УДК: 519.711(075)

РАЗРАБОТКА АЛГОРИТМИЧЕСКОЙ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ДИНАМИЧЕСКИХ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ

КАБУЛОВ АНВАР ВАСИЛОВИЧ
профессор Национального университета Узбекистана им. Мирзо Улугбека.
ВАРИСОВ АКМАЛ АББАСОВИЧ
соискатель Ташкентского университета информационных технологий им. Ал Хорезми

Аннотация: Предлагается способ анализа защищенности системы на основе построения динамических таблиц функционирования(ТФ) информационной системы на базе сетей Петри. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки. Алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем.
Моделирование на основе ТФ осуществляется на событийном уровне.
Ключевые слова: Информационная безопасность, сеть Петри, система защиты конфиденциальных информации, таблица функционирования, алгоритм, множество.

DEVELOPMENT OF ALGORITHMIC MODEL OF INFORMATION PROTECTION ON THE BASIS OF DYNAMIC TABLES OF FUNCTIONING

Kabulov Anvar Vasilovich,
Varisov Akmal Abbasovich

Abstract: A method for analyzing the security of a system based on the construction of dynamic tables of the functioning (TF) of an information system based on Petri nets is proposed. Using the algorithmic model based on TF, a survey of the functioning of the implemented protection system is conducted, and its shortcomings are revealed. Algorithmic models based on TF are used as a mathematical apparatus for modeling dynamic discrete systems.
Modeling on the basis of TF is carried out at the event level.
Key words: Information security, Petri net, system of protection of confidential information, table of functioning, algorithm, set.

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, устойчиво-

сти 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 [1, 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 базы Республики Узбекистан.

Алгоритмические модели на основе ТФ[1] используются как математический аппарат для моделирования динамических дискретных систем

Моделирование на основе ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнения 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 – внешнее воздействие (на $\Theta_{ij}\{A_i:O_j\}$);

S – множество переходов (переход из одной 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 стати-

ческой (стационарной). Функция F(t) , задающая изменения таблицы функционирования, называется функцией управления агрегатной системой или функцией планирования процессов в системе.

В каждый интервал времени 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 $\mu = (\mu_1, ... \mu_n),$ $n = |P| u \forall \mu_i \in N, i = \overline{1, n}.$ здесь 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, 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 α_i 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 z состояние На 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 приписывается определенное количество операций *d*. Множество операций α_i обозначим через D. Кроме того, они функционируют во времени и имеют пространственные координаты. Множество соединяется между собой дугами и образует коммуникационную сеть с потоками α (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 тд), 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). 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.

Воспользуюсь системами действий сетей Петри мы создадим блок схему СКЗИ (рис.2) и гибридного варианта сетей Петри в обеспечении ИБ. В блок схеме основным шагам является обнаружение угроз «Y», после идентификации угрозы «O_j» она проверяется общим архивом(П+И) просмотренных угроз. Если угрозы такова вида были рассмотрены ранее она сразу нормализируется 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.

