

# Методика моделирования систем информационной безопасности на основе SADT-моделирования и аппарата сетей Петри

**В.Г. Криволапов**, аспирант, Московский инженерно-физический институт (Государственный университет)

В качестве перспективного подхода к моделированию систем и процессов обеспечения безопасности информации, предлагается использование объектно-ориентированного моделирования в нечетком базисе, поскольку довольно сложно использовать строгие аналитические модели в виду неполноты данных в значениях параметров элементов моделей. Этот подход моделирования позволит описать сложный объект на основе описания простых объектов — моделей, их взаимосвязи друг с другом, а также изменение состояний элементов систем и функционирование модели системы в целом. Поскольку исследования вопросов обеспечения безопасности информационных технологий усугубляется большой неопределенностью условий функционирования информационной системы, предлагается использование методологии SADT-моделирования (Structured Analysis and Design Technique). В статье под SADT-моделированием мы будем понимать стандарт SADT/IDEF0. Это методология, которая довольно четко отражает такие системные характеристики как управление, обратная связь и исполнители; имеет развитые процедуры коллективной работы, а также имеет возможность проектирования на ранних стадиях создания системы; имеет возможность сочетания и синхронизации с другими структурными методами проектирования.

Модель, описанная на основе SADT-моделирования, имеет ряд преимуществ, а именно: позволяет за счет использования понятий «Цель» и «Точка зрения» очертить предметную область; графически представить модель; позволяет за счет декомпозиции более детально рассмотреть функционирование необходимых компонентов. Несмотря на это, данное моделирование не позволит рассмотреть динамическое изменение системы. Предлагается компенсировать недостатки модели системы на основе SADT-моделирования добавлением модели системы на основе аппарата Петри.

Сети Петри применяются в довольно широком кругу для анализа систем, позволяют описывать динамику, имитацию работы системы, и вместе с тем, как и SADT-моделирование, имеют небольшое количество «примитивов» и имеют наглядное представление.

Одним из немаловажных свойств сетей Петри является иерархическое представление. Это свойство позволяет:

— анализировать процессы в системы с нужной степенью детализации;

— определить место того или иного процесса в общей структуре системы,

процессы обеспечения безопасности информационных технологий на достаточном уровне детализации.

Не существует единого методологического базиса, позволяющего перейти от функциональной модели, которая описывает механизмы функционирования системы, к модели подсистемы обеспечения информационной безопасности. Для решения поставленной задачи необходимо разработать алгоритм преобразования полученной на этапе функционального моделирования SADT-модели в модель, построенную в терминах сетей Петри. Этот алгоритм позволит наглядно показать процесс перехода от функциональной модели, построенной с использованием SADT-моделирования, к выбору оптимального состава средств информационной безопасности, через функциональную модель, реализованную с использованием аппарата сетей Петри.

После построения функциональной модели в терминах аппарата сетей Петри реализуется моделирование подсистемы обеспечения информационной безопасности объекта также с использованием сетей Петри (рис. 1).

Согласно правилам построения модели методом SADT-моделирования, каждая сторона функционального блока имеет свое значение. Так, на левую сторону направляется интерфейсные дуги со значением «вход», из правой стороны выходят интерфейсные дуги с «выходным» значением. Сверху дуга имеет значение «управление», а снизу дуга со значением «механизм» [1].

Что касается моделирования сетями Петри, то существует несколько формальных определений сети Петри, отличающихся способами задания элементов и связей в сети [2, 3]. Дадим формальное определение сетей Петри, которое дает В.Е. Котов в своей монографии [4].

Под сетью будем понимать тройку  $(P, T, F)$ , где  $P$  — непустое множество элементов сети, называемых местами;

$T$  — непустое множество элементов сети, называемых переходами;

$F$  — функция инцидентности, задающая связи между элементами множеств  $P$  и  $T$ ;

$M_0$  — функция начальной разметки сети.

