МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

ISSN 0135-1710

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ПРИБОРЫ АВТОМАТИКИ

Всеукраинский межведомственный научно-технический сборник

Основан в 1965 г.

Выпуск 168

Харьков
2014

УДК 62-50

В сборнике представлены результаты исследований, касающихся компьютерной инженерии, управления, технической диагностики, автоматизации проектирования, оптимизированного использования компьютерных сетей и создания интеллектуальных экспертных систем. Предложены новые подходы, алгоритмы и их программная реализация в области автоматического управления сложными системами, оригинальные информационные технологии в науке, образовании, медицине.

Для преподавателей университетов, научных работников, специалистов, аспирантов.

У збірнику наведено результати досліджень, що стосуються комп'ютерної інженерії, управління, технічної діагностики, автоматизації проектування, оптимізованого використання комп'ютерних мереж і створення інтелектуальних експертних систем. Запропоновано нові підходи, алгоритми та їх програмна реалізація в області автоматичного управління складними системами, оригінальні інформаційні технології в науці, освіті, медицині.

Для викладачів університетів, науковців, фахівців, аспірантів.

Свидетельство о государственной регистрации
печатного средства массовой информации КВ № 12073-944ПР от 07.12.2006 г.

Адрес редакционной коллегии: Украина, 61166, Харьков, просп. Ленина, 14, Харьковский национальный университет радиоэлектроники, комн. 321, тел. 70-21-326

СОДЕРЖАНИЕ

БАРАННИК Д.В., БЕКИРОВ А.Э.
КОНЦЕПЦИЯ СТРУКТУРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ С МАСКИРОВАНИЕМ.....4

ЛЕВЫКИН В.М., ВОРОНИН А.А., ГАРЯЧЕВСКАЯ И.В.
РАЗРАБОТКА МОДЕЛИ КОНСТРУКТОРА WEB ФОРМ "ALVOR FORM BUILDER" И ЕЁ РЕАЛИЗАЦИЯ.....11

ГАЛУШКА И.Н., ЩЕРБАК С.С.
ОЦЕНКА ЭФФЕКТИВНОСТИ ИНТЕГРАЦИОННЫХ РЕШЕНИЙ НА ОСНОВЕ ХРАНИЛИЩ ТРИПЛЕТОВ.....18

ЛУГОВОЙ А.В., ПРИТЧИН А.С.
УСОВЕРШЕНСТВОВАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ РАСПРЕДЕЛЕНИЯ ЛЕГИРУЮЩЕЙ ПРИМЕСИ В ПРОЦЕССЕ ВЫРАЩИВАНИЯ СЛИТКОВ КРЕМНИЯ.....24

ОКСАНИЧ А.П., КОГДАСЬ М.Г., АНДРОСЮК М.С.
ИССЛЕДОВАНИЕ СТРУКТУРНЫХ И ОПТИЧЕСКИХ ХАРАКТЕРИСТИК СЛИТКОВ ПОЛУИЗОЛИРУЮЩЕГО GaAs БОЛЬШОГО ДИАМЕТРА.....30

МОСКАЛЕНКО В.В., РЫЖОВА А.С.
ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ С ОПТИМИЗАЦИЕЙ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ.....36

ШКИЛЬ А.С., ФАСТОВЕЦ Г.П., СЕРОКУРОВА А.С.
АВТОМАТИЗАЦИЯ ПОИСКА ОШИБОК ПРОЕКТИРОВАНИЯ В HDL-МОДЕЛЯХ КОНЕЧНЫХ АВТОМАТОВ.....43

БАБЕНКО В.Г., ЗАЖОМА В.М., НЕСТЕРЕНКО О.Б.
МЕТОД ВБУДОВУВАННЯ СТЕГОПОВІДОМЛЕННЯ НА ОСНОВІ КЛЮЧОВОГО ЕЛЕМЕНТА.....53

КОНАХОВИЧ Г.Ф.
ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ В СПЕКТРАЛЬНУЮ ОБЛАСТЬ ИЗОБРАЖЕНИЙ.....59

ХАХАНОВ В.И., ОБРИЗАН В.И., ЗАЙЧЕНКО С.А., ХАХАНОВ И.В.
MQT-АВТОМАТ ДЛЯ АНАЛИЗА БОЛЬШИХ ДАННЫХ.....64

РЕФЕРАТИ.....73

ПРАВИЛА ОФОРМЛЕНИЯ РУКОПИСЕЙ ДЛЯ АВТОРОВ НАУЧНО-ТЕХНИЧЕСКОГО СБОРНИКА.....77

УДК 629.391

Д.В. БАРАННИК, А.Э. БЕКИРОВ

КОНЦЕПЦИЯ СТРУКТУРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ С МАСКИРОВАНИЕМ

Рассматривается использование неравновесного позиционного кодирования в качестве функционального преобразования для числа с встроенной информацией. Обосновывается появление структурной избыточности в процессе неравновесного позиционного кодирования. Предлагается использовать наличие потенциальной избыточности для стеганографического встраивания информации. Разрабатывается стеганографический метод на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающий встраивание и изъятие скрываемой информации. Формулируется правило встраивания информации для структурного стеганографического кодирования.

1. Введение

Одним из возможных путей повышения безопасности информационных ресурсов является использование стеганографических методов скрытия данных в изображении – контейнере.

Наиболее распространенными стеганографическими методами являются алгоритмы непосредственного встраивания информации в элементы пространственно-временного представления изображения - контейнера. Но для таких систем существуют недостатки, обусловленные внесением значительных визуальных искажений в значения пространственно – временных элементов изображения – контейнера и низкой устойчивостью встроенных данных к активным атакам злоумышленника. В связи с этим наиболее актуальным является нахождение новых подходов для разработки альтернативных стеганографических алгоритмов непосредственного встраивания.

Возможным решением проблемы улучшения показателей визуальной устойчивости стеганограммы, а также стойкости к трансформации и атакам является разработка функционального преобразования для элемента с встроенными данными. В качестве кодообразующего функционала, соответствующего требованиям относительно процесса скрытия данных, предлагается использовать кодообразующую функцию для неравновесного позиционного числа. Отсюда, *цель исследований* состоит в разработке метода стеганографического кодирования неравновесного позиционного числа с имплантированным элементом.

2. Разработка метода стеганографического кодирования с маскированием структурной стеганографической избыточности

В процессе реализации функционального преобразования на основе неравновесного позиционного кодирования область исходного изображения, содержащая совокупность видеопоследовательностей, рассматривается как множество неравновесных позиционных чисел $\{A(j)\}$. Здесь неравновесное позиционное число $A(j)$ без имплантации для j-го столбца массива видеоизображения состоит из m элементов:

$$A(j)=\{a_{1,j};...;a_{i,j};...;a_{m,j}\}.$$

Имплантацию в число $A(j)$ предлагается проводить поэлементно, т.е. один элемент b_ξ на позицию γ-го разряда числа $A(j)$. Здесь b_ξ - ξ-й элемент встраиваемой последовательности $B=\{b_1;...;b_\xi;...;b_v\}$, $b_\xi \in [0;\,255]$, $\xi=\overline{1,v}$. В этом случае имплантация задается следующей формулой:

$$A(j)' = A(j) \cup b_\xi, \qquad b_\xi = a'_{\gamma,j}.$$

В результате имплантации, число $A(j)'$ примет следующий вид:

$$A(j)' = \{ a_{1,j};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \},$$

где $A(j)'$ – число с имплантированным элементом $a'_{\gamma,j}$ в γ-й разряд числа; $(m+1)$ – количество элементов в числе с имплантацией.

На следующем этапе число $A(j)'$ с имплантированным элементом кодируется, проводится встраивание скрываемой информации в коде-контейнера. Другими словами, реализуется стеганографическое кодирование или процесс одновременного встраивания информации и построения кода-контейнера. В этом случае значение кода-контейнера, содержащее скрываемую информацию, называется стеганокодом.

Значения стеганокода $N(j)'$ для НП числа с имплантацией определяется по следующей формуле:

$$N(j)' = (\sum_{i=1}^{\gamma-1} a_{i,j}\ V'_{i,j}) + a'_{\gamma,j}V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j}\ V'_{i,j}\ .$$

Здесь $V'_{i,j}$ – весовой коэффициент элемента $a_{i,j}$; j – количество столбцов в массиве фрагмента видеоизображения, $j=\overline{1,n}$; $V'_{\gamma,j}$ – весовой коэффициент имплантированного элемента $a'_{\gamma,j}$.

Значение весового коэффициента $V'_{i,j}$ для элемента $a_{i,j}$, позиция которого в числе $A(j)'$ старше позиции имплантированного элемента $a'_{\gamma,j}$, т.е. $i=\overline{1,\gamma-1}$, определяется на основе выражения:

$$V'_{i,j} = \psi'_{\gamma,j} \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}\ ,$$

где $\psi_{\xi,j}$ – основание $(i;j)$-го элемента числа $A(j)'$ с имплантацией; $\psi'_{\gamma,j}$ – основание имплантированного элемента $b_\xi \le \psi'_{\gamma,j} - 1$.

Весовой коэффициент $V'_{i,j}$ элемента $a_{i,j}$, позиция которого в числе $A(j)'$ младше позиции имплантированного элемента $a'_{\gamma,j}$, т.е. $i=\overline{\gamma+1,m+1}$, вычисляется по формуле:

$$V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}\ .$$

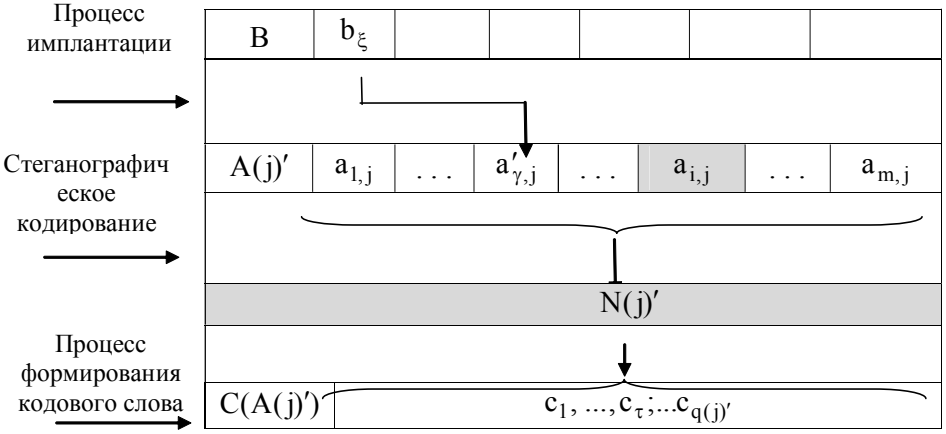
Весовой коэффициент $V'_{\gamma,j}$ имплантированного элемента $a'_{\gamma,j}$, равный накопленному произведению оснований старших элементов числа $A(j)'$, находится с помощью следующего выражения:

$$V'_{\gamma,j} = \prod_{\xi=\gamma+1}^{m+1} \psi_{\xi,j}\ .$$

Обобщив приведенные определения для весового коэффициента $V_{i,j}$, получим следующую систему выражений:

$$V_{i,j} = \begin{cases} \psi'_{\gamma,j} \prod\limits_{\xi=i+1}^{m+1} \psi_{\xi,j}, & \to i=\overline{1,\gamma-1}; \\ \prod\limits_{\xi=\gamma+1}^{m+1} \psi_{\xi,j} & \to i=\gamma; \\ \prod\limits_{\xi=i+1}^{m+1} \psi_{\xi,j}, & \to i=\overline{\gamma+1,m+1}. \end{cases}.$$

В случае такого встраивания фрагмент исходной видеопоследовательности рассматривается, как позиционное число $A(j)' = \{ a_{1,j};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \}$ с имплантированным элементом $a'_{\gamma,j}$, $i=\overline{1,m+1}$. Для числа $A(j)'$ кодовое представление $C(A(j)')$ его



стеганокода $N(j)'$ в неравновесном позиционном базисе формируется в два этапа (рис. 1).

Рис 1. Структурная схема построения кодограммы стеганокода для числа $A'(j)$ с имплантацией

Первый этап включает в себя вычисление стеганокода $N(j)'$, как взвешенного суммирования величин $a_{i,j} V'_{i,j}$ и $a'_{\gamma,j} V'_{\gamma,j}$. Кодограмма $C(A(j)')$ стеганокода формируется на втором этапе для величины $N(j)'$:

$$C(A(j))' = \{c_1, ..., c_\tau, ..., c_{q(j)'}\},$$

где $q(j)'$ – длина кодограммы $C(A(j)')$.

В результате стеганографического кодирования формируются кодовые комбинации, состоящие из двух частей: служебной $\Psi^{(1)}$ и информационной $N(j)'$ (значение стеганокода). Кодовую комбинацию, которая содержит служебную часть $\Psi^{(1)}$ (система оснований) и информационную часть (кодовое представление стеганокода $N(j)'$), будем называть стеганограммой.

Оценим длину $q(j)'$ кодограммы стеганокода $N(j)'$ для числа $A(j)'$ с имплантацией. Значение $q(j)'$ с учетом того, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j}$, будет определяться по формуле:

$$q(j)' = |N(j)'|_2 = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 = [\log_2 \psi'_{\gamma,j} + \sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 \text{ (бит)},$$

где $|N(j)'|_2$ – длина стеганокода $N(j)'$.

Сравним значение $q(j)'$ с длиной $q(j)$ кодограммы кода-контейнера $N(j)$ числа $A(j)$ без имплантированного элемента. Значение $q(j)$ определяется на основе следующего выражения:

$$q(j) = |C(A(j))| = [\ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 \text{ (бит)}.$$

Из сравнения выражений для $q(j)$ и $q(j)'$ можно сделать вывод, что имплантация бита в число $A(j)$ увеличивает длину кодового представления на $(\log_2 \psi'_{\gamma,j})$ бит. Это описывается выражением: $q(j)' - q(j) = \log_2 \psi_{\gamma,j}$.

Отсюда можно заключить, что в процессе формирования стеганокода для числа $A(j)'$ с имплантированным элементом относительно варианта до встраивания вносится структурная стеганографическая избыточность.

Данная избыточность $R(j)_{стег}$ определяется как разность длины $q(j)'$ кодограммы стеганокода числа $A(j)'$ с имплантацией и длины $q(j)$ кодограммы кода-контейнера для числа $A(j)$ без встроенной информации, т.е. $R(j)_{стег} = q(j)' - q(j) \geq 0$.

Теперь оценим величину остаточной структурной избыточности $R(j)_{ост}$, которая образуется в результате формирования стеганокода для числа с имплантацией в неравновесном базисе оснований относительно кодового представления исходной видеопоследовательности. Для этого оценим длину $q(j)_{исх}$ кодового представления исходной видеопоследовательности. Длина $q(j)_{исх}$ кодового представления числа $A(j)$ с постоянным основанием $\psi = 256$ определяется по формуле: $q(j)_{исх} = m \cdot \log_2 256 = 8 \cdot m$ (бит).

Сравним длину $q(j)'$ кодограммы стеганокода $N(j)'$ для числа $A(j)'$ с имплантацией с длиной $q(j)_{исх}$ кодового представления числа $A(j)$ с постоянным основанием $\psi = 256$ без имплантированного элемента. Это описывается выражением: $R(j)_{ост} = q(j)_{исх} - q'(j)$.

Очевидно, что возможность встраивания информации в условиях обеспечения ее скрытности будет обеспечиваться, когда количество структурной избыточности не будет равно нулю, т.е. $R(j)_{ост} = q_{исх} - q(j)' \neq 0$.

Проведем оценку того, как влияет появление стеганографической избыточности на возможность выявления факта встраивания информации. В этом случае необходимо учитывать, что стеганограмма содержит как информационную часть (значение стеганокода $N(j)'$), так и служебную (систему оснований $\Psi^{(1)}$). Отсюда, неавторизированный пользователь имеет доступ к базису оснований $\Psi^{(1)}$, на основе которого сформирован стеганокод $N(j)'$. Для выявления факта встраивания информации неавторизированный пользователь может предпринять следующее:

1. На основе имеющейся в кодограмме системы оснований $\Psi^{(1)}$ существует возможность вычислить длину $q(j)$ кодограммы для кода контейнера $N(j)$, т.е.

$$q(j) = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1.$$

2. Это позволяет установить предполагаемую длину информационной части текущей кодограммы, в результате чего будет считано значение кода $N(j)''$. Однако в действительности передается стеганокод и величина $q(j)$ не будет равна $q(j)'$. Длина кодового представления стеганокода превышает длину исходного кода-контейнера. Поэтому в общем случае считанное значение $N(j)''$ в информационной части кодограммы будет отличаться от исходного значения кода-контейнера, а именно: $N(j)'' \neq N(j)$.

Это приводит к тому, что:

1) реконструкция элементов в исходной видеопоследовательности будет проводиться с ошибками;

2) разница между длинами кодовых представлений стеганокода $q(j)'$ и кодограммы $q(j)$, которая остается не изъятой, будет восприниматься как первые биты служебной части следующей кодограммы $N(j)''$ (рис.2).

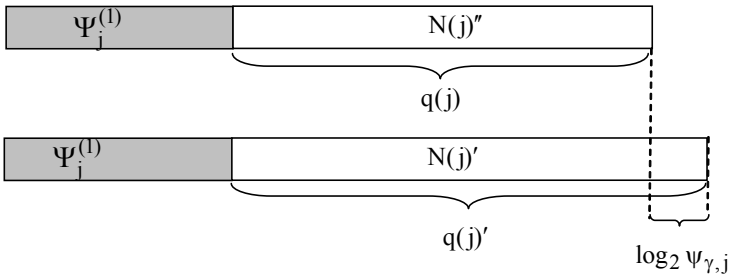


Рис. 2. Кодограммы для ошибочно изъятого стеганокода $N(j)''$ и стеганокода $N(j)'$

Поэтому можно заключить, что появление структурной стеганографической избыточности $R(j)_{стег}$ приводит к тому, что изображение будет декодироваться с наличием существенных искажений. Это позволит злоумышленнику установить факт наличия встроенной информации.

Рассмотрим, как влияет ошибочное значение $N(j)''$ кода-контейнера, считанное из информационной части кодограммы, в условиях, когда:

– с одной стороны, в реальности передается стеганокод $N(j)'$;

– с другой – неавторизированный пользователь будет считывать значение кода-контейнера $N(j)$.

В этом случае вместо того чтобы отобрать $q(j)'$ бит, неавторизированный пользователь выбирает $q(j)$ бит.

Рассмотрим процесс реконструкции элементов исходной видеопоследовательности, представленных как неравновесные позиционные числа в условиях использования ошибочного значения кода-контейнера $N(j)''$. Другими словами, проведем оценку влияния несоответствия длины стеганокода и кода-контейнера на процесс восстановления элементов исходной видеопоследовательности. Рассмотрим реконструкцию i-го элемента j-й видеопоследовательности. Для этого используем выражение:

$$a''_{i,j} = [N(j)''/V_{i,j}] - [N(j)''/\psi_{i,j}V_{i,j}]\psi_{i,j}$$

или

$$a''_{i,j} = N(j)''_i - \left[\frac{N(j)''_i}{\psi_{i,j}V_{i,j}}\right]\cdot\psi_{i,j},$$

где $a''_{i,j}$ – i-й элемент реконструированной видеопоследовательности; $N(j)''_i$ - остаточное значение кода неравновесного позиционного числа для декодирования очередного i-го элемента.

Из анализа этого выражения в условиях, когда

$$N(j)'' > N(j)',$$

следует, что как минимум начиная с некоторой β-й позиции, элементы видеопоследовательности будут обнуляться, т.е. $a''_{i,j} = 0$, для $i = \overline{\beta; m+1}$.

Значит, ошибочно установленная злоумышленником длина информационной части $N(j)''_i$ будет приводить к появлению искажений в процессе восстановления видеоизображения. Данные визуальные искажения могут служить дополнительным источником для стегоанализа.

Поэтому для устранения влияния стеганографической избыточности на возможность проведения атаки злоумышленником, в том числе установления факта наличия встроенной информации, необходимо разработать подход для устранения стеганографической избыточности. Для этого будем проводить локализацию количества избыточности путем маскирования структурной стеганографической избыточности.

Локализацию структурной стеганографической избыточности в процессе формирования стеганокода в неравновесном базисе предлагается осуществлять на основе коррекции длины кодограммы $C(A(j)')$ стеганокода $N(j)'$. Процесс коррекции предусматривает приведение длины кодограммы стеганокода $q(j)'$ к значению длины $q(j)$. В физическом плане реализация коррекции кодограммы заключается в отбрасывании $(\log_2 \psi'_{\gamma,j})$ наименее значимых бит кодограммы $C(A(j)')$, т.е.

$$C'''_j = [N(j)''']_2 = [N(j)'/\psi_{i,j}]_2,$$

где $N(j)'''$ – значение стеганокода, скорректированное в процессе маскирования структурной стеганографической избыточности; $[N(j)''']_2$ – двоичное значение скорректированного стеганокода $N(j)'''$; C'''_j – кодограмма кодового представления скорректированного стеганокода $N(j)'''$.

Как следует из выражения для $R(j)_{стег}$, степень локализации значения стеганокода, а значит и уровень его искажений, будет зависеть от значения основания $\psi'_{\gamma,j}$ встраиваемого элемента. Тогда для обеспечения минимального значения $R(j)_{стег}$ в процессе стеганографического кодирования должно выполняться условие: $(\log_2 \psi'_{\gamma,j}) \to \min$.

Поэтому для уменьшения уровня искажений стеганокода предлагается встраивать элементы в двоичном представлении, т.е. $b_\xi \in [0;1]$. В этом случае основание встроенного элемента будет равно $\psi'_{\gamma,j} = 2$.

Определим длину $q(j)'$ кодограммы стеганокода $N(j)'$ числа $A(j)'$ с имплантацией двоичного элемента. Учитывая, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j} = 2$, величина $q(j)'$ будет определяться по формуле:

$$q(j)' = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 \prod_{i=1}^{m} \psi_{i,j}] + 1 =$$

$$= [\log_2 \psi'_{\gamma,j} + \sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 2 \quad \text{(бит)}.$$

Можно сделать вывод, что имплантация бита в число $A(j)$ увеличивает длину кодового представления стеганокода относительно кода-контейнера на один бит. Количество $R(j)_{стег}$ структурной избыточности будет равно:

$$R(j)_{стег} = q(j)' - q(j) = 1 \quad \text{(бит)}.$$

Следовательно, встраивание двоичного элемента позволяет минимизировать степень несоответствия между значениями стеганокода и кода – контейнера. В этом случае правило локализации будет иметь вид:

$$C'''_j = [N(j)''']_2 = [N(j)'/2]_2.$$

Такой вариант локализации стеганографической избыточности заключается в использовании свойств устойчивости структурных характеристик и структурной избыточности кодов относительно обработки искаженных значений кодов неравновесного позиционного числа. После локализации стеганографической избыточности длина $q(j)''$ кодограммы скорректированного стеганокода $N(j)'''$ будет вычисляться с помощью следующей формулы:

$$q(j)'' = [(\sum_{i=1}^{m+1} \ell og_2 \psi_{i,j})/2] + 1 = q(j).$$

Несмотря на это, искажения в значение стеганокода все равно будут вноситься, причем наибольшим искажениям будут подвергаться младшие элементы неравновесного позиционного числа. Поэтому для повышения устойчивости встроенных данных предлагается размещать один бит скрываемой информации на позицию старшего элемента неравновесного позиционного числа. Вследствие такого встраивания число $A(j)'$ примет следующий вид:

$$A(j)' = \{a'_{1,j}; a_{2,j}; ...; a_{i,j}; ...; a_{m+1,j}\},$$

где $A(j)'$ – число с имплантированным битом $a'_{1,j}$ на позиции старшего элемента; $a'_{1,j}$ – имплантированный бит на позиции старшего элемента числа $A(j)'$, равный $a'_{1,j} = b_\xi$, $a'_{1,j} \in [0; 1]$, где b_ξ – ξ-й элемент встраиваемой последовательности $B = \{b_1; ...; b_\xi; ...; b_\nu\}$; $b_\xi \in [0; 1]$, $\xi = \overline{1, \nu}$; $(m+1)$ – количество элементов в числе $A(j)'$ с имплантацией.

В этом случае вес встраиваемого элемента $V'_{\gamma,j}$ в неравновесном позиционном числе будет наибольшим, т.е. $V'_{\gamma,j} = V'_{1,j} = \max\limits_{1 \le i \le m+1} .\{V'_{i,j}\}$.

Следовательно, встраиваемый элемент будет более устойчив к преобразованиям со стеганокодом. В то же время встраивание скрываемого элемента на старшую позицию в числе исключает влияние его оснований на реконструкцию элементов исходной видеопоследовательности. Действительно, рассмотрим данное свойство на примере i-го элемента j-й видеопоследовательности, т.е

$$a'''_{i,j} = [N(j)''' / V'_{i,j}] - [N(j)''' / \psi_{i.j} V'_{i,j}]\psi_{i.j} =$$

$$= [N(j)''' / \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}] - [N(j)''' / \psi_{i.j} \cdot (\prod_{\xi=i+1}^{m+1} \psi_{\xi,j})]\psi_{i.j} \quad \text{для } i = \overline{2, m+1}.$$

Из анализа данного выражения видно, что значения весовых коэффициентов $V'_{i,j}$ для $i = \overline{2, m+1}$ не содержат основание встроенного элемента $\psi_{1,j}$.

Отсюда, при стеганографическом кодировании неравновесного позиционного числа с имплантированным битом на позицию старшего элемента будет обеспечиваться устойчивость встроенных данных одновременно с минимизацией влияния при реконструкции остальных элементов.

3.Выводы

Разработана стеганографическая система на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающая встраивание и изъятие скрываемой информации на основе соответственно структурного стеганографического кодирования и декодирования.

Обосновано наличие структурной стеганографической избыточности в кодовом представлении стеганокода, образуемой на основе имплантации скрываемой информации в неравновесное позиционное число. Это создает дополнительную возможность для злоумышленника относительно установления факта наличия встроенной информации.

Создано правило встраивания информации для структурного стеганографического кодирования, заключающееся в том, что:

1) один бит скрываемого сообщения встраивается на старшую позицию неравновесного позиционного числа;

2) локализация стеганографической избыточности достигается на основе отсечения младшего бита стеганограммы.

Научная новизна. Впервые спроектирована стеганографическая система на основе непосредственного встраивания скрываемого элемента в видеопоследовательность. В отличие от других стеганосистем обеспечивается одновременное встраивание и изъятие скрываемой информации соответственно в процессе формирования и реконструкции кода-контейнера в неравновесном позиционном базисе оснований. Это обеспечивает встраивание скрываемой информации на основе учета количества структурной избыточности фрагментов видеоизображений.

Список литературы: 1. *Грибунин В.Г., Оков И.Н., Туринцев И.В*. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с. **2.** *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288с. **3.** *Тарасов Д.О., Мельник А.С., Голобородько М.М*. Класифікація та аналіз безкоштовних програмних засобів стеганографії // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка" 2010. № 673.С. 365-374. **4.** *Баранник В.В*. Метод формування функціонала стеганографічного кодування, стійкого до стегано-атак / *В.В. Бараннік, А.Е. Бекіров* //АСУ та прилади автоматики. 2013. Вип. 165. С. 34 – 43.

Поступила в редколлегию 16.09.2014

Баранник Дмитрий Владимирович, студент первого курса факультета КИУ ХНУРЭ. Научные интересы: обработка и передача информации. Адрес: Украина, 61023, Харьков, ул. Ленина, 14.

Бекиров Али Энверович, аспирант ХНУРЭ. Научные интересы: обработка и передача информации. Адрес: Украина, 61023, Харьков, ул. Ленина, 14.

УДК 681.518

В.М. ЛЕВЫКИН, А.А. ВОРОНИН, И.В. ГАРЯЧЕВСКАЯ

РАЗРАБОТКА МОДЕЛИ КОНСТРУКТОРА WEB ФОРМ "ALVOR FORM BUILDER" И ЕЁ РЕАЛИЗАЦИЯ

Описывается разработанный сервис – конструктор web-форм, который позволяет создавать, хранить и редактировать разработанные пользователями web-формы, а также скачивать файлы разметки и обработчиков.

Введение

В разработке web-сайтов, как правило, присутствует этап создания web-форм. Web-форма — это совокупность элементов, позволяющих вводить и редактировать информацию на web-страницах для последующей передачи и обработки php скриптом. Использование конструктора форм позволяет автоматизировать процесс создания web-форм, значительно ускорять и упрощать процесс разработки сайтов.

С помощью конструкторов web-форм владельцы и пользователи сайтов могут создавать такие web-формы: обратной связи, заявок, голосования, подписки, тестирования, оформления заказов на страницах интернет-магазинов и т.д.

Конструктор web-форм должен предоставлять разработчику возможность добавлять элементы на рабочую область, редактировать их свойства и стили и в конечном итоге предоставлять такие исходные файлы как: html, css, php и js.

Анализ предметной области

В настоящее время существует большое количество конструкторов web-форм, которые можно разделить на онлайн сервисы и инсталляционные программы. Из рассмотренных онлайн сервисов можно выделить несколько, наиболее широко известных в интернете, к примеру, MyTaskHelper (http://mytaskhelper.ru) и FormDesigner (http://formdesigner.ru). Оба этих сервиса позволяют создавать web-формы, но они имеют ряд недостатков, кроме того, они платные и оплата взимается за каждую разработанную пользователем web-форму, точнее за ее хранение в базе данных. При этом форма хранится на стороннем сервере, а пользователь получает лишь ссылку на нее. Возникает проблема защиты данных, полученных при обработке полей разработанной web-формы.

Существуют программные средства, лишенные этих недостатков, например, HTMLform (http://htmlform.com/form_builder) или Form Builder (http://csstemplateheaven.com/tools/form_builder). Однако данные сервисы генерируют web-форму в виде набора файлов с разметкой, стилями и обработчиками. Но в присланном архиве находятся некорректные файлы и папки, поэтому структура получается громоздкой и непонятной. На стороне разработчиков, предоставляемых подобные сервисы, информации о пользовательской web-форме после выдачи файлов не остается, и в случае необходимости внесения изменений в разработанную ранее web-форму ее придется создавать всю заново.

Из проведенного анализа можно сделать вывод, что конструктора, позволяющего разрабатывать и редактировать web-форму с генерацией обработчиков для нее, с понятным и

бесплатным интерфейсом, предоставляющего разработчику форм осуществить выбор способа её применения в качестве файлов разметки, стилей и обработчиков либо же только ссылку на форму, в настоящее время не существует.

Постановка задачи

Для обеспечения процессов разработки, редактирования, генерации различных web-форм необходимо разработать такой конструктор, который позволил бы разработчику из реализованных доступных элементов, создать свою web-форму. Разработанная web-форма и сгенерированные обработчики предоставляются пользователю как архив для скачивания файлов разметки, стиля и обработчиков.

В общем случае, задачу разработки конструктора web-форм (K) представим моделью следующего вида:

$$K : I(E, U) \xrightarrow{\text{БД}} O(F, D), \quad (1)$$

где I – входная информация, E – информация о элементах веб-форм, U – информация о пользователе, O – выходная информация, F – архив файлов, D – доступ к созданной форме (ссылка на форму на сервере).

Модель архива файлов представим выражением следующего вида:

$$F = \{f1, f2, f3, f4\}, \quad (2)$$

где f1 – файлы html, f2 – файлы css, f3 – файлы js, f4 – файлы php.

Основными сущностями используемой базы данных являются такие:

$$DB = \{e, s, r, u\}, \quad (3)$$

где e – элементы формы, s – стили, r – регулярные выражения, u – пользователи.

Для обеспечения редактирования, в разрабатываемый конструктор web-форм введём четыре программных модуля: модуль создания формы, модуль редактирования элементов, размещенных на пользовательской форме, модуль генерации файлов html, css, php и модуль архивации файлов.