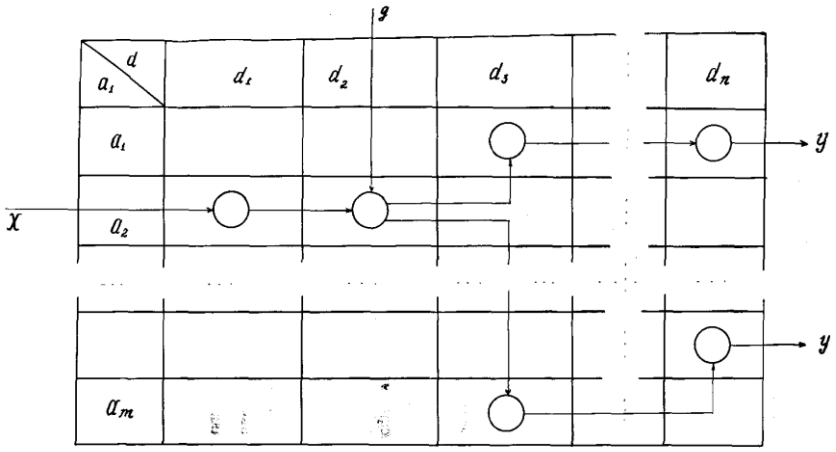
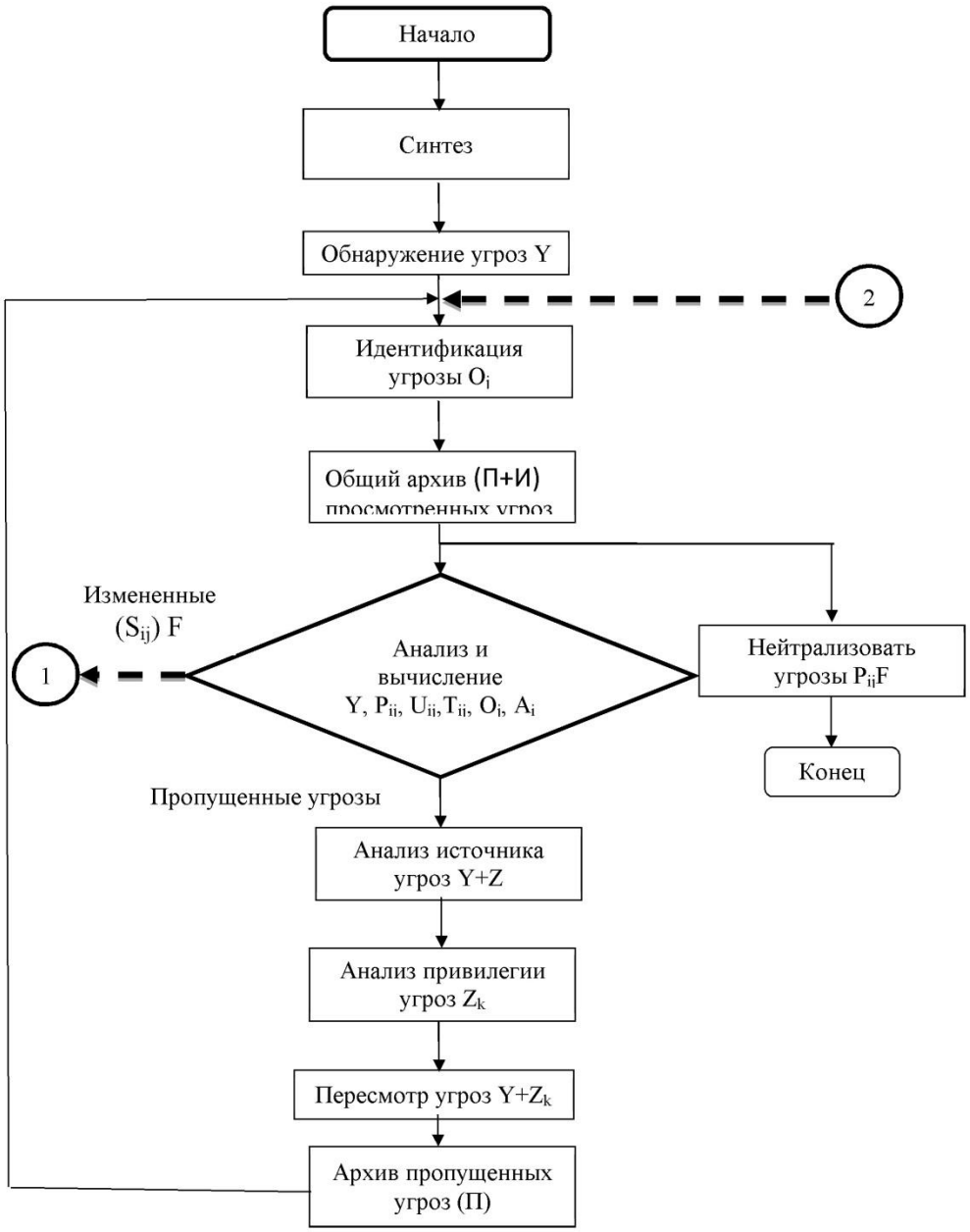


Рис. 1. ТФ гипотетического объекта управления Y {O_j}



Блок схема №1(Продолжение)

