

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

ISSN 1563-0064

РАДИОЭЛЕКТРОНИКА И ИНФОРМАТИКА

Научно-технический журнал

Основан в 1997 г.

№ 1(72), январь – март 2016

Выходит 4 раза в год

© Харьковский национальный
университет радиоэлектроники, 2016

Свидетельство о государственной регистрации КВ № 12097-968 ПР 14.12.2006

РИ, 2016, № 1

СОДЕРЖАНИЕ

РАДИОТЕХНИКА

ВЛАСЕНКО Л.А., РУТКАС А.Г. ОБ ОПТИМАЛЬНОМ УПРАВЛЕНИИ ПЕРЕХОДНЫМИ ПРОЦЕССАМИ В ЭЛЕКТРИЧЕСКИХ ЦЕПЯХ.....	3
---	---

ЭЛЕКТРОНИКА

ОКСАНИЧ И.Г., ПРИТЧИН А.С., КАСАТКИН А.В. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ВИРТУАЛЬНОГО МОНИТОРИНГА РАДИАЛЬНОЙ НЕРАВНОМЕРНОСТИ РАСПРЕДЕЛЕНИЯ ПРИМЕСИ В РАСПЛАВЕ И СЛИТКЕ КРЕМНИЯ НА ПРИМЕРЕ ФОСФОРА.....	8
---	---

ТЕЛЕКОММУНИКАЦИИ

ЮДИН А.К., БАРАННИК В.В., ФРОЛОВ О.В. ТЕХНОЛОГИЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ПРИ КОСВЕННОМ СТЕГАНОГРАФИЧЕСКОМ ВСТРАИВАНИИ.....	14
--	----

СИСТЕМЫ И ПРОЦЕССЫ УПРАВЛЕНИЯ

ПИЧУГИНА О.С., ЯКОВЛЕВ В.С. МЕТОД ШТРАФНЫХ ФУНКЦИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ НА ПОЛИЭДРАЛЬНО- СФЕРИЧЕСКИХ КОМБИНАТОРНЫХ МНОЖЕСТВАХ.....	18
НОВОЖИЛОВА М.В., ЛИТВИНЕНКО Є.М. ДИНАМІЧНА МОДЕЛЬ ОПТИМІЗАЦІЇ ТРАНСПОРТНИХ ВИТРАТ З УРАХУВАННЯМ НЕВИЗНАЧЕНОСТІ ТЕРМІНІВ ДОСТАВКИ.....	27
ПРОХОРОВ В. П., ПРОХОРОВ А. В. ПРИНЯТИЕ РЕШЕНИЙ В СИСТЕМЕ КОНТРОЛЯ И АНАЛИЗА ПАРАМЕТРОВ ДВИЖЕНИЯ АВТОТРАНСПОРТА.....	32

КОМПЬЮТЕРНЫЕ НАУКИ

ГРАБОВСЬКА Н.Р., РУСИН Б.П., ІВАНЮК В.Г. ПОХИБКА ТРИВИМІРНОЇ РЕКОНСТРУКЦІЇ ПОВЕРХНІ ЗА ТРИАДОЮ ЇЇ ЗОБРАЖЕНЬ.....	39
---	----

КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА

TAMER BANI AMER, ЧУМАЧЕНКО С.В., ЕМЕЛЬЯНОВ И.В. КУБИТНАЯ ФОРМА ОПИСАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР.....	47
---	----

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

НАРОЖНЫЙ В.В., НАРОЖНАЯ Е.В. ИССЛЕДОВАНИЕ КАЧЕСТВА СБОРКИ ПРИЛОЖЕНИЙ ПОД ОПЕРАЦИОННУЮ СИСТЕМУ ANDROID РАЗЛИЧНЫМИ КОМПИЛЯТОРАМИ.....	53
ЛЕВЫКИН В.М., ЧАЛАЯ О.В. ФОРМАЛИЗАЦИЯ НЕЯВНОГО ПРОЦЕДУРНОГО ЗНАНИЯ	57
БАРАННИК В.В., ПОДЛЕСНЫЙ С.А., ШУЛЬГИН С.С. МЕТОДОЛОГИЯ ОЦЕНКИ ВЛИЯНИЯ КИБЕРАТАК НА БЕЗОПАСНОСТЬ ВИДЕОИНФОРМАЦИОННОГО РЕСУРСА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ.....	61
РЕФЕРАТИ.....	65

КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА



УДК 004.45

КУБИТНАЯ ФОРМА ОПИСАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР

TAMER BANI AMER, ЧУМАЧЕНКО С.В.,
ЕМЕЛЬЯНОВ И.В.

Разрабатываются кубитные модели описания структур и функциональностей для повышения быстродействия анализа цифровых устройств за счет увеличения размерности структур данных и памяти. Вводятся основные понятия, термины и определения, необходимые для реализации квантовых вычислений в практику моделирования компьютерных структур. Описываются примеры, подтверждающие эффективность использования кубитных структур данных для параллельного выполнения операций над данными.

Ключевые слова: квантовые векторы, графы и функциональности, кубитные структуры, параллельные вычисления, моделирование цифровых систем.

Введение

Рыночная привлекательность эмуляции квантовых методов вычислений при создании компьютерных структур (КС) в киберпространстве основана на использовании кубитных моделей данных, ориентированных на параллельное решение задач проектирования, тестирования, дискретной оптимизации при существенном повышении затрат памяти. Не вдаваясь в детали физических основ квантовой механики, касающиеся недетерминированного взаимодействия атомных частиц [1, 3], далее используется понятие кубита как двоичного или многозначного вектора для совместного и одновременного задания булеана состояний в дискретной области киберпространства на основе линейной суперпозиции унитарных кодов, ориентированных на параллельное использование методов анализа и синтеза компонентов киберпространства. В быстро развивающейся теории квантовых вычислений векторы состояний образуют квантовый регистр из n кубитов, формирующих унитарное или гильбертово [4, 5] пространство H , размерность которого имеет степенную зависимость от числа кубитов $\dim H = 2^n$.

