УДК 51-7+004.415

МОДЕЛИРОВАНИЕ ДИНАМИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ СЕТЕЙ ПЕТРИ

А. С. Кацунова[1], Г. Ф. Кацунова[2], Н. А. Федорова[3]

Сибирский федеральный университет
Российская Федерация, 660041, г. Красноярск, просп. Свободный, 79
E-mail: askatsunova@gmail.com

В докладе предложен способ использования сетей Петри при моделировании динамики угроз информационной безопасности. Вопрос моделирования и обработки динамических угроз находит применение при анализе безопасности полета.

Ключевые слова: математическая модель, сети Петри, информационная безопасность, безопасность полета.

MODELING THE DYNAMICS OF THREATS TO INFORMATION SECURITY USING PETRI NETS

A. S. Katsunova[1], G. F. Katsunova[2], N. A. Feodorova[3]

Siberian Federal University
79, Svobodny Av., Krasnoyarsk, 660041, Russian Federation
E-mail: askatsunova@gmail.com

The report proposes a method for using Petri nets in modeling the dynamics of information security threats. The issue of modeling and processing dynamic threats finds application in flight safety analysis.

Keywords: mathematical model, Petri nets, information security, flight safety.

Введение. Для оценки степени безопасности (защиты) системы требуется построение динамической модели системы и динамической модели угроз. При создании дискретной динамической модели возникновения угроз несанкционированного доступа к информации в докладе использованы сети Петри. Вопрос обработки динамических угроз может быть использован также при анализе безопасности полета.

Постановка задачи. При рассмотрении вопроса возникновения угрозы информационной системы частым недостатком является формальное описание угроз и способов их устранения. Мы предлагаем рассмотреть этот вопрос с позиции построения дискретной динамической системы с помощью сети Петри [1–5]. Для моделирования динамики возникновения и реализации угроз несанкционированного доступа к информации часто используется комбинированная имитационно-аналитическая модель.

В качестве формальной модели динамики возникновения и реализации угроз несанкционированного доступа на объекте информации предлагается использовать расширения сетей Петри временным и вероятностным компонентом, а также механизмом учета приоритетов переходов в разрабатываемой дискретной динамической системы. Для этого представлены следующие возможности: задание для каждой позиции требуемого закона генерации фишек (равномерный, пуассоновский, и др.); задание для каждого перехода его параметров (значение приоритетов, вероятность срабатывания, время задержки, вносимое переходом в работе модели (в тактах)); возможность закрытия перехода; возможность настройки параметров эмуляции (длительности такта эмуляции и длительности межтактового интервала).

В процессе работы эмулятора сетей Петри сохраняется предыстория каждой позиции, т. е. существует возможность проследить число фишек в позиции на любом шаге эмуляции, что позволяет контролировать корректность работы модели. Предлагается следующий алгоритм анализа угроз.

1. Реализовать аналитическую модель динамики возникновения угроз несанкционированного доступа к информации.

2. Представить структуру модели как сеть Петри – ориентированный мультиграф, состоящий из совокупностей позиций и переходов, соединенных ориентированными дугами, определяющими входные и выходные позиции того или иного перехода.

3. Представить совокупность позиций как множество состояний системы, переходы должны соответствовать некоторым действиям (процессам), выполняемым в ней.

4. Ввести маркировку сетей Петри (каждый узел (позиция) сети имеет числовое значение маркировки) для определения очередности запуска того или иного перехода.

5. Для каждого позиции (узла) сети выполнить ввод функций уязвимости и функций защиты информации. Произведение этих функций $U \cdot Z = 1$, т. е. чем

больше функция защиты, тем меньше уязвимость, чем больше уязвимость, тем меньше защита.

6. Для каждой позиции (узла) сети Петри реализовать возможность задать источники компьютерных инцидентов (например, вирусы) в соответствии с принятой классификацией, например: **Unauthorised use** – неавторизованное использование одного или нескольких компьютеров в сети; **Password capture** – захват сведений о компьютере и паролей вирусом, «Троянским конем», и т. д. **/etc/passwd grabbed** – **/etc/** захваченный пароль файла был удален компьютером.

7. Задать для каждой позиции закон генерации фишек (равномерный, пуассоновский, и др.); этот закон генерации фишек определен функцией уязвимостей и свойств защиты информации для каждой позиции.

8. Сохранять предысторию каждой позиции, т. е. предусмотреть возможность проследить число фишек в позиции на любом шаге эмуляции, что позволяет контролировать корректность работы модели.

9. Задать для каждого перехода его параметры (значение приоритетов, вероятность срабатывания, время задержки, вносимое переходом в работе модели (в тактах)).

10. Предусмотреть возможность закрыть переход.

11. Ввести правило управления, определяющее во времени порядок изменения свойств позиций сети Петри и отражающее тем самым изменение текущего состояния объекта информации в условиях возникновения и реализации угроз несанкционированного доступа к информации. В общем случае структура управления может быть сложной, в ней нельзя заранее предсказать, какие операторы будут выполняться параллельно, последовательно, повторно и т. д.

