Моделирование комплекса средств защиты информации радиоканалов временными раскрашенными сетями Петри

Д. А. Лесняк[1], С. А. Матвеев[2]
Военно-космическая академия имени А. Ф. Можайского
[1]denislesnyk@mail.ru, [2]serg15332m@yandex.ru

***Аннотация*. An approach to the analysis of the information security of radio control channels based on the use of Petri nets is proposed and a model of unauthorized access to radio control channels is presented. Two strategies for maintaining the security of radio control channels are simulated.**

Ключевые слова: telecommunication systems; unauthorized access; temporary colored Petri nets

I. Инофомационная безопасность радиоканалов управления телекоммуникационных систем

На современном этапе развития телекоммуникационных систем управления, оперативность и гибкость управленческих воздействий в наземных, морских, авиационных, космических сегментах достигается путем использования радиоканала (радиорелейные, тропосферные и космические линии связи) [1]. Характерная особенность любого радиоканала заключается в пространственной электромагнитной доступности, которая создает условия для осуществления угроз несанкционированного доступа (НСД) к циркулируемой в ней информации. При этом НСД осуществляется, как правило, в сочетании с другими угрозами информационной безопасности (ИБ) (перехват, фальсификация, модификация передаваемой информации) и является, по сути, первой фазой их реализации [2]. Исходя из этого, к радиоканалам управления предъявляются высокие требования по обеспечению информационной безопасности и предотвращению НСД.

Как показывает практическая деятельность, применение инновационных разработок и новейшего комплекса средств защиты информации (КСЗИ) не позволяет гарантировать требуемую защищенность радиоканала управления. В большинстве случаев, это связано с постепенным снижением защищенности радиоканалов управления при неизменном составе средств защиты [3].

Поддержание защищенности радиоканалов управления на требуемом уровне в условиях конфликтного взаимодействия с противником основано на управлении КСЗИ под требуемые условия безопасности по результатам контроля или прогнозирования состояния защищенности радиоканалов управления. Исходя из, этого выделяют две базовые стратегии поддержания защищенности радиоканалов управления [4, 5]:

- на основе контроля текущего состояния;
- на основе прогнозирования текущего состояния.

Предотвращение НСД к радиоканалам управления, должно быть основано на использовании модели защищенности радиоканалов. В основе такой модели лежит формализованное описание процессов защиты и НСД к передаваемой информации с учетом как реализации противником угроз информационной безопасности, так и мер, направленных на их предотвращение. Решение антагонистических задач каждой из сторон информационного противоборства, а также некоторая информированность о действиях противоположной стороны приводит к необходимости его математического моделирования [6]. Одним из универсальных инструментов для анализа НСД к радиоканалам управления является использование сетей Петри [7].

Для основных стратегий поддержания защищенности радиоканалов управления [5] предлагается задать аналитическую модель, в которой выделим следующие этапы:

- Введение множества событий S и условий t реализации угроз НСД.
- Графическое представление сети Петри в виде двудольного графа с подробной детализацией событий и условий.
- Матричная запись логических функций срабатывания сети основных элементов.
- Представление сети Петри на основе системы интегрально-дифференциальных уравнений.
- Использование пуассоновского приближения среднего времени перемещения по сети Петри от исходного до конечного события.
- Определение вероятности обеспечения защиты радиоканалов управления.

II. Моделирование стратегий поддержаний защищенности в системе CPN Tools на основе языка сетей Петри

На рис. 1 представлено графическое представление сети Петри для стратегии поддержания защищенности на основе прогнозирования ее текущего состояния, разработанная в специальной моделирующей системе CPN Tools, которая использует язык сетей Петри для описания моделей [8].

В представленной модели позиции и переходы определены следующим образом:

S_1 – КСЗИ готово; S_2 – противник готов; t_1 – обнаружение предпосылок; S_3 – анализ уязвимостей; t_2 – оценка действий противника; S_4 – прогнозирование атак; t_3 – выработка воздействий на основе прогнозирования; S_5 – противодействие атаке; t_4 – нейтрализация атаки; S_6 – обеспечение защиты.

