УДК 004.056.53

МОДЕЛИРОВАНИЕ МЕХАНИЗМА АУТЕНТИФИКАЦИИ СУБЪЕКТА В ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

А. В. Яковлев, В. Е. Дидрих, К. М. Копылов

Тамбовский государственный технический университет

Наличие полной и достоверной информации, необходимой для принятия решений, в большинстве случаев является определяющим фактором достижения заданного результата. Следовательно, значимость эффективной защиты конфиденциальной информации в условиях постоянного совершенствования средств, способов и механизмов ее несанкционированного получения неуклонно возрастает [1]. В последнее время для анализа статических и динамических свойств сложных систем часто применяют математический аппарат сетей Петри, который позволяет наиболее адекватно формализовать динамику дискретных систем и процессов с параллельно функционирующими и асинхронно взаимодействующими компонентами [4]. В качестве формальной модели динамики возникновения и реализации угроз использовались сети Петри с временным, приоритетными и вероятностным механизмами. Для учета времени перехода ИС из состояния в состояние в процессе реализации угроз использовано время задержки срабатывания переходов сети Петри (реализации переходов с временем срабатывания ≠0). Для учета вероятностных характеристик моделируемого процесса использовалась вероятность срабатывания перехода. А путем добавления в модель приоритетов срабатывания переходов реализованы правила управления системой ЗИ в процессе функционирования ИС. Общее описание моделей можно представить в виде таблиц 1, 2, а общую структуру – рис. 1.

Таблица 1

Модель динамики возникновения и реализации угроз

$N = (P, T, I, O, \mu)$	
$P = \{p_1, p_2, \ldots, p_k\}$	
$T = \{t_1, t_2, \ldots, t_m\}$	
$I : T \to P^{\infty}$	$O : T \to P^{\infty}$
$\#(t_j, I(p_i)) = \#(p_i, O(t_j))$	$\#(t_j, O(p_i)) = \#(p_i, I(t_j))$
$\mu = \{\mu(p_i)\}$	

Таблица 2

Содержание компонентов модели динамики возникновения и реализации угроз

Обозначение элемента	Описание	Примечание
p1	Старт операционной системы	μ{p1}=1
p2	Инициализация ядра информационной системы	
p3	Инициализация подсистемы идентификации	
p4	Подготовка к запуску стартовых скриптов системных служб информационной системы	обобщенные позиции (возможно наличие нескольких позиций)
p5	Выполнение других функций	обобщенные позиции (возможно наличие нескольких позиций)
P6	Накопление значений параметра, не прошедших проверку	
p7	Передача параметра доступа к системе	
px1	Ввод идентификатора	μ{px1}=1
px2	Генерация и ввод нового значения параметра (пароля)	μ{p x2}=∞
t1	Загрузка операционной системы	
t2	Загрузка ядра информационной системы	
t3	Проверка идентификатора	
t4	Проверка аутентичности параметра	
t5	Регистрация пользователя и открытие сеанса	
I(ti)	I(t1)={p1}, I(t2)={p2}, I(t3)={px1,p3}, I(t4)={px2,p3}, I(t5)={p4, p5, p7}	
O(ti)	O(t1)={p2}, O(t2)={p3, p4, p5}, O(t3)={p3}, O(t4)={p6, p7}	

В качестве примера рассмотрим модели [2,3]:

- модель динамики реализации угрозы раскрытия параметров системы защиты методом «грубой силы» (например, подбор ключевой информации);
- модель динамики системы защиты при использовании схемы задержки обращения к средствам ВТ ИС после трех неудачных попыток подбора параметра;
- модель динамики системы защиты при использовании схемы блокировки ввода параметра после трех неудачных попыток подбора.

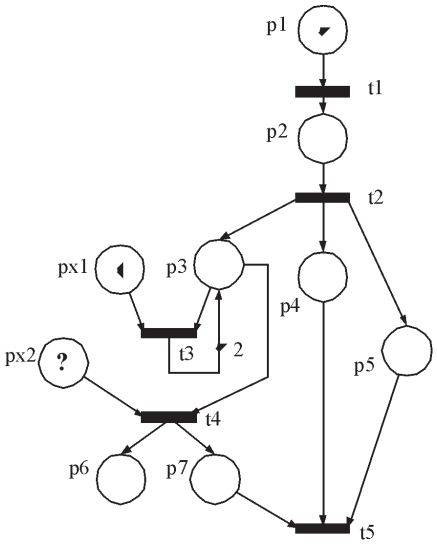

Рис.1. Сеть Петри, моделирующая этапы загрузки информационной системы

Структура сети Петри и ее описание, соответствующее первой модели, приведены на рис. 2. и в табл. 3 соответственно.

