Бердимуродов Мансур Алишерович
Старший преподаватель Международная исламская академия Узбекистана
e-mail: mansur_alisherovich@mail.ru
Кудайбергенов Адилбай Абатбаевич
Докторант Национальный университет Узбекистана
e-mail: adilbek_79@list.ru
Болтаев Шерзод Туйбоевич
Заведующий кафедрой Национальный университет Узбекистана
e-mail: boltayev@nuu.uz
Варисов Акмал Аббасович
Соискатель Национальный университет Узбекистана
e-mail: varisovakmal@mail.ru
УДК 519.711(075)

АЛГОРИТМИЧЕСКИЕ МЕТОДЫ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ МИКРОПРОЦЕССОРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В данной работе исследуется алгоритмизация процессов управления с применением современных средств вычислительной техники, которая требует не только совершенствования управления на всех уровнях, но и создания новых эффективных методов рационального и адекватного описания объектов исследования, оптимизации и построения алгоритма управления. Рассматривается процесс синтеза автоматов для реализации алгоритмов криптографии, методов и средств технической защиты информации. Исследуемый алгоритм представляется в виде граф-схемы алгоритмов (ГСА), состоящей из множества операторов-условных и безусловных. Считаются, что безусловные операторы в ГСА соответствуют агрегатам, а условные операторы – переходам между агрегатами в агрегативной системе, т.е. ГСА рассматривают как А-систему.*

Ключевые слова: *агрегат, А-система, криптография, микропроцессор,*

синхронизация.

Berdimuradov Mansur Alisherovich
Senior Lecturer of International Islamic Academy of Uzbekistan
Kudaybergenov Adilbay Abatbaevich
Doctoral student of National University of Uzbekistan,
Boltaev Sherzod Tuyboevich
Head of department of National University of Uzbekistan
Varisov Akmal Abbasovich
Researcher of National University of Uzbekistan

ALGORITHMIC METHODS FOR CREATION OF DISTRIBUTED MICROPROCESSOR CONTROL AND INFORMATION SECURITY SYSTEMS

Annotation. *In this paper, we study the algorithmization of control processes using modern computer technology, which requires not only improved management at all levels, but also the creation of new effective methods of rational and adequate description of the objects of study, optimization and construction of the control algorithm. The process of synthesis of automata for implementation of cryptography algorithms, methods and means of technical protection of information is considered. The investigated algorithm is represented as a graph-scheme of algorithms (GSA), consisting of a set of operators-conditional and unconditional. It is considered that unconditional operators in GSA correspond to aggregates, and conditional operators correspond to transitions between aggregates in aggregate system, i.e. GSA is considered as A-system.*

Key words: *aggregate, A-system, cryptography, microprocessor, synchronization.*

Berdimurodov Mansur Alisherovich
O‘zbekiston xalqaro islom akademiyasi katta o‘qituvchisi
Qudaybergenov Adilbay Abatbaevich
O‘zbekiston Milliy universiteti doktoranti
Boltayev Sherzod Tuyliboyevich
O‘zbekiston Milliy universiteti kafedra mudiri
Varisov Akmal Abbasovich
O‘zbekiston Milliy universiteti tadqiqotchisi

TAQSIMLANGANGAN MIKROPROTSESSORLAR BOSHQARUV TIZIMLARI VA AXBOROT XAVFSIZLIGINI YARATISHNING ALGORITMLASHTIRISH USULLARI

Annotatsiya. *Ushbu maqolada zamonaviy kompyuter texnologiyalaridan foydalangan holda boshqaruv jarayonlarini algoritmlashtirishni o‘rganadi, bu nafaqat barcha darajalarda boshqaruvni takomillashtirishni, balki tadqiqot obyektlarini oqilona va etarli darajada tavsiflash, optimallashtirish va boshqarish algoritmini yaratish uchun yangi samarali usullarni yaratishni talab qiladi. Kriptografiya algoritmlarini, axborotni texnik himoya qilish usullari va vositalarini amalga oshirish uchun avtomatik sintezi jarayoni ko‘rib chiqiladi. O‘rganilayotgan algoritm ko‘plab shartli va shartsiz operatorlar to‘plamidan tashkil topgan algoritmlarning graf-sxemasi (AGS) shaklida ifodalanadi. AGS dagi shartsiz operatorlar agregatlarga, shartli operatorlar esa agregativ tizimdagi agregatlar orasidagi o‘tishlarga, ya’ni GSA A-tizim sifatida qaraladi.*

Kalit so‘zlar: *агрегат, A-tizim, kriptografiya, mikroprosessor, sinxronizatsiya.*

Введение

В данной работе исследуется алгоритмизация процессов управления с применением современных средств вычислительной техники, которая требует не только совершенствования управления на всех уровнях, но и создания новых эффективных методов рационального и адекватного описания объектов исследования, оптимизации и построения алгоритма управления.

