УДК 004.02

АНАЛИЗ ЛОГИЧЕСКИХ ФУНКЦИЙ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И СПОСОБОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИХ ВЫЧИСЛЕНИЙ

Сизоненко Александр Борисович
к.т.н., доцент
Краснодарский университет МВД России, Краснодар, Россия

В статье проведен анализ средств и систем защиты информации. Анализ показал, что функционирование многих из них связано с выполнением интенсивных логических вычислений. Проанализированы способы представления булевых функций, приведены критерии эффективности и пути повышения производительности средств и систем защиты информации

Ключевые слова: УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СРЕДСТВА И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, БУЛЕВЫ ФУНКЦИИ, СПОСОБЫ ПРЕДСТАВЛЕНИЯ БУЛЕВЫХ ФУНКЦИЙ, ЛОГИЧЕСКИЕ ВЫЧИСЛЕНИЯ

UDK 004.02

ANALYSIS OF LOGIC FUNCTIONS USED IN INFORMATION SECURITY TOOLS AND SYSTEMS, AND METHODS OF IMPROVE THEIR COMPUTING EFFECTIVENESS

Sizonenko Alexander Borisovich
Cand.Tech.Sci, associate professor
Krasnodar University of the Ministry of the Interior of Russia, Krasnodar, Russia

The analysis of information security tools and systems is carried out in this article. This analysis revealed that the functioning of many of them associated with the implementation of intensive logical calculations. Ways of representing Boolean functions are analyzed, the criteria of efficiency and ways to increase productivity tools and security systems are presented

Keywords: INFORMATION SECURITY THREATS, MEANS AND SYSTEMS INFORMATION SECURITY, BOOLEAN FUNCTIONS, METHODS FOR REPRESENTING BOOLEAN FUNCTIONS, LOGICAL CALCULATIONS

1. Анализ угроз безопасности информационных систем и противодействующих им средств и систем защиты информации, использующих логические вычисления

В настоящее время информация уже стала товаром и мощным ресурсом. Развитие современных информационных технологий, под которыми понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, является одними из важнейших составляющих национальных интересов Российской Федерации в информационной сфере [1, 2].

Однако, наряду с преимуществами построения информационного общества, увеличиваются и риски, связанные с существованием угроз безопасности информационным и телекоммуникационным средствам и системам. Защита информационных ресурсов от несанкционированного до-

ступа, обеспечение безопасности информационных и телекоммуникационных систем, также является одним из основных национальных интересов в информационной сфере [2]. Для обеспечения безопасности информации необходимо решить задачи обеспечения конфиденциальности, целостности и доступности.

Таким образом, в условиях развития информационного общества, возникает **проблема**. **С одной** стороны повышаются объемы информации, обрабатываемой в информационных и телекоммуникационных системах. Об этом свидетельствует увеличение доли предоставления государственных услуг в электронном виде, развитие системы ситуационных центров, повсеместное введение электронного документооборота, использование сети видеоконференцсвязи. **С другой** стороны – увеличивается и вероятность рисков, связанных с существованием угроз безопасности информации. В связи с этим **возникает необходимость** разработки высокопроизводительных систем защиты информации от различных типов угроз во всех перечисленных системах. Так как обработка информации в информационных системах происходит средствами серийной вычислительной техники, то необходимо разработать такие алгоритмы защиты, которые позволяли бы, не сильно сказываясь на производительности, производить решать указанные задачи.

Достаточно большое количество средств и систем защиты информации используют в своей работе интенсивные логические вычисления. Это криптографические средства защиты информации, средства защиты от ошибок, системы разграничения доступа, а также процессы моделирования средств и систем защиты информации. На рис. 1 показаны угрозы информационным и телекоммуникационным системам и противодействующие им средства и системы, использующие в своей работе логические вычисления.