Мотивация нового подхода для проектирования КС обусловлена появлением облачных сервисов в рамках новой киберкультуры Internet of Things, которые представляют собой специализированные и рассредоточенные в пространстве виртуальные компьютерные системы [6-9], реализуемые в аппаратуре или в

программном продукте. Любой компонент функциональности, равно как и структура системы, представляется векторной формой, упорядоченной по адресам, таблицей истинности, реализуемой с помощью памяти. Логические функции в традиционном исполнении не рассматриваются. От этого частично уменьшается быстродействие, но, учитывая, что 94% SoC-кристалла составляет память [8], оставшиеся 6% следует реализовывать на памяти, что не будет критичным для большинства облачных сервисов. Практически для создания эффективных компьютерных структур следует использовать теорию, основанную на вычислительных компонентах высокого уровня абстракции: адресуемая память и транзакция.

Особенность организации данных в классическом компьютере состоит в адресации бита, байта или другого компонента. Адресуемость создает проблему обработки ассоциации неадресуемых элементов множества, которые не имеют порядка по определению. Решением может быть процессор, где образ универсума из n унитарно кодированных примитивов использует суперпозицию для формирования булеана $|B(A)| = 2^n$ всех возможных состояний [8].

Существует аналогия векторного представления булеана с кубитом квантового компьютера. Квантовому кубиту хранения информации в квантовом компьютере [1], разрешающей суперпозицию $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, можно поставить во взаимно-однозначное соответствие булеан состояний, формирующий алфавит Кантора $A^k = \{0, 1, X, \emptyset\}$, $X = \{0, 1\}$. Здесь примитивы алфавита унитарно кодируются векторами: $0 = (10)$ и $1 = (01)$. Коды других символов являются производными по операции суперпозиции $(10) \vee (01) = (11)$ и пересечения $(10) \wedge (01) = (00)$, что формирует булеан: $\{(10), (01), (11), (00)\}$ [6].

Корректность использования прилагательного «кубитная» для моделей цифровых устройств основана на сравнении линейной и булевой алгебры Кантора с алфавитом $A^k = \{0, 1, X, \emptyset\}$. Здесь первые два символа – примитивы. Третий определяется суперпозицией: $X = 0 \cup 1$. В гильбертовом пространстве линейная алгебра оперирует примитивами $\alpha|0\rangle$ и $\beta|1\rangle$ кубита, третий символ также есть суперпозиция двух составляющих: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. В линейной алгебре нет символа, соответствующего пустому множеству, он есть производная от функции, обратной по отношению к суперпозиции. В теории множеств такой операцией является пересечение, которое дает пустое множество на примитивах: $\emptyset = 0 \cap 1$. В гильбертовом пространстве такой операцией является скалярное произведение или функция Дирака $\langle a|b \rangle$ [4], которая имеет геометрическую интерпретацию:

$$\langle a|b \rangle \approx |a| \times |b| \times \cos \angle(a, b).$$

Если проекции a и b вектора квантового состояния ортогональны, получается:

$$\langle \alpha | \beta \rangle = |a| |b| \cos \angle(a, b) = |a| |b| \cos 90^\circ = 0.$$

Скалярное произведение ортогональных векторов равно нулю, что является аналогом символа пустого множества в алгебре Кантора. Таблица соответствия алгебры множеств и линейной алгебры, представленная ниже, подтверждает свойства изоморфизма между символами булеана и состояниями кубит-вектора:

Boolean $A^k =$	0	1	$X = 0 \cup 1$	$\emptyset = 0 \cap 1$
Qubit $ \psi\rangle =$	$ 0\rangle$	$ 1\rangle$	$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle \beta 1\rangle$

Следовательно, структуру данных «булеан» можно рассматривать как детерминированный образ квантового кубита в алгебре логики, элементы которой унитарно кодируются двоичными векторами и обладают свойствами суперпозиции, параллелизма и перепутывания. Это дает возможность использовать предлагаемые модели для повышения быстродействия анализа цифровых устройств на классических вычислителях, а также без модификации – в квантовых компьютерах, которые появятся через несколько лет на рынке электроники.

Квантовое описание цифровых функциональных элементов

Кубит (n -кубит) есть векторная форма унитарного кодирования универсума из n примитивов для задания булеана состояний 2^{2^n} с помощью 2^n двоичных переменных. Если $n=2$, то 2-кубит задает 16 состояний с помощью четырех переменных, при $n=1$, кубит задает четыре состояния на универсуме из двух примитивов (10) и (01) с помощью двух двоичных переменных (00,01,10,11) [7]. При этом допускается су-

перпозиция в векторе 2^n состояний, обозначенных примитивами. Кубит дает возможность использовать параллельные векторные логические операции вместо поэлементных теоретико-множественных для существенного ускорения процессов анализа дискретных систем. Далее кубит отождествляется с n -кубитом или двоичным вектором, если это не мешает пониманию излагаемого материала. Синонимом кубита при задании двоичного вектора логической функции является Q -покрытие (Q -вектор) [8] как унифицированная векторная форма суперпозиционного задания выходных состояний, соответствующих адресным кодам входных переменных функционального элемента. Формат структурного кубитного компонента цифровой схемы $Q^* = (X, Q, Y)$ включает интерфейс (входные и выходную переменные), а также кубит-вектор Q , задающий функцию $Y = Q(X)$, размерность которого определяется степенной функцией от числа входных линий $k = 2^n$. Новизна кубитной формы заключается в замене неупорядоченных по строкам таблиц истинности функциональных элементов векторами упорядоченных состояний выходов.

