МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

ISSN 1563-0064

РАДИОЭЛЕКТРОНИКА И ИНФОРМАТИКА

Научно-технический журнал **Основан в 1997 г.**

№ 2(81), апрель – июнь 2018 **Выходит 4 раза в год**

Свидетельство о государственной регистрации КВ № 12097-968 ПР 14.12.2006

Журнал включен в международные наукометрические базы Index Copernicus, Google Scholar, Cyberleninka, OECSP, OAJI, Scholar Steer, SIS, CiteFactor, TIU Hannover, I2OR, National Library of Ukraine named after Vernadsky V.I. (NBUV).

Відповідно до рішення Атестаційної колегії МОН України щодо діяльності спеціалізованих вчених рад від 12 грудня 2017 р., затвердженого 28 грудня 2017 р. наказом № 1714 “Про затвердження рішень Атестаційної колегії Міністерства щодо діяльності спеціалізованих вчених рад від 12 грудня 2017 року” Міністерства освіти і науки України, журнал "Радіоелектроніка та інформатика" поновлено в Переліку наукових фахових видань України у галузі технічних та фізико-математичних наук.

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ
к тематическому выпуску журнала
«Наукоемкие технологии в инфокоммуникациях: обработка и защита информации»

Наиболее знаковым среди терминов, появившихся в начале XXI века, по праву можно считать «Инфокоммуникации». Темпы развития инфокоммуникаций определяют динамику инфраструктурного обновления социально-экономической среды и перехода к Информационному обществу. Инфокоммуникации – это совокупность методов и средств накопления, обработки, хранения, защиты информации и переноса ее в пространстве, имплементированных в единую сетевую структуру, посредством которой обеспечивается доступность информационных ресурсов и информационный обмен. Развитие инфокоммуникаций является необходимым условием информационного обмена и построения информационной структуры общества. Это дает толчок развитию наукоемких технологий в инфокоммуникациях. Наукоемкость технологий определяется использованием строгого математического аппарата и высокоинтегрированных вычислительных средств при решении задач обработки, передачи и защиты информации в инфокоммуникационных системах. Это определяет актуальность обсуждения данных вопросов среди специалистов, работающих в области инфокоммуникаций.

Кафедра информационно-сетевой инженерии Харьковского национального университета радиоэлектроники совместно с кафедрой боевого применения и эксплуатации АСУ Харьковского национального университета воздушных сил провели в июне 2018 г. международную конференцию на тему «Наукоемкие технологии в инфокоммуникациях», которая связана с основным направлением научных исследований кафедр. Эта конференция продолжила традиции научно-практических семинаров по такой тематике, первый из которых был проведен еще в рамках международной Крымской конференции «КрыМиКо’2013».

На конференции были представлены доклады ведущих ученых по актуальным направлениям высокоинтеллектуальных инфокоммуникационных технологий хранения, обработки, защиты и передачи информации. На конференции работали четыре секции. На 1-й секции рассматривались общие вопросы инфокоммуникаций. На 2-й секции рассматривались вопросы обработки изображений. На 3-й секции рассматривались вопросы обработки даннях. На 4-й секции рассматривались вопросы защиты информации в инфокоммуникационных системах.

Материалы некоторых докладов, представленных на конференции, публикуются в виде статей настоящего тематического выпуска журнала «Радиоэлектроника и информатика». Кроме того, материалы докладов ведущих ученых использованы при подготовке третьего издания коллективной монографии на тему «Наукоемкие технологии в инфокоммуникациях: обработка и защита информации» (под общей редакцией В.М. Безрука, В.В. Баранника).

Заведующий кафедрой информационно-сетевой инженерии ХНУРЭ

д-р техн. наук, проф. В.М. Безрук

РАДИОТЕХНИКА

УДК 537.8.029.6;621.37.029.6

СВЧ СЕНСОР БЫСТРЫХ ТРАНСФОРМАЦИЙ СВОЙСТВ БИОЛОГИЧЕСКИХ ЖИДКОСТЕЙ

ЛЮ ЧАН, БОНДАРЕНКО И.Н., ПАНЧЕНКО А.Ю., СЛИПЧЕНКО Н.И.

Анализируется схема СВЧ сенсора, для которой можно создать строгую аналитическую модель. Рассматривается задача описания полей в рабочей области такого сенсора. Представленная схема допускает возможность использования математической модели и для той части задачи, которая относится к трансформации свойств исследуемого объекта. Обсуждаются предварительные результаты расчетов компонент электромагнитного поля в рабочей области сенсора, дается оценка ее размерам.

Ключевые слова: коаксиальная линия; апертура; емкость; граничные условия; собственные функции; собственные числа; компоненты электромагнитного поля.

Key words: coaxial line; aperture; capacity; border conditions; eigenfunctions; eigenvalues; electromagnetic field components.

1. Введение

Методы СВЧ контроля имеют ряд преимуществ. К ним относятся неинвазивность при исследовании биологических объектов in vivo и скорость измерений. Первичной информацией является комплексная диэлектрическая проницаемость $\tilde{\varepsilon}$, которая в значительной мере зависит от распределения свободной воды и воды, связанной с макромолекулами [1,2]. Скорость процессов создания и разрушения связей может быть высокой, что затрудняет использование биохимических и других методов, требующих подготовки образцов. СВЧ методы позволяют прослеживать изменения параметров биообъектов на протяжении всего периода трансформации. Это делает задачу адаптации СВЧ сенсоров для исследования биообъектов актуальной.

Определение передаточной функции СВЧ сенсора является весьма сложной и громоздкой задачей. Наиболее простой путь ее решения – использование численных методов, которые реализуются современными программными средствами. Эти методы дают наглядное представление распределения компонент электромагнитного поля и численные значения параметров для конкретной конструкции сенсора. Однако проследить зависимости, выяснить взаимосвязи с их помощью затруднительно. Требуются многократные повторения вычислений с эвристическим определением тенденций. Поэтому аналитические методы, результатом которых являются, возможно, громоздкие, но читаемые формулы, в этом случае представляются более предпочтительными.

Целью данной работы является поиск и обоснование на качественном уровне типа сенсора, оптимального для слежения за быстрыми трансформациями биообъектов. При этом необходимо решить задачу оптимизации конструкции так, чтобы можно было составить его строгую математическую модель [3].

2. Выбор типа СВЧ сенсора

СВЧ сенсоры находят все более широкое применение в различных областях [4-6]. Как правило, с их помощью определяют значения реальной ε' и мнимой ε'' части комплексной величины диэлектрической проницаемости $\tilde{\varepsilon}$ исследуемого вещества. Современный уровень развития полупроводниковой электроники СВЧ диапазона делает создание таких измерителей экономически целесообразным. Усложняются конструкции сенсоров [7-9], уточняются методы их описания [10-12].

Используются два типа СВЧ преобразователей: волноводный и резонаторный. Волноводный позволяет измерять в некотором диапазоне частот. Это является важным достоинством. Измерение параметров в диапазоне частот дает информацию, которая в данном случае определяется связью молекул воды с макромолекулами биовещества [1,2]. Но чувствительность у волноводных методов существенно ниже, чем у резонаторных.

Наиболее подходящим типом СВЧ преобразователя является четвертьволновой резонатор (ЧР) с сенсором в виде открытой коаксиальной измерительной апертуры (КИА) [13-15] (рис.1).

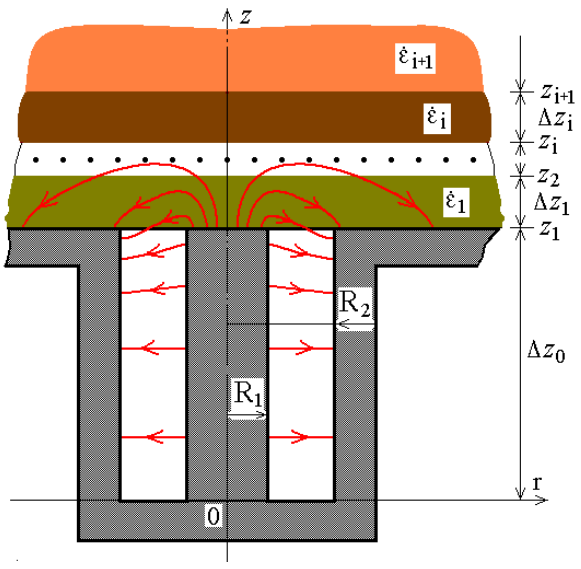


Рис. 1. Схема ЧР с сенсором в виде КИА

Он имеет ряд преимуществ. Значительная часть энергии электрического поля (показано стрелками) находится вне основного резонирующего объема. Поэтому при некоторой потере чувстви-

тельности рабочую область можно расположить вне резонатора. Связь поля резонатора с образцом осуществляется через КИА, которую можно снабдить диэлектрическими вставками, кольцами, позволяющими изменять передаточную функцию. Размеры КИА могут быть существенно меньше длины волны [16-18]. Поэтому сенсор в виде КИА может работать в широком диапазоне частот и с его помощью можно исследовать объекты, вплоть до наноразмерных [7,19,20]. Еще одно достоинство ЧР состоит в том, что он допускает изменение рабочей частоты в широком диапазоне. Для этого достаточно изменять его индуктивную, закороченную часть (Δz_0 на рис.1). Это в целом способствует повышению достоверности любого вида косвенных измерений [4,5,16,21]. В данном случае это достоинство носит принципиальный характер.

Основными критериями при определении формы рабочей области сенсора можно считать возможность неинвазивной диагностики образца in vivo и возможность аналитического представления параметров сенсора. Они определяются через описание компонент электромагнитного поля (ЭМП) в рабочей области. Поиск аналитических представлений полей наиболее доступен в тех случаях, когда образующие рабочей области совпадают с координатными поверхностями. С учетом указанных критериев наиболее рационально выполнить сенсор в виде КИА в плоском экране.

3. Компоненты ЭМП в рабочей области

Основная мода колебаний в ЧР получается трансформацией ТЕМ волны коаксиальной линии вблизи открытого конца. Поэтому в ЧР имеется азимутальная компонента магнитного поля (H_φ), радиальная компонента электрического поля (E_r) и осевая (E_z), которая усиливается вблизи выходной апертуры. На качественном уровне вид распределения электрической компоненты ЭМП в ЧР показан на рис.1.

Строгое математическое представление компонент ЭМП во всем объеме ЧР можно получить на основании известных тензорных функций Грина уравнений Максвелла для цилиндрических областей [22,23]. Поскольку в ЧР имеется только одна компонента магнитного поля, то наиболее просто решение записать для неё. Общее выражение имеет вид:

$$\bar{H}(\vec{r},z)=\int_V \Gamma^M(\vec{r},\vec{r}')\vec{j}^M(\vec{r}')dv .$$

При одной компоненте магнитного поля H_φ связана только с одной составляющей источника j_φ^M. Поэтому из 9 компонент тензора функции Грина для $\bar{H}(\vec{r},z)$ достаточно одной поперечной. При отсутствии вариаций по азимуту она упрощается до

$$G_{n\varphi\varphi}(\vec{r},\vec{r}')=\frac{1}{\lambda_n k_n^2}\frac{\partial}{\partial r}\chi_n(r)\frac{\partial}{\partial r'}\chi_n(r')g_n(z,z'),$$

где $\chi_n(r)$ – собственные функции; λ_n – нормы собственных функций; k_n – собственные числа; g_n – осевая компонента функции Грина.

Собственные функции χ представляются линейными комбинациями функций Бесселя-Неймана вида:

$$\chi_n(r,R)=\left[N_0(k_n r)J_0(k_n R)-J_0(k_n r)N_0(k_n R)\right],$$

где R – граница области.

Если область не ограничена, ряд k_n становится непрерывным: $0\le\kappa<\infty$.

Поскольку ЭМП в данной конструкции проникает только через поверхности поперечного сечения, то магнитные токи j_φ^M выражаются через E_r на этих поверхностях:

$$j_s^M=-\left[\vec{n}_o\vec{E}\right]=\begin{cases}-E_r(r,z=z_{i+1})\\ E_r(r,z=z_i)\end{cases}.$$

Для осевых составляющих функций Грина g_n в общем случае представляет следующий вид:

$$g_n(z,z')=\frac{\gamma_i^{-1}}{sh\,\gamma_i\Delta z_i}\begin{cases}ch\,\gamma_i(z-z_i)ch\,\gamma_i(z_{i+1}-z'), & z<z'\\ ch\,\gamma_i(z'-z_i)ch\,\gamma_i(z_{i+1}-z), & z>z'\end{cases},$$

где γ_i – продольные постоянные распространения.

Для случая неограниченной области: $\gamma_i=\sqrt{\kappa^2-\tilde{\varepsilon}_i k_0^2}$, где k_0 – волновое число в свободном пространстве; $\tilde{\varepsilon}_i$ – комплексная диэлектрическая проницаемость заполняющего материала i-й области. (Для ограниченной области используется k_n).

Выражение для H_φ в i-й неограниченной области имеет вид:

$$H_\varphi(r,z)=-j\omega\varepsilon_0\dot{\varepsilon}_i\int_0^\infty\int_0^\infty\frac{\frac{\partial}{\partial r}(\chi_\infty(r))\frac{\partial}{\partial r'}(\chi_\infty(r'))}{\lambda_\infty\kappa^2\gamma_i}2\pi r'\times$$

$$\times\left[\frac{ch[\gamma_i(z_{i+1}-z)]}{sh(\gamma_i\Delta z_i)}E_r(r',z_i)-\frac{ch[\gamma_i(z-z_i)]}{sh(\gamma_i\Delta z_i)}E_r(r',z_{i+1})\right]d\kappa dr',$$

где ε_0 –диэлектрическая постоянная вакуума;

ω – круговая частота.

Если образец представляет собой многослойную структуру, то можно привести все источники на границах слоев к источнику на апертуре. Для этого нужно записать H_φ над и под каждой гра-

ницей и приравнять их на основании граничных условий $H_{1\tau} = H_{2\tau}$. На основании $E_{1\tau} = E_{2\tau}$ источники на границах равны. Пределы интегрирования и собственные функции χ также одинаковы. Поэтому одинаковыми должны быть подынтегральные выражения для $H_\varphi(r, z_i + 0)$ и $H_\varphi(r, z_{i+1} - 0)$. На основании этого получаем коэффициенты связи между $E_r(r', z_{i+1})$ и $E_r(r', z_i)$ в виде «лестничной» структуры:

$$K_i = \operatorname{csh}(\gamma_i \Delta z_i)\left\{\operatorname{cth}(\gamma_i \Delta z_i) + \frac{\dot{\varepsilon}_{i+1}\gamma_i}{\dot{\varepsilon}_i \gamma_{i+1}}\left[\operatorname{cth}(\gamma_{i+1}\Delta z_{i+1}) - \frac{\operatorname{csh}^3(\gamma_{i+1}\Delta z_{i+1})}{K_{i+1}}\right]\right\}^{-1}.$$

На апертуре можно задать распределение $E_r(r', z_1)$ в виде $E_r = U_0 r'^{-1}$, где напряжение U_0 связано с напряжением между проводниками, образующими апертуру U_a как $U_0 = U_a / \ln(R_2 / R_1)$, что позволит определить величину эквивалентной емкости КИА, а значит, и передаточную характеристику сенсора [24]. Этого будет достаточно в большинстве практических приложений.

Можно использовать более строгий, но более громоздкий подход, включающий решение интегрального уравнения относительно $E_r(r', z_1)$ [25]. Но в обоих случаях поле внутри образца рассчитывается по приведенной выше процедуре.

4. Анализ распределений ЭМП КИА

Слоистый образец может быть приближенным представлением биологического объекта в период трансформации его свойств под действием физических или химических факторов, действующих со стороны, противоположной экрану. Но для создания строгой математической модели необходимо исключить влияние процессов на краях образца. Для этого радиальный размер образца должен быть существенно больше области, в которой сосредоточена основная энергия электромагнитного поля апертуры.

На качественном уровне оценить необходимые размеры вставки позволит визуализация распределения компонент ЭМП вблизи апертуры. Для этого используем наиболее простой вариант расчета с заданием источников поля в плоскости апертуры в виде $E_r(z_1) = U_0 r'^{-1}$. В этом случае выражения для распределений H_φ, E_r и E_z упрощаются до интегралов по волновым числам:

$$H_\varphi(r, z) = -j\omega\varepsilon_0 \tilde{\varepsilon}_1 U_0 \int_0^\infty \frac{[J_0(\kappa R_1) - J_0(\kappa R_2)]J_1(\kappa r)}{\gamma_1 \exp[\gamma_1(z - z_1)]} d\kappa,$$

$$E_r(r, z) = -U_0 \int_0^\infty \frac{[J_0(\kappa R_1) - J_0(\kappa R_2)]J_1(\kappa r)}{\exp[\gamma_1(z - z_1)]} d\kappa,$$

$$E_z(r, z) = U_0 \int_0^\infty \frac{[J_0(\kappa R_1) - J_0(\kappa R_2)]J_0(\kappa r)}{\gamma_1 \exp[-\gamma_1(z - z_1)]} \kappa d\kappa.$$

Для расчетов выберем наиболее простые условия: размеры апертуры $R_1 = 1$ мм, $R_2 = 2$ мм, напряжение $U_0 = 1$В, рабочая частота ЧР $\omega = 2\pi \cdot 10^{10}$ Гц, диэлектрическая проницаемость вставки $\tilde{\varepsilon}_1 = 3 + i0{,}001$. Размеры образца существенно больше размеров апертуры.

На рис. 2,3 представлены распределения магнитной компоненты ЭМП – $H_\varphi(r, z)$ [А/м] и радиальной компоненты электрического поля КИА $E_r(r, z)$ [кВ/м].

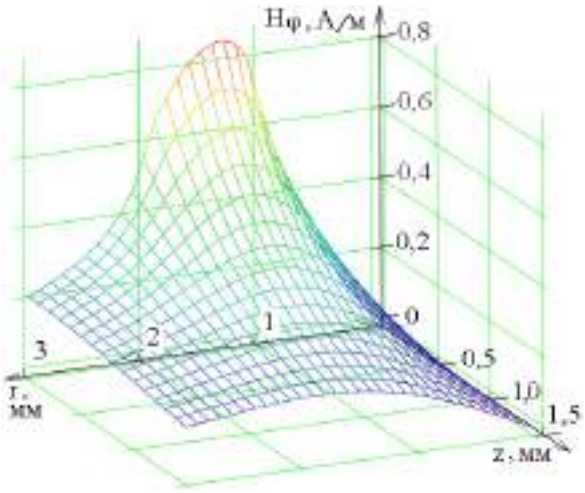


Рис. 2. Распределение $H_\varphi(r, z)$

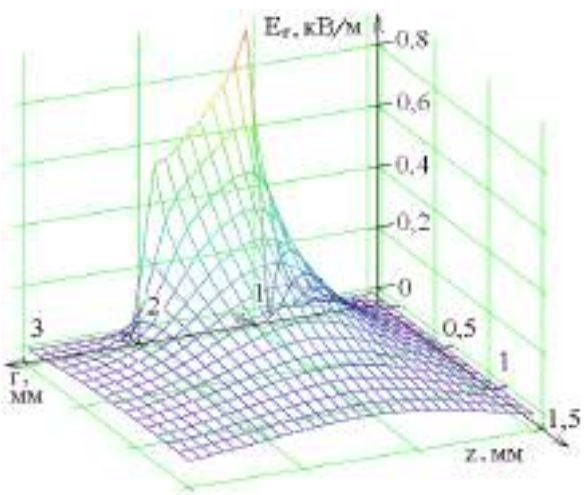


Рис. 3. Распределение $E_r(r, z)$

Основная энергия полей сосредоточена в области, прилегающей к апертуре, причем радиальная компонента электрического поля сконцентрирована в большей степени.

Осевая компонента электрического поля $E_z(r,z)$ в радиальном направлении затухает также быстро, но вдоль оси этот процесс идет медленнее (рис.4.).

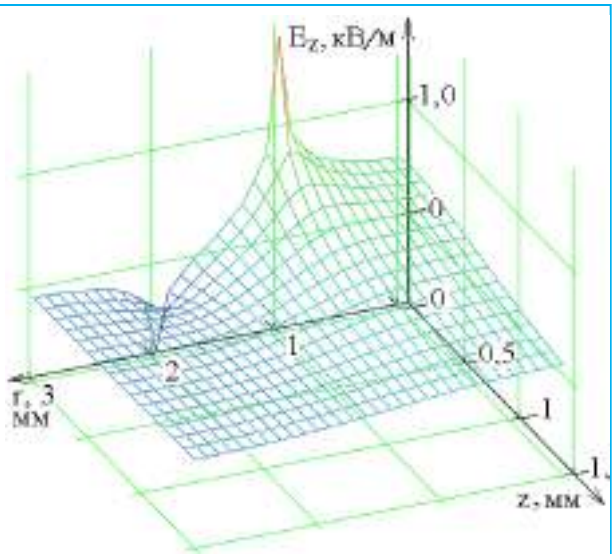


Рис. 4. Распределение $E_z(r,z)$

Поскольку воздействие диэлектрической проницаемости на ЭМП резонатора передается через электрическую компоненту поля, то результат внешнего воздействия на образец со стороны, противоположной экрану, можно будет оценить уже на расстоянии 0,8…1,0 внешнего радиуса апертуры.

В целом можно сделать вывод, что размеры эффективной области взаимодействия соответствуют размерам апертуры. Уменьшение размеров апертуры не имеет теоретических ограничений, поэтому размеры образца, а значит, и быстродействие в случае влияния внешних факторов будут ограничиваться только технологическими возможностями и свойствами самого биообъекта.

5. Выводы

Проведенный анализ соответствует реальным резонаторным преобразователям и имеет практическую ценность. Аналитическое представление обеспечивает возможность количественного определения основных параметров сенсора уже на этапе предварительного проектирования, что необходимо для упрощения этапов моделирования и проектирования конкретных измерителей.

Выбранная схема сенсора позволяет в случае существования аналитической модели процесса трансформации биовещества полностью провести все этапы теоретической градуировки сенсора.

Модельный расчет в данной работе проводился для рабочей частоты 10ГГц. Отметим, что уменьшение рабочей частоты не окажет принципиального влияния на результаты. Поэтому полезным для практического использования является оценка рабочей области для частоты, близкой к частоте релаксации свободной воды. Связь воды с макромолекулами биовещества приведет к снижению реальной части диэлектрической проницаемости и частоты релаксации. В этом случае не менее важным информативным параметром, чем сдвиг рабочей частоты, будет изменение добротности и частотный ход этих параметров. В совокупности эти факторы обеспечат наибольшую информативность измерений.

Литература: 1. *Щеголева Т.Ю.* Гидратное окружение и структура макромолекул // Успехи современной биологии. 1996. Т.116, №6. С.700-714. **2.** *Щеголева Т.Ю.* Исследование биологических объектов в миллиметровом диапазоне радиоволн. К.: Наук. думка, 1996. 182 с. **3.** *Panchenko A.Yu., Slipchenko N.I., Borodkina A.N.* On the development of a practical technique of theoretical calibration of resonant sensors for near-field microwave diagnostics // Telecommunication and Radio Engineering. 2014. V.73, №15. P. 1397-1407. **4.** *Hyde M.W., Havrilla M.J.* A broadband, nondestructive microwave sensor for characterizing magnetic sheet materials // IEEE Sensors J. 2016. V.16, No.12. P. 4740-4748. **5.** *Kempin M., Ghasr M.M., Case J., Zoughi R.* Modified waveguide range for evaluation of stratified composites // IEEE Trans. Instrum. Meas. 2014. V.63, No.6. P. 1524-1534. **6.** *Kaatze U.* Techniques for measuring the microwave dielectric properties of materials // Metrologia, 2012. Vol.47, No.2. P. S91-S113. **7.** *Hyde M. W. IV, Havrilla M. J., Bogle A. E.* Nondestructive Determination of the Permittivity Tensor of a Uniaxial Material Using a Two-Port Clamped Coaxial Probe // IEEE Trans. Microwave Theory and Technique. 2016. Vol.64, No.1. P. 239-246. **8.** *Cenanovic A. Schramm M., Schmidt L.* Measurement setup for non-destructive complex permittivity determination of solid materials using two coupled coaxial probes // IEEE MTT-S Int. Microw. Symp. Dig. 2011. P. 1-4. **9.** *Hyde M. W. et al.* Nondestructive electromagnetic materialcharacterization using a dual waveguide probe: A full wave solution // Radio Science. 2009. V.44, №3, P. 10-14. **10.** *Alanen E., Lahtinen T., Nuutinen J.* Variational Formulation of Open-Ended Coaxial Line in Contact with Layered Biological Medium // IEEE Transaction on biomedical engineering. 1998. Vol.45, No.10. P.1241-1247. **11.** *Huang R.. Zhang D.* Analysis of open-ended coaxial probes by using a two-dimensional Lnite-diŬerence frequency-domain method // IEEE Trans. Instrum. Meas. 2008. Vol.57, No.5. P. 931-939. **12.** *Maftooli H., Karami H.R., Sadeghi S.H.H., Moini R.* Output signal prediction of an open-ended coaxial probe when scanning arbitrary-shape surface cracksin metals // IEEE Trans. Instrum. Meas. 2012. Vol.61, No.9. P. 2384-2391. **13.** *Poumaropoulos C.L., Misra D.* A Study on the Coaxial Aperture Electromagnetic Sensor and Its Application in Material Characterization // IEEE Transaction on instrumentation and measurement. 1994. Vol.43, No.2. P.111-114. **14.** *Blackham D.V., Pollard R.D.* An Improved Technique for Permittivity

Measurements Using a Coaxial Probe // IEEE Transaction on Instrumentation and Measurement. 1997. Vol.46, No.5. P.1093-1099. **15.** *Gregory A.P., Clarke R.N.* Dielectric metrology with coaxial sensors/ A. P.Gregory, // Meas. Sci. Technol. 2007. No.18. P.1372-1386. **16.** *McLaughlin B.L., Robertson P.A.* Miniature open-ended coaxial probes for dielectric spectroscopy applications // J. Phys. D: Appl. Phys. 2007. No.40. P.45–53. **17.** *Nozokido T., Bae J., Mizuno K.* Scanning Near-Field Millimeter-Wave Mi-croscopy Using a Metal Slit as a Scanning Probe // IEEE Transaction on Microwave Theory and Technique. 2001. Vol.49, No.3. P.491-499. **18.** *Panchenko A.Yu.* Modeling a small aperture resonator type microwave meter of substance parameters // Telecommunications and Radio Engineering. 1998. V.52 No.8. P. 118-121. **19.** *Wen Mingming. Ch. Liu, Panchenko A.Yu., Slipchenko N.I.* Evaluation of influence of microwave radiation sensor in the form of an open end of the coaxial line on its metrological characteristics // Telecommunications and Radio Engineering. 2015. V.74, No.15. P.1355-1366. **20.** *Лю Чан, Панченко А.Ю., Слипченко Н.И., Зайченко О.Б.* Ближнеполевой коаксиальный сенсор открытого типа. Оценка пространственной разрешающей способности измерительной апертуры // Вестник НТУ КПИ. Серия Радиотехника. Радиоаппаратостроение. 2017. Вып.71. С.17-24. **21.** *Hosseini M. H. Heidar H., Shams M. H.* Wideband Nondestructive Measurement of Complex Permittivity and Permeability Using Coupled Coaxial Probes // IEEE Transactions on Instrumentation and Measurement. 2017. V.66, №. 1. P. 148-157. **22.** *Панченко Б.А.* Тензорные функции Грина уравнений Максвелла для цилиндрических областей // Радиотехника. 1970. Вып. 15. С. 82-91. **23.** *Tai C.T.* Dyadic Green's functions for a coaxial line. *IEEE* Trans. of Antennas and Propagation. 1983. Vol.48, No.2, P. 355-358. **24.** *Гордиенко Ю.Е., Панченко А.Ю., Фар Р.С.* Приближение заданного поля в задачах определения характеристик резонаторных СВЧ – датчиков апертурного типа // Радиотехника. 1998. Вып.107. С. 93-103. **25.** *Лю Чан, Панченко А. Ю., Слипченко Н. И., Зайченко О. Б.* Коаксиальный сенсор открытого типа. Интегральное уравнение электрического поля в плоскости апертуры // Вестник НТУ КПИ. Серия Радиотехника. Радиоаппаратостроение. 2017. Вып.69. С.11-16.

Transliterated bibliography:

1. *Shhegoleva T.Ju.* Gidratnoe okruzhenie i struktura makromolekul // Uspehi sovremennoj biologii. 1996. T.116. №6. C.700-714.

2. *Shhegoleva T.Ju.* Issledovanie biologicheskih ob#ektov v millimetrovom diapazone radiovoln. K.: Naukova dumka,1996. 182 s.

3. *Panchenko A.Yu., Slipchenko N.I., Borodkina A.N.* On the development of a practical technique of theoretical calibration of resonant sensors for near-field microwave diagnostics // Telecommunication and Radio Engineering. 2014. V.73, №15. P. 1397-1407.

4. *Hyde M.W., Havrilla M.J.* A broadband, nondestructive microwave sensor for characterizing magnetic sheet materials // IEEE Sensors J. 2016. V.16, No.12. P. 4740-4748.