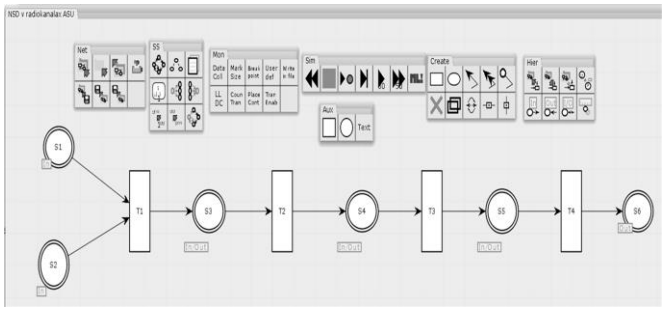

Рис. 1. Графическое представление сети Петри для стратегии поддержания защищенности на основе прогнозирования ее текущего состояния

Запишем матрицу, определяющую логические функции срабатывания сети:

$$V_{s_1\ t_4} = \begin{array}{c|cccc} & t_1 & t_2 & t_3 & t_4 \\ \hline s_1 & 1 & 0 & 0 & 0 \\ s_2 & 1 & 0 & 0 & 0 \\ s_3 & s_1t_1 \cap s_2t_1 & 1 & 0 & 0 \\ s_4 & 0 & 1 & 1 & 0 \\ s_5 & 0 & 0 & 1 & 1 \\ s_6 & 0 & 0 & 0 & 1 \end{array}. \quad (1)$$

Система интегрально-дифференциальных уравнений, для представленной сети будет иметь следующий вид:

$$\begin{aligned}
&\Phi_{s_1t_1}(t) = \pi_{11}\int_0^t f_{s_1t_1}(\tau)\,d\tau,\\
&\Phi_{s_2t_1}(t) = \pi_{21}\int_0^t f_{s_2t_1}(\tau)\,d\tau,\\
&\Phi_1(t) = \int_0^t f_{s_1t_1}(\tau)\Phi_{s_2t_1}(t) + \int_0^t f_{s_2t_1}(\tau)\Phi_{s_1t_1}(t)d\tau,\\
&\Phi_{s_3t_2}(t) = \pi_{32}\int_0^t f_{s_3t_2}(\tau)\Phi_1(\mathrm{t}-\tau)d\tau,\\
&\Phi_{s_4t_2}(t) = \pi_{43}\int_0^t f_{s_4t_3}(\tau)\Phi_{s_3t_2}(\mathrm{t}-\tau)d\tau,\\
&\Phi_{s_5t_4}(t) = \pi_{54}\int_0^t f_{s_5t_4}(\tau)\Phi_{s_4t_3}(\mathrm{t}-\tau)d\tau.
\end{aligned} \quad . \quad (2)$$

где $f_{st}(\tau)$ – плотность распределения вероятности времени перемещения из состояния S_i к переходу t_j, $\Phi_{st}(t)$ – соответствующий закон распределения, π_{ij} – вероятность срабатывания перехода, причем вероятности срабатывания всех переходов на данной траектории не зависят от времени, вероятность перемещения по всей сети рассчитывается по формуле:

$$\pi = \prod_{d_{ij}} \pi_{ij}. \quad (3)$$

где d_{ij} – все полушаги сети.

Будем считать, что плотность распределения вероятностей имеет экспоненциальную зависимость и имеет следующий вид:

$$f_{s_it\,j} = \lambda_{ij} e^{-\lambda_{ij}\tau}. \quad (4)$$

Использование прямого и обратного преобразования Лапласа получается довольно объемными, поэтому целесообразно применять пуассоновское приближение для плотности распределения вероятностей времени перемещения в переходы сети Петри.

Применяя пуассоновское приближение и эксппертные оценки, среднее время перемещения по сети Петри из начальной позиции до конечного перехода и зависимость вероятности этого пемещения примет следующий вид:

$$\tau = \frac{\tau_{11}^2 + \tau_{11}\times\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}} + \tau_{32} + \tau_{43} + \tau_{54}. \quad (5)$$

где τ_{11} – среднее время запуска и настройки КСЗИ; τ_{21} – среднее время запуска и настройки средств противника; τ_{32} – среднее время оценки и анализа уязвимостей; τ_{43} – среднее время выработки воздействий по результатам прогнозирования; τ_{54} – среднее время нейтрализации атаки.

