УДК 519

АЛГОРИТМИЧЕСКИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ

А.В. Кабулов[1], А.А. Варисов[2]
[1] доктор технических наук, профессор, заведующий кафедры,
[2] научный исследователь кафедры информационной безопасности
[1] Национальный Университет Узбекистана (Ташкент),
[2] Ташкентский университет информационных технологий, Узбекистан

Аннотация. *В данной статье рассматривается новый способ обеспечения системы комплексной защиты информации в алгоритмической модели информационной безопасности на основе таблицы функционирования.*

Ключевые слова: *таблицы функционирования, сеть Петри, модель, алгоритмическая модель, безопасность, система, угрозы.*

Безопасность – это отсутствие опасности или наличие возможности надежно защититься от нее. Опасным следует считать такое информационное воздействие, которое чревато дестабилизирующим, деструктивным, ущемляющим интересы личности или страны и т.д. результатом.

Информационная безопасность общества, государства – это состояние либо отсутствия информационных угроз, либо, при наличии таковых, состояние защищенности и, следовательно, устойчивости основных сфер жизнедеятельности (политики, экономики, науки, техносферы, сферы государственного управления, культуры, военного дела, общественного сознания и т.д.) по отношению к опасным информационным воздействиям, причем как внедрению, так и извлечению информации.

Системный подход к информационной безопасности (ИБ) требует выделять ее субъекты, средства и объекты, принципы обеспечения, источники опасности, направленность опасных информационных потоков.

Эволюция информационных технологий (ИТ) связана с интеллектуальными системами, в которых присутствуют процессы зарождения, адаптации и развития. Системный подход определяет методологию и принципы построения систем ИТ. Принцип моделируемости позволяет предотвратить ошибки проектирования кибернетических систем. Принцип связности при разработке эффективной системы рассматривает объект защиты комплексно, объединяя объект защиты, внешнюю среду, средства защиты и угрозы злоумышленника и учитывая взаимосвязи: источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).

Построение системы защиты является обязательным условием для обеспечения безопасности конфиденциальной информации, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы является построение динамических таблиц функционирования (ТФ) информационной системы на базе сетей Петри [2]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Развитие информационных систем обработки и хранения конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование информационной системы (ИС), в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности конфиденциальной информации (КИ), а также составляются требования к СЗКИ.

Требования к СЗКИ, в зависимости от вида КИ, определяются согласно нормативно-законодательной базе Республики Узбекистан.

Алгоритмические модели на основе ТФ [2] используются как математический аппарат для моделирования динамических дискретных систем.

Моделирование в ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнение событийной модели в ТФ описывает поведение системы. Анализ результатов выполнения может сказать о том, в каких состояниях пребывала или не пребывала система, какие состояния в принципе не достижимы. Таким образом, ТФ={X, Y, A, O, Θ, T, U, S, F, P} – алгоритмическая модель АСУ обеспечения безопасности ИС, а также предотвращения любого вида угроз к ИС и информационным ресурсам (ИР), где

Y – множество возможных угроз Y $\{O_j\}$;

X – множество решений предотвращения угроз X $\{A_i\}$;

A – определенное решение предотвращения угроз;

O – определенное действие угроз;

Θ – координаты между «A_i» и «O_j»;

T – время (для предотвращения и успешной реализации угрозы);

U – внешняя воздействие (на $\Theta_{ij}\{A_i,O_j\}$);

S – множество переходов (переход с одного Θ_{ij} на другую $\Theta_{i+n,\ j+m}$);

F(t) –функция изменения таблицы функционирования во времени;

P – множество вычислительных и логических операций ввода, вывода и управления;

Z – множество привилегий.

Если $\forall t_i \in T$ и функция, $F(t_i) = const$ то такая таблица функционирования называется статической (стационарной). Функция F(t), задающая изменения таблицы функционирования, называется функцией управления агрегатной системой или функцией планирования процессов в системе.

