УДК 004

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ВЛОЖЕННЫХ СЕТЕЙ ПЕТРИ

П.А. Щербинин, Ю.Ф. Мартемьянов

Рассматривается подход к моделированию воздействия угроз информационной безопасности на информационную систему основанный на применении вложенных сетей Петри

Ключевые слова: угрозы информационной безопасности, вложенные сети Петри

Одним из ключевых аспектов проблемы обеспечения безопасности информационных систем является определение и анализ актуальных угроз. Однако недостаточно только выявить актуальные угрозы, необходимо также определять текущее состояние информационной системы и прогнозировать её поведение с учётом их воздействия. В связи с этим актуальной становится задача моделирования состояний информационной системы, в которые она переходит под воздействием угроз информационной безопасности. Однако при построении модели необходим большой объём исходных данных, характеризующий набор состояний, в которых находится исследуемая система, формирование которого весьма затруднительно. Поэтому для решения рассматриваемой задачи предлагается использовать аппарат теории сетей Петри.

Наиболее подходящим с точки зрения адекватности результатов моделирования представляется использование вложенных сетей Петри. Вложенные сети Петри представляют собой расширение стандартного формализма сетей Петри, в котором маркеры, обозначающие ресурсы в позициях сети, сами являются сложными объектами с сетевой структурой.

Разрабатываемая сеть Петри позволяет построить модель, в которой на ресурсы и средства защиты (элементные сети) моделируемой информационной системы (системная сеть) воздействует множество угроз информационной безопасности (элементные сети). Количество угроз, воздействующих на информационную систему, потенциально не ограничивается, однако все возможные типы таких угроз определяются в [1] и признаются актуальными; множество ресурсов фиксировано и конечно. Кроме того, в рамках разрабатываемой сети моделируется автономное взаимодействие угрозы и ресурса или угрозы и защищённого ресурса (ресурса с установленным или встроенным средством защиты информации) информационной системы, на который она воздействует.

Таким образом, в общем случае разрабатываемая вложенная сеть Петри состоит из системной сети *SN*, моделирующей состояния информационной системы, и элементных сетей $TN_i\,(i=\overline{1;n})$ и $RN_j\quad(j=\overline{1;k})$, представляющих угрозы информационной безопасности и ресурсы информационной системы соответственно. Для того чтобы учитывать, какая именно угроза воздействует на конкретный ресурс, в качестве маркеров используются пары элементов. Тогда системная сеть *SN* будет содержать маркеры следующих типов: атомарные чёрные маркеры, сетевые маркеры – угрозы, сетевые маркеры – ресурсы и пары маркированных сетей (угроза-ресурс). В качестве выражений, приписанных дугам, используются переменные, константы и пары переменных. В разрабатываемой сети используется два вида синхронизации: вертикальная (переход в системной сети срабатывает одновременно с некоторыми переходами в элементных сетях) и горизонтальная (два находящихся в одной позиции перехода в элементных сетях срабатывают одновременно).

Функционально разрабатываемая вложенная сеть Петри может быть условно разделена на следующие модули (рис. 1):

Щербинин Павел Алексеевич – ТГТУ, аспирант,
Мартемьянов Юрий Федорович – ТГТУ, канд. техн. наук, профессор,

основной модуль функционирования системы; модуль генерации угроз; модуль функционирования угроз; модуль ресурсов (защищённых ресурсов); модуль взаимодействия угроз и ресурсов (защищённого ресурса); модуль сбора информации.

Функцией модуля генерации угроз разрабатываемой сети Петри является выработка сетевых маркеров системной сети, соответствующих конкретным возникающим угрозам, согласно вычисленным ранее вероятностям их возникновения, а также учёт взаимного влияния (порождения) угроз безопасности информации, действующих на систему.

Модуль функционирования угроз представляет собой элементные сети TN_i ($i = \overline{1;n}$), моделирующие динамику угроз в

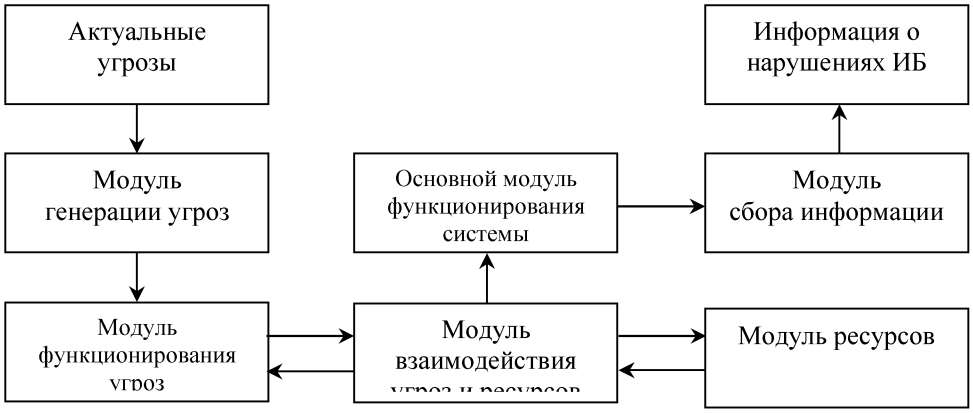

Рис. 1 – Структура модели

рассматриваемой информационной системе.