Взаимодействие введённых модулей и пользователей при разработке web-сайтов представлено на рис.1.

Рис. 1. Взаимодействие программных модулей и пользователей

Реализация модели (1) осуществляется следующим алгоритмом, представленным на рис.2.

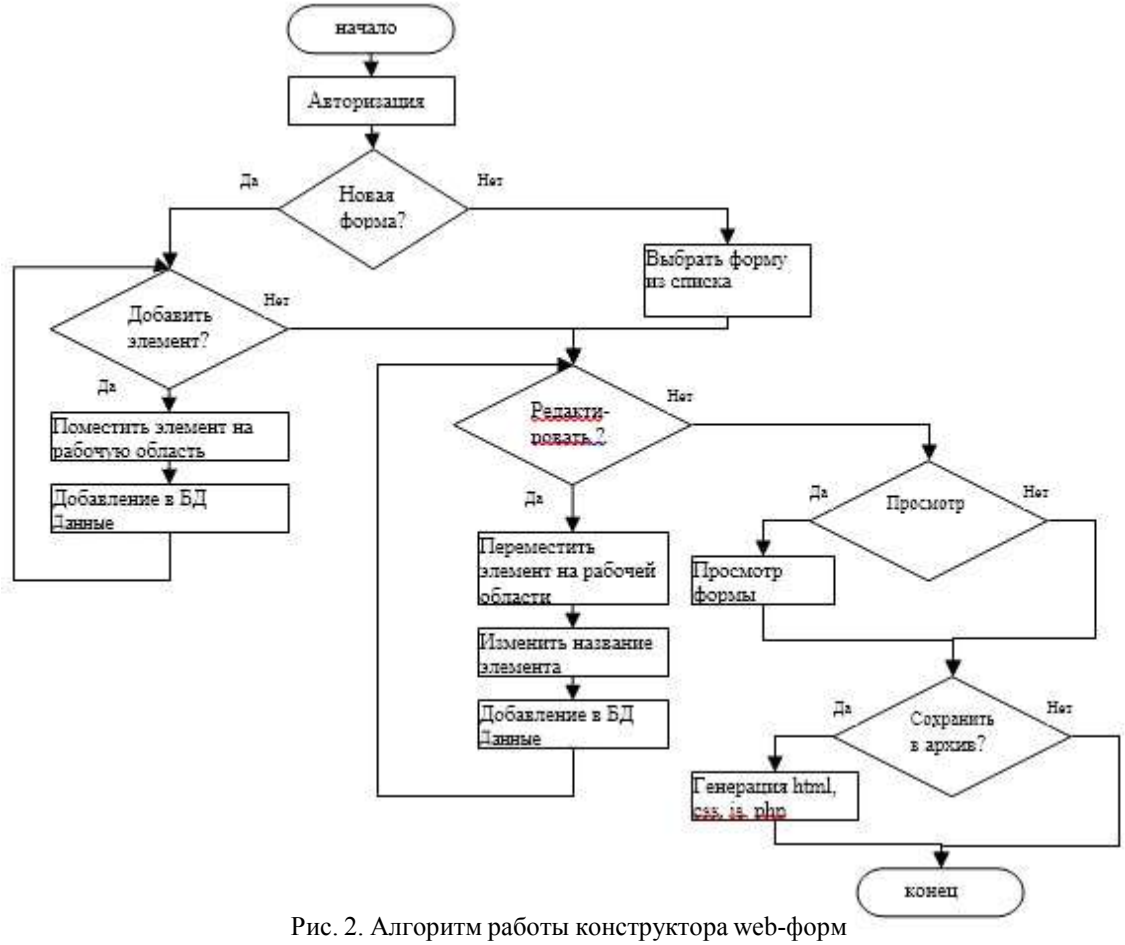


Рис. 2. Алгоритм работы конструктора web-форм

Разработка базы данных

В конструкторе web-форм должна быть предоставлена возможность просмотра и редактирования ранее созданных форм. Для реализации персональной страницы разработчика, которая формируется в следующих таблицах «Личный кабинет», необходимо хранить информацию о разработчиках и их web-формах, за что отвечает несколько таблиц: users, forms, form_elements, form_styles, form_handlers, reg_expressions, pack_forms, которые описаны ниже. Таблица users содержит информацию о разработчиках. Таблица forms содержит информацию обо всех элементах, которые могут быть размещены на форме. Таблица form_elements содержит пять полей: номер, название, описание, открывающий тег, закрывающий тег (по умолчанию NULL). Таблица reg_expressions содержит информацию о регулярных выражениях для валидации значений полей: id, название регулярного выражения, описание с примером применения данного регулярного выражения, регулярное выражение, информация о пользователе, добавившем новое регулярное выражение (по умолчанию user_id = 1 (admin)). Данное поле зарезервировано для возможности добавления своих регулярных выражений пользователями сервиса с возможностью дальнейшего применения их к элементам своей формы.

В конструкторе форм реализованы, на данный момент, следующие регулярные выражения:

– для проверки на корректность (URL) всех полей формы такого типа:

$$/ [^ \ x20-\ xFF] / ; \quad (4)$$

– для проверки поля Email на корректность:

$$/ (\ S +) @ ([a\text{-}z0\text{-}9. \text{-}] +) / Is ; \quad (5)$$

– для проверки поля на заполнение его числами не больше чем 25 символов:

$$/^[0\text{-}9]\{1,25\}\$/. \quad (6)$$

Таблица Forms содержит: номер формы, информацию о пользователе, разрабатывающем данную форму, название формы и ее описание, id выбранного стиля, id обработчика формы, id атрибута кодировки формы, метод отправки данных формы (по умолчанию GET), дату создания формы (по умолчанию текущая дата).

Таблица Pack_forms – сборка элементов формы, содержит: номер формы, номер элемента формы и поле для метки (обязательность заполнения данного поля), индекс регулярного выражения.

Таблица Form_styles содержит информацию о стиле создаваемой формы: номер стиля, название, ссылка на файл css

Таблица form_handlers – обработчики форм. Содержит: номер обработчика, id пользователя, добавившего обработчик (по умолчанию user_id = 1 (admin)), название обработчика, описание, ссылку на файл-обработчик с расширением php.

Таблица Form_enctypes содержит: номер и атрибут формы. Атрибут формы определяет способ кодирования данных при их отправке на сервер.

В процессе проектирования базы данных была разработана её логическая и физическая модель. База данных состоит из 8 таблиц, ее физическая модель представлена на рис.3. База данных была реализована в СУБД MySQL.

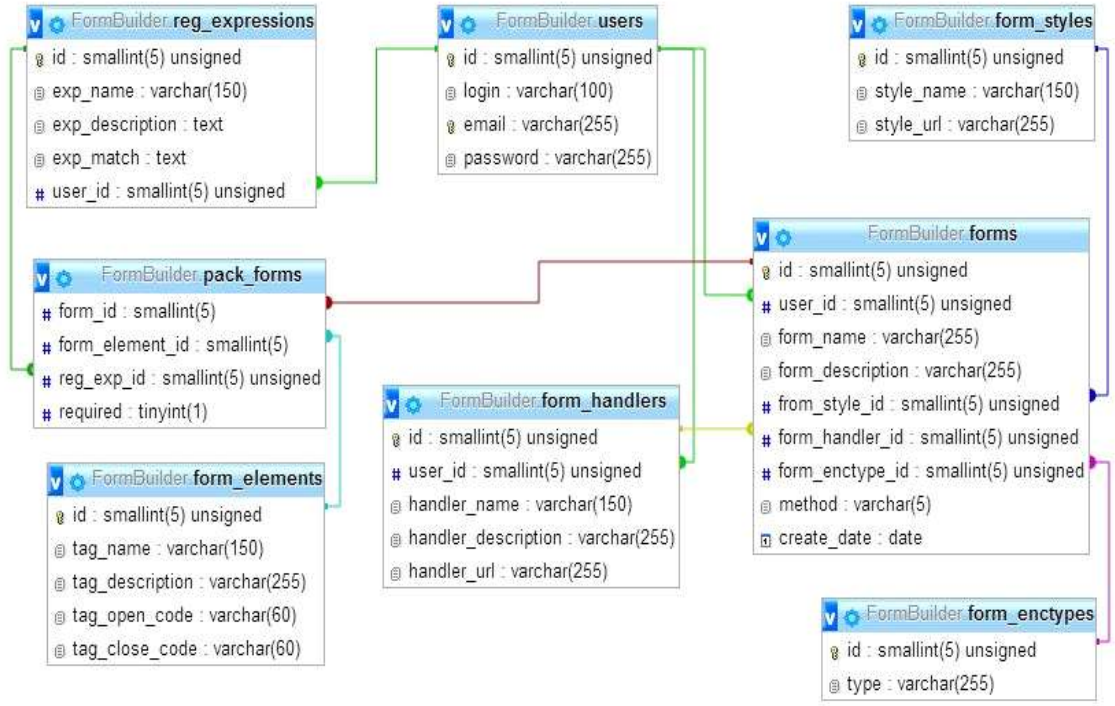


Рис. 3. Физическая модель базы данных

Разработка web-приложения

Для реализации конструктора web-форм «Alvor Form Builder» необходимо выполнить следующие функции:

1. Добавление элементов web-форм из списка в рабочую область.
2. Изменение местоположения элементов на рабочей области.
3. Добавление регулярного выражения к определенному элементу.

4. Изменение стиля web-формы.
5. Сохранение информации о разработанных web-формах.
6. Генерация пользовательской web-формы из рабочей области.

Генерация пользовательской web-формы — это процесс программного формирования архива с набором файлов html, css, php, js. На рис. 4 представлена UML диаграмма сценариев формирования такого архива.

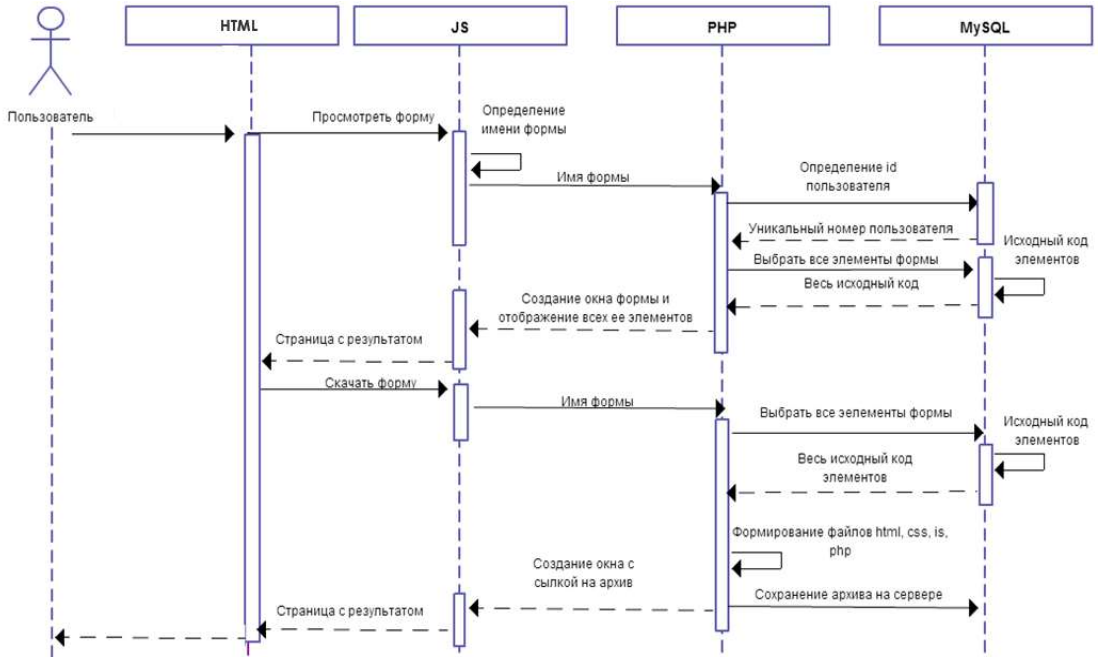


Рис.4. Диаграмма сценариев формирования архива

Разработанный конструктор web-форм имеет удобный и понятный пользовательский интерфейс. На рис.5 представлен интерфейс конструктора форм в виде web-страниц.

Рис. 5. Интерфейс конструктора форм

В левой части конструктора отображен список реализованных на данный момент элементов форм (рис.6), которые пользователь может добавлять на свою форму.

Рис. 6. Элементы форм

Следует отметить, что на рис.6 изменилось меню, позволяющее только авторизированному пользователю возможность разрабатывать или редактировать формы.

Реализованная возможность редактирования элементов позволяет вносить корректировки, например, в такие элементы как checkbox radio и button, добавляя или удаляя количество пунктов, что даёт возможность пользователю включать скачанный код формы без доработок и ручного редактирования (рис.7).

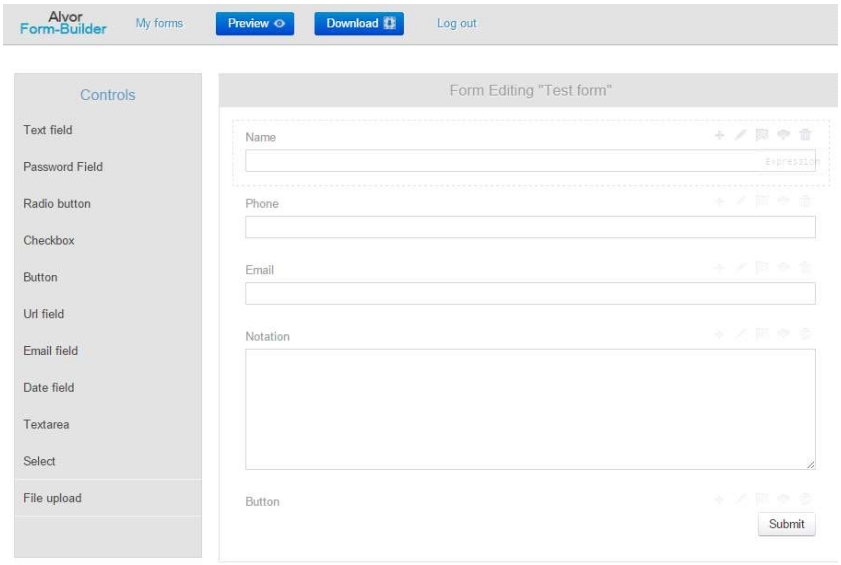


Рис. 7. Пример добавленных элементов на форме

После того, как пользователь разработал свою web-форму, все изменения будут сохранены, и она будет доступна на странице пользователя «Личный кабинет» представленный на рис.8.

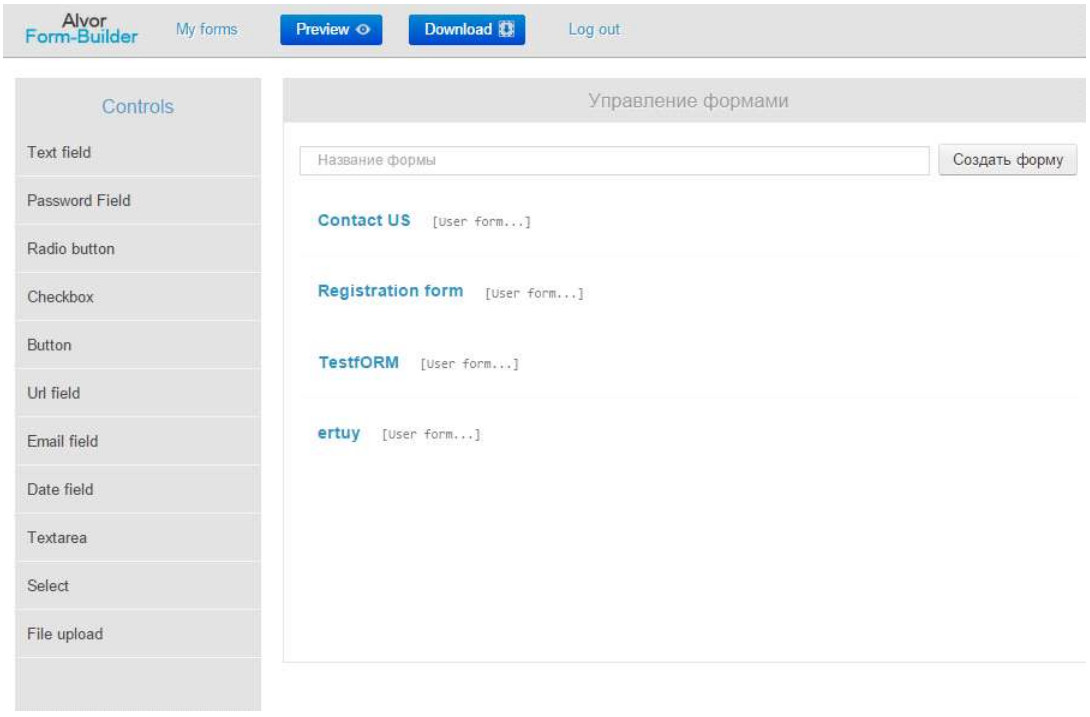


Рис. 8. Страница пользователя “Личный кабинет”

Пользователь, выбрав web-форму из представленного списка, может её предварительно просмотреть, отредактировать и скачать. Для предварительного просмотра полученной формы, перед ее скачиванием, необходимо перейти на пункт Preview, при этом в текущем окне браузера откроется модальное окно с сконструированной пользователем формой (рис.9).

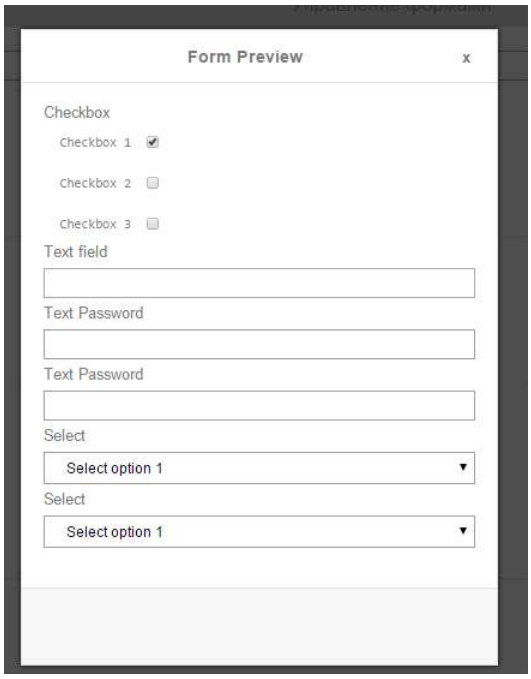


Рис. 9. Предварительный просмотр формы

После того как пользователь убедился, что форма отвечает его требованиям в модальном окне предпросмотра, он нажимает на кнопку Download и сохраняет архив на жестком диске. После этого, разархивировав его, сможет подключить файлы к своему web-сайту или другому web-приложению.

Заключение

В ходе работы над созданием конструктора web-форм был проведен анализ предметной области и существующих конструкторов форм, отмечены их недостатки. Разработана модель и алгоритм работы конструктора форм «Alvor Form Builder», структура базы данных для хранения информации об элементах форм, пользователях и пользовательских формах. База данных реализована в СУБД MySQL. Реализован конструктор web-форм, позволяющий пользователю осуществить онлайн разработку формы, сохранение ее в базе данных и получение набора файлов с разметкой, стилями и обработчиками формы.

Список литературы: 1. *Мельников А.В, Цытович П.Л.* Принципы построения обучающих систем и их классификация. **2**. *Новое* поколение систем контроля версий [Электронный ресурс] – Доступ к ст.: http://www.techinfo.net.ru/docs/Version_Control_Systems.html. **3.** *Мельников А.В, Цытович П.Л.* Модель взаимодействия виртуальных объектов для имитации работы в сети Internet

Поступила в редколлегию 12.07.2014

Левыкин Виктор Макарович, д-р техн. наук, зав. каф. ИУСТ ХНУРЭ. Адрес: Украина, 61023, Харьков, ул. Ленина, 14.

Воронин Александр Александрович, студент факультета компьютерных наук ХНУРЭ.Адрес: Украина, 61023, Харьков, ул. Ленина, 14.

Гарячевская Ирина Васильевна, канд. техн. наук, доц. кафедры информационных технологий в энергетических системах, Харьковский национальный университет имени В.Н.Каразина.

УДК 004.03

И.Н. ГАЛУШКА, С.С. ЩЕРБАК

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНТЕГРАЦИОННЫХ РЕШЕНИЙ НА ОСНОВЕ ХРАНИЛИЩ ТРИПЛЕТОВ

Проводится сравнительный анализ хранилищ триплетов, как основы для построения специализированной системы интеграции данных предприятия. Разрабатывается архитектура системы электронного документооборота на основе хранилищ триплетов и рассматриваются технические аспекты ее внедрения на территориально-распределенном предприятии. Предлагается критерий и методика оценки эффективности интеграционных решений на основе хранилищ триплетов, позволяющие продемонстрировать преимущества и эффективность.

Введение

На сегодняшний день решение проблемы интеграции данных на предприятии приобретает все большую актуальность. Это связано, прежде всего, с увеличением как объемов циркулируемых в информационных системах предприятия данных, так и с увеличением общего числа источников, которые представляют информацию для лиц, принимающих решения. Одним из наиболее эффективных подходов к интеграции корпоративных источников является применение методов и средств парадигмы связанных данных предприятия (Linked Enterprise Data, LED). В рамках этой парадигмы в качестве интеграционных компонентов выступает промежуточное программное обеспечение на основе хранилищ триплетов (Triple Store) или квадов (Quad Store), обеспечивающих унифицированный подход для организации межсистемного взаимодействия и эффективного доступа и обработки иерархически организованных данных.

Современные предприятия для автоматизации своих бизнес-процессов используют различные информационные системы, которые зачастую не интегрированы не только между собой, но и с системой электронного документооборота предприятия, что значительно снижает эффективность работы предприятия в целом, в связи с чем создание эффективных интеграционных решений является задачей актуальной и целесообразной.

Целью работы является повышение эффективности процесса интеграции новых источников корпоративных данных путем разработки архитектуры информационного пространства предприятия на основе хранилищ триплетов и критериев оценки эффективности интеграционных решений с помощью показателей временных затрат. Поэтому к задачам исследования относятся:

– сравнительный анализ хранилищ триплетов, как основы для построения систем электронного оборота и информационного пространства территориально-распределенного предприятия.

– формализация процесса оценки эффективности интеграционных решений на основе критериев временных затрат.

– разработка методики и исследование эффективности интеграционных решений на основе связанных данных.

1. Сравнительный анализ хранилищ триплетов

На сегодняшний день существует множество способов для хранения данных и средств их обработки, начиная с хранения данных в виде текстовых файлов, что быстро в реализации, но неудобно при дальнейшей их обработке, и заканчивая использованием баз данных со своими СУБД. Множество способов организации хранения данных зачастую приводит к тому, что данные, требуемые для управления бизнес-процессами, находятся в различных источниках с разнообразными средствами работы с ними [1].

В современных предприятиях роль промежуточного звена между источниками корпоративных данных и программой их обработки выполняют хранилища данных (ХД), аккумулируя срезы аналитических данных и предоставляя унифицированный интерфейс доступа к

ним. Рассмотрим реализацию хранилищ на основе парадигмы связанных данных. В рамках этой парадигмы минимальной единицей хранения информации является триплет, или в более продвинутых версиях соответствующего программного обеспечения четырехэлементная структура – квад.

Триплеты являются основой построения предложенной консорциумом W3C (World Wide Web Consortium) модели представления данных Resource Description Framework (RDF) [2], предназначенной для записи утверждений о ресурсах различной природы в виде, пригодном для машинной обработки. RDF является частью концепции Семантической Паутины (Semantic Web). Для обработки RDF-данных используются различные языки запросов. Языком запросов, рекомендуемым W3C, является SPARQL Protocol and RDF Query Language (SPARQL) [3].

Множество RDF-утверждений создают ориентированный граф, в котором вершины – это субъекты и объекты, а ребра помечены предикатами. Однако RDF-граф, взятый в отдельности, не раскрывает семантику описываемой предметной области. Для этой цели необходимы дополнительные средства. Одним их таких средств является RDF Schema (RDFS) – специальный словарь для RDF, предназначенный для определения таксономий классов, свойств [4].

Исходя из изложенного следует, что RDF и триплетная модель хранения связанных данных предоставляют гибкие и унифицированные средства для хранения распределенных иерархически-организованных данных.

Для хранения триплетов связанных данных применяются специализированные хранилища триплетов [5].

Проведем сравнительный анализ функциональных возможностей этих хранилищ.

Хранилища триплетов можно разделить на две основные группы (рис. 1):

1) реализованные как независимые решения (автономные);

2) являющиеся компонентом комплексной семантической системы хранения распределенных данных.

Примеры автономных решений: AllegroGraph, BigOWLIM и PelletDb.

Система AllegroGraph является наиболее развитым решением этого класса. Она широко используется такими средствами, как TopBraid Composer (редактор онтологий), RacerPro (механизм вывода на языке OWL DL) и другими. Приведем ее характеристику.

Архитектура AllegroGraph включает три уровня: памяти, серверный и клиентский. На уровне памяти находится RDF-хранилище AllegroGraph RDF Store. На серверном уровне находятся компоненты, обеспечивающие доступ различных платформ (Direct, HTTP, Sesame, SPARQL) к RDF-данным через общие серверные сервисы (Common Server Services). Клиентскую часть образуют средства создания интерфейсов (C#, Lisp, Java, Sesame, Jena, Clojure, Python, HTTP). Система AllegroGraph обладает хорошей информационной емкостью. Ее бесплатная версия способна хранить и обрабатывать до 50 миллионов триплетов [6].

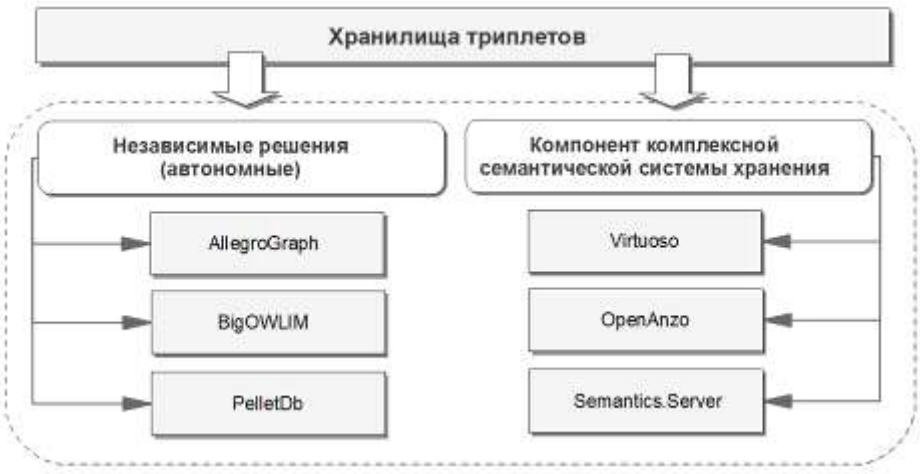


Рис. 1. Классификация хранилищ триплетов

Примерами второй группы хранилищ являются системы Virtuoso, OpenAnzo и Semantics.Server. Наиболее мощный из масштабируемых представителей этой группы – система Virtuoso [7]. Данная система имеет бесплатную версию. Универсальный сервер Virtuoso состоит из модулей однородных хранилищ и модулей виртуальных баз данных. Модули однородных хранилищ обеспечивают хранение данных в XML-формате, в реляционном виде (SQL-формате), в RDF-формате и в полнотекстовом виде. Модели виртуальных баз данных выполняют роль СУБД и создают на основе данных, хранящихся в однородных хранилищах, полнофункциональные базы данных следующего назначения: XML-базы данных, хранилища триплетов в формате RDF, реляционные базы данных, веб-сервисы и полнотекстовые базы. Сервер Virtuoso обеспечивает взаимодействие с компьютерными сетями (Internet/Intranet/Extranet) через большое количество платформ: ODBC, JDBC, OLEDB, .NET, HTTP, SOAP, SPARQL и другие [8].

С помощью драйверов ODBC и JDBC универсальный сервер может взаимодействовать с достаточно большим количеством реляционных СУБД: Oracle, SQL Server, Progress, Sybase, CA–Ingress, Informix, DB2 и другими. Наконец, через серверные расширения сервер может взаимодействовать с приложениями, разработанными на платформах Mono, .NET, Java, C, C++ и прочих, в целях импорта/экспорта логики, содержащейся в их классах и функциях. Таким образом, Virtuoso с полным основанием может считаться комплексной системой хранения, так как, помимо RDF-данных, она обеспечивает хранение и интеграцию данных в других наиболее популярных форматах [9].

В этом плане Virtuoso как основа для интеграционного решения выглядит более предпочтительной, чем система AllegroGraph. Кроме того, Virtuoso обладает высокой производительностью при работе с RDF–данными. Это подтверждается тестовыми оценками производительности различных систем хранения при обработке системой SPARQL-запросов, которые периодически проводятся в Берлинском университете Фрая (Berlin Freie University) на наборах тестов Berlin SPARQL Benchmark. Данные тесты являются ориентиром для сравнения производительности различных систем хранения связанных данных, систем отображения реляционных баз данных в RDF и SPARQL-приложений, ориентированных на другие типы данных [10].

Virtuoso позволяет реализовать гибридный подход к организации хранения данных [11], сочетающий реляционные базы данных для отображения нормализованных данных о событиях, XML-документы, отображающие политики безопасности, шаблоны атак, инциденты и т.д., и хранилища триплетов, позволяющие работать с онтологиями [9].

Таким образом, проведенный анализ хранилищ триплетов показал, что Virtuoso, являющаяся комплексной системой хранения разнородных данных, на наш взгляд, является наилучшим выбором для поставленной цели, так как она позволяет обеспечить высокопроизводительную основу для разработки интеграционных решений для совместного использования реляционных баз данных, XML-баз данных и хранилищ триплетов.

2. Архитектура информационного пространства территориально-распределенного предприятия на основе хранилищ триплетов

Современные предприятия характеризуются территориально-распределенной структурой, что выдвигает к информационным системам предприятия специфические требования по хранению, доступу и обработке корпоративных данных. Рассмотрим унифицированную инфраструктуру предприятия в виде набора унаследованных информационных систем (УИС). Коммуникационный интерфейс взаимодействия либо отсутствует, либо слабо развит и представляет собой точечное решение интеграционной задачи. В рамках такого подхода, в работах [12-13] рекомендуется создавать интеграционное информационное пространство предприятия (ИПП) на основе сервисной шины с разработкой интеграционных брокеров для подключения источников данных различного типа.

С учетом сказанного выше архитектуру информационного пространства предприятия построим на основе хранилищ триплетов.

Пусть $XT_1,...,XT_n$ – хранилища триплетов, которые обеспечат унифицированное решение для реализации процессов системной интеграции, хранения документов и их индекса, ССИ КД – специализированная система интеграции корпоративных данных, выполняющая

функции единого разноформатного и структурного интеграционного брокера, ESB – сервисная шина предприятия, обеспечивающая общую систему сообщений на основе протокола SPARQL, управление доступом и маршрутизацию сообщений, СЭД – система электронного оборота, обеспечивающая обработку и ввод документов. Тогда архитектуру информационного пространства территориально-распределенного предприятия с встроенной системой электронного документооборота на основе хранилищ триплетов представим на рис. 2.

Рассмотрим более подробно специализированную систему интеграции корпоративных данных. Эта система представляет собой множество процедур преобразования данных источников в информационное пространство предприятия на основе шаблонов с адаптивным интерфейсом доступа. В качестве шаблонов используются разрабатываемые специалистом по автоматизации бизнес-процессов предприятия структурно-логические схемы добавляемых в ИПП источников в виде частично-определенных схем RDF с правилами интерпретации структурных компонентов источников.

