачу информации от объекта субъекту, t_3 — переход, моделирующий взаимодействие субъекта и нарушителя, P_3 — состояние нарушителя, моделирующее запрос на ложный объект (например, ложный DNS-сервер), P_4 — состояние, моделирующее запрос субъекта на ложный объект, t_5 — переход, моделирующий передачу информации от ложного объекта субъекту.

S_0 (рис. 1, б) представляет собой начальное состояние субъекта, t_1 — переход, моделирующий взаимодействие субъекта и объекта, S_{0H} — начальное состояние нарушителя, t_2 — переход, моделирующий процесс перехвата запроса субъекта к объекту нарушителем, S_1 — состояние нарушителя, моделирующее ожидание ответа, t_3 — переход, моделирующий процесс получения ложного ответа, S_k — состояние объекта, моделирующее передачу информации нарушителю.



а б

Рис. 1. Моделирование процессов передачи данных в сети ТКС

Какой из переходов: *t1* (авторизованный субъект) или *t3* (нарушитель) на рис. 1, а сработает, сказать невозможно, а модель на рис. 1, б позволяет обнаружить нарушителя.

Разные модели не позволяют встроить одну в другую.

Периодичность проверок на наличие угроз информационной безопасности здесь не предусмотрена, что является значительным недостатком применения сетей Петри для моделирования защищенных информационных процессов в ТКС.

Однако на фоне перечисленных выше недостатков есть еще один существенный недостаток применения таких сетей.

Описание места и перехода носит больше формальный характер, что означает, что не всегда есть четкие технические возможности перевода системы из одного состояния в другое при моделировании процессов передачи данных в ТКС.

Формализм дает больше свободы, но, с другой стороны, ограничивается четкой структурой возможностей работы ТКС.

Цепи Маркова — это последовательность математических моделей, которые описывают упорядоченный набор дискретных состояний системы.

Переход от одного дискретного состояния к последующему (либо проверка состояния системы) совершается через заданный интервал времени, а значит, это процесс, контролируемый во времени.

Интервал проверки задается на этапе построения модели и зависит от рассматриваемой задачи.

Последовательность дискретных состояний системы можно считать последовательностью значений многомерных случайных величин.

Фиксирование возможных значений всех или некоторых показателей случайных величин и выход за границу критерия на каком-либо шаге проверки говорит о переходе модели в принципиально другое состояние.

Имеется возможность во времени отслеживать корректность работы системы.

Цепи Маркова представляют собой стохастические процессы, что связано с тем, что момент начала работы модели в измененном состоянии невозможно заранее ни задать, ни исключить — это случайные процессы.

Важно то, что, опираясь на модель Маркова, момент перехода работы системы в новое состояние можно установить. Именно это и является существенным плюсом.

Однако, проверка текущего состояния системы на любом шаге зависит только от предыдущего дискретного (точечного) состояния и совсем не зависит от проверок, проводимых до того, сколько бы их там ни было.

Цепи Маркова являются хорошим инструментом для анализа функционирования ТКС и позволяют быстро реагировать на возникшие проблемы, связанные в том числе и с нарушениями безопасности информации.

Например, в [1] строится цепь Маркова, которая позволяет осуществлять проверку такого свойства информации, как её доступность для авторизованных пользователей, использующих в качестве канала связи радиоканал.

На рис. 2 представлен граф состояний радиоканала.

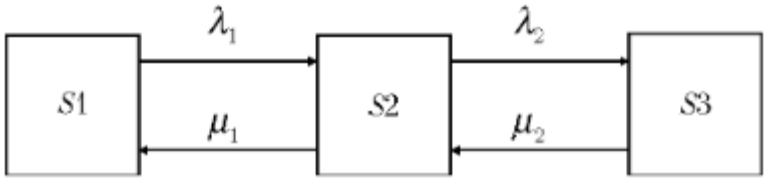


Рис. 2. Граф состояний радиоканала

На рис. 2 $S1$, $S2$ и $S3$ — состояния радиоканала, моделирующие соответственно обычный, предаварийный и аварийный режимы работы.

Заданы интенсивности переходов радиоканала из одного состояния в другое.

Составлена и решена система дифференциальных уравнений состояний радиоканала, из чего определены вероятности нахождения радиоканала в каждом из состояний в зависимости от начальных вероятностей.

Следить за надежностью функционирования радиоканала (определяющей доступность информации для авторизованных пользователей) позволяют границы допустимых ошибок в передаваемых сообщениях.

Их накопление переводит радиоканал из обычного состояния в предаварийное, а далее — в аварийное.

Чем хуже работает радиоканал, тем короче интервалы между проверками, что видно из рис. 3.

