Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 15-22 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ASSESSMENT OF THE TECHNICAL CONDITION OF THE OBJECT CYBERNETIC PROTECTION SYSTEM
ОЦЕНКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ СИСТЕМЫ КИБЕРНЕТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА

Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev, Ukraine
Браиловский Николай Николаевич, кандидат технических наук, доцент, доцент Киевского национального университета имени Тараса Шевченко (г. Киев).

Volodymyr Vasko Taras Shevchenko National University of Kyiv, Doctor of Engineering Science, Full Professor, Kiev, Ukraine
Владимир Васько, Киевский национальный университет имени Тараса Шевченко (г. Киев).

Vasily Kuzavkov, Taras Shevchenko National University of Kyiv, Doctor of Engineering Science, Full Professor, Kiev, Ukraine
Кузавков Василий Викторович, доктор технических наук, профессор, профессор Киевского национального университета имени Тараса Шевченко (г. Киев).

Volodymyr Khoroshko, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine
Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор Национального авиационного университета (г. Киев).

Khokhlachova Yulia, National Aviation University of Kiev, PhD in Technical Sciences, Associate Professor Kiev, Ukraine
Хохлачова Юлия Евгеньевна, кандидат технических наук, доцент, доцент Национального авиационного университета (г. Киев).

ABSTRACT: The functioning of infrastructure facilities in such a specific environment as cyberspace associated with vulnerability and threats, therefore, requirements are put forward for the development of new tools for ensuring cyber resilience in the face of cyber attacks. The management of the cybersecurity stability of the functioning of infrastructure facilities is based on knowledge of the state of both the protected objects and the technical system of cyber protection of the objects themselves. That is, the technical state of the cyber defense system has become the dominant threat to industrial and important infrastructures. The paper considers the possibility of using Petri nets to assess the technical state of the object's cyber protection system. The presented method, built on associative principles, makes it possible to predict the technical state of the technical assessment system with a given accuracy, which makes it possible to provide the required level of object cyber security.

АННОТАЦИЯ: Функционирование объектов инфраструктуры в такой специфической среде, как киберпространство, связанное с уязвимостью и угрозами, поэтому выдвигаются требования по разработке нового инструментария обеспечения киберстойкости в условиях кибератак. Управление стойкостью кибербезопасности функционирования объектов инфраструктуры базируются на знаниях состояния как защищаемых объектов, так и самой технической системы киберзащиты самих объектов. То есть, доминирующей угроз для промышленных и важных инфраструктур стало техническое состояние системы киберзащиты. В работе рассмотрена возможность применения сетей Петри для оценки технического состояния системы киберзащиты объекта. Представленный метод, построенный на ассоциативных принципах, дает возможность прогнозировать техническое состояние технической системы оценок с заданной точностью, что позволяет обеспечить требуемый уровень киберзащищенности объекта.

KEYWORDS*: Petri models, cyber security technical systems, cyber resilience*

КЛЮЧЕВЫЕ СЛОВА: *модели Петри, технические системы кибербезопасности, киберстойкость.*

Введение

События конца XX- начала XXI веков проходят на фоне трансформации общества от постиндустриального к информационному. В мире происходит бурное развитие информационных технологий и их проникновение во все сферы деятельности человека. При этом, к основным характеристикам процесса информатизации общества на современном этапе следует отнести глобализацию и интенсификацию информационных процессов, изменение современной картины мира.

Согласно революции, в области информатизации и коммуникации происходят изменения в управлении государства, отраслей этого государства и определенных объектов инфраструктуры.

На современном этапе развития государства, когда управление информатизацией становится функцией, критично важной для бизнеса, а объемы информации постоянно увеличиваются, все острее становятся вопросы информационной безопасности, в целом, и кибербезопасности в частности [1,2].

При этом функционирование объектов инфраструктуры в такой специфической среде, как киберпространство, связанное с уязвимостью и угрозами, выдвигаются требования по разработке нового инструментария обеспечения киберстойкости в условиях кибератак. Управление стойкостью кибербезопасности функционирования объектов инфраструктуры базируются на знаниях состояния как защищаемых объектов, так и самой технической системы киберзащиты самих объектов. То есть, доминирующей угроз для промышленных и важных инфраструктур стало техническое состояние системы киберзащиты [3].