Если функциональный примитив имеет двоичное покрытие, то ему можно поставить в соответствие кубит или Q -покрытие: $Q=(1110)$:

$P =$	<table> <tr> <th>X_1</th><th>X_2</th><th>Y</th></tr> <tr> <td>0</td><td>0</td><td>1</td></tr> <tr> <td>0</td><td>1</td><td>1</td></tr> <tr> <td>1</td><td>0</td><td>1</td></tr> <tr> <td>1</td><td>1</td><td>0</td></tr> </table>	X_1	X_2	Y	0	0	1	0	1	1	1	0	1	1	1	0	$\rightarrow Q = (1110).$
X_1	X_2	Y															
0	0	1															
0	1	1															
1	0	1															
1	1	0															

Преимущества n -кубита заключается в способности параллельно выполнять логические операции над векторным форматом теоретико-множественных данных. Например, хог-операция над $A = \{a, b, c, d, e, f\}$ и $B = \{a, c, f, g, h, k\}$ выполняется параллельно за один такт, если каждый элемент будет представлен унитарным кодом, а подмножества – векторами, которые являются кубит-операндами:

9-qubit	a	b	c	d	e	f	g	h	k
A =	1	1	1	1	1	1	0	0	0
B =	1	0	1	0	0	1	1	1	1
$A \oplus B =$	0	1	0	1	1	0	1	1	1

Квантовое описание графовых структур

Квантовый Q -вектор или кубит, естественно, можно и следует использовать для представления графовых структур. Функция и структура – две взаимно обратимые формы описания некоторой сущности. Рассмотренный выше кубит-вектор или квант идеально укладывается в технологию программируемых логических устройств, которые используют адресуемые элементы памяти. Учитывая определенный изоморфизм функций и структур, несложно «запихнуть» в память второй компонент описания дискретной сущности. Для этого необходимо представить некоторый ориентированный граф в виде вершин V , кодированных двоичными векторами и дугами A , создающими направленные переходы между

$$G = (V, A), V = (V_1, V_2, \dots, V_i, \dots, V_n), A = (A_1, A_2, \dots, A_j, \dots, A_{n^2}).$$

В этом случае ориентированный граф будет представлен таблицей адресов (кодов) всех вершин истоков и стоков, представляющих декартово произведение.

Каждой паре вершин $(V_i, V_j), i, j = \overline{1, n}$ ставится в соответствие 1, если существует дуга между ними $(V_i \rightarrow V_j)$, и 0, если такого соединения нет. Таким образом, квадратичная таблица или матрица смежностей для задания графа превращается в вектор, размерностью n^2 , который технологически тривиально размещается в адресуемом элементе памяти. Такой вектор описания структуры ничем не отличается от задания любой дискретной функциональности и к нему применимы все формальные методы анализа, моделирования, тестирования, верификации и синтеза

дискретных компонентов и систем. Следовательно, создается единый универсальный формат данных в виде кубита или квантового вектора для представления структуры вычислительного устройства и функциональных описаний всех его компонентов. Далее приводятся примеры кубитного задания тривиальных графовых структур, представленных на рис. 1.

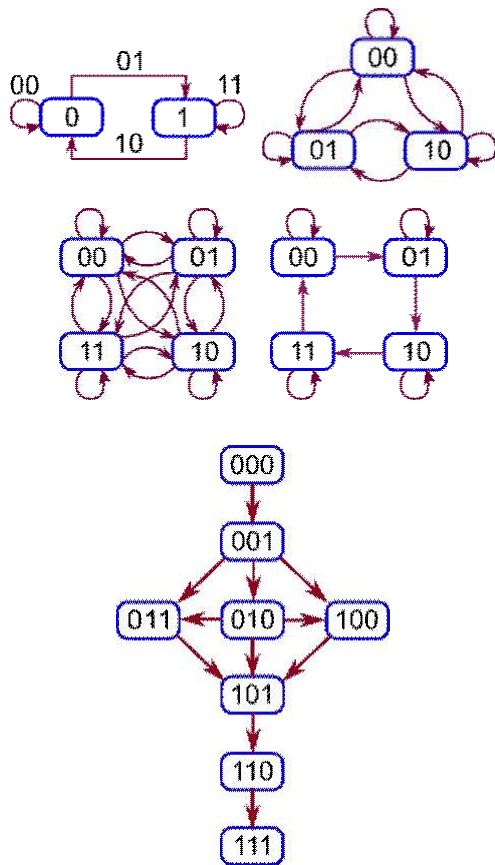


Рис. 1. Примеры примитивных графов для их кубитного описания (G1-G5)

Граф G1 представлен двумя вершинами, которые закодированы 0 и 1 соответственно. Между вершинами имеются четыре перехода, которые обозначены векторами: 00, 01, 10, 11. Данные пары двоичных символов составляют также адреса ячеек памяти, в которые записываются символы 1, поскольку каждый переход имеет место в графе:

$$\begin{array}{|c|c|c|} \hline 0 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline 1 & 0 & 1 \\ \hline 1 & 0 & 1 \\ \hline \end{array} \rightarrow \begin{array}{|c|} \hline 1 \\ \hline 1 \\ \hline 1 \\ \hline 1 \\ \hline \end{array} \rightarrow \boxed{1111} = Q(G_1)$$

Отсутствие некоторого перехода в графе идентифицируется символом 0 в соответствующей ячейке памяти, адрес которой составлен кодами вершин (источка и стока). Граф G2 представлен тремя вершинами, что означает наличие двух двоичных разрядов для кодирования его вершин. Таблица истинности данного графа (повернута для горизонтального инкремента адресов в целях экономии места) также имеет нулевые координаты, поскольку все перехо-

ды, связанные с теоретически возможной вершиной 11, отсутствуют:

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array} \rightarrow \boxed{1110111011100000} = Q(G_2)$$

Если использовать все четыре вершины и построить на них полный граф переходов (G3), то все ячейки кубита, содержащего 16 координат, будут равными 1:

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array} \rightarrow \boxed{1111111111111111} = Q(G_3)$$

Граф G4 также представлен четырьмя вершинами, но он уже не имеет всех возможных переходов, что означает присутствие нулевых координат в кубитном векторе:

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline \end{array} \rightarrow \boxed{110001100001110001} = Q(G_4)$$

Таким образом, кубитная форма описания графа будет более эффективной, если число вершин в структуре будет стремиться к степени двойки. Кубит следует рассматривать как компактную и неявную форму представления графа, которая однозначно и технологически просто может быть превращена в графический рисунок на основе анализа содержимого адресных ячеек памяти (двоичного вектора).

