УДК 004.056.5

АЛГОРИТМ ОБНАРУЖЕНИЯ И ОБЕЗВРЕЖИВАНИЯ УГРОЗ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ
AN ALGORITHM FOR DETECTING AND NEUTRALIZING THREATS BASED ON THE FUNCTIONING TABLES

Норматов Иброхимали Холмаматович
Normatov Ibrohimali H.

Национальный университет Узбекистана имени Мирзо Улугбека, Узбекистан, Ташкент
National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan, Tashkent
Международная инженерная академия
International Academy of Engineering
(e-mail: ibragim_normatov@mail.ru)

Аннотация. В статье предлагается разработка таблицы функционирования и граф-схемы переходов угроз на основе использования сети Петри для визуального отображения любых действий в системе в реальном процессе. Предлагается алгоритмическая система и вычислительные алгоритмы обнаружения и обезвреживания угроз при обеспечении защиты информации на основе таблиц функционирования (ТФ). Разработаны алгоритмические методы, технологии обнаружения и обезвреживания угроз на основе ТФ, позволяющие определить описание основных функций создаваемой программы и требования программному обеспечению.

Abstract: The article proposes the development of a functioning table and a graph diagram of threat transitions based on the use of a Petri net to visually display any actions in the system in a real process. An algorithmic system and computational algorithms for detecting and neutralizing threats while ensuring information protection based on functioning tables are proposed. Algorithmic methods and technologies for detecting and neutralizing threats based on functioning tables have been developed, allowing one to determine a description of the main functions of the program being created and the software requirements.

Ключевые слова: алгоритмизация, автоматизация, формализация, информационные и алгоритмические модели, агрегативные системы, таблица функционирования, угрозы, классификация, математические модели, оценка рисков, вычислительный алгоритм, сложная система, система управления, информационная система, разработка программ, обнаружение, обезвреживание.

Key words: algorithmization, automation, formalization, information and algorithmic models, aggregation systems, functioning table, threats, classification, mathematical models, risk assessment, computational algorithm, complex system, control system, information system, program development, detection, neutralization.

Одним из способов анализа защищенности системы является построение динамических ТФ информационных систем (ИС) [1]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки. Алгоритмические модели на основе ТФ [2, 7] используются как математический аппарат для моделирования динамических дискретных систем, обеспечивающий комплексную защиту ИС от всех внешних и внутренних угроз по заданной логической последовательности. Алгоритмическая модель обеспечения комплексной защиты ИС состоит из несколько основных частей:

1. Общая структурная модель обеспечения безопасности ИС на основе таблицы функционирования;

2. Математическая модель идентификации угроз от внешних и внутренних источников;

3. Синтез и анализ построения таблицы функционирования после получения необходимых данных на этапе «синтез».

4. Пути, способы, методы, модели и средства уничтожения обнаруженных угроз. Здесь также можно получить информацию об уничтожении последовательности обнаруженных угроз в таблице функционирования в виде графа. В цепях графа отображаются пути уничтожения угроз;

5. Анализ возможных угроз на информационную систему, анализ рисков и анализ защищенности ИС.

Постановка задачи. Разработка ТФ и граф-схемы переходов угроз. Использование сети Петри для визуального отображения любых действий в системе в реальном процессе является самим оптимальным решением. Процесс функционирования сети Петри может быть наглядно представлен графом достижимых маркировок. Состояние сети однозначно определяется её маркировкой-распределением фишек по позициям. Вершинами графа являются допустимые маркировки сети Петри, дуги помечены символом срабатывающего перехода [8]. Дуга строится для каждого активированного перехода. Построение прекращается, когда мы получаем маркировки, в которых не активирован ни один переход либо нет маркировки, содержащиеся в графе.

Отметим, что граф достижимых маркировок – представляет собой автомат. Пример траектории в сети Петри задана на рис 1.

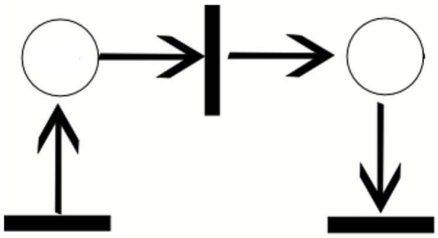

Рисунок 1 – Пример траектории в сети Петри

Рассмотрим некоторые виды сетей Петри [8]:

Временная сеть Петри – такая сеть, где переходы обладают весом, определяющим продолжительность срабатывания (задержку).

Стохастическая сеть Петри – сеть, в которой задержки являются случайными величинами.

Функциональная сеть Петри – сеть, в которой задержки определяются как функции некоторых аргументов, например, количества меток в каких-либо позициях, состояния некоторых переходов.

Цветная сеть Петри – сеть, в которой метки могут быть различных типов, обозначаемых цветами, тип метки может быть использован как аргумент в функциональных сетях.

