М. С. Соломатин,
ВУНЦ ВВС «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

Е. А. Рогозин,
доктор технических наук, профессор

И. Г. Дровникова,
доктор технических наук, доцент

СОЗДАНИЕ МОДЕЛИ ИНФОРМАЦИОННОГО КОНФЛИКТА «НАРУШИТЕЛЬ — СИСТЕМА ЗАЩИТЫ» НА ОСНОВЕ СЕТИ ПЕТРИ — МАРКОВА

THE CREATION OF A MODEL OF THE INFORMATION CONFLICT «INTRUDER — PROTECTION SYSTEM» ON THE BASIS OF PETRI — MARKOV NETWORK

В статье рассмотрен конфликт информационного взаимодействия «Нарушитель — Система защиты» с разными потенциальными возможностями сторон. Построена сеть Петри — Маркова, изображающая процесс протекания конфликта. Приведены основные интегрально-дифференциальные уравнения, описывающие информационный конфликт, и обоснован выбор параметров с целью исследования его динамических характеристик. Представлен алгоритм функционирования программно-аппаратного комплекса моделирования процесса протекания указанного конфликта.

The article considers the conflict of information interaction «Intruder — Protection system» with different potential capabilities of the parties. A Petri — Markov network depicting the conflict has been constructed. The basic integral-differential equations describing the information conflict are given and the choice of parameters for the purpose of research of dynamic characteristics of the specified conflict is proved. The algorithm of functioning of a hardware-software complex of modeling of process of the specified conflict is presented.

Введение. Уровень развития современных информационных технологий, появление новых угроз информационной безопасности и стремление снизить риски от возможных потерь конфиденциальных данных обуславливают высокую потребность в создании систем защиты информации.

Защита информационных ресурсов невозможна без определения возможностей каждой из сторон в информационном конфликте «Нарушитель — Система защиты». Ранее в работах, посвящённых исследованию информационного конфликта, предполагалось, что этапы конфликта начинаются одновременно, а возможности сторон равны [1]. На практике такое допущение выполняется довольно редко, поскольку реальные возможности одной из конфликтующих сторон, как правило, превышают возможности другой. Также следует учитывать ситуацию, в которой сторона, имеющая меньше возможностей и ресурсов, выигрывает конфликт в силу каких-либо обстоятельств или событий.

В связи с вышеизложенным возникает необходимость разработки модели информационного конфликта «Нарушитель — Система защиты» с разными потенциальными

возможностями сторон и обоснования её параметров с целью исследования динамических характеристик указанного конфликта, что является актуальным при создании информационных систем (ИС) в защищённом исполнении, а также при разработке и эксплуатации средств и систем информационной безопасности на объектах информатизации критического применения.

Теоретический анализ и новые научные результаты. Одной из основных задач при математическом моделировании отказоустойчивых систем как последовательности случайных событий является задача установления математического соответствия между временными и вероятностными характеристиками реально протекающих процессов и их аналитической моделью. Необходимо также учитывать, что при построении модели процессов в сложных системах должны быть отражены структурные и логические аспекты отказов.

Естественной моделью для описания случайной последовательности смены состояний некоторого объекта во времени является марковский, а в более общем случае — полумарковский процесс [2]. Однако наличие взаимосвязей в достаточно сложной системе приводит к необходимости учёта взаимодействия элементарных полумарковских процессов и формирования единого случайного процесса, учитывающего не только смену состояний отдельных элементов моделируемой системы, но и весь комплекс взаимодействий между элементами.

Традиционным инструментарием для анализа взаимодействия процессов являются сети Петри, однако, будучи асинхронными по определению, модели указанного типа позволяют лишь дать ответы на вопросы о принципиальной достижимости состояний системы, соответствующих заданным требованиям [3]. Спрогнозировать моменты переключения в указанные состояния с помощью сетей Петри в их классической интерпретации весьма затруднительно. Кроме того ограничения в моделировании параллельных процессов с помощью сетей Петри заключаются в ограниченности логических условий продолжения процессов элементарной конъюнкцией, что не позволяет учитывать всё многообразие взаимодействий элементов в реальных сложных системах.

Объединение двух подходов к моделированию отказов в сложных системах порождает сеть Петри — Маркова.