В каждый интервал времени t_i описание ТФ представляется в виде маркированной сети Петри:

$$M = \{P, D, I, O, \mu\}$$

где *P, D, I, O* – соответственно, множества позиций (состояний), операций (переходов), входных и выходных состояний; μ – функция, отображающая множество позиций в множестве натуральных чисел *N*:

$$\mu: P \to N$$

Каждая маркировка μ может быть представлена как вектор $\mu = (\mu_1 \dots \mu_n)$ здесь $n = |P| u \forall \mu_i \in N, i = \overline{1,n}$ Вектор μ определяет для каждой позиции p_i сети количество фишек, т.е. для $\mu_i, p_i, i = \overline{1,n}$ выполняется $\mu(pi) = \mu_i$.

Интервалы времени, t_i в течение которых сеть Петри не изменяется, будем называть технологическими циклами (ТЦ).

Таким образом, за неделимый элемент динамических дискретных систем принято рабочее место (РМ), соответствующее определенному решению предотвращения угроз. Обозначим его через α_i, а множество РМ – через А. Каждое α_i может быть представлено в виде работников, работника плюс машины или машины. Каждое α_i имеет входы **x** и выходы ***y***, внутреннее состояние. На *Z* входы передаются сигналы (информация) или материалы в виде продуктов, веществ (жидких или газообразных) и т.д. Некоторые входные воздействия сигналов могут быть управляющими (g). В качестве машин применяются станки и вычислительные машины. Машины выступают в качестве орудия труда, а информация, материалы – в качестве предметов труда.

Рабочее место α_i соответствует агрегату Н.П. Бусленко [1]. Каждому α_i приписывается определенное количество операций *d*. Множество операций обозначим через *D*. Кроме того, они функционируют во времени и имеют пространственные координаты. Множество α соединяется между собой дугами и образует коммуникационную сеть с потоками (имеются в виду потоки информации, веществ, а также транспортные, людские потоки и т.д.).

Так, система представляется в виде коммуникационной сети, вершины которой изображают РМ, способные выполнять определенное количество операций (решение задач, переработка материалов и т.д.), а дуги соответствуют потокам между этими местами. Такую сеть назовем R-сетью.

В процессе функционирования системы структура сети со временем может меняться: старые дуги и вершины аннулируются, а новые добавляются. Такие сети назовем ситуационными или RC-сетями. При решении определенного класса задач в течение времени (t_1, t_2) на каждом α выполняется одна из приписанных ему операций. Поэтому построение самой сети и определение приписанной операции является основной задачей системных исследований. В определенный промежуток времени сеть можно изобразить в виде ориентированного графа неизменной структуры (рис. 1.1).