Разработка и исследование математической модели технической системы кибербезопасности (ТСКБ) требует значительных затрат времени. Как показывает опыт, применение сетей Петри (СП) для таких целей ускоряет процесс их создания. Однако их математический аппарат несколько громоздкий и при реализации на ПЭВМ занимает большие объемы памяти. Для решения практических задач требуется компактная отражающая сущность поведения и функционирования ТСКБ модель. Особенно остро этот вопрос стоит для моделирования в реальном масштабе времени при эксплуатации систем.

Известные на сегодняшний день интерпретации расширения и модификации сетей Петри [4,5] позволяют в основном моделировать параллельные процессы в программном (алгоритмическом) обеспечении вычислительных систем (на разных уровнях – от системного до микропрограммного) т.е., для выполнения двух и более различных алгоритмов на одной и той же вычислительно-управляющей системе требуется при известных подходах создание двух и более сетей Петри для изучения алгоритмов. Кроме того, в таких случаях традиционно присутствует требование отсутствия критических свойств в построенных моделях. В случае обнаружения какого-либо критического свойства делается вывод о неработоспособности рассматриваемого алгоритма и выполняются действия по такому изменению алгоритма, чтобы во вновь построенной адекватной модели критические свойства не были обнаружены. Основной недостаток такого подхода заключается в большой трудоемкости процесса многократного построения моделей алгоритмов для изучения их работоспособности.

Цель работы.

Целью работы является рассмотрение возможности применения сетей Петри для оценки технического состояния системы киберзащиты объекта.

Основная часть.

Таким образом, опыт использования модификации сетей Петри для моделирования сложных систем и оценки технического состояния их позволяет утверждать, что средства моделирования должны обладать следующими свойствами [6,7,8]:

- иерархическое представление моделей;
- единые средства построения и описания моделей на всех уровнях иерархии;
- простота детализации моделей;
- легкость машинного представления создаваемых моделей;
- возможность концентрации внимания только на необходимых (анализируемых) состояниях и режимах работы системы;
- возможность использования одной модели в разных целях;
- возможность моделирования до уровня логических элементов;
- использование формальных методов оптимизации процессов моделирования и анализа;
- наличие способов контроля корректности построения модели и исследования свойств модели;
- возможность представления всего моделируемого и анализируемого процесса в динамике;
- простота и наглядность при формулировании проблемы или алгоритма оценки технического состояния объекта исследования (в нашем случае ТСКБ).

В результате проведения анализа известных попыток использования сетей Петри для анализа технического состояния ТСКБ была разработана оригинальная модифицированная система – аппаратные сети Петри [8].

Для эффективного использования широкого спектра возможностей аппаратных сетей Петри (АСП) необходимо на базе АСП-системы специального математического обеспечения с набором средств описания, ввода, вывода, трансляции, компоновки, имитации модели, обработки результатов моделирования и анализа.

В настоящее время известны ряд способов описания исходных моделей и внутримашинного представления моделей ТСКБ для проведения имитационных экспериментов на базе СП.

При построении системы имитационного моделирования на СП существенную роль играет выбор:

способа описания исходных моделей;

способа внутримашинного представления описанной модели и на его основе – организации алгоритма моделирования.

Внутримашинное представление СП может быть организовано в виде матриц, либо в виде списков структур.

В нашем случае внутримашинное представление организовывается матриц. Поэтому СП может быть описана двумя типами матриц: матрицей инцидентности E размерностью n x m, где n – число вершин мест, m – число вершин переходов модели, и матрицей движения меток F размерностью, которые определяются следующим образом:

1) $E(i,j) = 1, \text{если } P_i \in P_{ij}^I;\ E(i,j) = 0, \text{если } P_i \notin P_{ij}^I;$

2) $F(i,j) = \alpha + \beta$, где $\alpha = 1$, если $P_i \in P_{ij}^I$;

$\alpha = 0$, если $P_i \notin P_{ij}^I$; $\beta = -1$, если $P_i \in P_{ij}^0$

$\beta = 0$, если $P_i \notin P_{ij}^0$.

Обозначим A^j - j-й столбец матрицы A. Тогда можно утверждать:

а) переход t_j может быть запущен, если $E^j - m_0^{-(k)}$;

б) последующая разметка после срабатывания t вычисляется по формулам

$m_0^{-(k+1)} = m_0^{-(k)} + F^{(I)}$,

$-\left[E_j \longrightarrow m_0^{-(k)}\right] \equiv \left[E^j m_0^{-(k)}\right] = \left[E^j \Big/ m_0^{-(k)} = 0\right]$.