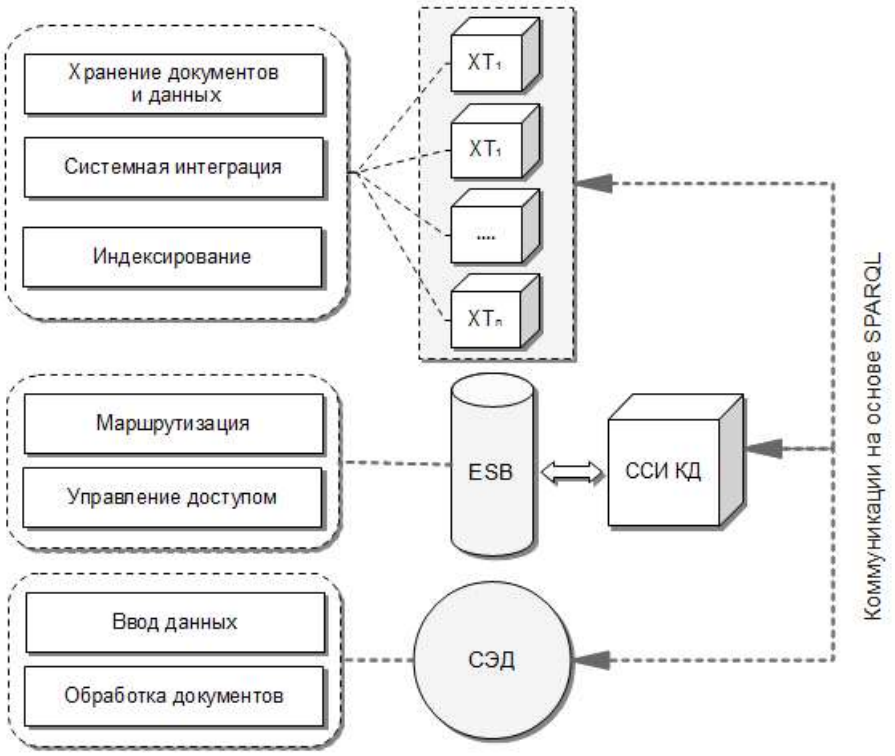


Рис. 2. Архитектура ИПП со встроенной системой электронного документооборота на основе хранилищ триплетов

Таким образом, с учетом внедрения в ИПП на основе хранилищ триплетов специализированной системы интеграции корпоративных данных архитектура ИПП может стать формальным базисом для разработки критериев эффективности интеграционных решений в территориально-распределенных предприятиях.

3. Оценка эффективности структурированности корпоративного документа

Для оценки производительности интеграционного решения рассмотрим задачу интеграции (рис. 3) источников данных (ИД) унаследованных информационных систем С в единое интеграционное пространство (ЕИП) предприятия на основе специализированной системы интеграции (СИ) корпоративных данных и показателей временных затрат на выполнение транзакций в УИС t и в СИ t‘. В качестве интегрируемых в ЕИП выступают базы данных некоторого типа, например, реляционные, что не уменьшает общности рассуждений и служит лишь для упрощения рассуждений об оценке производительности.

Пусть УИС предприятия осуществляет множество транзакций по обработке данных в ХД, в котором хранятся данные УИС. Тогда УИС представим как множество транзакций по доступу и обработке данных к ХД с помощью следующего выражения:

$$C^{ХД} =< TR^{ХД} >, \quad (1)$$

здесь $TR = \{L_1,...,L_m\}$, где $L_1,...,L_m$ – множества операторов языка манипулирования данными, связанных и последовательно выполняемых в рамках одной транзакции доступа к ХД.

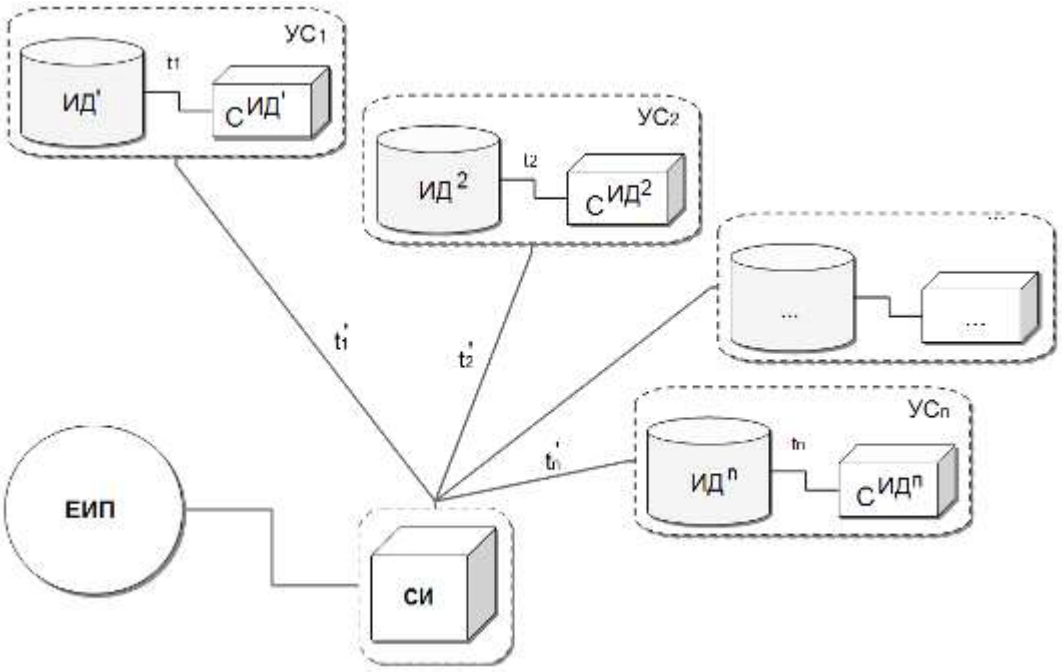


Рис. 3. Формальное представление задачи интеграции корпоративных данных на основе специализированной системы интеграции

Производительность транзакций $УС^{ХД}$ будем рассматривать как сумму времен выполнения t операторов L транзакции TR и представим в виде следующего выражения:

$$t^{TR}_{УС^{ХД}} = \sum_{j=1}^{m} t_j^{L_j^{УС^{ХД}}}. \quad (2)$$

Далее $УС^{ХД}$ рассмотрим как источник данных для информационного пространства предприятия, поэтому если это не будет приводить к противоречиям, будем рассматривать $УС^{ХД}$ и ИД как синонимические понятия.

Производительность интеграционного решения (ИР) выразим аналогично (2) как множество единиц времени выполнения аналогичных транзакций через ИР, представленное в виде СИ, на этом источнике данных и определим в виде следующего выражения:

$$tr^{TR}_{ИД^{ХД}} = \sum_{j=1}^{m} t_j^{L_j^{ИД}}. \quad (3)$$

Общую производительность УИС С выразим как сумму производительностей выполняемых УИС транзакций с помощью следующего выражения:

$$\xi^C = \sum_{i=1}^{p} t_i^{TR^C}. \quad (4)$$

Общую производительность ИР в виде СИ представим в виде следующего выражения:

$$\xi^{ИР} = \sum_{i=1}^{p} t_i^{TR^{ИР}} . \quad (5)$$

Эффективность решения ИР ξ^g рассмотрим как отношение производительности решений УИС и ИР и представим в виде следующей оценки:

$$\xi^g = \frac{\xi^{УС}}{\xi^{ИР}} . \quad (6)$$

Очевидно, что чем более ξ^g приближается к единице, тем эффективнее интеграционное решение.

С учетом сказанного выше, критерий оценки эффективности интеграционных решений на основе показателей временных затрат представлен с помощью формулы (6), что с учетом (1)-(5) формально представляет процесс оценки эффективности интеграционных решений на основе связанных данных.

Выводы

Предложена архитектура информационного пространства территориально-распределенного предприятия со встроенной системой электронного документооборота на основе хранилищ триплетов. Данная архитектура позволяет осуществлять межсистемные взаимодействия унаследованных информационных систем предприятия и ориентирована на хранение распределенных корпоративных данных.

Формализован процесс и предложена методика оценки эффективности интеграционных решений на основе критериев временных затрат для обеспечения возможности отслеживания изменения производительности этих решений в зависимости от использования различных типов транзакций по обработке связанных данных источников.

Предложен критерий оценки эффективности интеграционных решений на основе связанных данных, который базируется на использовании показателей временных затрат, для обеспечения объективной оценки производительности этих решений.

Список литературы: 1. *Деревянко А.В*. Концепция хранилищ данных в системе управления нанотехнологическими процессами // Системи обробки інформації. 2010. Вип. 2 (83). С. 78-83. **2.** *Resource* Description Framework (RDF): Concepts and Abstract Syntax. W3C Recommendation 10 February 2004. http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/ **3.** *SPARQL* Query Language for RDF. W3C Recommendation, 15 January 2008. http://www.w3.org/TR/rdf-sparql-query. **4.** *RDF* Vocabulary Description Language 1.0: RDF Schema. W3C Recommendation 10 February 2004. http://www.w3.org/TR/rdf-schema/. **5**. *Triplestore*. Wikipedia. http://en.wikipedia.org/wiki/Triplestore. **6.** *AllegroGraph* 4.9. http://www.franz.com/agraph/allegrograph/. **7.** *Virtuoso* Universal Server. http://virtuoso.openlinksw.com/. **8.** *Open* Link Software, - http://www.openlinksw.com/Donald E. Knuth, Tracy L. Larrabee, and Paul M. Roberts. Mathematical Writing. Mathematical Association of America, 1989. http://www-csfaculty.stanford.edu/knuth/klr.html. **9.** *Котенко И. В*., *И. Б. Саенко, О. В. Полубелова*. Перспективные системы хранения данных для мониторинга и управления безопасностью информации, Тр. СПИИРАН. 2013. № 25. С. 113-134. **10.** *BSBM* V3 Results (February 2011). http://wifo5-03.informatik.unimannheim.de/bizer/berlinsparqlbenchmark/results/V6/index.html. **11.** *Kotenko I., Polubelova O., Saenko I.* The Ontological Approach for SIEM Data Repository Implementation // 2012 IEEE International Conference on Internet of Things. Besanзon, France, November 20-23, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P.761-766. **12.** *Шапелл Д.* ESB - Сервисная Шина Предприятия: Пер. с англ. СПб.:БХВ-Перегбург.2008. 368 с. **13.** *Завгородний В.В., Щербак С.С.* Единое информационное пространство производственных предприятий на основе связанных данных / / Системи обробки інформації. 2013, вип. 2 (109). С. 275-278.

Поступила в редколлегию 25.08.2014

Галушка Илона Николаевна, ассистент кафедры информационно-управляющих систем Кременчугского национального университета им. Михаила Остроградского. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, E-mail: ilona.galushka@gmail.com, тел.: (05366) 3-01-57.

Щербак Сергей Сергеевич, канд. техн. наук, старший научный сотрудник, доцент кафедры информационно-управляющих систем Кременчугского национального университета им. Михаила Остроградского.Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 3-01-57.

УДК 621.315.592

А.В. ЛУГОВОЙ, А.С. ПРИТЧИН

УСОВЕРШЕНСТВОВАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ РАСПРЕДЕЛЕНИЯ ЛЕГИРУЮЩЕЙ ПРИМЕСИ В ПРОЦЕССЕ ВЫРАЩИВАНИЯ СЛИТКОВ КРЕМНИЯ.

Анализируется внедрение легирующей примеси в слиток при изменяющейся со временем скорости роста слитка. Усовершенствуется модель легирования слитка кремния. Предлагается уточненное аналитическое выражение для расчета легирующего профиля, которое может использоваться по диапазону типичных параметров роста слитка диаметром 150 – 300 мм.

1. Введение

Легирование является основным технологическим процессом получения полупроводников заданного типа проводимости, заданного удельного сопротивления и заданной концентрации носителей заряда. Его осуществляют в процессе либо выращивания полупроводников из расплава, либо изготовления структур из газовой фазы. Если распределение лигатуры в случае легирования из газовой фазы определяется сравнительно просто, то при легировании из расплава на процесс влияет множество факторов, которые сложно поддаются учету.

В результате этого распределение лигатуры по длине слитка имеет определённую неравномерность. Это приводит к необходимости выполнения операции отторцовывания, суть которой заключается в обрезке слитка с обеих сторон таким образом, чтобы на всей оставшейся длине параметры, определяемые легированием (например, удельное сопротивление), находились в границах заданных значений.

Наибольее влияет на распределение легирующей примеси (лигатуры) температура расплава и параметры выращивания, например, частота вращения тигля и скорость выращивания. Под влиянием системы регулирования диаметра слитка скорость выращивания изменяется со временем. Эти колебания вызывают неоднородное распределение лигатуры в слитке.

Влияние скорости выращивания на распределение примеси в слитке было в работе [1] (так называемая модель БПС). Недостатком данной модели является то, что учитывает только устойчивое состояние, и ее применение возможно только при постоянной скорости роста. Распространение лигатуры в пределах расплава зависит от его гидродинамического течения (потока расплава). Этот поток происходит из-за совместного воздействия вращения слитка и его роста. В модели БПС осевой компонент потока жидкости аппроксимируется по выражению, которое описывает поток на границе слиток/расплав. В результате авторы работы [1] получили аналитическую формулу для расчета эффективного коэффициента распределения лигатуры.

Однако когда скорость роста слитка в процессе выращивания изменяется, необходимо рассматривать всю систему уравнений Навье-Стокса с временной зависимостью для потока в расплаве.

Чтобы определить распределение лигатуры в процессе выращивания слитка с учетом возмущающих факторов, вызванных вращением слитка и тигля, необходимо усовершенствовать модель БПС. В результате можно получить математический аппарат для более точного определения оптимальных параметров технологического процесса выращивания, приводящих к равномерному распределению лигатуры по длине и диаметру слитка и, как следствие, уменьшению потерь при операции отторцовки.

Целью работы является усовершенствование модели распределения лигатуры по длине слитка кремния, которая в отличие от существующих должна учитывать влияние колебания скорости выращивания и повышать точность расчета профиля распределения лигатуры.

2. Материал и результаты исследований

В модели БПС граница слиток/расплав рассматривается как плоский бесконечный диск, вращающийся на полубесконечном расплаве. Для представления нижней части тигля вводится стационарный диск, параллельный вращающемуся диску. Тогда расплав будет ограничен по глубине, но бесконечен по ширине. В работах [2,3] был выполенен численный расчет относительно потока с временной зависимостью в конечном тигле.

Рассмотрим уравнения Навье-Стокса, уравнение непрерывности и уравнение диффузии:

$$\frac{\partial u}{\partial t} + u \cdot \nabla u = -\frac{1}{\rho}\nabla p + \nu \nabla^2 u, \tag{1}$$

$$\nabla \cdot u = 0, \tag{2}$$

$$\frac{\partial C}{\partial t} + u \cdot \nabla C = D\nabla^2 C, \tag{3}$$

где u – скорость потока в расплаве; p/ρ – отношение давления к плотности; ν – кинематическая вязкость; C – концентрация примеси; и D – коэффициент диффузии примеси; ∇ – оператор набла.

Так как слиток выращивается из расплава, поток течёт через границу слиток/расплав. Это означает, что границу нужно моделировать как пористый диск. Рост слитка может быть представлен универсальным всасыванием, применимым к пористому диску. Поток течёт в расплаве между стационарным и вращающимся диском, через который происходит всасывание. На границе тангенциальное движение жидкости такое же как в диске. Если слиток вытягивают из расплава с определенной скоростью роста, то позиция границы не меняется. Осевой поток через границу будет иметь такое-же значение, как скорость роста слитка f. В нижней части тигля все компоненты скорости потока исчезают.

Во время роста компоненты перераспределяются между жидкой и твердой фазой из-за эффекта сегрегации. Лигатура отталкивается от расплавленной стороны границы расплав/слиток. Она рассеивается назад в расплав, устанавливая градиент концентрации примеси. Предположим, что концентрация в твердой фазе C_S пропорциональна концентрации в расплаве на границе расплав/слиток. Введем константу пропорциональности в качестве равновесного коэффициента распределения k_0. Концентрация на границе расплав/слиток определяется выражением:

$$(1-k_0)Cf + DC_Z = 0,\ z = 0\ , \tag{4}$$

где C_Z обозначает производную C относительно оси z для цилиндрической системы координат с $C_Z = 0$ на границе. В нижней части тигля концентрация C_L является постоянной. Тогда эффективный коэффициент распределения, который представляет отношение концентрации лигатуры в твердой фазе и в жидкости, на растоянии от границы можно записать в виде:

$$k_e = C_S / C_L\ . \tag{5}$$

Предположим, что первоначально жидкость и диски находятся в покое и что концентрация примеси однородна и равна C_L по всему расплаву. С началом вращения диска его угловая скорость увеличивается до значения ω и затем остается постоянной. В этом случае рост слитка можно рассматривать как всасывание, происходящее через пористый вращающийся диск.

С учетом того, что скорость потока в расплаве u и концентрация примеси C берутся осесимметричными, можно сделать предположение [4] о том, что осевая скорость w радиально независима, является функцией z и t. Следовательно, радиальные и азимутальные скорости u и υ могут быть записаны как радиус r, умноженный на функции z и t. Таким образом, можно сделать вывод, что концентрация лигатуры в расплаве также является радиально независимой. В этом случае вся система частичных дифференциальных уравнений, граничных и начальных условий может быть уменьшена до системы, включающей

только независимые переменные z и t, что позволяет выполнить численное решение системы нелинейных уравнений второго порядка.

Записав уравнение сохранения энергии в безразмерной форме, можно видеть, что в него вошли два безразмерных значения: число Рейнольдса (которое является критерием подобия течения вязкой жидкости) $R = \omega d^2 / \nu$ и число Шмидта (которое является критерием подобия для течений жидкости, где наблюдаются одновременно как переносы вещества (лигатура), так и вязкие эффекты) $Sc = \nu / D$. Здесь ω – угловая скорость слитка, d - расстояние между границей и нижней частью тигля, ν – кинематическая вязкость расплава, D - коэффициент диффузии лигатуры. В качестве граничных условий возмем безразмерный равновесный коэффициент распределения k_0 и безразмерный параметр всасывания *a*, который связан со скоростью роста слитка f выражением:

$$a = f\omega^{-1/2}\nu^{-1/2}. \qquad (6)$$

В этом случае предлагаемая авторами усовершенствованная модель будет отличаться от аналогичных, например от модели, предлагаемой в работе [1], тем, что:

– модель остается зависимой от времени;

– модель более качественно описывает распределения лигатуры вследствие учета влияния нижней части тигля;

– устраняется много приближений динамики жидкости.

Основой усовершенствованной модели является моделирование потока расплава с лигатурой как потока, который возникает из-за вращающегося диска (зона кристаллизации) и через который происходит всасывание. Ранее предлагаемые модели [2,3] использовали суммирование потоков, что не совсем корректно. Кроме того, вместо представления осевой скорости алгебраическим приближением, что может быть допустимо только около границы тигля, решаются уравнения Навье-Стокса в цифровой форме, это позволяет получить решение по всей области.

Если рассматривать поток, на который влияет диск, вращающийся на полубесконечном носителе, то этот поток заставляет жидкость оттягиваться к диску (граница слиток/ расплав) от тела жидкой фазы и затем выбрасывается наружу центробежной силой. В основном изменение состаяния расплава происходит в пределах тонкого пограничного слоя зоны кристаллизации в районе вращающегося слитка. Объем расплава не вращается, а медленно перемещается к кристаллу.

Ситуация более усложняется при введении второго диска для представления нижней части тигля. Тонкие пограничные слои существуют около *обоих* дисков. Около слитка и в этом случае присутствует центробежный отток. Около нижней части тигля формируется сложный поток, который относится к входящему скручиванию. Остаток от потока, в базовой области, очень близок к остатку в твердом теле. Он вращается и перемещается к вращающемуся слитку, таким образом обеспечивая перемещение расплава к слитку.

Скорость вращения ω_c увеличивается с увеличением параметра всасывания a (или скорости роста слитка f), когда a = 0, $\omega_c(0) = 0.313\,\omega$, где ω - угловая скорость слитка.

В том случае, если число Рейнольдса достаточно велико, что типично для расплава кремния, толщина гидродинамического пограничного слоя становится пропорциональной $R^{-1/2}$. Таким образом, для данной вязкости ν и расстояния d, пограничные гидродинамические слои пропорциональны $\omega^{-1/2}$. С увеличением параметра всасывания толщина слоев изменяется.

Определяющие уравнения для концентрации лигатуры C в расплаве кремния включают четыре безразмерных коэффициента:

– равновесный коэффициент распределения k_0;

– число Рейнольдса R;

– число Шмидта Sc;

– параметр всасывания a.

Рассмотрим влияние этих коэффициентов на эффективный коэффициент распределения k_c . Представим нормализованное расстояние $\bar{z} = z/d$ от границы слиток/расплав и пусть $C(\bar{z})$ будет концентрацией лигатуры в расплаве при постоянной скорости выращивания слитка. Нормализованная функция концентрации может быть записана в виде:

$$D(\bar{z}) = (C(\bar{z}) - C_L)/(C(0) - C_L), \tag{7}$$

откуда с учетом (4) и (5) можно записать:

$$k_e = k_0/(k_0 + (1 - k_0)e^{-\bar{\Delta}}), \tag{8}$$

где

$$\bar{\Delta} = -\ln[1 + aScR^{1/2}/D_z^-(0)] \ . \tag{9}$$

Можно видеть, что функция $D(\bar{z})$ зависит от R, Sc и a, но не от k_0 . Таким образом, анализируя выражение (8), можно определить аналитическую зависимость k_e от k_0 . Как было записано выше, толщина гидродинамических пограничных слоев пропорциональна $R^{-1/2}$ в том случае, если R является большим. Таким образом, можно утверждать, что k_e не зависит от R.

В работе [1] показано, что k_e зависит от величины $B^{-1/3}$, которая в свою очередь пропорциональна $f\omega^{-1/2}$. В то же время $B^{-1/3}$ эквивалентно $aSc^{2/3}$, что является числовой константой, которая намного больше, чем единица [2,5].

Для оценки адекватности усовершенствованной модели был выполнен расчет значения $\bar{\Delta}$ и выполнено сравнение с результатами, приведенными в [2]. Полученные результаты представлены на рис. 1.

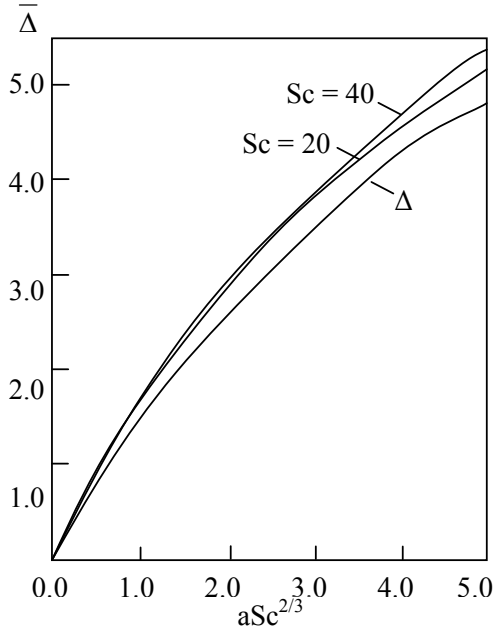


Рис. 1.

Можно видеть, что кривые, отображающие зависимость при Sc = 40 и 60, имеют незначительные различия. Типичные значения для числа Шмидта известны не очень хорошо, но могут быть несколько ниже, чем $\bar{\Delta}$. Также $\bar{\Delta}$ вычислена как функция $aSc^{2/3}$ для Sc = 20. В этом случае кривая для $\bar{\Delta}$ находится немного выше другой; несоответствие

увеличивается для более высоких значений $aSc^{2/3}$. При Sc = 10 отклонение увеличивается с уменьшением Sc.

В результате апроксимации данных получено следующее аналитическое выражение:

$$\bar{\Delta} = \frac{1.86aSc^{2/3}}{1+0.13aSc^{2/3}},\ aSc^{2/3} = f\omega^{-1/2}D^{-2/3}\nu^{1/6}. \qquad (10)$$

Данное выражение приближает расчетные значения для $\bar{\Delta}$ в пределах 0.8 % при Sc = 20 и $0 < a,\ aSc^{2/3} \le 1.0$. Приближение может также использоваться для других типичных значений Sc с небольшой потерей точности.

Как известно, концентрация примеси распределяется практически равномерно, за исключением очень близкой зоны к границе слиток/расплав. Получающийся на границе слой хорошо располагается в пределах гидродинамического пограничного слоя из-за потока в расплаве.

С точки зрения вычисленной функции $D(\bar{z})$, концентрацию можно определить как:

$$C(\bar{z})/C_L = 1 + D(\bar{z})[(C(0)/C_L) - 1] = 1 + D(\bar{z})\{1/[k_0 + (1-k_0)e^{-\bar{\Delta}}] - 1\}. \qquad (11)$$

Как было показано выше, вблизи границы $D(\bar{z})$ пропорционально $R^{-1/2}$ в том случае, если R имеет большие значения. Следовательно, можно утверждать, что локальный профиль концентрации примеси независим от d. Обозначим безразмерное расстояние до границы - $\zeta = z(\nu/\omega)^{1/2}$. Расчётные значения профиля концентрации $C(\zeta)/C_L$, показаны на рис. 2 для граничных условий $k_0 = 0$ с Sc = 40 и $aSc^{2/3} = 0.1, 0.3, 0.5$, и 1.0. Концентрация C(0) на границе существенно увеличивается с ростом $aSc^{2/3}$. Однако при типичных скоростях роста слитка, равных 1 мм/мин для слитков диаметром 100 - 150 мм, $aSc^{2/3}$ обычно довольно мало.

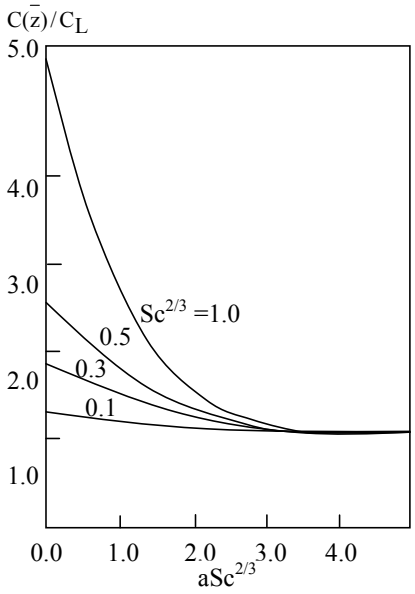


Рис. 2.

3. Выводы

1. Усовершенствована математическая модель распределения легирующей примеси в процессе выращивания слитков кремния, которая в отличие от существующих позволяет учитывать влияние на процесс легирования скорости выращивания слитка, что дает возможность уменьшить погрешность аналитических расчетов концентрационного профиля.

2. Показано, что когда число Шмидта $Sc = \upsilon / D$ достаточно велико ($Sc \geq 40$), количество лигатуры, переходящей в слиток ($\overline{\Delta}$), зависит от Sc и параметра всасывания $a = f\omega^{-1/2}\nu^{-1/2}$ только в комбинации $aSc^{2/3}$.

3. Получена приблизительная формула для расчета легирующего профиля, которая может использоваться по диапазону типичных параметров роста слитка диаметром 150 – 300 мм.

Список литературы: 1. *Burton J.A.* The Distribution of Solute in Crystals Grown from the Melt / J.A. Burton, R.C. Prim, W.P. Slichter // J. Chem. Phys. 1985. №21. P. 1987-1991. **2.** *Langlois W.E.* Digital Simulation of Flow Patterns in the Czochralski Crystal-Pulling Process/ W.E. Langlois, C .C. Shir. // Comp. Meth. Appl. Mech. Eng. 1977. №12. P. 145-152. **3.** *Langlois W.E.* Digital Simulation of Czochralski Bulk Flow in a Parameter Range Appropriate for Liquid Semiconductors / W.E. Langlois // J. Crystal Growth. 1977. №42. P. 386-399. **4.** *Von Karman T.* Tber laminare und turbulente Reibung / T. von Karman, Z. Angew // Math. Mach. – 1951. – №1. – P. 233-252. **5.** *Levich B.* Physicochemical Hydrodynamics. Prentice-Hall, 1962. 700 p.

Поступила в редколлегию 12.09.2014

Луговой Анатолий Васильевич, канд. техн. наук, профессор кафедры компьютерных и информационных систем КрНУ им. М. Остроградского. Научные интересы: информационные технологии управления. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. Email: alpritchin@ukr.net.

Притчин Алексей Сергеевич, аспирант кафедры компьютерних и информационных систем КрНУ им. М. Остроградського. Научные интересы: информационные технологии управления. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. Email: alpritchin@ukr.net.

УДК 621.315.59+546.681

А.П. ОКСАНИЧ, М.Г. КОГДАСЬ, М.С. АНДРОСЮК

ИССЛЕДОВАНИЕ СТРУКТУРНЫХ И ОПТИЧЕСКИХ ХАРАКТЕРИСТИК СЛИТКОВ ПОЛУИЗОЛИРУЮЩЕГО GaAs БОЛЬШОГО ДИАМЕТРА

Рассматриваются вопросы усовершенствования метода, методики и аппаратуры исследования структурных и оптических характеристик слитков GaAs. Определяется распределение поглощения ИК-излучения по пластине GaAs диаметром 100мм и показывается, что в направлении <001> коэффициент поглощения отсутствует, а по направлению <011> возрастает, что обусловлено формированием аномальных оптических островков по данному направлению.

1. Введение

Арсенид галлия (GaAs) является важным полупроводником, третьим по масштабам использования в промышленности после кремния и германия. Применяется для создания сверхвысокочастотных интегральных схем, светодиодов, лазерных диодов, диодов Ганна, туннельных диодов, фотоприёмников и детекторов ядерных излучений.

Некоторые электронные свойства CaAs превосходят свойства кремния. Арсенид галлия обладает более высокой подвижностью электронов, которая позволяет приборам работать на частотах до 250 ГГц.

Полупроводниковые приборы на основе GaAs генерируют меньше шума, чем кремниевые приборы на той же частоте. Из-за более высокой напряженности электрического поля пробоя в GaAs по сравнению с Si приборы из арсенида галлия могут работать при большей мощности. Эти свойства делают GaAs широко используемым в полупроводниковых лазерах, некоторых радарных системах. Полупроводниковые приборы на основе арсенида галлия имеют более высокую радиационную стойкость, чем кремниевые, что обусловливает их использование в условиях радиационного излучения (например, в солнечных батареях, работающих в космосе).

По физическим характеристикам GaAs – более хрупкий и менее теплопроводный материал, чем кремний. Подложки из арсенида галлия гораздо сложнее для изготовления и примерно впятеро дороже, чем кремниевые, что ограничивает применение этого материала.

Приборы, созданные на основе легированного GaAs, обладают лучшими параметрами при высоких температурах, чем кремниевые, и лучшими параметрами на более высоких частотах, чем германиевые. GaAs, легированный хромом, используется в инфракрасной оптике. GaAs, легированный цинком или теллуром, применяют в производстве оптоэлектронных приборов [1].

Существуют три метода промышленного производства монокристаллов GaAs:

– метод Чохральского с жидкостной герметизацией расплава слоем борного ангидрида (Liquid Encapsulated Czochralski – LEC);

– метод горизонтальной направленной кристаллизации в вариантах «по Бриджмену» (Horizontal Bridgman – HB) или «кристаллизации в движущемся градиенте температуры» (Horizontal Gradient Freeze – HGF);

– метод вертикальной направленной кристаллизации в тех же двух модификациях (Vertical Bridgman – VB, Vertical Gradient Freeze – VGF).

Метод LEC остается одним из основных в производстве GaAs уже более 40 лет. Основной вариант технологии LEC – совмещенный процесс синтеза GaAs и выращивания монокристалла в установках высокого давления. Типичные значения диаметров выращиваемых слитков составляют 100 – 150 мм, появились также коммерческие кристаллы диаметром 200 мм [2].