Ингибиторная сеть Петри – сеть, в которой возможны ингибиторные, то есть подавляющие дуги, запрещающие срабатывания перехода, если во входной позиции, связанной с переходом ингибиторной дугой, находится метка.

Иерархическая сеть Петри -сеть, содержащая не мгновенные переходы, в которые вложены другие, возможно, также иерархические, сети. Срабатывание такого перехода характеризует выполнение полного жизненного цикла вложенной сети.

Универсальная сеть Петри. В1974 году Тилак Аджервала показал, что ингибиторная сеть Петри является универсальной алгоритмической системой. В монографии В.Е. Котова приведён набросок доказательства, указывающий правила кодирования ингибиторной сетью программы счётного автомата Минского. Дж.Питерсон приводит примеры других расширенных классов сетей Петри, являющихся универсальной алгоритмической системой: синхронных и приоритетных. Построенная в явном виде универсальная сеть Петри насчитывала несколько тысяч вершин и недавно была уменьшена до 56 вершин.

Бесконечные сети Петри. Бесконечные сети Петри были введены для верификации вычислительных решёток и позволяют определять свойства сетей Петри для регулярных структур (линейная, древовидная, квадратная, треугольная, шестиугольная и гиперкуб)

произвольного размера, полученных путём композиции типовых фрагментов.

Сети Петри используются для моделирования асинхронных систем, функционирующих как совокупность параллельных взаимодействующих процессов. Анализ сетей Петри позволяет получить информацию о структуре и динамическом поведении моделируемой системы.

Причинно-следственная связь событий в асинхронных системах задаётся «события-условия».

Определяются события-действия, последовательность выполнения которых управляется состояниями системы. Состояния системы задаются множеством условий, формируемых в виде предикатов. Количественно условия характеризуются величиной, которая выражается числами натурального ряда.

Условия, в зависимости от значений их количественных характеристик, могут выполняться или нет. Выполнение условий обеспечивает возможность реализации событий. Условия, с фактом выполнения, которых связывается возможность реализации событий, называются предусловиями. Реализация события обеспечивает возможность выполнения других условий, находящихся с предусловиями в причинно-следственной связи. Эти условия называются постусловиями.

Построение системы защиты является обязательным условием для обеспечения безопасности КИ, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования ИС и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищённости системы является построение динамических ТФ ИС на базе сетей Петри. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются её недостатки.

Развитие ИС обработки и хранения КИ диктует необходимость построения надёжной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование 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 базой Государства. Алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем.

В разработке ТФ было выбрана идеологическая модель сети Петри. Построение системы защиты является обязательным условием для обеспечения безопасности КИ, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования ИС и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищённости системы является построение динамических ТФ ИС на базе сетей Петри. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Один из главной особенности ТФ является идентификация угроз распределения его по критериям, характеристиками и оказывающим негативными действиями систему. В данном случае ранее не известные угрозы после сканирования сравниваются уже известными классами угроз. Если угроза является уникальным для неё в ТФ отделяется отдельное ячейка, а если таковым не является тогда данную угрозу добавляют наиболее подходящим классам угроз.

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.

Если для $\forall t_i \in T$, 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 $\mu: P \to N$.

Каждая маркировка μ может быть представлена как вектор $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$, здесь $n = |P|$ и $\forall \mu_i \in N, i = \overline{1,n}$. Вектор μ определяет для каждой позиции P_i сети количество фишек, т.е. для $\mu_i, p_i, i = \overline{1,n}$ выполняется $\mu(p_i) = \mu_i, i = \overline{1,n}$.

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_iопределённому 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 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.

РМ α_i соответствует агрегату Н.П. Бусленко. Каждому приписывается определённое 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 определённое количество операций (решение задач, переработка материалов и т.д.), а дуги соответствуют потокам между этими местами. Такую сеть назовём R – сетью.

В процессе функционирования системы структура сети со временем может меняться: старые дуги и вершины аннулируются, а новые добавляются. Такие сети назовём ситуационными или RC – сетями. При решении определённого 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 определённый промежуток времени сеть можно изобразить в виде ориентированного графа неизменной структуры (рис.2).

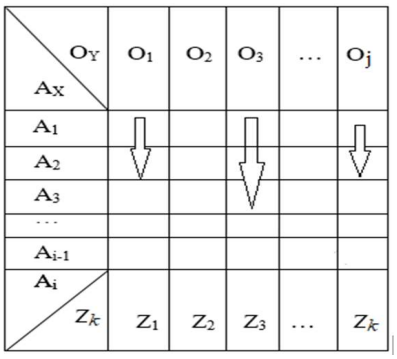

Рисунок 2 – Таблица функционирования

Такое представление соответствует определению ТФ и R-, RC сети представляются в виде ТФ. На этой сети можно фиксировать параметры потока и режим работы сети во времени. Проектируемая ТФ визуально отображает все идентифицированные угрозы в защищаемом нами системы. Все угрозы после идентификации по графам сети Петри двигаться по вертикали вниз, только если это угроза из одного типа.