На рис. 2 представлено графическое представление сети Петри в программе CPN Tools [8] для стратегии поддержания защищенности на основе контроля ее текущего состояния.

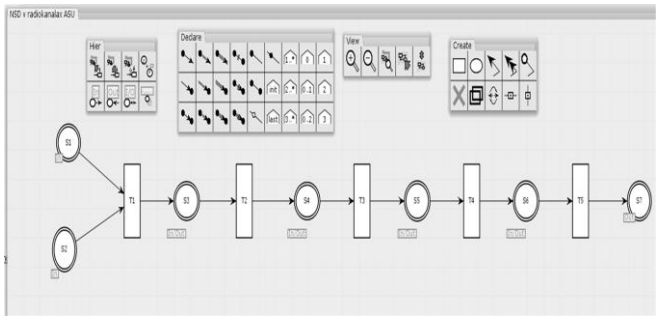

Рис. 2. Графическое представление сети Петри для стратегии поддержания защищенности на основе контроля ее текущего состояния

В представленной модели позиции и переходы определены следующим образом:

S_1 – КСЗИ готово; S_2 – противник готов; t_1 – обнаружение предпосылок; S_3 – анализ уязвимостей; t_2 – оценка действий противника; S_4 – обнаружение атак и фактов НСД; t_3 – оценка атаки; S_5 – идентификация атаки; t_4 – выработка воздействий; S_6 – устранение атаки; t_5 – нейтрализация атаки; S_7 – обеспечение защиты.

Запишем матрицу (6), определяющую логические функции срабатывания сети:

$$V_{s_1 t_5} = \begin{array}{c|ccccc} & t_1 & t_2 & t_3 & t_4 & t_5 \\ \hline s_1 & 1 & 0 & 0 & 0 & 0 \\ s_2 & 1 & 0 & 0 & 0 & 0 \\ s_3 & s_1 t_1 \cap s_2 t_1 & 1 & 0 & 0 & 0 \\ s_4 & 0 & 1 & 1 & 0 & 0 \\ s_5 & 0 & 0 & 1 & 1 & 0 \\ s_6 & 0 & 0 & 0 & 1 & 1 \\ s_7 & 0 & 0 & 0 & 0 & 1 \end{array} \qquad (6)$$

Система интегрально-дифференциальных уравнений, для представленной сети будет иметь следующий вид:

$$\begin{aligned}
&\Phi_{s_1 t_1}(t) = \pi_{11} \int_0^t f_{s_1 t_1}(\tau) d\tau, \\
&\Phi_{s_2 t_1}(t) = \pi_{21} \int_0^t f_{s_2 t_1}(\tau) d\tau, \\
&\Phi_1(t) = \int_0^t f_{s_1 t_1}(\tau) \Phi_{s_2 t_1}(t) + \int_0^t f_{s_2 t_1}(\tau) \Phi_{s_1 t_1}(t) d\tau, \\
&\Phi_{s_3 t_2}(t) = \pi_{32} \int_0^t f_{s_3 t_2}(\tau) \Phi_1(\mathrm{t}-\tau) d\tau, \\
&\Phi_{s_4 t_2}(t) = \pi_{43} \int_0^t f_{s_4 t_3}(\tau) \Phi_{s_3 t_2}(\mathrm{t}-\tau) d\tau, \\
&\Phi_{s_5 t_4}(t) = \pi_{54} \int_0^t f_{s_5 t_4}(\tau) \Phi_{s_4 t_3}(\mathrm{t}-\tau) d\tau, \\
&\Phi_{s_6 t_5}(t) = \pi_{65} \int_0^t f_{s_6 t_5}(\tau) \Phi_{s_5 t_4}(\mathrm{t}-\tau) d\tau.
\end{aligned} \qquad (7)$$

Применяя пуассоновское приближение, вычислим среднее время перемещения по сети Петри из начальной позиции до конечного перехода и зависимость вероятности этого пемещения по формуле (8):

$$\tau_{cp} = \frac{\tau_{11}^2 + \tau_{11} \times \tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}} + \tau_{32} + \tau_{43} + \tau_{54} + \tau_{65}. \qquad (8)$$

где τ_{11} – среднее время запуска и настройки КСЗИ; τ_{21} – среднее время запуска и настройки средств противника; τ_{32} – среднее время оценки и анализа уязвимостей; τ_{43} – среднее время оценки атаки; τ_{54} – среднее время выработки воздействий; τ_{65} – среднее время нейтрализации атаки.

