

# ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ДАННЫХ И УПРАВЛЕНИЯ

Р.С. ЯКУШЕВ, *асп. каф. систем автоматического управления МГУЛ*

*rsyakushev@gmail.com*

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает.

Трудности решения практических задач обеспечения безопасности в автоматизированных системах связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ

обеспечения защиты информации в современных условиях.

Прежде всего необходимо понять, что такое безопасность информационных технологий (информации), определить, что (кто) от чего (кого), почему (зачем) и как (в какой степени и какими средствами) необходимо защищать [1].

В общих понятиях безопасность есть защищенность от возможного ущерба, наносимого при реализации опасности (угрозы).

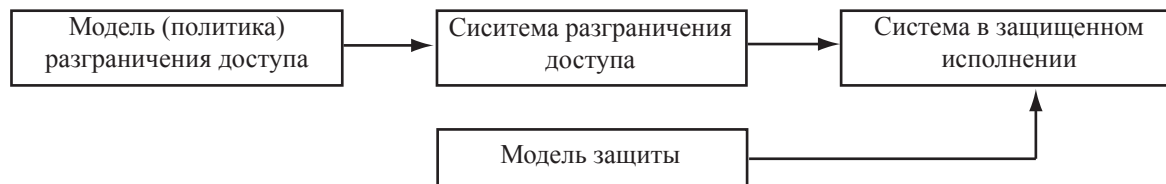


Рис. 1

Sub	MP	Obj	DB	Shared Files	Config Files	Devices
User group	1	MP	2	1	3	2
User	2					
Administrator	3					

Рис. 2

Sub \ Obj	MP	Shared Files	Config Files	Devices
User group	R	R/W	—	R
User	R/W	R	—	R/W
Administrator	R/W/D	R/D	R/W/D	R/W/D

Рис. 3

Для защиты информации от несанкционированного доступа создается модель защиты – абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств или организационных мер защиты от несанкционированного доступа.

Для управления доступом пользователей (субъектов доступа) к информации (объектам доступа) создается система разграничения доступа – совокупность различных правил разграничения доступа.

Система разграничения доступа отражает выбранную модель (политику) разграничения доступа. Последовательность построения системы в защищенном исполнении представлена на рис. 1.

Существует две основные политики безопасности: мандатная и дискреционная.

**Мандатной политикой безопасности** (модель Белла-Ла Падулла) считается любая политика, логика и присвоение атрибутов безопасности которой контролируются

системным администратором безопасности [2]. Пример реализации мандатной политики представлен на рис. 2.

**Дискреционная политика безопасности** (модель Харрисона-Руззо-Ульмана) считается любая политика, в которой пользователи могут принимать участие в определении функций политики и/или присвоении атрибутов безопасности [2]. Пример реализации мандатной политики представлен на рис. 3.

У каждой модели есть ряд преимуществ, кроме того, в некоторых операционных системах эти модели реализованы совместно и дополняют друг друга, однако есть общий недостаток, присущий всем моделям безопасности – до сих пор не существует методического аппарата, позволяющего анализировать результаты реализации выбранной модели безопасности. Это значительно затрудняет работу специалиста, занимающегося проектированием систем в защищенном исполнении.

Однако существует теория, позволяющая решить данную проблему. Такой теорией

является **теория сетей Петри**, моделирование в которой осуществляется на событийном уровне, при этом определяется, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия.

Развитие теории сетей Петри проводилось по двум направлениям. Формальная теория сетей Петри занимается разработкой основных средств, методов и понятий, необходимых для применения таких сетей. Прикладная теория сетей Петри связана главным образом с применением сетей Петри к моделированию систем, их анализу и получающимся в результате этого глубоким проникновением в моделируемые системы [3, 4].

Применение данной теории к моделированию системы в защищенном исполнении позволит определить эффективность и выявить слабые стороны реализации выбранной политики разграничения доступа субъектов системы к информационным ресурсам.