Вершины графа G5 кодируются уже тремя двоичными разрядами, поскольку число вершин $n=8$. Адрес каждой ячейки кубитного вектора содержит 6 разрядов – удвоенное число разрядов для кодирования вершины, а длина кубит-вектора представлена выражением $q = 2^{2 \times \log_2 n}$. В данном случае число разрядов кубита равно $q=64$, номера координат, в которых находятся единицы: 1, 10, 11, 12, 19, 20, 21, 29, 36, 46, 55, а кубит-вектор имеет следующий вид:

$$Q(G_5) = (010000000111000000111000000010000010000000001000000001000000001000000000)$$

Таким образом, длина кубит-вектора зависит только от количества вершин в графе. Если число дуг мало по сравнению с полным графом, который содержит n^2 направленных соединений, то эффективность E использования кубит вектора – отношение количества единичных координат кубита $\text{card}(1)$ к его общей

длине: $E = \text{card}(1) / 2^{2 \times \log_2 n}$ будет невысокой. На-

пример, для графа G5: $E = 11 / 2^{2 \times \log_2 8} = 0,172$.

Анализ кубитного описания графовых структур

Физическая сущность кубита – память (двоичный вектор), в которой каждая адресуемая ячейка хранит значение нуля или единицы. Логическая его сущность – кортеж, состоящий из трех компонентов: (A,B,C),

где А – первая часть адреса ячейки памяти, представленная двоичным кодом вершины истока, В – вторая часть адреса, соответствующая коду вершины стока, С – идентификатор истинности $C(AB)=1$ или ложности $C(AB)=0$ конкатенируемого высказывания: «существует дуга из вершины А в вершину В». Являясь одномерной формой матрицы смежностей кубит-вектор, ориентирован на решение всех задач дискретного моделирования, синтеза, анализа и оптимизации. Но вопрос заключается в нахождении того класса задач, для которого использование кубитного описания и адресно-ориентированных процедур, исключающих перебор, дает технологические или экономические преимущества.

Синтез (modeling) кубитной модели системы на основе кубитных описаний компонентов

Анализ или моделирование (simulation) кубитной модели структуры на основе заданных входных условий: поиск всех путей от входной или выходной вершины.

Поиск максимального или минимального пути в графе на основе моделирования начальных условий.

Покрывание минимальным количеством путей всех вершин графа для тестирования и верификации цифровых систем.

Поиск дефектов в вычислительных структурах на основе обратного прослеживания некорректной выходной реакции.

Процесс моделирования графа по его кубиту сводится к выполнению единственной процедуры – извлечение состояния из ячейки кубит-вектора по адресу, полученному на основе конкатенации адреса, составленного из кодов вершин истока и стока:

$M(A, B) = Q(A * B)$. Такая процедура отвечает на вопрос – существует ли в графе дуга (AB). Целью процедуры моделирования может быть: 1) нахождение максимального или минимального пути в графе; 2) определение всех путей от входной вершины; 3) вычисление всех вершин преемников для заданного выхода. Если некоторая система содержит совокупность взаимосвязанных графов, тогда процесс моделирования будет использовать следующее выражение: $M_i(A, B) = Q_i(A * B)$.

Интересен также квантовый формат представления графа для эффективного параллельного выполнения элементарных алгебраических операций. Речь идет об алгебро-логических операциях над кубит-векторами одной размерности: конъюнкция (пересечение графов), дизъюнкция (сложение графов), исключающее или (сравнение графов), инверсия (дополнение к графу). Здесь фактически в векторной форме осуществляются манипуляции с дугами на кубит-векторах одинаковой длины. Они могут быть получены, если все графы привести к одному универсальному множеству вершин, которое формирует одинаковое число потенциально возможных дуг. Примеры выполнения

алгебро-логических операций над графами, заданными кубит-векторами, представлены в следующей таблице:

G1	0 1 1 0 0 1 1 1 0 0 0 1 1 0 0 0
G2	0 0 1 1 0 0 0 1 1 1 0 0 1 0 1 0
And(G1, G2)	0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0
Or(G1, G2)	0 1 1 1 0 1 1 1 1 0 1 1 1 0 1 0
Xor(G1, G2)	0 1 0 1 0 1 1 0 1 1 0 1 0 0 1 0
Not G1	1 0 0 1 1 0 0 0 1 1 1 0 0 1 1 1

Операция хог показывает расстояние между графами, выраженное в количестве единиц, соответствующих кодовому расстоянию по Хэммингу. В данном примере расстояние между двумя графами равно $d(G1, G2) = 8$. Если два или более графа имеют разное число вершин, то для выполнения алгебро-логических операций над ними необходимо коды вершин всех графов привести к одинаковой размерности. Такая процедура создает одинаковое адресное пространство для кодов (A,B) ориентированных дуг всех графов. При этом размерность всех кубит-векторов станет одинаковой, что является необходимым и достаточным условием для алгебро-логических манипуляций над ними. Задача приведения или нормализации всех графовых структур к одинаковой размерности фактически означает перекодировку уже существующих вершин графа в новой системе координат. Если решение задачи нормализации связано с последующим сравнением графов, в целях определения степени их сходства (различия), то необходимо выполнять синтез кодов дуг, приближающий все графы к структуре максимального из них. Данная задача (нормализации, распознавания, кластеризации, классификации графов) чрезвычайно важна для теории, представляет самостоятельный практический интерес и здесь не рассматривается. Тем не менее, ниже представлены четыре квантовых вектора, которые описывают первые четыре графа, приведенные к формату четырех вершин и двухбитовых векторов (пробелы в таблице соответствуют нулевым координатам):

G1	1	1					1	1
G2	1	1	1	1	1	1	1	1
G3	1	1	1	1	1	1	1	1
G4	1	1		1	1		1	1
And(G3, G1) = G1	1	1					1	1
And(G3, G2) = G2	1	1	1	1	1	1	1	1
And(G3, G4) = G4	1	1		1	1		1	1
Xor(G2, G4) = 7	1	1		1	1	1	1	1

Операция логического умножения показывает, что в приведенном формате, состоящем из четырех вершин, все три структуры (G1, G2, G4) являются подмножеством графа G3. Кодовое расстояние по Хэммингу между вторым и четвертым графами (последняя строчка таблицы) равно 7 из 16.