5. *Kempin M., Ghasr M.M., Case J., Zoughi R.* Modified waveguide range for evaluation of stratified composites // IEEE Trans. Instrum. Meas. 2014. V.63, No.6. P. 1524-1534.

6. *Kaatze U.* Techniques for measuring the microwave dielectric properties of materials // Metrologia, 2012. Vol.47, No.2. P. S91-S113.

7. *Hyde M. W. IV, Havrilla M. J., Bogle A. E.* Nondestructive Determination of the Permittivity Tensor of a Uniaxial Material Using a Two-Port Clamped Coaxial Probe // IEEE Trans. Microwave Theory and Technique. 2016. Vol.64, No.1. P. 239-246.

8. *Cenanovic A. Schramm M., Schmidt L.* Measurement setup for non-destructive complex permittivity determination of solid materials using two coupled coaxial probes // IEEE MTT-S Int. Microw. Symp. Dig. 2011. P. 1-4.

9. *Hyde M. W. et al.* Nondestructive electromagnetic materialcharacterization using a dual waveguide probe: A full wave solution // Radio Science. 2009. V.44. №3. P. 10-14.

10. *Alanen E., Lahtinen T., Nuutinen J.* Variational Formulation of Open-Ended Coaxial Line in Contact with Layered Biological Medium // IEEE Transaction on biomedical engineering. 1998. Vol.45, No.10. P.1241-1247.

11. *Huang R.. Zhang D.* Analysis of open-ended coaxial probes by using a two-dimensional Lnite-diŬerence frequency-domain method // IEEE Trans. Instrum. Meas. 2008. Vol.57, No.5. P. 931-939.

12. *Maftooli H., Karami H.R., Sadeghi S.H.H., Moini R.* Output signal prediction of an open-ended coaxial probe when scanning arbitrary-shape surface cracksin metals // IEEE Trans. Instrum. Meas. 2012. Vol.61, No.9. P. 2384-2391.

13. *Poumaropoulos C.L., Misra D.* A Study on the Coaxial Aperture Electromagnetic Sensor and Its Application in Material Characterization // IEEE Transaction on instrumentation and measurement. 1994. Vol.43, No.2. P.111-114.

14. *Blackham D.V., Pollard R.D.* An Improved Technique for Permittivity Measurements Using a Coaxial Probe // IEEE Transaction on Instrumentation and Measurement. 1997. Vol.46, No.5. P.1093-1099.

15. *Gregory A.P., Clarke R.N.* Dielectric metrology with coaxial sensors/ A. P.Gregory, // Meas. Sci. Technol. 2007. No.18. P.1372-1386.

16. *McLaughlin B.L., Robertson P.A.* Miniature open-ended coaxial probes for dielectric spectroscopy applications // J. Phys. D: Appl. Phys. 2007. No.40. P.45–53.

17. *Nozokido T., Bae J., Mizuno K.* Scanning Near-Field Millimeter-Wave Mi-croscopy Using a Metal Slit as a Scanning Probe // IEEE Transaction on Microwave Theory and Technique. 2001. Vol.49, No.3. P.491-499.

18. *Panchenko A.Yu.* Modeling a small aperture resonator type microwave meter of substance parameters // Telecommunications and Radio Engineering. 1998. V.52 No.8. P. 118-121.

19. *Wen Mingming. Ch. Liu, Panchenko A.Yu., Slipchenko N.I.* Evaluation of influence of microwave radiation sensor in the form of an open end of the coaxial line on its

metrological characteristics // Telecommunications and Radio Engineering. 2015. V.74, No.15. P.1355-1366.

20 *Lju Chan, Panchenko A. Ju., Slipchenko N. I., Zajchenko O. B.* Blizhnepolevoj koaksial'nyj sensor otkrytogo tipa. Ocenka prostranstvennoj razreshajushhej sposobnosti izmeritel'noj apertury // Vestnik NTU KPI. Serija Radiotehnika. Radioapparatostroenie. 2017. Vyp.71. S.17-24.

21. *Hosseini M. H. Heidar H., Shams M. H.* Wideband Nondestructive Measurement of Complex Permittivity and Permeability Using Coupled Coaxial Probes //IEEE Transactions on Instrumentation and Measurement. 2017. V.66. №. 1. P. 148-157.

22. *Panchenko B.A.* Tenzornye funkcii Grina uravnenij Maksvella dlja cilindricheskih oblastej // Radiotehnika: Vseukrainskij mezhvedomstvennyj nauchno-tehnicheskij sbornik. 1970. Vyp. 15. S. 82-91.

23. *Tai C.T.* Dyadic Green's functions for a coaxial line. *IEEE* Trans. of Antennas and Propagation. 1983. Vol.48, No.2, P. 355-358.

24. *Gordienko Ju.E., Panchenko A.Ju., Far R.S.* Priblizhenie zadannogo polja v zadachah opredelenija harakteristik rezonatornyh SVCh - datchikov aperturnogo tipa // Radiotehnika: Vseukrainskij mezhvedomstvennyj nauchno-tehnicheskij sbornik. 1998. Vyp.107. S. 93-103.

25. Lju Chan, Panchenko A. Ju., Slipchenko N. I., Zajchenko O. B. Koaksial'nyj sensor otkrytogo tipa. Integral'noe uravnenie jelektricheskogo polja v ploskosti apertury // Vestnik NTU KPI. Serija Radiotehnika. Radioapparatostroenie. 2017. Vyp.69. S.11-16.

Поступила в редколлегию 03.04.2018

Рецензент: д-р физ.-мат. наук, проф. Грицунов А.В.

Лю Чан, Ph.D, начальник отдела внешних связей, преподаватель института электротехники и информатики Хэйлунзянского Бауи аграрного университета. Научные интересы: электродинамика, акустика. Адрес: ул. СинФон 5, г. Дачин, Хэйлунзян, КНР 163319.

Бондаренко Игорь Николаевич, д-р физ.-мат. наук, профессор, заведующий кафедрой микроэлектроники электронных приборов и устройств ХНУРЭ. Научные интересы: электродинамика, СВЧ техника. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. +38057-7021362.

Панченко Александр Юрьевич, д-р физ.-мат. наук, профессор, заведующий кафедрой проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: электродинамика, акустика атмосферы. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. +38057-7021494.

Слипченко Николай Иванович, д-р физ.-мате. наук, профессор, проректор по научной работе ХНУРЭ. Научные интересы: электродинамика, техника СВЧ, нанотехнологии, солнечная энергетика. Адрес: Украина, 61166, Харьков, пр. Науки, тел. +38057-7021013.

Liu Chang, PhD, Head of External Relations Department, Heilongjiang Bayi Agricultural University, 5, Xinfeng Str., Daqing, 163319, China.

Bondarenko Igor Nikolaevich, Doctor of Physical and Mathematical Sciences, Professor, Professor, Head of the Department of Microelectronics, Electronic Devices and Appliances, Kharkov National University of Radio Electronics. Scientific Interests: Electrodynamics, Microwave Engineering. Address: Ukraine, 61166, Kharkiv, Nauka Ave., 14, Phone/fax: +380577021362, e-mail: ihor.bondarenko@nure.ua

Alexander Panchenko, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Design and Operation of Electronic Devices of the Kharkov National University of Radio Electronics. Scientific interests: electrodynamics, atmospheric acoustics. Address: Ukraine, 61166, Kharkiv, Nauka Ave., 14, Phone/fax: +380577021494, e-mail: oleksandr.panchenko@nure.ua

Nikolai I. Slichenko, Doctor of Physical and Mathematical Sciences, Professor, pro-rector for scientific work of Kharkov National University of Radio Electronics. Scientific interests: electrodynamics, microwave technology, nanotechnology, solar energy. Address: Ukraine, 61166, Kharkiv, Nauka Ave., 14, Phone/fax: +380577021013.

ТЕЛЕКОММУНИКАЦИИ

УДК 621.382

ТЕХНОЛОГИЯ КОДИРОВАНИЯ ПРЕДСКАЗАННЫХ КАДРОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

ХИМЕНКО В.В.

Рассматривается метод кодирования информативных элементов последовательности предсказанных кадров.

Ключевые слова (Key words) предсказанные видеокадры, дифференциально-описанная спектрограмма, информативные элементы; predicted video frames, differential-described spectrograms, informative elements.

1. Введение

Для сокращения межкадровой интегрированной структурной избыточности с учетом особенностей информативной составляющей дифференциально-описанной спектограммы (ДОС) ***предлагается*** осуществлять их обработку по блоковому принципу.

Блоковая обработка информативной составляющей $E_{inf}^{(k,\ell)}$ ДОС :

$$E_{inf}^{(k,\ell)} = \{e(1)_{inf}^{(k,\ell)}; \ldots; e(\tau)_{inf}^{(k,\ell)}; \ldots e(n_{inf})_{inf}^{(k,\ell)}\}$$

обеспечивает условия для:

– выявления дополнительных структурных закономерностей, обусловленных неравномерностью соседних информативных (значимых) элементов $e(\tau)_{inf}^{(k,\ell)}$, т.е. наличием спектральных перепадов между соседними элементами информативной ДОС $E_{inf}^{(k,\ell)}$.

– сокращения количества алгоритмических операций при определении количества элементов, для которых формируется первая часть обобщенного синтаксического представления (ОСП) ДОС, в процессе отбора элементов для формирования составляющих обобщенного кодового значения с использованием значимых (информативных) элементов ДОС и их линейно-масштабирующих составляющих;

– снижения сложности обработки и вероятности возникновения потерь целостности, обусловленных топологической сложностью относительно установления соответствия между структурными компонентами синтаксического описания последовательности Р-кадров и их кодовыми конструкциями в едином битовом потоке. В данном случае за счет формирования единого блокового кода для ДОС упрощается топология кодовых конструкций всей последовательности предсказанных кадров, а именно:

– исключаются маркерные разделители между кодограммами структурных компонент последовательности Р-кадров;

– сокращается количество служебных сведений, используемых для позиционирования кодограмм в едином битовом потоке для последовательности Р-кадров.

В процессе формирования эффективного синтаксического представления информативной ДОС $E_{inf}^{(k,\ell)}$ требуется учитывать, что при формировании линейно-масштабирующих составляющих допускается наличие условия эквивалентности в ограниченном интервале ε_{fix} значений элементов $e(\tau)^{(k,\ell)}$ ДОС. В этом случае в процессе обработки допускается наличие коррекций значений спектральных диапазонов с учетом модели зрительного восприятия видеокадров. Следовательно, дополнительное использование технологий устранения психовизуальной избыточности в процессе формирования синтаксического представления информативной ДОС и вектора линейно-масштабирующих составляющих может быть причиной лавинного размножения ошибок и, как следствие, ухудшения качества или полного разрушения последовательности видеокадров. Поэтому для обеспечения заданного уровня целостности информации необходимо осуществлять обработку дифференциально-описанной спектрограммы без внесения потерь.

Для этого сформулируем и проведем решение следующей задачи.

2. Постановка задачи

Требуется получить систему соотношений $F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)}; \varepsilon_{fix}; \bar{d}_e^{(k,\ell)}; \overline{D''}_{inf}^{(k,\ell)}\}$ для определения кодового значения $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ информативной составляющей $E(\chi;\gamma)_{inf}^{(k,\ell)}$ ДОС (***одномерная последовательность в двухосновном позиционном прореженном пространстве***), а именно:

$$C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e = F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)}; \varepsilon_{fix}; \bar{d}_e^{(k,\ell)}; \overline{D''}_{inf}^{(k,\ell)}\}$$

при следующих ограничениях:

$$\begin{cases} e(\tau)_{inf}^{(k,\ell)} \le \bar{d}(\tau)''^{(k,\ell)}_{inf} = | e_{max}^{(k,\ell)} - e_{min}^{(k,\ell)} | + 1 - \mathrm{sign}(\tau - 1); \\ e_{min}^{(k,\ell)} = \min\limits_{2 \le \tau \le T} \{e(\tau)^{(k,\ell)}\}; \\ e_{max}^{(k,\ell)} = \max\limits_{2 \le \tau \le T} \{e(\tau)^{(k,\ell)}\}; \\ e(\tau)_{inf}^{(k,\ell)} \ne e(\tau(\mathrm{sign}(n_{inf} - \tau) + 1)_{inf}^{(k,\ell)}, \end{cases} \quad (1)$$

$$\tau = \overline{1, n_{inf}}.$$

Здесь приняты такие обозначения:

$E(\chi;\gamma)_{inf}^{(k,\ell)}$ - $(k;\ell)$-а информационная дифференциально-описанная спектрограмма для $(\chi;\gamma)$-го слота последовательности ДОТ кадров;

$\overline{D''}_{inf}^{(k,\ell)}$ - двохкомопнентный вектор динамических диапазонов $\bar{d}(\tau)''^{(k,\ell)}_{inf}$ элементов информативной ссоставляющей $E(\chi;\gamma)_{inf}^{(k,\ell)}$ дифференциально-описанной спектрограммы, а именно:

$$\overline{D''}_{inf}^{(k,\ell)} = \{\bar{d}(1)''^{(k,\ell)}_{inf} = \bar{d}_e^{(k,\ell)};\ \bar{d}(\tau)''^{(k,\ell)}_{inf}\};$$

$\bar{d}_e^{(k,\ell)}$ - величина общего динамического диапазона последовательности $E_{inf}^{(k,\ell)}$, т.е.:

$$\bar{d}_e^{(k,\ell)} = |e_{max}^{(k,\ell)} - e_{min}^{(k,\ell)}| + 1;$$

$e_{min}^{(k,\ell)}$ - минимальное значение элемента в информативной составной дифференциально-описанной спектрограммы, что вычисляется как:

$$e_{min}^{(k,\ell)} = \min_{2 \le \tau \le T} \{e(\tau)_{inf}^{(k,\ell)}\};$$

$e_{max}^{(k,\ell)}$ - максимальное значение элемента в информативной ДОС, которое определяется по формуле:

$$e_{max}^{(k,\ell)} = \max_{2 \le \tau \le T} \{e(\tau)_{inf}^{(k,\ell)}\};$$

$\bar{d}(\tau)''^{(k,\ell)}_{inf}$ - динамический диапазон значений элементов $e(\tau)_{inf}^{(k,\ell)}$ инфоматив ной ДОС в условиях выявления локально-структурных закономерностей, а именно с учетом наличия условия неровности значений сопредельных элементов, т.е.:

$$e(\tau)_{inf}^{(k,\ell)} \ne e(\tau(\text{sign}(n_{inf} - \tau) + 1)_{inf}^{(k,\ell)}; \qquad (2)$$

ε_{fix} - значение интервала эквивалентности элементов ДОС.

Согласно выражению (1), для динамического диапазона $\bar{d}(1)''^{(k,\ell)}_{inf}$ первого элемента $e(1)_{inf}^{(k,\ell)}$ информативной ДОС выполняется соотношение:

$$\bar{d}(1)''^{(k,\ell)}_{inf} = \bar{d}_e^{(k,\ell)} - \text{sign}(1-1) = \bar{d}_e^{(k,\ell)} = |e_{max}^{(k,\ell)} - e_{min}^{(k,\ell)}| + 1.$$

Это обусловлено тем, что для первого элемента вектора значимых (информативных) компонент ДОС отсутствует предыдущий элемент, а следовательно, не накладываются ограничения, которые обусловлены наличием сопредельных элементов с неравными значениями.

3. Суть метода эффективного кодирования информативных элементов последовательности предсказанных видеокадров

Процесс формирования кодового значения $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ для информативной составляющей $E(\chi;\gamma)_{inf}^{(k,\ell)}$ дифференциально-описанной спектрограммы рассматривается как синтез метода, представленного функционалом

$$F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)}; \varepsilon_{fix}; \bar{d}_e^{(k,\ell)}; \overline{D''}_{inf}^{(k,\ell)}\}.$$

Процесс синтеза такого функционала $F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)}; \varepsilon_{fix}; \bar{d}_e^{(k,\ell)}; \overline{D''}_{inf}^{(k,\ell)}\}$ зависит от интерпретации информативной составляющей $E(\chi;\gamma)_{inf}^{(k,\ell)}$ ДОС. В нашем случае для учета выявленных структурных закономерностей в последовательности $E(\chi;\gamma)_{inf}^{(k,\ell)}$ предлагается использовать ее интерпретацию как ***одномерной последовательности в двухосновном*** (базис оснований задается вектором $\overline{D''}_{inf}^{(k,\ell)}$) ***позиционном прореженном пространстве*** (ОПДППП или ОПДП^3), т.е. в ***одноосновном*** (основание $\bar{d}_e^{(k,\ell)}$) ***позиционном пространстве с учетом наличия неравенства между ее соседними элементами***.

Это позволяет описать и учесть наличие выдвинутых закономерностей для последовательностей $E(\chi;\gamma)_{inf}^{(k,\ell)}$, заданных системой (1), путем:

– варьирования значениями и количеством оснований позиционного пространства в соответствии с содержанием вектора $\overline{D''}_{inf}^{(k,\ell)}$;

– прореживания множества $\Omega(n_{inf}; \bar{d}_e^{(k,\ell)})_e$ допустимых последовательностей с учетом устанавливаемых запретов согласно условию неравенства соседних элементов, т.е.

$$e(\tau)_{inf}^{(k,\ell)} \ne e(\tau(\text{sign}(n_{inf} - \tau) + 1)_{inf}^{(k,\ell)},\ \tau = \overline{1, n_{inf}}.$$

Поэтому решение сформулированной задачи, а именно формирование системы выражений для определения кодового значения $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ *предлагается* осуществлять в рамках структурного подхода на базе кодовых конструкций позиционных чисел.

В рамках определения кодовых значений позиционных чисел при наличии дополнительных структурных ограничений необходимо вначале создать соотношения для оценки величины $Q(n_{inf}; \overline{D''}_{inf}^{(k,\ell)})_e$, задающей количество допустимых ОПДП^3 в зависимости от их длины в условиях, когда их элементы удовлетворяют системе ограничений (1). В этом случае речь идет об объеме $Q(n_{inf}; \overline{D''}_{inf}^{(k,\ell)})_e$ множества $\Omega(n_{inf}; \overline{D''}_{inf}^{(k,\ell)})_e$ допустимых ОПДП^3.

Согласно сформулированной интерпретации информативной ДОС величина $Q(n_{inf}; \overline{D''}_{inf}^{(k,\ell)})_e$ будет определяться с использованием следующего соотношения:

$$Q(n_{inf};\overline{D''^{(k,\ell)}_{inf}})_e = \prod_{\tau=1}^{n_{inf}} \bar{d}(\tau)''^{(k,\ell)}_{inf} =$$

$$= \prod_{\tau=1}^{n_{inf}} (\bar{d}_e^{(k,\ell)} - sign(\tau-1)) =$$

$$= (e_{max}^{(k,\ell)} - e_{min}^{(k,\ell)} + 1)(\bar{d}_e^{(k,\ell)} - 1)^{n_{inf}-1} . \quad (3)$$

Здесь учитывается двухосновность позиционного пространства (система выражений (1)), которому принадлежат информативные ДОС. При этом определение оснований проводится с учетом индекса их позиции в информативной ДОС по следующему соотношению:

$$\bar{d}(\tau)''^{(k,\ell)}_{inf} = \bar{d}_e^{(k,\ell)} - sign(\tau-1) = (e_{max}^{(k,\ell)} - e_{min}^{(k,\ell)}) + 1 - sign(\tau-1); \quad (4)$$

$$\tau = 1; \ \tau \geq 2 .$$

Величину $Q(n_{inf};\overline{D''^{(k,\ell)}_{inf}})_e$ согласно структуре множества допустимых позиционных чисел можно интерпретировать как количество $Q(e(0)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e$ допустимых ОПДП^3 (информативных ДОС), у которых первый элемент равен $e(0)^{(k,\ell)}_{inf}$, а остальные n_{inf} элементов принимают значения соответственно системе ограничений (1). С учетом этого величина $Q(e(0)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e$ будет равна:

$$Q(e(0)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e = Q(n_{inf};\overline{D''^{(k,\ell)}_{inf}})_e =$$

$$= \prod_{\tau=1}^{n_{inf}} (\bar{d}_e^{(k,\ell)} - sign(\tau-1)) .$$

Здесь важно отметить, что значение начального (дополнительного, вспомогательного) элемента $e(0)^{(k,\ell)}_{inf}$ выбирается так, чтобы обеспечить выполнение условия:

$$e(0)^{(k,\ell)}_{inf} \neq e(1)^{(k,\ell)}_{inf} .$$

По аналогии получаем, что если значение первого элемента допустимых ОПДП^3 (информативных ДОС) будет равно $e(1)^{(k,\ell)}_{inf}$, а остальные $(n_{inf}-1)$ элементов принимают значения соответственно системе ограничений (1), то количество $Q(e(1)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e$ таких последовательностей будет находиться исходя из выражения:

$$Q(e(1)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e = \prod_{\tau=1}^{n_{inf}-1} (\bar{d}_e^{(k,\ell)} - sign(\tau-1)) =$$

$$= (\bar{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-1} .$$

После этого в общем случае получаем, что если первые τ элементов допустимых последовательностей в ОПДП^3 (информативных ДОС) будут равны соответственно $(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau)^{(k,\ell)}_{inf})$, а оставшиеся $(n_{inf}-\tau)$ элементов принимают значения соответственно системе ограничений (1), то количество таких последовательностей будет равно величине $Q(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e$.

В частном случае, когда для элемента $e(\tau)^{(k,\ell)}_{inf}$ выполнятся ограничение на динамический диапазон, т.е. $e(\tau)^{(k,\ell)}_{inf} \leq \bar{d}_e^{(k,\ell)}$, и не устанавливается требование относительно неравенства с предшествующим элементом, величина $Q(e(1)^{(k,\ell)}_{inf},..., e(\tau)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e$ будет конкретизироваться следующим выражением:

$$Q(e(1)^{(k,\ell)}_{inf},..., e(\tau)^{(k,\ell)}_{inf} < \bar{d}_e^{(k,\ell)}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e =$$

$$= \prod_{\tau=1}^{n_{inf}-\tau} (\bar{d}_e^{(k,\ell)} - sign(\tau-1)) =$$

$$= (\bar{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-\tau} . \quad (5)$$

Теперь допустим, что в этой схеме значение τ-го элемента уже не является фиксированным, т.е. будет принимать некоторые значения в диапазоне $e(\tau)^{(k,\ell)}_{inf,min} \leq \eta \leq e(\tau)^{(k,\ell)}_{inf} - 1$, так чтобы выполнялось условие неравенства с предыдущим $(\tau-1)$-м элементом, т.е. $e(\tau-1)^{(k,\ell)}_{inf} \neq e(\tau)^{(k,\ell)}_{inf}$. Тогда количество $Q(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau-1)^{(k,\ell)}_{inf}, \eta)_e$ последовательностей, ***предшествующих*** последовательности, у которой первые τ элементов равны $(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau-1)^{(k,\ell)}_{inf}, \eta)$, а оставшиеся $(n_{inf}-\tau)$ элементов принимают значения соответственно системе ограничений (1), будет вычисляться с использованием такого соотношения:

$$Q(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau-1)^{(k,\ell)}_{inf}, \eta)_e =$$

$$= \eta \cdot Q(e(1)^{(k,\ell)}_{inf}, e(2)^{(k,\ell)}_{inf},..., e(\tau)^{(k,\ell)}_{inf}; n_{inf}; \overline{D''^{(k,\ell)}_{inf}})_e . \quad (6)$$

Синтез системы соотношений для кодирования ОПДП^3 предлагается осуществлять в два этапа. Первый этап заключается в определении кодового значения $C'(E(\chi;\gamma)^{(k,\ell)}_{inf})_e$ информативной дифференциально-описанной спектрограммы как последовательности в одноосновном позиционном пространстве с фиксированным значением основания, равного $\bar{d}_e^{(k,\ell)}$. Здесь информативные ДОС рассматриваются без учетом неравенства между ее соседними элементами.

Соответственно, с учётом полученного на первом этапе соотношения, организуется синтез выражения для определения кодового значения

$C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ информативной ДОС с наличием неравенства между ее соседними элементами, т.е. как последовательности в двухосновном позиционном прореженном пространстве. Для этого требуется исключить количество запрещенных позиционных чисел, которые содержат равные соседние элементы. Поэтому на втором, завершающем этапе синтеза функционального выражения $F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)};\varepsilon_{fix};\overline{d}_e^{(k,\ell)};\overline{D''}_{inf}^{(k,\ell)}\}$ нужно в процессе формирования кодового значения $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ дополнительно учитывать условие, состоящее в том, что между соседними элементами информативной дифференциально-описанной спектрограммы не может быть равенства. Следовательно, необходимо учитывать *дополнительное условие*, состоящее в неравенстве соседних элементов в информативной ДОС $E(\chi;\gamma)_{inf}^{(k,\ell)}$, т.е.:

$$e(\tau)_{inf}^{(k,\ell)} \neq e(\tau(sign(n_{inf}-\tau)+1)_{inf}^{(k,\ell)} \neq e(\tau+1)_{inf}^{(k,\ell)}, \rightarrow \tau < n_{inf}. \quad (7)$$

$$e(\tau)_{inf}^{(k,\ell)} < \overline{d}_e^{(k,\ell)}, \quad \tau = \overline{1, n}_{inf}.$$

Для заданных условий допустимыми будут такие последовательности, которые не содержат пар соседних элементов, имеющих равные значения, т.е. дополнительно выполняются соотношения (7). Соответственно запрещенными последовательностями будут такие комбинации, которые содержат хотя бы одну пару равных по значению соседних элементов информативной ДОС.

Отсюда ***предлагается*** определить количество $Q(e(1)_{inf}^{(k,\ell)}, e(2)_{inf}^{(k,\ell)},..., e(\tau-1)_{inf}^{(k,\ell)}, \eta)_e$ последовательностей, ***предшествующих*** последовательности, у которой первые τ элементов равны $(e(1)_{inf}^{(k,\ell)}, e(2)_{inf}^{(k,\ell)},..., e(\tau-1)_{inf}^{(k,\ell)}, \eta)$, а оставшиеся $(n_{inf}-\tau)$ элементов принимают значения в соответствии с системой ограничений (1), т.е. когда дополнительно накладывается условие относительно исключения случаев равенства между значениями соседних элементов следующим образом:

$$Q(e(1)_{inf}^{(k,\ell)},...,e(\tau-1)_{inf}^{(k,\ell)},e(\tau)'^{(k,\ell)}_{inf})_e = \begin{cases} e(\tau)'^{(k,\ell)}_{inf}(\overline{d}_e^{(k,\ell)}-sign(\tau-1))^{n_{inf}-\tau}, & \rightarrow \\ \rightarrow e(\tau-1)_{inf}^{(k,\ell)} > e(\tau)'^{(k,\ell)}_{inf}; & \\ (e(\tau)'^{(k,\ell)}_{inf}-1)(\overline{d}_e^{(k,\ell)}-sign(\tau-1))^{n_{inf}-\tau}, & \rightarrow \\ \rightarrow e(\tau-1)_{inf}^{(k,\ell)} < e(\tau)'^{(k,\ell)}_{inf}. & \end{cases} \quad (8)$$

Для упрощения записи системы (8) введем вспомогательный параметр $u(\tau)^{(k,\ell)}$, который определяется как:

$$u(\tau)^{(k,\ell)} = e'(\tau)_{inf}^{(k,\ell)} - sign(1-sign(e(\tau-1)_{inf}^{(k,\ell)} - e'(\tau)_{inf}^{(k,\ell)})) =$$

$$= \begin{cases} e'(\tau)_{inf}^{(k,\ell)}, & \rightarrow e'(\tau)_{inf}^{(k,\ell)} < e(\tau-1)_{inf}^{(k,\ell)}; \\ e'(\tau)_{inf}^{(k,\ell)}-1, & \rightarrow e'(\tau)_{inf}^{(k,\ell)} > e(\tau-1)_{inf}^{(k,\ell)}. \end{cases}$$

С учетом этого получим следующее соотношение для нахождения величины $Q(e(1)_{inf}^{(k,\ell)},..., e(\tau-1)_{inf}^{(k,\ell)}, e(\tau)'^{(k,\ell)}_{inf})_e$, а именно:

$$Q(e(1)_{inf}^{(k,\ell)},..., e(\tau-1)_{inf}^{(k,\ell)}, e(\tau)'^{(k,\ell)}_{inf})_e =$$
$$= e(\tau)'^{(k,\ell)}_{inf} \cdot (\overline{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-\tau} -$$
$$- sign(1-sign(e(\tau-1)_{inf}^{(k,\ell)} - e(\tau)'^{(k,\ell)}_{inf})) \times$$
$$\times (\overline{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-\tau} =$$
$$= (e'(\tau)_{inf}^{(k,\ell)} - sign(1-sign(e(\tau-1)_{inf}^{(k,\ell)} - e'(\tau)_{inf}^{(k,\ell)}))) \times$$
$$\times (\overline{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-\tau}. \quad (9)$$

Полученное выражение позволяет определить количество допустимых последовательностей, ***предшествующих*** последовательности, у которой первые τ элементов равны

$$(e(1)_{inf}^{(k,\ell)},..., e(\tau-1)_{inf}^{(k,\ell)}, e(\tau)'^{(k,\ell)}_{inf}),$$

а оставшиеся $(n_{inf}-\tau)$ элементов принимают значения в соответствии с системой ограничений (1), т.е. когда дополнительно накладывается условие относительно исключения случаев равенства между значениями соседних элементов с учетом исключения ситуаций, когда выполняется равенство $e(\tau)'^{(k,\ell)}_{inf} = e(\tau-1)_{inf}^{(k,\ell)}$.