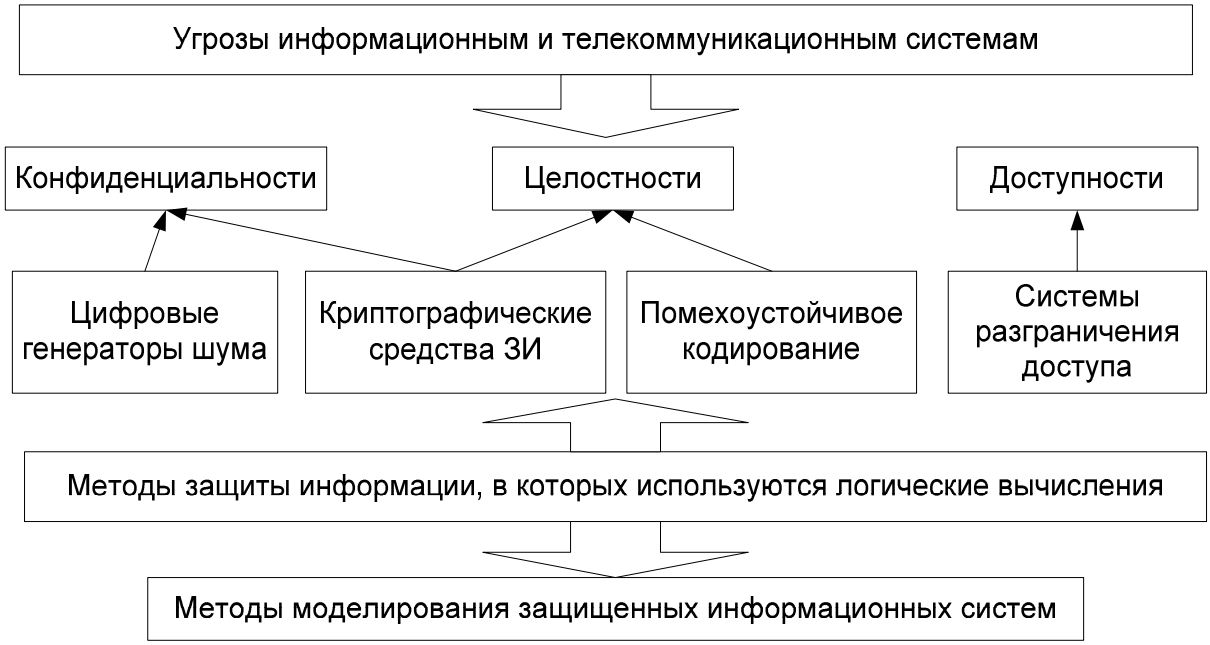

Рис. 1 Анализ угроз, методов и средств защиты информации, использующих в своих алгоритмах логические вычисления

Криптографические средства защиты информации, используя алгоритм шифрования и секретные ключи (либо пару секретный и открытый), осуществляют такие преобразования исходных сообщений, что злоумышленник, не зная секретный ключ, не сможет выполнить обратные преобразования и получить исходное сообщение. Основные направления применения криптографических средств это защита от несанкционированного доступа при передаче и хранении информации, а также подтверждение подлинности отправителя (аутентификация). Таким образом, криптографические средства решают задачи обеспечения конфиденциальности и целостности информации.

С интенсивными логическими вычислениями связано функционирование симметричных алгоритмов шифрования. Симметричный алгоритм шифрования выполняет некоторое число циклов (итераций). Каждый цикл состоит в применении базовых преобразований. Такой принцип построения дает возможность реализовать каждый цикл шифрования с использо-

ванием однотипных узлов, а также выполнять расшифрование путем обработки данных в обратном направлении. [12].

Получили распространение алгоритмы, в которых осуществляются преобразования над векторами, представляющими собой левую и правую половины содержимого регистра сдвига. Для построения таких алгоритмов часто используется конструкция, называемая сетью Фейстеля [20]. Данная конструкция была признана удачной и нашла широкое применение в дальнейших разработках блочных шифров (FEAL, DES, Khufu, Khafre, LOKI, ГОСТ) [12].

Анализ симметричных криптографических алгоритмов показал, что основными криптографическими узлами, использующих интенсивные логические вычисления, являются: рекуррентные регистры сдвига; нелинейные узлы усложнения; блоки подстановок; блоки перестановок; регистры циклического сдвига [12, 20].