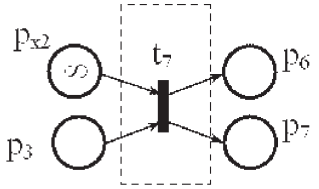

Рис.2. Структура сети Петри при реализации угрозы раскрытия параметров системы защиты методом «грубой силы»

Таблица 3

Описание сети Петри при реализации угрозы раскрытия параметров системы

Обозначение элемента	Описание	Примечание
px2	Генерация и ввод нового значения параметра (пароля)	μ{p1}=∞
p3	Инициализация подсистемы идентификации пользователей	
p6	Накопление значений параметра, не прошедших проверку	
p7	Передача параметра доступа к системе	
t4	Проверка аутентичности параметра	вероятность срабатывания≈ 3*10-12
I(ti)	I(t4)={px2, p3}	
O(ti)	O(t4)={p6, p7}	

Вместе с тем, чтобы уменьшить вероятность взлома системы данную модель можно несколько усложнить. Для этого используем следующую схему: после трех неудачных попыток подбора автоматически предусматривается задержка обращения к ЭВМ на время, выбранное исходя из необходимого уровня защиты, т.е. $t = t_0 + \Delta t$. Структура сети Петри и ее описание при реализации данного способа защиты приведены на рис. 3.

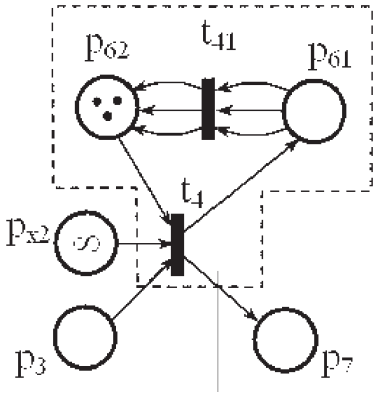

Рис. 3. Структура сети Петри при использовании схемы задержки обращения к средствам ВТ ИС после трех неудачных попыток подбора параметра

Результаты моделирования динамики угрозы несанкционированного получения аутентификационного фактора показывают эффективность предложенного метода защиты, особенно с накоплением времени задержки обращения. Так, при накоплении времени задержки в зависимости от попыток ввода *m*аутентификационного параметра: $\Delta t(m) = \exp(m) * 10^{-3}$, уже на 11 шаге итерации задержка превысит 1 минуту, а на 15 – 1 час.

Использование модифицированной модели позволяет определить, кроме ранее описанных параметров, функциональную зависимость параметров модели Δt >В m.

В качестве альтернативного способа уменьшения вероятность взлома системы защиты можно предложить другую схему: после трех неудачных попыток подбора блокировать ввод параметра. Структура сети Петри и ее описание при реализации данного способа защиты приведены на рис. 4.

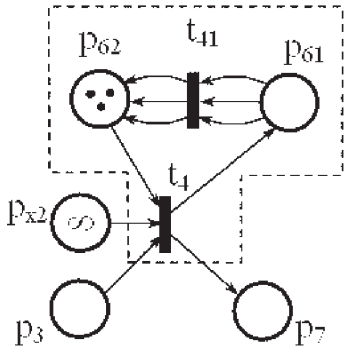

Рис. 4. Структура сети Петри при использовании схемы блокировки ввода параметра после трех неудачных попыток подбора

Данная модель также является эффективной в целях защиты [1], но при этом имеет ряд недостатков, одним из которых является необходимость реализации механизмов разблокировки системы ввода параметров после неудачной атаки.

Таким образом, разработанные модели позволяют:

определять параметры аутентификационного фактора (мощность алфавита; количество символов; время, требуемое на ввод очередной попытки; время задержки при вводе и т.д.);

оценивать надежность аутентификации (по временной сложности) при применении способов защиты информации в условиях корректного учета динамики процесса возникновения и реализации указанных угроз.

Список литературы

1. *Смит Р. Э.* Аутентификация: от паролей до открытых ключей : пер. с англ. / Р. Э. Смит. – М. : Вильямс, 2002. – 432 с.

2. *Зегжда Д. П.* Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая Линия – Телеком, 2000. – 452 с.

3. *Девянин П. Н.* Модели безопасности компьютерных систем / П. Н. Девянин. – М. :Академия, 2005.– 192 с.

4. *Питерсон Дж.* Теория сетей Петри и моделирование систем : пер. с англ. / Дж. Питерсон. – М. : Мир, 1984. – 264 с.

5. URL : http://s.aladdin-rd.ru/www/upload/iblock/1bb/authentication_authorization.pdf