Таким образом, представленные результаты имеют определенную научную и практическую значимость: 1) Предложена новая кубитная форма описания графов, которая характеризуется компактностью описа-

ния всех ориентированных дуг, векторным представлением структуры межсоединений, что дает возможность существенно повысить быстродействие методов анализа за счет выполнения параллельных логических операций. 2) Кубитная форма пригодна также для описания логических функциональностей, что делает ее универсальной структурой для применения в проектировании, синтезе и анализе современных специализированных компьютерных систем. 3) Высокая технологичность применения квантовых или кубитных форм в описании вычислительных устройств дает основания к ее эффективному использованию при решении широкого спектра задач дискретной оптимизации, синтеза и анализа, распознавания и диагностирования, моделирования и тестирования.

Моделирование кубитного описания цифровых структур

Процедура функционального моделирования на Q-векторе логической функциональности сводится к записи в выходную булеву переменную Y состояния бита Q-вектора, адрес которого сформирован на основе конкатенации значений входных переменных: $Y = Q(X) = Q(X_1 * X_2 \dots * X_j \dots * X_k)$. Для моделирования цифровых схем вводится M-вектор состояний линий, как аналог Q-вектора, задающий значения внутренних переменных системы, который связывает Q-векторы логических примитивов (Q-примитивов) в структуру с помощью нумерации входных и выходных переменных каждого функционального элемента [6]. Процедура обработки последнего определяется выражением:

$$M(Y) = Q[M(X)] = Q[M(X_1 * X_2 \dots * X_j \dots * X_k)].$$

С учетом сквозной нумерации Q-примитивов универсальная процедура моделирования текущего i-элемента будет иметь формат

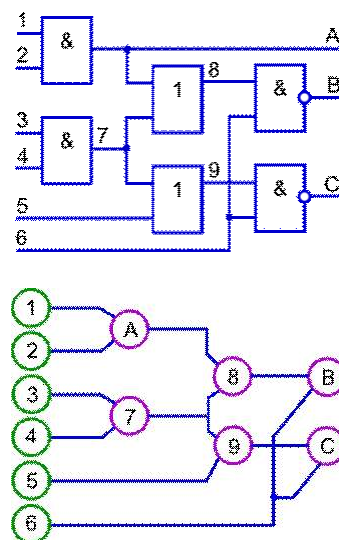
$$M(Y_i) = Q_i[M(X_i)] = Q_i[M(X_{i1} * X_{i2} \dots * X_{ij} \dots * X_{ik_i})]$$

Существенно упрощается алгоритм моделирования цифровой системы, который сводится к процедуре формирования адреса, что дает возможность в $2^n - 1$ раз повысить быстродействие интерпретативного моделирования за счет замены таблиц истинности примитивов на Q-векторы описания только выходных состояний. Кроме того, если логический элемент имеет n входов, то число строк таблицы истинности равно 2^n , что означает – ее размерность равна $d = 2^n \times n$. Учитывая, что длина Q-вектора для любого логического примитива равна 2^n , то выигрыш в объеме памяти для его хранения и обработки составляет:

$$r = \frac{2^n \times n}{2^n} = n.$$

Комбинационная схема (рис. 2) содержит шесть примитивов и три различных логических элемента [6].

Данной схеме соответствует кубит графа и Q-векторы для задания логических примитивов.



$$Q(G) = (.1 \dots 11 \dots 1 \dots 1 \dots \dots \dots),$$

$$G = \{000 - 001, 001 - 010, 001 - 011, 010 - 100, 011 - 101\},$$

$$Q(A) = (0001), Q(7) = (0001), Q(8) = (0111),$$

$$Q(9) = (0111), Q(B) = (1110), Q(C) = (1110).$$

Рис. 2. Граф цифрового устройства

Таким образом, структура графа $Q(G1: A=000, 7=001, 8=010, 9=011, B=100, C=101)$, а также все функциональные элементы $Q(A)-Q(8)$ представлены в форме кубитных покрытий или векторов, что существенно меньше по объему памяти, чем матрица смежностей и таблицы истинности логических элементов.

Выводы

1. Предложенные кубитные модели описания структуры цифровых систем и функций компонентов характеризуются компактностью описания матриц смежностей и таблиц истинности в форме Q-покрытий вследствие унитарного кодирования входных состояний, что позволяет повысить быстродействие программных и аппаратных средств для моделирования вычислительных устройств, благодаря адресной реализации анализа кубитных векторов.

2. Инновационная идея квантовых вычислений заключается в переходе от вычислительных процедур над байт-операндом, определяющим в дискретном пространстве одно решение, к логическим регистровым параллельным процессам над кубит-операндом, одновременно формирующим булеан решений. Это дает возможность определить новые пути создания высокопроизводительных компьютеров параллельного анализа и синтеза структур и компьютерных сервисов.

3. Предложена новая кубитная форма описания графов, которая характеризуется компактностью описания всех ориентированных дуг, векторным представлением структуры межсоединений, что дает возмож-

ность существенно повысить быстродействие методов анализа и моделирования за счет выполнения параллельных логических операций.

4. Высокая технологичность применения квантовых или кубитных форм в описании вычислительных устройств дает основания к ее эффективному использованию при решении широкого спектра задач дискретной оптимизации, синтеза и анализа, распознавания и диагностирования, моделирования и тестирования.

5. Дальнейшие направления исследований связаны с разработкой быстродействующих методов и алгоритмов синтеза, анализа, визуализации, нормализации, распознавания, кластеризации, классификации графово-функциональных структур и систем на основе использования универсальной метрики (например, Манхэттен) приведения и нормализации графов в единой системе координат.