Следовательно, условие запуска переходов t_j состоит в выполнении условия $E^j m_0^{-(k)} = 0$, а последующая разметка вычисляется следующим образом:

$m_0^{-(k+1)} = m_0^{-(k)} \oplus B^{(j)}$, где $\oplus$ - обозначение операции, исключающей ИЛИ; B(i,j) =1, если F(i,j)≠0; B(i,j) =0, если F(i,j)=0.

Здесь все операции выполняются над векторами булевых переменных, что позволяет достаточно эффективно реализовывать этот способ на ПЭВМ.

Недостаток указанного способа заключается в необходимости проверки на каждом шаге моделирования разметки всех входных мест каждого из переходов, что приводит к значительным неэффективным затратам времени. Более высокое быстродействие достигается путем представления каждого из переходов t_v одним из мест $P_E^\tau \in P_{tv}^I$. Для запуска перехода t_v необходимо (но недостаточно) выполнение $m(P_E^\tau) = 1$.

Определим вектор булевых переменных D размерностью m x 1, а также матрицы A и C размерностью m x m:

- D(j) = 1, если $m(P_i^\tau) = 1,\ P_i^\tau \in P_{ij}^I$;
- C (i,j) = 1, если t_j и t_i представлены одним и тем же местом P_ε^τ;
- A(i,j) =1, если t_j представлено местом $P_\varepsilon^\tau \in \Theta_{ij}$.

Тогда после срабатывания t_i последующая разметка вычисляется по формуле $D^+ = D \oplus A^j \oplus C^j$ и модулирующий алгоритм выглядит следующим образом:

DATA INPUT

FOR j: = 1 TO m DO

IF D(j) = 1

THEN IF $m_0^{-(k)} E_j = 0$

THEN < генерация действий, соответствующих t_j >

$m_0^{-(k+1)} = m_0^{-(k)} \oplus B^{(j)}$

$D^+ = D \oplus L^j$.

Здесь $L^j = A^j \oplus C^j$ позволяет экономить объем используемой памяти. При таком подходе можно сократить время выполнения программы с одновременным увеличением объема занимаемой памяти (за счет матрицы L и вектора D). Для снижения объема занимаемой памяти целесообразно внутримашинное представление моделей в виде стековых структур, так как E, F, L – разреженные матрицы. В результате размер используемой памяти линейно зависит от значений m и n, тогда как в случае матричного представления этот размер пропорционален m x n.

Одним из способов достижения компромисса между сложностью и достоверностью математической модели является упрощение эквивалентной объекту сети производящееся с помощью маршрутов функционирования системы [4] на основе аппарата нечетких множеств и нечетких отношений в пространстве, определенном расширяемой базой делимых ТСКБ. В эту

же базу данных заносятся сведения о поведении системы при внешних воздействиях. Модели, получаемые таким способом, имеют управляемую размерность и на основе строгих математических правил преобразуются либо в компактный, либо в расширенный вид. Достоверность модели ТСКБ является не выходным, а входным параметром для моделирования. Отсюда и главным достоинством такого подхода является маршрутная модель с заранее задаваемой достоверностью, позволяющая прогнозировать динамику состояния ТСКБ.

Рассмотрим принципы построения маршрутов, маршрутных моделей и моделирующей базы данных. Примем за X универсальное множество возможных состояний моделируемого объекта. Пусть X моделируется с требуемой достоверностью φ множеством описаний M_o, состоящих из элементов $\overline{m}$.

Поэтому

$$M_0 \leq \chi;$$
$$M_0 = \left\{ {}^{M}/_{\overline{M}} \in X,\ \mu(\overline{M}) \geq 1 - \varphi \right\}, \quad (1)$$

где $\mu(\overline{M})$ – функция принадлежности описания $\overline{M}$ множеству X.

Маршрут, как отображение Марковского процесса с нечеткими начальными условиями по отношению к нечеткому множеству описаний M_0, является множеством уровня $\alpha \neq 1 - \varphi$;

$$M = \left\{ {}^{\overline{M}}/_{M_0},\ \mu(\overline{M}) > \alpha \right\}, \quad (2)$$

Однако учитывая правила упорядочения элементов в M_0 маршрут можно представить в виде APN = (P,T,K,S), где M_0 отображает характер компонента APN.

Будем считать, что множество отношений, соответствующих «нормальному» маршруту $M_н$, определяется как:

$$M_н = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \mathrm{M}_0, \mu(\overline{\mathrm{M}}) > \beta \right\}, \quad (3)$$

где β – параметр задаваемой устойчивости ТСКБ к внешним воздействиям.