Искомое кодовое значение $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ информативной ДОС как одномерной последовательности в двухосновном прореженном позиционном пространстве определяется по формуле:

$$C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e = \sum_{\tau=1}^{n_{inf}} \sum_{e(\tau)'^{(k,\ell)}_{inf}=e^{(k,\ell)}_{inf,min}}^{e(\tau)^{(k,\ell)}_{inf}-1} Q(e(1)_{inf}^{(k,\ell)},...,, e(\tau)'^{(k,\ell)}_{inf})_e,$$

или с учетом использования вспомогательного параметра $u(\tau)^{(k,\ell)}$ получим

$$C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e = \sum_{\tau=1}^{n_{inf}} u(\tau)^{(k,\ell)} \cdot (\overline{d}_e^{(k,\ell)} - sign(\tau-1))^{n_{inf}-\tau}, \quad (10)$$

$$u(\tau)^{(k,\ell)} = e'(\tau)_{inf}^{(k,\ell)} - sign(1-sign(e(\tau-1)_{inf}^{(k,\ell)} - e'(\tau)_{inf}^{(k,\ell)})) =$$
$$= \begin{cases} e'(\tau)_{inf}^{(k,\ell)}, & \rightarrow e'(\tau)_{inf}^{(k,\ell)} < e(\tau-1)_{inf}^{(k,\ell)}; \\ e'(\tau)_{inf}^{(k,\ell)}-1, & \rightarrow e'(\tau)_{inf}^{(k,\ell)} > e(\tau-1)_{inf}^{(k,\ell)}. \end{cases} \quad (11)$$

При определении количества допустимых последовательностей в ОПДП3 имеет значение соотношение между текущим и предыдущим элементами информативной ДОС. В качестве нулевого значения $e(0)_{inf}^{(k,\ell)}$ последовательности $E(\chi;\gamma)_{inf}^{(k,\ell)}$ предлагается использовать следующее условие:

$$e(0)_{inf}^{(k,\ell)} = \bar{d}_e^{(k,\ell)}. \quad (12)$$

Такой выбор обусловлен, с одной стороны, тем, что на значения элементов, предшествующих элементу $e(1)_{inf}^{(k,\ell)}$, не накладываются ограничения относительно нулевого элемента, а с другой - обеспечивается неравенство:

$$e(0)_{inf}^{(k,\ell)} = \bar{d}_e^{(k,\ell)} > e(1)_{inf}^{(k,\ell)}.$$

В противном случае нарушается взаимооднозначность представления, когда $e(1)_{inf}^{(k,\ell)} = 0$.

Значит, система выражений (10) – (12) задает функциональное соотношение $F_e\{E(\chi;\gamma)_{inf}^{(k,\ell)}; \varepsilon_{fix}; \bar{d}_e^{(k,\ell)}; \overline{D''}_{inf}^{(k,\ell)}\}$ для определения кодового значения $C(E(\chi;\gamma)_{inf}^{(k,\ell)})_e$ для информативной составляющей $E(\chi;\gamma)_{inf}^{(k,\ell)}$ дифференциально-описанной спектрограммы, рассматриваемой как одномерная последовательность в ДП^3 в условиях соответствия системе ограничений (1).

4. Выводы

Можно заключить, что система выражений (10) – (12) обеспечивает:

1) формирование кодового значения для информативной ДОС, образованной значимыми компонентами диффренциально-описанной спектрограммы последовательности кадров Р-типа, рассматриваемой как одномерная последовательность в ДП^3 в условиях: наличия адаптивных ограничений на динамические диапазоны их элементов; исключения вариантов равенства между значениями соседних элементов;

2) исключение запрещенных последовательностей, для которых:

– значения элементов превышают уровень выявленного адаптивного значения динамического диапазона информативной ДОС;

– выполняется условие равенства между соседними элементами информативной ДОС.

Литература:

1. Richardson J. *Video encoding H.264 and MPEG-4 - standards of the new generation* [text]. / J. Richardson D.: TECHNOSPHERE, 2012. 156 - 192 p.

2. S. *Wang, X. Zhang, X. Liu, J. Zhang, S. Ma and W. Gao*, "Utility-Driven Adaptive Preprocessing for Screen Content Video Compression," in IEEE Transactions on Multimedia, vol. 19, no. 3, pp. 660-667, March 2017.

3. R.C. Gonzales and R.E. Woods, "*Digital image processing*," in Prentice Hall, New Jersey, edition. II, 2002 – 1072 p.

4. *Kubasov D.V.* Review of methods of motion compensation / D. S. Vatolin / Computer graphics and multimedia. - K.: KPI, 2010. - Vip. No. 3 (2). P. 33-43.

5. *W. J. Tsai and Y. C. Sun*, "Error-resilient video coding using multiple reference frames," 2013 IEEE International Conference on Image Processing, Melbourne, VIC, 2013.P. 1875-1879.

6. *Y. Zhang, S. Negahdaripour and Q. Li*, "Error-resilient coding for underwater video transmission," OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, 2016. P. 1-7.

7. *O. Stankiewicz, K. Wegner, D. Karwowski, J. Stankowski, K. Klimaszewski and T. Grajek*, "Encoding mode selection in HEVC with the use of noise reduction," 2017 International Conference on Systems, Signals and Image Processing (IWSSIP), Poznan, 2017. P. 1-6.

8. *H. Baccouch, P. L. Ageneau, N. Tizon and N. Boukhatem*, "Prioritized network coding scheme for multi-layer video streaming," 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017. P. 802-809.

9. *Bai X., Wang J.* Towards temporally-coherent video matting. Proceedings of the 5th international conference on Computer vision/computer graphics collaboration techniques. MIRAGE'11, Springer-Verlag. 2011. P. 63-74.

10. *Christophe E., Lager D., Mailhes C.* Quality criteria benchmark for hiperspectral imagery. IEEE Transactions on Geoscience and Remote Sensing. Sept 2005. Vol. 43, No 9. P. 2103–2114.

11. *B. Zheng and S. Gao*, "A soft-output error control method for wireless video transmission," 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, 2016. P. 561-564.

12. J. Miano. *Formats and image compression algorithms in action* [Text] - K.: Triumph, 2013. 336 p.

13. *Ding Z., Chen H., Gua Y., Peng Q.* GPU accelerated interactive space-time video matting. In Computer Graphics International. 2010. P. 163-168.

14. *Lee S. Y. Yoon J. C.* Temporally coherent video matting. Graphical Models 72. 2010. P. 25-33.

15. *Sindeev M., Konushin A., Rother C.* Alpha-flow for video matting. Technical Report. 2012. P. 41–46.

16. *Tan K. H., Ghanbari M.* Layered image coding using the DCT pyramid. IEEE Trans. Image Proc. 1995. V. 4, № 4. P. 512-516.

17. *Barannik V., Tarasenko D., Podlesny S., Barannik D.* The video stream encoding method in infocommunication systems. Modern Problems of Radio Engineering, Telecommunications and Computer Science, (TCSET'2018): XVIth Intern conf., (Lviv-Slavske, Ukraine, February 23–25, 2018). Lviv-Slavske: 2018. P. 538 – 541.

18. *Vladimir Barannik; Andrii Krasnorutsky; Vladimir Larin; Anna Hahanova; Sergii Shulgin* Model of syntactic representation of aerophoto images segments. Modern Problems of Radio Engineering, Telecommunications and Computer Science, (TCSET'2018): XVIth Intern conf., (Lviv-Slavske, Ukraine, February 23–25, 2018). Lviv-Slavske: 2018. P. 974 – 977.

19. *Barannik V., Ryabukha Yu., Tverdokhlib V., Dodukh A., Suprun O., Tarasenko D.* Integration the non-equilibrium position encoding into the compression technology of the transformed images // East-West Design & Test Symposium (EWDTS). – IEEE, 2017. P. 1-4.

20. *Barannik V.V., Ryabukha Yu.N., Tverdokhleb V.V., Baranmk D.V*. Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding. 2nd IEEE International Conference on Advanced Information and Communication Technologies, AICT 2017, Proceedings, Lviv, 2017. P. 188 - 192.

Поступила в редколлегию 11.06.2018
Рецензент: д-р техн. наук, проф. Баранник В.В.

Химeнко Виктория Викторовна, аспирант кафедры ИСИ ХНУРЭ. Научные интересы: обработка информации. Адрес: Украина, 61166, Харьков, пр. Науки, 14, e-mail: vika.iv55@gmail.com

Himenko Viktoria Viktorovna, postgraduate student of the Department of INI of the Kharkov National University of Radio Electronics. Scientific interests: information processing. Address: 61166, Kharkiv, Nauka ave.14, e-mail: vika.iv55@gmail.com.

УДК 519.713

ТЕХНОЛОГИЧЕСКАЯ КОНЦЕПЦИЯ ДИФФЕРЕНЦИРОВАННОЙ ОБРАБОТКИ СЕГМЕНТОВ ВИДЕОКАДРА С УЧЕТОМ КЛЮЧЕВОЙ ИНФОРМАЦИИ

МЕДВЕДЕВ Д.О.

Обосновывается подход для формирования ядра технологической концепции дифференцированной обработки сегментов видеокадра с учетом ключевой информации. Это позволит: с одной стороны, снизить сложность процессов синтаксического представления; с другой – обеспечить заданный уровень достоверности видеоинформации, т.е. осуществлять режим обработки с контролируемой потерей качества реконструируемых видеокадров.

1. Введение

Для снижения информационной интенсивности битового потока в условиях сохранения требуемого уровня достоверности информации предлагается осуществлять дифференцированную обработку сегментов видеокадра. В этом случае обработка сегментов, содержащих ключевую информацию, будет проводиться с учетом сохранения заданной достоверности. Наоборот, обработка базовых сегментов, несущих фоновую нагрузку, предлагается с наибольшим снижением информационной интенсивности. Такая концепция позволяет сформировать дифференцированное синтаксическое представление сегментов видеокадра с учетом ключевой информации

2. Построение ядра технологической концепции дифференцированной обработки сегментов видеокадра

Ядром реализации предложенной концепции дифференцированной обработки с учетом ключевой информации необходимо выбирать класс методов, обеспеивающих возможность снижения информационной интенсивности с контролируемыми параметрами. Такими параметрами в данном случае являются количество сокращаемой психовизуальной избыточности и вычислительная сложность обработки [1]. Значит, процессы компрессии и восстановления организуются с контролируемой потерей качества визуальной оценки видеоинформации. Под контролируемой обработкой с учетом модели психовизуального восприятия понимается возможность методов обеспечить требуемую достоверность реконструируемого видеокадра. В случае обработки сегментов ключевой информации требуется обеспечить режим без её потери.

Базовой составляющей методов данного класса является предварительная обработка, основанная на использовании ортогональных преобразований, wavelet-систем и аффинных преобразований.

Технологии, базирующиеся на таких подходах, реализованы в форматах на JPEG-платформе (используется дискретное косинусное преобразование (ДКП)) и платформе JPEG2000 (используется wavelet-преобразование).

Данные методы позволяют формировать эффективное синтаксическое представление видеокадров как без потери качества визуальной оценки (режим loss-less), так и с потерей качества. Регулирование потерь качества и степени сжатия осуществляется путём: выбора типа и схемы трансформирования сегментов видеокадра; квантизации компонент трансформант; дополнительной регенерирующей фильтрации на приемной стороне.

В то же время для методов такого класса характерны следующие проблемные стороны:

1. В режиме ограниченного сокращения психовизуальной избыточности (режим сохранения требуемого уровня достоверности) проявляется существенная зависимость уровня снижения информационной интенсивности битового потока от степени информативности и семантической сложности сегментов цифровых изображений, в том числе изображений аэрокосмического мониторинга.

При этом степень снижения информационной интенсивности остается ограниченной.

Данные недостатки объясняются низкими значениями степени компрессии насыщенных изображений (в среднем до 2 раз) и дополнительными временными задержками на обработку. Здесь наибольшая сложность процессов обработки соответствует методам арифметического кодирования и методам LZW.

2. В режиме устранения психовизуальной избыточности проявляется зависимость уровня снижения информационной интенсивности от качества визуальной оценки реконструируемых видеокадров.

Наибольший уровень ухудщения визуальной оценки характерен для высокоинформативных фрагментов видекадров. Здесь наблюдается наиболее быстрое падение качества и достоверности видеоинформации с ростом уровня снижения информационной интенсивности [2].

Это ограничивает возможность эффективного использования таких технологий в энергоэффективных телекоммуникационных системах.Данные проблемные стороны функционирования методов с контролируемыми параметрами обработки обусловлены следующими причинами:

1) ограниченная степень снижения информационной интенсивности для методов на платформах JPEG и JPEG 2000 при режиме $h \geq 35$ дБ. Наибольшее снижение степени компрессии проявляется при обработке высоко- и средненасыщенных цифровых изображений;
2) реализация двумерных ДКП и dwt-преобразований для бортовых вычислительных комплексов связана с необходимостью затрачивать от 10 до 70% временных затрат от суммарного времени на обработку. Время на их выполнение в процессе преобразования изображений может достигать десятков секунд. Это обусловлено выполнением большого количества операций умножения в пространстве как целочисленной, так и вещественной арифметики;
3) базовыми методами для устранения статистической избыточности в трансформированных изображениях являются коды Хаффмана и арифметическое кодирование, для которых свойственно:
– в случае обработки насыщенных изображений в режиме контролируемого качества происходит генерирование коротких нулевых цепочек. Отсюда длины таких цепочек будут иметь равномерное распределение и, как следствие, незначительное количество статистической избыточности. Это приводит к резкому снижению коэффициента компрессии видеоданных;
- существует необходимость использовать маркерные кодовые последовательности, разделяющие неравномерные кодовые комбинации статистических кодов. Это приводит к увеличению объема сжатого представления.

Поэтому дополнительное уменьшение информационной интенсивности битового потока обеспечит дополнительные возможности относительно повышения разрешающей способности [3]. При этом требуется учитывать ограничения на временной ресурс по обработке данных.

Проведенные исследования существующих технологий компрессии видеокадров показали, что их совершенствование требуется проводить в направлении:
– с одной стороны, снижения сложности процессов синтаксического представления;
– с другой - обеспечения заданного уровня достоверности видеоинформации, т.е. осуществления режима обработки с контролируемой потерей качества реконструируемых видеокадров.

В качестве ядра концепции дифференцированной обработки видеокадров *предлагается* использовать трансформацию изображений на основе ортогональных преобразований и перевод обрабатываемых данных в дифференциальное пространство. Это позволит использовать механизмы для управления коэффициентом снижения уровня информационной интенсивности и уровнем достоверности информации, а также за счет дифференцирования создать механизм для сокращения вычислительных затрат.

Для реализации выдвинутых направлений возможны следующие варианты дополнительного снижения уровня информационной интенсивности битового потока:
– совершенствование адаптивных вероятностно-статистических моделей трансформант. Но это, с одной стороны, приводит к увеличению времени на обработку и к росту количества разрядов на представление служебной информации. С другой - эффективность статистических методов по степени компрессии практически достигла своего максимального уровня. Избыточность статистических кодов относительно энтропии Марковского источника не превышает в среднем 10 – 20 %;
– дальнейшее развитие путей для дополнительного устранения психовизуальной избыточности при обработке трансформант преобразований. Например, увеличить количество отбрасываемых из дальнейшей обработки компонент трансформант. В то же время в условиях обработки цифровых изображений с высоким уровнем информативности и семантической сложности это влечет за собой разрушение семантической структуры либо отдельных фрагментов, либо всего видеокадра.

Таким образом, для методов, использующих ортогональные преобразования и дифференцирование, нужно применять технологии сокращения избытоности путем выявления новых закономерностей и устранения избыточности не только статистической, но и психовизуальной природы. Для этого *предлагается* дополнительно выявлять в трансформированных изображениях структурные закономерности. Данный подход базируется на учете структурных преимуществ трансформированных сегментов видеокадра.

3. Разработка метода синтаксического представления базовых сегментов

Рассмотрим разработку подхода относительно обработки базовых сегментов видеокадров. В данном случае в процессе формирования синтаксического представления необходимо учитывать возможность коррекции трансформант таких сегментов под особенности зрительного их восприятия. Другими словами, допускается использование коррекции частотных компонент трансформированных базовых сегментов под модель психовизуального восприятия [4]. Предложенная схема создает условия для повышения ко-

личества устраняемой психовизуальной избыточности.

Основными технологическими этапами такого подхода являются следующие.

Выполняется двумерное ДКП-преобразование, которое реализуется на основе выражения:

$$C(k,\ell) = F(k)\ X(i,j)_{k,\ell}\ F^{T}(\ell); \qquad (1)$$

где $X(i,j)_{k,\ell}$ – массив базового сегмента, образованный на основе цветоразностной плоскости изображения;

k, ℓ – соответственно индекс строки и столбца элемента массива $X(i,j)_{k,\ell}$, $k=\overline{1,q_\ell}$; $\ell=\overline{1,q_c}$;

$C(k,\ell)$ - матрица компонент трансформанты ДКП-преобразования сегмента видеокадра;

$F(k)$, $F^{T}(\ell)$ – соответственно вектор дискретных значений базисных функций ДКП и его транспонированный вид

$$F(k) = \begin{cases} \dfrac{1}{\sqrt{q_\ell}} & \to k=1; \\ \sqrt{\dfrac{2}{q_\ell}}\cos\dfrac{(2q_\ell+1)k\pi}{2q_\ell}, & \to k=\overline{2,q_\ell}. \end{cases} \qquad (2)$$

Для трансформант сегментов, содержащих фоновые области видеокадра, характерны следующие особенности [5]:

1) значение компоненты в верхнем левом углу трансформанты с координатами $(1;1)$ пропорционально средней яркости фонового сегмента, т.е. несет информацию о среднем фоне;

2) наибольшая энергетическая составляющая фонового сегмента сосредоточена в ограниченном количестве компонент трансформанты;

3) преобладающей областью трансформанты является область низких энергетических характеристик той или иной её особенности.

В зависимости от учета в процессе обработки трансформант ее особенности формируется конкретная технология кодирования для исключения избыточности [6]. Процесс реализуется на очередном технологическом этапе обработки трансформированных сегментов видеокадра.

С учетом того, что кодирование проводится для фоновых областей видеокадра, предлагается, с одной стороны, исключить этап дифференциального представления компонент смежных столбцов трансформанты, а с другой - использовать более высокий уровень коррекции частотных компонент под модель психовизуального восприятия изображений для повышения количества сокращения психовизуальной избыточности. Для формирования кодового значения $E''(R)$ предлагается учитывать следующую интерпретацию двумерной трансформанты ДКП [7].

Трансформанта Y'' представляет собой перестановку с повторениями, на компоненты $y''_{k,\ell}$ которой наложены ограничения на мощность алфавита $d''_{k,\ell}$:

$$d''_{k,\ell} = \min(d''_k; d''_\ell). \qquad (3)$$

Здесь d''_k, d''_ℓ - мощность алфавита соответственно для компонент k-й строки и ℓ-го столбца трансформанты.

В этом случае количество $V^{(2)}_{q_1\times q_2}$ различных двумерных трансформант, составленных из $q_1\times q_2$ количества элементов, удовлетворяющих соотношению (6), равно:

$$V^{(2)}_{q_1\times q_2} = \prod_{k=1}^{q_1}\prod_{\ell=1}^{q_2} d''_{k,\ell}. \qquad (4)$$

Согласно комбинаторной интерпретации двумерной трансформанты и соотношению (4) количество $\overline{H}_2$ информации, в среднем содержащееся в одной компоненте $y''_{k\ell}$, равно:

$$\overline{H}_2 = ([\sum_{k=1}^{q_1}\sum_{\ell=1}^{q_2} \ell og_2 d''_{k,\ell}]+1)/q_1\times q_2, \qquad (5)$$

где $\overline{H}_2$ – количество информации, приходящееся в среднем на одну комопненту двумерной трансформанты в случае его комбинаторной трактовки как цельного объекта для ограничений (2). Для устранения количества комбинаторной избыточности в двумерной трансформанте, определяемой как разница между количеством информации, приходящимся в среднем на один элемент, до и после учета ограничений на мощность алфавита ее компонент, предлагается использовать двумерные позиционные кодовые конструкции. Это объяняется тем, что количество комбинаторной избыточности зависит от количества перестановок с повторениями, которое можно составить для различных ограничений на комопненты двумерной трансформанты с учетом текущей мощности их алфавита. Тогда двумерная трансформанта Y'' представляется как двумерное неравновесное позиционное число, на элементы которого наложены ограничения, определяемые их мощностью алфавита [8].

Такая система будет зависеть от устраняемой психовизуальной избыточности, количество которой

зависит от параметра R, определяющего уровень коррекций частотных компонент [9]. При этом согласно комбинаторной трактовке двумерной трансформанты Y'' в качестве оснований выбираются значения мощности алфавита компонент, т.е.:

$$\psi''(R)_{k,\ell} = d''_{k,\ell}, \quad q_1 = q_2 = \overline{1, (Q_1 Q_2 / q_1 q_2)}. \quad (6)$$

В этом случае кодовое значение $E''(R)$ двумерного позиционного числа Y'' определяется как:

$$E''(R) = \sum_{k=1}^{q_1} \sum_{\ell=1}^{q_2} y''_{k,\ell}\, v(R)^{(2)}_{k,\ell}, \quad (7)$$

где $v(R)^{(2)}_{k,\ell}$ - весовой коэффициент компоненты $y''_{k,\ell}$.

В случае обхода элементов в направлении столбцов сверху вниз, а затем по строкам слева – направо значение весового коэффициента $v(R)^{(2)}_{k,\ell}$ будет равно:

$$v(R)^{(2)}_{k,\ell} = \prod_{\xi=\ell+1}^{q_2} \psi''(R)_{k,\xi} \prod_{\eta=k+1}^{q_1} \prod_{\xi=1}^{q_2} \psi''(R)_{\eta,\xi}. \quad (8)$$

Технологию выбора количества двоичных разрядов на представления кодового значения $E''(R)$ предлагается строить с учетом системы оснований. Тогда количество разрядов на представление кодограммы двумерной трансформанты будет определяться на основе следующего выражения: $h''(R)^{(2)} = ([\sum_{k=1}^{q_1} \sum_{\ell=1}^{q_2} \ell og_2 \psi''(R)_{k,\ell}] + 1)$. (9)

В этом случае будет выполняться неравенство

$$([\ell og_2 E''(R)] + 1)/q_1 \le \overline{h''}(R)^{(2)} \le \overline{H}_1,$$

где $\overline{h''}(R)^{(2)}$ - количество двоичных разрядов, приходящееся в среднем на одну компоненту двумерной трансформанты в случае его синтаксического представления как двумерного позиционного числа в условиях использования системы $\Psi''(R)$ оснований для позиционирования их кодограмм.Здесь количество двоичных разрядов $\overline{h''}(R)^{(2)}$, которое требуется выделить в среднем под одну компоненту синтаксического представления кодового значения $E''(R)$, не будет превышать величины $\overline{H}_1$ [10]. Это создает условия для сокращения количества комбинаторной избыточности, которое содержится в двумерной трансформанте дискретного косинусного преобразования.

Отсюда согласно принятым условиям построение эффективного синтаксического представления для базовых сегментов определяется такими выражениями:

$$E''(R) = \sum_{k=1}^{q_1} \sum_{\ell=1}^{q_2} y''_{k,\ell}\, v(R)^{(2)}_{k,\ell}; \quad (10)$$

$$h''(R)^{(2)} = ([\sum_{k=1}^{q_1} \sum_{\ell=1}^{q_2} \ell og_2 \psi''(R)_{k,\ell}] + 1) \le q_1 \cdot q_2 \overline{H}. \quad (11)$$

Эффективное синтаксическое представление всей трансформанты базового сегмента видеокадра в виде кодограмм кодовых значений $E''(R)$ двумерных позиционных взвешенных чисел с учетом коррекции частотных составляющих определяется величиной $h''(R)^{(2)}$.

В этом случае переполнение технологической длины h_{it} кодовых слов исключается путём выбора более высоких значений параметра R.

Созданный подход относительно синтаксического представления двумерной трансформанты обеспечивает снижение интенсивности битового потока с учетом особенностей базовых сегментов относительно возможности дополнительного повышения количества устраняемой психовизуальной избыточности. Значение $E''(R)$ будет зависеть от детальности базового сегмента. Значение кода будет тем меньше, чем больше отношение площади, имеющей слабоменяющуюся яркость, к площади изображения передаваемого объекта. Следовательно, соотношения (10) – (11) задают метод формирования эффективного синтаксического кодирования базовых сегментов, содержащих фоновую информацию видеокадра на основе формирования кодового значения двумерной трансформанты, рассматриваемой как взвешенное двумерное позиционное число с учетом коррекции частотных составляющих и последующего кодообразования с использованием системы оснований.

Литература: 1. *Баранник В. В., Тарасенко Д. А., Баранник Д. В., Медведев Д. О.* Технология балансированной обработки динамического видеоресурса для снижения информационной интенсивности в инфокоммуникационных системах// Безпека інформації. 2017. №3. С. 163–170. **2.** *Бараннік В. В., Тарасенко Д. А., Медведев Д. О., Хіменко В. В.* Технологія обробки передбачених кадрів відеопотоку для бортових інформаційних технологій // Наукоємні технології. 2017. №4(36). С. 276–282. **3** *Barannik. V.V, Ryabukha Yu.N., Podlesnyi S.A.* “Structural slotting with uniform redistribution for enhancing trustworthiness of information streams”.

Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017. №76 (7), pp.607. doi: 10.1615 / TelecomRadEng.v76.i7.40. **4**. *Barannik. V.V, Ryabukha Yu.N., Tverdokhleb V.V., Barannik D.V.* , "Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding". 2nd IEEE International Conference on Advanced Information and Communication Technologies, AICT 2017, Proceedings, Lviv, 2017. P. 188. **5**. *Barannik V, Podlesny S, Tarasenko D, Barannik D, Kulitsa O*. "The video stream encoding method in infocommunication systems". Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International, Proceedings of the 14th International Conference on TCSET 2018 Lviv, 2018, pp. 538-541, doi: 10.1109/TCSET.2018.8336259. **6**. *Barannik V.V., Shulgin S.S.*. "The method of increasing accessibility of the dynamic video information resource". Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Proceedings of the 13th International Conference on TCSET 2016 Lviv, 2016. P.621. **7**. *Zhang Y., Negahdaripour S. and Li Q.*, "Error-resilient coding for underwater video transmission," OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, 2016. P. 1-7. **8.** *Wang S., Zhang X., Liu X., Zhang J., Ma S. and Gao W.*, Utility-Driven Adaptive Preprocessing for Screen Content Video Compression, in IEEE Transactions on Multimedia, vol. 19, no. 3. P. 660-667, March 2017. **9**. *Stankiewicz O., Wegner K., Karwowski D., Stankowski J., Klimaszewski K. and Grajek T.*, Encoding mode selection in HEVC with the use of noise reduction, 2017 International Conference on Systems, Signals and Image Processing (IWSSIP), Poznan, 2017. P. 1-6. **10**. *Barannik V.V.*. Creation of the rule of formation of positional structural and weight numbers in the conditions of codes formation with given length / Barannik V., Krasnorutskij A. // Information security. – 2016. – T 20. – 6 p.

Transliterated bibliography:

1. *Barannyk V.V., Tarasenko D.A., Barannyk D.V., Medvedev D.O.* Tekhnolohyia balansyrovannoi obrabotky dynamycheskoho vydeoresursa dlia snyzhenyia ynformatsyonnoi yntensyvnosty v ynfokommunykatsyonnykh systemakh. Bezpeka informatsii. 2017. №3. S. 163–170.

2. *Barannik V.V., Tarasenko D.A., Medvedev D.O., Khimenko V.V.* Tekhnolohiia obrobky peredbachenykh kadriv videopotoku dlia bortovykh informatsiinykh tekhnolohii. Naukoiemni tekhnolohii. 2017. №4(36). S. 276–282.

3. *Barannik V.V., Ryabukha Yu.N., Podlesnyi S.A.* "Structural slotting with uniform redistribution for enhancing trustworthiness of information streams". Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017. №76 (7), pp.607. doi: 10.1615 / TelecomRadEng.v76.i7.40

4. *Barannik V.V., Ryabukha Yu.N., Tverdokhleb V.V., Barannik D.V.* Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding // 2nd IEEE International Conference on Advanced Information and Communication Technologies, AICT 2017, Proceedings, Lviv, 2017, pp. 188.