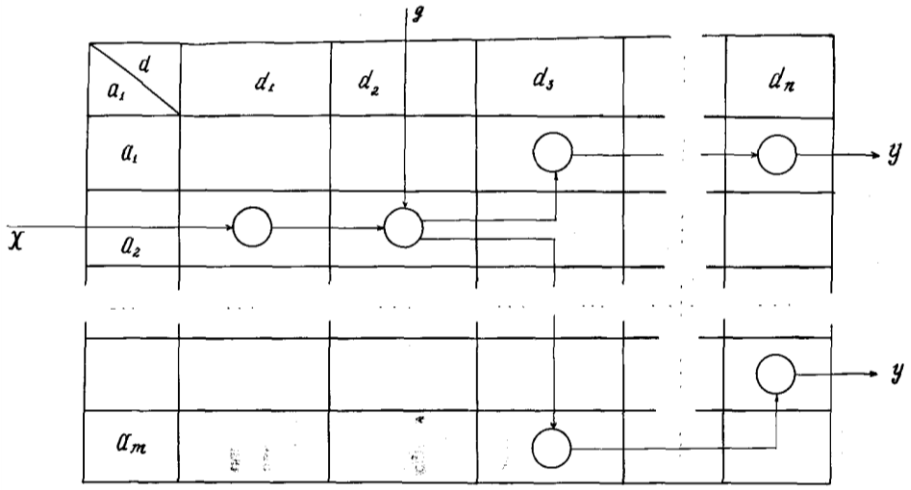
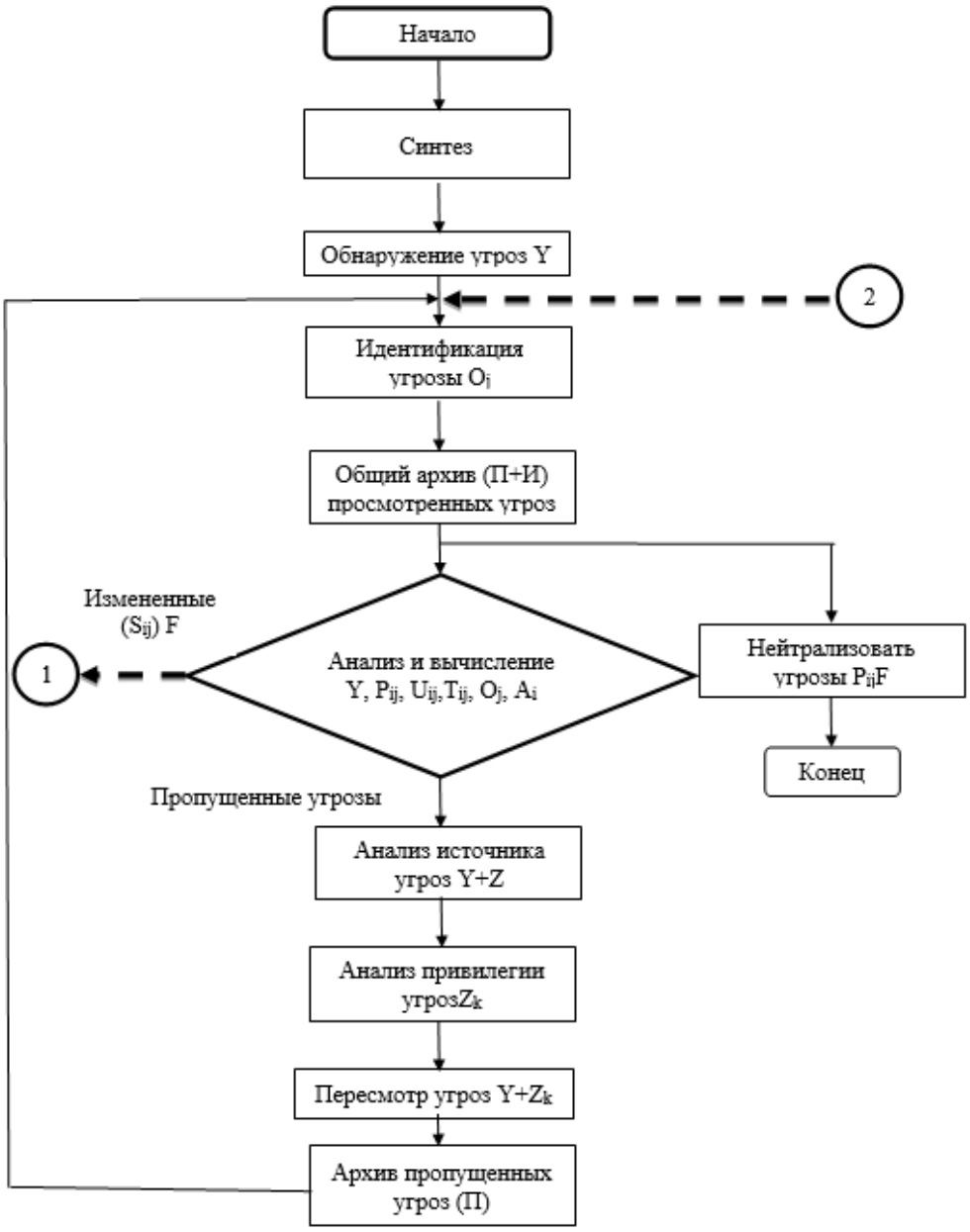


Рис. 1.1. ТФ гипотетического объекта управления

Такое представление соответствует определению таблицы функционирования, и *R–,RC* сети представляются в виде ТФ. На этой сети можно фиксировать параметры потока и режим работы сети во времени.

Воспользуясь системами действий сетей Петри, мы создадим блок схему СКЗИ (рис. 1.2) и гибридного варианта сетей Петри в обеспечении ИБ.