Рассматривается процесс синтеза микропрограммных автоматов для реализации алгоритмов управления, криптографии и защиты информации. Исследуемый алгоритм представляется в виде граф-схемы алгоритма(ГСА), состоящей из множества операторов-условных и безусловных. Считается, что безусловные операторы в ГСА соответствуют агрегатам, а условные операторы – переходам между агрегатами в агрегативной системе, т.е. ГСА рассматривается как А-система

Исследуется задача синтеза агрегата (монитора) управления и информационной безопасности представляя алгоритмы в виде граф-схем алгоритмов, состоящих из множества операторов-условных и безусловных на основе булевых функций в классе дизъюнктивных нормальных форм. Для реализации А-систем строятся распределенные микропроцессорные системы управления и информационной безопасности.

Таким образом основными задачами данной статьи являются:

- Реализация алгоритмов криптографии, методов и средств технической защиты информации на базе программируемых микроконтроллеров.
- Построение управляющих мониторов на основе конечных автоматов.
- Алгоритмизация проектирования встроенных систем логического управления технологическими модулями на основе синтеза управляющих автоматов.

Задача синтеза агрегата (монитора) управления и информационной безопасности на основе булевых функций в классе дизъюнктивных нормальных форм

Исследуем алгоритмические автоматные модели агрегатных систем информационной безопасности. Алгоритмическая модель А-систем информационной безопасности определяется таблицей функционирования ($Ф_т$) академика В.К.Кабулова и в работе применяется в защите информации. В данной диссертации таблица функционирования информационной безопасности определяется следующей формулой:

$\Phi_T = < X, Y, \psi, \varphi, Q, T, K, S, F, P, Z >$ - алгоритмическая модель обеспечения безопасности ИС, а также предотвращения любого вида операция к ИС и информационным ресурсам (ИР) [3,4] , где:

X–множество входных символов $X=\{x_i\}$,

Y–множество выходных символов $Y=\{y_j\}$,

ψ–функция переходов $\psi(x_i, a_i)=a_{i+1}$,

φ–функция выходов $\varphi(x_i, a_i) = y_{i+1}$,

Q–множество координат Q_{ij} соответствия ψ_i и φ_j,

T–время предотвращения и успешной реализации операции,

K–внешнее воздействие на $\{\psi_i, \varphi_j\}$ по координате ключа Q_{ij},

S–множество переходов S_{ij} $S=\{a_i\}$,

F(t,P)–функция изменения таблицы функционирования во времени,

P–множество вычислительных и логических операций ввода, вывода и управления, **Z**–множество ролей

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

$$M= \{P, D, I, O, \mu\}, \quad (1)$$

где *P,D,I,O* – соответственно, множества позиций (состояний), операций (переходов), входных и выходных состояний [3,4]. В $Ф_т$ таким образом есть таблица и определена сеть системы (например сеть Петри) и в каждый интервал времени t_i происходит выполнение операции управляющим универсальным монитором.

В работе дается определение универсального монитора как монитора, состоящего из агрегата информационной безопасности, получающего в качестве входной информации набор инструкций для исполнения. Примером универсального автомата является автомат с магазинной памятью и алфавитом магазинных символов. Для синтеза конечного алфавита применяем метод проектирования автоматов по ГСА в информационной безопасности, который состоит из двух этапов и на первом этапе применяется операция разметки ГСА символами.

Метод состоит из двух этапов. Первый этап заключается в разметке ГСА символами (метками) по следующему алгоритму. Первоначально символом α_1 отмечается вход вершины, следующей за начальной, и выход конечной вершины. Затем входы всех вершин, следующих за операторными, отмечаются символами $\alpha_2 \ldots \alpha_n$. Далее входы различных вершин, за исключением конечной отмечаются разными символами.