5. *Barannik V., Podlesny S., Tarasenko D., Barannik D., Kulitsa O*. The video stream encoding method in infocommunication systems // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International, Proceedings of the 14th International Conference on TCSET 2018 Lviv, 2018, pp. 538-541, doi: 10.1109/TCSET.2018.8336259

6. *Barannik V.V., Shulgin S.S.* The method of increasing accessibility of the dynamic video information resource // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Proceedings of the 13th International Conference on TCSET 2016 Lviv, 2016, pp.621.

7. *Zhang Y., Negahdaripour S. and Li Q.* Error-resilient coding for underwater video transmission // OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, 2016, pp. 1-7.

8. *Wang S., Zhang X., Liu X., Zhang J. , Ma S. and Gao W.* "Utility-Driven Adaptive Preprocessing for Screen Content Video Compression // IEEE Transactions on Multimedia, vol. 19, no. 3, pp. 660-667, March 2017.

9. *Stankiewicz O., Wegner K., Karwowski D. , Stankowski J., Klimaszewski K. and Grajek T.* Encoding mode selection in HEVC with the use of noise reduction // 2017 International Conference on Systems, Signals and Image Processing (IWSSIP), Poznan, 2017, pp. 1-6.

10. *Barannik V.V.*. Creation of the rule of formation of positional structural and weight numbers in the conditions of codes formation with given length / Barannik V., Krasnorutskij A. // Information security. – 2016. – T 20. – 6 p.

Поступила в редколлегию10.06.2018

Рецензент: д-р техн. наук, проф. Баранник В.В.

Медведев Денис Олегович, аспирант кафедры ИСИ ХНУРЭ. Научные интересы: обработка информации. Адрес: Украина, 61166, Харьков, просп. Науки, 14, e-mail: domedvedo@gmail.com

Medvedev Denis Olegovich, postgraduate student of the Department of ISI of the Kharkov National University of Radio Electronics. Scientific interests: information processing. Address: 61166, Kharkiv, Nauka ave.14, e-mail:domedvedo@gmail.com

УДК 004.627

ПРОГНОЗИРОВАНИЕ ПАРАМЕТРОВ ВНОСИМЫХ ИСКАЖЕНИЙ ПРИ СЖАТИИ ИЗОБРАЖЕНИЙ С ПОТЕРЯМИ

КРИВЕНКО С.С., ЗРЯХОВ М.С., ЛУКИН В.В.

Анализируется зависимость среднеквадратической ошибки (СКОш) искажений, вносимых при сжатии изображений с потерями от шага квантования для современного кодера на основе дискретного косинусного преобразования (ДКП) и схемы разбиения. Показывается, что поведение зависимости определяется как степенью сложности (насыщенностью) изображения, так и характеристиками помех, которые могут присутствовать на сжимаемом изображении. Предлогаются метод и средства прогнозирований СКОш, позволяющие выбирать шаг квантования с учетом требований к уровню вносимых искажений.

Ключевые слова: сжатие с потерями, изображение с шумом, ДКП, прогнозирование.

Key words: lossy compression, noisy image, DCT, prediction.

Введение

С помощью современных систем формирования изображений различного назначения получают все больший объем данных, которые необходимо передавать, обрабатывать и хранить [1, 2]. Как при подготовке данных к передаче, так и при их подготовке к хранению часто используют сжатие изображений [2, 3]. При этом, в принципе, возможно применение методов как сжатия без потерь, так и сжатия изображений с потерями. Для методов сжатия без потерь достигаемые значения коэффициента сжатия (КС) обычно малы и не удовлетворяют требованиям. Поэтому приходится использовать методы сжатия с потерями.

Эту группу методов характеризуют зависимостью (rate distortion curve – RDC) между параметром (метрикой, количественным критерием), описывающим вносимые искажения (потери), который рассчитывается между сжатым и исходным изображениями, и КС или параметром, определяющим КС [1-3]. На практике могут возникать разные задачи, связанные с этой зависимостью: 1) выбрать наилучший метод сжатия, 2) обеспечить заданный КС, 3) обеспечить качество сжатого изображения не хуже, чем заданное, в соответствии с выбранным критерием.

Что касается выбора наилучшего метода сжатия, то здесь приходится учитывать не только RDC, но и такие аспекты, как соответствие стандартам, быстродействие, особенности практической реализации используемого ортогонального преобразования. Отметим, что в настоящее время разработаны методы сжатия изображений, которые существенно лучше, чем стандарт JPEG2000 [4, 5]. Одним из них является метод [5], основанный на использовании оптимизированной схемы разбиения, адаптированной к контенту изображения, и ДКП в блоках разного размера. Существенный выигрыш в соответствии с такими критериями как СКОш или пиковое отношение сигнал-шум (ПОСШ) при фиксированном КС достигается обычно для изображений средней и низкой сложности (насыщенности) [4] благодаря использованию блоков большого размера для однородных фрагментов изображений и блоков меньшего размера для окрестностей границ или малоразмерных объектов. Преимуществом кодера ADCT [5] (доступен для бесплатного скачивания на сайте http://ponomarenko.info/adct.htm) является больший КС при одном и том же уровне (СКОш или ПОСШ) вносимых искажений, где выигрыш по КС может достигать десятков процентов в сравнении с JPEG и JPEG2000.

Что касается второй и третьей задач, то обеспечение желаемого КС, безусловно, проще всего выполняется JPEG2000 и аналогичными ему методами сжатия. Впрочем, для методов сжатия на основе ДКП задача обеспечения заданного КС была решена в работе [6].

Обеспечение желаемых СКОш или ПОСШ – задача более сложная. Ее легко решить, если нет ограничений на временные и вычислительные затраты [4, 7]. Достаточно выполнить итерационную процедуру компрессии-декомпрессии с контролем значения анализируемой метрики и соответствующим изменением в нужную сторону параметра, управляющего сжатием – bpp (bits per pixel) для JPEG2000 или шага квантования (ШК) для кодеров на основе ДКП.

Недостаток такой процедуры состоит в том, что в начале обработки не ясно, сколько итераций понадобится. Поэтому временные затраты на сжатие могут быть достаточно большими, особенно если используемый метод (алгоритм) сжатия является не быстрым. Для кодера ADCT [5] этот недостаток проявляется в заметной степени, поскольку сжатие требует определенных затрат на оптимизацию схемы разбиения.

Поэтому *цель данного исследования* состоит в разработке метода и алгоритмов обеспечения желаемого СКОш (или ПОСШ) для кодера ADCT [5]. При этом учитывается, что сжимаемое изображение может быть как «чистым», т е. таким, на котором шум практически отсутствует или, по крайней

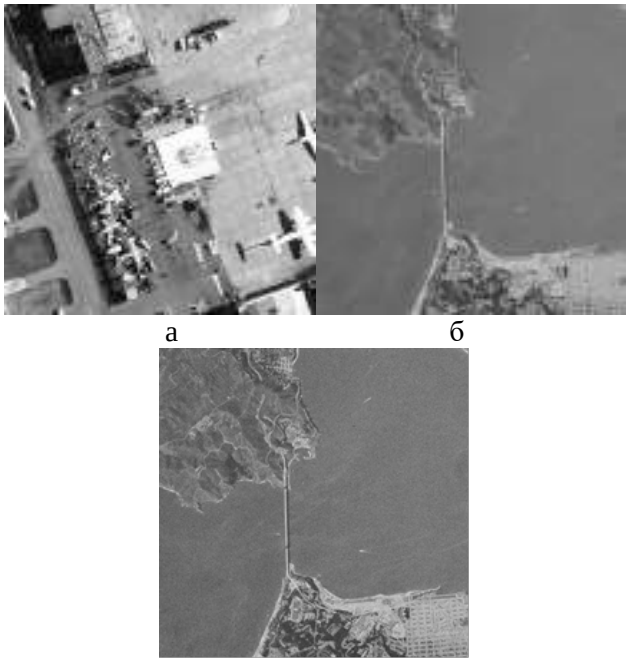
мере, визуально незаметен, так и искаженным помехами. В этом случае сжатие с потерями имеет специфику [8, 9] - оно приводит к эффекту своеобразной фильтрации и возможному наличию оптимальной рабочей точки (ОРТ) [9, 10], где под ОРТ понимаются такие значения параметров сжатия, что сжатое изображение является максимально близким к истинному изображению (без помех) и более близким, чем исходное изображение с помехами. Близость можно характеризовать как традиционными метриками (СКОш или ПОСШ), так и метриками визуального качества [10].

1. Особенности сжатия изображений с потерями

Прежде всего, рассмотрим традиционный подход к получению RDC и ее анализу. Представим себе, что имеется изображение $I_{ij}^{n}, i = 1,..., N_1, j = 1,..., N_2$, где i и j – индексы пикселей, N_1N_2 - общее количество пикселей. После сжатия этого изображения с потерями получаем $I_{ij}^{c}, i = 1,..., N_1, j = 1,..., N_2$, которое отлично от исходного изображения $I_{ij}^{n}, i = 1,..., N_1, j = 1,..., N_2$, т.е. в исходное изображение внесены искажения. Самый простой и обычный способ описывать эти искажения – вычислить СКОш $MSE_{nc} = \frac{1}{N_1N_2 - 1}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(I_{ij}^{n} - I_{ij}^{c})^2$ или ПОСШ $PSNR_{nc} = 10\lg(255^2 / MSE_{nc})$. При увеличении ШК или КС СКОш монотонно возрастает, а ПОСШ, соответственно, монотонно убывает.

Приведем примеры некоторых зависимостей, полученных для кодера ADCT для трех тестовых изображений, показанных на рис. 1. Отличия этих тестовых изображений состоят в степени сложности или насыщенности (изображение Airfield является более сложным, чем Frisco) и в том, что рассматриваются два варианта изображения Frisco – без шума и с аддитивным белым гауссовым шумом со среднеквадратичным отклонением σ=10.

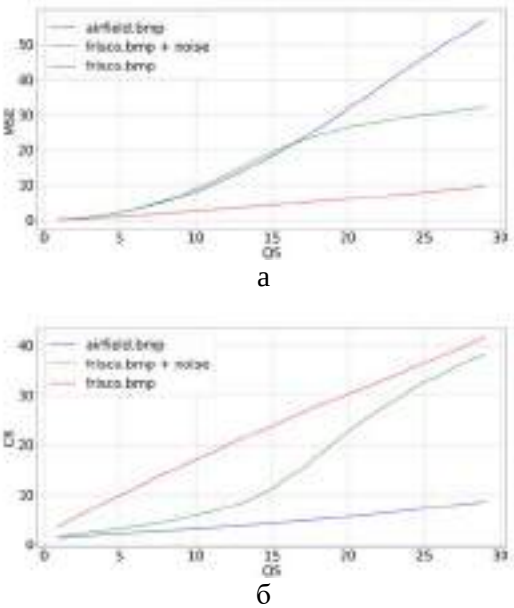
Зависимость MSE_{nc} от ШК приведена на рис. 2,а. Хорошо видно, что все три зависимости являются монотонно возрастающими, но ведут себя поразному. Значения MSE_{nc} для тестового изображения Frisco без шума являются наименьшими, начиная с малых значений ШК. Для двух других тестовых изображений кривые ведут себя примерно одинаково для ШК<15, а затем «расходятся» - для тестового изображения Airfield рост MSE_{nc} более быстрый. При этом для ШК<15 возрастание MSE_{nc} примерно квадратичное, а затем более медленное. Таким образом, вид зависимости MSE_{nc} от ШК определяется как свойствами изображения, так и свойствами помех.



а б в

Рис. 1. Изображение Airfield без шума (а) и изображение Frisco без шума (б) и с шумом, σ=10 (в)

Интересны и зависимости КС от ШК, приведенные на рис. 2,б. Лучше всего сжимается изображение Frisco без шума, немного хуже - Frisco с шумом и хуже всех - изображение Airfield без шума.



а

б

Рис. 2. Зависимости MSE_{nc} от ШК (а) и КС(ШК) (б) для трех рассматриваемых тестовых случаев (σ=5)

Объясним, почему для практики желательно обеспечить то или иное СКОш или ПОСШ. Если речь идет о сжатии изображений, на которых шум практически отсутствует, то часто желательно обеспечить ПОСШ порядка 35 дБ (СКОш порядка 20 для

изображений в восьмибитном представлении) для того, чтобы внесенные искажения были визуально незаметны [3, 11]. Если же сжимаются изображения, которые искажены помехами, то для них нецелесообразно вносить искажения со СКОш, превышающей эквивалентную дисперсию шума [6, 7]. При этом предполагается, что дисперсия аддитивных помех или эквивалентная дисперсия сигнально-зависимых помех заранее известна или достаточно точно оценена [12] для того типа изображений, которые предполагается сжимать.

Могут быть и другие причины и требования, например, не исказить диагностически важные признаки для медицинских изображений или текстурные признаки для изображений дистанционного зондирования. В рассматриваемом случае важно то, что задачей является обеспечить некоторое MSE_{des}.

2. Известные подходы к прогнозированию СКОш

Если до квантования и кодирования известны все значения ДКП-коэффициентов в блоках, то можно сначала определить, какие ошибки в каждый коэффициент внесет квантование с исследуемым ШК, затем, используя теорему Парсеваля, определить СКОш для каждого блока, а затем и для всего изображения:

$$MSE(QS) = \frac{1}{N_1 N_2} \sum_{n=1}^{N_{bl}} \delta^2(n), \quad (1)$$

$$\delta^2(n) = \sum_{q=1}^{Q(n)} (QS \times D_{qt}(q,n) - D(q,n))^2, \quad (2)$$

где $D(q,n)$ – q-й ДКП-коэффициент ($q = 1,...,Q(n)$) в n-м блоке, включающем $Q(n)$ отсчетов и, соответственно, ДКП-коэффициентов; $D_{qt}(q,n)$ – q-й ДКП-коэффициент в n-м блоке после квантования с использованием ШК QS; N_{bl} – число блоков.

После этого можно изменить ШК и достигнуть в несколько итераций нужного значения MSE_{des} [13]. Поиск нужного значения ШК является итеративным, но выполнять компрессию и декомпрессию несколько раз не нужно. Достоинство состоит в том, что можно обеспечить MSE_{des} достаточно точно благодаря постепенному уточнению ШК. Недостатком является то, что нужно хранить в памяти все значения ДКП-коэффициентов, т. е. фактически создавать массив того же размера, что и само изображение, что не всегда возможно. Надо также квантовать все значения ДКП-коэффициентов и рассчитывать квантованные значения ДКП-коэффициентов и $MSE(QS)$ для каждого значения ШК.

В связи с указанными выше сложностями были предложены несколько путей более простой обработки. В работе [14] для стандарта JPEG разработан алгоритм, основой которого является предположение о том, что распределение ДКП-коэффициентов (за исключением ДКП-коэффициента в каждом блоке, ответственного за постоянный уровень) описывается распределением Лапласа, для которого при нулевом математическом ожидании есть только один свободный параметр, связанный с дисперсией ДКП-коэффициентов. Именно этот параметр предлагается оценивать, а затем использовать заранее известную зависимость СКОш вносимых искажений от этого параметра и ШК. Для расчета параметра распределения нет необходимости хранить все значения ДКП-коэффициентов. Зная его, можно быстро определить нужный ШК.

Недостаток метода состоит в том, что предположение о Лапласовом законе распределения ДКП-коэффициентов верно лишь весьма приблизительно. Существенные отличия могут наблюдаться, если на изображении присутствует шум. Вследствие этого прогнозируемое значение ПОСШ может отличаться от наблюдаемого на практике, ошибки составляют до 1 дБ. Кроме того, алгоритм [14] разработан только для стандарта JPEG. Его применимость не анализировалась для других методов сжатия на основе ДКП.

В работе [13] метод [14] был существенно модифицирован. Прежде всего, показано, что статистика ДКП-коэффициентов, оцененная в блоках 8x8 пикселей, которые используются в стандарте JPEG, может быть полезна при прогнозировании $MSE_{pred}(QS)$ для других методов сжатия на основе ДКП, в том числе для кодера ADCT [5]. Кроме того, было предложено использовать не все возможные блоки изображения размером 8x8 пикселей, а их ограниченное количество, например 500 блоков, выбранных случайным образом, т. е. надо рассчитать и хранить для последующего анализа лишь около 30000 ДКП-коэффициентов, что гораздо меньше, чем $N_1 N_2$. Далее для рассматриваемых блоков рассчитывают

$$\delta^2(n) = \sum_{q=1}^{63} (QS \times D_{qt}(q,n) - D(q,n))^2, \quad (3)$$

т.е. исключая ДКП-коэффициент для постоянного уровня в блоках, а затем рассчитывают

$$MSE_{pred}(QS) = \kappa \frac{1}{63 N_{abl}} \sum_{n=1}^{N_{abl}} \delta^2(n), \quad (4)$$

где N_{abl} – число анализируемых блоков; к - поправочный коэффициент для данного кодера, близкий к единице. Далее подбирают ШК квантования таким образом, чтобы обеспечить $MSE_{pred}(QS) \approx MSE_{des}$. По сравнению с методом [14] метод [13] существенно быстрее благодаря меньшему числу анализируемых блоков и требует меньше памяти.

Однако метод, предложенный в [15] для кодера AGU (http://ponomarenko.info/agu.htm) на основе ДКП, позволил дополнительно ускорить определение необходимого ШК. Основная идея состоит в следующем. Предположим, что $MSE_{pred}(QS)$ можно представить в виде

$$MSE_{pred} = (QS^2/12)f(\vec{X}), \quad (5)$$

где $f(\vec{X})$ – относительно простая функция от одного или нескольких параметров, которые легко рассчитать для ДКП-коэффициентов в ограниченном количестве блоков размером 8x8 пикселей. Такая запись учитывает тот факт, что при малых значениях ШК реально выполняется соотношение $MSE(QS) \approx (QS^2/12)$. Тогда $f(\vec{X})$ фактически вводит коррекцию при относительно больших значениях ШК.

В работе [15] для кодера AGU удалось показать, что одним из аргументов $f(\vec{X})$ может быть параметр P_0 – вероятность того, что значение ДКП-коэффициента после квантования окажется равным 0, т.е. фактически надо определить процент ДКП-коэффициентов, модульные значения которых не превышают QS/2. Очевидно, что рассчитать такую вероятность очень легко.

Использование только одного входного параметра P_0 дало очень хорошие результаты при $P_0 < 0,6$ для изображений как без шума, так и с шумом. А при $P_0 \geq 0,6$, что соответствует достаточно большим КС, оказалось, что для изображений с шумом начинает влиять дисперсия помех. Ее учет позволил повысить точность прогнозирования за счет использования обученной машины опорных векторов в качестве аппроксиматора, но возникли другие проблемы. Во-первых, был рассмотрен только случай аддитивного белого гауссова шума, а на практике возможны и другие варианты. Во-вторых, характеристики помех не всегда известны заранее. Их автоматическое оценивание возможно, но оно может занять время, сравнимое со сжатием или даже больше.

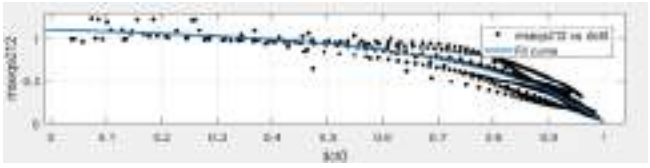
Таким образом, под вопросом оказывается целесообразность применения подхода для $P_0 \geq 0,6$. Поэтому ниже внимание уделено возможности усовершенствования методики, предложенной в работе [15], и исследованию ее применимости для кодера ADCT.

3. Особенности прогнозирования для изображений с помехами и без помех

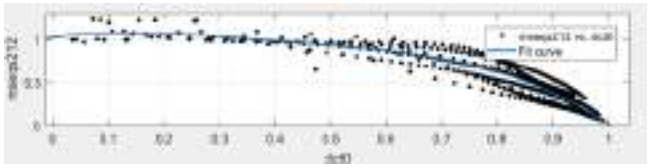
Разработанная в [15] методика прогнозирования нуждается в предварительном пояснении. Во-первых, предполагается, что до начала прогнозирования получена аппроксимация (или обучен аппроксиматор), позволяющая рассчитать прогнозируемое значение (например, СКОш или ПОСШ), используя один или несколько входных параметров, рассчитанных для изображения, которое предполагается сжимать. Во-вторых, предполагается, что эти входные параметры можно рассчитать очень быстро, а результат прогнозирования будет достаточно точен для практического применения.

Поясним процесс получения аппроксимации на простом примере. Прежде всего, получение аппроксимации происходит off-line. Предположим, что будут сжиматься изображения, на которых шум практически отсутствует. Возьмем большое количество таких тестовых изображений и выполним их сжатие кодером ADCT с разными значениями ШК с расчетом полученных значений MSE_{nc}. Кроме того, для каждого тестового изображения и каждого значения ШК рассчитаем P_0. Представим результаты в виде скаттерограммы, где для каждого тестового изображения и значения ШК получим точку, вертикальная координата которой равна ($12MSE_{nc}/QS^2$), а горизонтальная – P_0. Пример такой скаттерограммы приведен на рис. 3.

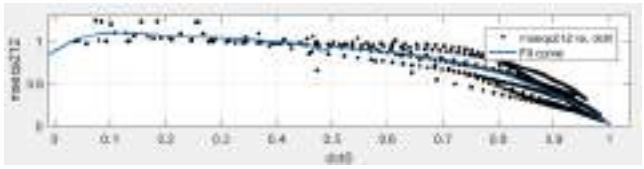
Анализ скаттерограммы на рис. 3 (скаттерограммы одинаковы на всех трех рисунках) показывает следующее. При $P_0 < 0,6$ большинство значений близко к единице и сложно выделить явную тенденцию изменения значений $12MSE_{nc}/QS^2$, хотя и наблюдается, в среднем, небольшое уменьшение значений с ростом P_0. Для участка $P_0 \geq 0,6$ разброс значений $12MSE_{nc}/QS^2$ больше и имеет место явная тенденция к их уменьшению при возрастании P_0. Таким образом, характер зависимости для кодера ADCT такой же, как и для кодера AGU [15].



а



б



в

Рис. 3. Скаттерограмма ($12MSE_{nc}/QS^2$) от P_0 и вписанные в нее аппроксимирующие функции в виде суммы двух экспонент с весами (а), ограниченного ряда Фурье (б), суммы пяти экспонент с весами и сдвигами (в)

Отдельный вопрос – как аппроксимировать зависимость, используя полученную скаттерограмму. В настоящее время это несложный практический вопрос, поскольку имеются унифицированные средства Матлаба, Экселя и других программных продуктов, позволяющих относительно быстро и эффективно решать эту задачу. На рис. 3 приведены три примера решения, хотя использование других функций (полиномов невысокой степени, степенных функций) обеспечивает аналогичные результаты.

Здесь необходимо отметить два момента.

Во-первых, существуют количественные критерии точности вписывания аппроксимирующих кривых [16]. Наиболее часто используемым является критерий R^2, значение которого при явно выраженной статистической зависимости выходного и входных параметров и хорошем вписывании аппроксимирующей кривой стремится к единице, и среднеквадратическое отклонение (root mean square error – RMSE), которое должно быть как можно меньше. С точки зрения обоих критериев качество вписывания для всех трех случаев на рис. 3 одинаково: значения R^2 примерно равны 0,92, а значения RMSE примерно равны 0,084, т. е. СКО отличий прогнозируемого и истинного значения ПОСШ составляет 0,3 дБ (на том же уровне, что и для метода [14]).

Во-вторых, результат вписывания целесообразно контролировать визуально. Например, для результата вписывания на рис. 3,в имеется небольшой локальный минимум, а значения $12MSE_{nc}/QS^2$ для P_0, близких к нулю, меньше единицы, что несколько расходится с результатами экспериментов для малых значений ШК, для которых имеют место малые значения P_0. В этом плане результаты регрессии, представленные на рис. 3,а и б, можно считать в большей степени соответствующими физическому смыслу и результатам исследований. Для аппроксимирующей кривой на рис. 3,а формула такова:

$$f(P_0)=-0{,}007721\exp(4{,}824P_0)+1{,}112\exp(-0{,}1455P_0). \quad (6)$$

Если речь идет о сжатии изображений, искаженных шумом, то для получения аппроксимирующих зависимостей необходимо моделировать такие изображения. В первую очередь были смоделированы изображения, искаженные аддитивным белым гауссовым шумом $I_{ij}^{n}=I_{ij}^{true}+n_{ij}$, где I_{ij}^{true} – истинное значение изображения в ij-м пикселе (изображение без шума), n_{ij} – аддитивный шум с нулевым средним и дисперсией σ^2 в ij-м пикселе. При получении скаттерограммы использовались те же тестовые изображения, что и при получении скаттерограммы на рис. 3, и использовался широкий диапазон значений σ^2 – от 4 и 9, соответствующих визуально незаметному шуму, до 625 и 900, что соответствует очень интенсивным помехам. Полученная скаттерограмма показана на рис. 4. Там же показан вариант вписывания аппроксимирующей функции в виде суммы двух экспонент с весами.

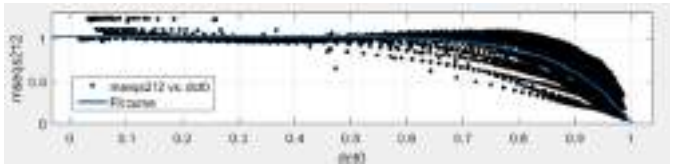


Рис. 4. Скаттерограмма ($12MSE_{nc}/QS^2$) от P_0 и вписанные в нее аппроксимирующие функции в виде суммы двух экспонент с весами для изображений с шумом

Вследствие большего количества изображений на скаттерограмме больше точек. Они расположены достаточно компактно в области $P_0<0{,}6$, которая примерно соответствует небольшим значениям дисперсии помех, и гораздо менее компактно в области $P_0\geq 0{,}6$, где закон распределения ДКП-коэффициентов во многом видоизменяется вследствие помех и по мере увеличения их дисперсии приближается к гауссову с «примесью» тяжелых хвостов. Полученные аппроксимации, например

$$f(P_0)=-0.000177\exp(8.676P_0)+1.027\exp(0.0187P_0), \quad (7)$$

характеризуются R^2 порядка 0,83, а значения RMSE примерно равны 0,135, т.е. точность прогнозирования оказывается гораздо хуже, чем для

рассмотренного ранее случая сжатия изображений, не искаженных помехами.

Одной из причин может быть то, что используемый входной параметр P_0 не является лучшим решением (вопрос выбора наилучшего входного параметра или параметров требует отдельного тщательного исследования). В качестве альтернативы был рассмотрен параметр $P_1=QS/STD_{DCT}$, STD_{DCT} – СКО ДКП-коэффициентов в анализируемых блоках, равный

$$STD_{DCT} = (\frac{1}{63N_{abl}} \sum_{n=1}^{N_{abl}} \sum_{q=1}^{Q(n)} (D(q,n)^2)^{1/2}. \qquad (8)$$

ДКП-коэффициенты в блоках, соответствующие среднему уровню, исключены из рассмотрения.

Очевидно, что параметр P_1 может быть очень быстро и легко рассчитан, что является его несомненным достоинством. Но результаты регрессии для этого параметра хуже, чем для P_0 - значения R^2 порядка 0,67, а значения RMSE примерно равны 0,195. Это означает, что существует взаимосвязь между $12MSE_{nc}/QS^2$ и параметром P_1, но эта взаимосвязь не слишком сильная и она не позволяет точно спрогнозировать $12MSE_{nc}/QS^2$ по рассчитанному для сжимаемого изображения значению P_1. Таким образом, нужны подходы, позволяющие прогнозировать $12MSE_{nc}/QS^2$ более точно.

4. Прогнозирование с использованием машины опорных векторов

Аппроксимация зависимостей для расчета выходного параметра при заданном входном может быть выполнена не только аналитически на основе регрессионных кривых (функций), но и с применением других методов, позволяющих решать задачи определения выходного параметра на основе агрегации входных воздействий. Такими методами, в частности, являются машины опорных векторов (support vector machine – SVM) [17] и искусственные нейронные сети. Их достоинства состоят в том, что можно заранее выполнить обучение и получить сложную нелинейную зависимость выходного параметра от входных.

При построении SVM регрессора использовалось RBF-ядро. Выбор такого экспоненциального ядра обусловлен его хорошей обобщающей способностью, благодаря чему большинство SVM-моделей обладают хорошей способностью прогнозирования на новых данных. Общий набор входных данных делился случайным образом в пропорции 70/30%. При этом 70% использовались для обучения (обучающая выборка), а 30% - для оценки способности прогнозирования полученной модели (тестовая выборка). Для оценки качества регрессии для тестового набора вычислялись показатели RMSE (корень из среднеквадратической ошибки) и R^2 – коэффициент детерминации [16].

Необходимо отметить следующее. Как показывает анализ скаттерограмм на рис. 2 и 3, нет особой необходимости использовать сложный аппроксиматор при $P_0 < 0,6$. Поэтому изучим два подхода.

Первый состоит в том, чтобы не использовать SVM при $P_0 < 0,6$ (а применять в этом случае аппроксимацию (6) или (7), можно вообще считать, что $MSE_{nc}=QS^2/12$ и после этого рассчитывать $QS=(12MSE_{nc})^{1/2}$). Если же $P_0 \geq 0,6$, то будем использовать SVM, который и обучим только для данных, полученных для $P_0 \geq 0,6$.

