УДК 004

ИСПОЛЬЗОВАНИЕ СЕТИ ПЕТРИ ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Донецков Анатолий Михайлович
Доцент, кандидат технических наук, доцент,
КГУ им К.Э. Циолковского,
г.Калуга

Мачехин Кирилл Витальевич
Студент,
КГУ им К.Э. Циолковского,
г.Калуга

Сети Петри – это мощный инструмент, который позволяет моделировать динамическое поведение сложных систем и выявлять потенциальные уязвимости. Анализируя взаимодействия и состояния системы с помощью сетей Петри, можно эффективно обнаружить слабые места, избыточные связи и потенциальные угрозы. Такой подход позволяет не только оценить текущий уровень безопасности системы, но и предложить меры по её улучшению. Это способствует повышению надёжности и защите данных.

Ключевые слова*: сеть Петри; информационная система; свойства сети Петри; информационная безопасность; преимущества сети Петри; состояние информационной системы.*

Сети Петри – инструмент исследования систем [1]. Анализ сетей Петри поможет получить важную информацию о структуре и динамическом поведении моделируемой системы. С помощью этой информации можно оценить моделируемую систему и выработать предложения по ее усовершенствованию и изменению. Следовательно, развитие сетей Петри основывается на применимости их к моделированию и проектированию систем.

Классические и потоковые сети Петри различаются типами вычислительных процессов: управляющие и функциональные. Это подчёркивает необходимость разработки новых сетей Петри с использованием современных технологий и методов анализа. Такой подход позволяет эффективно использовать возможности сетей Петри в различных областях моделирования, предоставляя инструменты для детального и точного анализа сложных систем. Эти сети позволяют визуализировать структуру системы и моделировать её динамическое поведение. Классические и потоковые сети Петри различаются типами вычислительных процессов: управляющие и функциональные. Это подчёркивает необходимость разработки расширенных сетей Петри с использованием новейших технологий и методов анализа. Такой подход позволяет максимально эффективно использовать возможности сетей Петри в различных сферах моделирования, предоставляя инструменты для детального и точного анализа сложных систем. Модель системы по своей природе является абстракцией моделируемой системы. Поэтому она игнорирует все возможные специфические детали.

Ключевые характеристики сетей Петри:

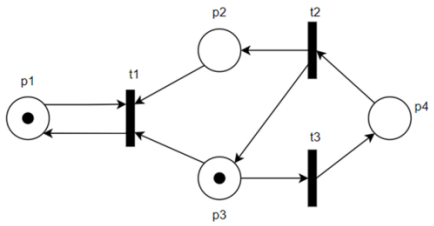

Рисунок 1 – Сеть Петри

- Переход t_j в сети C считается потенциально активным, если существует разметка μ, при которой переход может быть активирован. Переход t_j в сети C считается активным, если он потенциально активен при любой разметке. Переход t_j считается потенциально неактивным, если не существует разметка μ из пространства состояний R(C, μ), в которой переход разрешен. Такая разметка называется тупиковой. Сеть считается активной, если все её переходы активны. Сеть на рисунке 1 не является активной, поскольку в ней существуют тупиковые разметки.
- Переход называется устойчивым, если после его срабатывания сохраняется возможность срабатывания других переходов. Сеть является устойчивой, если все её переходы обладают этим свойством [2].

В современном мире, где информационные технологии играют ключевую роль, обеспечение безопасности данных становится одной из приоритетных задач. Множество компьютеров, подключённых к интернету, обрабатывают и хранят информацию, представленную на веб-страницах. Одной из важнейших задач является защита этой информации как на персональных компьютерах пользователей, так и на серверах. Это включает в себя обеспечение безопасного соединения между браузером и веб-сервером, а также своевременное предотвращение информационных атак злоумышленников. Для моделирования информационных процессов в условиях угроз информационной безопасности могут использоваться цепи Маркова. Одним из полезных инструментов для анализа изменений состояния информационных систем, включая безопасность данных, являются сети Петри. Сети Петри позволяют выявить вмешательства злоумышленников, влияющие на информационные процессы в системе, и своевременно принять меры для их защиты. Рассмотрим пример применения сетей Петри в DNS-службе, которая используется для назначения IP-адресов пользовательским компьютерам. DNS-протокол работает по принципу «клиент-сервер». Персональный компьютер пользователя отправляет запрос на сервер для получения IP-адреса, а сервер формирует ответ, включающий IP-адрес и дополнительные данные. Этот процесс может заинтересовать злоумышленников, которые, зная структуру запросов и ответов, могут организовать информационную атаку, наносящую ущерб как пользователю, так и DNS-серверу [3].

Одним из методов информационной атаки является перенаправление трафика целевого хоста на ресурс злоумышленника. В этом случае злоумышленник перехватывает запрос пользователя к DNS-серверу, создаёт ложный ответ и перенаправляет его пользователю, что приводит к отправке данных на поддельный IP-адрес. Для обнаружения таких атак применяется метод анализа переходов системы, основанный на использовании сетей Петри [4]. Этот подход рассматривает информационную атаку как вмешательство, приводящее к изменению состояния системы, что можно зафиксировать и отследить. Сеть Петри можно получить из блок-схемы работы системы. Таким образом, любые изменения, вызванные воздействием злоумышленника, будут заметны и позволят принять меры для защиты данных. На

рисунке 2 позиция p1 – первоначальное состояние системы. Переход t1 – запрос компьютера пользователя к серверу. Состояние p2 – ожидание ответа. Переход t2 – получение ответа от сервера. Состояние p3 – запуск соединения.

