ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.5

ПРИМЕНЕНИЕ СЕТЕЙ ПЕТРИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Баранов Александр Сергеевич,
студент,
Самарский государственный технический университет, г. Самара
as_baranov@bk.ru

Аннотация

Проблема управления действиями сотрудников охраны, когда объект состоит из разветвлённой коридорной структуры, актуальна. В работе предлагается рассмотреть варианты применение сетей Петри в различных аспектах обеспечения информационной безопасности. Автор приходит к выводу, что задача поиска преступника на объекте с применением имитационного моделирования на основе сетей Петри и их модификаций при рассмотрении двух параллельных процессов (движения злоумышленника и охранников), которые должны сходиться в одной точке (цели преступника), в практических работах отсутствует, либо работы, посвященные комплексным системам защиты, касаются других вопросов.

Ключевые слова: системы физической защиты, сети Петри, злоумышленник, объект.

APPLICATION OF PETRI NETS IN INFORMATION SECURITY

Aleksandr S. Baranov
student,
Samara State Technical University, Samara
as_baranov@bk.ru

ABSTRACT

The problem of managing the actions of security personnel when the object consists of a branched corridor structure is relevant. The paper proposes to consider various applications of Petri nets in various aspects of information security. The author concludes that the task of searching a criminal at the object using simulation based on Petri nets and their modifications when considering two parallel processes (movements of an intruder and guards), which should converge at one point (the criminal's target), is absent in practical works, or works devoted to complex protection systems deal with other issues.

Keywords: physical protection systems, Petri nets, intruder, object.

Кражи, связанные с проникновением на частную территорию, происходят часто, поэтому были разработаны системы безопасности, которые помогают защитить необходимые объекты от несанкционированного доступа. В большинстве случаев руководители организаций понимают необходимость в обеспечении защиты организации, однако финансовые издержки, связанные с установкой и обслуживанием дорогостоящих охранных систем, не позволяют создать систему безопасности с повышенными требованиями.

Одним из выходов в данной ситуации является использование алгоритмов, которые могут определять предполагаемые места проникновения на контролируемую территорию или вырабатывать стратегию по поиску злоумышленника, оказавшегося на территории организации. Поскольку проникновение на охраняемую территорию является одним из наиболее простых методов совершения несанкционированного доступа, будем рассматривать его как актуальную угрозу для любого предприятия.

Задачу поиска злоумышленника на охраняемом объекте несколькими сотрудниками охраны и координацию их действий можно рассматривать с использованием сетей Петри.

Существуют разные классы сетей Петри: раскрашенные и сети Петри высокого уровня; временные сети; предикатные сети; стохастические сети.

Раскрашенные и сети Петри высокого уровня. Данный класс позволяет отображать сложные параллельные процессы в компактном виде, который достигается за счёт того, что маркерам приписываются переменные (цвета), кратности дуг интерпретируются как функции от этих переменных.

Предикатные сети являются дальнейшим расширением раскрашенных сетей. В этих сетях маркерами могут быть и цвета и переменные с областью определения из множества цветов, и, кроме того, каждому переходу поставлен в соответствие предикат, истинность которого разрешает срабатывание.

Существует два типа временных сетей: сети, в которых позициям приписывают продолжительность пребывания в них маркеров, и сети, в которых переходам приписывается продолжительность срабатывания.

Стохастические сети введены для количественной оценки некоторых параметров функционирования систем: надежности, производительности. Стохастические сети – это модификация временных сетей. В них каждому переходу приписана вероятность его срабатывания за определенное время.

Временные сети Петри подходят для решения задачи поиска преступника на объекте. Применение имитационного моделирования на основе временных сетей Петри обусловлено тем, рассматривается два параллельных процессов (движение преступника и сотрудника охраны), которые должны сходиться в одной точке (цели преступника) [1].

На рисунке 1 показан пример работы сети Петри для последовательности срабатывания σ=[t1,t3]. Для удобства активные переходы помечены звездочкой. Также следует отметить, что для каждого случая имеется только одна возможная последовательность срабатывания σ=[t1,t2]