Второй подход – обучить SVM для всего диапазона (ВД) значений P_0 и использовать в любом случае.

Некоторые результаты обучения приведены в таблице. Анализируются два метода аппроксимации (линейная регрессия (ЛР) и SVM). В качестве входных параметров рассматриваются σ, P_0, P_1 и их комбинации по два параметра.

Метод	Область обучения	RMSE	R^2	Входные параметры
ЛР	ВД	0,267	0,35	σ
SVM	ВД	0,272	0,34	σ
ЛР	$P_0 \geq 0,6$	0,241	0,41	σ
SVM	$P_0 \geq 0,6$	0,243	0,41	σ
ЛР	ВД	0,198	0,64	P_1
SVM	ВД	0,191	0,67	P_1
ЛР	$P_0 \geq 0,6$	0,220	0,51	P_1
SVM	$P_0 \geq 0,6$	0,213	0,55	P_1
ЛР	ВД	0,225	0,54	P_0
SVM	ВД	0,138	0,83	P_0
ЛР	$P_0 \geq 0,6$	0,177	0,69	P_0
SVM	$P_0 \geq 0,6$	0,150	0,77	P_0
ЛР	ВД	0,140	0,82	P_1 и σ
SVM	ВД	0,100	0,91	P_1 и σ
ЛР	$P_0 \geq 0,6$	0,139	0,80	P_1 и σ
SVM	$P_0 \geq 0,6$	0,104	0,89	P_1 и σ
ЛР	ВД	0,183	0,70	P_0 и σ
SVM	ВД	0,104	0,90	P_0 и σ
ЛР	$P_0 \geq 0,6$	0,108	0,88	P_0 и σ
SVM	$P_0 \geq 0,6$	0,092	0,92	P_0 и σ
ЛР	ВД	0,190	0,67	P_1 и P_0
SVM	ВД	0,117	0,88	P_1 и P_0
ЛР	$P_0 \geq 0,6$	0,172	0,70	P_1 и P_0
SVM	$P_0 \geq 0,6$	0,128	0,84	P_1 и P_0

Очевидно, что использование только σ или дисперсии помех приводит к неудовлетворительной точности прогнозирования – значения R^2 очень низкие, а значения RMSE – слишком велики. Точность выше, если использовать в качестве входно-

го параметра P_1, особенно если применять SVM, обученный только для области $P_0 \geq 0{,}6$. Еще лучше результаты, если использовать в качестве входного параметра P_0 и обученный SVM.

Рассмотрим теперь случай применения двух входных параметров. Совместное использование P_1 и σ дает заметный положительный результат, особенно при применении SVM. Еще лучше результаты для совместного использования P_0 и σ. Но в обоих этих случаях нужно знать σ. Наконец, совместное применение P_1 и P_0 дает несколько худший результат (нужно использовать SVM), но оба входных параметра рассчитываются исключительно быстро и легко.

Перейдем теперь к рассмотрению сигнально-зависимых помех. В этом случае изображение описывается как $I_{ij}^{n} = I_{ij}^{true} + n_{ij}$, где шум имеет нулевое среднее и дисперсию вида $\sigma_{ij}^2 = kI_{ij}^{true} + \sigma_0^2$, где σ_0^2 – дисперсия сигнально-независимой составляющей, а k – параметр сигнально-зависимой составляющей. Возможны различные практические ситуации превалирующего влияния как первой, так и второй составляющей. В значительных пределах может варьироваться и интенсивность помех, характеризуемая эквивалентной дисперсией:

$$\sigma_{ij}^2 = \sigma_0^2 + k\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} I_{ij}^{true} / (N_1 N_2) .$$

При моделировании рассматривались все возможные комбинации для следующих наборов параметров: пять значений σ_0, равных 0, 5, 10, 15 и 20, а также семь значений k, равных 0, 0,05, 0,1, 0,2, 0,4, 0,6, 0,8.

Кривые, вписанные в скаттерограммы для параметра P_0 для случаев чисто аддитивного и смешанного (сигнально-зависимого) шумов, приведенных на рис. 5. Хорошо видно, что эти кривые практически совпадают, а коэффициент корреляции между функциональными зависимостями равен 0.998.

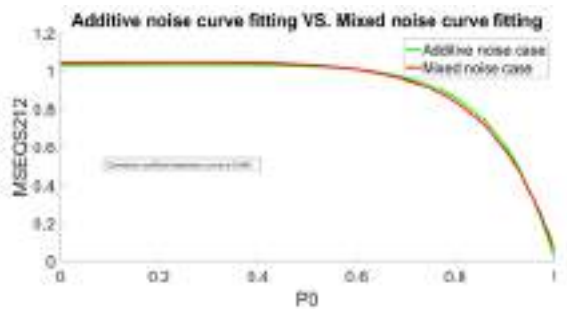


Рис. 5. Сравнение аппроксимирующих функций для случаев аддитивного и смешанного шумов при P_0

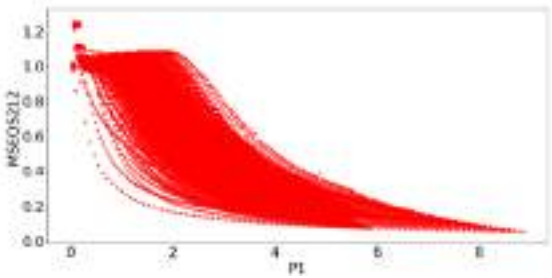


Рис. 6. Скаттерограмма для случая смешанного шума

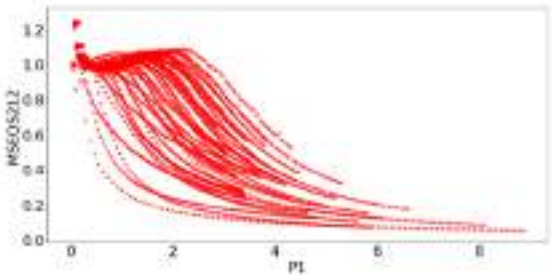


Рис. 7. Скаттерограмма для случая аддитивного шума

Скаттерограммы для P_1 для обоих рассматриваемых типов помех приведены на рис. 6 и 7. Полученные скаттерограммы очень похожи друг на друга, что косвенно подтверждает близость результатов и возможность применения прогнозирования для обоих типов помех.

SVM, обученный для сигнально-зависимых помех при совместном использовании параметров P_1 и P_0 в качестве входных обеспечивает RMSE, равное 0.089. Это позволяет применять его для предсказания искажений как для изображений, искаженных аддитивными, так и для изображений, на которых присутствуют сигнально-зависимые помехи.

Выводы

Как свидетельствуют приведенные результаты, СКОш помех, вносимых при сжатии изображений с потерями, достаточно жестко связана с шагом квантования и может быть предсказана. Предложены параметры, позволяющие выполнять предсказание достаточно быстро и точно, причем для изображений как без шумов, так и с шумами. Рассмотрен достаточно общий случай сигнально-зависимых помех и показано, что для предсказания не обязательно знать характеристики помех.

Литература: 1. *Taubman D., Marcellin M.* JPEG2000 Image Compression Fundamentals, Standards and Practice. Springer, Boston: Kluwer, 2002. 777 p. 2. *Blanes I., Magli E., Serra-Sagrista J.* A Tutorial on Image Compression for Optical Space Imaging Systems // IEEE Geoscience and Remote Sensing Magazine. 2014. Vol 2(3). P. 8-26. 3. *Баранник В.В., Яковенко А.В.* Информационная технология сжатия изображений на основе двумерного плавающего полиадического кодирования трансформант Уо-

лша // Системи обробки інформації. 2008. Вип. 3. С. 13-17. 4. *Zemliachenko A., Ponomarenko N., Lukin V., Egiazarian K., Astola J.* Still Image/Video Frame Lossy Compression Providing a Desired Visual Quality // Multidimensional Systems and Signal Processing. June 2015. 22 p. 5. *Ponomarenko N.N., Lukin V.V., Egiazarian K.O., Astola J.T.* High Quality DCT Based Image Compression Using Partition Schemes // IEEE Signal Processing Letters, Vol. 14, Febr. 2007. P. 105-108. 6. *Zemliachenko A., Kozhemiakin R., Abramov S., Lukin V., Vozel B., Chehdi K., Egiazarian K.* Prediction of compression ratio for DCT-based coders with application to remote sensing images // Journal on Selected Topics in Applied Earth Observations and Remote Sensing. 2018. Vol. 11, No 1. P. 257-270. 7. *Ponomarenko N., Lukin V., Zriakhov M., Egiazarian K.* Lossy compression of images with additive noise. / Proceedings of International Conference on Advanced Concepts for Intelligent Vision Systems, Antwerpen, Belgium, 2005. P. 381-386. 8. *Al-Chaykh O.K., Mersereau R.M.* Lossy compression of noisy images // IEEE Transactions on Image Processing. 1998, Vol. 7(12). P. 1641-1652. 9. *Zemliachenko A.N., Kozhemiakin R.A., Uss M.L., Abramov S.K., Ponomarenko N.N., Lukin V.V., Vozel B., Chehdi K.* Lossy compression of hyperspectral images based on noise parameters estimation and variance stabilizing transform // Journal of Applied Remote Sensing. 2014. Vol 8 (1). 25 p. 10. *Zemliachenko A., Abramov S., Lukin V., Vozel B., Chehdi K.* Lossy Compression of Noisy Remote Sensing Images with Prediction of Optimal Operation Point Existence and Parameters // SPIE Journal on Advances in Remote Sensing, , 2015. Vol. 9(1). 26 p. 11. *Lukin V., Ponomarenko N., Egiazarian K., Astola J.* Analysis of HVS-Metrics' Properties Using Color Image Database TID2013 / Proceedings of ACIVS, October 2015, Italy. P. 613-624. 12. *Uss M.L., Vozel B., Lukin V., Chehdi K.* Image Informative Maps for Component-wise Estimating Parameters of Signal-Dependent Noise // Journal of Electronic Imaging, 2013. Vol. 22(1). Doi:10.1117/1.JEI.22.1.013019. 13. *Kozhemiakin R., Lukin V., Vozel B.* Image Quality Prediction for DCT-based Compression / Proceedings of CADSM 2017. February 2017, Ukraine, P. 225-228. 14. *Minguillon J., Pujol J.* JPEG Standard Uniform Quantization Error Modeling with Applications to Sequential and Progressive Operation Modes // *Electron. Imaging*, 2001, Vol. 10(2), P. 475-485. 15. *Krivenko S., Zriakhov M., Lukin V., Vozel B.* MSE Prediction in DCT-based Lossy Compression of Noise-Free and Noisy Remote Sensing Images / Proceedings of TCSET, Februry 2018, Lviv-Slavske, Ukraine, 6 p. 16. *Cameron C., Windmeijer A., Frank A.G., Gramajo H., Cane D.E., Khosla C.* An R-squared measure of goodness of fit for some common nonlinear regression models // Journal of Econometrics, 1997. Vol. 77(2). 16 p. 17. *Chih-Chung Chang and Chih-Jen Lin*, LIBSVM : a library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2:27:1--27:27, 2011. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

Поступила в редколлегию 11.05.2018
Рецензент: д-р техн. наук, проф. Безрук В.В.

Кривенко Сергей Станиславович, канд. техн. наук, старший научный сотрудник кафедры информационно-коммуникационных технологий им. А.А. Зеленского, Национальный аэрокосмический университет. Научные интересы: сжатие изображений. Адрес: Украина, 61000, Харьков, e-mail: krivenkos@ukr.net

Зряхов Михаил Сергеевич, канд. техн. наук, доцент, кафедры информационно-коммуникационных технологий им. А.А. Зеленского, Национальный аэрокосмический университет. Научные интересы: цифровая обработка сигналов и изображений. Адрес: Украина, 61000, Харьков, e-mail: m.zriakhov@khai.edu

Лукин Владимир Васильевич, д-р техн. наук, профессор, зав. кафедрой информационно-коммуникационных технологий им. А.А. Зеленского, Национальный аэрокосмический университет. Научные интересы: цифровая обработка сигналов и изображений. Адрес: Украина, 61000, Харьков. e-mail: lukin@ai.kharkov.com

Krivenko Sergey, candidate of science, Senior Researcher, Dept of Information Communication Technologies named after A.A. Zelensky, National aerospace university. Scientific interests: Image compression. Ukraine, Kharkov, e-mail: krivenkos@ukr.net

Mikhail Zriakhov, candidate of science, associate professor, Dept of Information Communication Technologies named after A.A. Zelensky, National aerospace university. Scientific interests: Image and signal processing. Ukraine, Kharkov. e-mail: m.zriakhov@khai.edu

Lukin Vladimir, doctor of science, professor, Head of Dept of Information Communication Technologies named after A.A. Zelensky, National aerospace university. Scientific interests: Image and signal processing. Ukraine, Kharkov. e-mail: lukin@ai.kharkov.com

СИСТЕМЫ И ПРОЦЕССЫ УПРАВЛЕНИЯ

УДК 004.056.53

БЕЗПЕКА ІНТЕРНЕТ РЕСУРСІВ: АНАЛІЗ РОЗПОВСЮДЖЕНОСТІ ЗАГРОЗ ТА ТЕХНОЛОГІЇ ЗАХИСТУ

СЛОБОДЯНЮК О.В., ХАХАНОВА А.В., КОМОЛОВ Д.И.

Описуються основні підходи до класифікації відомих вразливостей веб-ресурсів. Аналізується активність найбільш розповсюджених типів загроз на основі звітів компаній, що займаються моніторингом інцидентів порушення безпеки веб-ресурсів. Розглядаються основні технології захисту від можливих реалізацій погроз.

Ключові слова: уразливість, загроза, OWASP, WASC, WAF.

Keywords*:* vulnerability, threat, OWASP, WASC, WAF.

Вступ

Питання захисту веб-ресурсів від несанкціонованих втручань ззовні є однією із найбільших проблем забезпечення їх сталого функціонування. Сучасний веб-ресурс являє собою досить складну програмну структуру, що включає у себе цілий ряд технологій із модульним підходом та можливістю постійної модифікації й вдосконалення. Як наслідок цього, більшість веб-сайтів та веб-сервісів характеризуються цілим рядом вразливостей, через які зловмисники мають реальні можливості проводити атаки на найрізноманітніші сайти із використанням досить широкого інструментарію. Дані вразливості викликані як ненавмисно допущеними помилками розробниками на стадії проектування, так і недосконалістю технологій, що були використані при створенні ресурсу. Окремо можна виділити зумисно допущені помилки, які генеруються недобросовісними розробниками, планують у подальшому використати їх для несанкціонованого втручання у роботу ресурсу. Як правило усі системи керування вмістом (CMS) та фреймворки, що використовуються при створенні веб-сайтів, мають великі спільноти шанувальників, завдяки яким вдається вчасно локалізувати та виправити помилки у підсистемах безпеки. Однак часто буває так, що служби підтримки ресурсів вчасно не проводять заходи щодо оновлення програмних модулів, не забезпечують належного контролю за даними, не виконують перевірки доступу та інше. Більшість вразливостей, що використовуються середньостатистичним зловмисником, не є архіскладними і не вимагають високої кваліфікації для їх застосування.

1. Ризики безпеки веб-застосунків

При проведенні аналізу рівня захищеності веб-ресурсу найчастіше використовується поняття ризику та вразливості. Так, коли говорять про нездатність інформаційної системи протидіяти зовнішнім втручанням або протистояти реалізації певних загроз, то це мається на увазі поняття вразливості (англ. vulnerability) [5]. Під ризиком, згідно з документом «Основні поняття. НД ТЗІ 1.1-003-99: «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» розуміють функцію ймовірності реалізації певної загрози, виду і величини завданих збитків [5]. Також дуже часто організації, що займаються моніторингом та обліком інцидентів, пов'язаних з кібербезпекою, використовують поняття загрози (англ. threat).

Збором відомостей, моніторингом активності та класифікацією відомих чи нових вразливостей займається цілий ряд організацій та об'єднань, серед яких варто виділити відкритий проект забезпечення безпеки веб-застосунків (Open Web Application Security Project, OWASP), консорціум безпеки веб- застосунків (Web Application Security Consortium, WASC), науково-дослідницький центр корпорації MITRE (National Cybersecurity Center of Excellence's, NCCoE's)), центр комп'ютерної безпеки університету Карнегі Меллон (Computer Emergency Response Team Coordination Center, CERT/CC), центр ресурсів комп'ютерної безпеки уряду США (Computer Security Resource Center, CSRC) та інші. Звичайно кожна серйозна організація, що займається питаннями інформаційної безпеки веб-застосунків, має свої розроблені методики виявлення загроз та протидії ризикам їхніх впливів. Однак переважна більшість користуються класифікаторами OWASP, WASC TD та CWE/SANS.

2. Класифікація ризиків OWASP

OWASP являє собою проект забезпечення безпеки веб- застосунків. Спільнота OWASP є повністю відкритою й ставить собі за мету сприяння організаціям у розробці, придбанні та підтримці застосунків, безпеці яких можна довіряти. Структурно спільнота складається з корпорацій, освітніх організацій та приватних осіб зі всього світу. Для вирішення основних задач по збору й класифікації вразливостей веб-застосунків члени спільноти працюють над створенням наукових статей, навчальних посібників, документації, інструментів та технологій, які потім викладають у вільний доступ. Також OWASP пропонує безкоштовний доступ до інструментів та стандартів безпеки застосунків, детальних рекомендацій щодо тестування,

розробки та аналізу безпеки програм.

Один раз на три роки спільнота публікує зведений рейтинг ТОП-10 [7] найнебезпечніших ризиків (вразливостей), який відображає сучасні тенденції безпеки веб-застосунків. OWASP TOP-10 – це інформаційний документ, який широко використовується багатьма організаціями. Він актуальний в рамках програм винагород за виявлені вразливості (bug bounty programs), а також для класифікації вразливостей за рівнем небезпеки.

Остання версія документу була опублікована у 2017 році і містить такі типи найнебезпечніших ризиків веб-застосунків:

1) Вставка ін'єкцій (A1:2017 – Injection).
2) Некоректна аутентифікація та управління сеансами (A2:2017 – Broken Authentication).
3) Витік критичних даних (A3:2017 – Sensitive Data Exposure).
4) Вставка XML інструкцій (A4:2017 – XML External Entities (XXE).
5) Порушений контроль доступу (A5:2017 – Broken Access Control).
6) Неправильна конфігурація безпеки (A6:2017 – Security Misconfiguration).
7) Міжсайтове виконання сценаріїв (A7:2017 – Cross-Site Scripting (XSS).
8) Небезпечна десеріалізація (A8:2017 – Insecure Deserialization).
9) Використання компонентів з відомими вразливостями (A9:2017 – Using Components with Known Vulnerabilities).
10) Недостатнє журналювання та моніторинг (A10:2017 – Insufficient Logging&Monitoring) [7].

Якщо провести кількісний аналіз зафіксованих протягом 2017 року вразливостей у базі OWASP (рис. 1), то можна бачити, що кількість випадків міжсайтового виконання сценаріїв сумарно перевищує усі інші разом взяті типи вразливостей і доходить до 2 млн.

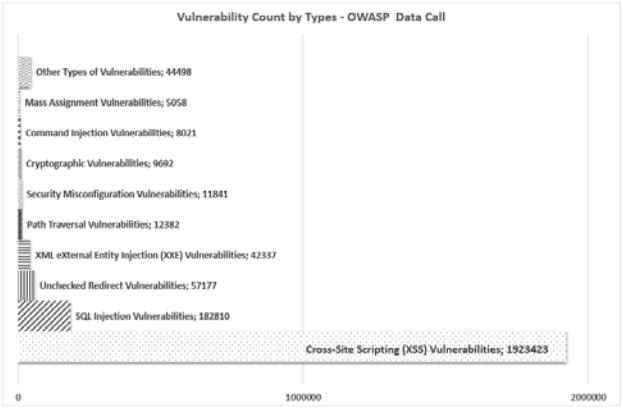


Рис. 1. Кількість зафіксованих у 2017 році вразливостей за їхніми типами згідно з даними OWASP

Дана статистика кардинально відрізняється від позицій у ТОП – 10, оскільки при складанні рейтингу OWASP використовує методологію, що основана на методиці оцінки ризиків. Для кожної позиції рейтингу оцінюється типовий ризик, який кожне слабке місце може викликати у типовому веб-застосунку, розглядаючи фактори, що впливають на ймовірність та на наслідки для кожного слабкого місця. Потім складається рейтинг Топ-10 відповідно до слабких місць, що, як правило, стають причиною найбільш значущих ризиків для застосунку. Методика оцінки ризиків OWASP визначає численні фактори для розрахунку ризиків визначеної уразливості. Однак Топ 10 призначений для розгляду загальних випадків, а не конкретних вразливостей у реальному застосунку. Саме тому OWASP ніколи не прагне досягти точності, аналогічної тій, яку можуть досягти власники систем при розрахунку ризиків для своїх застосунків. Зазначена методика включає в себе три фактори, що впливають на ймовірність для кожного слабкого місця (поширеність, можливість виявлення та легкість вторгнення), та один фактор, що впливає на наслідки (технічні наслідки). Поширеність слабкого місця – це фактор, який, як правило, не потрібно розраховувати. Дані щодо поширеності отримують від різних організацій і потім обраховують з цих даних середнє значення для визначення ймовірності їх включення у Топ-10 за поширеністю. Потім ці дані поєднують з іншими двома факторами ймовірності (можливість виявлення та легкість вторгнення) з метою розрахунку рейтингу ймовірності кожного слабкого місця. Після цього отримані результати множать на розраховані технічні наслідки для кожної позиції і, як результат, отримують загальний рейтинг ризиків по кожній позиції Топ-10 [7].

3. Класифікація загроз WASD

The WASC Threat Classification – це результати спільної роботи членів консорціуму безпеки вебзастосунків, які спрямовані на опис та упорядкування відомих загроз безпеки веб-сайтів. Даний проект був створений для розробки та популяризації стандартної термінології опису зазначених проблем. Це дає можливість розробникам застосунків, спеціалістам в області безпеки, виробникам програмних продуктів та аудиторам використовувати спільну термінологічну базу для взаємодії. Цілями учасників консорціуму є: визначення всіх відомих класів атак на вебзастосунки; узгодження назв для кожного з класів; розробка структурованого підходу до класифікації атак; створення документації, що містить загальний опис кожного з класів.

Згідно з класифікатором атаки на веб-застосунки поділяються на:

1. Аутентифікація (Authentication) – атаки, які спрямовані на використовувані веб-застосунком методи перевірки ідентифікатора користувача, служби або програми. Аутентифікація використ-

товує як мінімум один з трьох механізмів (факторів): «щось, що ми маємо», «щось, що ми знаємо» або «щось, що ми є». Атаки даного класу спрямовані на обхід або експлуатацію вразливостей в механізмах реалізації аутентифікації вебсерверів.

2. Авторизація (Authorization) – атаки, що направлені на методи, які використовуються вебсервером для визначення того, чи має користувач, служба або застосунок необхідні для виконання операції зміни дозволів. Багато веб-сайтів дозволяють тільки певним користувачам отримувати доступ до деякого вмісту або функцій програми. Доступ іншим користувачам повинен бути обмежений. Використовуючи різні техніки, зловмисник може підвищити свої привілеї і отримати доступ до захищених ресурсів.

3. Атаки на клієнтів (Client-side Attacks) – атаки на користувачів веб-сервера. Під час відвідування сайту між користувачем і сервером встановлюються довірчі відносини як в технологічному, так і в психологічному аспекті. Користувач очікує, що сайт буде надавати йому легітимний вміст. Крім того, користувач не очікує атак з боку сайту. Експлуатуючи цю довіру, зловмисник може використовувати різні методи для проведення атак на клієнтів сервера.

4. Виконання коду (Command Execution) – клас атак, які спрямовані на виконання коду на вебсервері. Всі сервери використовують дані, що були надіслані користувачем при обробці запитів. Часто ці дані використовуються при складанні команд, що застосовуються для генерації динамічного вмісту. Якщо при розробці не враховуються вимоги безпеки, зловмисник отримує можливість модифікувати виконувані команди.

5. Розголошення інформації (Information Disclosure) – атаки, що спрямовані на отримання додаткової інформації про веб-застосунок. Використовуючи ці вразливості, зловмисник може визначити використовувані дистрибутиви, номери версій клієнта й сервера, а також встановлені оновлення. В інших випадках в інформації, що витікає, можуть міститися відомості про розташування тимчасових файлів або резервних копій. У багатьох випадках ці дані не потрібні для роботи користувача. Більшість серверів надають доступ до надмірного обсягу даних, однак необхідно мінімізувати обсяг службової інформації. Чим більші знання про програму буде мати у своєму розпорядженні зловмисник, тим легше йому буде скомпрометувати систему.

6. Логічні атаки (Logical Attacks) – спрямовані на експлуатацію функцій застосунка або логіки його функціонування. Логіка застосунка – це очікуваний процес функціонування програми при виконанні певних дій. Як приклади можна навести відновлення паролів, реєстрацію облікових записів, аукціонні торги, транзакції в системах електронної комерції. Застосунок може вимагати від користувача коректного виконання декількох послідовних дій для певного завдання. Зловмисник може обійти або використовувати ці механізми в своїх цілях [9].

На відміну від OWASP консорціум не веде статистику активності та кількості проведених на веб-ресурси атак. Однак таким займаються організації-члени консорціуму. Однією з них є компанія Positive Technologies. Аналіз звіту за 2016 рік [6] показує, що кожен третій виявлений недолік відноситься до високого класу небезпеки (рис. 2).

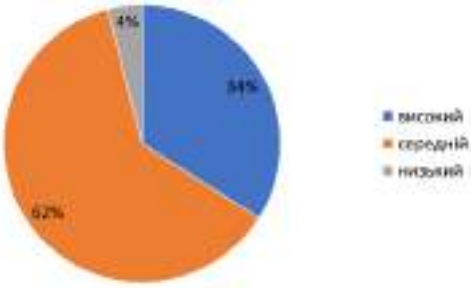


Рис. 2. Доля вразливостей різного ступеня ризику

Хоча більшість виявлених вразливостей характеризуються середнім рівнем ризику (62%), а 4% віднесені до низького рівня ризику, але абсолютно усі застосунки, які були досліджені, містили щонайменше одну вразливість середнього рівня небезпеки. Розподіл знайдених спеціалістами компанії вразливостей різного класу небезпеки веб-застосунках протягом 2011-2015 років показано на рис. 3.

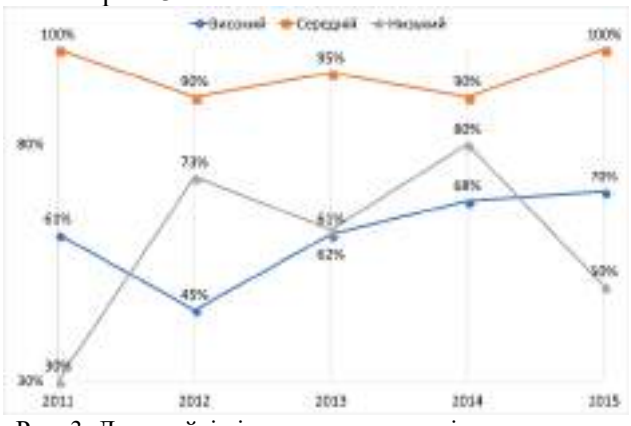


Рис. 3. Доля сайтів із вразливостями різного ступеня ризику

Незважаючи на те, що дані досліджень не є достатньо репрезентативними через відносно невелику кількість проаналізованих веб-ресурсів, але вони гарно показують загальну тенденцію зростання класу небезпеки вразливостей, що ідентифікуються спеціалістами із кібербезпеки. Це викликано як різким зростанням складності технологій, що використовуються під час розробки сучасних веб-застосунків (зростає ймовірність

виникнення помилки, використання засобів розробки із непідтвердженим рівнем безпеки тощо), так і створенням більш ефективних інструментів несанкціонованого втручання у роботу програмних систем.

4. Методи та підходи до захисту веб-застосунків

Вислів «Попереджений – значить озброєний!» повністю працює в галузі безпеки веб-застосунків та веб-ресурсів в цілому. Тому найпершим засобом захисту від ризиків є періодичне проведення аудиту безпеки та своєчасне оновлення програмних модулів.

Існує декілька методологій проведення аудиту застосунку. Вони є найбільш ефективними у окремі періоди життєвого циклу програмного забезпечення. Кожен з них представляє певні цикли часу, зусилля, витрати щодо знаходження цих уразливостей.

1) Метод «білої скриньки» або аудит коду. Особа, що проводить аудит, глибоко розуміє застосунок та вручну переглядає початковий код, записуючи вразливості безпеки. Аудитору надається доступна вичерпна інформація про структуру застосунку, особливості побудови всіх його елементів та забезпечується коректність взаємодії його частин.

2) Метод «чорної скриньки». Даний вид аудиту передбачає те, що інформація про досліджуваний об'єкт повністю відсутня. Функції об'єкта можна визначити лише за реакцією його на зовнішні фактори. До початку аудиту за цим методом аудитор має визначити внутрішню архітектуру. Саме тестування проводиться за допомогою імітаційного моделювання відомих типів атак на веб-ресурси.