Работу современных цифровых систем передачи и хранения информации невозможно представить без использования методов **помехоустойчивого кодирования**. Необходимость их применения продиктована тем, что каналы связи несовершенны и при передаче и хранении информации возможно появление ошибок. Можно привести примеры систем, использующих методы помехоустойчивого кодирования, это: системы сотовой, транкинговой, спутниковой связи, системы цифрового телевидения, беспроводные сети, системы записи информации на оптические диски и др. [7, 15, 17]

Помехоустойчивые коды делятся на два класса: блочные коды и сверточные [15]. В блочных кодах передаваемое сообщение разбивается на блоки определенной длины, которые кодируются и декодируются независимо друг от друга. В сверточных кодах передаваемая информационная последовательность не разделяется на блоки, проверочные элементы раз-

мещаются в определённом порядке между информационными и зависят от нескольких предыдущих значений передаваемого сообщения.

В реально действующих системах для обнаружения и исправления ошибок в основном используются коды линейные блочные коды двух типов: циклические и итеративные (матричные), что обусловлено простотой аппаратурной или программной реализации кодирования и декодирования.

Среди линейных блочных кодов наибольшее значение имеют коды с одной проверкой на чётность, Хэмминга, Голея, Боуза–Чоудхури - Хоквингема, CRC-коды, Рида-Маллера и др. [15]

Для обеспечения безопасности информации, при ее обработки в информационных системах, разрабатывают и используют политику безопасности, под которой понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы [8]. Формальное выражение политики безопасности называется моделью политики безопасности. Основные модели политик безопасности могут быть следующие: дискреционная, мандатная, ролевая, безопасности информационных потоков, изолированной программной среды [5].

В дискреционной модели разграничения доступа основой является матрица доступа, определяющая наличие того или иного права субъекта по отношению к объекту информационной системы. Определение прав в соответствии с матрицей доступа можно свести к вычислению системы булевых функций. Политика ролевого разграничения доступа является развитием политики дискреционного разграничения доступа, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли [5].

В настоящее время разработан целый ряд методов защиты информации в информационных системах, для реализации которых существует

множество постоянно обновляющихся средств защиты. Каждая конкретная защищенная информационная система имеет свои особенности (значимость обрабатываемой и хранимой информации, условия функционирования и т. п.), которые определяют требования к системе защиты информации. В этих условиях практически важным является получение оценок эффективности различных вариантов реализации системы защиты информации, что впоследствии может быть использовано для выбора оптимального с точки зрения предъявляемых требований комплекса защитных методов и средств, необходимых для её создания [11, 13].

Ущерб, наносимый защищенной информационной системе угрозами, часто реализуется достаточно быстро, поэтому для корректной оценки эффективности системы защиты информации необходимо учитывать динамику функционирования рассматриваемой системы [13]. Получение оценок эффективности системы защиты информации с учётом динамики, возможно на основе математического моделирования процесса функционирования защищенной информационной системы в условиях воздействия угроз, которое, осуществляется с использованием теории автоматов [13]. Как известно [18], реализация автоматов на ЭВМ, связана с выполнением логических вычислений.

2. Анализ способов представления булевых функций

Для того чтобы повысить производительность логических вычислений необходимо выбрать такую форму представления, реализация которой средствами серийной вычислительной техники была бы наиболее оптимальной. Проанализируем формы представления булевых функций (рис. 2).

При теоретико-множественном задании булева функция задается

множествами M_f^1 и M_f^0 наборов значений аргументов, на которых она принимает значения 1 и 0 соответственно [6].

При табличном способе задания булевой функции (табл. 1) каждому набору аргумента приписывается определенное значение функции [20]. Наборы и соответствующие им значения группируются в таблицу. Достоинством такого способа представления является наибольшая скорость вычисления значений булевой функции или системы булевых функций. Недостатком – то, что для хранения всех значений необходим большой объем памяти.