Предприятия Украины, занятые производством GaAs, в основном используют для выращивания слитков метод Чохральского с жидкостной герметизацией расплава слоем борного ангидрида. При выращивании слитков арсенида галлия этим методом процесс осуществляется при достаточно больших осевых и радиальных градиентах температуры вблизи фронта кристаллизации. Это приводит к высокой плотности дислокаций, которая лежит в диапазоне от $1x10^4$ до $2x10^5$ $см^{-2}$ в зависимости от диаметра слитка.

2. Постановка задачи

Использование GaAs для изготовления оптических элементов в ИК-разработках вызывает необходимость изучать влияние структурных несовершенств кристаллов на их оптические свойства (что наиболее важно дислокации и мелкие угловые зерна), а также внутреннего напряжения в них. Дефекты кристаллической решетки и внутренние напряжения в показателе преломления неоднородных оптических частиц уменьшают оптический коэффициент пропускания и увеличивают фракцию рассеянного излучения.

Наличие температурно-ростовых напряжений может привести к растрескиванию кристаллов как во время охлаждения (на завершающей стадии роста), так и при механической обработке. Эти эффекты наиболее ярко выражены для большого монокристалла GaAs (более чем 100 мм в диаметре), используемого для изготовления оптических передатчиков ИК-систем.

Температурные градиенты, которые провоцируют формирование дислокаций, определяются температурным распределением в растущем слитке, и для того чтобы создать оптимальные температурные условия роста, необходимо исследовать температурные поля роста кристалла и процесс формирования фронта кристаллизации.

Качественные зависимости плотности дислокаций от осевых и радиальных температурных градиентов в процессе кристаллизации известны, но во внимание нужно принять то, что структура дислокации растущего кристалла определяется полем температурного напряжения (температурного распределения) во всем диапазоне пластичности GaAs в довольно широком температурном интервале.

При решении многих практических проблем, в том числе и роста кристаллов, эффективно использовать подход, который заключается в анализе условий формирования структуры дислокаций, основанных на сравнении моделирования и расчёта термоупругого напряжения в системе с полученной путём эксперимента картиной распределения в выращенных кристаллах. Этот поход не может с высокой точностью дать количественное определение плотности дислокации в кристалле, но позволяет определить условия для того, чтобы получить слитки с низкими плотностями дислокаций, выполнить сравнительный анализ режимов роста и распознать отличия наиболее интенсивного формирования дислокаций в растущем кристалле, а также создает условия для целенаправленного изменения температурных условий роста.

3. Модернизация установки для определения внутренних напряжений

Простейшим устройством, позволяющим наблюдать картину наведенной оптической анизотропии, является плоский поляриском [3], состоящий (рис. 1) из источника света 1, поляризатора 2 и анализатора 3, между которыми помещается исследуемый объект 4. Такой поляриском позволяет визуально наблюдать картину двойного лучепреломления. В зависимости от значения угла α между осями поляризатора и анализатора различают плоский скрещенный поляриском, поляриском темного поля и параллельный (поляриском светлого поля).

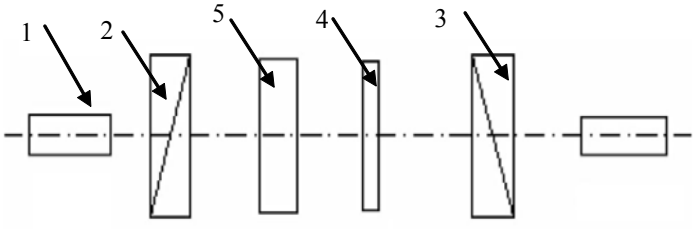


Рис. 1. Схема плоского полярископа

В случае скрещенного полярископа $\alpha = \pi/2$ и интенсивность света за анализатором [4] будет равна

$$j_+ = \sin^2 2\beta \sin^2 \frac{\sigma}{2}; \quad (1)$$

в случае параллельного $\alpha = 0$

$$j_{II} = 1 - \sin^2 2\beta \sin^2 \frac{\sigma}{2}. \quad (2)$$

Здесь β – угол наклона главных площадок относительно поляризатора, а σ – относительная разность фаз двух ортогонально поляризованных компонент излучения. Значение σ связано с толщиной образца d и длиной волны λ:

$$\sigma = \frac{d}{2\pi\lambda}(n_2 - n_1) = \frac{dC}{2\pi\lambda}(\sigma_2 - \sigma_1). \quad (3)$$

Множители $\sin 2\beta$ в (1) и (2) предопределяет основной недостаток плоского полярископа: картина двойного лучепреломления искажается наложением картины изоклин [5]. Тем не менее, этот тип полярископа является незаменимым устройством при визуальном импульсном контроле качества полупроводниковых пластин [6]. Если же между измеряемой пластиной и анализатором ввести компенсатор 5 (см.рис. 1), то становится возможным и количественный контроль внутренних напряжений.

Непосредственный визуальный контроль внутренних напряжений в пластинах полупроводников не всегда возможен, так как большинство из них не прозрачны в видимой области спектра. Для визуализации картины двойного лучепреломления в ближней ИК-области спектра наиболее эффективным представляется использование телевизионной системы с ИК-видиконом.

Нами была разработана установка для измерения внутренних напряжений подобного типа (рис. 2). Рассмотрим ее устройство.

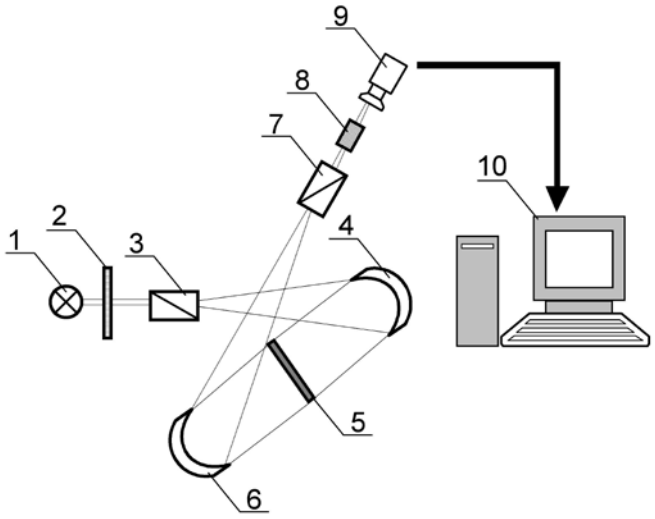


Рис.2. Структурная схема установки для измерения внутренних напряжений (1 – источник ИК-излучения, 2 – светофильтр, 3 – поляризатор, 4, 6 – длиннофокусное зеркало, 5 – образец GaAs диаметром 100 мм., 7 – анализатор, 8 – инфракрасный видикон, 9 – ТВ камера, 10 – ПК)

Излучение осветителя 1, пройдя через светофильтр 2, прозрачный в области волн $\lambda > 0{,}9$ мкм, поляризуется поляризатором 3 и направляется зеркалом 4 на исследуемую пластину 5. Далее полученное ИК-излучение отражается от второго зеркала 6 и проходит через анализатор 7, попадает на поверхность фоточувствительного слоя ИК-видикона 8, полученное изображение обрабатывается видеокамерой и передается на ПК.

Исследование внутренних напряжений проводились на пластинах арсенида галлия диаметром 100 мм, выращенных в направлении [100], легированных хромом, с концентрацией

примесей $5 \cdot 10^{14}$ см$^{-3}$, удельным сопротивлением 10^7 Ом·см. Пластины вырезаны перпендикулярно к направлению [100], по 2 пластины с краев слитка и по 5 пластин из средины слитка.

Каждая из пластин подвергалась двухсторонней алмазной полировке до толщины 1,2 мм.

Рентгеновским методом в плоскости пластины GaAs (100) определялись кристаллографические направления.

На рис. 3 показана картина двойного лучепреломления в пластине GaAs, сделаного с экрана монитора полярископа. Поляризационные призмы полярископа были установлены в скрещенное положение. На рисунке отчетливо виден так называемый «крест изоклин», обусловленный сомножителем $\sin 2\beta$ в соотношении (2). Наблюдаемая картина двулучепреломления позволяет сделать вывод о центральной симметрии полей напряжений в пластине, что обусловлено симметрией температурных полей технологических процессов, применяемых в технологии производства GaAs.

Для монокристаллов GaAs оптического применения существуют различные методы определения оптического качества. Основными параметрами являются оптическое пропускание T, коэффициент отражения R и коэффициент поглощения α.

Спектры пропускания и отражения проводились на тех же образцах GaAs и измерялись с помощью Фурье спектрометра Infralum FT-801 в спектральном диапазоне 3-15 мкм. Исследования выполнялись при комнатной температуре по основным кристаллографическим направлениям по следующей схеме (рис. 4).

Точка A0 на рис. 4 – центр пластины, точки с индексом 1 – средина от цента пластины до ее края, точки с индексом 2 – расположены на расстоянии 10мм от края пластины. Диаметр отверстий 5мм.

Коэффициент поглощения определяется по выражению:

$$\alpha = \frac{1}{h} \ln\left[\frac{(1-R^2) + \sqrt{(1-R)^4 + 4T^2R^2}}{2T}\right], \qquad (4)$$

где R – коэффициент отражения; %; T – коэффициент пропускания; %; h – толщина образца, мм.

На рис. 5-8 показаны рассчитанные нами по формуле (4) коэффициенты поглощения α основных кристаллографических направлений.

Как видно из рис. 5-8, оптические характеристики имеют неоднородность по площади пластины арсенида галлия, что связано, в первую очередь, с неоднородностью показателя преломления, который зависит от однородности механических характеристик в плоскости пластины. Оптическую неоднородность $\Delta\alpha$ можно связать с дислокационной неоднородностью по площади пластины арсенида галлия.

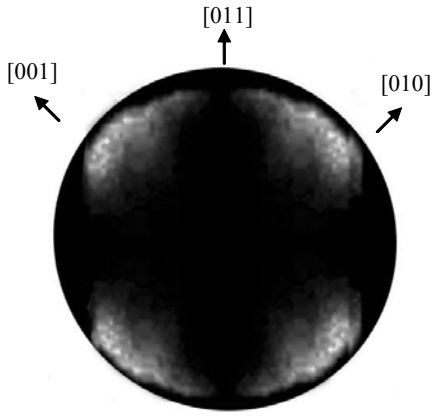


Рис. 3. Картина двулучепреломления в пластине GaAs (100) диаметром 100мм

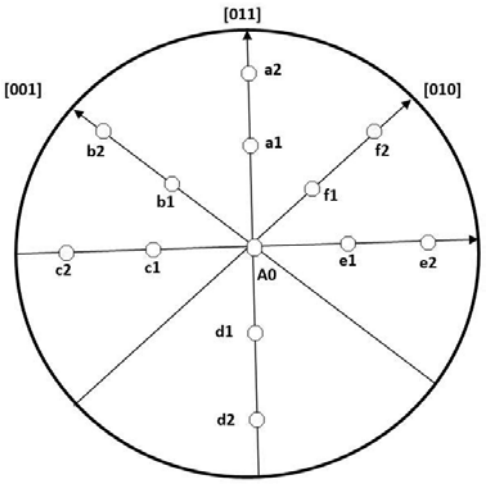


Рис. 4. Схема измерений спектров пропускания и отражения в пластинах GaAs (100) диаметром 100мм

Также на рис. 5 и 6 можно заметить, что коэффициент поглощения на краю пластины (точка b2) больше, чем в ее центре (точка A0). Это может быть обусловлено возникновением внутренних напряжений в данной области пластины.

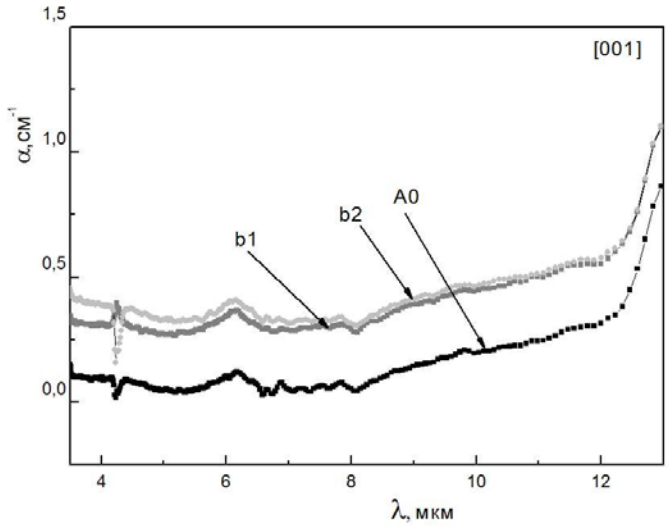


Рис.5. Коэффициент поглощения α , рассчитанный по направлению [001] в пластине GaAs (100) диаметром 100мм

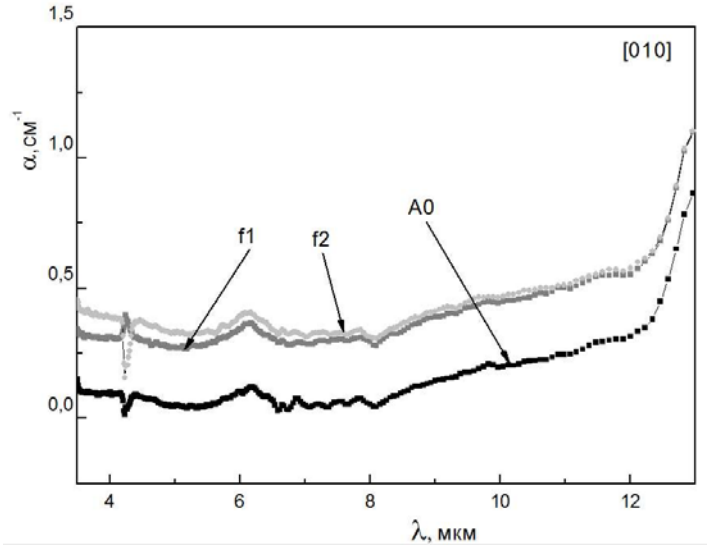


Рис.6. Коэффициент поглощения α , рассчитанный по направлению [010] в пластине GaAs (100) диаметром 100мм

По направлениям [011] и [01 $\bar{1}$] (см. рис.7, 8) значительное увеличение коэффициента поглощения отсутствует, так как в данной области внутренние напряжения уменьшаются или и вовсе отсутствуют.

4. Выводы

1. Разработана методика определения аномальных оптических областей, которая позволяет экспрессно контролировать оптические качества слитков арсенида галлия большого диаметра, применяемого в оптике.

2. Проведенные по предложенной методике исследования оптических характеристик пластины арсенида галлия ориентации (100) и диаметром 100 мм показали наличие в плоскости пластины оптических аномалий в виде локальных островков.

3. Уточнены научные данные о распределении поглощения ИК-излучения по пластине GaAs диаметром 100мм и показано, что в направлении <001> коэффициент поглощения отсутствует, а по направлению <011> возрастает, что обусловлено формированием аномальных оптических островков по данному направлению.

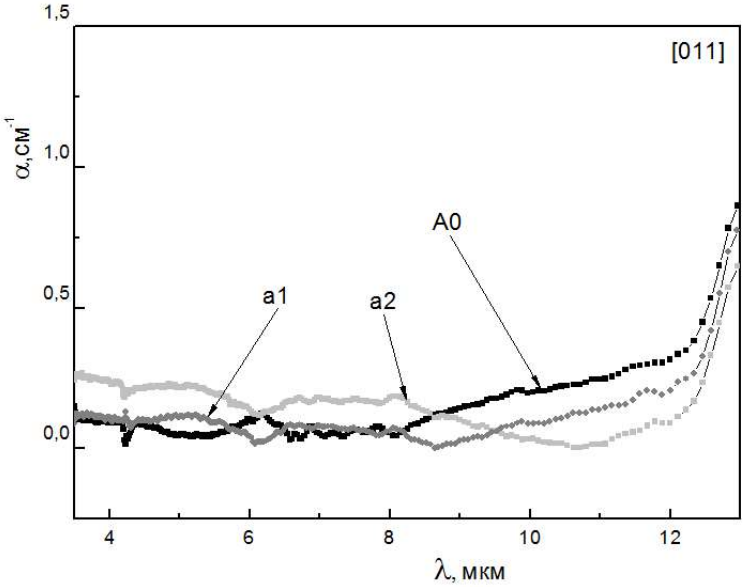


Рис.7. Коэффициент поглощения α, рассчитанный по направлению [011] в пластине GaAs (100) диаметром 100мм

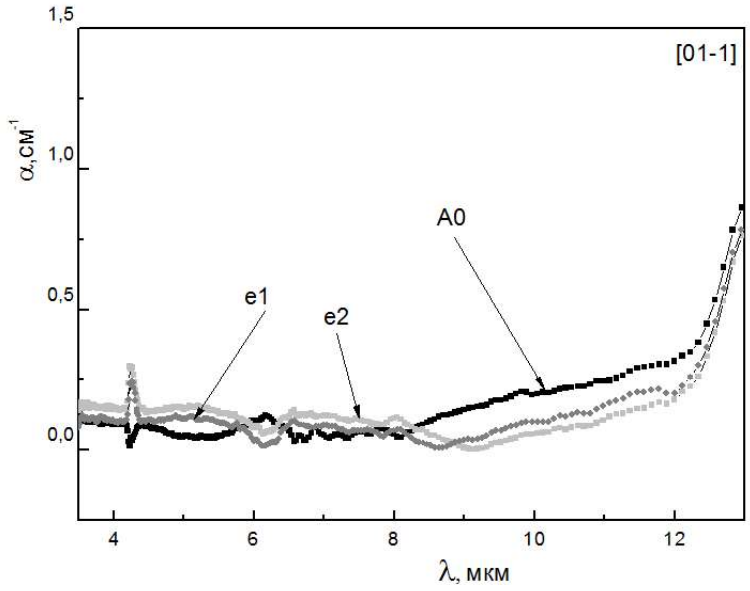


Рис.8. Коэффициент поглощения α, рассчитанный по направлению [01 $\bar{1}$] в пластине GaAs (100) диаметром 100 мм

Список литературы: 1. *Наумов А.В.* Обзор мирового рынка арсенида галлия // Технология и конструирование в электронной аппаратуре. 2005. №6. С.53-57. **2.** *Shenai-Khatkhate D. V.* Environment, health and safety issues for sources used in MOVPE growth of compound semiconductors. / D. V. Shenai-Khatkhate, R. Goyette, R. L. DiCarlo and G. Dripps // Journal of Crystal Growth. 2004. Vol. 4. P. 816-821. **3.** *Метод* фотоупругости: В 3 т. / Под общ. ред. Н.Л. Стрельчука. М.: Стройиздат, 1975. Т.2: Методы поляризационно упругих измерений. Динамическая фотоупругость. С. 14–45. **4.** *Chu T., Yamada M.* Photoelastic measurement of chip-bonding induced strains by infrared polariscope // Indium Phosphide and Related Materials. 1998. P. 541 – 544. **5.** *Fukuzawa M., Yamada M.* Photoelastic characterization of Si wafers by scanning infrared polariscope // Journal of Crystal Growth. 2001. Vol. 229. P.22-25. **6.** *Fukuzawa M., Yamada M.* Photoelastic characterization of Si wafers by scanning infrared polariscope // Journal of Crystal Growth. 2001. Vol. 229. P.22-25.

Поступила в редколлегию 25.08.2014

Оксанич Анатолий Петрович, д-р техн. наук, профессор, директр НИИ технологии полупроводников и информационно-управляющих систем Кременчугского национального университета им. Михаила Остроградского, зав. кафедрой информационно-управляющих систем. Научные интересы: методы и аппаратура контроля структурно-совершенных полупроводниковых монокристаллов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. Email: oksanich@kdu.edu.ua

Когдась Максим Григорович, канд. тех. наук, ст. преп. кафедры информационно-управляющих систем Кременчугского национального университета им. Михаила Остроградского. Научные интересы: автоматизация процессов управления производством полупроводниковых материаллов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. Email: kogdasMax@yahoo.com

Андросюк Максим Степанович, асист. кафедры информационно-управляющих систем Кременчугского национального университета им. Михаила Остроградского. Научные интересы: автоматизация процессов управления производством полупроводниковых материаллов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. Email:

УДК 681.518:004.93.1’

В.В. МОСКАЛЕНКО, А.С. РЫЖОВА

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ С ОПТИМИЗАЦИЕЙ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ

В рамках информационно-экстремальной интеллектуальной технологии рассматривается способ оптимизации пространственно-временных параметров функционирования интеллектуальной системы поддержки принятия решений для управления нестационарным технологическим процессом. Определение границ квазистационарных интервалов наблюдения за технологическим процессом предлагается осуществлять на базе нормированных статистик числа попаданий признаков распознавания в свои поля контрольных допусков.

1. Введение

Основным путём повышения функциональной эффективности автоматизированных систем управления технологическими процессами (АСУТП), функционирующими в условиях априорной неопределенности, является придание им свойства адаптивности на основе идей и методов машинного обучения и распознавания образов [1,2].

На практике в условиях нестационарности управляемого процесса его рабочий цикл делят на несколько временных интервалов, на каждом из которых производится обучение АСУТП [3,4]. Это позволяет уменьшить степень пересечения классов распознавания, характеризующих возможные функциональные состояния технологического процесса. Однако при этом неоптимальный выбор временных параметров обработки входных данных приводит к снижению функциональной эффективности машинного обучения. Например, при относительно больших временных интервалах могут существенно измениться начальные условия управляемого процесса, что приводит к уменьшению достоверности управляющих решений. А при неоправданном увеличении количества временных интервалов снижается оперативность обучения и статистическая устойчивость из-за отсутствия необходимого объема статистики для формирования репрезентативных обучающих выборок.

В работе предлагается информационно-экстремальный алгоритм обучения АСУТП с оптимизацией временных интервалов обработки информации для формирования управляющих воздействий на примере технологического процесса выращивания крупногабаритных сцинтилляционных монокристаллов из расплава.

2. Постановка задачи

Рассмотрим АСУТП, в состав которой входит обучающаяся система поддержки принятия решений (СППР). Пусть продолжительность технологического процесса разбита на R

равных интервалов наблюдения продолжительностью T_r. Для каждого интервала наблюдения сформированы упорядоченный алфавит параметрических классов распознавания $\{X^o_m(T_r) \mid m = \overline{1,M}\}$, характеризирующих функциональное состояние технологического процесса в режимах «Норма», «Меньше нормы» и «Больше нормы», и обучающая матрица $\| y^{(j)}_{m,i}(T_r) \mid i = \overline{1,N}; j = \overline{1,n}; r = \overline{1,R} \|$, где N – количество признаков распознавания; n – количество наблюдений функционального состояния процесса на интервале T_r. При этом известен структурированный вектор параметров обучения СППР:

$$g = < T_r, \delta_{K,i,r}, d_{m,r} >, \tag{1}$$

где $\delta_{K,i,r}$ – параметр поля контрольных допусков на i-й признак распознавания, определяющийся относительно базового класса распознавания $X^o_1(T_r)$; $d_{m,r}$ – радиус гиперсферического контейнера класса $X^o_m(T_r)$, восстанавливаемый в процессе обучения в радиальном базисе пространства признаков распознавания. При этом заданы ограничения на параметры обучения:

$$\begin{cases} d^*_{m-1,r} < d_{m,r} < N - 1; \\ T_r > \Delta \cdot n_{min}; \\ \delta \in [0; 0{,}5 \cdot \delta_H], \end{cases} \tag{2}$$

здесь $d^*_{m-1,r}$ – радиус контейнера предыдущего класса распознавания, принадлежащего упорядоченному алфавиту классов $\{X^o_m(T_r)\}$; Δ – шаг квантования во времени реализаций образа; n_{min} – минимальный репрезентативный объем выборки для каждого класса распознавания; $\delta_{H,i,r}$ – нормированное поле допусков, определяющее область значений параметра поля контрольных допусков $\delta_{K,i,r}$.

Необходимо в процессе обучения СППР найти оптимальные значения координат вектора параметров обучения (1) с учётом ограничений (2), обеспечивающих максимальное значение усреднённого по алфавиту классов распознавания информационного критерия функциональной эффективности (КФЭ):

$$\overline{E}^*[T_r] = \frac{1}{M} \sum_{m=1}^{M} \max_{\{k\}} E_m[T_r], \tag{3}$$

где $E_m[T_r]$ – информационный КФЭ обучения СППР распознавать реализации класса $X^o_m(T_r)$; $\{k\}$ – упорядоченное множество шагов обучения.

При найденных на интервале T_r оптимальных параметрах обучения СППР необходимо вычислить для кожного класса $X^o_m(T_r)$ экстремальную порядковую статистику (ЭПС) $S^*_{m,n}(T_r)$, построить для них вариационный ряд и определить границы вариационных блоков.

При функционировании СППР в режиме разведывательного анализа необходимо определить принадлежность распознаваемой реализации одному из классов сформированного на этапе обучения алфавита $\{X^o_m\}$ и при условии, что текущая ЭПС принадлежит соответствующему вариационному блоку, идентифицировать функциональное состояние АСУТП и при необходимости скорректировать временной интервал наблюдения процесса.

3. Описание алгоритма

В отличие от методов прямого перебора предлагаемый эвристический алгоритм позволяет ускорить поиск оптимальной длительности интервалов наблюдения $\{T_r \mid r = \overline{1,N}\}$ за

счет использования прогностической функции, способной определять момент снижения функциональной эффективности классификатора без переобучения при каждом изменении границ интервалов наблюдения (рис.1).

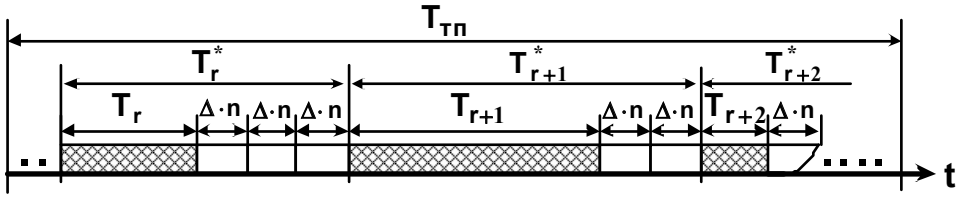


Рис. 1. Временные интервалы в режимах обучения и разведывательного анализа данных

Предполагается, что вычислительная сложность прогностической функции значительно меньше основного алгоритма обучения. В основе предложенного эвристического алгоритма оптимизации границ интервалов наблюдения лежит идея обучения на минимально допустимом интервале наблюдения и последующее использование полученных решающих правил в режиме экзамена на расширенном временном интервале, в пределах которого изменение статистических свойств образов не снижает эффективность распознавания функциональных состояний АСУ ТП.

Чтобы прогнозировать снижение функциональной эффективности обучения на расширенном интервале наблюдения в рамках информационно-экстремальной технологии, предлагается использовать нормированную статистику числа попаданий признаков распознавания в свои поля контрольных допусков, которая вычисляется для экзаменационного выборочного множества объемом n векторов-реализаций [5]:

$$S_{m,n} = \sum_{j=1}^{n} \left(\frac{k_{m,j} - \bar{k}_{m,n}}{s_{m,n}} \right)^2, \quad m = \overline{1,M}, \tag{4}$$

где $k_{m,j}$ – число успехов при j-м испытании; $\bar{k}_{m,n}$ – выборочное среднее числа успехов после n испытаний; $s^2_{m,n}$ – выборочная несмещенная дисперсия за n испытаний.

Таким образом, разведывательный анализ данных на интервале времени, расширяющем начальный интервал наблюдения, осуществляется в процессе прогностического экзамена (рис.2).

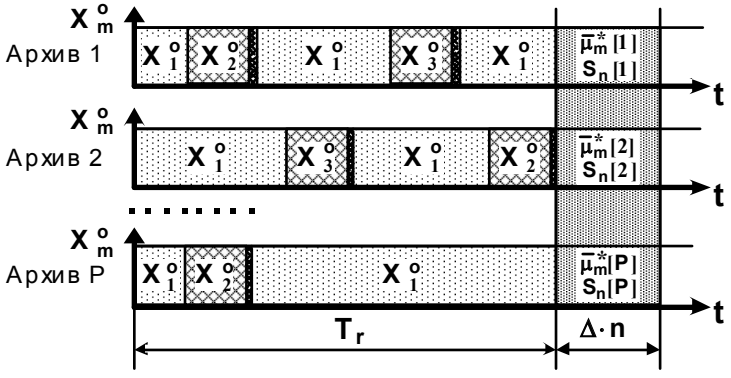


Рис. 2. Временные интервалы формирования обучающей и экзаменационной выборок по данным архивных историй

Анализ рис.2 показывает, что прогностический экзамен, как инструмент разведывательного анализа, осуществляется отдельно для данных каждой из имеющихся архивных историй, хранящихся в базе данных.

Рассмотрим этапы реализации алгоритма определения длительности временных интервалов наблюдения в процессе информационно-экстремального обучения классификатора с вложенными контейнерами классов распознавания, имеющими общий центр рассеивания реализаций образов:

1) инициализация текущей метки времени от начала архивной истории: $t_{П} := 0$;

2) инициализация счетчика интервалов наблюдения: $r := 0$;

3) $r := r + 1$;

4) сопоставление архивных ретроспективных данных мониторинга технологического процесса с маркерами отклонений технологического режима от нормы, начиная с момента $t_{П}$;

5) если на интервале $\Delta t = T_{ТП} - t_{П}$, где $T_{ТП}$ – полная длительность технологического процесса, существует репрезентативный объем выборок ($n > n_{min}$) закрытого алфавита классов распознавания $\{X_m^o[T_r]\}$, то переход к шагу 6, иначе – к шагу 20;

6) определение минимальной длительности интервала времени $T_r = \min\limits_{n}\{T_r\}$, отсчитываемого от момента $t_{П}$, на котором выполняется условие $n > n_{min}$ для всего алфавита классов распознавания;

7) формирование обучающей матрицы $\{y_m^{(j)}[T_r]\}$;

8) обучение классификатора с вложенными контейнерами за алгоритмом параллельно-последовательной оптимизации ПКД и построение вариационного ряда ЭПС $< S_{m,n}^*[T_r] >$;

9) $t_{П} := t_{П} + T_r$;

10) если $T_{ТП} - t_{П} \geq \Delta \cdot n_{min}$, то переход к шагу 11, иначе – к шагу 20;

11) инициализация счетчика архивных историй протекания ТП: $p := 0$;

12) $p := p + 1$;

13) формирование экзаменационной матрицы $\{x_m^{(j)}[p], j = \overline{1,n}\}$ на интервале времени $[t_{П}; t_{П} + \Delta \cdot n_{min}]$;

14) вычисление функций принадлежности $\{\mu_{m,j}[p]\}$ и текущей ЭПС $S_n[p]$;

15) если текущая статистика $S_n[p]$ не выходит за границы своего вариационного блока, то переход к шагу 16, иначе – к шагу 3;

16) если $p < P$, то переход к шагу 12, иначе – к шагу 17.

17) $T_r = T_r + \Delta \cdot n_{min}$;

18) $t_{П} := t_{П} + \Delta \cdot n_{min}$;

19) переход к шагу 10;

20) ОСТАНОВ.

Оптимизация ПКД осуществляется за параллельно-последовательным алгоритмом, в котором выполнение параллельного алгоритма позволяет определить стартовые ПКД, которые есть входными для алгоритма последовательной оптимизации [5]. При этом структура процедуры оптимизации ПКД за параллельным алгоритмом имеет вид

$$\delta_r^* = < \arg\max_{G_\delta} \left[\frac{1}{M} \sum_{m=1}^{M} \left[\max_{\{d_m\} \in G_{d_m}} E_{m,r} \right] \right] >, \qquad (5)$$

где G_δ – допустимая область значений параметра ПКД $\delta_r = \delta_{i,r}, i = \overline{1,N}$ для интервала T_r; G_{d_m} – допустимая область значений радиуса гиперсферического контейнера класса $X_m^o(T_r)$.