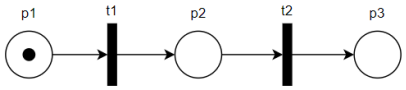

Рисунок 2 – Работа системы без вмешательства злоумышленника

На схеме, представленной на рисунке 3, можно увидеть, что система изначально находится в состоянии p1. Затем происходит переход t1, когда компьютер пользователя отправляет запрос на сервер. Далее система переходит в состояние p3, ожидая ответа от сервера. В это же время злоумышленник, находящийся в состоянии p2, перехватывает запрос. После этого происходит переход t2, и злоумышленник формирует ложный ответ. Затем происходит переход t3, и злоумышленник получает подменённый ответ от сервера. Система переходит в состояние p4. Наконец, происходит переход t4, и система оказывается в состоянии p5, где происходит соединение с компьютером злоумышленника.

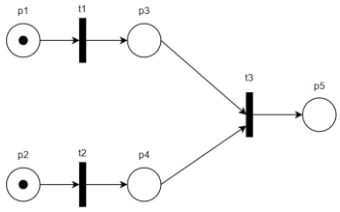

Рисунок 3 – Функционирование системы в условиях, когда в неё пытается проникнуть злоумышленник

Изменение состояний в системе происходит под влиянием событий, которые воздействуют на управление информационными процессами. Это может включать активацию приложений и установку TCP-соединений, что, в свою очередь, открывает возможности для информационных атак злоумышленников. Ключевое преимущество использования сетей Петри заключается в их способности фиксировать заметные изменения в системе, связанные с нарушением информационной безопасности. Эти изменения отображаются в виде новых состояний системы, что позволяет своевременно обнаруживать и реагировать на потенциальные угрозы [5]. В таблице 1 представлены ключевые преимущества использования сети Петри для выявления таких изменений.

Таблица 1 – Преимущества использования сети Петри

Преимущества	**Описание**
Моделирование процессов	Сети Петри позволяют визуализировать и анализировать различные процессы в системе.
Обнаружение атак	Возможность моделирования информационных атак и их последствий для системы.
Гибкость	Легкость преобразования блок-схем в сети Петри, что делает их универсальным инструментом.

Переходы состояний	Анализ переходов системы из одного состояния в другое чтобы определить и провести анализ вероятных угроз.
Информативность	Детальное описание событий в системе, которое помогает проводить глубокий анализ и мониторинг.

Для надёжного функционирования информационной системы необходимо обеспечить её защиту на всех уровнях. Ключевую роль здесь играет информационная безопасность, которая становится особенно актуальной как на этапе проектирования ИС, так и в процессе её эксплуатации. Сети Петри предоставляют уникальные возможности для моделирования и анализа безопасности информационных систем. Эта сеть позволяет детально исследовать процессы внутри системы и выявлять потенциальные уязвимости. Сети Петри включают состояния и переходы, которые соединены дугами, что позволяет моделировать и анализировать взаимодействия в системе. Это особенно полезно для выявления потенциальных слабых мест и угроз. Использование сетей Петри для анализа безопасности информационных систем позволяет более глубоко понять поведение системы, оценить её защищенность и предотвратить возможные атаки. Этот подход предоставляет инструменты для повышения надёжности и защиты данных от потенциальных угроз. Один из действенных способов моделирования потенциальных кибератак – это анализ изменений состояния системы, который базируется на использовании сетей Петри. Это предоставляет гибкий инструмент для визуализации и анализа различных сценариев развития событий в информационной системе. Поэтому сети Петри являются мощным средством для обнаружения и предотвращения широкого спектра информационных атак в реальных условиях эксплуатации. Таким образом, использование сетей Петри помогает не только идентифицировать уязвимости, но и предпринимать своевременные меры для защиты информационной системы.

ЛИТЕРАТУРА

1. Питерсон Дж. Теория сетей Петри и моделирование систем/ Пер. с англ. – М.: Мир, 1984. С. 264

2. Котов В.Е. Сети Петри. – М.: Наука, 1984. С. 160

3. Бабкин Александр Николаевич, Акчурина Людмила Васильевна, Алексеенко Сергей Павлович ПРИМЕР ПРИМЕНЕНИЯ СЕТЕЙ ПЕТРИ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ // Вестник ВИ МВД России. 2022. №4. URL: https://cyberleninka.ru/article/n/primer-primeneniya-setey-petri-dlya-analiza-zaschischennosti-informatsionnyh-protsessov (дата обращения: 15.11.2024).

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

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 5-изд. – СПб. : Питер, 2016. – 992 с.

USING A PETRI NET TO ANALYZE THE SECURITY OF AN INFORMATION SYSTEM

Donetkov A.M., Machekhin K.V.

Petri nets are a powerful tool that allows you to model the dynamic behavior of complex systems and identify potential vulnerabilities. By analyzing the interactions and states of the system using Petri nets, it is possible to effectively detect weaknesses,

redundant connections and potential threats. This approach allows you not only to assess the current level of security of the system, but also to propose measures to improve it. This helps to improve the reliability and protection of data.

Keywords: Petri net; information system; properties of the Petri net; information security; advantages of the Petri net; state of the information system.