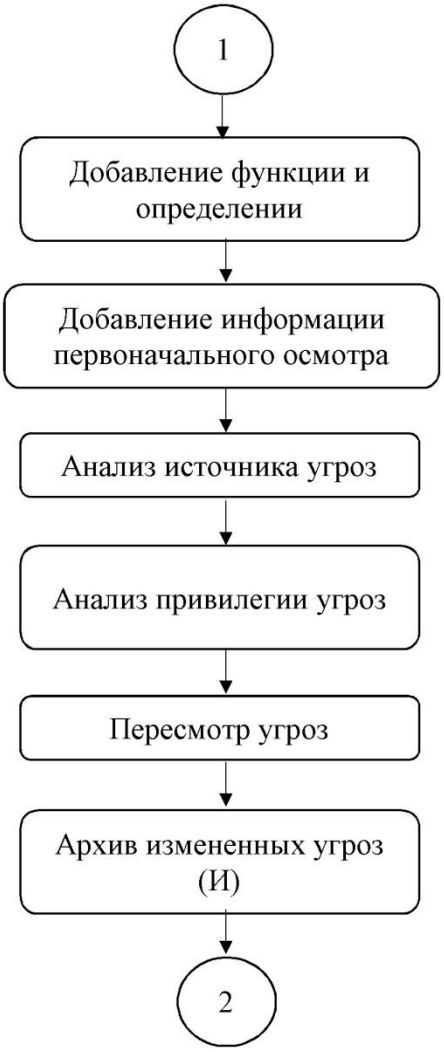


Рис. 2. Схема построения алгоритмической модели СКЗИ на основе ТФ

На рис.3 в таблице функционировании представлены множество угроз «O_Y», а также множество действий «A_i» для предотвращения угроз. Для функционирования данной ТФ необходимо 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 θ_{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 управление передаётся в другую ячейку. В нашем случае в (A_3 O_3). Переход осуществляется по формуле (S_{ij}) F.

После всей обработки угроза выводится из таблицы, т.е. уничтожается или добавляется в архив. При этом нужно учитывать то, что блок схема №1 является гибким и всегда может изменятся при обработке данных и будет совершенствоваться. Это отразится и на ТФ, которая будет постоянно дополнятся новыми критериями. Эти действия в сетях Петри представлены в таблице на рис.3.

Анализируя выше сделанные выводы и полученную таблицу функционирования, можно сконструировать для определенной внешней угрозы на систему, а также действие предотвращения угрозы, пути вычисления, анализа и график работы в предлагаемой нами сети СКЗИ.

В первом случае рассмотрим угрозу AB исходящую из сети интернет и состоящую из двух отдельных частей A и B (A – полезная программа, утилит, драйвер, рисунок, обычный файл и т.д., B – скрытая за A фоновая угроза).