Сеть Петри — Маркова, представляющая собой структурно-параметрическую модель, заданную множеством, имеет следующий вид:

$$Y = \{\Pi, \mathrm{M}\}, \tag{1}$$

где: Π — описание структуры двудольного графа, представляющего собой сеть Петри;

M — описание параметров, накладываемых на структуру Π и определяющих временные, вероятностные и логические характеристики.

Структура сети Петри — Маркова характеризуется множеством

$$\Pi = \{\mathrm{A}, \mathrm{Z}, \mathrm{I}_A(\mathrm{Z}), \mathrm{O}_A(\mathrm{Z})\}, \tag{2}$$

где: $A = \{\mathrm{a}_{1(a)}, ..., \mathrm{a}_{\mathrm{j}(a)}, ..., \mathrm{a}_{\mathrm{J}(a)}\}$ — конечное множество позиций;

$Z = \{\mathrm{z}_{1(a)}, ..., \mathrm{z}_{\mathrm{j}(a)}, ..., \mathrm{z}_{\mathrm{J}(a)}\}$ — конечное множество переходов;

$I_A(Z) = \{I_A(\mathrm{z}_{1(\mathrm{z})}), ..., I_A(\mathrm{z}_{\mathrm{j}(\mathrm{z})}), ..., I_A(\mathrm{z}_{\mathrm{J}(\mathrm{z})})\}$

и $O_A(Z) = \{O_A(\mathrm{z}_{1(\mathrm{z})}), ..., O_A(\mathrm{z}_{\mathrm{j}(\mathrm{z})}), ..., O_A(\mathrm{z}_{\mathrm{J}(\mathrm{z})})\}$ — соответственно входная и выходная функции переходов;

$J(a)$ — общее количество позиций;

$J(z)$ — общее количество переходов [4].

В процессе функционирования ИС могут находиться последовательно в следующих состояниях: сотрудничество, соревнование, интеграция и противостояние (конфликт). Необходимо учитывать, что фиксация состояния ИС затруднена и не поддаётся

оценке с использованием формальных методов. Кроме того, не исключается возможность нахождения ИС в нескольких состояниях одновременно.

Остановимся более подробно на рассмотрении состояния конфликта ИС, для которого характерны как внутренние (обусловленные неправильно настроенным программным обеспечением, низкой квалификацией пользователей и т.д.), так и внешние («рукотворные») конфликты, вызванные действиями конкурентов. К последним можно отнести комплекс мероприятий, воздействующих на ИС в надежде получения какого-либо выигрыша (экономического, технологического и т.д.). Установление контроля над информационными ресурсами ИС (базами данных, программным обеспечением, вычислительной техникой, периферийным оборудованием, телекоммуникациями и т.д.) является основной целью информационного конфликта.

В свою очередь, к тактическим и стратегическим задачам информационного конфликта могут быть отнесены следующие:

- поражение элементов инфраструктуры ИС с использованием методов и средств информационного воздействия, в том числе средств уничтожения, искажения и хищения информации, преодоление механизмов защиты и системы информационной безопасности, ограничения или запрещения доступа законным пользователям, дезорганизация работы и т.д.;

- установление скрытого контроля (мониторинга) за использованием информационных ресурсов ИС.

Условно нарушителей можно объединить в две группы:

1. Исследователи, которые в рамках своей профессиональной деятельности связаны с разработкой, тестированием и сертификацией компонентов системы информационной безопасности.

2. «Энтузиасты» — специалисты, чья деятельность направлена на исследование существующих методов, средств и механизмов защиты информационных ресурсов на предмет их преодоления, причём подобная деятельность может преследовать коммерческие и криминальные цели.

Рассмотрим возникновение информационного конфликта с учётом разных потенциальных возможностей сторон, в зависимости от которых одна из них изначально получает преимущество и стремится в дальнейшем его усилить. Однако даже в этом случае слабая сторона может выиграть при условии, что действия противоположной стороны либо запаздывают, либо не являются адекватной реакцией на воздействие. Подобное развитие событий присуще как нарушителю, так и системе защиты. Кроме того возможен вариант паритетного исхода информационного конфликта [5].

Имея приведённые выше исходные данные и учитывая условия протекания информационного конфликта, представим его в виде сети Петри — Маркова (рис. 1). Это позволит наглядно учитывать все состояния и условия переходов в рассматриваемом конфликте.