3) Інструментарій. Аудит проводиться із застосуванням автоматизованих інструментів, які перевіряють наявність недоліків та дефектів безпеки, часто з більшою позитивною швидкістю, ніж залучення людини. До такого інструментарію відносяться сканери, брандмауери, антивіруси, фільтри тощо [1].

Для організації захисту інформаційної інфраструктури використовується велика кількість типів захисних рішень – Firewall, IPS/IDS (система запобігання вторгнень/система виявлення вторгнень), NGFW (Next Generation Firewall), WAF (Web-Application Firewall). Однак сьогодні понад 80% атак експлуатують уразливості саме веб-застосунків, а не мережевої архітектури. Тому класичні системи захисту мереж виявляються малоефективними проти сучасних кіберзагроз. До того ж сьогодні існує величезна кількість веб-застосунків (кожен з яких потенційно може містити в собі певні вразливості), тобто загальна кількість вразливостей набагато більша, ніж кількість сигнатур в базах сучасних систем запобігання вторгнень. За оцінками багатьох експертів з кібербезпеки, саме проникнення через веб-застосунки останнім часом стають основним вектором атак на корпоративні мережі, причому традиційні системи безпеки, такі як брандмауер та антивірусна система, не здатні ефективно запобігати подібним атакам. Для надійного захисту необхідний кардинально інший підхід: з глибоким аналізом змісту пакетів і хорошим знанням структури веб-застосунків, включаючи URL-параметри, форми введення даних і ін. Таким умовам задовольняє Web Firewall Application – брандмауер для застосунків, які здійснюють передачу даних через HTTP і HTTPS [3].

Принцип дії WAF нагадує прозорий проксі-сервер або міст. Підтримується, як правило, також реплікація трафіка. Для виявлення атак WAF застосовує як сигнатурний, так і поведінковий підходи. Другий метод також дуже важливий, оскільки для атак на веб-застосунок кіберзлочинці можуть застосовувати уразливості нульового дня (0day vulnerability), що зводить до нуля ефективність сигнатурного аналізу. Основним компонентом WAF є модуль машинного навчання, який призначений для створення еталонної моделі комунікації з об'єктом захисту. При цьому передбачається, що при проведенні першого раунду перевірки вразливості веб-застосунку не експлуатуються. Таким чином, формується список дозволених ідентифікаторів доступу і будується модель нормального функціонування застосунку. На відміну від класичних брандмауерів, які генерують великі обсяги помилкових спрацьовувань на різні підозрілі події, WAF здатний аналізувати тисячі подій і будувати ланцюг розвитку атаки – від першого етапу до останнього.

Однак не все так райдужно, як би хотілося, і з WAF. Так, в силу своїх функціональних обмежень, він не здатний захистити веб-застосунок від усіх можливих вразливостей. WAF не видаляє вразливість, а лише (частково) закриває вектор атаки.

Висновки

Аналізуючи ситуацію навколо питань безпеки веб-ресурсів, можна зробити висновок, що даний напрямок є наразі найбільшою «гарячою точкою» в інформаційній безпеці загалом. Зростання у геометричній прогресії кількості типів нових вразливостей та офіційно зафіксованих успішних атак на веб-ресурси може свідчити про те, що даний напрямок ще доволі довго залишатиметься найбільш популярним у кіберзлочинців та спеціалістів із комп'ютерної безпеки.

На превеликий жаль, доводиться констатувати той факт, що до цих пір не запропоновано більш ефективної технології захисту, ніж регулярне проведення аудиту вразливостей. При цьому найбільшу якість може гарантувати лише ручна перевірка за складеними чек-листами і залученням відповідних спеціалістів. Наприклад, на популярних Bug Bounty платформах (hackerOne, BugCrowd, Synack, Zerocopter, Cobalt, Intigrity, HackenProof та інші).

Література: 1. *Безпека* додатків [Електронний ресурс]. 2018. Режим доступу до ресурсу: https://bit.ly/2LL77JC. **2.** *Годовой* отчет Cisco по информационной безопасности [Електронний ресурс]. 2017. Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/products/security/security-reports.html. **3.** *Захист* веб-додатків: чому це важливо? [Електронний ресурс]. 2016. Режим доступу до ресурсу: https://itbiz.ua/ua/zashhita-veb-prilozheniy-pochemu-yeto-vazhn. **4.** *Основні* поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс] // Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999. Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_НД_ТЗІ_1.1-003-99.pdf. **5.** *Поповский В.В.* Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков. Х.: ООО "Компания СМИТ", 2006. Т. 2. 292 с. **6.** *Уязвимости* веб - приложений [Електронний ресурс] // Positive Technologies. 2016. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerability-2016-rus.pdf. **7.** *OWASP* Top 10 – 2017. The Ten Most Critical Web Application Security Risks. [Електронний ресурс]. 2017. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. **8.** *Prakhar P.* Mastering Modern Web Penetration Testing / Prasad Prakhar. – BIRMINGHAM - MUMBAI: Packt Publishing, 2016. 298 с. **9.** The WASC Threat Classification v2.0 [Електронний ресурс] // WEB APPLICATION SECURITY CONSORTIUM – Режим доступу до ресурсу: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf. **9.** *Yaworski P.* Web Hacking 101. How to Make Money Hacking Ethically [Електронний ресурс] / Peter Yaworski // Lean Publishing. 2017. Режим доступу до ресурсу: http://leanpub.com/web-hacking-101.

Транслітерований список літератури

1. Bezpeka dodatkiv [Elektronnij resurs]. – 2018. – Rezhim dostupu do resursu: https://bit.ly/2LL77JC.
2. Godovoj otchet Cisco po informacionnoj bezopasnosti [Elektronnij resurs]. – 2017. – Rezhim dostupu do resursu: https://www.cisco.com/c/ru_ru/products/security/security-reports.html.
3. Zahist veb-dodatkiv: chomu ce vazhlivo? [Elektronnij resurs]. – 2016. – Rezhim dostupu do resursu: https://itbiz.ua/ua/zashhita-veb-prilozheniy-pochemu-yeto-vazhn.
4. Osnovni ponjattja. ND TZI 1.1-003-99: Terminologija v galuzi zahistu informacії v komp'juternih sistemah vid ne-sankcionovanogo dostupu. [Elektronnij resurs] // Kiïv: Depa-rtament special'nih telekomunikacijnih sistem ta zahistu informacії Sluzhbi bezpeki Ukraïni. – 1999. – Rezhim dostu-pu do resursu: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_ND_TZI_1.1-003-99.pdf.
5. Popovskij V.V. Zashhita informacii v telekommunikacionnyh sistemah: uchebnik / V.V. Popovskij, A.V. Persikov. – H.: OOO "Kompanija SMIT", 2006. T. 2. – 292 s.
6. Ujazvimosti veb prilozhenij [Elektronnij resurs] // Positive Technologies. – 2016. – Rezhim dostupu do resursu: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerability-2016-rus.pdf.
7. OWASP Top 10 – 2017. The Ten Most Critical Web Appli-cation Security Risks. [Elektronnij resurs]. – 2017. – Rezhim dostupu do resursu: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.
8. Prakhar P. Mastering Modern Web Penetration Testing / Prasad Prakhar. – BIRMINGHAM - MUMBAI: Packt Publishing, 2016. – 298 s.
9. The WASC Threat Classification v2.0 [Elektronnij resurs] // WEB APPLICATION SECURITY CONSORTIUM – Rezhim dostupu do resursu: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf.
10. Yaworski P. Web Hacking 101. How to Make Money Hacking Ethically [Elektronnij resurs] / Peter Yaworski // Lean Publishing. – 2017. – Rezhim dostupu do resursu: http://leanpub.com/web-hacking-101.

Надійшла до редколегії 06.06.2018

Рецензент: д-р техн. наук, проф. Бараннік В.В.

Слободянюк Олександр Васильович, канд. техн. наук, доцент кафедри інформатики Кам'янець-Подільського національного університету імені Івана Огієнка, Кам'янець-Подільський, e-mail: slobodyanyuk.olexandr@kpnu.edu.ua.

Хаханова Анна Володимирівна, канд, техн. наук, доцент, докторант кафедри АПОТ ХНУРЕ. Наукові інтереси: обробка інформації. Адреса: Україна, 61166, Харків, пр. Науки, 14. E-mail: Ann.hahanova@gmail.com.

Комолов Дмитро Іванович, канд. техн. наук, старший викладач кафедри ІМІ ХНУРЕ. Наукові інтереси: обробка інформації. Адреса: Україна, 61166, Харків, пр. Науки, 14, e-mail: elsdefan@gmail.com.

Slobodyanyuk Oleksandr, PhD, Associate Professor at Kamianets-Podilskyi National Ivan Ohiienko University, e-mail: slobodyanyuk.olexandr@kpnu.edu.ua

Hahanova Anna, Candidate of Technical Science, docent, post doc, Design Automation Department, Kharkov National University of Radioelectronics. Scientific interests: processing of information. Address: Ukraine, 61166, Kharkiv, Nauki Ave, 14, e-mail: Ann.Hahanova@gmail.com.

Komolov Dmitry Ivanovich, PhD, Senior Lecturer of the Department of INI, Kharkiv National University of Radioelectronics. Scientific interests: processing of information. Address: 61166, Kharkiv, avenue. Sciences 14, e-mail: elsdefan@gmail.com

КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ

УДК 658:512.011:681.326:519.713

СИНТЕЗ И АНАЛИЗ ЛОГИЧЕСКИХ Х-ФУНКЦИЙ

ЛЮБАРСКИЙ М.М., АБДУЛЛАЕВ В.Г., ХАХАНОВ В.И., ЧУМАЧЕНКО С.В., ЛИТВИНОВА Е.И., ХАХАНОВ И.В.

Предлагаются модели и методы кубитного синтеза и анализа логических Х-функций (xor, not-xor) от n переменных [1-8], которые являются мощным математическим средством для решения задач генерации тестов, моделирования неисправностей, создания тестопригодных схем. Их основное преимущество заключается в проверяемости неисправностей, инверсных по отношению к исправному поведению логической схемы.

Введение

Компьютинг – вычислительный процесс, представленный транзакциями записи-считывания данных на адресуемой памяти [1]. Такое определение на самом низком уровне убирает теоретические барьеры, создаваемые теоремой Поста и полнотой функционального базиса, устраняет логику (ALU) и шины передачи данных между процессором и памятью в классическом компьютинге. Более того, транзакционный (MAT – Memory-Address-Transaction) компьютинг настоятельно предлагает отказаться от квантовой логики, реализация которой создает технологические проблемы при создании квантового компьютера. Вполне достаточно реализовать фотонные транзакции записи-считывания данных на устойчивой структуре атомарных электронов, выполняемые со скоростью света.

Memory-driven компьютинг – вычислительный процесс, реализуемый в памяти, содержащей три компонента архитектуры: control-, computational- and conventional memory. Memory-driven классический компьютинг имеет существенный недостаток, который заключается в длительном цикле (read-write) обращения к памяти, в десятки раз большем, чем время выполнения логической операции. Однако реализация memory-driven компьютинга на квантовых (фотонных) транзакциях в атомарной структуре электронов устраняет низкое быстродействие обращения к памяти, благодаря световой скорости фотонного обмена данными, что дает возможность убрать из компьютинга технологически сложно реализуемую квантовую логику.

Квантовый компьютинг – отрасль знаний, занимающаяся теорией и практикой параллельного решения комбинаторных задач на вычислителях, использующих субатомные частицы при создании структур данных и их физического взаимодействия для реализации логических операций.

Квантовый эмулирующий компьютинг – структуры данных, модели, методы и алгоритмы для создания software приложений в целях параллельного решения комбинаторных задач на классических компьютерах путем использования дополнительной памяти.

Квантовый компьютинг – вычислительный процесс, использующий фотонные транзакции в атомарной структуре электронов для реализации параллельных алгоритмов и программных приложений. Квантовый компьютер без квантовых параллельных алгоритмов – всего лишь дорогая игрушка. Поэтому стратегия создания квантового компьютинга заключается в одновременной разработке квантовой аппаратуры и квантовых программных приложений на основе параллельных алгоритмов. Параллельное и раздельное развитие двух ветвей квантового компьютинга предоставляет в недалеком будущем возможность ученым из слаборазвитых стран активно участвовать в проектировании, моделировании и верификации квантовых алгоритмов и программных приложений на классических компьютерах в целях их последующей имплементации в рыночно доступные квантовые компьютеры.

Метрика квантового и классического компьютинга не имеет существенных структурных различий. Странно, но в научных публикациях отсутствует метрическое сравнение квантовой и классической логики. Естественно, существует аналогия между квантовыми операциями на кубитных структурах данных и теоретико-множественными операциями на символах алгебры Кантора. Изоморфизм двух структур: квантовой логики и алгебры множеств заключается в подобии носителей и сигнатур. Взаимнооднозначное соответствие носителей определяется отношениями между булеаном и кубитными структурами данных [1-3]:

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

Изоморфизм сигнатур определяется взаимнооднозначным соответствием между двумя операциями: объединение – суперпозиция, дополнение – перепутывание. Для операции пересечения соответствующий аналог в квантовой логике не определен. При этом унитарное кодирование символов алфавита Кантора дает возможность параллельно выполнять любые логические операции даже на классическом компьютере. Но дизрапторное инновационное решение заключается в отказе от операций суперпозиции и пере-

путывания в сторону создания memory-driven квантового компьютинга, использующего только операции записи-считывания на памяти, где двоичные состояния реализованы, например, в спиновых моментах электронов.

Моделирование на классических компьютерах параллельных квантовых алгоритмов дает существенный прирост производительности за счет использования избыточной памяти для унитарного кодирования кубитных структур данных. Более того, моделирование квантовых алгоритмов стратегически призвано решать проблему создания квантового интеллекта планеты путем разработки банка параллельных программных приложений для будущего парка рыночно доступных квантовых компьютеров.

Design and Test является самой передовой областью деятельности ученых и компаний, направленной на создание новых технологий компьютинга по метрике: быстродействие, энергосбережение, компактность и надежность. Параметр time-to-market при создании компьютинговой продукции, наряду с качеством, является доминирующим. Поэтому квантовые параллельные методы и алгоритмы проектирования, тестирования, верификации, моделирования и диагностирования цифровых изделий на кубитных структурах данных являются актуальными при их имплементации в современные классические и в будущие квантовые компьютеры, в целях существенного уменьшения time-to-market. Особый интерес представляет использование кубитных покрытий примитивных функциональностей для минимизации, синтеза, анализа и диагностирования цифровых систем на кристаллах. Рассматриваются логические (xor, notxor) Х-функции, задаваемые симметричными кубитными покрытиями, для технологичного параллельного решения задач синтеза тестов и дедуктивного моделирования неисправностей. Синтез дедуктивных формул для Х-функций формирует компактную структуру для транспортирования входных списков неисправностей, которая инвариантна ко входным тестовым наборам. Это делает Х-функцию привлекательной для ее использования при проектировании тестопригодных цифровых систем. Уникальность Х-функций проявляется также в технологической простоте процедуры взятия булевых производных на основе встречного сдвига двоичных разрядов, что является основой для генератора тестов, использующего кубитные покрытия логических схем.

Цель исследования – анализ тестопригодных свойств логических Х-функций от n переменных, а также их синтез путем разработки рекурсивных моделей и формул, использующих симметрию свойств их кубитных покрытий.

Задачи: 1) Формирование модели замечательных свойств Х-функций, используемых для их синтеза и анализа. 2) Создание архитектуры секвенсора для синтеза Q-покрытий Х-функций от конечного числа переменных. 3) Разработка метода синтеза дедуктивных ДНФ для моделирования неисправностей на основе анализа таблиц истинности. 4) Разработка метода параллельного синтеза дедуктивных кубитных покрытий и дедуктивных ДНФ для моделирования неисправностей на основе анализа кубитных векторов описания функциональностей. 5) Разработка метода параллельного синтеза матриц кубитных покрытий дедуктивного анализа на основе свойств симметрии эвристически разработанных матриц перестановки битов. 6) Разработка метода синтеза тестов для логических Х-функций путем перестановки битов в кубитных покрытиях.

1. Свойства логических Х-функций

Практически полезными для синтеза и анализа цифровых схем могут быть следующие 12 свойств Х-функций, интегрированные в модель отношений, представленную на рис. 1.

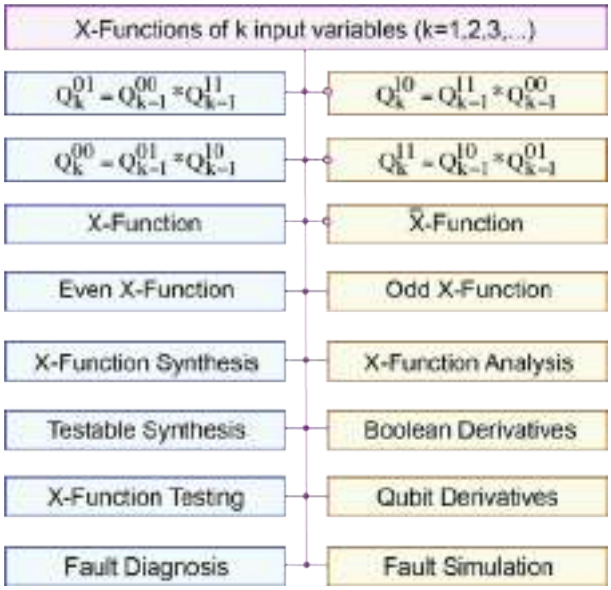


Рис. 1. Структурная модель взаимодействия Х-функций

1) Кубитное покрытие Х-функции имеет равное количество нулевых и единичных координат.

2) Количество Х-функций от n булевых переменных всегда равно двум:

$$Q^{2x}(n) = Q^{x}(n) \vee \bar{Q}^{x}(n).$$

Состояния координат кубитных покрытий обеих Х-функций от n переменных являются взаимноинверсными.

3) Х-функции от одной логической булевой переменной представлены повторителем и инвертором:

$$Y = X;\ Y = \bar{X}.$$

4) X-функции от двух булевых переменных представлены известными логическими примитивами xor, not-xor:

$$Y = X_1\bar{X}_2 \vee \bar{X}_1X_2;\ Y = X_1X_2 \vee \bar{X}_1\bar{X}_2.$$

5) Кубитная производная по любой переменной X-функции равна единичному вектору. Булева производная по любой переменной X-функции равна единице.

6) Для активизации входной переменной X-функции в целях изменения выхода не требуется никаких условий по состоянию других переменных.

7) Пара входных наборов, имеющая инверсные сигналы по всем координатам, всегда изменяет состояние выхода X-функции от нечетного числа переменных. Изменение состояния входа X-функции всегда приводит к изменению состояния выхода.

8) Синтез двух X-функций от n переменных реализуется путем конкатенации (*) кубитных векторов X-функций от n-1 переменной:

$$Q^{2x}(n) = Q^{x}(n-1) * \bar{Q}^{x}(n-1) \vee \bar{Q}^{x}(n-1) * Q^{x}(n-1).$$

Структура секвенсора, предназначенного для синтеза кубитных покрытий X-функций от n=1,2,3,4 переменных посредством конкатенации и инверсии, обозначенной кружочком, представлена на рис. 2.

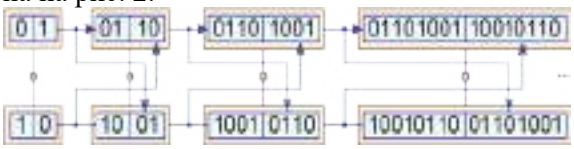


Рис. 2. Секвенсор синтеза Q-покрытия для X-функции

Другая интерпретация X-функций связана с их идентификацией по первому и последнему биту кубитного покрытия: 01–10, 00–11. Тогда синтез кубитных векторов X-функций от k переменных можно реализовать путем применения операции конкатенации к двум Q-покрытиям X-функций от k-1 переменных:

$$Q_k^{01} = Q_{k-1}^{00} * Q_{k-1}^{11};$$
$$Q_k^{10} = Q_{k-1}^{11} * Q_{k-1}^{00};$$
$$Q_k^{00} = Q_{k-1}^{01} * Q_{k-1}^{10};$$
$$Q_k^{11} = Q_{k-1}^{10} * Q_{k-1}^{01}.$$

Естественно, что между двумя кубитными покрытиями X-функций от k переменных существует взаимно-однозначное отношение инверсии:

$$Q_k^{01} = \bar{Q}_k^{10};$$
$$Q_k^{10} = \bar{Q}_k^{01};$$
$$Q_k^{00} = \bar{Q}_k^{11};$$
$$Q_k^{11} = \bar{Q}_k^{00}.$$

Это означает, что если известна одна X-функция от k переменных, то легко можно получить вторую функцию, как двоичное дополнение к первой.

9) Любой входной набор для X-функции проверяет 50% неисправностей по внешним входам, которые являются инверсными по отношению к состояниям исправного поведения упомянутых линий. Два взаимно-инверсных тестовых набора проверяют все одиночные константные неисправности входных переменных и выхода в X-функции от нечетного числа переменных.

10) Дедуктивная формула X-функции транспортирует на выход симметрическую разность входных списков неисправностей. Это означает объединение входных списков проверяемых дефектов, за исключением случая, когда списки неисправностей на всех входах идентичны. X-функция от n переменных, которая отождествляется с xor-примитивом, является единственной, где логическая и дедуктивная функции равны между собой на любом входном двоичном наборе.

11) Тестом для одиночных константных неисправностей всех линий логической X-функции от n переменных является ее СДНФ, дополненная любым термом обратной СДНФ данной функции:

$$T = T^1 \vee T_i^0.$$

Размерность полного проверяющего теста для X-функции всегда равна

$$Q = 1 + \frac{1}{2} \times 2^{2^n}.$$

12) Покоординатная xor-сумма всех кодов X-функции, соответствующих СДНФ (обратной СДНФ), равна нулевому (по всем координатам) вектору.

Таким образом, логические X-функции, обладающие уникальными свойствами тестирования, могут быть использованы для синтеза тестопригодных и самовосстанавливаемых логических цифровых устройств, а также для транспортирования дефектов от внешних входов до выходов булевой структуры.

2. Метод синтеза дедуктивного кубитного покрытия и ДНФ по таблице истинности

Метод синтеза дедуктивной формулы по аналитической форме функциональности [5-7], представленной в виде ДНФ, является достаточно сложной и нерегулярной вычислительной процедурой, которая нуждается в упрощении. Далее предлагается простая и тривиальная формула-процедура получения для входной последовательности (T) дедуктивной таблицы (L), а по ней и записи дедуктивной формулы для функциональности от n переменных, заданной таблицей

истинности (C) или кубическим покрытием функциональности (рис. 3):

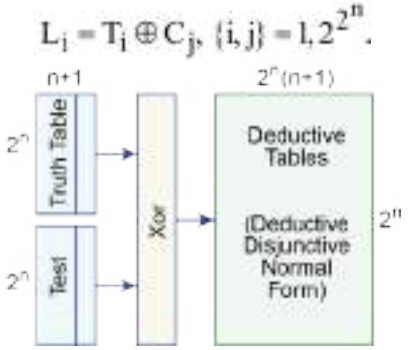


Рис. 3. Секвенсор синтеза дедуктивных таблиц для теста

Для понимания процедуры синтеза дедуктивной таблицы ниже предлагаются логические примитивы и результаты, которые можно использовать для записи дедуктивных выражений в форме ДНФ по единичным значениям выходов логических элементов (and, or, xor, not-xor, not, rep):

C			$T_0=000$	$T_1=010$	$T_2=100$	$T_3=111$
X_1	X_2	Y_{and}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	010	100	111
0	1	0	010	000	110	101
1	0	0	100	110	000	011
1	1	1	111	101	011	000

C			$T_0=000$	$T_1=011$	$T_2=101$	$T_3=111$
X_1	X_2	Y_{or}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	011	101	111
0	1	1	011	000	110	100
1	0	1	101	110	000	010
1	1	1	111	100	010	000

C			$T_0=000$	$T_1=011$	$T_2=101$	$T_3=110$
X_1	X_2	Y_{xor}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	011	101	110
0	1	1	011	000	110	101
1	0	1	101	110	000	011
1	1	0	110	101	011	000

C			$T_0=001$	$T_1=010$	$T_2=100$	$T_3=111$
X_1	X_2	Y_{nxr}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	1	000	011	101	110
0	1	0	011	000	110	101
1	0	0	101	110	000	011
1	1	1	110	101	011	000

C		$T_0=01$	$T_1=10$
X_1	Y_{not}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$
0	1	00	11
1	0	11	00

C		$T_0=00$	$T_1=11$
X_1	Y_{rep}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$
0	0	00	11
1	1	11	00

Представленные таблицы истинности не являются упорядоченными по возрастанию двоично-десятичных кодов входных наборов. Поскольку таблица истинности представляет собой множество отношений, то такого упорядочения не требуется, чтобы записать аналитическую форму полученной функциональности. Для каждой функции и каждого входного набора ниже записаны дедуктивные функции примитивных элементов (and, or, xor, not-xor, not, rep) в форме СДНФ, которые можно использовать как для аппаратного синтеза логических схем моделирования неисправностей, так и для создания облачного программного сервиса, выполняющего дедуктивный анализ цифровых проектов:

$$L_{and}(000) = X_1X_2;$$
$$L_{and}(010) = X_1\bar{X}_2;$$
$$L_{and}(100) = \bar{X}_1X_2;$$
$$L_{and}(111) = \bar{X}_1X_2 \vee X_1\bar{X}_2 \vee X_1X_2 = X_1 \vee X_2;$$
$$L_{or}(000) = \bar{X}_1X_2 \vee X_1\bar{X}_2 \vee X_1X_2 = X_1 \vee X_2;$$
$$L_{or}(011) = \bar{X}_1X_2;$$
$$L_{or}(101) = X_1\bar{X}_2;$$
$$L_{or}(111) = X_1X_2.$$
$$L_{xor}(000) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{xor}(011) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{xor}(101) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{xor}(110) = \bar{X}_1X_2 \vee X_1\bar{X}_2.$$
$$L_{nxr}(001) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{nxr}(010) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{nxr}(100) = \bar{X}_1X_2 \vee X_1\bar{X}_2;$$
$$L_{nxr}(111) = \bar{X}_1X_2 \vee X_1\bar{X}_2.$$
$$L_{not}(01) = X_1;$$
$$L_{not}(10) = X_1.$$
$$L_{rep}(00) = X_1;$$
$$L_{rep}(11) = X_1.$$

Здесь взаимодействие логических переменных определяет пересечение, вычитание или объединение списков, или векторов неисправностей

$$(X_1X_2,\ X_1\bar{X}_2,\ X_1 \vee X_2)$$

соответственно, принадлежащих внешним входам примитивов.

Таким образом, представленный метод для синтеза дедуктивных покрытий и ДНФ, ориентированных на дедуктивный анализ цифровых систем, значительно отличается от существующих аналогов быстродействием Q, которое определяется параллелизмом выполнения регистровых операций между очередным входным воздействием и n кубами покрытия: $Q = 2^{2^n}$.

3. Метод синтеза дедуктивного кубитного покрытия и ДНФ по кубитным покрытиям функциональностей

Еще более высокое быстродействие вычислительных процедур для синтеза дедуктивных функций можно получить, если использовать вместо кубических покрытий (таблиц) кубитные векторы. Для этого необходимо упорядочить полученные ранее кубические формы дедуктивных функций в соответствии с возрастанием двоично-десятичных кодов входных наборов:

C			$T_0=000$	$T_1=010$	$T_2=100$	$T_3=111$
X_1	X_2	Y_{and}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	000	000	000
0	1	0	010	010	011	011
1	0	0	100	101	100	101
1	1	1	111	110	110	111

C			$T_0=000$	$T_1=011$	$T_2=101$	$T_3=111$
X_1	X_2	Y_{or}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	000	000	000
0	1	1	011	011	010	010
1	0	1	101	100	101	100
1	1	1	111	110	110	111

C			$T_0=000$	$T_1=011$	$T_2=101$	$T_3=110$
X_1	X_2	Y_{xor}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	0	000	000	000	000
0	1	1	011	011	011	011
1	0	1	101	101	101	101
1	1	0	110	110	110	110

C			$T_0=001$	$T_1=010$	$T_2=100$	$T_3=111$
X_1	X_2	Y_{nxr}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$	$L_2=T_2\oplus C$	$L_3=T_3\oplus C$
0	0	1	000	000	000	000
0	1	0	011	011	011	011
1	0	0	101	101	101	101
1	1	1	110	110	110	110

C		$T_0=01$	$T_1=10$
X_1	Y_{not}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$
0	1	00	00
1	0	11	11

C		$T_0=00$	$T_1=11$
X_1	Y_{rep}	$L_0=T_0\oplus C$	$L_1=T_1\oplus C$
0	0	00	00
1	1	11	11

Вместо упорядоченных по возрастанию двоично-десятичных кодов входных наборов таблиц истинности можно записывать кубитные покрытия, которые представляют собой дедуктивную матрицу размерностью m**2:

and	$Q_1=0$	$Q_2=0$	$Q_3=0$	$Q_4=1$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$	$L_3=Q_3\oplus Q$	$L_4=Q_4\oplus Q$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
1	1	0	0	1

or	$Q_1=0$	$Q_2=1$	$Q_3=1$	$Q_4=1$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$	$L_3=Q_3\oplus Q$	$L_4=Q_4\oplus Q$
0	0	0	0	0
1	1	1	0	0
1	1	0	1	0
1	1	0	0	1

xor	$Q_1=0$	$Q_2=1$	$Q_3=1$	$Q_4=0$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$	$L_3=Q_3\oplus Q$	$L_4=Q_4\oplus Q$
0	0	0	0	0
1	1	1	1	1
1	1	1	1	1
0	0	0	0	0

nxr	$Q_1=1$	$Q_2=0$	$Q_3=0$	$Q_4=1$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$	$L_3=Q_3\oplus Q$	$L_4=Q_4\oplus Q$
1	1	1	1	1
0	0	0	0	0
0	0	0	0	0
1	1	1	1	1

not	$Q_1=1$	$Q_2=0$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$
1	0	0
0	1	1

rep	$Q_1=0$	$Q_2=1$
Q	$L_1=Q_1\oplus Q$	$L_2=Q_2\oplus Q$
0	0	0
1	1	1

Далее предлагается более простой путь получения матрицы кубитных дедуктивных векторов без использования таблиц истинности на основе только кубитного покрытия функциональности.