В блок схеме основным шагом является обнаружение угроз «Y», после идентификации угрозы «O_j» она проверяется общем архиве (П+И) просмотренных угроз. Если угрозы такого вида были рассмотрены ранее, они сразу нормализируются соответственными действиями «$P_{ij}F$». Если угроза рассматривается первые, тогда она анализируется и вычисляется «Y, P_{ij}, U_{ij},T_{ij}, O_j, A_i». После анализа источника Y+Z и анализ привилегии Z_k угрозы не обнаружатся, тогда она пересматриваются Y+ Z_k. После этого добавляются в архив пропущенных угроз (П). Если при анализе и вычислении угроза обнаружатся, то тогда действия будет идти по блок схеме №1, Продолжение. Здесь после всех шагов угроза добавляются в архив для быстрого обнаружения и идентификации угроз.



Блок схема № 1

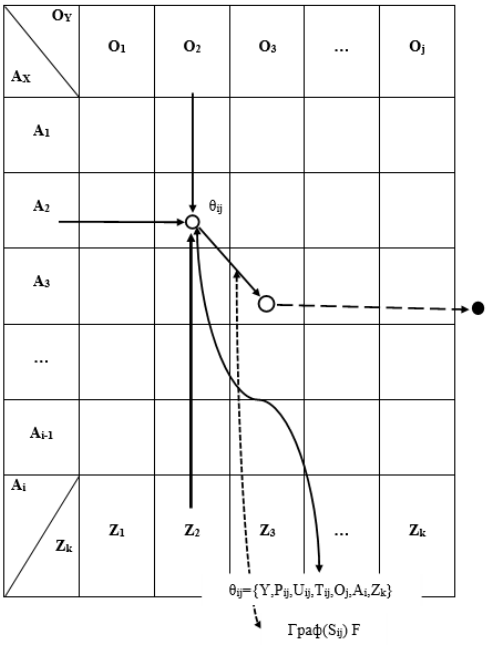
Блок схема № 1 (Продолжение)

Рис. 1.2. Блок схема СКЗИ

В таблице 1 представлены множество угроз «O_Y», а также множество действий «A_i» для предотвращения угроз. Для функционирования данной ТФ необходимо, чтобы в каждой ячейке было предоставлено минимум 3 входа: сама угроза; способы предотвращения данной угрозы; привилегия пользователя в данной ситуации (например – системный, администратор и пользователи разных уровней).

После обработки действия в ячейке (A_2 O_2) по формуле $\theta_{ij}=\{Y,P_{ij},U_{ij},T_{ij},O_j,A_i,Z_k\}$ состояние угрозы меняется исходя из своей сущности и скрипта кода, после этого она переходит в другую ячейку. В нашем случае в (A_3 O_3). Переход осуществляется по формуле (S_{ij}) F.

Таблица 1



После всей обработки угроза выводятся из таблицы, т.е. уничтожается и добавляется в архив. При этом нужно учитывать то, что блок схема №1 является гибкой и всегда может изменятся при обработке данных и бесконечно будет совершенствоваться. Это отразится и на ТФ, которая будет постоянно дополнятся новыми критериями. Эти же действия в сетях Петри представлены в таблице 1.

СПИСОК ЛИТЕРАТУРЫ

1. Бусленко, Н.П. Моделирование сложных систем / Н.П. Бусленко. – М.: Наука, 1978. – с. 390.
2. Кабулов, В.К. Вопросы формализации в исследовании систем / В.К. Кабулов // Вопросы кибернетики, вып.126. – Ташкент: НПО "Кибернетика" АН УзССР, 1984. – С. 3-15.

Материал поступил в редакцию 02.05.17.

ALGORITHMIC MODELS OF INFORMATION SECURITY BASED ON FUNCTION TABLES

A.V. Kabulov[1] A.A. Varisov[2]

[1] Doctor of Technical Sciences, Professor, Head of Department,
[2] Scientific Researcher of the Information Security Department
[1] National University of Uzbekistan (Tashkent),
[2] Tashkent University of Information Technology, Uzbekistan

Abstract. *In this article the new way of providing complex information security system in algorithmic model of information security on the basis of the functioning table is considered.*

Keywords: *functioning tables, Petri net, model, algorithmic model, security, system, threats.*