Если машины, которые должные обрабатывать и уничтожить угрозы не смогут выполнить свою работу данная задача передаётся другой машины, стоящей ниже. В конечном итоге угроза должна быть уничтожена, в ином случае система оповестит о не уничтоженным угрозой в системе.

Если угроза является комбинированным тогда действия графа приобретает абсолютно иной вид.

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

После запуска программного обеспечение также одновременно с ней запускается угрозы, и система начинает противостоять на эти угрозы. Большинство случаях это противостояния приобретает в виде звезды. Причина распространение в виде звезды является тем, что здесь принимается условия проникновение угрозы в систему в виде множества.

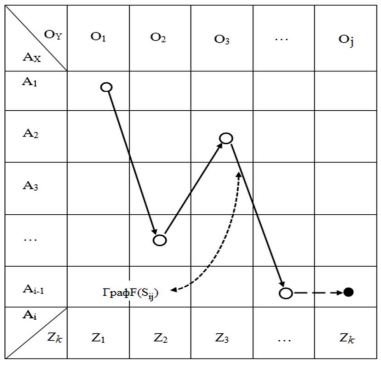

Рисунок 3 – Графы переходов угроз

Расчёты по переходам осуществляются следующим способом.

В ТФ по вертикали имеются 127 средств защиты от угроз. Если проникающая угроза является комбинированной, тогда она проверяется в каждом ячейке, т.е. 127 раз угроза обрабатывается системой. Для вычисления более эффективного переходя для уничтожения угроз имеем формулу $P = \sum_{i=1}^{\infty} U_i$, где U – Угроза P – переходы по ТФ.

Пусть A – антиугрозы, K – класс угроз. Когда U=1, тогда P_{max} Когда U=2, тогда P_{max} Значить P_{max}

Если определены класс угроз и по классу пути уничтожения угрозы тоже ясны тогда формула будет $P_{max_i} = U(A - (A - K_i)), i = \overline{1,9}$. Здесь, если в угрозах один из классов не определяется, то она равняется к 0.

Поскольку угрозы проникают разнообразными способами, для вычисления эффективного пути уничтожения угроз невозможно использовать одну или несколько из них. Необходимо использование всех антиугроз. Значить $P = \sum_{i=1}^{9} P_{max_i}$. Если проникающая угроза является не комбинированной тогда максимум обрабатывая ячейка будет исчисляется по вертикали считывая строки, а минимальная будет равен на одного.

Таким образом, ТФ $= \{X, Y, A, O, \Theta, T, U, S, F, P\}$ – 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 – определённое решение предотвращения угроз;

O – определённое действие угроз;

Θ – координаты между «A_i» и «O_j»;

T – время $\left(\text{для предотвращения и успешной реализации угрозы}\right)$;

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.

Воспользуясь системами действий сетей Петри можно создать блок схему СКЗИ и гибридного варианта сетей Петри в обеспечении ИБ.

Выводы

Таким образом, в работе предложено построение алгоритмической модели СКЗИ для исследования сложных ИС на основе ТФ. 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., Кабулов А.В., Норматов И.Х. Алгоритмизация в теории управляющих систем//Монография: Ташкент-2017, Изд. “Навруз” С.176.

2. Кабулов В.К., Кабулов А.В., Норматов И.Х. Логические методы алгоритмизации в теории управляющих систем. Монография: Германия.2018, Изд. “Ламберт” с.191.

3. Кабулов А.В., Варисов А. Algorithmic information security models on the basis of operation tables// The 4th International conference on big data applications and services (BIGDAS 2017) proceeding August 15-18, 2017, Tashkent, Uzbekistan. National University of Uzbekistan and Korea Big Data Service Society.

4. Кабулов А.В., Варисов А.А. Оценка рисков информационной безопасности. Инновационной развитие науки и образования: Сб.статей международной научной конференции. Пенза. 15/02/2018

5. A.V. Kabulov, I.X. Normatov, I.I. Kalandarov, A.A. Karimov. Algorithmic Method of Organization of Specialized Workshops. International Journal of Advanced Research in Science, Engineering and Technology Vol. 5, Issue 4, April 2018, c.5670-5675, ISSN: 2350-0328

6. Kabulov A.V. and Normatov I.H. About problems of decoding and searching for the maximum upper zero of discrete monotone functions// Journal of Physics Conference Series 1260(10):102006·August 2019 DOI: 10.1088/1742-6596/1260/10/102006 (№ 6, Scopus, IF - 0.22).

7. Kabulov A.V., Normatov I.H. and Ashurov A.O. Computational methods of minimization of multiple functions// Journal of Physics Conference Series 1260(10):102007·August 2019 DOI: 10.1088/1742-6596/1260/10/102007 (№ 6, Scopus, IF - 0.22).

8. Дж.Питерсон Теория сетей Петри и моделирование систем//- М.: Мир, 1984.