Алгоритм оптимизации ПКД за последовательным алгоритмом направлен на приближение глобального максимума информационного КФЭ к граничному его значению в допустимой области значений функции критерия и имеет такую структуру:

$$\{\delta^{*}_{i,r}\} =< \arg \overset{L}{\underset{l=1}{\otimes}} \left[\max_{G_{\delta_i}} \left[\frac{1}{M} \sum_{m=1}^{M} \left[\max_{\{d_m\} \in G_{d_m}} E_{m,r} \right] \right] \right] >, \; i = \overline{1, N}, \tag{6}$$

где G_{δ_i} – область допустимых значений параметра ПКД для i-го признака; $\otimes$ – символ операции повторения; L – количество прогонов итерационной процедуры.

В качестве КФЭ обучения СППР используется модифицированная информационная мера Кульбака, где рассматривается отношение полной вероятности правильного принятия решений P_t к полной вероятности ошибочного принятия решений P_f. Для двухальтернативных гипотез критерий имеет вид

$$E_m^{(k)} = \left[P_{t,m}^{(k)} - P_{f,m}^{(k)} \right] \cdot \log_2 \frac{P_{t,m}^{(k)}}{P_{f,m}^{(k)}} = \left[D_{1,m}^{(k)} - \beta_m^{(k)} \right] \cdot \log_2 \left(\frac{1 + (D_{1,m}^{(k)} - \beta_m^{(k)})}{1 - (D_{1,m}^{(k)} - \beta_m^{(k)})} \right), \tag{7}$$

здесь $D_{1,m}^{(k)}$ – первая достоверность, вычисленная для m-го класса на k-м шаге оптимизации параметров СППР; $\beta_m^{(k)}$ – ошибка второго рода.

Допустимая (рабочая) область определения функции информационного КФЭ ограничена неравенствами $D_1 \geq 0{,}5$ и $D_2 \geq 0{,}5$, где $D_2 = 1 - \beta$ – вторая достоверность.

Нормированную модификацию критерия (7) представим в виде

$$E_m^{(k)\prime} = \frac{E_m^{(k)}}{E_{max}}, \tag{8}$$

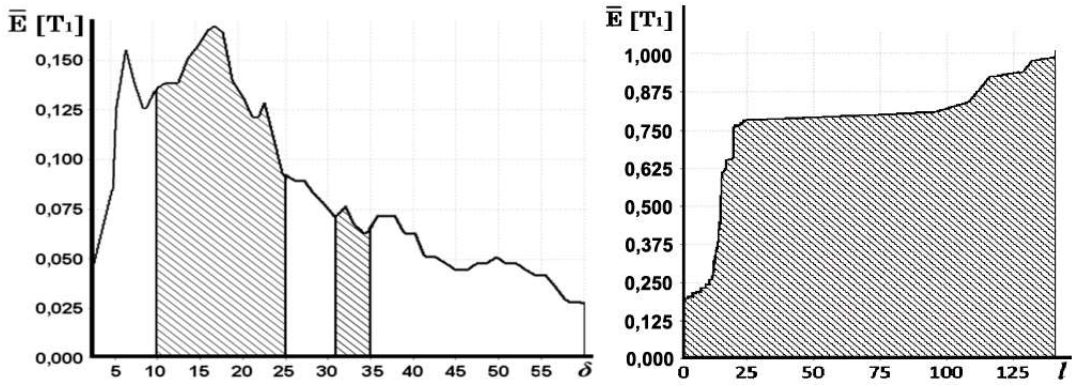
где E_{max} – значение критерия (7), вычисленное при $D_{1,m}^{(k)} = 1$ и $\beta_m^{(k)} = 0$.

Таким образом, информационно-экстремальный алгоритм обучения СППР заключается в реализации итерационной процедуры приближения глобального максимума информационного КФЭ (7) к его граничному значению путем оптимизации пространственно-временных параметров функционирования СППР (1).

4. Пример реализации алгоритма обучения СППР

Рассмотрим результаты реализации предложенного алгоритма на примере обучения СППР для управления выращиванием монокристаллов из расплава на установке типа “РОСТ” по методу Чохральского [3]. По результатам анализа архивной истории серии аналогичных выращиваний сформированы выборочные последовательности показаний датчиков с метками времени начала и конца формирования отклонения показателей монокристалла от нормы. При этом количество признаков распознавания, характеризирующих как технологические параметры процесса выращивания, так и динамику их изменения (разности первого и второго порядка), равнялось $N = 34$. Алфавит классов распознавания характеризует выпуклость фронта кристаллизации за системой оценок «Меньше нормы», «Норма» и «Больше нормы». При симметрической стратегии формирования контрольных допусков на признаки распознавания наиболее природной будет вложенная структура классов, где класс X_2^o с оценкой «Норма» буде находиться посредине, а оценка «Меньше нормы» будет отвечать базовому классу распознавания X_1^o.

Рассмотрим на примере первого интервала времени наблюдения за технологическим процессом оптимизацию длительности интервала при использовании прогностической функции (4). На рис.3 показан процесс параллельно-последовательной оптимизации ПКД за процедурами (5) и (6) для первого интервала времени наблюдения минимально допустимой длительности до начала его расширения.

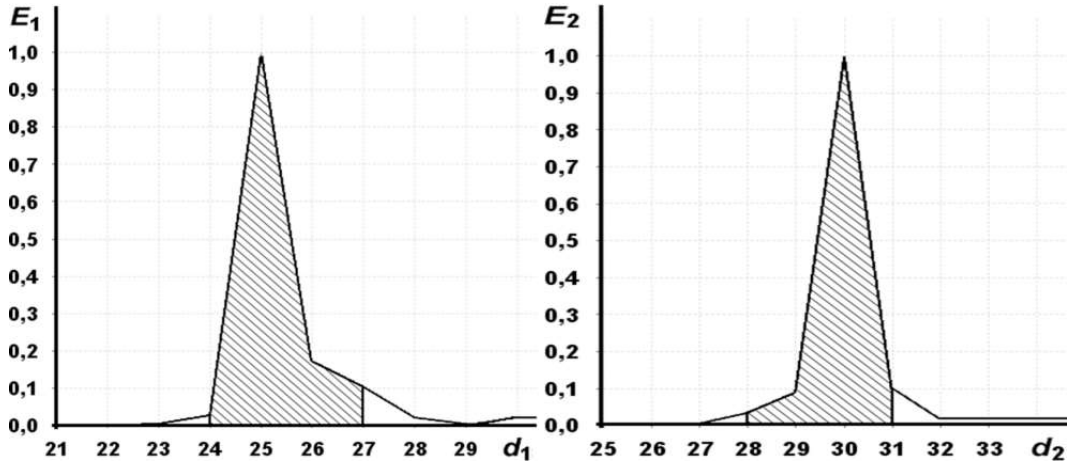


а б

Рис. 3. Графики изменения критерия в процессе оптимизации контрольных допусков на признаки распознавания

Анализ рис.3,а показывает, что полученные на этапе параллельной оптимизации квазиоптимальные значения параметра ПКД на признаки распознавания равны $\delta^* = 17\,\%$ от выборочного среднего признаков распознавания базового класса $X_1^o(T_1)$. При этом максимальное значение нормированного усредненного КФЭ (8) равно $\overline{E}^* = 0{,}1823$. На рис. 3,б показано, что в процессе 140 прогонов алгоритма последовательной оптимизации найдено оптимальный вектор $\{\delta_i^* \mid i = \overline{1,N}\}$, соответствующий граничному значению глобального максимума усредненного нормированного КФЭ, $\overline{E}^* = 1{,}00$. Это свидетельствует о построении безошибочных по обучающей матрице решающих правил.

На рис.4 показан процесс оптимизации геометрических параметров разбиения для классификатора с вложенными контейнерами для первого интервала времени наблюдения начальной длительности.



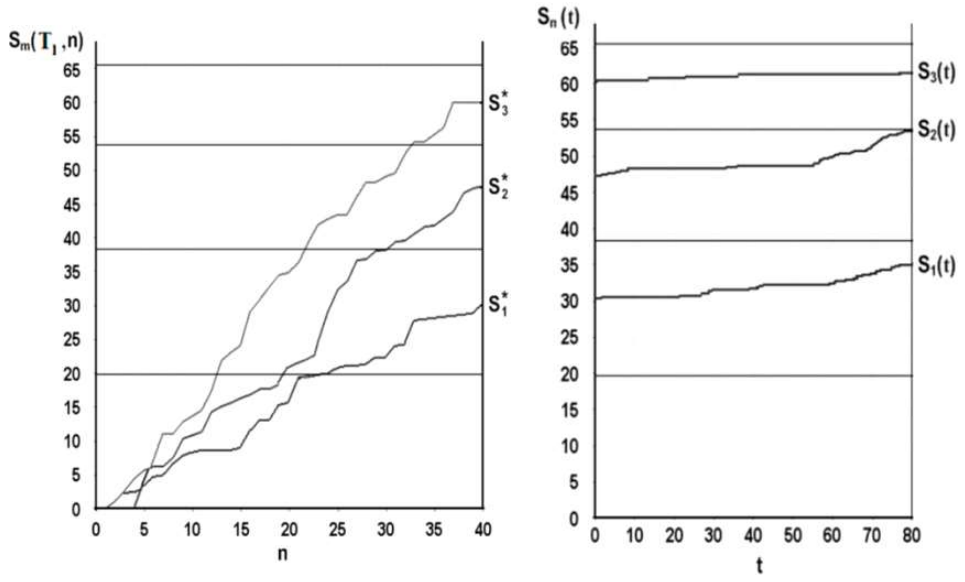
а б

Рис. 4. Графики зависимости нормированного критерия от радиуса контейнера:

а — X_1^o; б — X_2^o

Анализ рис. 4 показывает, что в результате обучения удалось получить безошибочный по обучающей матрице классификатор, поскольку критерии оптимизации достигают граничных максимальных значений. При этом оптимальные значения радиусов контейнеров классов распознавания X_1^o и X_2^o равняются в кодовых единицах $d_1^* = 25$ и $d_2^* = 30$ соответственно.

На рис. 5,а показано графики изменения ЭПС, полученные при оптимальных параметрах обучения СППР и бинарных обучающих матриц, состоящих из n векторов-реализаций для каждого из трёх классов распознавания.



а б

Рис. 5. Графики изменения ЭПС: а — при построении вариационного ряда;
б — в режиме разведывательного экзамена

Анализ рис.5,б показывает, что, начиная с 81-го шага процедуры разведывательного анализа, принимается решение о начале нового интервала наблюдения, поскольку ЭПС для класса X_2^0 вышла за пределы своего вариационного блока, что свидетельствует об изменении статистических характеристик управляемого процесса.

Таким образом, использование нормированных статистик числа попаданий признаков распознавания в свои ПКД позволяет определять с малыми вычислительными затратами моменты времени снижения функциональной эффективности решающих правил, обусловленного изменением статистических свойств управляемого процесса. Предложенный эвристический алгоритм при оптимизации длительности интервалов наблюдения заменяет вычислительно трудоемкие процедуры переобучения на несложные процедуры разведывательного анализа. Это дает возможность значительно уменьшить количество итераций процедуры оптимизации пространственно-временных параметров функционирования СППР по сравнению с методами прямого перебора.

5. Заключение

В рамках ИЭИ-технологии разработан алгоритм оптимизации пространственно-временных параметров функционирования интеллектуальной СППР на базе информационно-экстремального классификатора с вложенными контейнерами классов распознавания и единым центром рассеивания векторов-реализаций.

Физическое моделирование по архивным данным выращивания монокристаллов показало возможность использования нормированных статистик числа попаданий признаков распознавания в свои поля контрольных допусков для выявления с малыми вычислительными затратами моментов времени снижения функциональной эффективности решающих правил СППР, обусловленного изменением статистических свойств управляемого процесса. Построенный на этом принципе эвристический алгоритм оптимизации пространственно-временных параметров функционирования СППР позволяет значительно уменьшить количество итераций по сравнению с методами прямого перебора.

Список литературы: 1. *Antsaklis P.J.* An Introduction to Intelligent and Autonomous Control / P.J. Antsaklis, K.M. Passino. Norwell, Massachusetts, USA: Kluwer Academic Publishers. 1992. 448 p. **2.** *Bhagat P.* Pattern Recognition in Industry / P. Bhagat. Amsterdam, Netherlands : Elsevier Science. 2005. 200 p. **3.** *Москаленко В.В.* Інтелектуальна автоматизована система керування з оптимізацією часових параметрів аналізу вхідних даних / В.В. Москаленко, А.С. Довбиш, А.С. Рижова // Вісник Сумського державного університету. Суми, Україна: СумДУ. 2013. №3. Р. 7-14. **4.** *Lecoeuche S.* Modelling of non-stationary systems based on a dynamical decision space / S. Lecoeuche, G. Mercere, H. Amadou-Boubacar // 14th IFAC Symposium on System Identification. Newcastle, Australia : Elsevier Science. 2006. P.1222 – 1227. **5.** *Довбиш А.С.* Основи проектування інтелектуальних систем : підручник / А.С. Довбиш. Суми, Україна : СумДУ. 2009. 171 р.

Поступила в редколлегию 26.09.2014

Москаленко Вячеслав Васильевич, канд. техн. наук, ассистент кафедры компьютерных наук Сумского государственного университета. Научные интересы: интеллектуальные системы управления слабоформализованными процессами. Адрес: Україна, 40035, Сумы, ул. Н.-Сыроватская, 66, кв. 84, м.т. +380664291318, e-mail: systemscoders@gmail.com.

Рыжова Алёна Сергеевна, аспирантка Сумского государственного университета. Научные интересы: машинное обучение и распознавание образов. Адрес: Україна, 42303, Сумской район, с. Стецковка, ул. Школьная, 17, м.т. +38(095) 738-44-74, e-mail: alenarizhova@gmail.com.

УДК 681.518.5

А.С ШКИЛЬ, Г.П.ФАСТОВЕЦ, А.С.СЕРОКУРОВА

АВТОМАТИЗАЦИЯ ПОИСКА ОШИБОК ПРОЕКТИРОВАНИЯ В HDL-МОДЕЛЯХ КОНЕЧНЫХ АВТОМАТОВ

Предлагается автоматизация диагностирования HDL-моделей конечных автоматов с использованием программы ASFTEST. Рассматривается вариант восстановления графа переходов по HDL-модели автомата в форме автоматного шаблона и анализ обхода всех дуг графа для поиска ошибок проектирования.

1. Введение

При проектировании операционных или управляющих устройств с использованием конечных автоматов алгоритм их функционирования, как правило, задается или в виде граф-схемы алгоритма (flow chart), или путем описания функции выходов в словесном или табличном виде. При автоматизированном проектировании подобных устройств их описание на языке аппаратуры (HDL) создается в форме автоматного шаблона, т.е. специальной структуры HDL-кода, которая строится на основе графа переходов автомата (state diagram). Переход от других способов описания закона функционирования конечного автомата к его графу переходов является искусством проектировщика и подробно описан в [1].

Одним из важных этапов автоматизированного проектирования цифровых устройств является верификация HDL-модели, т.е. определение соответствия полученного HDL-кода заданной спецификации. Один из традиционных подходов к верификации и диагностированию HDL-моделей состоит в следующем. С учетом выбранного стиля описания составляется список ошибок проектирования и для них строятся тесты. HDL-модель компилируется, и в ней устраняются синтаксические ошибки. Полученная HDL-модель моделируется в среде верификации на построенных тестах, и результат сравнивается с эталоном, который получен на основе спецификации. Если результат не совпал с эталоном, то выполняется диагностический эксперимент (ДЭ) по поиску места нахождения ошибки проектирования с последующим исправлением HDL-кода, и повторяется процедура верификации [2].

Возможные ошибки проектирования в HDL-моделях определяются стилем описания HDL-кода. Под ошибкой проектирования понимается ошибка в HDL-операторе, которая не относится к классу синтаксических и нарушает алгоритм функционирования модели устройства, заданный спецификацией.

Типы ошибок проектирования :

- «замена оператора» (логического или арифметического),
- «замена операнда» (в операторе назначения или условном).

Выделение фрагментов HDL-кода, описывающих поведение конечных автоматов стилем «автоматный шаблон», позволяет определить ошибки проектирования типа «неправильный переход в графе переходов автомата», что соответствует ошибке:

- в выборе текущего состояния в операторе when,
- в выборе следующего состояния в функции переходов (a_i вместо a_j),
- в операторе if( ) при анализе входного сигнала;
- в назначении выходного сигнала.

В [3] предложен «ручной» подход к поиску ошибок проектирования в автоматных HDL-моделях цифровых устройств. Но данный подход, во-первых, предусматривает наличие спецификации в виде графа переходов, а во-вторых, применим только для достаточно несложных HDL-моделей в форме автоматного шаблона. Таким образом, необходимо разработать автоматизированный метод поиска ошибок проектирования в HDL-моделях цифровых автоматов при задании спецификации в произвольном виде.

2. Подготовка к проведению диагностического эксперимента

Предлагается следующий подход к диагностированию HDL-моделей (локализации места возникновения ошибок проектирования в них). Имеется спецификация в словесной форме или в виде таблицы выходов. На ее основе построен HDL-код в форме автоматного шаблона. По HDL-коду с помощью специальных инструментальных средств (например, Code2Graphics в составе Active-HDL) восстанавливается граф переходов, соответствующий HDL-коду (с возможными ошибками). С помощью инструмента автоматического построения тестов (например, ASFTEST в составе Active-HDL) подготавливается диагностический эксперимент над HDL-моделью автомата (проверка достижимости вершин с использованием линий сброса, обход всех дуг, обход всех вершин) путем построения теста в форме TestBench и маршрутов обхода путей. ДЭ проводится с использованием инструментальных средств системы моделирования HDL-кода Active-HDL. По результатам прохождения теста и сравнения с эталоном спецификации (функцией выходов) строится вектор экспериментальной проверки (ВЭП), и путем анализа таблицы путей находится ошибочная дуга (дуги) в графе. При этом ошибка в HDL-коде, вероятнее всего, находится во фрагменте кода автоматного шаблона, связанного с вершиной (состоянием), откуда исходит ошибочная дуга.

В качестве элементарной проверки P_i при проведении ДЭ используется реализация определенного маршрута обхода графа, при этом номер маршрута (строка матрицы путей) соответствует номеру элементарной проверки. Результат элементарной проверки v_i считается отрицательным, если терминальная (конечная) вершина на этом маршруте достигнута, в противном случае результат элементарной проверки считается положительным:

$$v_i = \begin{cases} 0 \rightarrow \text{если на этом маршруте обхода выход совпадает с эталоном (тест прошел);} \\ 1 \rightarrow \text{если на этом маршруте обхода выход не совпадает с эталоном (тест не прошел).} \end{cases}$$

ВЭП для диагностического эксперимента определяется $V = (v_1, v_2, .. v_m)$, где m – число элементарных проверок P_i.

Если предположить наличие в схеме одиночной ошибки проектирования, то по результатам ДЭ область подозреваемых дефектов формируется на основе пересечения строк таблицы путей, отмеченных единичными значениями в ВЭП, по формуле:

$$D = \cap|_{v_j=1} M_j - \cup|_{v_j=0} M_j, \qquad (1)$$

где M_j – j-я строка таблицы путей.

Если результат вычислений по формуле (1) оказался пустой, то предполагается, что в схеме присутствует кратная ошибка проектирования, и область подозреваемых ошибок определяется объединением строк, соответствующих единичным значениям координат ВЭП по формуле [4]:

$$D = \cup|_{v_j=1} M_j - \cup|_{v_j=0} M_j. \qquad (2)$$

Для проведения ДЭ по поиску ошибок проектирования используется VHDL-модель автомата Мили, который выполняет распознавание набора 1100 во входной битовой последовательности. На рис.1 представлен фрагмент архитектуры двухпроцессного автоматного шаблона HDL-модели без ошибок проектирования (хотя в реальности такой эталонной модели при проведении ДЭ не существует).

```
begin
p1: process (state, data)
begin
    case state is
                when a0 =>
                    if data='0' then nextstate<= a0; y<='0';
                                else nextstate<= a1;y<='0';
                    end if;
                when a1 =>
                    if data='1' then        nextstate<= a2; y<='0';
                                else nextstate<= a0; y<='0';
                    end if;
                when a2 =>
                    if data='0' then        nextstate<= a3; y<='0';
                                else nextstate<= a2; y<='0';
                    end if;
                when a3 =>
                    if data='0' then nextstate<= a0; y<='1';
                                else nextstate<= a1; y<='0';
                    end if;
    end case;
end process;
p2: process (clk,reset)
begin
if reset='1' then state <= a0;
elsif clk'event and clk = '1' then state <= nextstate;
end if;
end process;
```

Рис. 1. Фрагмент эталонной VHDL-модели автомата

Используя программный инструмент Code2Graphics в составе Active-HDL [5], восстанавливаем граф переходов данного автомата (рис.2).

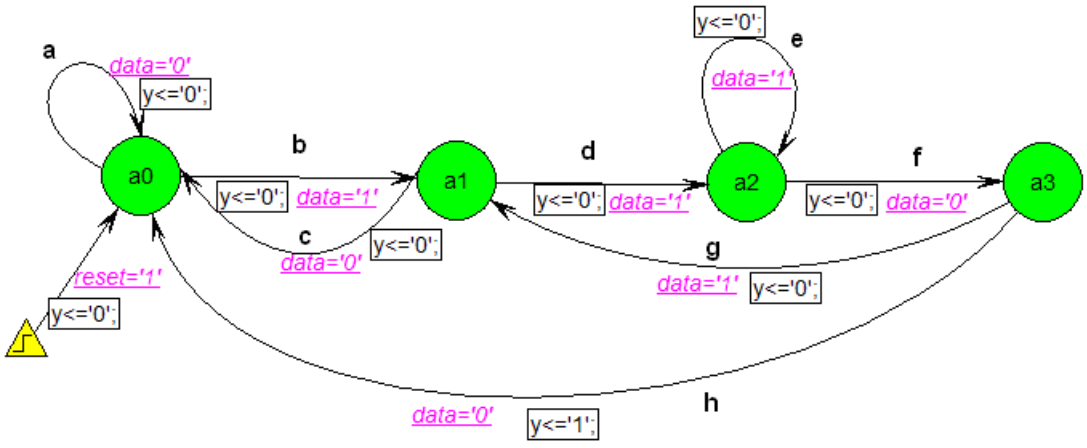


Рис. 2. Восстановленный граф переходов в диаграмме состояний Active-HDL

Для данного графа с помощью инструмента автоматического построения тестов ASFTEST в составе Active-HDL автоматически генерируются тестовые наборы в форме TestBench. Входной информацией является содержательный граф автомата, представленный в формате ASF. В результате работы ASFTEST формируются минимизированные тестовые последовательности в виде файла на языке VHDL (Verilog) для проверки правильности (в англоязычной литературе используется термин – validation) и верификации проекта с помощью программ моделирования на языках VHDL и Verilog. Возможна генерация теста по 3 различным стратегиям, в зависимости от целей моделирования и необходимой полноты теста. ASFTEST также выполняет анализ модели на корректность, генерирует описание на языке VHDL, генерирует макрокоманды для среды Active-HDL, фиксирует в файле отчета статистическую информацию [6].

При компиляции *.asf-файла генерируется модель автомата на языке VHDL, но при данном подходе к проведению ДЭ не используется.

Запуск программы автоматической генерации тестов осуществляется с помощью следующей командной строки:

asftest.exe -in [path]\fsm.asf – tb2 fsm_tb2.vhd,

где [path]\ - путь к файлу, fsm.asf – имя входного файла.

В результате работы программы ASFTEST генерируются следующие файлы:

fsm_asft.cov – файл отчета, содержит информацию о покрытии состояний и путей при каждой стратегии;

fsm_asft.err – файл отчета об ошибках. Ошибок не содержится. Файл пуст;

fsm_asft.rpt – файл статистики, содержит информацию об обрабатываемом графе;

fsm_gen.vhd – файл описания автомата на языке VHDL;

fsm_tb2.vhd – файл, содержащий сгенерированную по стратегии 2 (обход всех дуг графа переходов автомата) тестовую последовательность на языке VHDL (рис.3);

fsm_tb2.do – файл с макрокомандами для моделирования теста из файла fsm_tb2.vhd.

```
architecture fsm_arch_tb2 of fsm_ent_tb2 is
…begin
… begin
  clk <= ‘0’; cycle_num <= 0;
  wait for delay_wr_in;
  data <= ‘0’; reset <= ‘1’;
   wait for delay_pos_edge;
  test_sreg <= a0; clk <= ‘1’;
  wait for delay_wr_out;
  wait for delay_neg_edge; — a0
…end architecture fsm_arch_tb2;
…
```

Рис. 3. Фрагмент TestBench на языке VHDL для теста, полученного по стратегии 2

ASFTEST генерирует файл fsm_asft.cov с описанием всех дуг графа переходов (рис.4), что в дальнейшем значительно упрощает создание таблицы путей.

```
28=(a0->a0)31=(a0->a1)33=(a1->a2)35=(a1->a0)
38=(a2->a3)40=(a2->a2)42=(a3->a0)45=(a3->a1)48=(@any_state->a0)
```

Рис. 4. Листинг файла fsm_asft.cov по стратегии 2

Каждая дуга в файле fsm_asft.cov имеет символическое (цифровое) имя, а присвоенные ниже для наглядности имена дуг графа эталонного кода показаны на рис.2:

a=(a0->a0), b=(a0->a1), c=(a1->a0), d=(a1->a2), e=(a2->a2),
f=(a2->a3), g=(a3->a1), h=(a3->a0).

Для упрощения изложения материала будем рассматривать автомат с тривиальной функцией выходов, т.е. выходной сигнал непосредственно связан с переходом (дугой). Это

упрощает наблюдаемость обхода графа автомата, но является частным случаем HDL-модели конечного автомата.

3. Проведение диагностических экспериментов

В качестве примеров применения изложенной стратегии проведем несколько ДЭ по поиску ошибок проектирования разных типов. Последовательность этапов проведения ДЭ следующая. По HDL-коду восстанавливается граф переходов, по графу строится тест, тест моделируется и по waveform выполняется сравнение результатов моделирования с эталоном (спецификацией). На основании результатов сравнения строится ВЭП и по нему по формулам (1) и (2) находятся ошибочные дуги в графе. После этого выполняется визуальная инспекция HDL-кода и находится ошибочный оператор.

Вначале рассмотрим вариант HDL-модели, где заведомо отсутствуют ошибки проектирования (см.рис.2). Такой вариант кода в дальнейшем будем называть исправным.

На рис.5 приведены результаты моделирования теста по стратегии 2 в Active-HDL для HDL-модели исправного автомата.

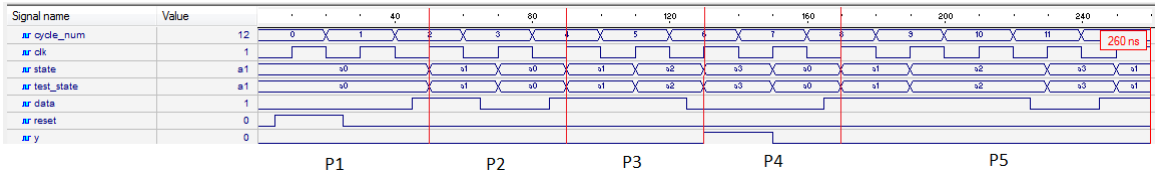


Рис. 5. Waveform с временными границами элементарных проверок P_i для исправной HDL-модели автомата

Результаты проведения ДЭ представим в виде таблицы путей (маршрутов) обхода графа, строками которой являются элементарные проверки, а столбцами – имена дуг графа переходов. Кроме того, в данной таблице представлены реальное и эталонное значение функции выходов y и ВЭП (рис.6). Отметим, что столбец $y_{эт}$ связан со спецификацией и используется для получения ВЭП.

	data	a	b	c	d	e	f	h	g	y	$y_{эт}$	ВЭП(V)
P_1	0	1								0	0	0
P_2	10		1	1						0	0	0
P_3	11		1		1					0	0	0
$P_3 + P_4$	**1100**		1		1		1	1		1	1	0
$P_3 + P_5$	11101		1		1	1	1		1	0	0	0

Рис. 6. Маршруты обхода исправного графа переходов и ВЭП

Анализируя таблицу путей на рис.6, можно сделать два вывода:

1) в тесте присутствует последовательность 1100 (элементарные проверки $P_3 + P_4$), дающая значение 1 на выходе, что соответствует спецификации;

2) для исправного кода ВЭП=0, что соответствует отсутствию ошибок в HDL-коде.

Рассмотрим вариант ошибочного HDL-кода с ошибкой в выборе текущего состояния (рис.7) (в операторе when вместо состояния a2 задано a4, что помечено серым цветом).

```
when a4 => (вместо when a2)
                if data='0' then        nextstate<= a3; y<='0';
                else nextstate<= a2; y<='0';
                end if;
```

Рис. 7. Фрагмент VHDL-модели автомата с ошибочным оператором when

Ошибка такого вида не пропускается компилятором, так как a4 – это необъявленное состояние. Поэтому, такая ошибка проектирования обнаруживается еще на этапе компиляции VHDL-модели.

Рассмотрим вариант ошибочного кода с ошибкой в выборе следующего состояния. На рис.8 приведен фрагмент VHDL-модели рассматриваемого автомата с ошибочным оператором назначения нового состояния a3 вместо a2 (помечено в коде серым цветом).

```
when a2 =>
    if data='0' then          nextstate<= a3; y<='0';
    else nextstate<= a3; y<='0'; (вместо nextstate <= a2)
    end if;
```

Рис. 8. Фрагмент VHDL-модели автомата с ошибочным оператором назначения

Моделирование кода с внесенной ошибкой встроенным инструментом Code2Graphics генерирует граф автомата (рис.9), новый asf-файл, из которого генерируются тесты. Необходимо отметить, что в Active-HDL граф-модель автомата является более сложной, чем модели Мили и Мура (на рис.9 выходной сигнал автомата Мили привязан к выходу из вершины графа переходов), но это не влияет на результаты проведения ДЭ.

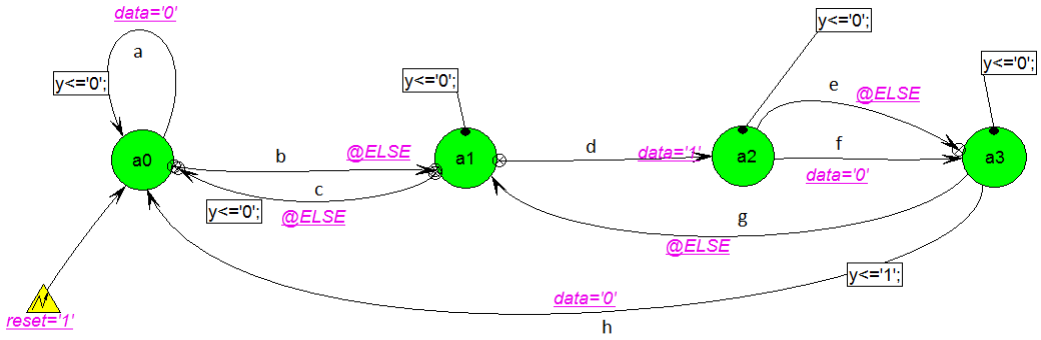


Рис. 9. Граф переходов с ошибочным оператором назначения нового состояния a3

Результаты моделирования тестов в среде Active-HDL приведены на рис. 10.