Таким образом работа первого этапа заканчивается получением размеченной ГСА. Теперь символами $\alpha_2 \ldots \alpha_m$ отмечаются вершины графа автомата Мили. Рассмотрим ГСА и если существует путь перехода из α_m в α_s то соответственно исследуем автомат Мили и на графе автомата вершина α_m соединяется дугой с вершиной α_s направленной из α_m в α_s. В начале дуги записывается конъюнкция $X(\alpha_m, \alpha_s)$ сформированная для этого пути; в конце дуги формируется подмножество операций $Y(\alpha_m, \alpha_s)$ из операторной вершины, через которую проходит путь.

Рассмотрим процесс синтеза автоматов для реализации операции управления и информационной безопасности. Введем понятие монитора - специального агрегата, выполняющего операцию управления в А-системах. Монитор - это агрегат или комплекс А-системы, предназначенный для управления агрегатами этой системы. Монитор отвечает за распределение соответствующей входной информации для агрегатов системы, а также контролирует процессы функционирования агрегатов. Например, в операционных системах могут существовать монитор основной памяти и монитор центрального процессора, в системах информационной безопасности могут быть монитор реализации алгоритмов криптографии, методов и средств технической защиты информации, а в системах механообработки - мониторы локального управления группой станков с ЧПУ [5] и т.д.

Монитору предоставлено право доступа к информационным таблицам и к другим управляющим структурам А-системы, связанным с управляющим агрегатом [1-2].

Универсальным монитором мы называем такой монитор, который состоит из управляющего агрегата, получающего в качестве входной информации набор инструкций для исполнения. Моделью универсального монитора А-системы может служить конечный автомат с магазинной памятью [6]. Для получения конечного алфавита магазинных символов используем методику синтеза управляющих автоматов по ГСА [7]. Согласно

[6-7], методика состоит из двух этапов. Первый этап заключается в разметке ГСА символами (метками) по следующему алгоритму:

Шаг 1. Символом a_r отмечается вход вершины, следующей за начальной, и выход конечной вершины.

Шаг 2. Входы всех, вершин, следующих за операторными, отмечаются символам $a_2,\ldots,a_r$.

Шаг 3. Входы различных вершин, за исключением конечной отмечаются разными символами.

На первом этап е получаем размеченную ГСА. Если теперь каждому символу $a_2,\ldots,a_m$ поставить в соответствие вершину графа автомата Мили, и если на ГСА существует путь перехода из a_m в a_s то на графе автомата вершина a_m соединяется дугой с вершиной α_s направленной из a_m в a_s. В начале дуги записывается конъюнкция $X(a_m,a_s)$ сформированная для этого пути в конце дуги формируется подмножество операций $Y(a_m,a_s)$ из операторной вершины, через которую проходит путь [8].