### Основные положения теории сетей Петри

Сеть Петри состоит из четырех элементов: множество *позиций*  $P$  (схематически обозначаются кружками), множество *переходов*  $T$  (обозначаются черточками), входная функция  $I$  и выходная функция  $O$ . Входная и выходная функция связаны с переходами и позициями. Входная функция  $I$  отображает переход  $t_j$  в множество позиций  $I(t_j)$ , называемых входными позициями перехода. Выходная функция  $O$  отображает переход  $t_j$  в множество позиций  $O(t_j)$ , называемых выходными позициями перехода [5]. Структура сети Петри определяется ее позициями, переходами, входной и выходной функциями, т.е. сеть Петри  $S$  задается четверкой вида

$$S = \langle P, T, I, O \rangle.$$

Представленная таким образом сеть Петри  $S$  может использоваться только для отражения статики моделируемой системы (взаимосвязи событий и условий), но не позволяет отразить в модели динамику функционирования моделируемой системы. Для представления динамических свойств объекта вводится функция маркировки (разметки)  $M: P \rightarrow \{0, 1, 2, \dots\}$ . Маркировка  $M$  есть присвое-

ние неких абстрактных объектов, называемых метками (фишками), позициям сети Петри, причем количество меток, соответствующее каждой позиции, может меняться [6].

Маркированная (размеченная) сеть Петри может быть описана в виде  $S_M = \langle P, T, I, O, M \rangle$  и является совокупностью сети Петри  $S$  и маркировки  $M$  [5].

Фишки используются для определения выполнения сети Петри. Фишки находятся в кружках (позициях) и управляют выполнением переходов сети. Функционирование сети Петри отражается путем перехода от разметки к разметке. Начальная разметка обозначается как  $M_0$ . Сеть Петри выполняется путем срабатывания (запуска) переходов. Выполнением сети Петри управляют количество и распределение фишек в сети. Переход запускается удалением меток из его входных позиций и образованием новых меток, помещаемых в выходные позиции. Переход может запускаться только в том случае, когда он разрешен. Переход называется *разрешенным*, если каждая из его входных позиций имеет число меток, по крайней мере равное числу дуг из позиции в переход [6].

### Применение теории сетей Петри для создания модели защиты информации в автоматизированных системах

В качестве примера применения теории сетей Петри для моделирования систем в защищенном исполнении рассмотрим процесс доступа субъекта к объекту системы. Структура сети Петри, моделирующей данный процесс, представлена на рис. 4.

В этой схеме (рис. 4) могут быть следующие состояния:

$p_1$  – поступил запрос субъекта на доступ к объекту;

$p_2$  – обработка запроса;

$p_3$  – доступ к объекту разрешен;

$p_4$  – метка доступа к объекту;

и могут происходить следующие события:

$t_1$  – поступление запроса субъекта на доступ к объекту;

$t_2$  – начало обработки запроса;

$t_3$  – конец обработки запроса;

$t_4$  – предоставление доступа субъекта к объекту.

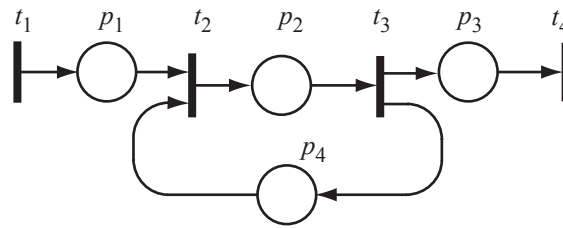


Рис. 4.