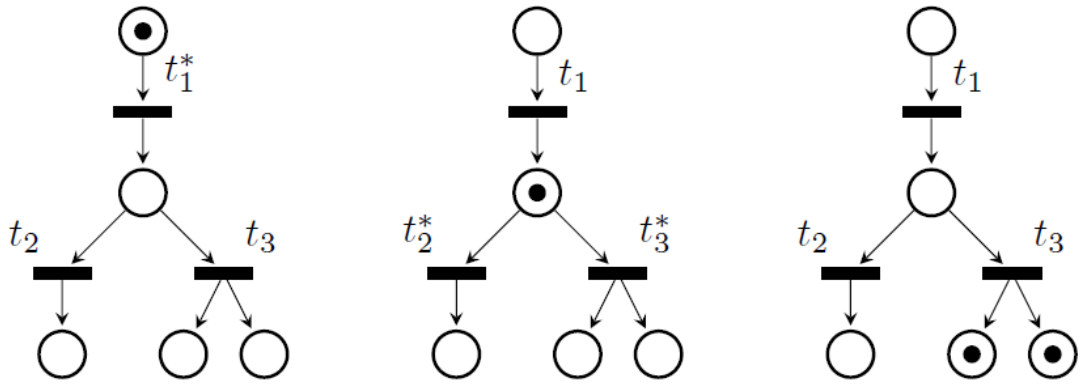

Рисунок 1. Пример работы временной сети Петри.

Формальным образом сети Петри определяются как четверка

〈S, T,W, μ0〉 , где

S – конечное множество мест (|S|=n);

T – конечное множество переходов (|T|=m, S∩T = Ø);

W: (S×T) ∪ (T×S) → Z - мультимножество дуг;

μ0 : S→Z Начальная разметка сети.

Работы в области информационной безопасности, в которых используются сети Петри, посвящены либо отдельным аспектам физической защиты объекта, либо защите информационных систем от компьютерных атак, а также анализу защищенности систем [2-8].

М. Ю. Шрейдер, А.С. Боровский в [2] разработали модель обработки информации в процессе функционирования отдельных элементов системы защиты для организации ее эффективного управления. Структурно-логическая модель системы на основе сетей Петри изображается в виде гиперграфа, элементы которого представлены «в виде точек контроля, которые подразделяются по выполняемым функциям: точка обнаружения, точка доступа, точка видеонаблюдения, точка задержки и управляющих элементов, представленных периферийными и магистральными контроллерами».

В.В. Юдаев, А.В. Богданов, О.А. Королёв в [3] рассмотрели подход к обеспечению авиационной безопасности аэропорта за счет повышения качества досмотра багажа путем оптимизации структуры и организации работы многоуровневой системы контроля с помощью аппарата сетей Петри. Ими разработана математическая модель процесса контроля багажа, базирующаяся на пяти уровнях досмотра. Авторы замечают, что реализация модели в программной среде Colored Petri nets Tools позволяет осуществить проверку установленного порядка работы пункта досмотра, оценить его пропускную способность и временные характеристики, что, в конечном счете, позволяет оптимизировать и повысить качество досмотра.

В.Т. Еременко, М.Ю. Рытов, А.П. Горлов, В.И. Аверченко, В.П. Фёдоров в [4] предложили подход к оценке угроз уровня информационной безопасности объекта информатизации, позволяющий значительно сократить материальные и временные затраты на проведение аудита информационной безопасности, а также повысить качество проектных решений при создании и внедрении комплексных систем защиты информации. Математический аппарат раскрашенных, вероятностных, ингибиторных сетей Петри позволяет оценить эффективность системы защиты объекта с учетом своевременности реагирования средств противодействия и одновременности реализации угроз.

М.С. Соломатин, Е.А. Рогозин, И.Г. Дровникова в [5] рассмотрели конфликт информационного взаимодействия «Нарушитель — Система защиты» с разными потенциальными возможностями сторон. Построена сеть Петри — Маркова,

изображающая процесс протекания конфликта. В работе приведены основные интегрально-дифференциальные уравнения, описывающие информационный конфликт, и обоснован выбор параметров с целью исследования его динамических характеристик. Разработанный на основе формальной модели алгоритм функционирования программно-аппаратного комплекса моделирования процесса протекания информационного конфликта «Нарушитель — Система защиты» позволит разработать рекомендации по оптимизации выбора параметров системы защиты информации информационных систем.

Миронов В.Г., Шелупанов А.А. в [6] рассмотрел анализ защищенности системы путем построения раскрашенных сетей Петри. В работе с помощью аппарата сетей Петри проводится обследование функционирования реализованной системы защиты и выявляются ее недостатки. Автор замечает, что аппарат сети Петри является средством моделирования различных информационных систем и систем защиты конфиденциальной информации и дает возможность получить информацию о структуре и динамическом поведении информационных систем, систем защиты конфиденциальной информации и тем самым спроектировать надежную систему защиты конфиденциальной информации, а использование фишек различных цветов при проведении обследования системы защиты конфиденциальной информации позволяет выявить уязвимые места информационных систем и систем защиты конфиденциальной информации.

И.В. Яхонтовой в [7] проведен анализ методов оценки и построения систем защиты информации на основе сетей Петри. Выявлены ограничения каждого из подходов и показаны возможные пути их применения в задачах анализа защищенности корпоративных систем.