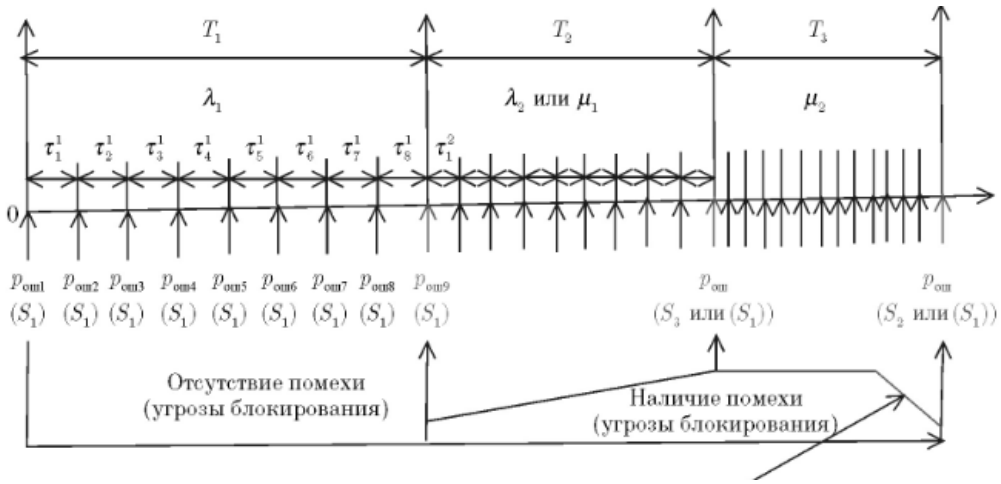


Рис. 3. Временная диаграмма функционирования радиоканала

Попадание в зону аварийной работы радиоканала обозначает его отказ, необходимость применения дополнительных кардинальных мер для восстановления работы.

Значительным преимуществом цепи Маркова перед сетью Петри является техническая возможность фиксирования момента начала отказа (возникновения угрозы информационной безопасности) в сети и своевременное на нее реагирование.

Недостатком является то, что проводить проверку необходимо постоянно (с указанным интервалом), так как просчитать момент начала угрозы не представляется возможным, что и подтверждается формулой для определения надежности функционирования радиоканала P_j:

$$P_j(k) = \sum_{j=0}^{n} P_j(k-1)p_{ij}.$$

Данная формула указывает, что k-й шаг проверки учитывает только предыдущее (k-1)-е состояние работы радиоканала.

В работе [2] сеть Маркова применяется для анализа функционирования ТКС на возможность информационного обмена по сети, где также может находиться нарушитель, маскирующийся под авторизованного пользователя сети.

Перехват информации с дальнейшей возможностью её раскрытия и модификации (потеря конфиденциальности и целостности) со стороны нарушителя может нанести непоправимый вред авторизованным пользователям.

Применяемая модель приведена на рисунке 4.

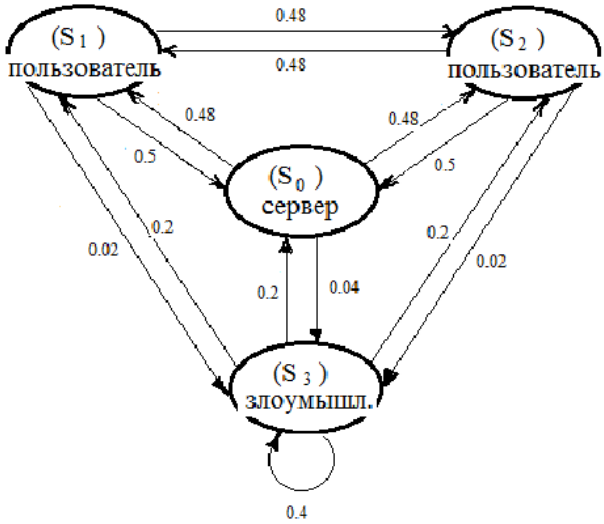


Рис. 4. Цепь Маркова, моделирующая работу телекоммуникационной сети

На данном рисунке:

S_1 и S_2 — авторизованные субъекты (пользователи, например, их рабочие станции), S_0 — авторизованный объект (например, сервер), S_3 — неавторизованный субъект (злоумышленник, например, его рабочая станция).

Заданы начальные вероятности и считается, что необходимая информация на начальный момент времени находится у авторизованного пользователя S_1.

Авторизованный пользователь S_1 передает информацию по сети.

Пошагово рассчитываются вероятности нахождения информации у субъектов и объекта.

Процесс привязан ко времени.

Пошаговое дискретное вычисление позволяет прийти к заключению, что при заданных на рис. 4 вероятностях имеется небольшая (4,3%) вероятность получения неавторизованным субъектом (злоумышленником) информации.

Считать данную вероятность большой или нет, зависит от степени важности (конфиденциальности) информации, циркулирующей в сети, последствий, связанных с нарушением её безопасности (потерей конфиденциальности, целостности или доступности).

Применяемая математическая модель позволяет решать задачи такого содержания.

Логичным шагом будет снижение вероятностей возникновения информационной атаки на авторизованных субъектов и авторизованный объект и повторного пересчета вероятностей.

На основе анализа применения сетей Маркова можно сделать вывод, что они действительно позволяют своевременно на этапе возникновения угрозы (рис. 2), или предваряя такую угрозу (рис. 3), сделать выводы о необходимости принятия своевременного решения и быстрого реагирования на возможные угрозы информационной безопасности.

Вывод. Для моделирования защищенных информационных процессов в телекоммуникационных сетях широко применяются цепи Маркова и сети Петри [4—6].

