Куринных Д.Ю.[1], Сахно В.В.[1], Ганжур М.А.[2] ©
[1]Студент, [2]старший преподаватель,
Донской государственный технический университет

АНАЛИЗ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СЕТИ ПЕТРИ

Аннотация

В результате реализации угроз информационной безопасности предприятия терпят существенные материальные и репутационные потери, поскольку на предприятиях хранится большое количество информации, в том числе конфиденциальной. В работе предлагается моделирование системы обнаружения вторжений с помощью сети Петри. Проведен анализ данных моделирования. Проведен анализ разработанной модели. Показано, что применение данной модели позволяет снизить время реакции на возможные атаки и увеличивает возможность специалистов информационной безопасности своевременно предотвратить появление новых угроз.

Ключевые слова: риск информационной безопасности, система обнаружения вторжений, сеть Петри, ориентированный граф, система защиты информации.
Keywords: information security risk, intrusion detection system, Petri net, oriented graph, information security system.

Введение

В настоящее время ни одно предприятие или учреждение не обходится без собственной информационной системы. Постоянное увеличением объемов данных, находящихся в глобальных и локальных вычислительных сетях, возрастание сложности обработки информации, усложнение компонентов вычислительных сетей, является причиной повышения вероятности появления уязвимостей и наличия ошибок в системах. Проблема обеспечение безопасности информационных систем является одной из наиболее важных проблем связанных с их надежным функционированием. Следовательно, повышаются и требования системам защиты информации (СЗИ), которые должны своевременно обнаруживать атаку, найти причины появления угрозы и, проанализировав, устранить[1, 5-16].

Определение и постановка задачи

Наиболее важным фактором при оценке возможных рисков, а также анализе угроз информационной безопасности является обнаружение непосредственно источников угроз[2]. В процессе проектирования комплексных и интегрированных систем защиты информационных ресурсов, чаще всего прибегают к моделированию основных процессов, происходящих непосредственно внутри информационной системы и на стыке система-среда. Также модели используют для мониторинга, анализа и аудита безопасности на различных этапах сопровождения системы. В основе модели СЗИ нередко используют теорию графов, автоматов и сетей Петри[3, 65-74]. Определим сеть Петри как <P,T,I,O>, в которой <P,T> - конечными множествами переходов и позиций, а <I,O> - множество входных и выходных функций. Входной позицией перехода I(tj) назовем входную функцию I, которая отображает переход в tj., а выходные позиции перехода O(tj). Наглядным представлением сети Петри является двудольный ориентированный мультиграф (рисунок 1).

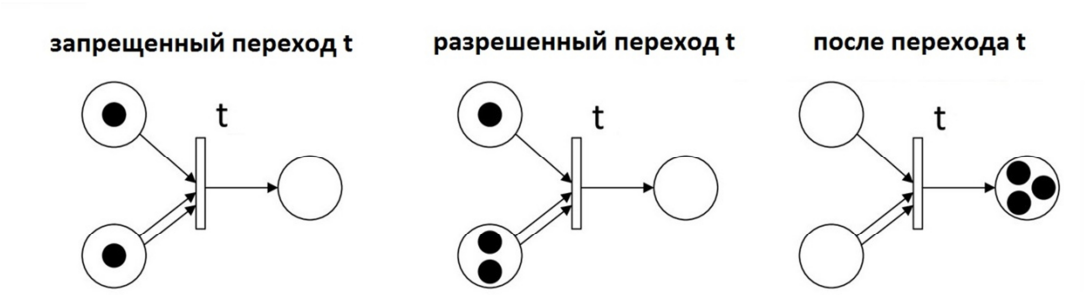

Рисунок 1 – Выполнение сети Петри.

Целью использования сети Петри в системе обнаружения вторжений (СОВ)[4, 346-348] является моделирование процесса работы, что позволяет показать совокупность условий, необходимых для успешного предотвращения атаки. В случае, если таких условий нет или частично присутствуют, тогда можно сказать, что либо атака отсутствует, либо существует с малой долей вероятности.

В информационной безопасности событием является появление такого состояния информационной системы или сети, которое указывает на потенциальное нарушение политик ИБ или отказа мер защиты, а инцидент – появление нежелательных событий ИБ. Если имеется вероятность, что событие ИБ совершено или развивается, его необходимо как можно быстрее обнаружить и сообщить администратору в форме отчета о событии, с описанием произошедших инцидентов ИБ. Одной из особенностей инцидентов ИБ является то, что они могут быть незаметны даже при работе пользователя, однако могут нанести большой ущерб системе и находящимся в ней информационным ресурсам. В связи с этим необходимо производить четкую процедуру регистрации и распределения инцидентов ИБ, а также своевременно информировать пользователей данной системы.

СОВ - программное или аппаратное средство, которое предназначено для выявления фактов неавторизованного доступа в систему или сеть (рисунок 2).