Таким образом, сеть можно описать выражением (1):

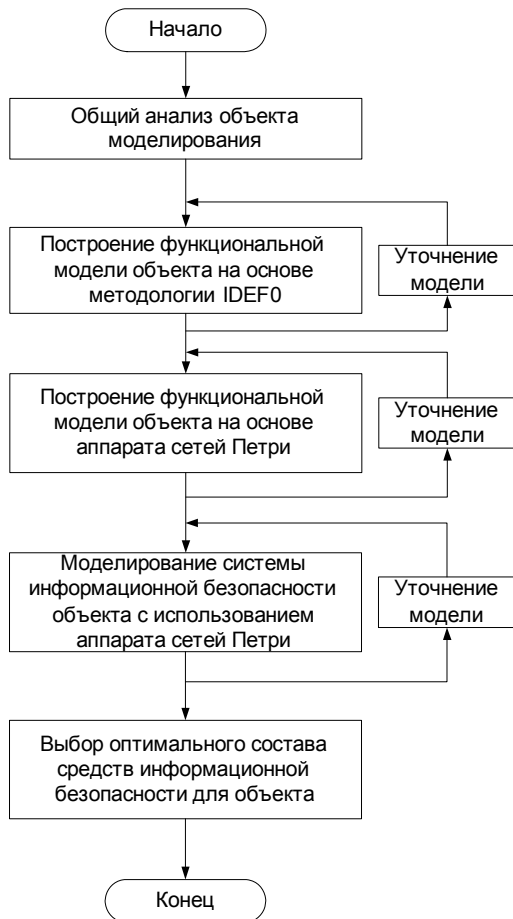


Рис. 1 – Алгоритм преобразования модели, описанной SADT-методологией, в модель, представленную в терминах аппарата сетей Петри

$$P_N = (P, T, F, M_0). \quad (1)$$

Согласно теории построения моделей с использованием аппарата сетей Петри, переход  $t$  сработает, если будут выполнены все предусловия для срабатывания перехода. После срабатывания перехода появляются постусловия (2).

$$M' = M - {}^*F(t) + F^*(t), \quad (2)$$

где  $M$  – начальная разметка или предусловия;

$M'$  – разметка после срабатывания перехода  $t$  или постусловия;

${}^*F(t)$  – функция инцидентности до срабатывания перехода  $t$ ;

$F^*(t)$  – функция инцидентности после срабатывания перехода  $t$ .

Опишем методику перехода от модели, реализованной на методологии SADT-моделирования, к модели описанной методологией сетей Петри.

В моделировании посредством SADT функциональный блок выполнит свое назначение, если будет предоставлена вся заявленная информация для этого блока, т.е. входная информация, управление, механизмы. После выполнения завершения работы функционального блока появляется выходная информация. Прimitives в SADT-моделировании часто называют ICOM-кодом (Input, Control, Output, Mechanism).

Таким образом, после анализа функционирования вышеописанных способов моделирования, получаем преобразования SADT-модели в сети Петри (табл. 1).

1. Таблица преобразований примитивов SADT-моделирования в сеть Петри

ICOM, SADT	Сеть Петри
Вход, Управление, Механизм	Предусловия (состояния)
Функциональный блок	Переход
Выход	Постусловия (состояния)

В качестве примера приведем преобразование модели, описывающий подпись документа, реализованной посредством SADT-моделирования, в модель реализованную на основе методологии сетей Петри (рис. 2).

Для полученной сети Петри входная функция (начальная разметка)  $I(t1)$   $\{p1, p2, p3, p4, p5\}$ , а выходная функция (конечная разметка)  $O(t1)$   $\{p6\}$ . Множество мест  $p1...p5$  идентичны