Модуль ресурсов состоит из элементных сетей RN_j ($j = \overline{1;k}$), описывающих изменение состояния ресурсов информационной системы при воздействии (отсутствии воздействия) угроз безопасности.

Модуль взаимодействия угроз и ресурсов представляет собой отдельную сеть Петри другого уровня иерархии, которая запускается при срабатывании составного перехода и моделирует процесс взаимодействия конкретной угрозы, действующей на определённый ресурс.

Основной модуль функционирования системы описывает динамику изменения состояний рассматриваемой информационной системы с учётом воздействия угроз безопасности информации и её переходы в состояния нарушения характеристик безопасности.

Модуль сбора информации осуществляет накопление маркеров в конечных состояниях системы для дальнейшего анализа полученной информации.

Определим формально структуру двухуровневой вложенной сети Петри, моделирующей воздействие n угроз информационной безопасности, признанных актуальными в информационной системе. Согласно определению из [2], двухуровневой вложенной сетью Петри называется набор

$$NPN = (Atom, Lab, SN, (EN_1, ..., EN_n), \Lambda),$$

где:

– $Atom = Var \cup Con$ – множество имён переменных и множество имён констант ($Con = Con_{net} \cup Con_{atom}$ – множество сетевых и атомарных меток); $Var = \{u_i\}_{i=1}^{n} \cup \{r_j\}_{j=1}^{k} \cup \{x\}$;

$Con_{net} = \{TN_i\}_{i=1}^{n} \cup \{RN_j\}_{j=1}^{k}$ с нанесённой на них разметкой; множество Con_{atom} представляет собой чёрный маркер.

– $Lab = Lab_v \cup Lab_h$ – множество меток, $\forall l \in Lab_v$, $\forall \lambda \in Lab_h$ существуют двойственные метки $\bar{l} \in Lab_v$, $\bar{\lambda} \in Lab_h$ соответственно, такие что если $\bar{l}_1 \neq \bar{l}_2$ для $l_1, l_2 \in Lab_v$, то $l_1 \neq l_2$; если $\bar{\lambda}_1 \neq \bar{\lambda}_2$ для

$\lambda_1\lambda_2 \in Lab_h$, то $\lambda_1 \neq \lambda_2$; $\overline{\overline{l}} = l$, $\overline{\overline{\lambda}} = \lambda$, использующихся для вертикальной и горизонтальной синхронизации соответственно;

– $\{TN_i\}_{i=1}^{n} \cup \{RN_j\}_{j=1}^{k}$ – конечный набор обыкновенных сетей Петри (элементные сети вложенной сети);

– $SN = (N, L, U, W, M_0)$ – сеть Петри высокого уровня, в которой: $N = (P, T, F)$ – сеть (P – множество позиций с приписанной им арностью, T – множество переходов, F – множество дуг); L – язык выражений над множеством $Atom$; $U = (A, I)$ – модель языка L (где $A = A_{net} \cup A_{atom}$ – множества маркированных элементных сетей (множество сетевых маркеров сети SN) и атомарных маркеров сети SN; $I : Con \to A$ – интерпретация констант языка L; W – функция сопоставляющая каждой дуге $(x, y) \in F$ некоторое выражение $W(x, y) = (\theta_1, ..., \theta_n)$, где $\theta_i \in L$ $(i = \overline{1;n})$ и n есть арность позиции, инцидентной дуге (x, y); M_0 – начальная разметка сети SN;

– Λ – частичная функция пометки переходов, помечающая некоторые переходы системной сети метками из Lab_v и некоторые переходы в элементных сетях метками из $Lab_v \cup Lab_h$.

В результате построена двухуровневая вложенная сеть Петри, которая состоит из системной сети, являющейся предикатной сетью Петри и обыкновенных сетей Петри, задающих структуру сетевых маркеров. Некоторые переходы в системной и элементных сетях, для обеспечения их синхронизации, снабжены специальными метками. Срабатывания переходов в системной и элементных сетях определяются по правилам срабатывания переходов предикатных и обыкновенных сетей соответственно. Правила синхронных срабатываний переходов определяются отдельно.

Рассмотрим фрагмент общей структуры системной сети Петри, моделирующей воздействие угроз информационной безопасности определенного типа на заданную информационную систему (рис. 2).