Метод синтеза дедуктивной матрицы для анализа неисправностей на основе Q-покрытия функциональности содержит две операции (рис. 4):

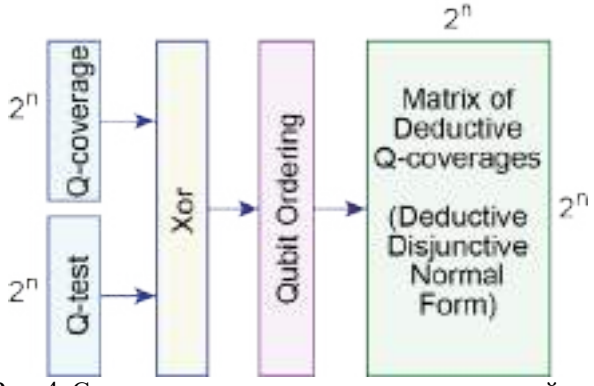


Рис. 4. Секвенсор синтеза дедуктивных покрытий для Q-теста

1) Синтез матрицы кубитных покрытий дедуктивных функций, зависящей от двоично-десятичного номера входного набора и координат Q-вектора функциональности от n переменных:

$$L^{*}_{ij}=(Q_i \overset{m}{\underset{i=1}{\oplus}} Q_j)^{m}_{j=1},\ m=2^{2^n}.$$

Фактически берется первая координата кубитного покрытия, которая xor-складывается со всеми координатами Q-вектора для формирования де-

дуктивного вектора на первой входной последовательности. Затем берется вторая координата Q-вектора, которая также xor-складывается со всеми координатами. Процедура заканчивается после того, как все координаты Q-вектора были xor-сложены с кубитным вектором. Вычислительная сложность данной процедуры равна m**2, которая может быть уменьшена до m путем аппаратной параллельной реализации xor-операции.

2) После получения дедуктивной матрицы на всех входных наборах по кубитному покрытию функциональности необходимо выполнить процедуру перестановки битов в столбцах по правилу

$$L_{ij} = [L^{*}(H_{ij})]_{i,j=1}^{m}$$

в соответствии с номерами, представленными в матрице перестановки, которая по размерности равна матрице кубитных покрытий дедуктивных функций. Далее представлены примеры получения дедуктивных функций на основе использования только кубитных покрытий функциональностей:

Q_{and}	L_1	L_2	L_3	L_4
0	0	0	0	1
0	0	0	0	1
0	0	0	0	1
1	1	1	1	0

→

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

→

X_1X_2	L_1	L_2	L_3	L_4
00	0	0	0	0
01	0	0	1	1
10	0	1	0	1
11	1	0	0	1

→

$$L = (00)(X_1X_2) \vee (01)(X_1\bar{X}_2) \vee (10)(\bar{X}_1X_2) \vee (11)(X_1 \vee X_2).$$

Q_{or}	L_1	L_2	L_3	L_4
0	0	1	1	1
1	1	0	0	0
1	1	0	0	0
1	1	0	0	0

→

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

→

X_1X_2	L_1	L_2	L_3	L_4
00	0	0	0	0
01	1	1	0	0
10	1	0	1	0
11	1	0	0	1

→

$$L = (00)(X_1 \vee X_2) \vee (01)(\bar{X}_1X_2) \vee (10)(X_1\bar{X}_2) \vee (11)(X_1X_2).$$

Q_{xor}	L_1	L_2	L_3	L_4
0	0	1	1	0
1	1	0	0	1
1	1	0	0	1
0	0	1	1	0

→

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

→

X_1X_2	L_1	L_2	L_3	L_4
00	0	0	0	0
01	1	1	1	1
10	1	1	1	1
11	0	0	0	0

→

$$L = (00 \vee 01 \vee 10 \vee 11)(\bar{X}_1X_2 \vee X_1\bar{X}_2) = (xx)(\bar{X}_1X_2 \vee X_1\bar{X}_2).$$

Q_{nxt}	L_1	L_2	L_3	L_4
1	0	1	1	0
0	1	0	0	1
0	1	0	0	1
1	0	1	1	0

→

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

→

X_1X_2	L_1	L_2	L_3	L_4
00	0	0	0	0
01	1	1	1	1
10	1	1	1	1
11	0	0	0	0

→

$$L = (00 \vee 01 \vee 10 \vee 11)(\bar{X}_1X_2 \vee X_1\bar{X}_2) = (xx)(\bar{X}_1X_2 \vee X_1\bar{X}_2).$$

Q_{not}	L_1	L_2
1	0	1
0	1	0

→

1	2
2	1

→

X	L_1	L_2
0	0	0
1	1	1

→

$$L = (0 \vee 1)(X \vee X) = (xx)(X).$$

Q_{rep}	L_1	L_2
0	0	1
1	1	0

→

1	2
2	1

→

X	L_1	L_2
0	0	0
1	1	1

→

$$L = (0 \vee 1)(X \vee X) = (xx)(X).$$

4. Метод синтеза матрицы перестановки битов для формирования дедуктивных функций

В общем случае метод синтеза матрицы перестановки битов в столбцах для формирования дедуктивных функций от n переменных может быть представлен в следующем виде:

$$H_{ij}(n = 1,2,3) = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Каждая матрица обладает симметрией относительно диагоналей, которые представлены минимальными и максимальными числами. Существует также вертикальная и горизонтальная симметрия, где симметричные пары чисел находятся в отношении $H + \bar{H} = 2^n + 1$. Если нумеровать координаты столбцов матрицы начиная с нуля, то предыдущее отношение будет иметь вид $H + \bar{H} = 2^n$. Квадратичная по размеру матрица чисел в своем синтезе имеет следующие закономерности: первый столбец является вектором упорядоченных по возрастанию чисел; второй столбец представляет собой перестановку двух соседних чисел в каждой паре относительно предыдущего столбца; третий создает перестановку соседних пар чисел; четвертый столбец определяется перестановкой соседних тетрад чисел, идущих в обратном порядке. Остальные столбцы для функции от 3-х переменных генерируются как зеркальные отображения синтеза четырех предыдущих столбцов, начиная с последнего столбца, который представляет собой первый столбец, занумерованный в обратном порядке.

Синтез матрицы перестановки битов основан на всех видах симметрии (вертикальная, горизонтальная, диагональная), которая дает возможность, имея один известный квадрант, получить все остальные путем применения формулы:

$$H + \bar{H} = 2^n + 1 \rightarrow \bar{H} = (2^n + 1) - H.$$

Следующая структура матриц объясняет тривиальность построения сколь угодно сложной матрицы перестановки битов от n=1,2,3, … переменных:

$$\begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \\ \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \\ \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \\ \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \\ \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} & \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix} \end{bmatrix}$$

Фактически, зная любой квадрант от n-1 переменной, за 4 автоматных такта можно получить матрицу перестановки битов для дедуктивной функциональности от n переменных:

$$H^1 \in H^2 \in H^3 \in \ldots \in H^n.$$

Масштабируемость квадрантов можно продемонстрировать следующей структурой, которая инварианта к количеству переменных анализируемой логической функциональности:

$$\begin{bmatrix} H^1 \\ H\ \bar{H} \\ \bar{H}\ H \end{bmatrix} = H \in H^2 \rightarrow \begin{bmatrix} H^2 \\ H\ \bar{H} \\ \bar{H}\ H \end{bmatrix} = H \in H^3 \rightarrow \begin{bmatrix} H^3 \\ H\ \bar{H} \\ \bar{H}\ H \end{bmatrix} \ldots = H \in H^n \rightarrow \begin{bmatrix} H^n \\ H\ \bar{H} \\ \bar{H}\ H \end{bmatrix}.$$

Примером рекурсивной генерации матриц перестановки битов для переменных n=1,2,3 может служить следующая структура:

$$H_{ij}(n=1,2,3) = \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} & \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} \\ \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} & \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} & \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} & \begin{bmatrix} 5\ 6 \\ 6\ 5 \end{bmatrix} & \begin{bmatrix} 7\ 8 \\ 8\ 7 \end{bmatrix} \\ \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} & \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} & \begin{bmatrix} 7\ 8 \\ 8\ 7 \end{bmatrix} & \begin{bmatrix} 5\ 6 \\ 6\ 5 \end{bmatrix} \\ \begin{bmatrix} 5\ 6 \\ 6\ 5 \end{bmatrix} & \begin{bmatrix} 7\ 8 \\ 8\ 7 \end{bmatrix} & \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} & \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} \\ \begin{bmatrix} 7\ 8 \\ 8\ 7 \end{bmatrix} & \begin{bmatrix} 5\ 6 \\ 6\ 5 \end{bmatrix} & \begin{bmatrix} 3\ 4 \\ 4\ 3 \end{bmatrix} & \begin{bmatrix} 1\ 2 \\ 2\ 1 \end{bmatrix} \end{bmatrix}$$

Рекурсивное взаимодействие матриц перестановки битов показывает: для получения сколь угодно сложной матрицы от n переменных необходимо знать только один элемент (в данном случае единицу) в матрице для функции от одной переменной.

Если первым элементом нумерации входных двоично-десятичных кодов (начальный адрес) принять ноль, то взаимодействие матриц перестановки битов будет иметь следующий вид:

$$H_{ij}(n=1,2,3) = \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} & \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} \\ \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} & \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} \end{bmatrix} \rightarrow \begin{bmatrix} \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} & \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} & \begin{bmatrix} 4\ 5 \\ 5\ 4 \end{bmatrix} & \begin{bmatrix} 6\ 7 \\ 7\ 6 \end{bmatrix} \\ \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} & \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} & \begin{bmatrix} 6\ 7 \\ 7\ 6 \end{bmatrix} & \begin{bmatrix} 4\ 5 \\ 5\ 4 \end{bmatrix} \\ \begin{bmatrix} 4\ 5 \\ 5\ 4 \end{bmatrix} & \begin{bmatrix} 6\ 7 \\ 7\ 6 \end{bmatrix} & \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} & \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} \\ \begin{bmatrix} 6\ 7 \\ 7\ 6 \end{bmatrix} & \begin{bmatrix} 4\ 5 \\ 5\ 4 \end{bmatrix} & \begin{bmatrix} 2\ 3 \\ 3\ 2 \end{bmatrix} & \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix} \end{bmatrix}$$

Из приведенной структуры, иллюстрирующей синтез матриц перестановки битов для получения кубитных покрытий дедуктивного анализа, вытекают следующие полезные свойства, характеризующие метод:

1) Матрица любого уровня иерархии содержит 4 квадранта, которые диагонально равны друг другу (рис. 5):

$$H = \begin{bmatrix} H_1 & H_2 \\ H_3 & H_4 \end{bmatrix} = \begin{bmatrix} H & \bar{H} \\ \bar{H} & H \end{bmatrix}, \quad H_1 = H_4; \quad H_1 = \bar{H}_2; \quad H_2 = H_3; \quad H_3 = \bar{H}_4.$$

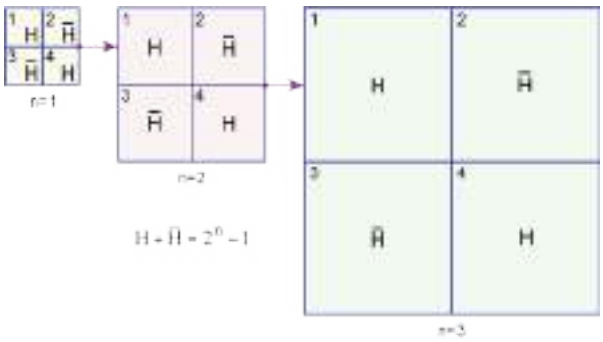


Рис. 5. Структурная иерархия матриц для получения кубитных покрытий

2) Горизонтальные и вертикальные отношения между квадрантами определяются дополнениями (при нулевом начальном элементе или адресе):

$$H_1 + \bar{H}_2 = 2^n - 1 \rightarrow \bar{H}_2 = (2^n - 1) - H_1;$$
$$\bar{H}_3 + H_4 = 2^n - 1 \rightarrow \bar{H}_3 = (2^n - 1) - H_4;$$
$$H_1 + \bar{H}_3 = 2^n - 1 \rightarrow \bar{H}_3 = (2^n - 1) - H_1;$$
$$\bar{H}_2 + H_4 = 2^n - 1 \rightarrow \bar{H}_2 = (2^n - 1) - H_4.$$

Сумма двух чисел, симметричных относительно горизонтальной или вертикальной оси, делящей матрицу от n переменных на две одинаковые части, равна $h + \bar{h} = 2^n - 1$. Четверку компонентов примитивной матрицы, не содержащей других матриц в качестве составных частей, всегда формируют два соседних числа или цифры.

3) Рекурсивная формула получения матрицы перестановки битов для синтеза дедуктивной функции от i=1,2,3,… переменных имеет следующий вид:

$$H^i = \begin{bmatrix} H^i & \bar{H}^i \\ \bar{H}^i & H^i \end{bmatrix}, \quad H^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix};$$
$$H_1^i = \begin{bmatrix} H^{i-1} & \bar{H}^{i-1} \\ \bar{H}^{i-1} & H^{i-1} \end{bmatrix};$$
$$H_4^i = H_1^i = \begin{bmatrix} H^{i-1} & \bar{H}^{i-1} \\ \bar{H}^{i-1} & H^{i-1} \end{bmatrix};$$
$$H_2^i = \bar{H}_1^i = (2^n - 1) - \begin{bmatrix} H^{i-1} & \bar{H}^{i-1} \\ \bar{H}^{i-1} & H^{i-1} \end{bmatrix};$$
$$H_3^i = \bar{H}_2^i = (2^n - 1) - \begin{bmatrix} H^{i-1} & \bar{H}^{i-1} \\ \bar{H}^{i-1} & H^{i-1} \end{bmatrix}.$$

На каждом шаге рекурсии формируются всегда четыре компонента, где два из них, расположенных по диагонали, переносятся из матрицы предыдущего шага, а два других генерируются путем дополнения каждого нового элемента в квадранте к соответствующим, относительно вертикальной или горизонтальной оси симметрии, битам перенесенных диагональных компонентов:

$$\bar{H}^i = (2^n - 1) - H^i.$$

Следует напомнить, что синтезированные столбцы матрицы используются для окончательного формирования кубитного покрытия дедуктивной функции путем перестановки битов, полученного для транспортирования входных векторов (списков) неисправностей на внешний выход функциональности при заданном входном тестовом наборе.

Таким образом, предложенный метод синтеза дедуктивных кубитных покрытий для моделирования неисправностей отличается от известных в мире аналогов оригинальностью математических решений, высоким уровнем параллелизма и компактностью структур данных, что дает возможность использовать его программную (аппаратную) реализацию для синтеза, анализа, тестирования, верификации и диагностирования цифровых систем на кристаллах. Высокое быстродействие синтеза дедуктивных кубитных покрытий на заданном входном наборе, определяемое битовыми операциями $Q=2x2^n=2^{n+1}$, является основанием для его использования в целях тестирования. моделирования и диагностирования цифровых систем в режиме online. Регистровая реализация фактически двух операций: xor-сравнения и перестановки битов позволит свести упомянутую оценку к двум (нескольким) автоматным тактам. Кроме того, две упомянутые операции можно объединить в одну процедуру, исполняемую в автоматном такте.

5. Синтез тестов для логических Х-функций

Сущность или уникальная особенность теста для любой Х-функции заключается в его непостроении, поскольку существуют две Т-аксиомы, объясняющие отсутствие синтеза: 1) Логическая Х-функция, записанная в виде единичных термов СДНФ

$$T_i \in T,\ f(T_i)=1,$$

представляет собой тестовые наборы для проверки одиночных константных 0-неисправностей входных, внутренних переменных и выхода:

$$T^1(\equiv 0)=\bigvee_{\forall i[f(T_i)=1]} T_i,$$

$$T=\{T_0, T_1, ..., T_i, ..., T_k\},$$

$$k=2^{2^n}-1;\ f(T_i)=\{0,1\}.$$

2) Тест в форме СДНФ логической Х-функции всегда дополняется единственной входной последовательностью – любым термом обратной СДНФ:

$$T_i \in T^0,\ f(T_i)=0,$$

который проверяет все константные 1-неисправности внутренних линий и выхода:

$$T^0(=1)=T_i \leftarrow \forall i: f(T_i)=0.$$

В частности, дополнение к 1-тесту Х-функции (Q=01101001) определяется нулевым тестовым набором (000) по всем входным координатам; дополнение к 1-тесту для Х-функции (Q=10010110) задается первым тестовым набором (001), содержащим в последнем разряде единицу на фоне всех остальных нулей. На самом деле дополнением к 1-тесту является любая входная последовательность, которая отсутствует в 1-тесте. Поэтому полным проверяющим тестом для Х-функции всегда является тест размерностью

$$Q=1+\frac{1}{2}\times 2^{2^n}.$$

Следовательно, тестом для логической Х-функции от n переменных является ее СДНФ, дополненная любым термом обратной СДНФ данной функции:

$$T=T^1\vee T_i^0,$$

$$T^1=\forall T_i: f(T_i)=1$$

$$T_i^0 \in T^0=\forall T_i: f(T_i)=0;$$

$$T(01101001)=(001\vee 010\vee 100\vee 111)\vee 000;$$

$$T(10010110)=(000\vee 011\vee 101\vee 110)\vee 001.$$

Другое уникальное свойство Х-функции определяется как покоординатная xor-сумма всех кодов, соответствующих СДНФ (обратной СДНФ), равна нулевому (по всем двоичным разрядам) вектору:

$$\bigoplus_{i=1}^{n_1} C(T_i^1)=0;$$

$$\bigoplus_{i=1}^{n_0} C(T_i^0)=0;$$

$$n_0+n_1=2^{2^n}.$$

Иллюстрация факта конволюции пространства СДНФ или обратной СДНФ в нуль-вектор представлена двумя Х-функциями от трех переменных:

$$Y(01101001)=\bar{X}_1\bar{X}_2X_3\vee\bar{X}_1X_2\bar{X}_3\vee X_1\bar{X}_2\bar{X}_3\vee X_1X_2X_3\rightarrow$$
$$\rightarrow 001\oplus 010\oplus 100\oplus 111=000;$$

$$Y(10010110)=\bar{X}_1\bar{X}_2\bar{X}_3\vee\bar{X}_1X_2X_3\vee X_1\bar{X}_2X_3\vee X_1X_2\bar{X}_3\rightarrow$$
$$\rightarrow 000\oplus 011\oplus 101\oplus 110=000.$$

Свойство конволюции дает возможность вычислять неизвестные термы теста или СДНФ на основе известных компонентов путем применения, например, следующего равенства для Х-функции от трех переменных:

$$T_1\oplus T_2\oplus T_3\oplus T_4=0;$$
$$001\oplus 010\oplus 100\oplus 111=0(000).$$
$$T_2\oplus T_3\oplus T_4=T_1;$$
$$010\oplus 100\oplus 111=001.$$

Для логических Х-функций от двух переменных (рис. 6), которые известны как xor, not-xor примитивы, ниже представлено моделирование исправного поведения всех входных наборов (таблица Т), анализ неисправностей (таблица D) и кубитная форма четырех вариантов минимальных тестов – таблица T(Q):

T(xor)	1	2	3	4	5
0	0	0	0	0	0
1	0	1	0	1	1
2	1	0	1	0	1
3	1	1	0	0	0

→

D	1	2	3	4	5
0	1	1	1	1	1
1	1	0	.	0	0
2	0	1	0	.	0
3	0	0	1	1	1

→

T(Q)	1	2	3	4
0	0	1	1	1
1	1	0	1	1
2	1	1	0	1
3	1	1	1	0

T(nxr)	1	2	3	4	5
0	0	0	1	0	1
1	0	1	0	0	0
2	1	0	0	0	0
3	1	1	0	1	1

→

D	1	2	3	4	5
0	1	1	0	.	1
1	1	0	1	1	0
2	0	1	1	1	0
3	0	0	.	0	1

→

T(Q)	1	2	3	4
0	0	1	1	1
1	1	0	1	1
2	1	1	0	1
3	1	1	1	0

Для обеих функций здесь получены минимальные тесты, состоящие из трех входных наборов. Это связано с тем, что противоположные входные векторы имеют одинаковые состояния выходной переменной.

Тест, использующий Т-аксиомы для записи входных последовательностей, проверяющих все одиночные константные неисправности цифровых схем (xor, nxr), имеет следующий вид:

$$T(xor, nxr) = T^1 \vee T_i^0,$$
$$T(Q = 0110)(xor) = (01 \vee 10) \vee 00;$$
$$T(Q = 1001)(nxr) = (00 \vee 11) \vee 01.$$

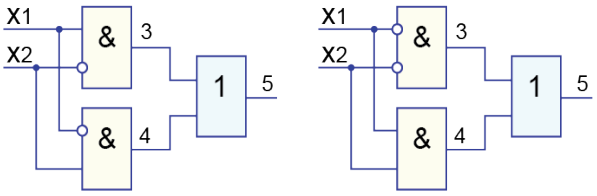


Рис. 6. Х-функции от двух переменных

Для двух логических Х-функций от одной переменной (рис. 7)

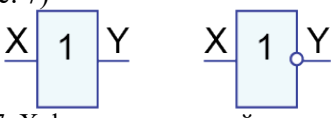


Рис. 7. Х-функции от одной переменной

ниже представлено моделирование исправного поведения всех входных наборов (таблица Т), анализ неисправностей (таблица D) и кубитная форма минимальных тестов – таблица T(Q), рассматриваются функциональные элементы (повторитель – rep, инвертор – not):

T(rep)	X	Y
0	0	0
1	1	1

→

D	X	Y
0	1	1
1	0	0

→

T(Q)
1
1

T(not)	X	Y
0	0	1
1	1	0

→

D	X	Y
0	1	0
1	0	1

→

T(Q)
1
1

Тест, использующий Т-аксиомы для записи входных последовательностей, проверяющих все одиночные константные неисправности цифровых примитивов (rep, not), имеет следующий вид:

$$T(rep, not) = T^1 \vee T_i^0,$$
$$T(Q = 01)(rep) = 1 \vee 0;$$
$$T(Q = 10)(not) = 0 \vee 1.$$

Таким образом, применение двух упомянутых выше Т-аксиом дает возможность записывать без вычислений полный проверяющий тест для одиночных константных неисправностей входных, внутренних и выходных линий любой сколь угодно сложной логической Х-функции.

Выводы

1) Разработана структурная модель взаимодействия Х-функций и производных компонентов, ориентированных на синтез и анализ цифровых систем в целях получения тестопригодных решений, связанных с уменьшением времени проектирования и тестирования вычислительных устройств.

2) Впервые введено понятие простых Х-функций от конечного числа переменных, которые характеризуются отсутствием минимизации и наличием свойств тестопригодности, что дает возможность синтезировать цифровые устройства, технологичные для решения задач тестирования, моделирования и диагностирования.

3) Сформулированы метрические свойства Х-функций от конечного числа переменных, которые дают возможность использовать их в практике разработки тестопригодных цифровых устройств, генерирования проверяющих тестов и оценки их качества путем дедуктивного моделирования проверяемых константных неисправностей на кубитных структурах данных.

4) Предложено аналитическое выражение для синтеза кубитных покрытий Х-функций от конечного числа переменных, что дает возможность создавать тестопригодные логические схемы, не требующие экспоненциальных затрат на синтез и анализ тестов проверки и диагностирования неисправностей.

5) Получены дедуктивные формулы транспортирования входных списков неисправностей на внешние выходы для Х-функций от конечного числа переменных, которые характеризуются единичными векторами производных по всем переменным, что дает возможность построить секвенсор моделирования дефектов, инвариантный к входным тестовым наборам.

6) Предложен метод синтеза дедуктивных кубитных покрытий для моделирования неисправностей на основе использования Q-покрытий функциональностей, который отличается от известных в мире аналогов оригинальностью математических решений, высоким уровнем парал-

лелизма и компактностью структур данных, что дает возможность использовать его программную (аппаратную) реализацию для синтеза, анализа, тестирования, верификации и диагностирования цифровых систем на кристаллах.

7) Предложен метод синтеза тестов на основе кубитных покрытий Х-функций, который имеет линейную вычислительную сложность от числа переменных.

Дальнейшие исследования связаны с созданием технологий преобразования фрагментов логических схем к форме Х-функций, которые технологичны для решения задач тестирования и верификаци цифровых систем.

Литература:

1. *Hahanov V.* Cyber Physical Computing for IoT-driven Services. New York. Springer. 2018. 279 p.

2. *Hahanov V.I., Bani Amer T., Chumachenko S.V., Litvinova E.I.* Qubit technology for analysis and diagnosis of digital devices // Electronic modeling, J 2015. 37 (3). P. 17-40.

3. *Hahanov V., Gharibi W., Litvinova E., Liubarskyi M., Hahanova A.* Quantum memory-driven computing for test synthesis // IEEE East-West Design and Test Symposium, Novi Sad, Serbia. 2017. Pp. 123-128.

4. *Hahanov V.* Infrastructure intellectual property for SoC simulation and diagnosis service // Design of Digital Systems and Devices. Springer. 2011. P. 289-330.

5. *Abramovici M.* Digital System Testing and Testable Design, Comp. Sc. Press, 1998.

6. *Fujiwara H.* Fault Simulation // Logic Testing and Design for Testability. MIT Press, 1985. P.84-108.

7. *Pomeranz I., Reddy Sudhakar M.* Aliasing Computation Using Fault Simulation with Fault Dropping // IEEE Transactions on Computers, 1995. P. 139-144,

8. *Hahanov V., Barkalov A., Adamsky M.* Design of Digital Systems and Devices. Infrastructure intellectual property for SoC simulation and diagnosis service. 2011. Springer. P. 289-330.

Поступила в редколлегию 11.02.2018

Рецензент: д-р техн. наук, проф. Меликян В.

Любарский Михаил Михайлович, соискатель кафедры АПВТ ХНУРЭ. Научные интересы: проектирование и тестирование цифровых систем. Хобби: путешествия. Адрес: Украина, 61166, Харьков, пр. Науки, 14.

Абдуллаев Вугар Гаджимахмудович, канд. техн. наук, доцент кафедры «Компьютерная инженерия технологии и программирование» Азербайджанской Государственной Нефтяной Академии (АГНА), Институт Кибернетики НАНА. Научные интересы: информационные технологии, веб-программирования, мобильные приложении. Увлечение: электронная коммерция, B2B, B2C проекты, научные книги, спорт. Адрес: Азербайджан, AZ1129, Баку, ул. М. Гади, 53, кв. 81, тел. (99412)5712428, (050)3325483, e-mail: abdulvugar@mail.com

Хаханов Владимир Иванович, д-р техн. наук, профессор, главный научный сотрудник кафедры АПВТ ХНУРЭ. Научные интересы: проектирование и тестирование цифровых систем. Хобби: футбол, горные лыжи. Адрес: Украина, 61166, Харьков, пр. Науки, 14, e-mail: hahanov@icloud.com.

Чумаченко Светлана Викторовна, д-р техн. наук, профессор, зав. кафедрой АПВТ ХНУРЭ. Научные интересы: математическое моделирование вычислительных процессов, теория рядов, методы дискретной оптимизации, инновационные формы обучения. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. +380577021326, e-mail: svetlana.chumachenko@nure.ua

Литвинова Евгения Ивановна, д-р техн. наук, проф. кафедры АПВТ ХНУРЭ. Научные интересы: проектирование и тестирование цифровых систем. Хобби: музыка. Адрес: Украина, 61166, Харьков, пр. Науки, 14, тел. +380577021326, e-mail: litvinova_eugenia@icloud.com.

Хаханов Иван Владимирович, студент ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, программирование. Хоби: горные лыжи, английский язык. Адреса: Украина, 61166, Харьков, пр. Науки, 14, тел. +3805770-21-326,e-mail: ivanhahanov@icloud.com.