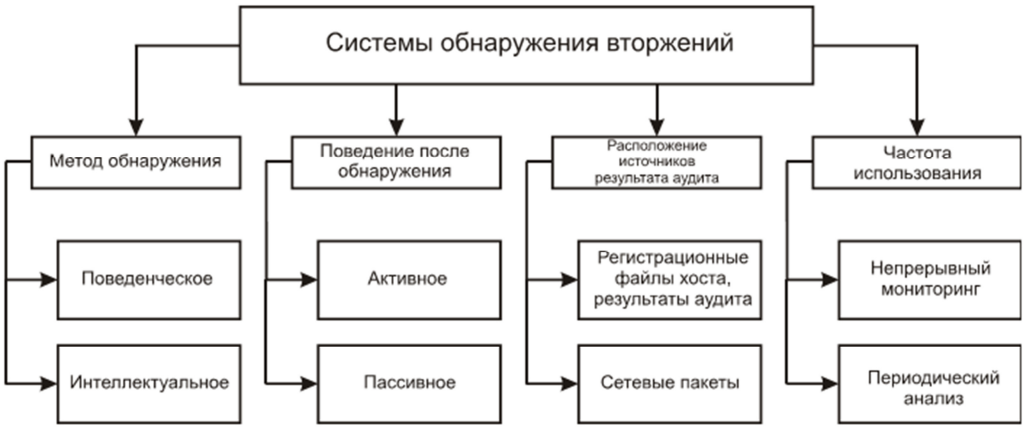

Рисунок 2 — Система обнаружения вторжений.

Разработка модели с помощью сети Петри

Анализ СОВ[5] можно провести с помощью изучения динамических свойств сети Петри:

— проблема достижимости заключается в установлении принадлежности μ к множеству R(μ), при заданной маркировки μn в сети (N,μ);

— сеть будет называться K – ограниченной, если для любой маркировки μn в любой позиции, количество фишек не будет больше числа K;

— активной сеть будет называться, если для любого перехода, независимо от достигнутой маркировки, будет существовать возможность дальнейшего запуска;

— сеть Петри будет являться обратимой при условии, что маркировка μ достижима от маркировки μn;

— проблема достижимости тупиковой разметки возникает в случае, если срабатывание любого перехода сети Петри является невозможным.

Процесс функционирования разработанной модели СОВ можно наглядно представить графом множества всевозможных достижимых маркировок (рисунок 3). Проанализировав свойства нашей сети Петри, можно сказать, что данная сеть Петри является: достижимой, 1-ограниченной, обратимой, активной, отсутствует достижение тупиковой разметки.

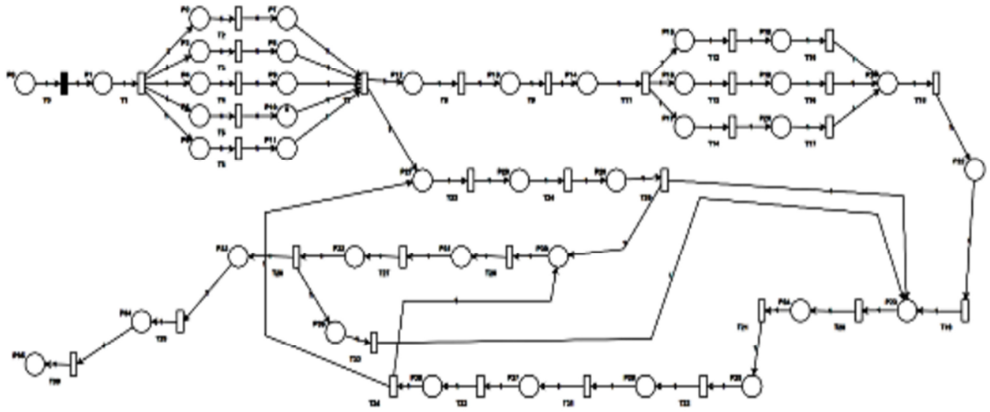

Рисунок 3 – Модель СОВ на основе сети Петри.

Таким образом, можно сделать вывод, что данная сеть Петри, моделирующая СОВ, находится в одном из множества состояний в каждый момент времени, и для каждого такого состояния можно определить отсутствие или наличие атаки с определенной долей вероятности.

Заключение

Разработанная формальная модель СОВ, построенная на основе сети Петри, позволяет осуществить моделирование процесса обнаружения вторжений, что дает больше возможностей специалистам информационной безопасности предприятия для предотвращения возможных угроз, а также своевременно предотвратить появление новых.

Литература:

1. Левин В. К. Защита информации в информационно-вычислительных системах и сетях. —2004 — №5.
2. Виды и источники угроз информационной безопасности [Электронный ресурс]. — режим доступа: http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti (дата обращения 9.04.2019).
3. Воробьёв В.А., Березовская Ю.В. Теория систем и системный анализ. Стохастические системы. — Архангельск — 2012.
4. Шаньгин В.Ф. Информационная безопасность компьютерный систем и сетей. — Москва — 2011.
5. Системы обнаружения вторжений [Электронный ресурс]. — режим доступа: https://ozlib.com/809567/informatika/sistemy_obnaruzheniya_vtorzheniy (дата обращения 7.04.2019).