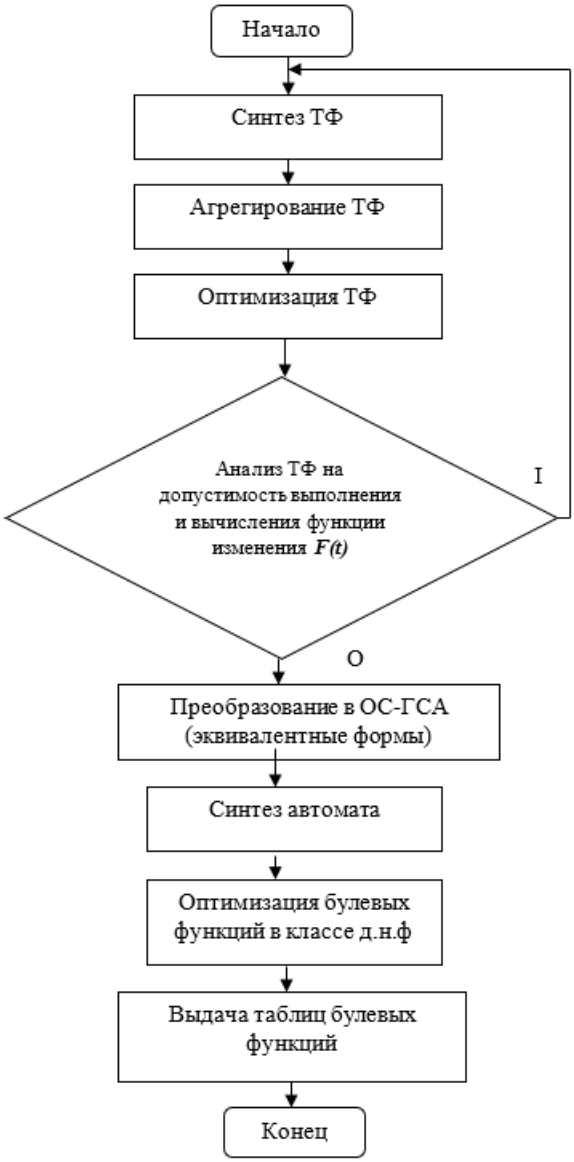

Рис.1. *Общий алгоритм построения мониторов для А-системы*

Общий алгоритм построения мониторов для А-системы графически представлен на рис.1. Описание процесса в виде ОС или ГСА приводит часто к значительному дублированию одинаковых операций при их записи. В связи с этим синтез автомата для монитора отображает в компактном виде ОС или ГСА в систему булевых функций в классе ДНФ. Система булевых функций является управляющей таблицей для реализации мониторов А-систем в виде автоматов с магазинной памятью. Следовательно, описанная выше алгоритмическая модель решения задач проектирования и управления СС позволяет осуществить проектирование процесса управления СС и управление программным оборудованием. Такая схема позволяет гибко и без дополнительных затрат на разработку новых программных средств управлять

объектом с учетом воздействия внешних факторов на производственную систему, в частности на ход производстве.

Таким образом, необходимо комплексное исследование объектов, начиная с предварительного изучения, получения адекватных моделей, алгоритмизации процессов и кончая созданием эффективных систем управления. Следовательно, алгоритмизация процессов управления с применением современных средств вычислительной техники требует не только совершенствования управления на всех уровнях, но и создания новых эффективных методов рационального и адекватного описания объектов исследования, оптимизации и построения алгоритма управления [3-4]. Наконец, рассмотрим процесс синтеза автоматов для реализации алгоритмов криптографии, методов и средств технической защиты информации. Исследуемый алгоритм представляем в виде граф-схемы алгоритмов., состоящей из множества операторов-условных и безусловных. Будем считать, что безусловные операторы в ГСА соответствуют агрегатам, а условные операторы – переходам между агрегатами в агрегативной системе, т.е. ГСА рассматриваем как А-систему.

Таким образом основными задачами являются:

- Реализация алгоритмов криптографии, методов и средств технической защиты информации на базе программируемых микроконтроллеров.
- Построение управляющих мониторов на основе конечных автоматов.
- Алгоритмизация проектирования встроенных систем логического управления технологическими модулями на основе синтеза управляющих автоматов.
- Разработка своего ПТК-программатора на базе известных высокопроизводительных аналогах и системы CAD -проектирования программируемых логических контроллеров.

Распределенные системы информационной безопасности

Структурная схема микропроцессорной системы[4] с распределенным алгоритмов показана на рис.2. Для подключения к микропроцессору (МП)

внешних устройств (ВУ), оперативного запоминающего устройства (ОЗУ), постоянного запоминающего устройства и клеточного автомата информационной система (КА ИС) используется магистральный принцип.

Взаимодействие различных функциональных блоков микропроцессорной системы осуществляется через общие шины: однонаправленную шину адреса; двунаправленную шину данных (ШД) и однонаправленную шину управления (ШУ), последнюю составляют однонаправленные линии, входящие или выходящие из МП. УА дополнительно имеет собственной ШД, которой может быть одно или двунаправленной.

Блок синхронизации (БС) обеспечивает синхронную работу КА ИС и МП. МП является универсальным элементом и без учета временных ограничений позволяет осуществлять любое множество операций $\psi=\{\psi_1,\ldots,\psi_t\}$ над операндами, представленными двоичными векторами из множества, с вычислением результата, представленного двоичным вектором из множества W. Выполнение операций из множества ψ представляется в виде алгоритма *Ф*, записанного в терминах команд МП. Последовательность команд для выполнения алгоритма *Ф* составляет программу, хранимую в управляющей памяти (ПЗУ или ОЗУ). При заданной системе команд эффективность реализации различных операций из тожества МП неодинакова.