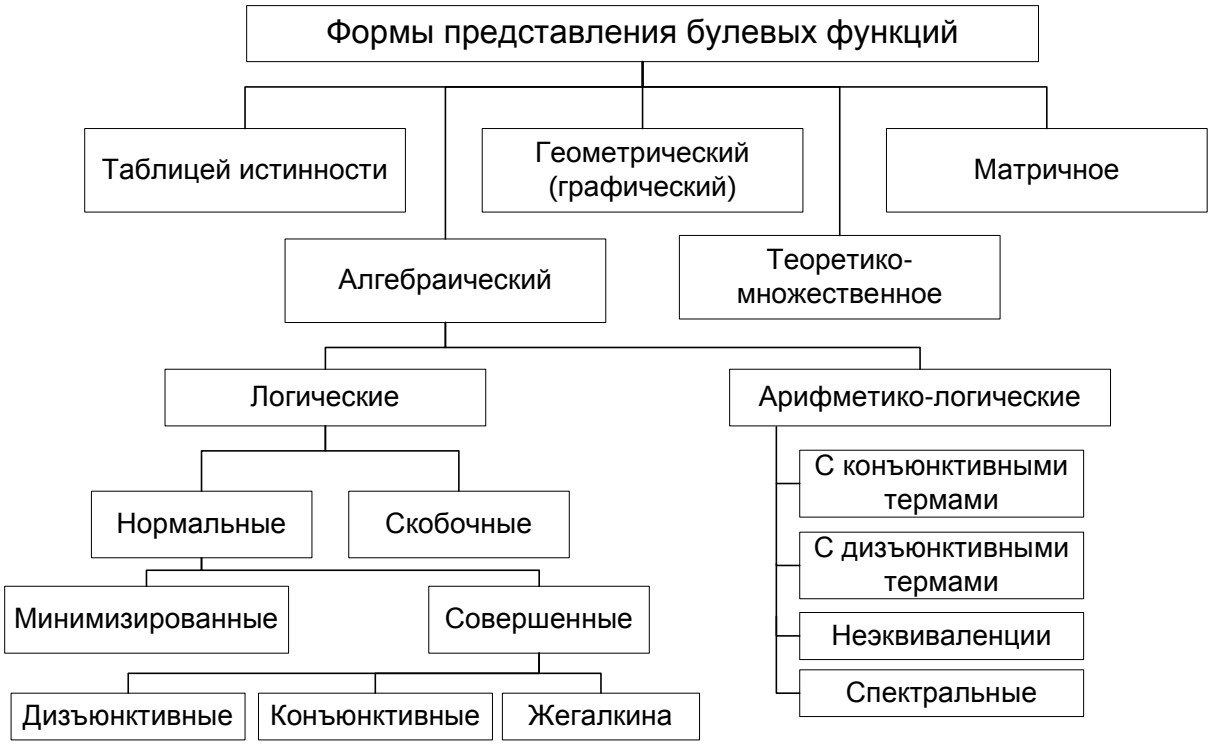

Рис. 2 Формы представления логических функций

Под геометрическим способом задания булевой функции $f(X)$ понимается выделение тех вершин *n*-мерного двоичного куба, на наборах координат которых функция принимает единичное значение [20]. Графическое задание булевой функции $f(X)$ реализуется неориентированным графом с множеством вершин, в котором ребрами соединены пары соседних наборов.

Булева функция может быть представлена в виде алгебраического выражения суперпозиции элементарных логических операций – в виде формул [6].

В нормальных формах последовательно выполняется не более двух базовых операций [14]. В совершенных нормальных формах, кроме того, все члены имеют одинаковую размерность [14].

Анализ источников [4, 6, 10, 14, 19, 20, 21] показывает, что в общем случае совершенные полиномиальные формы можно описать формулой:

$$f(X) = \overset{2^{n-1}}{\underset{i=0}{*}} a_i x_{n-1}^{i-1} \mathbf{o} \mathbf{K} \mathbf{o} x_1^1 \mathbf{o} x_0^0,$$

где название формы, операции $*$ и ○, степенная операция x_j^i, область значений коэффициента a_i представлены в таблице 1.

Таблица 1 – Полиномиальные формы представления булевых функций

Название формы	Операция *	Операция ○	Степенная операция	a_i
Конъюнктивная	$\wedge$	$\vee$	$x_j^i = \begin{cases} x_j, i=0 \\ \bar{x}_j, i=1 \end{cases}$	$a_i \in \{0,1\}$
Дизъюнктивная	$\vee$	$\wedge$	$x_j^i = \begin{cases} \bar{x}_j, i=0 \\ x_j, i=1 \end{cases}$	$a_i \in \{0,1\}$
Жегалкина	$\oplus$	$\wedge$	$x_j^i = \begin{cases} 1, i=0 \\ x_j, i=1 \end{cases}$	$a_i \in \{0,1\}$
Арифметическая 1	+	$\wedge$	$x_j^i = \begin{cases} 1, i=0 \\ x_j, i=1 \end{cases}$	$a_i \in \mathbf{Z}$
Арифметическая 2	+	$\vee$	$x_j^i = \begin{cases} 1, i=0 \\ x_j, i=1 \end{cases}$	$a_i \in \mathbf{Z}$
Арифметическая 3	+	$\oplus$	$x_j^i = \begin{cases} 1, i=0 \\ x_j, i=1 \end{cases}$	$a_i \in \mathbf{Z}$
Спектральная	+	$\times$	$x_j^i = \begin{cases} 1, i=0 \\ (-1)^{x_j}, i=1 \end{cases}$	$a_i \in \mathbf{Z}$