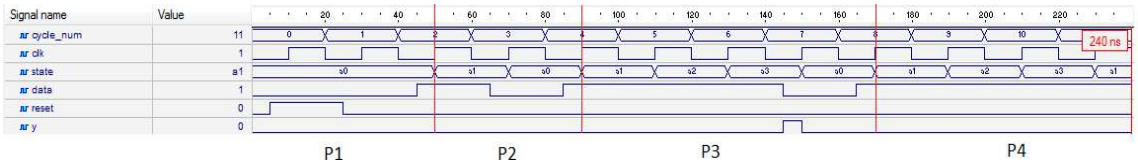


Рис. 10. Результаты моделирования автомата с ошибочным оператором назначения

Результатом проведения ДЭ по обходу графа является вектор экспериментальных проверок, в котором на P_3 произошло несовпадение с эталоном. Исходя из спецификации, y может быть равен 1 только при подаче на вход последовательности 1100, соответственно, а возникновение 1 на выходе при подаче 1110 неверно, что свидетельствует об ошибке.

Таблица путей для данного ДЭ (маршруты обхода графа) и ВЭП представлены на рис.11. Отметим, что тестовые входные последовательности представлены в столбце data.

	data	a	b	c	d	e	f	h	g	y	$y_{эт.}$	ВЭП(V)
P_1	0	1								0	0	0
P_2	10		1	1						0	0	0
P_3	1110		1		1	1		1		1	0	1
P_4	1111		1		1	1			1	0	0	0

Рис. 11. Таблица путей для ошибочного графа переходов и ВЭП

Место возникновения ошибки в маршруте обхода графа переходов находится по формуле (1):

D = {b, d, e, h} – {a} ∪ {b, c} ∪ { b, d, e, g} = { b, d, e, h } – {a, b, c, d, e, g} = { h },

т.е. в графе переходов подозревается ошибочная дуга h .

Для нахождения места возникновения ошибки проектирования необходимо возвратиться к HDL-коду автоматного шаблона и выполнить визуальное инспектирование участка кода для вычисления ошибочной дуги. Анализ фрагмента кода, связанного с состоянием a3, показывает отсутствие ошибок. Попадание же в список подозреваемых ошибочных переходов дуги h связано с тем, что ASFTEST генерирует однократное покрытие обхода дуг графа и маршрута b – d – f – h в списке обхода нет.

В этом случае надо возвратиться к предыдущему состоянию a2. Анализ фрагмента кода, связанного с состоянием a2, показывает наличие ошибочного оператора (else nextstate <= a3), данный оператор корректируется (else nextstate <= a2), и ДЭ по проверке корректности VHDL-кода повторяется.

Следующий вариант ошибочного кода – ошибка в операторе if, что выделено на рис.12 жирным текстом.

```
when a3 =>
    if data='1' then (вместо data='0')
                    nextstate<= a0; y<='1';
    else nextstate<= a1; y<='0';
    end if;
```

Рис. 12. Фрагмент VHDL-модели автомата с ошибочным оператором if

По результатам моделирования тестов в среде Active-HDL строим таблицу путей и ВЭП (рис.13). Здесь и далее ошибочный граф переходов и сравнение графических результатов моделирования по waveform не приводятся ввиду громоздкости рисунков.

	data	a	b	c	d	e	f	h	g	y	$y_{эт.}$	ВЭП(**V**)
P_1	0	1								0	0	0
P_2	10		1	1						0	0	0
P_3	11		1		1					0	0	0
$P_3 + P_4$	1101		1		1		1	1		1	0	1
$P_3 + P_5$	1**1100**		1		1	1	1		1	0	1	1

Рис. 13. Таблица путей для ошибочного графа переходов и ВЭП

Место возникновения ошибки в маршруте обхода графа переходов будет:

D = {b, d, f, h} ∩ {b, d, e, f, g} – {a} ∪ {b, c} ∪ {b, d} = {b, d, f } – {a, b, c, d,} = {f}, т.е. подозревается ошибочная дуга f в графе переходов.

Инспекция фрагмента кода, связанного с исходящей вершиной a2, не находит ошибки проектирования. Данная ситуация состоит в следующем. Фрагмент ошибочного кода if data='1' порождает фактически две ошибочные дуги: g и h, которые, маскируя друг друга, приводят к ошибке в общей для них входящей дуге f. Это связано с особенностью построения маршрутов обхода графа в ASFTEST (переход 48=(@any_state->a0)на рис.4 фактически является безусловным). В этом случае ошибку нужно искать в дугах, исходящих из a3. А там находится ошибочный фрагмент кода: if data='1'.

Следующий пример ошибочного кода связан с наличием ошибки в назначении выходного сигнала в состоянии a3, что показано на рис.14 жирным текстом.

```
when a3 =>
    if data='0' then nextstate<= a0; y<='1';
                        else nextstate<= a1; y<='1'; (вместо y<='0')
    end if;
```

Рис. 14. Фрагмент VHDL-модели автомата с ошибкой в назначении выходного сигнала

По результатам моделирования тестов в среде Active-HDL строим таблицу путей и ВЭП (рис.15).

	data	a	b	c	d	e	f	h	g	y	$y_{эт.}$	ВЭП(*V*)
P_1	0	1								0	0	0
P_2	10		1	1						0	0	0
P_3	11		1		1					0	0	0
$P_3 + P_4$	**1100**		1		1		1	1		1	1	0
$P_3 + P_5$	11101		1		1	1	1		1	1	0	1

Рис. 15. Таблица путей для ошибочного графа переходов и ВЭП

Место возникновения ошибки в маршруте обхода графа переходов будет:

$$D = \{b, d, e, f, g\} - \{a\} \cup \{b, c\} \cup \{b, d\} \cup \{b, d, f, h\} = \{b, d, e, f, g\} - \{a, b, c, d, f, h\} = \{e, g\},$$

т.е. подозреваются ошибочными дуги e и g в графе переходов.

Анализ фрагмента кода, связанного с состоянием a2 (дуга e), показывает отсутствие ошибок, а анализ фрагмента кода, связанного с состоянием a3 (дуга g), показывает ошибку в назначении выходного сигнала y (else nextstate<= a1; y<='1').

Внесем в код сразу две ошибки: ошибку назначения состояния и ошибку в условии перехода. Ошибочный код приведен на рис.16, а результаты ДЭ приведены на рис.17.

```
when a2 =>
    if data='0' then
                nextstate<= a3; y<='0';
    else nextstate<= a3; y<='0'; (вместо nextstate <= a2)
    end if;
…
when a3 =>
    if data='1' then (вместо data='0')
                nextstate<= a0; y<='1';
    else nextstate<= a1; y<='0';
    end if;
```

Рис. 16. Фрагменты VHDL-модели автомата с ошибочным оператором назначения и ошибкой в условии перехода

	data	a	b	c	d	e	f	h	g	y	$y_{эт.}$	ВЭП(**V**)
P_1	0	1								0	0	0
P_2	10		1	1						0	0	0
P_3	11		1		1					0	0	0
$P_3 + P_4$	1101		1		1	1		1		1	0	1
$P_3 + P_5$	1110		1		1	1			1	1	0	1

Рис. 17. Таблица путей для ошибочного графа переходов и ВЭП

Место возникновения ошибки в маршруте обхода графа переходов находится по формуле (1):

$$D = \{b, d, e, h\} \cap \{b, d, e, g\} - \{a\} \cup \{b, c\} \cup \{b, d\} = \{b, d, e\} - \{a, b, c, d\} = \{e\},$$

т.е. подозревается ошибочная дуга e . Анализируя фрагмент кода, связанный с a2, находим ошибочный фрагмент кода else nextstate<= a3; y<='0'и исправляем его. После этого ДЭ

повторяется, и по аналогичному принципу находим вторую ошибку проектирования (результаты на рис.12 и 13).

Рассмотрим еще один вариант ошибочного кода с двумя ошибками проектирования: ошибка назначения выходного сигнала и ошибка в условии перехода. Ошибочный код приведен на рис.18, а результаты ДЭ приведены на рис.19.

```
when a0 =>
    if data='0' then
                nextstate<= a0; y<='1'; (вместо y<='0')
                else nextstate<= a1;y<='0';
    end if;
…
when a3 =>
    if data='1' then (вместо data='0')
                nextstate<= a0; y<='1';
    else nextstate<= a1; y<='0';
    end if;
```

Рис. 18. Фрагменты VHDL-модели автомата с ошибкой назначения выходного сигнала и ошибкой условия перехода

	data a	b	c d e f h	g y	$y_{эт.}$	ВЭП(**V**)
P_1	0 1			1	0	1
P_2	10	1	1	0	0	0
P_3	11	1	1	0	0	0
P_3 + P_4	1101	1	1 1 1	1	0	1
P_3 +P_5	1**1100**	1	1 1 1	1 0	1	1

Рис. 19. Таблица путей для ошибочного графа переходов и ВЭП

Место возникновения ошибки в маршруте обхода графа переходов пытаемся найти по формуле (1):

$$D = \{a\} \cap \{b, d, f, h\} \cap \{b, d, e, f, g\} - \{b, c\} \cup \{b, d\} = \varnothing - \{b, c, d\} = \varnothing .$$

Значит, требуется использовать формулу нахождения кратных ошибок (2):

$$D=\{a\} \cup \{b, d, f, h\} \cup \{b, d, e, f, g\} - \{b, c\} \cup \{b, d\}=\{a, b, d, e, f, g, h\} - \{b, c, d\}=\{a, e, f, g, h\}.$$

Подозреваются ошибочные дуги a, e, f, g и h в графе переходов.

Инспекция кода показывает следующее. Дуга *a* связана с фрагментом ошибочного кода в состоянии a0 (nextstate<= a0; y<='1'). А дуги {e, f, g,, h} связаны с маскируемой ошибкой проектирования (if data='1'), нахождение которой подробно рассматривалось в комментариях к рис.13.

4. Выводы

Показана принципиальная возможность автоматизации поиска ошибок проектирования в HDL-моделях конечных автоматов в форме автоматного шаблона с использованием программного продукта ASFTEST.EXE в составе среды проектирования Active–HDL. В качестве примера использована модель конечного автомата Мили на языке VHDL и рассмотрены примеры поиска различных ошибок проектирования. Используемая стратегия позволяет находить область местонахождения ошибки проектирования в фрагментах HDL-кода, т.е. значительно сузить область визуального инспектирования кода.

Вопросы эквивалентности исправного и неисправных автоматов, выбора стратегий обхода графа, длины диагностического эксперимента, существования диагностических тестов и глубины диагностирования не рассматривались в данной работе и являются предметом дальнейших исследований.

Список литературы: 1. *Баранов С.И.* Синтез микропрограммных автоматов (граф-схемы и автоматы). 2-е изд., прераб. и доп. / *С.И. Баранов* Л.: Энергия, 1979. 232 с. **2.** *Шкиль А.С.* Структурное и функциональное диагностирование HDL-моделей цифровых устройств в САПР РЭА /*А.С. Шкиль, Е.Е. Сыревич, С. Альмадхоун, Г.П. Фастовец* // Інформаційно-керуючі системи на залізничному транспорті. 2013. № 2. С. 75-82. **3.** *Альмадхоун С.* Поиск ошибок проектирования в HDL-моделях цифровых автоматов / *С. Альмадхоун, Е.Е. Сыревич, А.С. Шкиль* // Вестник Херсонского государственного технического университета. 2013. №2 (46). С. 377-383. **4.** *Шкиль А.С.* Методы поиска ошибок проектирования в HDL-коде */ А.С. Шкиль, Е.Е. Сыревич, Д.Е. Кучеренко, Г.П. Фастовец* // Радиоэлектроника и информатика. 2008. №. 3. С. 47–53. **5.** Code2Graphics™ Converter [Электронный ресурс] / *ALDEC*. The design verification company. Режим доступа : www\ URL : https://www.aldec.com/en/products/fpga_simulation/active-hdl/feature/29 – 10.05.14. Загл. с экрана. **6.** *Хаханов В.И.* Система генерации тестов для проектирования цифровых автоматов в среде ACTIVE-HDL / *В.И. Хаханов, Е.В. Ковалев, В.В. Ханько, Масуд М.Д. Мехеди* // АСУ и приборы автоматики. Харьков. 2000. Вып.111. С. 15-22.

Поступила в редколлегию 20.09.2014

Шкиль Александр Сергеевич, канд. техн. наук, доцент кафедры АПВТ ХНУРЭ. Научные интересы: диагностика цифровых систем, дистанционное образование. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.

Фастовец Геннадий Павлович, канд. техн. наук, доцент кафедры АПВТ ХНУРЭ. Научные интересы: диагностика цифровых систем. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.

Серокурова Анна Сергеевна, аспирантка кафедры АПВТ ХНУРЭ. Научные интересы: техническая диагностика цифровых автоматов. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-13-26.

УДК 004.056 (043.2)

В.Г. БАБЕНКО, В.М. ЗАЖОМА, О.Б. НЕСТЕРЕНКО

МЕТОД ВБУДОВУВАННЯ СТЕГОПОВІДОМЛЕННЯ НА ОСНОВІ КЛЮЧОВОГО ЕЛЕМЕНТА

Розробляється стеганографічний метод вбудовування інформації, який здійснюється на основі використання випадково визначеного ключового елемента пустого контейнера, значення якого забезпечує вибір способу вбудовування повідомлення в контейнер. Наводиться опис етапів виконання стеганографічного перетворення для розробленого методу вбудовування інформації, а також формальна модель стегосистеми, що базується на використанні даного методу вбудовування інформації на основі ключового елемента. Визначається ряд переваг та недоліків розробленого методу вбудовування повідомлення в стегоконтейнер.

1. Вступ

Сучасні тенденції розвитку засобів інформаційної комунікації посприяли значному збільшенню обсягів і швидкості обробки та передавання інформації, а також забезпеченню організації дистанційного доступу до глобальних інформаційних ресурсів. Характерною рисою сучасного суспільства є організація та ведення інформаційної діяльності. Тому задачі забезпечення захисту інформації сьогодні виходять на перше місце та набувають особливого значення. Захист від головних видів загроз мережевої взаємодії, як правило, реалізується на основі криптографічних методів. Використання криптографічних перетворень забезпечує конфіденційність, автентичність та цілісність інформації, яку передають. Конфіденційності інформації досягають шляхом її шифрування. Проте доступні сучасні інформаційні технології відкривають також нові можливості і для порушників інформаційної безпеки, тому використання для захисту даних лише криптографічних засобів сьогодні не гарантує безпечного обміну інформацією в комп'ютерних і телекомунікаційних мережах. Одним із можливих способів рішення зазначеної проблеми інформаційної безпеки є комп'ютерна стеганографія, яка дозволяє передавати повідомлення шляхом вбудовування їх в цифрові дані, що мають аналогову природу – мова, аудіозаписи, зображення, відео, текстові файли і навіть виконувані файли програм. Вбудовування інформації відбувається шляхом її стеганографічного перетворення. Головною перевагою стеганографічних методів захисту інформації є приховування самого факту передачі повідомлення. Найефективнішим способом забезпечення конфіденційності інформації є суміщене використання стеганографічних і криптографічних засобів. Отже, розробка нових та вдосконалення або модифікація існуючих алгоритмів стеганографічних перетворень є досить актуальною задачею, що підлягає вирішенню.

Аналіз останніх досліджень та публікацій. В останні роки спостерігається значне збільшення кількості кібератак, зокрема спроб перехоплення конфіденційної інформації, яка передається засобами глобальних інформаційних мереж. Особливу увагу у наукових публікаціях присвячено основним принципам та засобам забезпечення інформаційної безпеки, серед яких важливе місце посідає організація та здійснення прихованого обміну інформації на основі застосування методів комп'ютерної стеганографії [1-4].

Серед останніх досліджень і публікацій варто виділити дослідження, що стосуються аналітичного огляду великої кількості алгоритмів вбудовування, запропонованих за останні роки [5, 6], класифікації стегосистем та методів вбудовування, формального математичного опису та структурної схеми стеганографічної системи захисту інформації на основі теорії секретних систем, проблем цифрової обробки сигналів, що виникають при вбудовуванні інформації, детального дослідження підвищення пропускної здатності стегоканалу, забезпечення стійкості та непомітності вбудовування [7].

Аналіз останніх досліджень і публікацій [5-7] показує, що найбільшу популярність в комп'ютерній стеганографії здобули стеганографічні методи, які використовують у ролі носія прихованого конфіденційного повідомлення зображення. Цьому сприяє те, що зобра-

ження мають велику надлишковість. Фізіологічні можливості людини є обмеженими, а око людини подібне до низькочастотного фільтру, для якого непомітні спотворення у високочастотній області зображення. Саме принцип, що базується на використанні наявної в зображеннях психо-візуальної надлишковості, покладений в основу методів стеганографії.

Проте дослідженням щодо використання як селектора способу вбудовування інформації в контейнер самого елемента контейнера не приділялась достатня увага.

Мета дослідження – розробити метод формування стеганограми на основі використання значення випадково визначеного ключового елемента, який забезпечує вибір способу вбудовування повідомлення в контейнер.

2. Основний матеріал

Сутність стеганографічного методу вбудовування інформації, що розробляється, полягає у поєднанні процесів стиснення повідомлення та його вбудовування за допомогою заздалегідь визначеного елемента контейнера. Особливістю розробленого методу вбудовування є можливість вибору алгоритмів вбудовування інформації в контейнер, де безпосередньо сам алгоритм вбудовування однозначно визначається ключовим елементом контейнера. Контейнер, який використовується в даному випадку, є нерухомим зображенням. Для забезпечення стиснення інформації визначається зміщення розгорнутої послідовності ключового елемента, кожен елемент якої з урахуванням зміщення відображає номер елемента стегоконтейнера, що збігається з номером елемента повідомлення. В ідеальному випадку при відомому ключовому елементі та зміщенні вбудовування повідомлення в стегоконтейнер проводиться без його модифікації. Проте зміщення залежить від контейнера, ключового елемента та повідомлення і, як правило, на приймальній стороні невідоме. Виходячи з цього, в стегоконтейнер необхідно вбудовувати не саме повідомлення, а зміщення послідовності ключового елемента.

Запропонований стеганографічний метод можливо представити у вигляді етапів виконання процесу вбудовування інформації, які описані нижче.

Етапи реалізації стеганографічного методу:

1. Вибір контейнера для вбудовування повідомлення. Аналіз інформативності елемента контейнера.

2. Генерація способів вбудовування інформації.

3. Визначення кількості способів вбудовування інформації на основі інформативності елемента контейнера.

4.Вибір набору способів вбудовування інформації шляхом обмеження їх кількості на основі псевдовипадкової послідовності(ПВП).

5. Генерація ключової послідовності.

6. На основі стегоключа визначення елемента контейнера, значення якого однозначно здійснює вибір способу вбудовування інформації.

7. Підготовка повідомлення, яке потрібно вбудувати в контейнер.

8. Формування стеганограми. Визначення зміщення ключової послідовності для відображення повідомлення в стегоконтейнері. Здійснення процесу вбудовування зміщення (формалізованого або стисненого повідомлення) у вибраний контейнер за допомогою алгоритму, який визначений елементом контейнера.

9. Передача стегоконтейнера та стегоключа каналами зв'язку.

10. Аналіз отриманої стеганограми.

11. Виокремлення прихованого повідомлення зі стегоконтейнера.

Враховуючи сказане вище, можна визначити, що способи вбудовування обмежуються:

- довжиною повідомлення;
- розміром контейнера;
- інформативністю вибраного ключового елемента контейнера.

Потрібно зазначити, що інформативність ключового елемента контейнера визначається довжиною його коду, яка, в свою чергу, визначає кількість варіантів значень ключового елемента контейнера. Таким чином, максимальне значення інформативності ключового елемента контейнера визначається як

$$I \le 2^n, \qquad (1)$$

де n – довжина коду ключового елемента.

На основі виразу (1) визначимо максимальну кількість способів вбудовування зміщення як

$$S_{max} = C_{t-k}^{V},$$

тут C – кількість сполучень ($C_n^m = \frac{n!}{m!(n-m)!}$); $V = L/m$; t – загальна кількість елементів контейнера; k – кількість ключових елементів контейнера; V – кількість елементів, необхідна для вбудовування повідомлення в контейнер; L – довжина зміщення; m – кількість біт елемента контейнера, що використовують для вбудовування зміщення.

Здійснимо формальну модель стегосистеми, що базується на використанні даного методу вбудовування інформації на основі ключового елемента.

Алгоритм вбудовування повідомлення складається з трьох основних етапів: 1) кодування зміщення (повідомлення); 2) вбудовування повідомлення в кодері; 3) виявлення зміщення в детекторі та виділення повідомлення. При розгляді стегосистеми обмежимося вбудовуванням формалізованих повідомлень (зміщень) та будемо розглядати їх як повідомлення.

Введемо основні функціональні елементи і математичні оператори, що абстрактно описують запропоновану стеганографічну систему захисту інформації.

Нехай W^*, K^*, I^*, B^* є множини можливих формалізованих повідомлень, ключів, контейнерів і способів вбудовування приховуваних повідомлень відповідно. Тоді вибір контейнера для вбудовування повідомлення може бути представлено у вигляді [7]

$$F: I^* \times K^* \times B^* \to W^*, \quad W = F(I, K, B),$$

де W, K, I, B – представники відповідних множин. Крім цього, функція F повинна задовольняти відповідним вимогам, тобто на неї накладаються обмеження, а саме $F(I, K, B) \approx F(I + \varepsilon, K, B)$. Це означає, що незначно змінений контейнер не призводить до зміни повідомлення. Функція F зазвичай складена [7]:

$$F = T \circ G, \text{ де } G: K^* \times B^* \to C^* \text{ та } T: C^* \times I^* \to W^*.$$

Крім цього, запропонований стеганографічний метод характеризується тим, що спосіб вбудовування однозначно визначається елементом контейнера.

Аналіз контейнера здійснюється з врахуванням довжини повідомлення:

$$I \to \text{довж}(W).$$

Контейнер характеризується кількістю елементів (N_e) та інформативністю одного елемента (R_e^i):

$$I \to (N_e, R_e^i).$$

При цьому потрібно, щоб обов'язково виконувалась основна вимога: кількість елементів контейнера повинна бути набагато більша за кількість елементів (довжину) повідомлення, що потрібно приховати:

$$\text{довж}(W) << N_e,$$

де $W = W' + W_{контрол}$; W' – інформаційні розряди повідомлення, а $W_{контрол}$ – додаткові розряди для контролю інформаційних розрядів.

Контроль інформаційних розрядів може бути використаний як для виявлення помилок в інформаційних розрядах, так і для виправлення помилок залежно від введеної надлишковості.

Нехай $W = \{W_0, W_1, W_2, ..., W_m\}$ – множина можливих повідомлень, що з'являються на виході джерела інформації, де символом W_0 формально позначено «пусте повідомлення». Зафіксуємо формально множину інформаційних даних $M = \{M_0, M_1, M_2, ..., M_m\}$, де кожне $M_i, i = 1, 2, ..., m$ відповідає результату попереднього кодування повідомлень із множини W, тобто $M_i = f(W_i), i = 0, 1, 2, ..., m$, де $f(x)$ – формальне позначення функції попереднього кодування, яка реалізується відповідним пристроєм. Тоді основною задачею стеганографічної системи є така організація передачі повідомлень, при якій для будь-якого $W_j, j = 0, 1, 2, ..., m$ відкритий канал зв'язку, що спостерігається порушником, не розрізняється, тобто передача будь-якого із «осмислених повідомлень» $W_1, W_2, ..., W_m$ для порушника не відрізняється від передачі «пустого повідомлення» W_0, коли інформаційні дані зовсім не передаються [7].

Якщо розглядати модель стеганографічної системи з деяким зафіксованим секретним стегоключем, то процес стеганографічного перетворення можна представити у вигляді фіксованого відображення множини *M* відкритих текстів у множину стегограмм E:

$$\varphi_i : M \xrightarrow{K_i} E .$$

Кожне конкретне відображення j_i із множини j відповідає способу вбудовування за допомогою конкретного ключа K_i. Якщо відомий ключ, то в результаті стеганографічного перетворення можливий лише єдиний елемент множини E:

$$E_w = \varphi_i\left(K_i, M_j\right).$$

Зафіксуємо множину відображень:

$$j = \{j_1, j_2, \ldots, j_k\}, \text{ де } \varphi_i : (M, I) \to E, i = 1, 2, \ldots, k,$$

тобто множина відображень, які встановлюють функціональні відповідності кожної пари «інформаційні дані, пустий контейнер» із відповідним заповненим контейнером [7]:

$$E_w = \varphi_i(M_j, L_u) .$$

Зафіксуємо множину ключів $K = \{K_1, K_2, \ldots, K_k\}$ так, що для всіх $i = 1, 2, \ldots, k$ вибір відображення $j_i \in j$ однозначно задається ключем K_i, тобто:

$$\varphi_i : (M, I) \xrightarrow{K_i} E .$$

Кожне конкретне відображення j_i із множини j відповідає способу вбудовування інформаційних даних із множини M в контейнер із множини I за допомогою конкретного ключа K_i, який, в свою чергу, задається випадково вибраним елементом пустого контейнера, тобто спосіб вбудовування в пустий контейнер визначається самою інформацією контейнера:

$$K_i = l_{(k_i)}, \quad (2)$$

де l – це елемент пустого контейнера, а k_i - порядковий номер елемента контейнера, що дорівнює конкретному значенню ключа.

Таким чином, за допомогою відображення j_i (а в нашому випадку це спосіб вбудовування), яке відповідає вибраному ключу K_i, який визначається як (2), по повідомленню M_j, що надійшло, та контейнеру L_u із врахуванням виявлених особливостей формується стеганограма [7]:

$$E_w = \varphi_i(K_i, M_j, L_u),\ i \in [1,2,...,k],\ j \in [0,1,...,m],\ u \in [1,2,...,l],\ w \in [1,2,...,n],\ n = (m+1)l.$$

Процес виявлення особливостей означає необхідність виділення та аналізу особливостей природної надлишковості даних контейнера, які будуть використані при стеганокодуванні та дозволять приховати факт присутності в стеганограмі вбудованих інформаційних даних.

Результат здійснення даного процесу повинен надходити на стеганокодер разом з проаналізованими контейнером.

Для виявлення факту вбудовування інформаційних даних і подальшого їх вилучення на приймальній стороні реалізується зворотне відображення φ_i^{-1} множини E^*.

Процес стеганодекодування реалізує функціональну відповідність кожної пари «прийнята стеганограма, порожній контейнер» з відповідною «оцінкою» M_q^* інформаційних даних M_j [7]:

$$M_q^* = \varphi_i^{-1}(E_q^*, L_u).$$

Кожне конкретне відображення φ_i^{-1} із множини зворотних відображень $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_k^{-1}\}$ відповідає способу стеганодекодування, тобто способу формування «оцінки» M_q^* інформаційних даних M_j. Кожний такий спосіб задається за допомогою конкретного секретного ключа K_i^* зворотного відображення, тобто:

$$\varphi_i^{-1} : (E^*, L) \xrightarrow{K_i^*} M^*.$$

Оскільки секретний ключ при формуванні стеганограми K_i дорівнює випадково вибраному елементу пустого контейнера, тобто $K_i = l_{(k_i)}$, то і секретний ключ K_i^* зворотного відображення повинен збігатися з K_i ($K_i^* = K_i$). А це означає, що на приймальній стороні мати оригінал пустого контейнера не вимагається, і тоді виконується:

$$\varphi_i^{-1} : (E^*) \xrightarrow{K_i^*} M^*.$$

Але це спричиняє вразливість стегосистеми, тому що будь-яка зміна значення елемента контейнера, що є ключовим, навіть помилка при передачі каналами зв'язку, призведе до неможливості проведення процесу стеганодекодування.

Розроблений метод вбудовування повідомлення в стегоконтейнер має і переваги і недоліки.

Основними перевагами даного методу порівняно з LSB є:

1. Залежність алгоритму вбудовування інформації в стегоконтейнер від ключового елемента стегоконтейнера.

2. Зменшення кількості інформації, яку необхідно вбудовувати.

3. Відсутність необхідності передачі контейнера-оригінала для виокремлення прихованого повідомлення зі стегоконтейнера.

Основний недолік запропонованого методу пов'язаний із необхідністю гарантованої передачі ключового елемента контейнера без змін. Помилка в ключовому елементі контейнера призводить до зміни алгоритму розміщення повідомлення в контейнері та неможливості його відтворення одержувачем.

Для забезпечення надійності передачі ключового елемента та підвищення надійності визначення елементів повідомлення в контейнері необхідно використовувати завадостійке кодування.

Завадостійке кодування необхідно використовувати в двох напрямках:

– для забезпечення гарантованої передачі ключового елементу контейнера необхідно застосовувати методи виправлення помилок ключового елемента на основі введення надлишковості. Задача вибору методу завадостійкого кодування ключового елементу на даний час не вирішувалася;

– для підвищення достовірності відтворення повідомлення зі стегоконтейнера доцільно використовувати коди, контролюючі помилки, для побудови кодерів стегосистеми.

Дані пропозиції повинні використовуватися спільно з методами підвищення достовірності повідомлення.

3. Висновки

Розроблений стеганографічний метод забезпечує варіативність алгоритму вбудовування інформації в стегоконтейнер від його ключового елемента, а також стиснення повідомлення при його вбудовуванні. Запропонований стеганографічний метод характеризується тим, що спосіб вбудовування однозначно визначається елементом контейнера. При реалізації даного методу відсутня необхідність передачі контейнера-оригінала для виокремлення прихованого повідомлення зі стегоконтейнера.

Список літератури: 1. *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии и стеганографии. 2-е изд. М.: Горячая линия - Телеком, 2013. 232 с. **2**. *Завьялов С.В., Ветров Ю.В.* Стеганографические методы защиты информации : учеб.пособие. Спб.: Изд-во Политехн. ун-та, 2012. 190 с. ***3***. *Юдин О.К., Корченко О.Г., Конахович Г.Ф.* Захист інформації в мережах передачі даних. К. Вид-во ТОВ «НВП-ІНТЕРСЕРВІС», 2009. 716 с. **4**. *Аграновский А.В.* Стеганография, цифровые водяные знаки и стеганоанализ / Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. М : Изд-во "Вузовская книга", 2009. 220 с. **5**. *Стасюк О.І.* Сучасні стеганографічні методи захисту інформації / Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. // Захист інформації. 2011. № 1. С. 1-7. **6**. *Бабич І.В.* Огляд стеганографічних методів перетворення інформації в зображеннях / Бабич І.В., Паламарчук С.А., Паламарчук Н.А., Овсянніков В.В. // Захист інформації. 2012. № 1. С. 18-24. **7**. *Смирнов А.А.* Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: монография / А.А. Смирнов. К.: Изд. «КОД» 2012. 350 с.

Поступила в редколегію 23.08.2014

Бабенко Віра Григорівна, канд. техн. наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету. Наукові інтереси: системи і методи захисту інформації. Адреса: Україна, 18000, Черкаси, бул. Тараса Шевченка, 333, корп.10, тел.: +380 (472) 71-00-92. Email:zolot_verba@rambler.ru.

Зажома Віталій Михайлович, начальник відділу персоналу Черкаського інституту пожежної безпеки ім. Героїв Чорнобиля НУЦЗ України. Адреса: Україна, 18034,Черкаси, вул. Онопрієнка, 8, тел.: +380 (472) 55-09-39.

Нестеренко Оксана Борисівна, ад'юнкт Черкаського інституту пожежної безпеки ім. Героїв Чорнобиля НУЦЗ України. Адреса: Україна, 18034, Черкаси, вул. Онопрієнка, 8, тел.: +380 (472) 55-09-39.

УДК 629.391

Г.Ф. КОНАХОВИЧ

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ В СПЕКТРАЛЬНУЮ ОБЛАСТЬ ИЗОБРАЖЕНИЙ

Рассматриваются методы стеганографического встраивания скрываемой информации в спектральную область изображения-контейнера. Анализируются существующие стеганографические методы. Описываются показатели эффективности функционирования стеганографических методов для скрытого встраивания информации. Проводится оценка эффективности наиболее распространенных стеганографических методов встраивания в спектральную область.