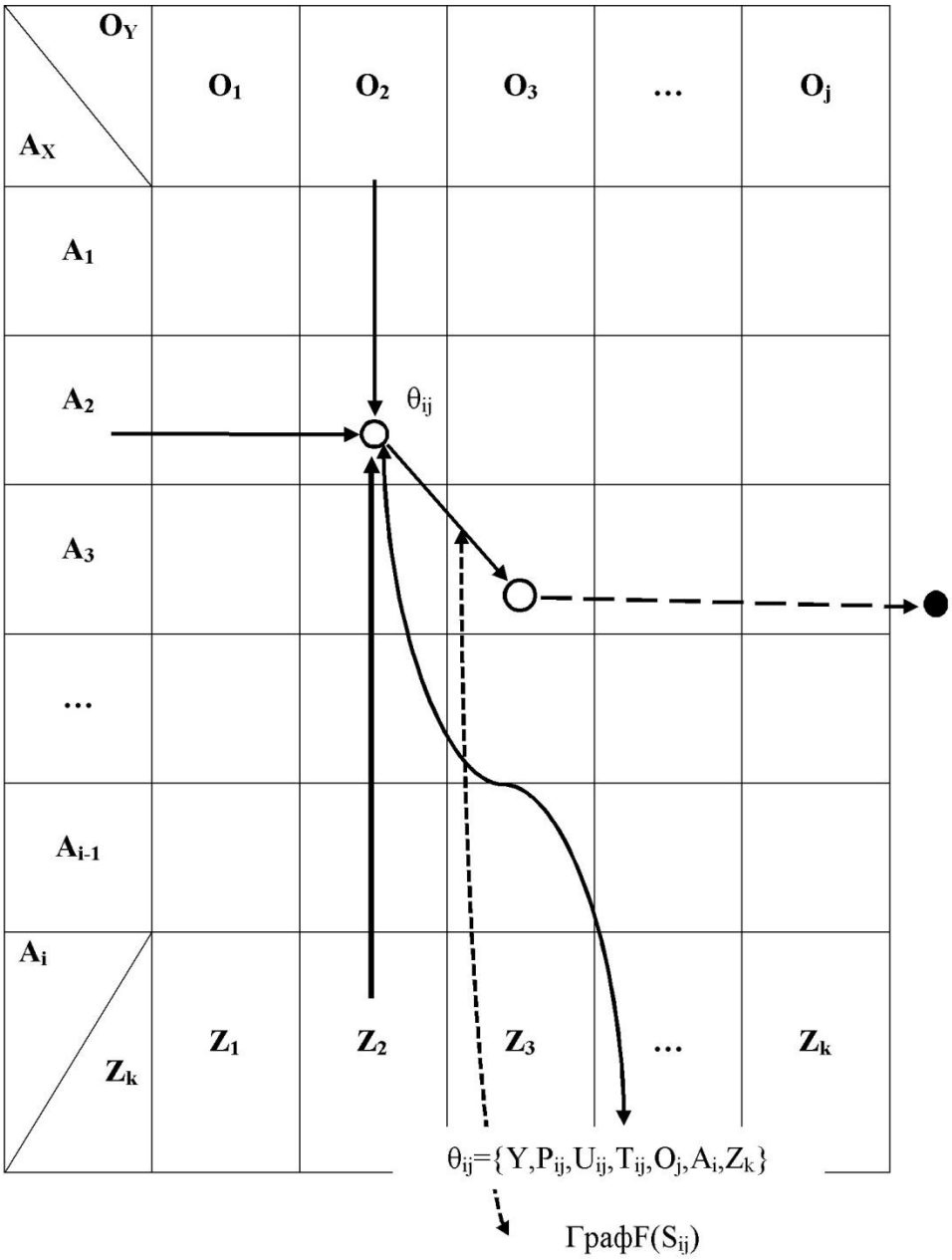


Рис.3. Таблица функционирование СКЗИ

В первом примере считается, что угроза ранее была рассмотрена и поэтому ее источник сразу блокируется и удаляется(рис.4). Угроза предотвращается, не причинив вреда системе.

В втором примере угроза рассматривается впервые, поэтому каждый ее возможный переход обозначается отдельно(рис.5). В таблицах примера 1 и примера 2 в строке OY расположены возможные угрозы на систему. В таблице примера 2 красным цветом обозначены пути угрозы, а зеленым - предотвращения этих угроз и наконец черным - переход действующих угроз на другую ячейку и их предотвращение.

На нижней строке представлены привилегии системы для уничтожения угроз.

На первом этапе пользователь получает ссылку для АВ в интернете. После нажатия ссылки и запуска АВ в сети ТФ ссылка разделяется на две части: А и В. Вторая часть сможет без разрешений администратора запускать вредоносные части своей программы, которые смогут загружать другие вредоносные программы без разрешения администратора.