В минимизированной нормальной форме количество первичных термов минимально и последовательно выполняется не более двух базовых

операций алгебры логики. Для получения минимизированной нормальной формы из СНФ применяется аналитический метод минимизации или графический (диаграммы Вейча) [14].

При вынесении в нормальных формах общих членов за скобки количество последовательно выполняемых операций, необходимых для вычисления значения функции (порядок функции), увеличивается. Такие формы называют скобочными [14].

Для представления систем булевых функций одним полиномом используют обобщенные формы [10]. Пусть дан произвольный кортеж булевых функций: $f_{d-1}(X) * f_d(X) * \mathbf{L} * f_0(X)$. Для получения обобщенной формы необходимо выполнить следующий алгоритм:

Шаг 1. Получить полиномиальное представление в выбранном базисе каждой из d функций:

$$\begin{cases} f_0(X) = \overset{2^{n-1}}{\underset{i=0}{*}} a_{0i} x_{n-1}^{i-1} \mathbf{o} \mathbf{K} \mathbf{o} x_1^1 \mathbf{o} x_0^0; \\ f_1(X) = \overset{2^{n-1}}{\underset{i=0}{*}} a_{1i} x_{n-1}^{i-1} \mathbf{o} \mathbf{K} \mathbf{o} x_1^1 \mathbf{o} x_0^0; \\ \text{M} \\ f_{d-1}(X) = \overset{2^{n-1}}{\underset{i=0}{*}} a_{(d-1)i} x_{n-1}^{i-1} \mathbf{o} \mathbf{K} \mathbf{o} x_1^1 \mathbf{o} x_0^0. \end{cases}$$

Шаг 2. Умножить каждый коэффициент a_{ji} функции $f_j(X)$, на 2^j $(j = 1, \mathbf{K}, d-1)$.

Шаг 3. Привести подобные слагаемые и получить обобщенный полином:

$$F(X) = \overset{2^{n-1}}{\underset{i=0}{*}} A_i x_{n-1}^{i-1} \mathbf{o} \mathbf{K} \mathbf{o} x_1^1 \mathbf{o} x_0^0.$$

Вычисление обобщенного полинома производится поразрядным суммированием коэффициентов A_i, если операция $*$ логическая, и по прави-

лам арифметического сложения, если $* \Rightarrow +$.

3. Выбор показателей и критериев эффективности, пути повышения эффективности вычислений логических функций средств, систем, алгоритмов защиты информации

При выборе показателей и критериев эффективности вычисления логических функций средств и систем защиты информации на ЭВМ за основу примем подход, предложенный в [4].

Показателем пространственной эффективности является отношение количества ячеек памяти, необходимых для хранения таблицы истинности $N_t^{яп}$ к количеству ячеек памяти, необходимых для хранения коэффициентов полиномиального представления $N_p^{яп}$: $h = \frac{N_t^{яп}}{N_p^{яп}}$.

Показателем эффективность по трудоемкости вычислений будем считать отношение количества операций (тактов процессора), необходимых для вычисления значения функции при табличном представлении N_t^T к количеству операций (тактов процессора), необходимых для вычисления значения функции пре полиномиальном представлении N_p^T: $x = \frac{N_t^T}{N_p^T}$.

Комплексным показателем эффективности будет являться произведение эффективности по трудоемкости и информационной эффективности: $u = h \cdot x$.

При задании системы булевых функций таблицей истинности $u = 1$. Полиномиальная реализация будет эффективной, если $u > 1$.

Критерием эффективности будет являться максимальное значение комплексного показателя эффективности: $u \to \max$.