На рис. 3 представлен график, демонстрирующий зависимость вероятности обеспечения защиты радиоканалов управления от времени, который наглядно иллюстрирует преимущество стратегии поддержания защищенности на основе прогнозирования ее текущего состояния (кривая 1) перед стратегией поддержания защищенности на основе контроля ее текущего состояния (кривая 2) [5]. Однако данная стратегия не лишена недостатков. Главным из них является риск того, что угроза является прогнозируемым фактом, который может и не случиться. Недостатком стратегии поддержания защищенности на основе контроля ее текущего состояния риском является то, что момент обнаружения угрозы есть состоявшийся факт, который мог быть зафиксирован несколько позже и ущерб уже причинен.

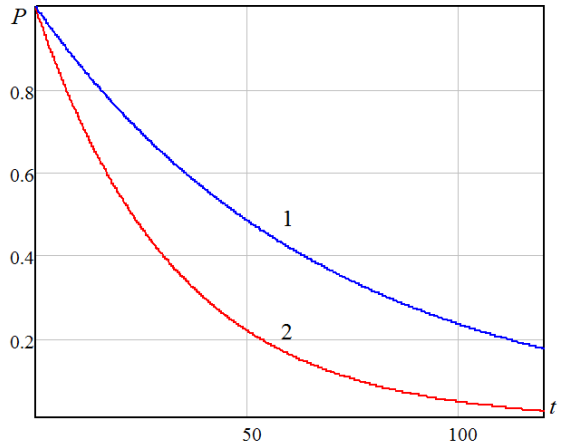

Рис. 3. Зависимость вероятности обеспечения защиты радиоканалов управления от времени

В то же время данная стратегия является единственной при поддержании защищенности радиоканалов управления и по возможности дополняется операциями непосредственной оценки текущего состояния защищенности с использованием средств обнаружения атак и фактов НСД. За счет соответствующего выбора математических моделей, используемых при прогнозировании, обеспечивается возможность аналитического расчета достижимых вероятностных характеристик уровня защищенности на интересующих интервалах времени, а задание критериев снижения уровня защищенности может осуществляться с запасом,

учитывающим достоверность прогнозирования. Кроме того, по своей природе текущая стратегия является упреждающей и направлена на недопущение реализации угроз информационной безопасности.

Модели, построенные с использованием сетей Петри представляет целостное формальное описание процесса обеспечения защиты радиоканалов управления, от момента появления источника угрозы до его предотвращения. Модель содержит графическое представление процесса защиты информации, в виде сетей Петри, носящих последовательный характер противодействий угрозам и в виде интегро-дифференциальных уравнений, описывающих процесс этот процесс. Реализовано сочетание экспериментальных методов для оценки временных характеристик и методов математического моделирования на основе сетей Петри, что позволяет оценить защищенность радиоканалов управления и определить наиболее эффективную стратегию поддержания защищенности.

СПИСОК ЛИТЕРАТУРЫ

[1] Спутниковая связь и вещание. Справ. / Под ред. Л.Я Кантора. М.: Радио и связь, 1997. 528 с.

[2] Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия–Телеком, 2004. 280 с.

[3] Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000. 248 с.

[4] Гаценко О.Ю. Защита информации. Основы организационного управления. СПб.: Издательский дом «Сентябрь», 2001. 228 с.

[5] Мальцев Г.Н., Лесняк Д.А. Применение стратегий поддержания защищенности в информационных системах // Информационно-управляющие системы. 2017. №3 (88). С.67-74.

[6] Владимиров В.И., Лихачев В.П., Шляхин В.М. Антагонистический конфликт радиоэлектронных систем. Методы и математические модели. М.: Радиотехника, 2004. 384 с.

[7] Питерсон Дж. Теория сетей Петри и моделирование систем: пер. с англ. М.: Мир, 1984. 264 с.

[8] Зайцев Д.А., Шмелева Т.Р. Моделирование телекоммуникационных систем в CPN Tools. Одесса, 2008. 68 с.