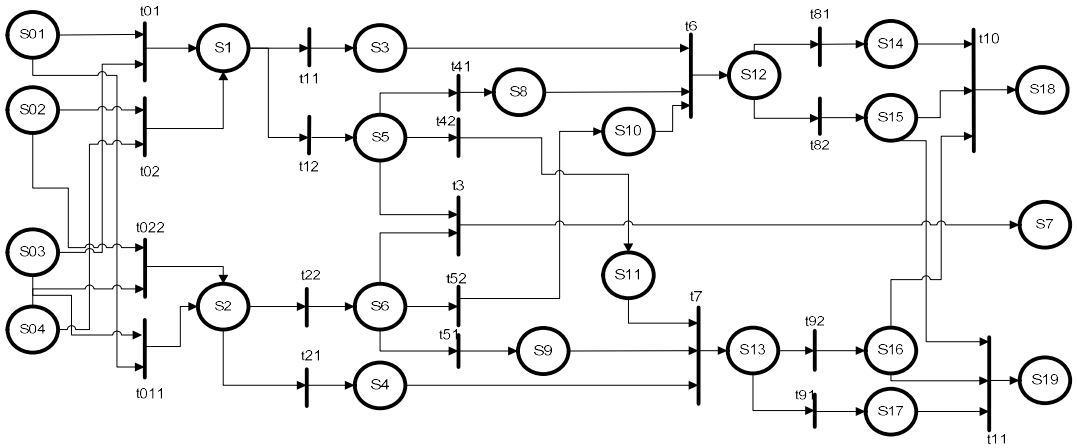

Рис. 1. Сеть Петри — Маркова, изображающая информационный конфликт «Нарушитель — Система защиты»

Обозначения наиболее важной части состояний s_i и переходов t_i этой сети приведены ниже:

S_{01} — производительность системы нарушителя задана;
S_{02} — объём памяти системы нарушителя задан;
S_{03} — производительность системы защиты задана;
S_{04} — объём памяти системы защиты задан;
t_{01}, t_{011} — сравнение производительности систем;
t_{02}, t_{022} — сравнение объёмов памяти систем;
S_1 — нарушитель имеет преимущество;
S_2 — система защиты имеет преимущество;
S_{14} — преимущество за нарушителем закреплено;
S_{15} — система защиты противостоит нарушителю;
S_{16} — нарушитель взламывает систему;
S_{17} — преимущество за системой защиты закреплено;
t_{10} — преодоление системы;
t_{11} — блокирование действий нарушителя;
S_7 — финальное состояние: паритетный исход конфликта;
S_{18} — финальное состояние: взлом системы, победа нарушителя;
S_{19} — финальное состояние: защита системы, победа системы защиты.

Для приведённых выше частей обозначений элементов сети и особенно важных состояний и переходов имеют место следующие уравнения [6]:

$$\Phi_{t011}(t) = \int_0^t (f_{s01}(\tau)\Phi_{s03t011}(t-\tau) + f_{s03}(\tau)\Phi_{s01t011}(t-\tau))d\tau, \tag{3}$$

$$\Phi_{t022}(t) = \int_0^t (f_{s02}(\tau)\Phi_{s04t022}(t-\tau) + f_{s04}(\tau)\Phi_{s02t022}(t-\tau))d\tau, \tag{4}$$

$$\Phi_{s16t11}(t) = \int_0^t f_{s16t11}(\tau)\Phi_{s13t92}(t-\tau)d\tau, \tag{5}$$

$$\Phi_{s17t11}(t) = \int_0^t f_{s17t11}(\tau)\Phi_{s13t91}(t-\tau)d\tau, \tag{6}$$

$$\Phi_3(t) = \int_0^t (f_{s5}(\tau)\Phi_{s6t3}(t-\tau) + f_{s6}(\tau)\Phi_{s5t3}(t-\tau))d\tau\,, \tag{7}$$

$$\Phi_{11}(t) = \int_0^t (f_{s17}(\tau)(1-\Phi_{s15t11}(t-\tau))(1-\Phi_{s16t11}(t-\tau)) + f_{s16}(\tau)(1-\Phi_{s15t11}(t-\tau))(1-\Phi_{s17t11}(t-\tau)) + \quad (8)$$
$$+ f_{s17}(\tau)(1-\Phi_{s16t11}(t-\tau))(1-\Phi_{s17t11}(t-))d\tau,$$

где: $f_{s_i t_j}(t)$ — плотность вероятности времени перемещения из состояния s_i к переходу t_j, $\Phi_{s_i t_j}(t)$ — соответствующий закон распределения, τ — среднее время перемещения по сети Петри — Маркова.