Литература: 1. *Michael A. Nielsen & Isaac L. Chuang*. Quantum Computation and Quantum Information. Cambridge University Press. 2010. 676 p. 2. *Mark G. Whitney*. Practical Fault Tolerance for Quantum Circuits. PhD dissertation. University of California, Berkeley. 2009. 229 p. 3. *Mikio Nishihara*. Quantum Computing. An Overview. Higashi-Osaka: Kinki University, 2010. 53p. 4. *Курош А.Г.* Курс высшей алгебры. М.: Наука. 1968. 426с. 5. *Горбатов В.А.* Основы дискретной математики. М.: Высшая школа, 1986. 311 с. 6. *Hahanov V.I., Litvinova E.I., Chumachenko S.V.* et al. Qubit Model for solving the coverage problem // Proc. of IEEE East-West Design and Test Symposium.

Kharkov. 14-17 September, 2012. P.142-144. 7. *Хаханов В.И., Ваджеб Гариби, Литвинова Е.И., Шкиль А.С.* Кубитные структуры данных вычислительных устройств // Электронное моделирование. 2015. № 1. С.76-99. 8. *Хаханов В.И., Тамер Бани Амер, Чумаченко С.В., Литвинова Е.И.* Кубитные технологии анализа и диагностирования цифровых устройств // Электронное моделирование. 2015. Том 37. № 3. P. 17-40. 9. *Vladimir Hahanov, Wajeb Gharibi, Igor Iemelianov, Dmitry Shcherbin*. «Quantum» Processor for Digital Systems Analysis // Proceedings of IEEE East-West Design & Test Symposium (EWDTS-2015). 2015. Batumi, Georgia. P. 104-110.

Поступила в редколлегию 12.02.2016

Рецензент: д-р техн. наук, проф. Кривуля Г.Ф.

Tamer Bani Amer, аспирант ХНУРЭ. Научные интересы: квантовые вычисления, тестирование и диагностика цифровых систем. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. +3805770-21-326.

Чумаченко Светлана Викторовна, д-р техн. наук, профессор, зав. кафедрой АПВТ ХНУРЭ. Научные интересы: математическое моделирование, теория рядов, методы дискретной оптимизации. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. + 3805770-21-326, e-mail: ri@kture.kharkov.ua.

Емельянов Игорь Валерьевич, научный сотрудник каф. АПВТ ХНУРЭ. Научные интересы: квантовые вычисления, тестирование и диагностика цифровых систем. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. + 3805770-21-326.

РЕФЕРАТИ

УДК 517.9

Щодо оптимального керування перехідними процесами в електричних колах /Л.А. Власенко, А.Г. Руткас // Радіоелектроніка та інформатика. 2016. № 1. С. 3-7.

Описана задача оптимального керування перехідними процесами в електричних колах зі зосередженими лінійними елементами. Якість керування характеризує квадратичний функціонал енергії, що залежить від параметрів кола. Перехідні процеси змодельовано лінійними диференціально-алгебраїчними рівняннями, для яких одержано умови існування та єдиності оптимального керування.

Л. 1. Бібліогр. : 9 назв.

УДК 621.315.592

Математична модель для віртуального моніторингу радіальної нерівномірності розподілу домішки в розплаві та злитку кремнію на прикладі фосфору /І.Г. Оксанич, О.С. Притчин, А.В. Касаткін // Радіоелектроніка та інформатика. 2016. № 1. С. 8-13.

Удосконалена математична модель для віртуального моніторингу радіальної та осевої нерівномірності розподілу домішки в розплаві й злитку кремнію. У результаті апробації моделі шляхом порівняння розрахункових і експериментальних даних отримане добре узгодження між виміряною експериментальним методом і розрахованою радіальною концентрацією легуючої домішки в злитках кремнію.

Табл. 3. Л. 4. Бібліогр.: 15 назв.

УДК 681.3

Технологія підвищення безпеки інформаційних ресурсів на основі використання функціонального перетворення при непрямому стегаграфічному вбудовуванні /Юдін А.К., Бараннік В.В., Фролов О.В.// Радіоелектроніка та інформатика. 2016. № 1. С. 14- 17.

В статті розглянуто можливість підвищення безпеки інформаційних ресурсів на основі використання методів комп'ютерної стегаграфії. Проведено порівняльний аналіз існуючих методів безпосереднього та непрямого стегаграфічного вбудовування інформації в зображення - контейнер. Визначено основні показники якості функціонування систем непрямого стегаграфічного вбудовування. Проведено порівняльний аналіз найбільш розповсюджених існуючих стегаграфічних методів. Для усунення виявлених недоліків існуючих стегаграфічних систем сформульовано підхід, заснований на синтезуванні функціоналу для використання структурної надлишковості зображення.

Бібліогр.: 7 назв.

ABSTRACTS

UDC 517.9

On the optimal control of transient processes in electrical circuits /L.A. Vlasenko, A.G. Rutkas // Radioelectronika i informatika. 2016. № 1. P. 3-7.

We examine the optimal control problem of transient processes in electrical circuits with lumped linear elements. The control performance criterion is a quadratic energy functional depending on circuit parameters. Transient processes are described by linear differential-algebraic equations, for which we have received existence and uniqueness conditions of optimal control.

Fig. 1. Ref.: 9 items.

UDC 621.315.592

Mathematical model for the virtual monitoring of radial non-uniformity of distribution of impurities in the silicon melt and the ingot on phosphorus example /I.G. Oksanich, O.S. Prytchyn, A.V. Kasatkin // Radioelektronika i informatika. 2016. № 1. P. 8-13.

The mathematical model for the virtual monitoring of radial and axial non-uniformity of distribution of impurities in the silicon melt and the ingot improved. A good agreement between measured by the experimental and calculated radial dopant concentration of the silicon ingots obtained as a result of the model validation by comparing the calculated and experimental data.

Tab. 3. Fig. 4. Ref.: 15 items.