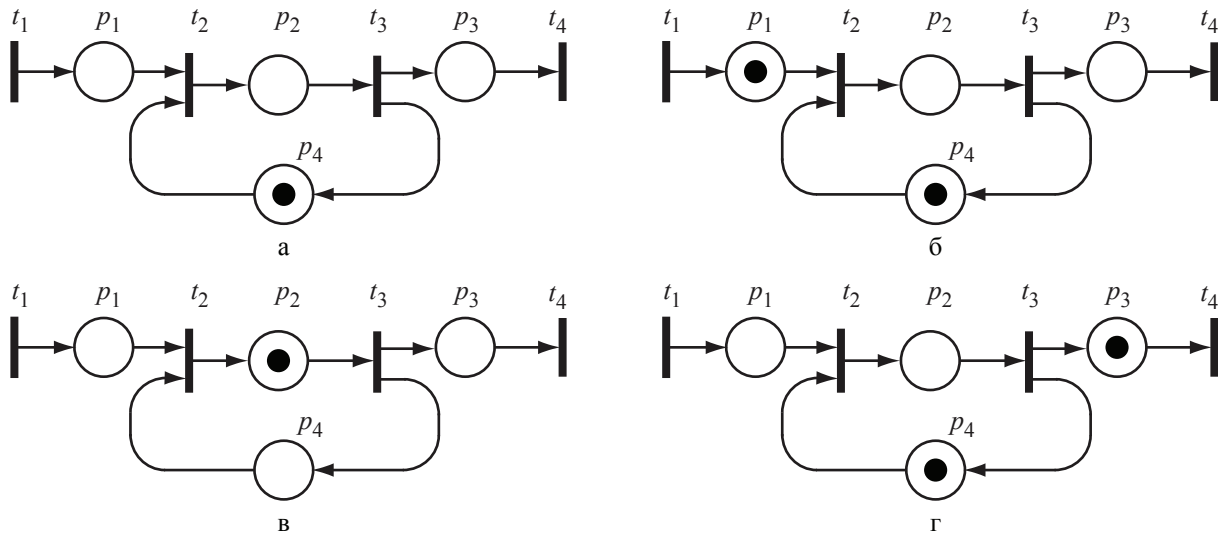


Рис. 5

Предположим, что начальная разметка сети, моделирующей процесс доступа субъекта к объекту, остается нулевой:  $M_0 = (0,0,0,0)$ . Тогда при поступлении запроса ( $p_1 = 1$ ) на доступ к объекту предоставлен не будет, т.к. в схеме не будет переходов, которые могут сработать. Однако, если начальная маркировка будет  $M_0 = (0,0,0,1)$  (рис. 5 а), переход  $t_2$  при поступлении запроса ( $p_1 = 1$ ) (рис. 5 б) станет разрешенным, и в конечном итоге доступ к объекту будет разрешен (рис 5 в, г).

Таким образом, применение сетей Петри для создания модели защиты информации в автоматизированных системах обработки данных и управления, позволяет анализировать результаты, выявлять ошибки реализации выбранной модели безопасности и определять эффективность защиты.

### Библиографический список

1. Безопасность информационных технологий. Руководство слушателя курса. – М.: Учебный центр «Информзащита», 2002. – 208 с.
2. Кулябов, Д.С. Необходимость обеспечения безопасности операционных систем на системном уровне / Д.С. Кулябов, А.В. Королькова // Вестник РУДН. – 2004. – Т. 3. – № 1. – С. 144–161.
3. Калянов, Г.Н. Консалтинг при автоматизации предприятий: подходы, методы, средства. [Электронный ресурс]: учебное пособие. – Режим доступа: <http://www.interface.ru>, свободный.
4. Ломазова, И.А. Вложенные сети Петри и моделирование распределенных систем / И.А. Ломазова // Программные системы: теория и приложения. – 2004. – С. 337–352.
5. Питерсон, Дж. Теория сетей Петри и моделирование систем: пер. с англ. / Дж. Питерсон. – М.: Мир, 1984. – 264 с.
6. Советов, Б.Я. Моделирование систем: учеб. для вузов – 5-е изд., стер. / Б.Я. Советов, С.А. Яковлев. – М.: Высшая Школа, 2007. – 343 с.