Воздействие любой угрозы из перечня актуальных либо переводит систему в состояние нарушения одной из характеристик безопасности информации (конфиденциальности, целостности, доступности), либо оставляет систему в состоянии штатного функционирования (при срабатывании средства защиты информации или невозможности реализации угрозы в конкретный момент времени).

Классифицируем состояния нарушения информационной безопасности по степени критичности (некритичные нарушения, нарушения средней критичности, критичные нарушения) и по нарушаемой характеристике безопасности (конфиденциальность, доступность, целостность). Степень критичности нарушения безопасности определяется в зависимости определённых в [1] опасности угрозы и степени критичности ресурса, на который она воздействует.

Таким образом, фрагмент системной сети состоит из следующих позиций: p_0 – угроза инициализирована в информационной системе; p_1 – угроза поступила в информационную систему; p_2 – воздействие угрозы завершено; p_3 – система функционирует в штатном режиме; p_4, p_5, p_6 – система функционирует с некритичным нарушением конфиденциальности, целостности, доступности соответственно; p_7, p_8, p_9 – система функционирует соответственно с нарушением конфиденциальности, целостности, доступности средней критичности; p_{10}, p_{11}, p_{12} – система функционирует с критичным нарушением конфиденциальности, целостности, доступности соответственно; p_{13}, p_{14}, p_{15} – выделен ресурс системы (в зависимости от типа ресурса); T_0 – составной переход (модуль генерации угроз); T_1 – поступление угрозы в информационную систему; T_2 – воздействие угрозы на выделенный ресурс;

T_3 – переход системы в штатный режим функционирования;

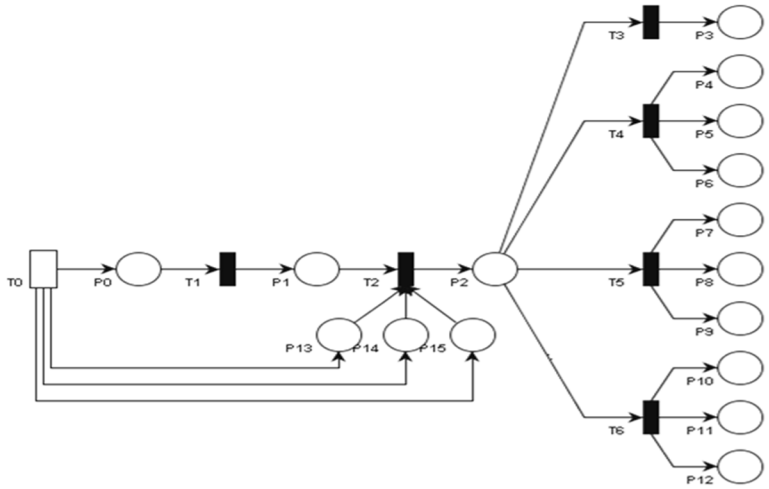

Рис. 2 – Фрагмент системной сети Петри

T_4, T_5, T_6 – соответственно некритичное, средней критичности и критичное нарушения характеристик безопасности.

Генерация новых угроз системной сети происходит в зависимости от возможности реализации угрозы, определённой в [1] (начальная генерация угрозы), либо под воздействием предшествующих угроз за счёт вертикальной синхронизации (при реализации цепочки последовательных угроз). В зависимости от способа генерации вложенные сети, характеризующие угрозы информационной безопасности, обладают различной начальной маркировкой и характеристиками переходов.

Позиции p_3 – p_{12} системной сети Петри являются стоковыми и накапливают информацию о нарушениях характеристик безопасности под воздействием угроз на информационную систему для дальнейшего анализа полученной информации и расчёта частных и показателей защищённости по характеристикам безопасности, а также обобщённого показателя защищённости информационной системы.

Таким образом, определена двухуровневая вложенная сеть Петри, моделирующая воздействие угроз информационной безопасности на ресурсы информационной системы, позволяющая моделировать динамику развития угроз и их взаимодействия с ресурсами информационной системы и её средствами защиты.

Литература

1. Щербинин, П.А. Логико-лингвистическая модель определения актуальности угроз информационной безопасности / П.А. Щербинин, Ю.Ф. Мартемьянов // Актуальные проблемы прикладной математики, информатики и механики: Сборник трудов Международной конференции, 26-28 сентября 2011г., Воронеж: Издательско-полиграфический центр ВГУ, 2011. – С.429-433.

2. Ломазова, И.А. Вложенные сети Петри: моделирование и анализ распределённых систем с объектной структурой.–М.: Научный мир, 2004. – 208с.

Тамбовский государственный технический университет
Tambov State Technical University

MODELING THE IMPACT OF INFORMATION SECURITY THREATS BASED ON NESTED PETRI NETS

P.A. Scherbinin, Y.F. Martemyanov

The approach to modeling the impact of information security threats for the information system based on nested Petri nets is consider

Key words: information security threats, nested Petri nets