UDC 681.3

Technology for safety increasing of information resources on the basis of use of functional transformations, the indirect steganographically embedding /Yudin A., Barannik V., Frolov O.// Radioelektronika i informatika. 2016. № 1. P. 14-17.

In this article the possibility of safety increasing of information resources on the basis of using computer steganographic methods is considered. The comparative analysis of methods of direct and indirect steganographic embedding of information to the image the container is carried out. The main indicators for quality of functioning of indirect steganographic embedding systems are defined. The comparative analysis of the widespread existing steganographic methods is carried out. For elimination of the revealed shortcomings of the existing steganographic systems formulated approach based on use of functionality for using for embedding the structural redundancy of the image.

Ref.: 7 items.

Метод штрафних функцій для розв'язання задач оптимізації на поліедально-сферичних комбінаторних множинах / О.С.Пічугіна, С.В.Яковлев // Радіоелектроніка та інформатика. 2016. № 1. С. 18-26.

Представлено новий підхід до розв'язання задач оптимізації на вписаних в сферу евклідових комбінаторних множинах, що ґрунтується на застосуванні функціональних представлень дискретних множин і опуклих продовжень з них у методі штрафних функцій. Дано порівняльний аналіз застосування у запропонованому методі різних способів опуклого продовження цільової функції, а також її верхні та нижні оцінки.

Бібліогр.: 29 назв.

Динамічна модель оптимізації транспортних витрат з урахуванням невизначеності термінів доставки / М.В.Новожилова, Є.М. Литвиненко // Радіоелектроніка та інформатика. 2016. № 1. С. 27-31.

Розглянута транспортно-логістична система обслуговування клієнтів з організацією доставки та вивезення інструментів. Запропонована динамічна модель виконання портфелю замовлень на визначеному горизонті планування з мінімізацією транспортних витрат.

Л. 5. Бібліогр.: 15 назв.

Прийняття рішень в системі контролю і аналізу параметрів руху автотранспорту / В. П. Прохоров, О. В. Прохоров // Радіоелектроніка та інформатика. 2016. № 1. С. 32-38.

Розглянуто проблеми автоматизації процесу прийняття рішень в інформаційно-навігаційних системах контролю і аналізу параметрів руху автотранспорту на основі інтелектуальних інформаційних технологій. Показана можливість застосування для цих цілей інтелектуальних систем підтримки прийняття рішень. Наведено структуру, принципи побудови та вирішувані задачі систем підтримки прийняття рішень. Розкрито основні режими функціонування і наведено ефективний алгоритм логічного висновку при різних стратегіях скорочення перебору, що забезпечує підвищення ефективності вирішення логіко-аналітичних завдань і прийнятих рішень в інформаційно-навігаційних системах контролю і аналізу параметрів руху автотранспорту.

Л. 5. Бібліогр.: 8 назв.

Похибка тривимірної реконструкції поверхні за тріадою її зображень / Н.Р. Грабовська, Б.П. Русин, В.Г. Іванюк // Радіоелектроніка та інформатика. 2016. № 1. С. 39-46.

У статті розглянуто проблему оцінки похибки тривимірної реконструкції поверхні за двовірними зображеннями. Для відеозйомки зображень запропоновано використовувати три напрямки освітлення. Від точності встановлення напрямків освітлення визначально залежить точність реконструкції. Проведено оцінку похибки реконструкції похідних поверхні залежно від вертикального напрямку освітлення. Зокрема на основі технічних характеристик системи тривимірної реконструкції та пристрою

The penalty method for solving optimization problems over polyhedral-spherical combinatorial sets / O.S.Pichugina, S.V.Yakovlev // Radioelektronika i informatika. 2016. N 1. P. 18-26.

A new approach to optimization problems over euclidean combinatorial sets inscribed into a sphere is presented. It is based on utilization in the penalty method of functional representations of discrete sets and convex extensions from

them onto $\square^n$. For the proposed method, a comparative analysis of the applying different techniques of convex extension of objective function and its upper and lower bounds are given.

Ref.: 29 items.

Dynamic optimization model transport costs with uncertainty delivery time / M.V. Novozhilova, Y. M. Lytvynenko // Radioelektronika i informatika. 2016. N 1. P. 27-31.

We consider the transport and logistics system servicing the organization of the delivery and removal tools. Proposed dynamic model portfolio execution orders for specified planning horizon of minimizing transportation costs.

Fig. 5. Ref.: 15 item.

Decision-making in the system of control and analysis of vehicle motion parameters / V. P. Prokhorov, A.V. Prokhorov // Radioelektronika i informatika. 2016. N 1. P. 32-38.

The problems of automating the decision-making in information and navigation systems of monitoring and analysis of vehicle motion parameters based on intelligent information technologies are considered. The possibilities of using for this purpose intelligent decision support systems are presented. The decisions support systems structure, principles and tasks to be solved are described. The efficient reasoning algorithm for various strategies to reduce of iterations is described. It provides to increase of logical and analytical tasks solution efficiency in information and navigation systems of monitoring and analysis of vehicle motion parameters.

Fig. 5. Ref.: 8 items.

An error of three-dimensional reconstruction of surface is after the triad of images / Hrabovcska N.R., Rusyn B.P., Ivanyuk V.G. // Radioelektronika i informatika. 2016. № 1. P. 39-46.

The article considers the problem of error estimation for three-dimensional surface reconstruction with two-dimensional images. For recording images it offers to use three directions of illumination. The accuracy of the determination of directions of illumination initially depends on the accuracy of the reconstruction. The estimation error of the reconstruction of the derivatives of the surface depending on vertical direction of illumination. In particular on the basis of technical descriptions of the system of three-dimensional reconstruction and device of the vertical ray the calculation of estimation of error of reconstruction of derivatives of surface of the investigated object is conducted. As a result

вертикального променя проведено розрахунок оцінки похибки реконструкції похідних поверхні досліджуваного об'єкта. В результаті аналізу отриманої залежності представлено рекомендації по встановленню експлуатаційних меж кутових відхилень напрямків освітлення та формуванню діапазонів реконструкції похідних.