Анализ источников [3, 4, 6, 9, 16, 19, 21] позволил определить пути

повышения эффективности средств и систем защиты информации, при вычислении их логических функций на ЭВМ (рис. 3).

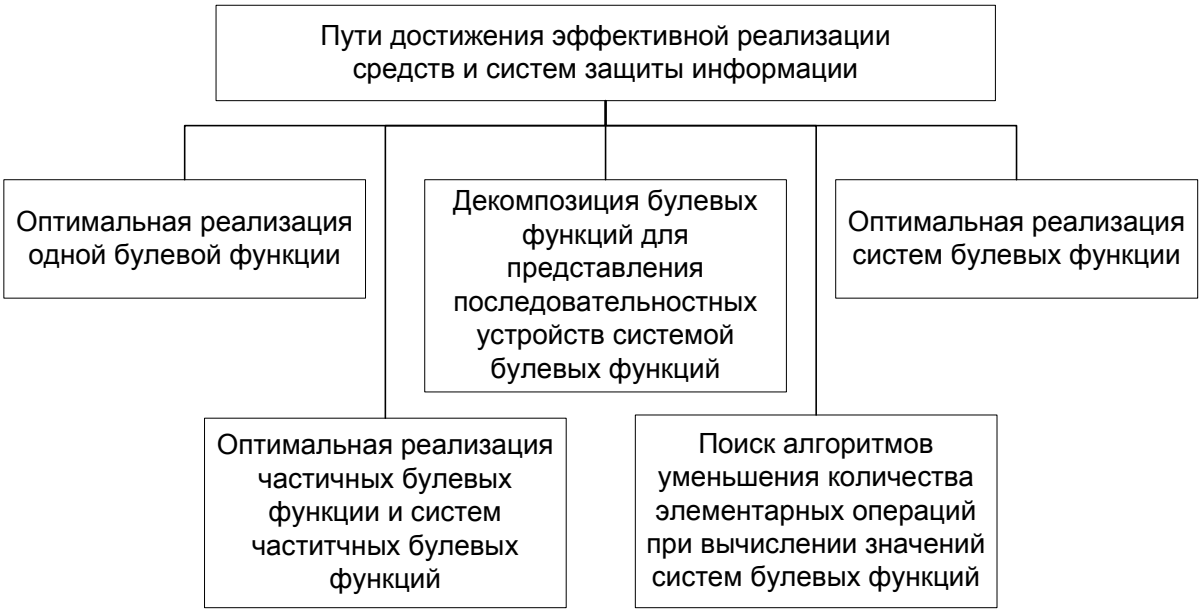

Рис. 3 Пути повышения эффективности логических вычислений

Для логической функции или системы логических функций, описывающей функционирование средства или системы защиты информации необходимо, в соответствии с выбранным критерием, найти оптимальную форму представления. Но даже оптимальное представление может быть по-разному реализовано на ЭВМ. Например, при полиномиальном представлении можно вычисления производить последовательно, а можно применить алгоритмы распараллеливания вычисления термов [16, 22]

Следующим направлением повышения эффективности вычислений является приведение последовательностных устройств к такому виду, чтобы одной системой булевых функций описывалось несколько шагов функционирования. Это направление будет эффективным, когда полученная система позволит более полно использовать вычислительные возможности процессора, такие как, например, разрядность и набор команд. Такой подход реализован при получении арифметического полинома, описывающего несколько шагов функционирования рекуррентного регистра сдвига, устройства усложнения, кодера сверточного кода, автоматной модели за-

щищенной информационной системы [23, 24].

Однотипные вычисления над большим количеством переменных в средствами вычислительной техники выполняются одновременно над всеми битами регистра. Выделив в реализуемом устройстве группы элементов, выполняющих однотипные операции, возможно применение кратных логических вычислений [3, 22].

Как было отмечено выше, в дискреционных моделях разграничения доступа используются матрицы доступа. Определение прав доступа с использованием матрицы доступа можно свести к вычислению системы булевых функций. Однако, в зависимости от количества объектов доступа, такая булева функция может быть определена не на всех наборах. Алгоритм оптимизации не полностью определенных булевых функций позволяет выбрать наиболее оптимальную форму представления [6].