1. Введение

Современное распространение и развитие информационно-телекоммуникационных сетей диктует необходимость поиска новых подходов для обеспечения требований информационной безопасности. Одним из возможных решений задачи повышения информационной безопасности является применение методов цифровой стеганографии. Подходы, основанные на цифровой стеганографии, позволяют скрытно передавать информацию в цифровом контейнере. Среди наиболее распространенных методов цифровой стеганографии можно выделить методы встраивания в изображение-контейнер. Это обусловлено рядом причин: распространение цифровых изображений, наличие областей с психовизуальной избыточностью, большой объем пропускной способности стеганографического канала; низкая чувствительность человеческого глаза к незначительным изменениям цвета, яркости и контрастности изображения.

Встраивание скрываемой информации в изображение-контейнер осуществляется в пространственную и спектральную область изображения после преобразования. Для обеспечения стойкости встроенных данных к атакам сжатием в методах стеногрaфического встраивания осуществляется модификация спектральных коэффициентов изображения после преобразования. Отсюда, *цель исследования* – оценить эффективность функционирования существующих методов стеганографического встраивания информации в спектральную область изображения-контейнера.

2. Анализ существующих методов стеганографического встраивания в спектральную область изображения

Среди стеганографических методов встраивания в спектральную область наибольший интерес представляют подходы, которые используют в качестве контейнера изображения, где осуществляется сжатие с потерями (форматы JPEG и JPEG 2000). Актуальность таких методов объясняется устойчивостью встроенных данных к атакам сжатием. Такая устойчивость обеспечивается в результате встраивания в область коэффициентов преобразований, используемых в алгоритмах сжатия.

Рассмотрим типы трансформаций для спектрального представления изображения. Среди таких преобразований можно выделить:

– дискретное косинусное преобразование (ДКП);
– дискретное вейвлет-преобразование (ДВП);
– дискретное преобразование Фурье (ДПФ);
– преобразование Карунена-Лоева (ПКЛ).

Такие преобразования обладают хорошими характеристиками робастности. Также среди преимуществ подходов встраивания в спектральную область можно выделить возможность применения трансформаций либо к отдельным частям изображения, либо к изображению в целом. При встраивании целесообразно использовать именно те преобразования изображений, которые будут применяться при атаке сжатием. Алгоритм ДКП является базовым в формате JPEG, а ДВП – в стандарте JPEG 2000. Поэтому для стеганографичес-

кого встраивания для формата JPEG используются коэффициенты ДКП, а для формата JPEG 2000 коэффициенты ДВП.

При встраивании в коэффициенты ДКП изображение вначале разбивается на блоки 8x8 пикселей. Дискретное косинусное преобразование применяется к каждому блоку, в результате чего получаются матрицы коэффициентов ДКП с аналогичным размером.

Для реализации встраивания в коэффициенты ДВП изображение подвергается чередующимся последовательностям вертикальных и горизонтальных одномерных вейвлет-преобразований. Сначала преобразуются все строки, а затем все столбцы. На следующем этапе левая верхняя четверть матрицы, получившейся в результате предыдущего преобразования, опять преобразуется. Количество этапов соответствует количеству уровней вейвлет-декомпозиции. В результате преобразования получается множество частотных диапазонов, которые содержат информацию о том, как ведет себя исходный сигнал (изображение) при разном разрешении.

Рассмотрим стеганографические методы встраивания информации в спектральную область. Такие алгоритмы, как правило, называются по имени разработчиков. В табл. 1 приведены наиболее популярные алгоритмы встраивания скрываемого сообщения в частотную область изображения.

Для удовлетворения требований информационной безопасности стеганографические алгоритмы должны обеспечивать извлечение встроенной информации «вслепую», т.е. в условиях отсутствия исходного скрытого сообщения и изображения-контейнера. Также большой интерес представляют методы, которые обладают высокой стойкостью встроенных данных к внешним воздействиям.

При анализе методов, которые приведены в табл. 1, можно сделать вывод, что наибольшими показателями стойкости встроенных данных к активным атакам обладают следующие алгоритмы: Wang, Ouled-Zaid, Makhloufi & Olivier, Chirag-Ganesh и Li & Zhang.

3. Оценка эффективности методов стеганографического встраивания в спектральную область

Для сравнения и оценки стеганографических алгоритмов встраивания информации в спектральную область необходимо наличие адекватной системы показателей оценки качества их функционирования. Такое оценивание должно давать полную картину успешности их использования для скрытия данных.

Показатели качества стеганографических алгоритмов встраивания в спектральную область можно разделить на следующие группы характеристик:

I. Группа показателей, характеризующих стеганографический метод позиции скрытности, т.е. стойкости метода к выявлению факта скрытого сообщения в изображении.

Качественно скрытность стеганографического алгоритма может быть определена при помощи экспертных оценок.

При наличии исходного изображения-контейнера стойкость стеганографического метода может быть оценена с помощью количественных разностных и корреляционных показателей. Наиболее широко используемым показателем является пиковое отношение сигнал-шум (ПОСШ). Данная величина показывает степень отличия исходного изображения-контейнера от стеганограммы и измеряется в децибелах (дБ). ПОСШ вычисляется на основе следующей формулы:

$$\mathrm{PSNR} = \frac{m \cdot n \cdot \max (I_{i,j})^2}{\sum\limits_{i,j} (I_{i,j} - C_{i,j})^2},$$

где $m \cdot n$ – размер изображения; $I_{i,j}$ – пиксель исходного изображения-контейнера; $C_{i,j}$ – пиксель стеганограммы (изображения со встроенными данными).

Таблица 1

Алгоритмы встраивания в спектральную область изображения-контейнера

Название метода	Область встраивания	Встраиваемая информация	Особенности метода
Elbasi-Eskicioglu	Модификация коэффициентов LL и HH поддиапазонов 2-х уровневого разложения ДВП	Битовая строка	Устойчивость к широкому спектру атак в результате различных частотных поддиапазонов
Wang	Модификация коэффициентов HH поддиапазонов	Битовая строка	Высокая скрытность встраивания
Chirag-Ganesh	Модификация трех коэффициентов LL поддиапазона	Битовая строка	Высокая устойчивость к сжатию с потерями
Fan, Chiang & Shen	Встраивание в область выделяемых регионов (ROI)	Битовая строка	Встроенная информация устойчива к обработке выделяемых регионов. Алгоритм работает только при активированной функции кодирования выделяемых регионов
Ouled-Zaid, Makhloufi & Olivier	Встраивание в коэффициенты LH и LL	Битовая строка	Высокая стойкость к внешним воздействиям
Hsu	Модификация HL и LH областей двухуровневого ДВП	Бинарное изображение	Большой размер скрываемого сообщения, но для извлечения встроенной информации необходимо наличие исходного изображения
Huo-Gao	Модификация коэффициентов HL и LH поддиапазонов 3-х уровневой декомпозиции	Битовая строка	Для изъятия встроенного сообщения не требуется наличие исходного изображения
Meerwald	Встраивание в коэффициенты при квантовании индексов модуляции (QIM)	Битовая строка	Высокая стойкость к внешним воздействиям, но при этом низкая скрытность встраивания
Li & Zhang	Модифицируются коэффициенты в зависимости от целевой скорости битового потока	Битовая строка	Высокая скрытность встраивания

В табл. 2 представлены результаты оценки рассматриваемых методов по величине пикового отношения сигнал-шум для различных классов изображений.

Из анализа значений табл. 2 можно сделать вывод, что увеличение степени сжатия стеганограммы будет сопровождаться уменьшением скрытности встраивания.

II. Группа показателей, характеризующих стеганографический метод с позиции пропускной способности.

Таблица 2

Значения ПОСШ для стеганографических методов встраивания в спектральную область

Название метода	Тип изображения	Коэффициент качества JPEG, %	ПОСШ, дБ
Chirag-Ganesh	Светлые	50	51.5
		90	46.2
	Темные	50	34.7
		90	27.3
Li & Zhang	Светлые	50	49.2
		90	45.5
	Темные	50	39.8
		90	27.6
Wang	Светлые	50	47.8
		90	43
	Темные	50	33.5
		90	26.6
Ouled-Zaid, Makhloufi & Olivier	Светлые	50	52.2
		90	46.7
	Темные	50	36.4
		90	28.2

Здесь под пропускной способностью стеганографического метода понимается максимальное количество информации, которая может быть встроена в один элемент изображения-контейнера при обеспечении требований по скрытности и устойчивости.

Значение пропускной способности для стеганографического метода встраивания в спектральную область определяется на основе следующей формулы:

$$w = 0{,}5 \cdot \log_2 (1 + \frac{\tau_w^2}{\tau_I^2 + \tau_N^2}),$$

где τ_w^2 – мощность встроенного сообщения; τ_I^2 – мощность изображения-контейнера; τ_N^2 – мощность шума при сжатии.

В табл. 3 представлена оценка рассматриваемых методов по значению пропускной способности для изображений с различным размером.

Таблица 3

Значения величины пропускной способности стеганографических методов встраивания

Название метода	Размер изображения, пиксели	Коэффициент качества JPEG, %	Пропускная способность, бит
Chirag-Ganesh	1000x800	50	2246
		90	2870
Li & Zhang	1000x800	50	2594
		90	3050
Wang	1000x800	50	2030
		90	2440
Ouled-Zaid, Makhloufi & Olivier	1000x800	50	2950
		90	3550

Из анализа табл. 3 можно сделать следующие выводы:

– при сжатии изображений более высоким коэффициентом, мощность шума существенно возрастает, что влечет за собой уменьшение пропускной способности;

– наименьшей пропускной способностью обладает метод Wang, наоборот, наибольшая пропускная способность наблюдается для стеганографического метода.

4. Выводы

Проведен анализ наиболее распространенных стеганографических методов встраивания информации в спектральную область изображения-контейнера. Для оценки эффективности функционирования выбрано четыре наиболее устойчивых стеганографических метода.

Проведена оценка скрытности и пропускной способности стеганографических методов встраивания в спектральную область.

Оценка скрытности проводится по величине пикового отношения сигнал-шум. При этом увеличение степени сжатия изображения со встроенными данными будет сопровождаться уменьшением скрытности встроенных данных.

Оценка эффективности максимальной скрытой пропускной способности для исследуемых алгоритмов встраивания показывает, что сжатие изображения более высоким коэффициентом влечет за собой уменьшение пропускной способности.

Список литературы: **1.** *Грибунин В.Г., Оков И.Н., Туринцев И.В*., Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с. **2.** *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288с. 3. *Li Fan, Tiegang Gao* A Novel Blind Robust Watermarking Scheme Based on Statistic Characteristic of Wavelet Domain Coefficients // Proceedings of the 2009 International Conference on Signal Processing Systems. 2009. P. 121-125. **4.** *Li Zhiyong* An Improved Algorithm of Digital Watermarking Based on Wavelet Transform // Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering. 2009. Vol. 7. P. 280-284. **5.** *T. Bianchi, A. Piva, and M. Barni* Composite signal representation for fast and storage-efficient processing of encrypted signals // IEEETrans. Inf. Forensics Security. Mar. 2010. Vol. 5, no. 1. P. 180–187. **6.** *Ouled-Zaid A., Makhlou A., Olivier C*. Improved QIM-Based Watermarking Integrated to JPEG2000 Coding Scheme // Springer journal of Signal, Image and Video Processing/ 2009. Vol. 3. P. 197-207. **7.** *Fan Y., Chiang A., Shen J*. ROI-based watermarking scheme for JPEG 2000 // Springer journal of Circuits, Systems, and Signal Processing 27(5). 2008. P. 763-774.

Поступила в редколлегию 12.07.2014

Конахович Георгий Филимонович, д-р техн. наук, профессор, зав. кафедрой телекоммуникационных систем Национального авиационного университета. Научные интересы: системы и технологии обработки и передачи информации, методы защиты информации. Адрес: Украина, 03680, Киев, просп. Космонавта Комарова, 1.

УДК 004:519.713

В.И. ХАХАНОВ, В.И. ОБРИЗАН, С.А. ЗАЙЧЕНКО, И.В. ХАХАНОВ

MQT-АВТОМАТ ДЛЯ АНАЛИЗА БОЛЬШИХ ДАННЫХ

Предлагается новый подход векторно-логической обработки больших данных с полным исключением арифметических операций, влияющих на быстродействие и аппаратную сложность, который может быть эффективно реализован как на основе использования современных мультипроцессорных цифровых систем на кристаллах, так и с помощью виртуальных параллельных процессоров, функционирующих под эгидой киберфизических систем или облачных сервисов-фильтров. Предлагается модель вычислительного дискретного автомата, которая характеризуется транзакционным взаимодействием компонентов памяти, исполняющих роль комбинационных и последовательностных элементов, реализованных в форме кубитных или «квантовых» примитивов, необходимых для создания параллельных виртуальных компьютеров и облачно-ориентированных процессоров.

1. Введение

Прорывными системо-образующими дизрапторами для инвестиций временных, финансовых и людских ресурсов в ближайшие 8 лет будут: 1) Crowd-sourcing/open-sourcing of hardware development (419240), 2) Changes in educational structure/design (MOOCs) (387777), 3) Virtual/alternative currencies (Bitcoin) (71), 4) Smartphone for payment (216), 5) Cloud computing (20291), 6) Robots as source of labor (281), 7) Nonvolatile memory influencing big data accessibility and portability (2308), 8) Quantum/nondeterministic computing (7653), 9) 3D printing (1335), 10) Green computing (5827), 11) New user interfaces (Siri, Kinect) (11051).

Гармония предполагает создание кибер-интеллекта, который к 2050 году должен позиционироваться как мозг человечества (Humanity Brain); цифровую идентификацию всех физических процессов, объектов и трехмерного пространства с помощью технологий Internet of Things, Smart Everything и Big Data.

При этом можно выделить несколько дифференцирующих принципов, характеризующих Big Data [1-8]. Вместо причинно-следственных связей предлагается использовать доминирование корреляции информационных объектов. Вместо выборки данных (максимум пользы из минимума информации) – полное множество материалов. Вместо хранения данных – инновационно декларируется, что ценность данных заключается в уровне их многократного или массового использования вчера, сегодня и завтра для прогнозирования и/или управления действительностью. Вместо традиционных знаний для понимания прошлого предлагается приобретать способность прогнозировать будущее. Вместо структур данных с жесткими связями – адресная организация физических и виртуальных объектов и процессов. Вместо ручного ввода данных – использование Интернета как входа для киберсистемы: smart everything + internet of everything. Вместо вывода данных за пределы киберпространства – применение в качестве выхода киберсистемы Интернета и управляющих регуляторных воздействий cyber physical systems. Вместо технологий пассивного отображения реального и виртуального мира – киберфизические системы мониторинга и анализа данных для управления физическими и виртуальными процессами. Вместо универсальных и тяжеловесных систем сбора и анализа информации – специализированные виртуальные параллельные мультипроцессоры мониторинга и управления физическими и виртуальными процессами. Вместо хаоса статических данных и знаний в киберпространстве Интернета – постепенная семантическая структуризация динамических потоков больших данных киберфизических процессов и явлений для их эффективного мониторинга, анализа и управления. Вместо неупорядоченных данных, трудных для понимания и использования человеком или киберсистемой – умные, метрически ранжированные информационные структуры, ориентированные на принятие оптимального решения. Вместо обособленного развития реального и виртуального пространств – постепенное создание замкнутой киберфизической экосистемы планеты для совместного гармонического развития реального и виртуального миров. В дополнение к дифференцирующей метрике big data можно еще добавить совсем не уникальную характеристику VVVV: volume – большая размерность данных;

velocity – высокое быстродействие предоставления сервиса; variety – мощная пространственно-временная семантика и онтология данных; veracity – высокая валидность и точность полезной информации.

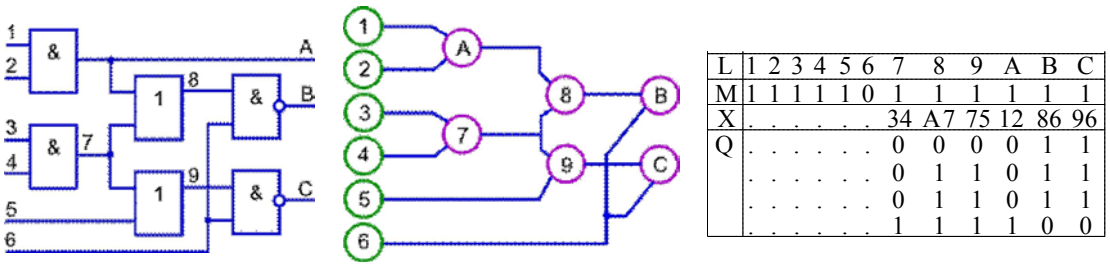
Цель исследования – проектирование виртуальных компьютеров и повышение процессов моделирования за счет использования кубитных структур данных.

Задача - разработка автоматной MQT-модели описания цифровых функциональностей.

2. Автоматная MQT-модель описания цифровых функциональностей

Модельная схемотехника, не привязанная непосредственно к транзисторам, может быть представлена графовыми структурами, в которых каждая вершина отождествляется с функциональным преобразованием, задаваемым кубитным Q-вектором. Тогда дуга определяет взаимосвязи между функциональными кубитными Q-покрытиями, а также входные и выходные переменные. Реализация таких структур связана с ячейками памяти (LUT (Look Up Table) FPGA), которые способны хранить информацию в виде Q-вектора, где каждый бит или разряд имеет свой адрес, отождествляемый с входным словом. Тем не менее, программная реализация таких структур становится конкурентоспособной по быстродействию на рынке проектирования цифровых систем на кристаллах в результате адресной реализации процессов моделирования функциональных примитивов.

Рассмотрим комбинационную структуру (рис. 1), содержащую шесть примитивов и три различных логических элемента. Данной схеме соответствует графовая форма цифровой функциональности, в которой использованы Q-векторы для задания поведения логических примитивов.



L	1	2	3	4	5	6	7	8	9	A	B	C
M	1	1	1	1	1	0	1	1	1	1	1	1
X	.	.	.	.	.	.	34	A7	75	12	86	96
Q	.	.	.	.	.	.	0	0	0	0	1	1
	.	.	.	.	.	.	0	1	1	0	1	1
	.	.	.	.	.	.	0	1	1	0	1	1
	.	.	.	.	.	.	1	1	1	1	0	0

а б в

Рис. 1. Три формы описания структуры логических примитивов

Структура, представленная на рис. 1, содержит 12 линий (дуг), нагруженных на квантовые функциональности (1 = 0001, 7=0111, 14=1110).

Одномерный Q-вектор описания функциональности можно привязать к выходной (внутренней) линии устройства, состояние которой формируется в процессе моделирования рассматриваемого Q-покрытия. Тогда регистровая реализация комбинационного устройства может быть представлена вектором моделирования M, невходные линии которого непосредственно связаны с выходами функциональных элементов. Упорядоченные значения входных переменных задают адрес бита Q-вектора, формирующего состояние рассматриваемой невходной линии (см. рис. 1). Если функциональности описываются одновыходовыми примитивами, то каждый из них можно отождествить или идентифицировать с номером или координатой невходной линии, на которую нагружен данный элемент. Если функциональность многовыходовая, то Q-покрытие представляется матрицей с числом строк, равным числу выходов. Эффект от такого примитива заключается в параллелизме одновременного вычисления состояний нескольких выходов за одно обращение к матрице по текущему адресу.

Данное обстоятельство является существенным аргументом в пользу синтеза обобщенных кубитов для фрагментов цифрового устройства или всей схемы в целях их параллельной обработки в одном временном такте. Близкой к идеальной по компактности и времени обработки структурой данных, где Q-векторы функциональностей и номера входных переменных привязаны к невходным линиям устройства, является таблица, представленная на рис. 1.

Она дает представление о том, какие переменные цифровой схемы являются внешними, сколько функциональных примитивов имеется в структуре, а также какие входы нагруже-

ны на каждый Q-вектор. Достоинством этой таблицы является отсутствие вектора номеров выходов для каждого примитива, но при этом сохраняется необходимость иметь номера входных переменных для формирования адресов, манипулирование которыми есть достаточно времязатратный процесс. Модель функционирования цифровой структуры упрощается до вычисления двух адресов при формировании вектора моделирования

$$M_i = Q_i[M(X_i)]$$

путем исключением сложного адреса выхода примитива в процессе записи состояний выходов в координаты М-вектора.

Иначе, первой выполняется процедура конкатенации состояний битов М-вектора, соответствующих номерам вектора входных переменных Xi. Затем по двоичному вектору сконкатенированных битов, который авляется адресом, считывается соответствующий бит информации из функционального кубит-вектора Qi. Считанный из кубита бит заносится в вектор моделирования М по адресу i. М-вектор может иметь координаты с символами X, что дает возможность выполнять троичное моделирование цифровых устройств для решения задач тестирования и верификации. Сказанное выше иллюстрируется следующим аналитическим выражением (k – число входных переменных i-примитива, * – операция конкатенации битов, A – адрес бита Q-вектора):

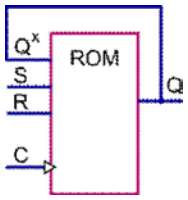
$$\langle M_i \;\; \bar{Q}_i(A) \rangle - \left\langle A \;\; \underset{j\;1}{\overset{k}{*}} M(X_{ij}) \right\rangle - \left\langle \begin{matrix} M \\ X_i \\ Q_i \end{matrix} \right\rangle .$$

Исходя из характеристического уравнения адресно-автоматной модели цифровой системы можно сделать вывод, что современный (виртуальный) компьютер <MQT> следует представлять как адресную организацию структуры функциональных примитивов памяти без гальванических или проводных связей, на которых определены адресные транзакции данных во времени и пространстве для достижения поставленной цели.

Что касается описания последовательностных примитивов (триггеры, регистры, счетчики), то их модели также можно представлять Q-покрытиями или кубитными векторами, которые имеют псевдопеременные для задания внутреннего состояния. Например, функциональное описание SR-триггера трансформируется в квантовый примитив, заданный Q-покрытием, а затем реализуется на адресуемом элементе памяти FPGA с диаграммами проверки, что представлено на рис. 2.

S	R	Q^x	Q
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$\begin{pmatrix} S = a \\ R = b \\ Q^x = c \end{pmatrix} (11110001)(Q = f)$$



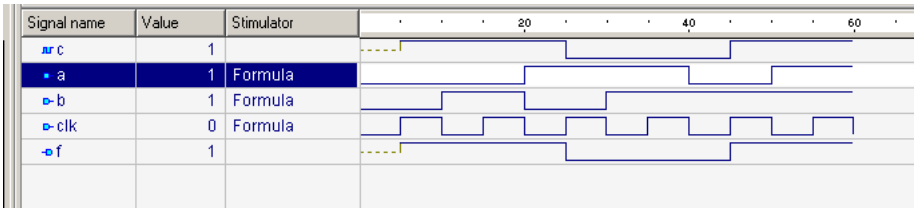


Рис. 2. Реализация SR-триггера на элементе памяти

Таблица истинности триггера может быть представлена в форме вектора выходных состояний $Q(S,R,Q^x) = (11110001)$, который записывается в элемент постоянной памяти, имеющий три адресных входа, сигнал синхронизации, а также обратную связь, которая

соединяет выход элемента памяти с одним адресным входом. HDL-код модели триггера для синтеза и верификации представлен следующим листингом:

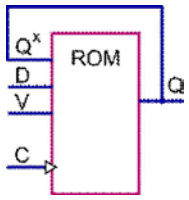
```
use IEEE.STD_LOGIC_1164.all;
use IEEE.STD_LOGIC_unsigned.all;
entity model_RS_flip-flop is
port(
a : in STD_LOGIC;
b : in STD_LOGIC;
clk : in STD_LOGIC;
f : out STD_LOGIC
);
end model_RS_psevdo;

architecture model_RS_psevdo of model_RS_psevdo is
constant func: std_logic_vector(0 to 7):= “11110001”;
— DV-trigger constant func: std_logic_vector(0 to 7):= “01000111”;
signal c: STD_LOGIC;
begin
process(clk)
variable temp:integer;
begin
temp:=conv_integer(a&b&c);
if clk=’1' and clk’event then
c <= func(temp);
end if;
end process;
f <= c;
end model_RS_psevdo;
```

HDL-реализация в системе проектирования Active HDL 9.1 (Aldec Inc.), а также результаты верификации синтезированного SR-триггера (см. рис. 2) подтверждают корректность схемотехнического решения.

Другой пример связан с синтезом на элементе постоянной памяти синхронного DV-триггера. Таблица истинности триггера трансформирована в вектор выходных состояний $Q(D,V,Q^X) = (01000111)$, который записывается в элемент памяти, имеющий три адресных входа, сигнал синхронизации, а также обратную связь, которая соединяет выход примитива памяти с одним адресным входом. Все упомянутые компоненты, включая временные диаграммы верификации HDL-кода модели DV-триггера, представлены на рис. 3.

D	V	Q^X	Q
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$$\begin{pmatrix} D = a \\ V = b \\ Q^X = c \end{pmatrix} (01000111)(Q = f)$$



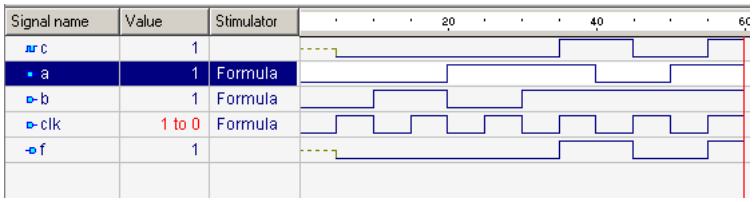
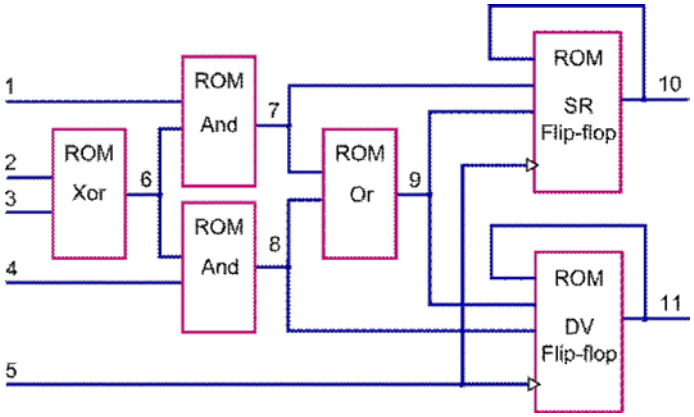


Рис. 3. Реализация DV-триггера на элементе памяти

На рис. 4 изображена схема с триггерами и комбинационной логикой, которая также описана в виде элементов памяти, куда занесены выходные состояния таблицы истинности каждого логического элемента. Структуры данных, необходимые для моделирования циф-

рового устройства, сведены в таблицу, где основными компонентами являются: M – вектор моделирования или состояния занумерованных линий, имеющих в данном случае 5 входных, 6 внутренних и выходных линий, состояния которых подлежат определению; X – вектор номеров входных линий для каждого примитива, необходимых для формирования адреса в целях извлечения по нему состояния выхода элемента Qi, функциональность которого задается Q-вектором.



L	1	2	3	4	5	6	7	8	9	10	11
M	0	0	1	1	1	1	0	1	1	1	1
X	.	.	.	.	.	(2,3)	(1,6)	(6,4)	(7,8)	(10,7,9)	(11,9,8)
Q	.	.	.	.	.	0	0	0	0	1	0
	.	.	.	.	.	1	0	0	1	1	1
	.	.	.	.	.	1	0	0	1	1	0
	.	.	.	.	.	0	1	1	1	1	0
	.	.	.	.	.	.	.	.	.	0	0
	.	.	.	.	.	.	.	.	.	0	1
	.	.	.	.	.	.	.	.	.	0	1
	.	.	.	.	.	.	.	.	.	1	1

Рис. 4. Memory-based комбинационная схема с триггерами

В процессе моделирования адресно извлеченное состояние ячейки Q-покрытия заносится в разряд вектора моделирования M по адресу i. Результаты обработки всех Q-векторов схемной структуры позволили сформировать состояния линий M-вектора (6 – 11). Первоначальные состояния неопределенностей на псевдовходах функциональных примитивов доопределяются сигналами нуля или единицы в зависимости от внутренней технологической культуры компании, предоставляющей промышленные средства моделирования и верификации. Количество входных переменных примитива q связано с длиной Q-вектора соотношением: $\mathrm{card}(Q) = 2^q$. Правильность работы устройства на основе его HDL-описания была также верифицирована с помощью средств моделирования Active HDL 9.1 (Aldec Inc.). Особенность структурно-функционального задания цифровой системы заключается в представлении всех примитивов элементами памяти, куда записываются Q-векторы выходных состояний.

Выводы: 1) Любые структурные компоненты вычислительных устройств, комбинационные и/или последовательностные, а также системы в целом можно описывать кубитными Q-векторами и реализовывать в элементах памяти FPGA, CPLD или VLSI. Это предоставит рынку электронных технологий возможность не использовать reusable логику при синтезе вычислительных устройств, которая составляет сегодня всего 6 процентов аппаратуры SoC (остальные 94% – память), но доставляет разработчикам 90 процентов проблем, связанных с тестированием, верификацией и встроенным дистанционным ремонтом жесткой проводной реализации цифровых изделий. 2) Memory-based интерпретативное адресно-ориентированное моделирование комбинационных и последовательностных примитивов

цифровых устройств становится соизмеримым по быстродействию с компилятивным анализом дискретных объектов. Кроме того, становится возможным реализовывать на программируемых логических устройствах аппаратное моделирование цифровых систем, где комбинационные и последовательностные функциональные примитивы будут представлены стандартными элементами памяти, в которые зашиваются Q-векторы или кубитные покрытия.

Q-метод проектирования кубитного покрытия комбинационной схемы (без таблиц истинности логических элементов). Синтез Q-покрытия схемной структуры на основе примитивов, заданных Q-векторами, сводится к получению обобщенного покрытия-вектора путем декартово-адресного координатного выполнения логической операции над разрядами кубитных векторов. Декартова процедура для двух четырехразрядных кубитов, которые суперпозиционируются логической операцией (or, and, xor), представлена в следующей таблице:

$\vee,\wedge,\oplus$	b(0)	b(1)	b(2)	b(3)
a(0)	$c(0) = a(0) \vee b(0)$	$c(1) = a(0) \vee b(1)$	$c(2) = a(0) \vee b(2)$	$c(3) = a(0) \vee b(3)$
a(1)	$c(4) = a(1) \vee b(0)$	$c(5) = a(1) \vee b(1)$	$c(6) = a(1) \vee b(2)$	$c(7) = a(1) \vee b(3)$
a(2)	$c(8) = a(2) \vee b(0)$	$c(9) = a(2) \vee b(1)$	$c(10) = a(2) \vee b(2)$	$c(11) = a(2) \vee b(3)$
a(3)	$c(12) = a(3) \vee b(0)$	$c(13) = a(3) \vee b(1)$	$c(14) = a(3) \vee b(2)$	$c(15) = a(3) \vee b(3)$

Примеры, использующие логические суперпозиции двух кубитов для получения Q-покрытий схемных структур

$$c_1 = (a_1 \wedge a_2) \vee (b_1 \vee b_2), c_2 = (a_1 \wedge a_2) \wedge (b_1 \vee b_2), c_3 = (a_1 \wedge a_2) \oplus (b_1 \vee b_2),$$

представлены следующей таблицей:

a(and) =	0001
b(or) =	0111
c_1 = a(and) $\vee$ b(or)	0111011101111111
c_2 = a(and) $\wedge$ b(or)	0000000000000111
c_3 = a(and) $\oplus$ b(or)	0111011101111000

Здесь построены Q-покрытия трех схем, состоящих из трех элементов каждая, где два логических примитива суперпозиционно объединяются третьим элементом (or, and, xor). В результате получаются три вектора, каждый из которых имеет размерность в 16 бит. Вычислительная сложность процедуры синтеза Q-покрытия комбинационной схемы равна произведению длин Q-векторов p примитивов, входящих в нее: $\eta = \prod_{i=1}^{p} \mathrm{card}(Q_i)$.