Сравнивая возможности такого моделирования, следует отметить достаточно поверхностное отражение всех причинно-следственных связей в составлении сети Петри.

Цепи Маркова дают действительные, осязаемые приборами результаты проверок, по которым можно установить надежность функционирование ТКС.

Можно просчитать заранее, к каким вероятностям сводятся угрозы от возможных информационных атак со стороны злоумышленника.

Сети Петри позволяют описать логику последовательности событий, переложить которую на функционирование ТКС в реальных условиях эксплуатации достаточно сложно из-за формализма в способе описания.

В статье рассматривались и сравнивались два подхода к моделированию защищенных информационных процессов в ТКС.

Приоритет отдается именно цепям Маркова.

Тем не менее выбор одного из рассматриваемых в статье способов моделирования зависит от целей и назначения телекоммуникационных сетей, а также информационного ресурса, циркулирующего в сети.

ЛИТЕРАТУРА

1. Бабкин А. Н., Акчурина Л. В. Применение марковских моделей для оценки доступности информации в радиоканале // Вестник Воронежского института ФСИН России. — 2020. — № 4. — С. 9—15.

2. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Практическая реализация цепей Маркова в исследовании телекоммуникационных сетей при воздействии угроз информационной безопасности // Вестник Воронежского института МВД России. — 2022. — № 1. — С. 18—23.

3. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Моделирование угроз информационных атак в сети Internet на основе сетей Петри // Вестник Воронежского института МВД России. — 2023. — № 2. — С. 105—110.

4. Питерсон Дж. Теория сетей Петри и моделирование систем. — М. : Мир, 1984. — 264 с.

5. Кудж С. А., Логинова А. С. Моделирование с использованием сетей Петри // Вестник МГТУ МИРЭА. — 2015. — № 1.

6. Зейфман А. И., Бенинг В. Е., Соколов И. А. Марковские цепи и модели с непрерывным временем : монография. — М. : ТОРУС ПРЕСС, 2008. — 168.

REFERENCES

1. Babkin A. N., Akchurina L. V. Primenenie markovskix modelej dlya ocenki dostupnosti informacii v radiokanale // Vestnik Voronezhskogo instituta FSIN Rossii. — 2020. — № 4. — S. 9—15.

2. Babkin A. N., Akchurina L. V., Alekseenko S. P. Prakticheskaya realizaciya cepej Markova v issledovanii telekommunikacionny`x setej pri vozdejstvii ugroz informacionnoj bezopasnosti // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 1. — S. 18—23.

3. Babkin A. N., Akchurina L. V., Alekseenko S. P. Modelirovanie ugroz informacionny`x atak v seti Internet na osnove setej Petri // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 2. — S. 105—110.

4. Piterson Dzh. Teoriya setej Petri i modelirovanie sistem. — M. : Mir, 1984. — 264 s.

5. Kudzh S. A., Loginova A. S. Modelirovanie s ispol`zovaniem setej Petri // Vestnik MGTU MIRE`A. — 2015. — № 1.

6. Zejfman A. I., Bening V. E., Sokolov I. A. Markovskie cepi i modeli s neprery`vny`m vremenem : monografiya. — M. : TORUS PRESS, 2008. — 168.

СВЕДЕНИЯ ОБ АВТОРАХ

Акчурина Людмила Васильевна. Доцент кафедры прикладной математики и механики.
Кандидат технических наук.
Воронежский государственный технический университет.
E-mail: ac.mila@yandex.ru.

Россия, 394006, Воронеж, ул. 20-летия Октября, 84.

Бабкин Александр Николаевич. Доцент кафедры информатики и вычислительной техники. Кандидат технических наук, доцент.
Международный институт компьютерных технологий.
E-mail: alex_babk@mail.ru.
Россия, 394026, Воронеж, ул. Солнечная, 29б.

Алексеенко Сергей Павлович. Доцент кафедры информационной безопасности. Кандидат физико-математических наук, доцент.
Воронежский институт МВД России.
E-mail: aleks_serg@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Akchurina Lyudmila Vasilyevna. Associate Professor of the chair of Applied Mathematics and Mechanics. Candidate of Technical Sciences.
Voronezh State Technical University.
E-mail: ac.mila@yandex.ru.
Work address: Russia, 394006, Voronezh, 20-letiya Oktyabrya Str., 84.

Babkin Alexander Nikolaevich. Associate Professor of the chair of Computer Science and Applied Technology. Candidate of Technical Sciences, Associate Professor.
International Institute of Computer Technology.
Email: alex_babk@mail.ru.
Work address: Russia, 394026, Voronezh, Solnechnaya Str., 29b.

Alekseenko Sergey Pavlovich. Assistant Professor of the chair of Information Security. Candidate of Sciences (Physics and Mathematics), Associate Professor.
Voronesh Institute of the Ministry of the Interior of Russia.
E-mail: aleks_serg@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: телекоммуникационная сеть; угроза информационной безопасности; моделирование; вероятность; сети Петри; цепи Маркова.

Key words: telecommunications network; information security threat; modeling; probability; Petri networks; Markov circuits.

УДК 621.396.62