Лл. 6. Бібліогр.: 16 назв.

УДК 004.45

Кубітна форма опису обчислювальних структур / Tamer Bani Amer, С.В. Чумаченко, І.В. Ємельянов // *Радіоелектроніка і інформатика*. 2016. № 1. С. 47-52.

Розроблені кубітні моделі опису структур і функціональностей для підвищення швидкодії аналізу цифрових пристроїв за рахунок збільшення розмірності структур даних і пам'яті. Введені основні поняття, терміни і визначення, необхідні для реалізації квантових обчислень в практику моделювання комп'ютерних структур. Описані приклади, що підтверджують ефективність використання кубітних структур даних для паралельного виконання операцій над даними.

Лл. 2. Бібліогр.: 9 назв.

УДК 004.45

Дослідження якості збірки додатків під операційну систему Android різними компіляторами / В.В. Нарожний, R.В. Нарожна // *Радіоелектроніка та інформатика*. 2016. № 1. С. 53-56.

Розглянуто проблему оцінки якості збірки додатку трьома компіляторами: Android Development Tools, Android Studio 2 и Visual Studio 2015. Як критерії оцінки обрані швидкодія та розмір отриманих додатків. Для чистоти експерименту, написані три додатки для кожного компілятора. Проведено оцінку додатків на пристрої Galaxy Ace 3 GT-S7272. Зокрема на основі отриманих результатів побудовані графіки залежності за обома критеріями. В результаті аналізу отриманої залежності зроблені попередні висновки про якість зборки додатку трьома компіляторами.

Лл. 11. Бібліогр.: 9 назв.

УДК 519.7

Формалізація неявного процедурного знання / В.М. Левикін, О.В. Чала // *Радіоелектроніка та інформатика*. 2016. № 1. С. 57-60.

Розглянута проблема формалізації явного знання, а також особливості неявного процедурного знання. Запропонована модель такого знання, що містить явну складову в формі послідовностей дій і неявну складову в формі неформалізованих відносин між сутностями предметної області, які задають необхідні і достатні умови для виконання таких дій. Запропоновано підхід до формалізації неявних процедурних знань, заснований на поетапному доповненні явного уявлення формалізованим неявним контекстом предметної області.

Бібліогр.: 10 назв.

of analysis of the got dependence the presented recommendations are on establishment of operating limits of angular rejections of directions of illumination and forming of ranges of reconstruction

Fig. 6. Ref.: 16 items.

UDC 004.45

Qubit description form of computer systems / Tamer Bani Amer, S.V. Chumachenko, I.V. Yemelyanov // *Radioelektronika i informatika*. 2016. № 1. P. 47-52.

Qubit models for describing the structures and functionalities are developed in order to improve the performance of the analysis of digital devices through increasing the dimension of the data structures and memory. The basic concepts, terminology and definitions are Introduced; they are necessary for the implementation of quantum computation in modeling computer structures. Examples, confirming the efficiency of the use of qubit data structures for parallel operations on the data are described.

Fig.2. Ref.: 9 items.

UDC 004.45

The study build quality applications for the Android operating system different compilers / V.Narozhnyy, E.Narozhna // *Radioelektronika i informatika*. 2016. № 1. P. 53-56.

A problem of quality assessing of an application build by three compilers such as Android Development Tools, Android Studio 2 and Visual Studio 2015 has been considered. As evaluation criteria have been selected speed and size of the application. For the integrity of test three applications have been written for each compiler. The evaluation of applications has been done using Galaxy Ace 3 GT-S7272 devices. Also the based obtained results, depended on both criteria, have been plotted. As a result of the received dependence analysis the three compilers build quality has been concluded.

Fig.2. Ref.: 9 items.

UDC 519.7

Formalization of tacit procedural knowledge / V.M. Levykin O.V. Chala // *Radioelektronika i informatika*. 2016. N 1. P. 57-60.

The problem of explicit knowledge formalization is considered. The features of implicit procedural knowledge and a model of such knowledge are proposed. Model contains an explicit component in the form of sequences of actions and implicit component in the form of formalized relationships between entities subject area, that specify the necessary and sufficient conditions for the implementation of such actions. An approach to formalization of implicit procedural knowledge is proposed. The approach is based on step by step externalization of implicit context domain.

Ref.: 10 items.

Методологія оцінки впливу кібератаки на безпеку відеоінформаційного ресурсу в телекомунікаційній системі / В.В. Бараннік, С.А. Підлісний, С.С. Шулгін // Радіоелектроніка та інформатика. 2016. Вип. 1. С. 61-65.

Викладено основні етапи методології дії кібератак на безпеку відеоінформаційного ресурсу. Проведено аналіз сучасних загроз інформаційно-телекомунікаційних систем. Обґрунтована актуальність захисту відеоінформаційного ресурсу. Дана методологія враховує взаємодію операторів, які описують роботу телекомунікаційної системи, з операторами дії DDoS атак. Описано прояв найбільш істотних атак типу "Distributed Denial of Service". Запропоновано основні вимоги для технології кодування, які забезпечують необхідний захист.

Ключові слова – інформаційна безпека, розподілена атака типу "відмова в обслуговуванні", відеокодування, відеоінформаційний ресурс.

Табл. 2. Іл. 2. Бібліогр.: 5 назв.

Methodology of impact assessment of safety cyber-attacks on video information resources in telecommunications system / V. Barannik, S. Podlesny, S. Shulgin // Radioelektronika i informatika 2016. N 1. P. 61-65.

The article describes the main stages of the methodology of action on cyber security video information resource. Modern threats to information and telecommunication systems were analyzed. The actuality of protecting video information resource was described. This methodology takes into account the interaction of the operators that describe the work of the telecommunications system, the operator acts DDoS attacks.

The article describes most important manifestation of the type attacks "Distributed Denial of Service". The article proposes the basic requirements for coding technologies which provide the required protection.

Keywords – information security, distributed attack such as "denial of service", video encoding, video information resource.

Tab. 2. Fig. 2. Ref.: 5 items.