Более сложной представляется проблема синтеза Q-покрытия схемы, входные линии которой имеют гальванические или проводные соединения (здесь по переменной a_2): $c = (a_1 \wedge a_2) \vee (a_2 \vee a_3)$. В данном случае после синтеза Q-покрытия схемы необходимо выполнить его верификацию относительно существования противоречивых адресов на переменных a_2 в целях минимизации Q–вектора путем последующего исключения упомянутых адресов из рассмотрения, что уменьшает размерность Q-покрытия до $\mathrm{card}(Q) = 2^q$ координат, где q – общее число входных переменных схемы:

Q =	0111011101111111
a_1 =	0000000011111111
a_2 =	0000111100001111
a_2 =	0011001100110011
a_3 =	0101010101010101

=

Q =	0111011101111111
a_1 =	0000000011111111
a_2 =	00xx xx1100xx xx11
a_2 =	00xx xx1100xx xx11
a_3 =	0101010101010101

=

Q =	01110111
a_1 =	00001111
a_2 =	00110011
a_2 =	00110011
a_3 =	01010101

=

Q =	01110111
a_1 =	00001111
a_2 =	00110011
a_3 =	01010101

Процедура синтеза Q-покрытия: строится таблица соответствия адресов разрядам Q-вектора схемы; далее противоречивые координаты по двум строкам a_2 отмечаются символами x; затем все столбцы с данными символами исключаются из таблицы; после чего получаются две идентичные строки a_2, которые объединяются в одну, что дает в результате Q-вектор комбинационной схемы, но уже существенно меньшей размерности. Преимущества предложенного Q-метода синтеза вычислительных устройств, которые заключаются в компактности их описания Q-векторами и высоком быстродействии адресного моделирования логических элементов, создают условия для рыночно привлекательной «квантовой» теории проектирования цифровых систем на кристаллах, использующей векторно-кубитную форму задания структурных компонентов.

Анализ кодов адресного пространства. Вопрос – можно ли синтезировать кубит-вектор схемы без явного задания адресного пространства? Чтобы ответить на данный вопрос необходимо научиться минимизировать или уменьшать размерность Q-вектора в зависимости от гальванических соединений входных линий (существенности входных переменных). В такой постановке состояния Q-вектора не влияют на формирование нового уменьшенного адресного пространства, а следовательно, на размерность самого Q-вектора. Она зависит только от фактического гальванического соединения входных переменных между собой, которые накладывают ограничения, связанные с непротиворечивостью сигналов на соединенных переменных. Поэтому правило минимизации адресного пространства заключается в устранении адресных кодов, которые создают противоречия по соединенным переменным. Пусть имеется Q-вектор схемы и его адресное пространство, где переменные b,c,d (a,b,c) соединены гальванически. Ниже приведены таблицы преобразования или минимизации адресного пространства в целях получения уменьшенного Q-вектора:

Q =	0111011101111111
a =	0000000011111111
b =	0000111100001111
c =	0011001100110011
d =	0101010101010101

Q =	0xxx xxx10xxx xxx1
a =	0000000011111111
b =	0xxx xxx10xxx xxx1
c =	0xxx xxx10xxx xxx1
d =	0xxx xxx10xxx xxx1

=

Q	0101
a =	0011
b =	0101

Q =	0111011101111111
a =	00xx xxxx xxxx xx11
b =	00xx xxxx xxxx xx11
c =	00xx xxxx xxxx xx11
d =	0101010101010101

=

Q	0111
a =	0011
d =	0101

Во-первых, здесь следует отметить, что в таблицах наблюдается зеркальная осевая симметрия с инверсией сигналов на координатах адресного пространства, которая создает свойство, описываемое следующим выражением: $L \oplus R = 1 \rightarrow L_{ij} \oplus R_{ij} = 1.$ Данное обстоятельство следует использовать для уменьшения размерности анализируемого пространства в два раза и соответствующего снижения вычислительной сложности задачи синтеза квантовой вектор-функциональности цифровой схемы. Во-вторых, количество различных вариантов взаимодействий на q входных переменных, связанных с гальваническим соединением различных сочетаний входных линий, определяется функциональной зависимостью, значения которой находятся в интервале: $\mathrm{card}(Q) = [2^q - 3^q]$. Тем не менее, имеется эффективная процедура для минимизации размерности Q-вектора путем выявления противоречий в кодах-столбцах, на координатах (Aij), соответствующих гальванически связанным w-переменным по j-параметру. Такую процедуру достаточно выполнить на половине адресного пространства $\mathrm{card}(Q) = 2^{q/2}$, а остальная часть противоречивых столбцов удаляется в соответствии с зеркальным отображением номеров тех столбцов, которые были удалены из первой половины таблицы кодов адресов:

$$\{Q_i, Q_{2^q-i}\} = \varnothing \leftrightarrow (\bigwedge_{j=1}^{w} A_{ij}) \oplus (\bigvee_{j=1}^{w} A_{ij}) = 1,\ i \le 2^q/2.$$

Если в столбце Ai на группе из w связанных переменных зафиксировано, что конъюнкция их состояний равна нулю, а дизъюнкция имеет значение единицы, то i-столбец и его зеркальное отображение $2^q - i$ удаляются из адресного пространства A, что автоматически приводит к исключению из Q-вектора двух полученных $\varnothing$-координат (в таблицах обозначены символами x), соответствующих данным столбцам.

Естественно, что также наблюдается симметрия пространства векторов-расстояний по Хэммингу, полученных путем xor-взаимодействия между соседними строками таблицы адресного пространства, для которых суперпозиция левой и правой частей дает результат $L \oplus R = 0 \rightarrow L_{ij} \oplus R_{ij} = 0$:

Q =	0111011101111111
a ⊕ b	0000111111110000
b ⊕ c	0011110000111100
c ⊕ d	0110011001100110
d ⊕ a	0101010110101010

$= (L, R);\ (L \oplus R) =$

Q =	0111011101111111
a ⊕ b	00000000
b ⊕ c	00000000
c ⊕ d	00000000
d ⊕ a	00000000

$\leftrightarrow (L = \overline{R})$

Целесообразно ли минимизировать логическую функцию, описанную квант-вектором? Ответ: минимизация Q-векторов для получения нормальных или скобочных форм не имеет практического значения, существенно только уменьшение размерности вектора функционального описания, что может быть лишь следствием определения несущественности некоторых входных (адресных) переменных. Тем не менее, существует проблема разбиения квант-вектора на составляющие части меньшей размерности, что связано с имплементацией функциональности в конструктивные компоненты LUT FPGA. В этом случае выполняется разбиение Q-вектора на два равных подвектора Q=(L,R), которые соединяются в структурно-адресную организацию функциональности с помощью мультиплексора $Q = (\bar{a} \wedge L) \vee (a \wedge R)$. Если переменная мультиплексирования a=0, то функциональность Q формируется с помощью ячеек левого L-вектора, в противном случае, когда a=1, значение функции Q формируется битами правого R-вектора. Алгоритмы разбиения и имплементации сложных логических функций имеются в каждой промышленной системе синтеза, моделирования и верификации компонентов SoC.

3. Выводы

Предложена новая модель технологии проектирования (виртуального) компьютера, которая характеризуется: 1) использованием элементов памяти для реализации транзакционного взаимодействия всех компонентов операционного и управляющего автоматов; 2) концепцией синтеза и анализа, основанной на суперпозиции кубит-векторных примитивов задания функциональностей, имплементируемых в элементы памяти, что дает возможность существенно повысить быстродействие средств моделирования и верификации, а также значительно упростить процедуры создания виртуальных облачных компьютеров.

Предложен новый подход векторно-логической обработки больших данных с полным исключением арифметических операций, влияющих на быстродействие и аппаратную сложность, может быть эффективно реализован как на основе использования современных мультипроцессорных цифровых систем на кристаллах, так и с помощью виртуальных параллельных процессоров, функционирующих под эгидой киберфизических систем или облачных сервисов-фильтров.

Фактическая реализация подхода основана на предложении инновационных моделей и методов, использующих идею векторно-логической метрики киберпространства:

1. Метрика анализа киберпространства (big data), которая характеризуется применением единственной логической xor-операции для определения кибер-расстояния путем циклического замыкания не менее одного объекта, что дает возможность на порядок повысить

быстродействие анализа big data и подсчет структурных критериев качества взаимодействия информационных объектов на основе использования векторных логических операций для точного поиска, распознавания образов и принятия решений [9].

2. Новая модель вычислительного дискретного автомата, которая характеризуется транзакционным взаимодействием компонентов памяти, исполняющих роль комбинационных и последовательностных элементов, реализованных в форме кубитных или «квантовых» примитивов, что дает возможность создавать параллельные виртуальные компьютеры для эффективного решения задач анализа big data без наличия арифметических команд и обеспечивать высокое быстродействие облачно-ориентированных процессоров. Дано более простое, ориентированное на киберпространство, определение компьютера –<MQT> есть (адресная) структурно-функциональная организация памяти, на которой заданы транзакции данных во времени и пространстве для достижения поставленной цели.

Практическая значимость предложенных моделей заключается в необходимости реструктуризации киберпространства путем замены концепции аморфных big data на семантически классифицируемую информационную инфраструктуру полезных данных, предназначенных для управления киберфизическими процессами. В связи с этим предложены направления формирования технологической культуры big data для постепенного повышения уровня полезной информации от 0,4 до 10% путем компетентностной инфраструктуризации киберпространства больших данных.

Дальнейшие исследования будут направлены на проектирование big data driven cyber physical systems, которые ориентированы на постоянную метрико-семантическую реструктуризацию киберпространства в целях удобного извлечения знаний.

Список литературы: 1. [http://www.tssonline.ru/articles2/fix-corp/rost-obema-informatsii – realii-tsifrovoy-vselennoy#sthash.rpNOdQLF.dpuf] **2.** *Mayer-Schцnberger V.* Big Data: A Revolution that Will Transform How We Live, Work / V. Mayer-Schцnberger, K. Cukie / Виктор Майер-Шенбергер, Кеннет Кукьер. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. Изд-во: Манн, Иванов и Фербер. 2013. 240 с. **3.** *Demchenko Y., de Laat C., Membrey P.* Defining architecture components of the Big Data Ecosystem // International Conference on Collaboration Technologies and Systems (CTS). 2014. P. 104 – 112. **4.** *Grolinger K., Hayes M., Higashino W.A., L'Heureux A., Allison D.S., Capretz M.A.M.* Challenges for MapReduce in Big Data // IEEE World Congress on Services (SERVICES). 2014. P. 182 – 189. **5.** *Lichen Zhang.* A framework to specify big data driven complex cyber physical control systems // International Conference on Information and Automation (ICIA). 2014. P. 548 – 553. **6.** *Zhang Lichen.* Designing big data driven cyber physical systems based on AADL // International Conference on Systems, Man and Cybernetics (SMC). 2014. P. 3072 – 3077. **7.** *Michalik P., Stofa J., Zolotova I.* Concept definition for Big Data architecture in the education system // 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). 2014. P. 331 – 334. **8.** *Munoz M.* Space systems modeling using the Architecture Analysis & Design Language (AADL) // International Symposium on Software Reliability Engineering Workshops (ISSREW). 2013. P. 97 – 98. **9.** *Хаханов В.И., Мищенко А.С., Обризан В.И., Tamer Bani Amer.* Метрика для анализа BIG DATA // Радиоэлектроника и информатика. 2014. №2. С. 26-29.

Поступила в редколлегию 24.09.2014

Хаханов Владимир Иванович, декан факультета КИУ ХНУРЭ, д-р техн. наук, профессор кафедры АПВТ ХНУРЭ, IEEE Senior Member, IEEE Computer Society Golden Core Member. Научные интересы: техническая диагностика цифровых систем, сетей и программных продуктов. Увлечения: баскетбол, футбол, горные лыжи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. +380 57 70-21-326. E-mail: hahanov@kture.kharkov.ua.

Обризан Владимир Игоревич, старший преподаватель кафедры АПВТ ХНУРЭ. Научные интересы: облачные технологии, программирование мобильных платформ. Увлечения: путешествия. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. +380 57 70-21-326, E-mail: Volodymyr.obrizan@gmil.com.

Зайченко Сергей Александрович, канд. техн. наук, доцент кафедры АПВТ ХНУРЭ. Научные интересы: автоматизированное проектирование и верификация цифровых систем. Увлечения: технологии онлайн-образования. Адрес:Украина, 61045, Харьков, ул. Космическая, 23а, тел. (057)-760-47-25.

Хаханов Иван Владимирович, студент факультета компьютерной инженерии и управления ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, программирование. Увлечения: горные лыжи, английский язык. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. +380 57 70-21-326.

РЕФЕРАТИ

УДК 629.391

Концепція структурного стеганографічного кодування з маскуванням / Д.В. Бараннік, А.Е. Бекіров // АСУ та прилади автоматики. 2014. Вип.168. С. 4 – 11.

Розглянуто використання нерівновагового позиційного кодування як функціонального перетворення для числа з вбудованою інформацією. Обґрунтовано появу структурної надлишковості в процесі нерівновагового позиційного кодування. Запропоновано використовувати наявність потенційної надлишковості для стеганографічного вбудовування інформації. Розроблено стеганографічний метод на основі прямого та зворотного функціонального перетворення для нерівновагового позиційного числа з імплантованим елементом, який забезпечується вбудовування та вилученням. Створено правило вбудовування інформації для структурного стеганографічного кодування.

Іл. 2. Бібліогр.: 4 назви.

УДК 629.391

The concept of structural steganographic encoding with masking / D. Barannik, A. Bekirov // Management Information System and Devices. 2014. N168. P.4-11.

In this article the using of nonequilibrium positional coding as the functional conversion for number with the embedded information is considered. Appearance of structural redundancy in the course of nonequilibrium positional coding is justified. It is offered to use existence of potential redundancy for steganographic embedding of information. The steganographic method on the basis of direct and inverse functional transformation for nonequilibrium positional number with the implanted element providing embedding and exception of the hidden information is developed. The rule of embedding of information for structural steganographic coding is created.

Fig. 2. Ref.: 4 items.

УДК 681.518

Розробка моделі конструктора WEB форм «Alvor form builder» та її реалізація / В.М. Левикін, А.А. Воронін, І.В. Гарячевская//АСУ та прилади автоматики. 2014. Вип.168. С. 11 – 17.

Описано розроблений сервіс - конструктор веб-форм. Даний сервіс дозволяє створювати, зберігати і редагувати розроблені користувачами веб-форми, а також завантажувати файли розмітки і обробників.

Іл. 9. Бібліогр.: 3 назви.

UDC 681.518

Model development Designer WEB forms «Alvor form builder» and its implementation / V. M. Levykin, A. A. Voronin, I. V. Karachevsky // Management Information System and Devices. 2014. N 168. P.11-17.

The developed tools – designer, web-forms and handlers to it. This service allows you to create, store and edit user developed web forms, and download files markup and handlers.

Fig. 9. Ref.: 3 items.

УДК 004.03

Оцінка ефективності інтеграційні рішення на основі сховищ триплетів / І.М. Галушка, С.С. Щербак // АСУ та прилади автоматики. 2014. Вип.168. С. 18 – 23.

Запропонована архітектура інформаційного простору територіально-розподіленого підприємства з вбудованою системою електронного документообігу на основі сховищ триплетів. Формалізовано процес і запропонована методика оцінки ефективності інтеграційних рішень на основі критеріїв тимчасових витрат для забезпечення можливості відстеження зміни продуктивності цих рішень залежно від використання різних типів транзакцій по обробці пов'язаних даних джерел. Запропоновано критерій оцінки ефективності інтеграційних рішень на основі пов'язаних даних, який базується на використанні показників тимчасових витрат, для забезпечення об'єктивної оцінки продуктивності цих рішень.

Іл. 3. Бібліогр.: 13 назв.

UDC 004.03

Evaluation of efficiency of integration solutions based on triplets storages / I.Galushka, S. Shchrerbak // Management Information System and Devices. 2014. N168. P.18-23.

The paper presents the architecture of information space of geographically distributed enterprise with built-in electronic document flow system based on triplets storages. The process is formalized and the technique for evaluating the effectiveness of integration solutions based on time-consuming criteria to enable tracking of change performance of these solutions based on the use of different types of transaction processing related data sources is proposed. The criterion for evaluating the effectiveness of integration solutions based on linked data based on time spent using indicators to ensure objective evaluation of the performance of these solutions.

Fig. 3. Ref.: 13 items.

УДК 621.315.592

Удосконалення математичної моделі розподілу легуючої домішки в процесі вирощування злитків кремнію. / А.В. Луговой, О.С. Притчин //АСУ та прилади автоматики. 2014. Вип.168. С. 24 – 29.

Показано, що легування є основним технологічним процесом, що забезпечує одержання напівпровідників заданого типу провідності, заданого питомого опору і заданої концентрації носіїв заряду. Виконано аналіз впровадження легуючої домішки в злиток при мінливій з часом швидкості росту злитка. Удосконалена модель легування злитка кремнію. Отримано уточнений аналітичний вираз для розрахунку легуючого профілю, який може використовуватися по діапазону типових параметрів росту злитка діаметром 150-300 мм.

Іл. 2. Бібліогр.: 5 назв.

UDC 621.315.592

Improvement of the impurities distribution model in the process of silicon growth / A.V. Lugovoy, O.S. Prytchyn // Management Information System and Devices. 2014. N168. P.24-29.

Doping is the main technological process for obtaining semiconductors of given type conductivity, resistivity and given concentration of charge carriers. As a result of the influence of a variety of complex identifiable factors on the process of doping of the melt distribution of ligature along the length of the ingot has a certain unevenness. In the paper an analysis of the introduction of the dopant in the ingot, with a time varying rate of growth of the ingot conducted. The model of silicon ingot doping improved. Accuracy of the analytical expression for the calculation of the doping profile, which can be used over a range of typical parameters of growth ingot with diameter of 150 - 300 mm increased.

Fig. 2. Ref.: 5 items.

УДК 621.315.59 + 546,681

Дослідження структурних і оптичних характеристик злитків напівізолюючих GaAs великого діаметра /А.П. Оксаніч, М.Г. Когдась, М.С. Андросюк //АСУ та прилади автоматики. 2014. Вип.168. С. 30 – 35.

Розглянуто питання удосконалення методу, методики та апаратури дослідження структурних і оптичних характеристик злитків GaAs. Визначено розподіл поглинання ІЧ-випромінювання по пластині GaAs діаметром 100мм і показується, що в напрямку <001> коефіцієнт поглинання відсутня, а у напрямку <011> зростає, що обумовлено формуванням аномальних оптичних острівців по даному напрямку.

Іл. 2. Бібліогр.: 5 назв.

UDC 621.315.59+546.681

The study of structural and optical characteristics of ingots seminsulating GaAs large diameter / A.P. Oksanych, M.G. Cogdas, M.S. Androsiuk // Management Information System and Devices. 2014. N 168. P.30-35.

They discussed the issues of improvement of the method and apparatus of the study of structural and optical characteristics of GaAs ingots. Determined by the distribution of absorption of IR radiation by GaAs wafer with a diameter of 100mm and it is shown that in the direction <001>, the coefficient of absorption is absent, and in the direction of <011> increases, due to the formation of anomalous optical islets in this area.

Fig. 2. Ref.: 5 items.

УДК 681.518:004.93.1’

Інтелектуальна система підтримки прийняття рішень з оптимізацією просторово-часових параметрів функціонування / В.В. Москаленко, А.С. Рижова // АСУ та прилади автоматики. 2014. Вип. 168. С. 36-43.

Розглянуто алгоритм оптимізації просторово-часових параметрів функціонування інформаційно-екстремальної системи підтримки прийняття рішень для керування нестаціонарним технологічним процесом. Запропоновано визначати з малими обчислювальними затратами межі квазістаціонарних часових інтервалів спостереження, використовуючи нормовані статистики числа потраплянь ознак розпізнавання у свої поля контрольних допусків.

Іл. 5. Бібліогр.: 5 назв.

UDC 681.518:004.93.1’

Intelligent decision support system with optimization of time-spatial parameters of its functioning / V.V. Moskalenko, A.S. Righova // Management Information System and Devices. 2014. N 168. P. 36-43.

In this article the algoritm of the time-spatial parameters optimization of functioning information-extreme Decision Support System for control of non-stationary technological process is considered. Determination of boundaries of quasi-stationary time-intervals of observation with small computational expenses using normalized statistics of number of occurrences features into its receptive fields is proposed.

Fig. 5. Ref.: 5 items.

УДК 681.518.5

Автоматизація пошуку помилок проектування в HDL-моделях кінцевих автоматів/ О.С. Шкіль, Г.П.Фастовець, А.С.Сірокурова // АСУ та прилади автоматики. 2014. Вып. 168. С.43-52.

Запропонована автоматизація діагностування HDL-моделей кінцевих автоматів з використанням програми ASFTEST. Розглянуто варіант відновлення графа переходів по HDL-моделі у формі автоматного шаблону та аналіз обходу усіх дуг графа для пошуку помилок проектування.

Іл. 19. Бібліогр.: 6 назв.

UDC 681.518.5

Search automation of design errors in the HDL-models of finite machines \ A.S. Shkil, Г.П.Фастовець, A.S.Sirokurova // Management Information System and Devices. 2014. N 168. P.43-52.

Proposed automation of diagnosing HDL-models of finite state machines using the program ASFTEST. Consider the option restoring the transition graph of HDL-model of machine in the form of an automaton pattern and analysis of bypass all the arcs to find design errors.

Fig. 19. Ref.: 6 items.

УДК 004.056 (043.2)

Метод вбудовування стегосообщенія на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко // АСУ та прилади автоматики. 2014. Вип. 168. С .53-58.

Розроблений стеганографічний метод вбудовування інформації, здійснюваний на основі використання випадково певного ключового елемента порожнього контейнера, значення якого забезпечує вибір способу вбудовування повідомлення в контейнер. Наведено опис етапів виконання стеганографічного перетворення для розробленого методу вбудовування інформації. Наведено формальну модель стегосистеми, що базується на використанні даного методу вбудовування інформації на основі ключового елемента. Визначено ряд переваг і недоліків розробленого методу вбудовування повідомлення в стегоконтейнер. Основною перевагою даного методу є відсутність необхідності передачі контейнера-оригіналу для відтворення прихованого повідомлення з стегоконтейнер.

Бібліогр.: 7 назв.

УДК 004.056 (043.2)

The method of embedding message based on the key element / V.G. Babenko, V.M. Zazhoma, O.B. Nesterenko// Management Information System and Devices. 2014. N 168. P.53-58.

This paper is designed steganographic method of embedding information, carried out through the use of randomly identify the key elements of the empty container, the value of which provides a variety of ways to embed the message in the container. The description of the stages of steganograpy conversion of developed method of embedding information. Shown stegosystem formal model based on the use of this method of embedding information based on the key element. Identified a number of advantages and disadvantages of this method of embedding the message in stegocontainer. The main advantage of this method is no need to transfer the original container, to reconstruct a hidden message from stegocontainer.

Ref.: 7 items.

УДК 629.391

Оцінка ефективності методів стеганографічного вбудовування інформації в спектральну область зображень / Г.Ф. Конахович // АСУ та прилади автоматики. 2014. Вип. 168. С. 59–63.

Розглянуті методи стеганографічного вбудовування інформації в спектральну область зображення контейнера. Проведено аналіз існуючих стеганографічних методів. Розглянуто показники ефективності функціонування стеганографічних методів для скритного вбудовування інформації. Проведена оцінка ефективності найбільш розповсюджених стеганографічних методів вбудовування в спектральну область.

Табл. 3. Бібліогр.: 7 назв.

UDC 629.391

Performance evaluation steganographic hiding information methods in the spectral region of the images / G.F. Konahovich // Management Information System and Devices. 2014. N 168.P. 59-63.

This article describes methods of steganographic embedding of hidden information in the spectral region of the image container. Analyzes of existing steganographic methods. The indicators of the of the steganographic methods of embed hidden information efficiency are considered. Assess the effectiveness of the most common methods of steganographic embedded in the spectral region.

Tab. 3. Ref.: 7 items.

УДК 004:519.713

MQT-автомат для аналізу великих даних / В.І. Хаханов, В.І. Обрізан, С.О. Зайченко, І.В. Хаханов // АСУ та прилади автоматики. 2014. Вип. 168. С. 64-72.

Запропоновано новий підхід векторно-логічної обробки великих даних з повним виключенням арифметичних операцій, що впливають на швидкодію і апаратну складність. Він може бути ефективно реалізований як на основі використання сучасних мультипроцесорних цифрових систем на кристалах, так і за допомогою віртуальних паралельних процесорів, що функціонують під егідою кіберфізичних систем або хмарних сервісів-фільтрів. Запропоновано модель обчислювального дискретного автомата, яка характеризується транзакційною взаємодією компонентів пам'яті, що виконують роль комбінаційних і послідовних елементів, реалізованих у формі кубітних або «квантових» примітивів, необхідних для створення паралельних віртуальних комп'ютерів і хмарно-орієнтованих процесорів.

Рис. 4. Бібліогр.: 9 назв.

UDC 004:519.713

MQT-automaton for big data analysis / V.I. Hahanov, V.I. Obrizan, S.A. Zaychenko, I.V. Hahanov // Management Information System and Devices. 2014. N 168. P. 64-72.

A new approach for vector-logical processingBig Data based on complete exception of arithmetic operations, which influent on the performance and hardware complexity, is proposed. It can be effectively implemented through the use of both modern multiprocessor digital systems on chips and virtual parallel processors of cyberphysical systems or cloud service-filters. A model of computing discrete automatonis offered. It is characterized by thetransactional interaction of the memory components, which are combinational and sequential elements, implemented in the form of qubit or "quantum" primitives needed to create a parallel virtual computers and cloud-focused processors.

Fig. 4. Refs.: 9 items.

ПРАВИЛА

оформления рукописей для авторов научно-технического сборника

"АСУ и приборы автоматики"

Формат страницы — А4 (210х297мм), поля: сверху, справа, слева, снизу – 30 мм. Редактор: Pagemaker 6.0, 6,5 (можно, но нежелательно Word), гарнитура Times New Roman Cyr, кегль – 11 пунктов, межстрочное расстояние — 110 %, табуляция — 5 мм.

Объем рукописи – до 10 с. (языки: русский, украинский, английский). Содержание должно отражать актуальность исследования, постановку задачи, цель, сущность, научные и практические результаты, сравнение с лучшими аналогами, выводы.

Структура рукописи: заголовок, аннотация, текст, литература, реферат на украинском и английском языках, сведения об авторах.

ОБРАЗЕЦ ОФОРМЛЕНИЯ

УДК 519.713

И.О. ФАМИЛИЯ

НАЗВАНИЕ РУКОПИСИ

Аннотация (абзац 5-10 строк, кегль 10) помещается в начале статьи и содержит информацию о результатах описанных исследований.

Основной текст можно разделять на 2 и более подразделов с заголовками, выделенными полужирным шрифтом, пронумерованными арабскими цифрами, как показано в следующей строке.

1. Название раздела

Рисунки и таблицы (черно-белые, контрастные) помещаются в текст после первой ссылки в виде *переносимых объектов* и раздельно нумеруются, при наличии более одного рисунка (таблицы), арабскими цифрами. Рисунок содержит подрисуночную центрированную подпись (текстовая строка, расположенная вне рисунка, кегль 10) под иллюстрацией, как показано на рис. 1.

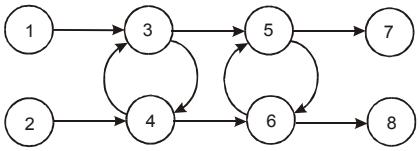


Рис. 1. Граф с контурами

Табличный заголовок располагается справа над таблицей, что иллюстрируется табл.1. Редакторы: CorelDraw, Table Editor и др.

Таблица 1

Шаг i	1	2	3	4	5	6
Ф1(1,3)	1	2	2	4	6	1

Формулы нумеруются при наличии ссылок на них в рукописи. Рекомендуемый кегль формульного набора: обычный (переменная) – 11 пунктов, крупный индекс – 8, мелкий индекс (над- и подиндекс) – 8, крупный символ (основной) – 12, мелкий (индексный) математический символ – 10:

$$F_{i+j} = \sum_{i=1}^{b^k} F_j^i - \prod_{j=1}^{1+h^2} P_{R\,j+i} + F^{j-1} + X^{\Sigma n^k}. \qquad (1)$$

Формат переменных (желательно не курсивом – без наклона) в тексте и формулах должен быть идентичным. В тексте над- и подиндексы составляют 70 % от кегля, которые рекомендуется опускать (поднимать) на 17 (33) % относительно основной строки.

Список литературы (включает опубликованные источники, на которые имеются ссылки в тексте, заключенные в квадратные скобки) печатается без отступа, кегль 9 пунктов.

Образец окончания текста рукописи (литература, сведения об авторах, реферат) представлен ниже.

Список литературы: 1. *Фамилия И.О.* Название книги. Город: Издательство, 1900. 000 с. 2. *Название* сборника / Под ред. И.О. Фамилия. Город: Издательство, 1900. 000 с. 3. *Фамилия И.О.* Название статьи / / Название журнала. Название серии. 1997. Т. 00, № 00. С. 00-00 .

Поступила в редколлегию 00.00.00

Фамилия, имя, отчество, ученая степень, звание, должность и место работы. Научные интересы. Адрес, контактный телефон.

Рефераты на украинском и английском языках:

УДК 000.000.00

Назва статті українською мовою / Ініціали. Прізвище // АСУ та прилади автоматики. 2000. Вип. 00. С. 000-000.

Текст реферату.

Табл. 00. Іл. 00. Бібліогр.: 00 назв.

UDC 000.000.00

Title of paper / Initials. Surname // Management Information System and Devices. All-Ukr. Sci. Interdep. Mag. 2000. N 00. P. 000-000.

Text.

Tab. 00. Fig. 00. Ref.: 00 items.

Представление материалов

Рукопись, реферат, сведения об авторах — в одном файле, *поименованном фамилией первого автора*, на дискете 3,5 дюйма. Твердая копия материалов – для граждан Украины — в одном экземпляре: рукопись, подписанная авторами, рефераты, акт экспертизы, внешняя рецензия, подписанная доктором наук, заявление на имя главного редактора со сведениями об авторах.

Адрес редакции: Украина, 61166, Харьков, пр. Ленина, 14, ХНУРЭ, комната 321, тел. 70-21-326, e-mails: ri@kture.kharkov.ua; hahanov@kture.kharkov.ua. http://www.ewdtest.com/ri

Тематика статей, публикуемых в сборнике:

– Компьютерная инженерия
– Математическое моделирование
– Оптимизация и процессы управления
– Автоматизация проектирования и диагностика
– Информационные интеллектуальные системы
– Проектирование интегральных схем и микросистем
– Компьютерные технологии в образовании

Відповідальний випусковий В.І. Хаханов
Редактор О.П. Гужва
Комп'ютерна верстка Г.В. Хаханова, С.В. Чумаченко

Підп. до друку 27.09.2014. Формат 60x84 1/8. Умов. друк. арк. .
Обл.-вид. арк. 10,2. Тираж 300 прим.
Зам. № б/н. Ціна договірна.

Харківський національний університет радіоелектроніки (ХНУРЕ).
Україна, 61166, Харків, просп. Леніна, 14.

Оригінал-макет підготовлено в навчально-науковому видавничо-поліграфічному центрі ХНУРЕ
Україна, 61166, Харків, просп. Леніна, 14.
Надруковано у видавництві ПП "Степанов В.В."
61168, Харків, вул. Акад. Павлова, 311