В.Г. Криволапов в [8] рассмотрел методику моделирования систем информационной безопасности на основе SADT-моделирования и аппарата сетей Петри. Автор отмечает, что оценка параметров системы информационной безопасности в условиях неопределенности ее функционирования должна вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся в процессе уточнения исходных данных. Представленная методика моделирования систем информационной безопасности на основе сетей Петри позволяет строить масштабируемые и расширяемые модели, которые впоследствии можно анализировать известными методами.

Можно прийти к выводу, что задача поиска преступника на объекте с применением имитационного моделирования на основе сетей Петри и их модификаций при рассмотрении двух параллельных процессов (движения злоумышленника и охранников), которые должны сходиться в одной точке (цели преступника), в практических работах отсутствует, либо работы, посвященные комплексным системам защиты, касаются других вопросов.

Список литературы:

1. Проститенко О.В. Моделирование дискретных систем на основе сетей Петри: учебное пособие / О.В. Проститенко, В.И. Халимон, А.Ю. Рогов. – СПб.: СПбГТИ(ТУ), 2017. - 69 с.
2. Шрейдер М.Ю., Боровский А.С. Разработка моделей описания обработки информации в задачах управления системой защиты объекта на основе сетей петри // Вопросы кибербезопасноти. – 2018 - №1 (25). – С. 46-53.
3. Юдаев В.В., Богданов А.В., Королев О.А. Моделирование систем физической безопасности на основе аппарата сетей Петри // Научно-аналитический журнал

Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России» – 2019 – №4. – С. 82–88.
4. Еременко В.Т., Рытов М.Ю., Горлов А.П., Аверченков В.И., Фёдоров В.П. Моделирование процесса оценки эффективности комплексных систем защиты информации промышленных предприятий при одновременной реализации угроз // Вестник Брянского государственного технического университета – 2017 – №7(60). – С. 56–61.
5. Соломатин М.С., Рогозин Е.А., Дровникова И.Г. Создание модели информационного конфликта «нарушитель-система защиты» на основе сети Петри-Макарова // Вестник Воронежского института МВД – 2019 – №2. – С. 93–100.
6. Миронов В.Г., Шелупанов А.А. Сети Петри как инструмент анализа системы защиты конфиденциальной информации // Известия ЮФУ. Технические науки – 2011 – № 12(125). – С. 64– 70.
7. Яхонтов И.В. Анализ моделей систем защиты информации на основе модифицированных сетей Петри // Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки – 2012 – №3 – С. 57-65.
8. Криволапов В.Г. Методика моделирования систем информационной безопасности на основе SADT-моделирования и аппарата сетей Петри // Известия Оренбургского государственного аграрного университета – 2008 – №3(19). – С. 175– 177.

References:

1. Prostitenko O.V. Modeling of Discrete Systems on the Basis of Petri Nets: Tutorial / O.V. Prostitenko, V.I. Khalimon, A.Yu. Rogov. - SPb: SPbGTI(TU), 2017. - 69 p.
2. Schrader M.Y., Borovsky A.S. Development of information processing description models in the management tasks of the object protection system based on petri nets // Voprosy kiberbezopasnosti. - 2018 - №1 (25). - P. 46-53.
3. Yudaev V.V., Bogdanov A.V., Korolev O.A. Modeling of physical security systems based on Petri nets apparatus // Scientific and analytical journal Vestnik of Saint-Petersburg University of State Fire Service of EMERCOM of Russia" - 2019 - № 4. - P. 82-88.
4. Eremenko V.T., Rytov M.Y., Gorlov A.P., Averchenkov V.I., Fedorov V.P. Modeling the process of assessing the effectiveness of integrated information protection systems of industrial enterprises with simultaneous implementation of threats // Bulletin of Bryansk State Technical University - 2017 - № 7(60). - P. 56-61.
5. Solomatin M.S., Rogozin E.A., Drovnikova I.G. Creating a model of information conflict "intruder-protection system" based on the Petri-Makarov network // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs - 2019 - № 2. - P. 93-100.
6. Mironov V.G., Shelupanov A.A. Petri nets as a tool for analyzing the protection of confidential information // Izvestia SFU. Technical Sciences - 2011 - № 12(125). - P. 64- 70.
7. Yakhontov I.V. Analysis of Information Protection Systems Models Based on Modified Petri Networks // Modern Science: Actual Problems of Theory and Practice. Series: Natural and Technical Sciences - 2012 - №3 - P. 57-65.

8. Krivolapov V. G. Technique of modeling of information security systems on the basis of SADT-modeling and Petri nets apparatuses// Proceedings of Orenburg State Agrarian University - 2008 - №3(19). - P. 175- 177.