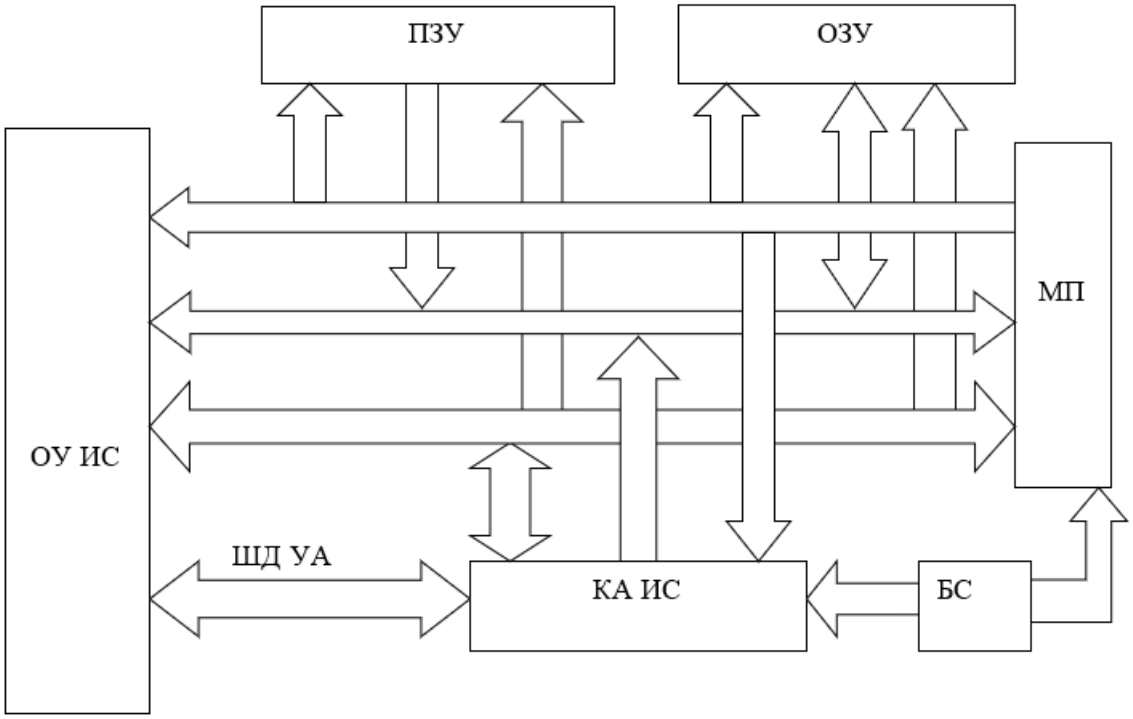

Рис.2. *Структурная схема системы с распределенным вычислением*

Можно рассмотреть следующий алгоритм информационной безопасности с распределением обработки информации на КА ИС и микропроцессором.

Пусть алгоритм криптографии или информационной безопасности задан в виде операторной или блок схемы алгоритмов и построена ГСА алгоритма. Допустим $X_1, X_2, \ldots, X_n$ – условные операторы блок-схемы алгоритмов, принимающие значения 0 или 1. Заданы $Y_1, Y_2, \ldots, Y_m$ – безусловные операторы алгоритма. Пути вычисления алгоритма задаются бинарными наборами ($a_1, a_2, \ldots, a_n$), которые определяют по координатно для заданного алгоритма переходы от начало до конечнего оператора. При этом каждому набору соответствует цепочка вычислений операторов из последовательности $Y_1, Y_2, \ldots, Y_m$.

Набор ($a_1, a_2, \ldots, a_n$) вычисляется на основе $X_1, X_2, \ldots, X_n$ – следующим образом: При вычислении значения X_i получается значние a_i. Таким образом последовательности $Y_1, Y_2, \ldots, Y_m$ соответствует последовательность бинарных

переменных $y_1, y_2, \ldots, y_m$ а последовательности $X_1, X_2, \ldots, X_n$ – последовательность бинарных переменных $x_1, x_2, \ldots, x_n$. В результате имеем таблицу истинности систем булевых функций

$$\begin{cases} y_1 = f_1(x_1, x_2, \ldots, x_n) \\ y_2 = f_2(x_1, x_2, \ldots, x_n) \\ \quad \ldots\ldots \\ y_m = f_m(x_1, x_2, \ldots, x_n) \end{cases} \quad (2)$$