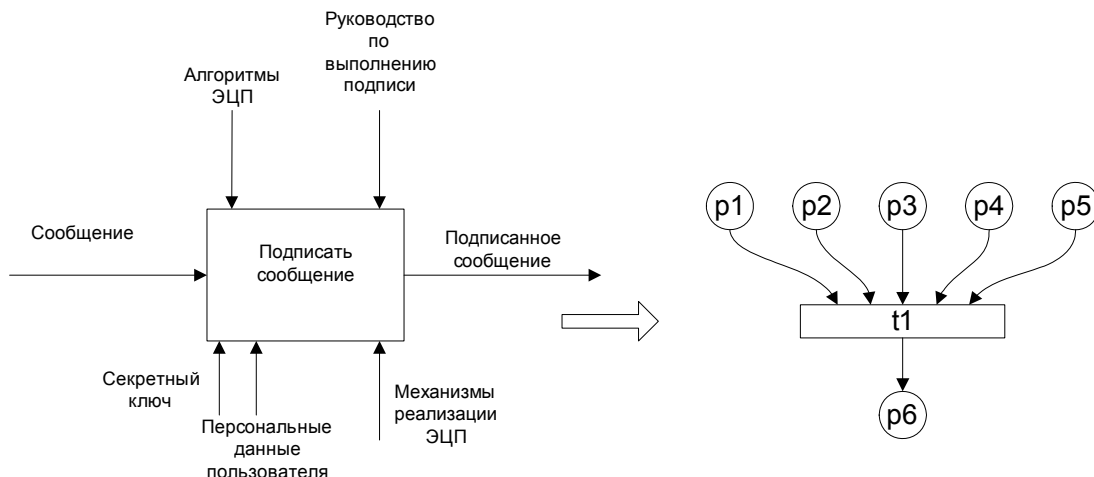


Рис. 2 – Преобразование с SADT-моделирования в сеть Петри

следующим значениям дуг SADT-модели: сообщение, алгоритмы ЭЦП, руководство по выполнению подписи, секретный ключ, персональные данные пользователя, механизмы реализации ЭЦП. Переход  $t_1$  охарактеризует значение функционального блока «подписать сообщение», а место  $p_6$  — представляет подписанное сообщение в SADT-модели. Таким образом, чтобы подписать сообщение, необходимы предусловия (табл. 2).

## 2. Соответствие примитивов SADT-модели примитивам сети Петри в рассматриваемом примере

SADT-модель	Сеть Петри
Сообщение, Алгоритмы ЭЦП, Рук. по вып. подписи, Секретный ключ, Персональные данные пользователя, Механизмы реализации ЭЦП	Предусловия ( $p_1, p_2, p_3, p_4, p_5$ )
Подписать сообщение	Переход ( $t_1$ )
Подписанное сообщение	Постусловия ( $p_6$ )

Следует отметить, что при преобразовании из SADT-модели в сеть Петри, не всегда удается точно найти соответствие коду ICOM и функциональному блоку в SADT-модели соответствующие переходы и состояния в сети Петри. Неко-

торые функциональные блоки и ICOM-коды удается описать с использованием нескольких состояний и переходов. Эта проблема приводит к повышению сложности понимания преобразованной модели.

Оценка параметров системы информационной безопасности в условиях неопределенности ее функционирования должна вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся в процессе уточнения исходных данных.

Представленная методика моделирования систем информационной безопасности на основе сетей Петри позволяет строить масштабируемые и расширяемые модели, которые впоследствии можно анализировать известными методами.

## Литература

1. Девид, Л. Методология структурного анализа и проектирования / Л. Девид, К. Мак Гоуэн, М. Мак Гоуэн. М.: Мета Технология, 1993.
2. Дж. Питерсон. Теория сетей Петри и моделирование систем. М.: Мир, 1984.
3. V. Alturi, W.K. Huang. A Petri net based safety analysis of workflow authorization model. J. of computer security. 2000.
4. Котов, В.Е. Сети Петри. М.: Наука. Главная редакция физико-математической литературы, 1984.

# Управленческие технологии как инструмент реализации стратегии развития организации

**А.Х. Курманова**, к.э.н., доцент, Оренбургский ГУ

В современных условиях эффективная деятельность организации в долгосрочной перспективе возможна только с использованием новых управленческих технологий. Современные управленческие технологии призваны обеспечить построение ключевых элементов управления таким образом, чтобы повысить эффективность и результативность достижения целей организации [1–3].

Основными управленческими технологиями в стратегии являются технологии разработки стратегии и сбалансированной системы показателей. Главный фактор, влияющий на качество разработки стратегии, — это наличие в организации достоверной информации о внешней и внутренней среде, в том числе о рынках, конкурентах, технологиях и т.д. Анализ внешней среды представляет собой процесс, посредством которого разработчики стратегического плана оценивают внешние по отношению к организации факторы с целью определения возможностей и угроз для нее. Анализ внешней среды дает организации время для прогнозирования возможностей, время

для разработки стратегий, которые могут превратить прежние угрозы в любые выгодные возможности. При помощи анализа внешней среды организация может составить перечень опасностей и возможностей, с которыми она сталкивается в этой среде. Перечень включает как взвешивание факторов (для измерения значимости каждого фактора для данной организации), так и оценку воздействия фактора на организацию.

Угрозы и возможности, с которыми сталкивается организация, обычно можно выделить в семь областей. Этими областями являются экономика, политика, рынок, технология, конкуренция, международное положение и социальное поведение. Одним из инструментов (методов) анализа внешней среды является СТЭП-анализ, позволяющий изучить влияние четырех факторов: социальных (С), технологических (Т), экономических (Э), политических (П).

После анализа перечня внешних опасностей и возможностей руководству необходимо оценить сильные и слабые стороны организации, а также возможности и угрозы, которые могут ждать ее в будущем. Для успешного планирования руковод-