12. В модели определить показатель стойкости выбранного пароля к вскрытию методом простого перебора. Этот показатель рассчитывается как полупроизведение числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов:

$$T_{\text{ож}} = \frac{A^s t}{2},$$

где A – число символов в алфавите, из которых составляется пароль; s – длина пароля; t – время, требуемое на попытку введения пароля: $t = \dfrac{E}{R}$, где R – скорость передачи (символы/с) в линии связи; E – число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы).

13. В качестве способа защиты от взлома пароля использовать следующую схему: подбор автоматически вызывает задержку обращения к компьютеру на 100 мкс.

14. Производить протоколирование последовательности взаимодействий последовательных процессов. В терминах сетей Петри это называется трассировкой поведения и записывается как последовательность срабатывания переходов сети.

15. Запоминать все компьютерные инциденты, произошедшие за время работы в системе. Для этого занести информацию в таблицу с полями данных: шаги по времени ($h, 2h, 3h, 4h, \ldots$); номера позиций (узлов); виды компьютерных инцидентов X_i; их количество (по каждому виду инцидента).

16. Полученная таблица представляет собой временной ряд. Объединить разные виды нарушений информационной безопасности в малое число групп, чтобы генерализовать данные по отдельным видам преступлений и получить устойчивые и статистически представительные результаты.

17. Например, сформировать несколько групп событий, соответствующих величине их интенсивности, то есть более сильные нарушения и менее сильные.

18. Просуммируем каждый временной ряд числа событий X_i данного вида инцидентов на суммарное число случаев и разделим на среднеквадратическое отклонение, а именно для каждого вида инцидентов заменим исходный числовой ряд $\{X_i\}_{i=1}^N$ нормированным рядом $\{x_i\}_{i=1}^N$:

$$x_i = \frac{(X_i - m(X))}{\sqrt{D(X)}}.$$

Тем самым будет достигнуто единообразие диапазона изменений числа событий по разным видам компьютерных инцидентов.

19. Рассмотреть пронормированные ряды данных $\{x_i\}_{i=1}^N$ в координатах вид инцидента – время и проинтерполировать полученную матрицу многочленами, эта интерполяция выполняется с помощью программных средств. Изобразив на рисунке строки матрицы, отвечающие пронормированным значениям числа инцидентов разного вида в некоторые моменты времени, проанализировать интенсивности нарушений безопасности.

20. Объектами прогноза будут моменты времени, на которые приходятся большие скачки числа событий.

21. Для каждой точки исходного ряда сильных нарушений $\{X_i\}_{i=1}^N$, начиная с k-й точки, вычислить среднее за k предыдущих измерений, то есть провести сглаживание ряда k-м фактором:

$$\langle X \rangle_i^k = \frac{1}{k}\sum_{i=1}^{k} X_{i-k}, \quad i = \overline{k, N}.$$

22. Составить ряд остатков, состоящий из разницы между числом событий по каждому виду инцидентов за данный период и полученным средним значением

$$X_i^S = X_i - \langle X_i \rangle_i^k.$$

Таким образом, вопросы информационной безопасности могут быть эффективно описаны с помощью конкретной дискретной динамической модели в виде системы Петри, исследованной в докладе. Алгоритм реализован в виде программы. Проведены тестовые расчеты.

Библиографические ссылки

1. Шувалов И. А., Семенчин Е. А. Математическая модель воздействия угроз на информационную систему обработки персональных данных // Фундаментальные исследования. 2013. № 10-3. С. 529–533.

2. Газизов Т. Т., Мытник А. А., Бутаков А. Н. Типовая модель угроз безопасности персональных данных для информационных систем автоматизации учебного процесса // Доклады ТУСУР. 2014. № 2 (32). С. 47–50.

3. Модель угроз безопасности информации и ее носителей / А. К. Новохрестов, А. А. Конев, А. А. Шелупанов, Н. С. Егошин // Вестник ИрГТУ. 2017. Т. 21, № 12 (131). С. 93–104.

4. Карпов В. С., Ивутин А. Н., Дараган Е. И. Сети Петри-Маркова и верификация программного обеспечения реального времени // Известия ТулГУ. Технические науки. 2010. № 4. С. 266–271.

5. Ивутин А. Н., Дараган Е. И. Теория сетей Петри и ее расширения // Известия ТулГУ. Технические науки. 2012. № 10. С. 211–221.

References

1. Shuvalov I. A., Semenchin E. A. A mathematical model of the threat impact on the information system processing personal data // Fundamental'nye issledovanija [Fundamental researches]. 2013. № 10-3. P. 529–533 (In Russ.).

2. Gazizov T. T., Mytnik A. A., Butakov A. N. Generic model of security threats for personal data in regard of information systems dedicated to academic planning // Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki [Proceedings of Tomsk State University of Control Systems and Radioelectronics]. 2014. № 2(32). P. 47–50 (In Russ.).

3. Information and information carrier security threat model / A. K. Novokhrestov, A. A. Konev, A. A. Shelupanov, N. S. Egoshin // Proceedings of ISTU. 2017. Vol. 21, № 12 (131). P. 93–104 (In Russ.).

4. Karpov V. S., Ivutin A. N., Daragan E. I. Networks of Petri – Markova and verification of the software of real time // Proceedings of TSU. 2010. № 4. P. 266–271 (In Russ.).

5. Ivutin A. N., Daragan E. I. Theory of the Petris networks and its expansion // Proceedings of TSU. 2012. № 10. P. 211–221 (In Russ.).