Таблица 1

Таблица истинности

X_1	X_2	$\cdots$	$\cdots$	X_n	Y_1	Y_2	$\cdots$	$\cdots$	Y_m
0	0	0	0	0	β_{11}	β_{12}	$\cdots$	$\cdots$	β_{1m}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
α_{i1}	α_{i2}	$\cdots$	$\cdots$	α_{in}	β_{i1}	β_{i2}	$\cdots$	$\cdots$	β_{im}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
1	1	1	1	0	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
1	1	1	1	1	$\beta_{2^n 1}$	$\beta_{2^n 2}$			$\beta_{2^n m}$

В таблице 1 каждому набору $(a_1, a_2, \ldots, a_n)$ переменных $x_1, x_2, \ldots, x_n$. соответствует бинарный набор $(b_1, b_2, \ldots, b_m)$ переменных $y_1, y_2, \ldots, y_m$ таких, что если $b_i = 1$, то оператор Y_i выполняется в цепочке $(a_1, a_2, \ldots, a_n)$ переменных $x_1, x_2, \ldots, x_n$. Тогда, если в наборе $(b_1, b_2, \ldots, b_m)$ элементы $b_{i_1}, b_{i_2}, \ldots, b_{i_k}$ суть единичные элементы, то в цепочке $X_1, X_2, \ldots, X_n$ с набором $(a_1, a_2, \ldots, a_n)$ соответствуют набор $(b_1, b_2, \ldots, b_m)$ переменных $y_1, y_2, \ldots, y_m$, где операторы $Y_{i_1}, Y_{i_2}, \ldots, Y_{i_k}$ вычисляются в данной цепочке.

Кроме таблицы истинности также можно рассмотреть таблицу интервалов, где в наборах $(a_1, a_2, \ldots, a_n)$ переменных $x_1, x_2, \ldots, x_n$. значения a_i, $i = 1, 2, \ldots, n$ принимают значения 1, 0 или 2, где 1-соответствует x_i, 0 – $\bar{x}_i$ с отрицанием, 2-переменная x_i отсутствует в конъюнкции данного интервала.

Распределенная обработка строится на основе таблицы истинности или таблицы интервалов следующим образом: Блок синхронизации (БС) обеспечивает синхронную работу КА ИС и МП на основе таблицы истиности используя каждую строку таблицы по последовательности переменных $x_1, x_2, \ldots, x_n$. и переменных $y_1, y_2, \ldots, y_m$. Причем значение булевой функции как логическая операция вычисляется в КА ИС, который функционирует в дискретном времени *t*, принимающем целые неотрицательные значения $(t = 0,1,2,\ldots)$. Для каждого вычисленного значения систем булевых функций т.е. для каждой строки выделяются безусловные операторы Y_i и они распределяются по микропроцессорам M_i, соответствующим оператору Y_i.

Микропроцессорная система (АМ-схема) функционирует в дискретном времени *t*, принимающем целые неотрицательные значения (*t=0,1,2,...*). Определим состояние АМ - схемы в моменты времени, непосредственно следующие за начальным *(t=0)*. Положим, что начиная с момента *t=0*, либо КА ИС, либо МП выполняет функциональную основную нагрузку (является ведущим).