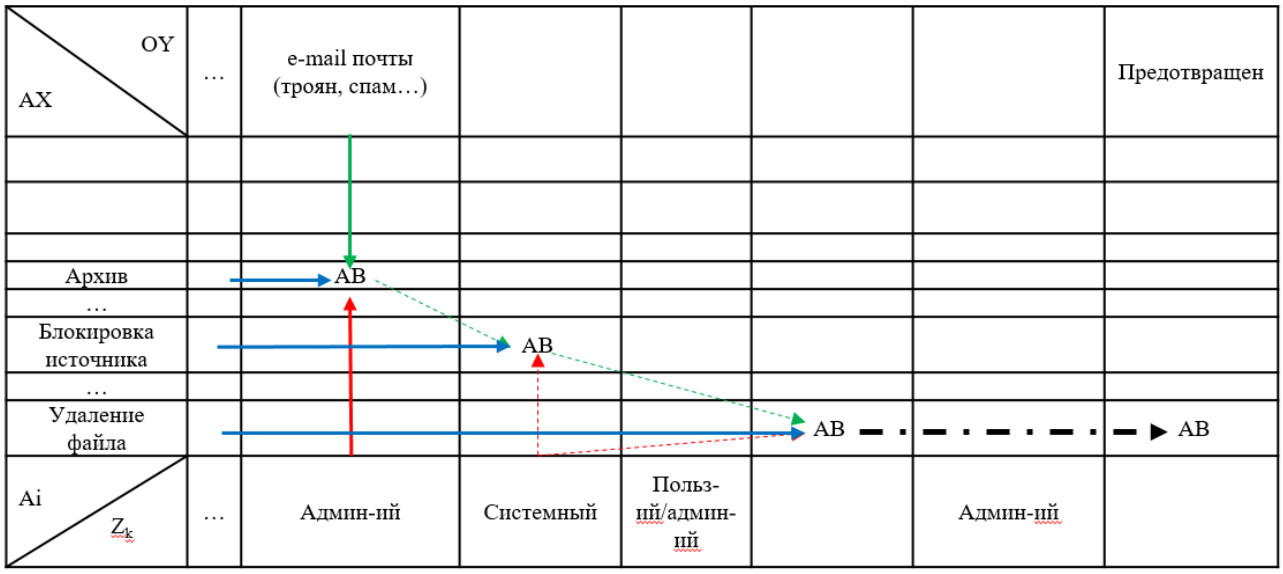


Рис.4. Пример 1 таблицы функционирования

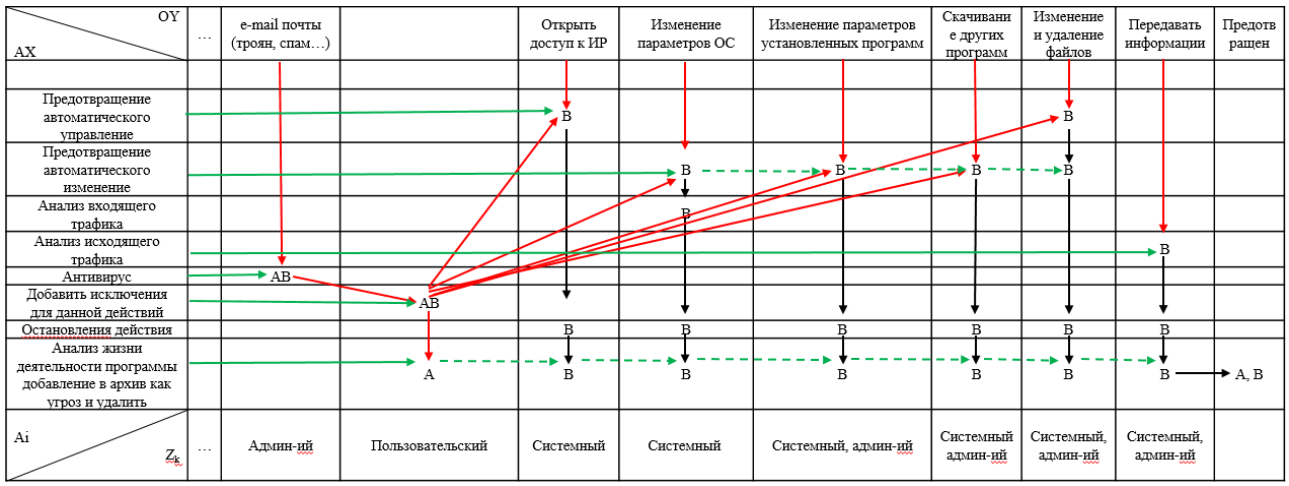


Рис.5. Пример 2 таблицы функционирования

Таким образом в работе предложена построение алгоритмической модели СКЗИ для исследования сложных информационных систем на основе таблиц функционирования. С точки зрения информационной безопасности алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем

Список литературы

1.Кабулов В.К. Вопросы формализации в исследовании систем.-Вопросы кибернетики, вып.126, Ташкент: НПО "Кибернетика" АН УзССР, 1984, с.3-15.

2.В.Г. Миронова, А.А. Шелупанов «Сети петри как инструмент анализа системы защиты конфиденциальной информации» Известия ЮФУ. Технические науки, 64-70 стр. Волгоград;

3.http://books.ifmo.ru/file/pdf/325.pdf;

4.http://www.volsu.ru/download.php?id=000023815-1.pdf