Считаем, что все переходы, необходимые для определения преимущества одной из сторон, описываются нормальным законом распределения и имеют плотность распределения вида [7]:

$$f_{s0it0j}(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-m)^2}{2\sigma^2}}, \quad (9)$$

где: $i = 1 \ldots 4, j = 1,\ 2,\ 11,\ 22$.

В качестве параметров используются математические ожидания и среднее квадратичное отклонение средней производительности систем нарушителя и защиты, а также математические ожидания и среднее квадратичное отклонение объёмов памяти систем.

Полагаем, что все действия по оставшимся переходам сети Петри — Маркова описываются экспоненциальным законом распределения вероятности и имеют плотность распределения вида [8]:

$$f_{sitj}(t) = \lambda_{ij} e^{-\lambda_{ij} t}, \quad (10)$$

где $\lambda_{ij} = \frac{1}{\tau_{ij}}, \tau_{ij}$ — средние времена переходов.

Значения средних времён переходов определяются на основе результатов исследований, опубликованных в [6]. Приведём в качестве примера значения средних времён некоторых основных переходов:

$\tau_{111} = 48$ с — среднее время обнаружения нарушителем системы защиты;

$\tau_{222} = 60$ с — среднее время обнаружения системой защиты действий нарушителя:

$\tau_{47} = 2$ с — среднее время начала противодействия системы защиты нарушителю.

Задавая математические ожидания и средние квадратичные отклонения систем, а также значения средних времён переходов, средних времён обнаружения или реагирования, можно не только в динамике наблюдать процесс развития информационного конфликта систем, но и определить вероятность достижения каждого из его финальных состояний.

Использование различных законов распределения случайных величин позволяет разработать рекомендации по выбору оптимальных параметров системы защиты информации.

На основе приведённой выше сети Петри — Маркова представляется возможным создать программно-аппаратный комплекс моделирования процесса протекания информационного конфликта «Нарушитель — Система защиты» (рис. 2).

Программно-аппаратный комплекс позволит моделировать информационный конфликт в его динамике, учитывая различные начальные условия и параметры системы защиты информации, воздействия и реакции на них, а итогом работы станет разработка рекомендаций по оптимизации выбора параметров системы защиты информации ИС.

Рис. 2. Блок-схема алгоритма функционирования программно-аппаратного комплекса моделирования процесса протекания информационного конфликта

Заключение. В статье рассмотрен информационный конфликт «Нарушитель — Система защиты» с разными потенциальными возможностями сторон, разработана его формальная модель с использованием аппарата сетей Петри — Маркова, получены основные аналитические выражения, описывающие информационный конфликт, обоснован выбор параметров для определения преимущества одной из конфликтующих сторон, указаны средние времена наиболее важных переходов сети. 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 ИС.

ЛИТЕРАТУРА

1. Язов Ю. К., Панфилов А. П. К вопросу о применении аппарата сетей Петри — Маркова для оценки вероятностно-временных характеристик динамики реализации угроз безопасности информации в компьютерных системах // Информационная безопасность. — 2008. — № 1. — С. 110—113.

2. Моделирование марковских случайных процессов. — URL: http://stratum.ac.ru/education/textbooks/modelir/lection33.html (дата обращения: 19.03.2019).

3. Сети Петри. Структура и правила выполнения сетей Петри. — URL: https://bit.ly/2TcBs6B. (дата обращения: 19.03.2019).

4. Модель процесса возникновения и протекания конфликта информационных средств разных видов / Ю. Л. Козирацкий [и др.] // Радиотехника. — 2011. — № 11. —

С. 6—11.

5. Методический подход к построению моделей информационного конфликта, обеспечивающих детальный анализ выигрышных ситуаций / В.И. Подлужный [и др.] // Радиотехника. — 2004. — № 5. — С.63—67.

6. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникацинных систем при реализации угроз удалённого и непосредственного доступа. — М. : РадиоСофт, 2010. — 232 с.

7. Нормальный закон распределения и его параметры. — URL: http://sernam.ru/book_tp.php?id=25 (дата обращения: 19.03.2019).

8. Экспоненциальное распределение и его свойства. — URL: http://statistica.ru/theory/ eksponentsialnoe-raspredelenie/ (дата обращения: 19.03.2019).