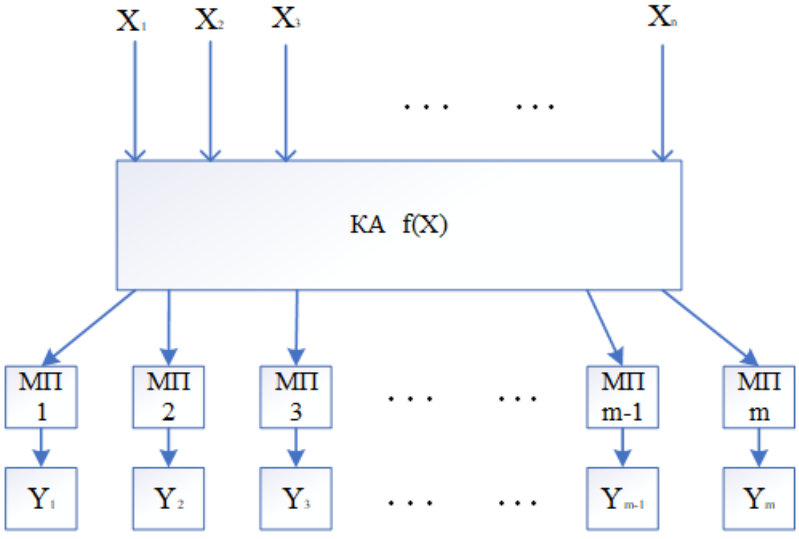

Рис3. *Логическая схема системы с распределенным вычислением*

Пусть ведущим является КА ИС, тогда функционирование системы можно представить следующим образом, УА выполняет операции, реализуемые им по сравнению с МП более эффективно. При необходимости

выполнения операции в МП по некоторой программе $\prod j$ сигналом запроса от КА ИС прерывается работа МП, который мог выполнять некоторую фоновую (вспомогательную) программу. Далее КА ИС передает МП всю необходимую информацию для выполнения требуемой операции. Параллельно с МП КА ИС может выполнять дальнейшие действия в соответствии с алгоритмом *Ф*. Если в программе возникает необходимость выполнения логической операции, то МП прерывает работу КА ИС и обращается к нему за помощью. Рассмотренный процесс взаимных прерываний может продолжаться и далее. Максимальное число таких прерываний (вложений) определяется конкретными параметрами АМ - схемы. В случае, когда ведущим является МП, процесс функционирования системы представляется точно так же. При необходимости выполнения операции (например, A_i) в КА ИС сигналом запроса от МП прерывается работа КА ИС (который мог выполнять фоновый алгоритм) и ему передается вся необходимая информация. В это время МП может продолжать выполнение алгоритма *Ф*.

Рассмотренные принципы построения и функционирования АМ- схемы отвечают концепции модульного программирования систем [5] и позволяют описывать алгоритм *Ф* поэтапно, начиная от укрупненной блок-схемы и кончая подробным описанием операций, с точностью до команд МП и микроопераций, формируемых КА ИС. Представление общего алгоритма *Ф* на различных уровнях с его постепенной детализацией дает возможность сконцентрировать внимание проектировщика на наиболее важных моментах каждого уровня, а не всего алгоритма в целом. В результате существенно сокращается размерность задачи, легко учитываются временные характеристики, влияющие на перераспределение функций между КА ИС и МП, снижается трудоемкость проверки программ и т.д.

Таким образом, процесс проектирования встроенных систем управления и информационной безопасности заключается в следующем:

- описание алгоритмов функционирования технологических модулей и информационной безопасности;
- синтез СЛУ на основе описанных алгоритмов с применением САПР;
- технологическая реализация СЛУ;
- синтез микропроцессорной системы с распределенным управлением.

Заключение

Исследована задача синтеза агрегата (монитора) управления и информационной безопасности на основе представления алгоритмов криптографии в виде граф-схем алгоритмов, состоящих из множества операторов-условных и безусловных на основе булевых функций в классе дизъюнктивных нормальных форм. Для реализации агрегативных систем, алгоритмов криптографии, методов и средств технической защиты информации на базе программируемых микроконтроллеров построены распределенные микропроцессорные системы управления и информационной безопасности.

Литература

1. Бусленко Н.П. Моделирование сложных систем- М.: Наука,1978, С. 390.
2. Бусленко В.Н., Каганович В.Л., Дашкова *В.Г.* Вопросы разработки технологии агрегативного моделирования- Программирование, 1988, №1, С. 66-76.
3. Кабулов В.К., Кабулов А.В., Норматов И.Х. Алгоритмизация в теории управляющих систем//Монография: Ташкент-2017, Изд. “Навруз” С.176.
4. Кабулов В.К., Кабулов А.В., Норматов И.Х. Логические методы алгоритмизации в теории управляющих систем. Монография: Германия.2018, Изд. “Ламберт” С.191.
5. Майоров С.А. и др. Гибкое автоматизированное производство. М.: Машиностроение, 1985, с.454

6. Скляров В.А. Синтез автоматов на матричных БИС. М.: Наука и техника, 1984, С.285.
7. Скляров В.А., Кабулов А.В. Микропроцессорная система с распределенным управлением// ДАН УзССР, 1988, № 7, С.12-14.