Таким образом, можно сделать вывод, что для оптимальной реализации на ЭВМ средств и систем защиты информации, использующих интенсивные логические вычисления необходимо не только выбрать оптимальную форму представления системы булевых функций, но и попытаться найти оптимальный способ вычисления, наиболее рационально использующий ресурсы ЭВМ: память, процессорное время, набор команд.

Список используемой литературы

1. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Консультант плюс].
2. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) [Консультант плюс].
3. Выхованец В.С. Кратные логические вычисления // Автоматика и телемеханика. – 1998. – № 6. – С. 163-171.
4. Выхованец В.С. Обработка сигналов в дискретных базисах на основе обобщенных полиномиальных форм // Доклады 2-й Международной конференции «Цифровая обработка сигналов и ее применение». – М., 1999. Т. 2. С. 372-377.
5. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

6. Закревский А.Д., Поттосин Ю.В., Черемисинова Л.Д. Логические основы проектирования дискретных устройств. – М.: ФИЗМАТЛИТ, 2007. – 592 с.
7. Защищенные радиосистемы цифровой передачи информации/ П.Н.Сердюков, А.В.Бельчиков, А.Е.Дронов и др. – М.: АСТ, 2006. – 403 с.
8. Зегжда Д. П. Ивашко А.М. Основы безопасности информационных систем. – М., 2000. –425 с.
9. Лапкин Л. Я. О векторной программной реализации логических функций // Автоматика и телемеханика. 1983, № 3. С. 120-128.
10. Малюгин В.Д. Параллельные логические вычисления посредством арифметических полиномов. – М.: Наука. Физматлит, 1997. – 192 с.
11. Меньших В.В. Петрова Е.В. Теоретическое обоснование и синтез математической модели защищённой информационной системы ОВД как сети автоматов // Вестник Воронежского института МВД России. – 2010. – №3. – С. 134 – 143.
12. Основы криптографии: Учебное пособие/ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. — М.: Гелиос АРВ, 2001. — 480 с.
13. Петрова Е.В. Математическое моделирование защищённых информационных систем органов внутренних дел на основе использования методов теории автоматов. Автореф. дис. ... канд. техн. наук: 05.13.18. Воронеж: Воронежский институт МВД России, 2010. 16 с.
14. Пухальский Г. И., Новосельцева Т. Я. Цифровые устройства: Учебное пособие для ВТУЗов. — СПб.: Политехника, 1996. — 885 с.
15. Р. Мореллос-Сарагоса Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Трансфера, 2006. – 320 с.
16. Сизоненко А.Б. Высокопроизводительный алгоритм вычисления термов нелинейного арифметического полинома средствами серийной вычислительной техники // Сборник научных трудов по материалам международной НПК «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании 2010». 20-27.12.2010. Том 4. Технические науки. – Одесса: Черноморье, 2010. С. 35-38.
17. Скляр, Бернард Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 1104.
18. Теория автоматов / Ю.Г. Карпов. – СПб.: Питер, 2003. – 208 с.
19. Финько О.А. Модулярная арифметика параллельных логических вычислений: Монография/ под ред. В.Д. Малюгина. — М.: Институт проблем управления им. В.А. Трапезникова РАН; Краснодар: Краснодарский военный институт, 2003. — 224с.
20. Фомичев В. М. Дискретная математика и криптология: Курс лекций/ Под общ ред. Н. Д. Подуфалова. — М.: Диалог-МИФИ, 2003. — 400 с.
21. Шалыто А. А. Логическое управление. Методы аппаратной и программной реализации алгоритмов. — СПб.: Наука, 2000. — 747 с.
22. Малюгин В.Д., Соколов В.В. Интенсивные логические вычисления // Автоматика и телемеханика. 1993, № 4. С. 160-167.
23. Сизоненко А.Б. Моделирование работы кодера сверточного кода посредством арифметических полиномов // Вестник Воронежского института МВД России. 2010, № 3. С. 144-151.
24. Сизоненко А.Б. Нелинейная арифметическая модель рекуррентного регистра сдвига // Труды IV Межведомственной научно-технической конференции «Проблемы совершенствования систем защиты информации и образовательных технологий подготовки специалистов в области информационной безопасности»/ КВИ. Том 1. — 2003. —С. 144 -147.