В тоже время для «экспериментального» маршрута $M_э$ справедливо следующее утверждение:

$$M_э = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \mathrm{M}_0,\ \mu_э(\overline{\mathrm{M}}) > \beta^I \right\}, \quad (4)$$

где β^I – параметр задаваемой границы неустойчивости ТСКБ.

При расширении и сужении множеств моделирующих отношений следует руководствоваться следующими принципами расширения нормативного маршрута с учетом экспериментального маршрута:

$$M_1 = \left\{ {}^{\mathrm{M}}/_{\overline{\mathrm{M}}} \in \overline{\mathrm{M}}_0,\ \mathrm{M}_1(\overline{\mathrm{M}}) \right\}, \quad (5)$$

где

$$\mathrm{M}_1(\overline{\mathrm{M}}) = \begin{cases} 0, \text{ если } \{\mu_э(\overline{\mathrm{M}}) \mathrm{X} \mu_н(\overline{\mathrm{M}})\} < \beta \\ max[\mu_э(\overline{\mathrm{M}})] \text{ если } \left[\mu_н(\overline{\mathrm{M}}) V \mu_{ij}(\overline{M})\right] \geq \beta \end{cases}.$$

Сужение экспериментального маршрута с учетом нормативного маршрута описывается:

$$M_2 = \left\{ \overline{\mathrm{M}}/_{\mathrm{M}} \in \overline{\mathrm{M}}_0,\ \mathrm{M}_2(\overline{\mathrm{M}}) \right\}, \quad (6)$$

где

$$\mathrm{M}_2(\mathrm{M}) = \begin{cases} 0, \text{ если } [\mathrm{M}_э(\overline{\mathrm{M}}) V \mu_н(\mathrm{M})] \geq \beta \\ max[\mathrm{M}_э(\mathrm{M}), \mathrm{M}_н(\mathrm{M})] \text{ если } [\mathrm{M}_э(\mathrm{M}), \mathrm{M}_н(\mathrm{M})] \leq \beta \end{cases}.$$

Из условий (5) и (6) следует

$$\lim_{\beta \to 0} M_1 = \lim_{\beta \to 0} M_2 = M_0. \quad (7)$$

Скорость переходов и достоверность размещений для позиций моделирующей СП является мерой информативности соответствующим им отношений.

При $\beta = 1$ в СП, синтезируемую на маршрутных множествах, войдут наиболее «живые» переходы СП, построенные на M_0 [8]. По мере роста количества узлов СП функция принадлежности перехода множеству «живых» переходов убывает. Заменив понятия скорость на экспертную оценку принадлежности перехода множеству «живых» переходов, удается отойти от непосредственного решения вопроса о возможности срабатывания того или иного перехода.

Для множества состояний типа маршрутных множеств исходное состояние обозначим через M_p , а достижимое из него как M_p^+. Тогда прогноз как линейный оператор описывается следующим образом:

$$F = M_p^- = M_p^+, \quad (8)$$

где F - линейный оператор прогноза:

$$M_p^- \subseteq \text{ и } M_p^+ \subseteq M_1.$$

Прогноз как функция определяется в базисе M_0 как функция принадлежности состояния M_p^- множеству оценок технического состояния ТСКБ [9]. Аспекты прогноза имеют свои прогнозы в APN и формализуется как линейный оператор в пространстве, порождаемом M_0, и как функционал, определяемый линейной формой в пространстве M_0.

Из соотношения (8) видно, что прогноз как линейный оператор и как, функционал образуют дерево возможностей, так как по определению из выражений (5) и (6) следует, что мощность M_1 больше, чем M_2. При машинной реализации это приводит к решению задач комбинаторного типа и к экспоненциальному росту размерности модели. Вследствие этого проводим отсечение ветвей, т.е. принимаем к рассмотрению только те ветви дерева возможностей, функция принадлежности которых M_0 менее β. Основой для реализации такого подхода на ПЭВМ следует выделение и анализ так называемых стационарных состояний ТСКБ. По отношению к M_0 множество стационарных состояний определяется как

$$M_0 \leq M_c,$$

$$M_c\{\overline{M}/\overline{M} \in M_{01} M_c(\overline{M})\} \cong 1,$$

где M_c – множество стационарных событий. Все элементы M_c являются корнями нормированного маршрута при отсутствии внешних воздействий. Внешние воздействия образуют пространство возмущений, базисом которого является элементарное воздействия [10,11]. Каждому элементу M_c соответствует нечетко ограниченное подпространство пространства возмущений. Иными словами, элементом M_c присваивается чувствительность к элементам базиса пространства возмущений, тем самым давала начало экспериментальному

маршруту. OS каждого стационарного состояния ведет свое начало множество экспериментальных маршрутов, по одному на каждый нулевой элемент базиса подпространства возмущений. Отношения между маршрутными множествами и множеством стационарных состояний поля

$$M_э \cap M_c = M_н \cap M_c = M_c.$$

Другими словами, базисные воздействия порождают символы деревьев возможностей.

Анализ стационарных состояний ТСКБ должен выявить возможность между ними. В случае большой сложности оборудования применяются экспериментальные оценки взаимосвязанности элементов M_0. Результат анализа – СП стационарных состояний, является основой для построения базы данных и прогнозирования технического состояния ТСКБ.

Так как СП стационарных состояний включает в себя узловые моменты функционирования ТСКБ, то она отражает характер поведения оборудования согласно заложенному алгоритму. Таким образом, СП стационарного состояния является моделью штатной работы ТСКБ. Прогнозируемость технического состояния системы опирается на марковский характер функционирования оборудования, с одной стороны и на систему оценок ТСКБ – с другой стороны.

Для корректного определения технического состояния ТСКБ необходима система оценок, которая удовлетворяла бы следующим требованиям [11]:

1) система оценок технического состояния должна содержать приоритеты (веса) соответствующих выходных ветвей СП стационарных состояний, выражающихся в виде функций принадлежностей состояний выходной ветви множества технических состояний ТСКБ;
2) глубина рассмотрений (детализации) технических состояний ТСКБ определяется задаваемой достоверностью φ.

С учетом этих требований модель системы реализуется на основании выражений (1)-(8) и представляет собой модель построенную на ассоциативных принципах. В зависимости от требуемой достоверности моделирования глубины поиска в базе данных и подключения узлов сетей Петри может изменяться в широких пределах, так как данные в базе данных упорядочены в виде множества пересекающихся деревьев. Пересечение деревьев следует понимать, как нечеткое отношение. Узел пересечения представляет собой нечеткие множества, которым придана мера в виде функции принадлежности узла дерева узлу ассоциации. В зависимости от переходных требований ассоциации требования к модели могут расширятся, распределяться или образовывать с другими ассоциациями новую, более широкую модель системы. Сведенные в базу данных маршруты организуют ассоциативный доступ к характерным состояниям ТСКБ, одновременно дополняя содержащуюся в базе данных информацию новой необходимой и при этом удаляя старую ненужную.

Выводы

Представленный в работе метод позволяет прогнозировать техническое состояние технической системы оценок с заданной точностью, что дает возможность обеспечить требуемый уровень киберзащищенности объекта.

ЛИТЕРАТУРА

1. Грищюк Р.В., Даник Ю.Г. Основи кібернетичної безпеки – Житомир: ЖНАЕУ, 2016. – 636 с.
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К: ТОВ «СІК ГРУП Україна», 2015. – 449 с.

3. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. – К: ЦП «Компринт», 2021. – 296 с.
4. Питерсон Дж. Теория сетей Петри и моделирующие системы. Изд. 2-е. – М.: Мир, 2001. – 266 с.
5. Котов В.Е. Сети Петри. Изд. 3-е. – М.: Наука, 2004. – 168 с.
6. Томашевский В.М. Моделирование систем. К.: Вид. Груп BHV, 2007 – 352 с.
7. Креденцер Б.П., Буточнов О.М., Міночкін А.І., Могилевич Д.І. Надійність систем з надлишковістю: методи, моделі, оптимізація. – К.: «Фенікс» 2013. 342 с.
8. Хорошко В.А., Моржов С.В. Применение сетей Петри для моделирования параллельных процессов// Проблемы управления и информатики, №2, 2004. – с. 86-94.
9. Опірський І.Р. Проблематика основного постулату прогнозування НСД // Сучасна Спеціальна Техніка, №2 (41), 2015.- с. 3-8.
10. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности – К.: Изд. ГУИКТ, 2009. – 215 с.
11. Хорошко В.А., Чирков Д.В. Исследование процессов и структур систем защиты на основе аппарата Петри // Системи обробки інформації. – Вип. 7 (88), 2010. – с.236-245.