Lyubarsky Mikhail Mikhailovich, PhD student, Design Automation Department, NURE. Scientific interests: project-bathing and testing digital systems. Scientific interests: design and testing of digital systems. Hobbies: traveling. Address: Ukraine, 61166, Kharkov, Nauki Ave, 14.

Abdullaev Vugar Gadzhimakhmudovich, Cand. tech. Sci., Associate Professor of Computer Engineering and Technology Programming at the Azerbaijan State Oil Academy (ASAN), Institute of Cybernetics of ANAS. Scientific interests: information technology, web programming, mobile application. Hobbies. e-commerce, B2B, B2C projects, science books, sports. Address: Azerbaijan, AZ1129, Baku, M. Gadi, 53, apt. 81, tel. (99412) 5712428, (050) 3325483, e-mail: abdulvugar@mail.com

Hahanov Vladimir Ivanovich, Dr., Prof., Chief Scientific Officer, Design Automation Department, NURE. Scientific interests: design and testing of digital systems. Hobby: football, downhill skiing. Address: Ukraine, 61166, Kharkov, Science, 14, e-mail: hahanov@icloud.com.

Chumachenko Svetlana Victorovna, Dr., Prof., Head of Design Automation Department, NURE. Scientific interests: mathematical modeling of computational processes, theory of series, methods of discrete optimization, educational innovations. Address: Ukraine, 61166, Kharkov, Nauki Ave, 14, phone + 3805770-21-326, e-mail: svetlana.chumachenko@nure.ua

Litvinova Evgenia Ivanovna, Dr., Prof., Design Automation Department, NURE. Scientific interests: design and testing of digital systems. Hobbies: music. Address: Ukraine, 61166, Kharkov, Nauki Ave, 14, e-mail: litvinova_eugenia@icloud.com.

Hahanov Ivan Vladimirovich, student, Design Automation Department, NURE. Scientific interests: technical diagnostics of digital systems, programming. Hobby: mountain skiing, English. Address: Ukraine, 61166, Kharkov, Nauki Ave., 14, ph. + 3805770-21-326, e-mail: ivanhahanov@icloud.com.

КОМПЬЮТЕРНЫЕ НАУКИ

УДК 004.056.53

БАГАТОРІВНЕВИЙ ПІДХІД ДО ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ ДОДАТКІВ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

КУПЕРШТЕЙН Л.М., ВОЙТОВИЧ О.П., ОСТАПЕНКО-БОЖЕНОВА А.В., ПРОКОПЧУК С.А.

Аналізуються можливі загрози комерційним додаткам на мобільних пристроях з операційною системою Android, існуючі методи та засоби захисту додатків від несанкціонованого доступу. Розробляється багаторівнева модель захисту та програмний засіб для мобільних пристроїв під керуванням операційної системи Android, яка включає в себе модуль захисту коду, модуль віддаленого контролю, модуль захисту бази даних і модуль багатофакторної автентифікації.

Ключові слова: несанкціонований доступ та використання, ОС Android, загрози мобільному додатку, багаторівневий захист.

Key words: unauthorized access and use, Android OS, to mobile application threats, multilevel protection.

Вступ

З моменту виходу ОС Android на споживчий ринок в 2008 році увага до даної операційної системи збільшується. З кожним роком кількість додатків, що випускаються для цієї операційної системи, зростає в геометричній прогресії. Додатки використовуються для полегшення різних дій та завантажуються мільярдами людей по всьому світу [1]. За останній час додатки поширилися настільки, що практично кожен аспект людської діяльності тепер можна здійснити за допомогою програми, написаної для ОС Android [2].

Нові програми продовжують з'являтися, надаючи послуги, починаючи від новин, погоди та розваг, до таких серйозних компаній, як банківська справа, медична допомога, фінанси та навіть безпека у домі. Додатки для цих підприємств містять конфіденційну та особисту інформацію (наприклад, дані банківського рахунку, хвороби та ліки, інвестиційна таємниця тощо). Комерційні додатки, зазвичай, не мають належного захисту як коду додатку, так і даних, що зберігаються [1-3]. Тому актуальною задачею є вдосконалення захисту мобільних додатків.

Отже, метою дослідження є підвищення захищеності додатків в операційній системі Android від несанкціонованого використання як коду додатку, так і даних.

Постановка задачі

Викрадення даних, що зберігаються у додатках, завжди вважається однією з найбільш критичних загроз безпеці Android. Дослідження показують [4, 5], що це може статися навіть для додатків, які в принципі не мають вразливостей, але вразливості можуть бути у самій операційній системі, наприклад, спільне використання мережевих даних. Під час атаки шкідливий додаток може функціонувати у фоновому режимі і збирати дані цільового додатку.

Багато додатків використовують інформацію, що зберігається в базах даних. Крім того, додаток може взаємодіяти з базами даних іншого додатку, що надає такі функціональні можливості. Вразливий додаток може дозволити шкідливій програмі порушувати цілісність та конфіденційність даних, що зберігаються в базах даних [5, 6]. Така легкість в отриманні несанкціонованого доступу до вмісту файлів спровокувала появу великої кількості спеціальних інструментів, розрахованих на усунення проблеми доступу до коду додатків.

Крім того, важливою проблемою залишається можливість аналізу коду додатку за допомогою реверс - інженірингу. А саме, дослідження коду додатку, а також документації на нього з метою розуміння принципів його роботи, захисних механізмів, зберігання даних тощо для виконання несанціонованої зміни або копіювання, використання додатку чи іншого об'єкта з аналогічними функціями [7, 8].

Загалом можна виділити такі загрози безпеки для Android-додатків:

– несанкціонований доступ до даних у додатку;
– перехоплення даних в каналах передачі;
– несанкціонований доступ до даних у базах даних;
– аналіз коду додатку;
– несанкціоноване використання додатку.

Існуючі засоби захисту додатків реалізують окремі механізми (наприклад, тільки обфускацію коду або автентифікацію користувачів при доступі до даних), не враховуючи весь комплекс загроз, що може призвести до зменшення рівня безпеки, замість очікуваного покращення. А багаторівневий підхід, який враховує різноманітні особливості функціонування додатків у операційній системі Android, дозволить реалізувати перекриття вказаних загроз і тим самим покращити безпеку додатків.

Багаторівнева модель захисту додатків в ОС Android

Для захисту мобільних Android-додатків пропонується комплексний системний підхід на основі багаторівневої моделі. На рис. 1 наведена узагальнена графічна модель такого підходу.

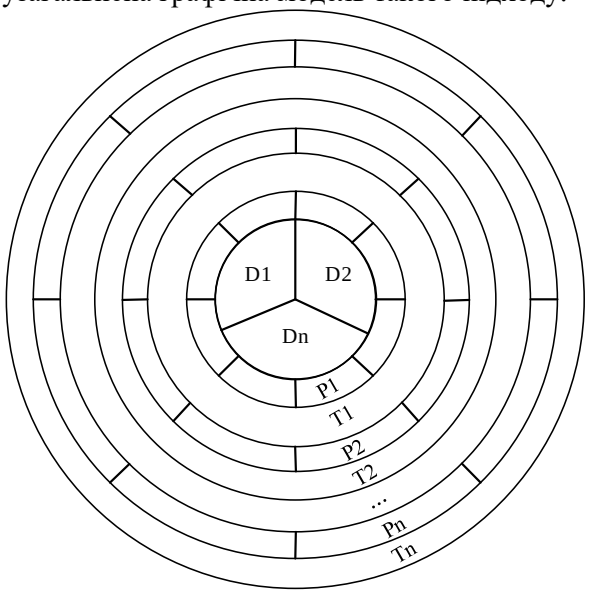


Рис. 1. Загальна графічна модель багаторівневого захисту

Рівень захищеності на мобільних пристроях з ОС Android можна описати такою моделлю:

$$Z = \{D, T, P\},$$

$$D = \{D1, D2, ..., Dn\},$$

$$T = \{T1, T2, ... Tn\},$$

$$P = \{P1, P2, ..., Pn\},$$

де **D** – об'єкт захисту; **T** – методи захисту; **P** – загрози.

В центрі моделі знаходяться об'єкти захисту додатку **D**, в кільцях навколо об'єктів − загрози **P** і контрзаходи **T**, що протидіють цим загрозам.

Для підвищення захищеності мобільного додатку, а саме зменшення ймовірності виникнення та реалізації атак шодо його несанкціонованого використання зловмисником пропонується структура системи захисту з певною надлишковістю, а саме перекриттям загроз низкою контрзаходів. На рис. 2 наведена графічна модель багаторівневого захисту мобільного Android-додатку, який містить чутливу інформацію з урахуванням типових загроз несанкціонованого використання.

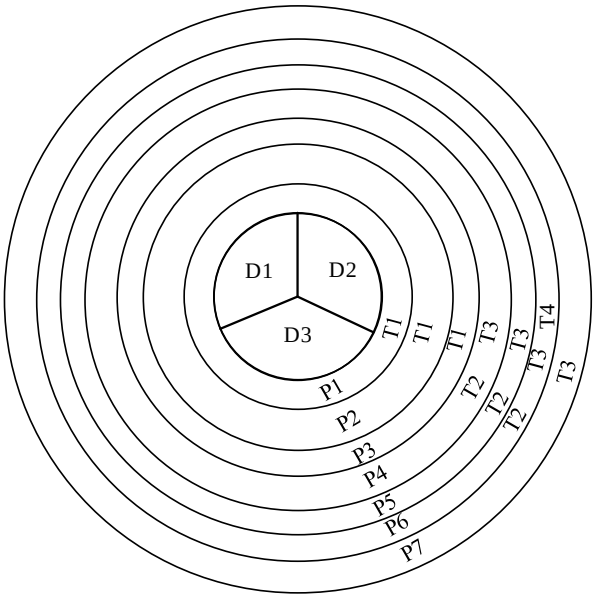


Рис. 2. Графічна модель багаторівневого захисту мобільних додатків з ОС Android від несанкціонованого використання

Об'єктами захисту є:

– код додатку D1,

– дані додатку D2,

– доступ до інфтерфейсу додатку D3.

Методи та засоби захистуAndroid-додатку:

– обфускація коду T1,

– автентифікація T2,

– віддалений контроль та управління додатком T3,

– захист бази даних (БД) T4.

Зарози несанкціонованого використання додатку та відповідні контрзаходи:

– копіювання коду P1 захищається T1;

– аналіз коду P2 захищається T1;

– аналіз структури коду P3 захищається T1;

– заміна даних P4 захищається T2 і T3;

– крадіжка даних P5 захищається T2 і T3;

– перегляд даних P6 захищається T2, T3 та T4;

– перехоплення в каналах передачі P7 захищається T3.

Застосування такого підходу дозволить значно підвищити надійність системи захисту, а також забезпечити гнучкість у її комплектуванні залежно від пріоритетів користувача.

Дана модель має надлишковість методів захисту, але її перевагою є перекриття деяких загроз кількома методами захисту, що значно зменшує ймовірність виникнення цієї загрози.

Архітектура системи захисту

На основі моделі багаторівневого захисту розроблено та реалізовано архітектуру системи захисту мобільного додатку (рис. 3).

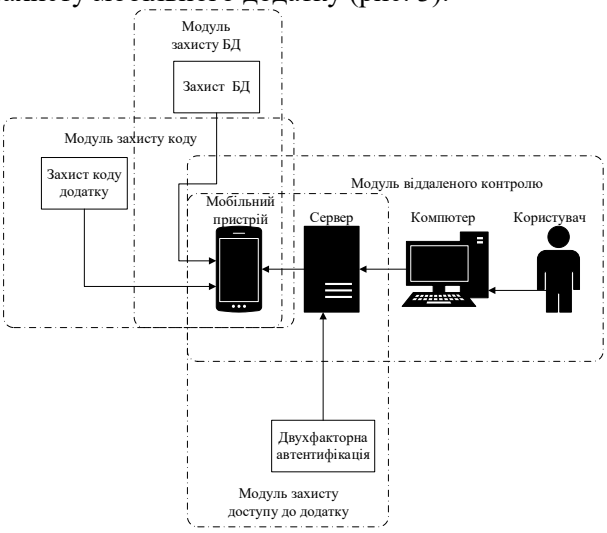


Рис. 3. Архітектура системи захисту

Архітектура системи (рис. 3.) включає модуль обфускації коду додатку для захисту від реверс-інженірингу, модуль багатофакторної автентифікації для контролю доступу до додатку, модуль віддаленого контролю додатку та управління даними, модуль захисту БД для шифрування даних додатку.

Для спрощення впровадження та використання системи захисту пропонується її розробка, програмна реалізація у вигляді бібліотеки.

Модуль захисту коду додатку від реверс-інженірингу використовує обфускації коду під час збору додатку в інсталяційний apk-файл.

Модуль віддаленого контролю має серверну і клієнтську частину. Користувач за допомогою веб-інтерфейсу може відправляти на мобільний пристрій команди керування додатком, а саме:

– очищення даних додатку;

– блокування/розблокування доступу до додатку;

– резервне копіювання даних додатку;

– відновлення даних додатку.

Модуль багатофакторної автентифікації також має клієнт-серверну архітектуру. Спочатку користувач відправляє логін та пароль на сервер. Якщо вони підтверджуються, то додаток за допомогою Bluetooth починає шукати апаратний токен. Для апаратного токену використовується браслет з вбудованим Bluetooth-адаптером. Модуль захисту БД орієнтований на шифрування інформації, у тому числі даних автентифікації. На рис. 4 наведено загальну модель функціонування системи захисту.

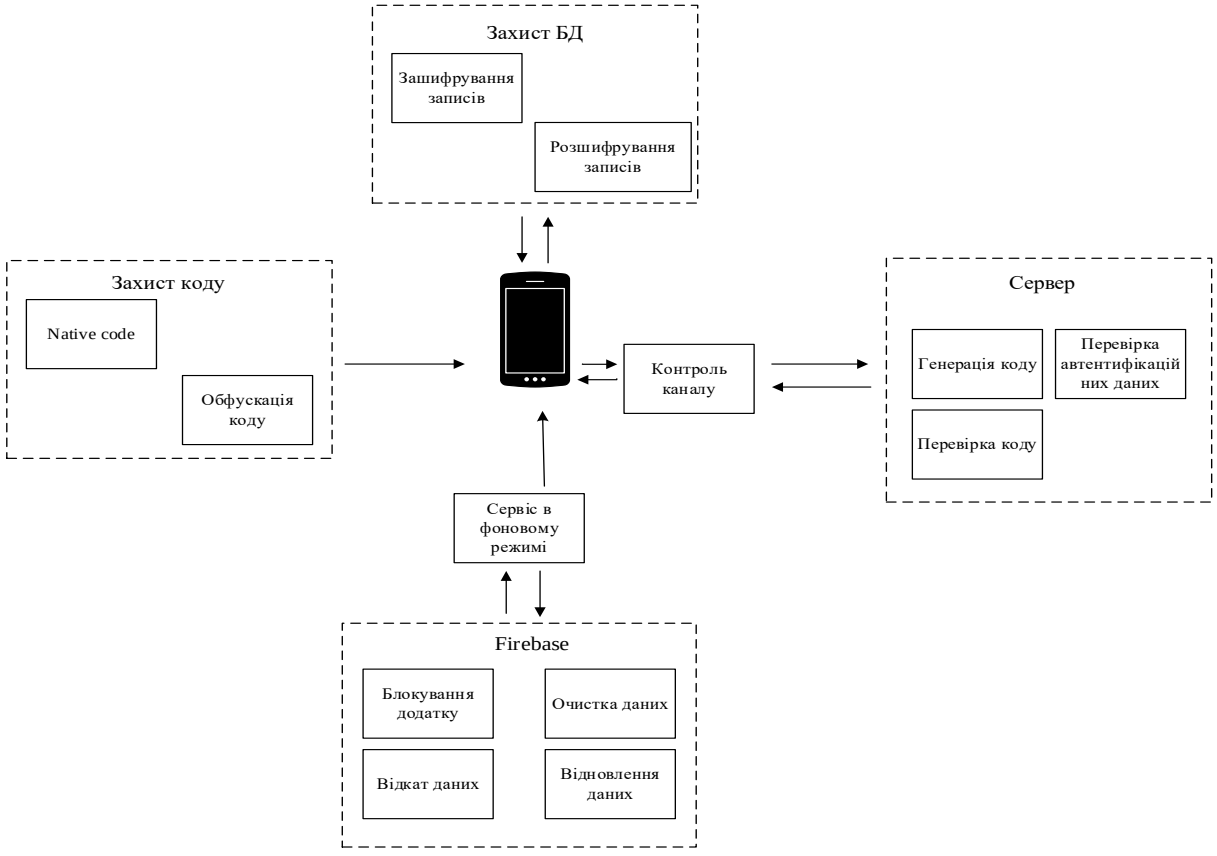


Рис. 4. Загальна модель функціонування системи захисту

Модуль багатофакторної автентифікації використовує сервер для перевірки автентифікаційних даних, генерації коду підтвердження та перевірки цього коду. Модуль віддаленого контролю включає в себе серверну частину, з якої відправляються команди на мобільний пристрій, команди приймаються сервісом, який завжди працює в фоновому режимі. Модуль захисту БД зашифровує всі записи в базу даних протоколом AES і розшифровує їх при читанні з бази. Для захисту роботи з сервером в додатку виконується примусовий контроль каналу, тобто перевірка на те, щоб дані не відправлялись/приймались з посторонніх серверів.

Модуль захисту коду додатку

На основі аналізу досліджених варіантів для захисту коду від реверс-інженірингу було обрано засіб ProGuard [9], код додатку та всіх бібліотек, код яких стискається, зачищається від "мертвого" коду і невикористовуваних змінних і обфускується. Для захисту коду Java винесено частину функцій в native-код. Обфускація коду виконується в момент збору apk-файлу. Ресурси додатку, aidl-файли та код додатку відправляються на Java-компілятор, де код додатку обфускується і отриманий код перетворюється в байт-код. Далі береться код бібліотек, доданих в проект, і разом з основним кодом додатку вони записуються в файл classes.dex. Далі завантажуються інші ресурси, що розміщені в підключених бібліотеках або jar-файлах, і додаток збирається в apk-файл. Потім в файл додається інформація про його підпис debug- або release-ключем.

При цьому виконується лексична обфускація коду додатку. В загальному модель роботи обфускації можна представити так:

$$\mathbf{R} = \{\mathbf{K}, \mathbf{Cl}\}$$

де **R** – результат обфускації; **K** – значення з таблиці заміни; **Cl** – назва класу, методу або змінної.

Під час збору додатку в apk-файл збираються всі файли додатку і викликається функція обфускації коду. Значення, якими заміняються назви класів, методів і змінних, знаходиться в таблиці. Таблиця складається з послідовного списку літер англійського алфавіту a…z. У разі, якщо клас достатньо великий і літер не вистачає, послідовність продовжується, включаючи по 2 літери алфавіту aa…zz. Обирається перший параметр з класу, який буде замінений, з таблиці заміни, по порядку обираються значення для заміни. Якщо значення з таблиці не збігається з назвою класу, методу або змінної, виконується заміна, якщо збігається, береться наступне значення з таблиці. Після завершення обфускації процес збору apk-файлу продовжується.

Модуль віддаленого контролю додатком

Для віддаленого контролю та управління додатком використані такі функції: повне очищення даних додатку; блокування входу в додаток; створення бекапу даних додатку на сервері; відновлення даних додатку з сервера.

При розробці запропоновано безкоштовний постачальник хмарних сервісів Firebase [10] від компанії Google. Він дозволяє налаштувати базу даних для збереження користувачів та відправляти push-повідомлення з командами в додаток, щоб контролювати його віддалено. В Firebase також є вбудована база даних, в якій зберігаються токени для відправки команд.

При першому вході в мобільний додаток генерується токен розміром в 225 символів для ідентифікації мобільного пристрою. Загальну модель генерації токен можна предстаивти так:

$$\mathbf{To} = \{\mathbf{Pa}, \mathbf{I}, \mathbf{M}\},$$

де **To** – токен; **Pa** – назва пакету додатку; **I** – id-додатку; **M** – період повторної генерації ключа.

Після того, як токен був згенерований, на мобільний пристрій можна відправляти команди для віддаленого контролю.

На віддаленому сервері додаток шифрує повідомлення для додатку і відправляє push notification на мобільний пристрій. Загальна модель процесу шифрування команд наведена нижче:

$$\mathbf{H} = \{\mathbf{Te}, \mathbf{Key}\},$$

де **H** – зашифрований текст; **Te** – текст для шифрування; **Key** – ключ шифрування розмірністю 128 біт.

Додаток за допомогою сервіса, що працює в фоновому режимі, отримує команду. Перед виконанням команди додаток перевіряє достовірність сервера; якщо сервер пройшов перевірку, команда виконується, якщо ні - ігнорується. Після цього виконується розшифрування отриманого повідомлення.

Додаток з серверу може приймати такі команди:

clear_app – повне очищення даних додатку;

block_app – блокування входу в додаток;

backup_data – створення бекапу даних додатку на сервері;

recovery_data – відновлення даних додатку з сервера.

Отримавши одну з наведених вище команд, додаток в фоновому режимі викликає модуль, який виконує дії залежно від команди. Команда clear_app виконує очищення даних додатку, видалення всіх таблиць бази даних, очищення

кешу додатку, вихід з облікового захисту. Команда block_app виконує блокування входу в додаток, тобто в момент запуску головного екрану в методі onCreate, який викликається першим в життєвому циклі Activity, викликається метод для перевірки, чи не заблокований додаток. Якщо вхід заблоковано, метод завершує роботу додатку. Команда backup_data призначена для створення бекапу даних додатку та відправки його на сервер у вигляді zip архіву, якщо це файли, і у файлі розширення json, якщо це дані з бази. Для цього користувачу потрібно викликати метод з бібліотеки та вказати, які дані та у якому вигляді він буде зберігати. Команда recovery_data призначена для відновлення даних з сервера в додаток.

Модуль автентифікації

Парольна схема автентифікації має як значні переваги (простота реалізації, відомість тощо), так і значні недоліки (підглядування, підбір слабких паролів, повторне введення тощо). Використання лише парольної схеми не дозволяє реалізувати активну автентифікацію (постійну перевірку особистості користувача на основі аспектів його взаємодії з обчислювальним пристроєм) для контролю за географічним місцезнаходженням або взаємним положенням пари користувач/мобільний пристрій.

На основі аналізу варіантів активної автентифікації [1, 2] було обрано апаратні токени, які дозволяють виконувати багатофакторну автентифікацію за парольною схемою та на основі апаратного бездротового токену, що додатково влючає в себе такі можливості:

– перевірку MAC-адреси бездротового пристрою;

– налаштування радіусу прийняття сигналу;

– налаштування часу повторної перевірки наявності токена.

Користувач відправляє автентифікаційні дані на сервер, сервер перевіряє їх і дає відповідь мобільному додатку. Як база даних в додатку використовується Firebase, в ній знаходиться таблиця з логінами та паролями, з якими зрівнюються дані, що приходять з мобільного пристрою. Якщо дані збігаються, то мобільний додаток запускає сервіс, який починає перевіряти, чи є поруч апаратний токен, наприклад, підключений через вбудований Buetooth, за яким мобільний пристрій підключається до нього і зчитує токен. Після підтвердження токена можна працювати з додатком.

В додатку при кожному вході незалежно від того, коли останній раз використовувався додаток, викликається вікно автентифікації. Автентифікаційні дані (наприклад, логін та пароль) відправляються на сервер для перевірки. У разі, якщо користувача з такими даними не існує, сервер повертає в додаток повідомлення про помилку. Після підтвердження даних користувача на мобільний пристрій відправляється повідомлення про вдалу автентифікацію, в цей момент на мобільному пристрої вмикається Bluetooth і сервіс пошуку. Він знаходить всі BLE-пристрої і отримує їх MAC-адреси. Загальна модель роботи автентифікації

$$\mathbf{R} = \{\mathbf{L}, \mathbf{Pw}, \mathbf{RT}\},$$

де **L** – логін; **Pw** – пароль; **RT** – результат, повернутий на основі перевірки апаратного токена:

$$\mathbf{RT} = \{\mathbf{MA}, \mathbf{Ti}, \mathbf{Ra}\},$$

тут **MA** – MAC-адреса апаратного токена; **Ti** – часовий інтервал, через який здійснюється опитуванння; **Ra** –відстань, на якій сигнал вважається автентичним.

Кожна MAC-адреса (**MA**) порівнюються зі збереженою при реєстрації на мобільному пристрої. При відповідності у базі даних надається доступ до роботи з додатком. Через заданий інтервал часу (**Ti**) відбувається перевірка, чи апаратний токен знаходиться на відстані, що не перевищує задану (**Ra**). Якщо користувач з апаратним токеном вийде з радіусу дії Bluetooth-зони мобільного пристрою, між ними розірветься зв’язок, і додаток завершить роботу.

Модуль захисту бази даних

Для вирішення проблеми несанкціонованого копіювання інформації з бази даних, наприклад, у випадку отримання доступу до мобільного пристрою зловмисником або шкідливим процесом, було реалізовано модуль криптографічного захисту бази даних. Шифрування здійснюється для окремих записів, а не БД в цілому. Шифрування даних здійснюється на основі блокового симетричного шифру AES з ключем 128 біт. Ключ шифрування генерується на основі пакету додатку і випадкового числа, збереженого в ресурсах додатку. При цьому кожному запису БД відповідає свій ключ. Ключі шифрування можуть зберігатися як локально, так і віддалено, і при цьому можуть бути також додатково зашифровані. Модуль реалізовано на основі системи керування базами даних Realm, яка є однією із найбільш швидких мобільних систем [13].

Висновки

Набула подальшого розвитку модель захисту Android-додатку від несанкціонованого використання, яка відрізняється своєю багаторівневою структурою з перекриттям загроз, що дозволяє організувати ефективний захист доступу до додатку на основі багатофакторної автентифікації, захисту програмного коду на основі обфускації та захисту даних додатку на основі віддаленого контролю та управління ним, а також збереження даних в захищеній базі даних.

На основі запропонованої моделі розроблено архітектуру системи захисту Android-додатку. Система містить модуль обфускації коду додатку для захисту від реверс-інжинірингу, модуль автентифікації для контролю доступу до додатку, модуль віддаленого контролю додатку та управління даними, модуль захисту БД для шифрування даних додатку.

На основі запропонованої архітектури системи розроблено програмний модуль для захисту від несанкціонованого використання Android-додатку у вигляді бібліотеки, який дозволяє забезпечити захист від загроз конфіденційності, цілісності та доступності. Розроблена бібліотека дозволяє зменшити тривалість розробки Android-додатків на етапі робочого проектування при реалізації вимог щодо безпеки за рахунок зниження трудозатрат. При цьому система захисту є гнучкою, тобто при розробці додатку можна до нього інтегрувати той чи інший модуль захисту залежно від встановлених вимог.

Литература:

1.*Voitovych O.P., Hurskyi M.V., Snigovyy D.S., Kupershtein L.M.* “Monitoring tool for Android operating system”, in Scientific journal Herald of Khmelnytskyi national university 2017. Issue 3, Volume 249. 236-241 p.

2. *Tabassum, Gulista, Shikha Pandit, and Nupur Ghosh*. "Android Application Security", in Journal of Emerging Technologies and Innovative Research. Vol. 1. No. 7. 2014.

3. Kupershtein L.M., Voitovych O.P., Kaplun V. A., Prokopchuk S.O. “The database-oriented approach to data protection in Android operation system”, in Scientific journal Herald of Khmelnytskyi national university 2018, Issue 1, 18-22 p.

4. *Zhang, N., Yuan, K., Naveed, M., Zhou, X., & Wang, X*. “Leave me alone: App-level protection against runtime information gathering on android” In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 915-930). IEEE.

5. *Hassanshahi, B., & Yap, R.H.* “Android Database Attacks Revisited”. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. P. 625-639.

6. *Baryshev, Y., Kaplun, V. and Neiyumina, K.* “Discretional model and method of distributed information resources access control”. In Scientific Works of Vinnytsia National Technical University. 2 (Jun. 2017).

7. *Kim, N. Y., Shim, J., Cho, S. J., Park, M., & Han, S.* “Android Application Protection against Static Reverse Engineering based on Multidexing”. J. Internet Serv. Inf. Secur., 6(4), 54-64 (2016).

8. *Dong, S., Li, M., Diao, W., Liu, X., Liu, J., Li, Z., & Zhang, K.* “Understanding Android Obfuscation Techniques: A Large-Scale Investigation in the Wild”. arXiv preprint arXiv:1801.01633 (2018).

9. http://proguard.sourceforge.net/.

10. Firebase is Google’s mobile platform that helps you quickly develop high-quality apps. URL: https://firebase.google.com/.

11. *Baryshev Yu., Kaplun V.* “Remote user authentication method for network services” in Information Technology and Computer Engineering. 2014 Vol. 2, no. 30, 1.

12. *Fridman, L., Weber, S., Greenstadt, R., & Kam, M.* “Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location” in IEEE Systems Journal, 11(2), 513-521. (2017).

13. https://realm.io.

Надійшла до редколлегії 02.06.2018

Рецензент: д-р техн. наук, проф. Бараннік В.В.

Куперштейн Леонід, канд. техн. наук, доцент кафедри захисту інформації Вінницького національного технічного університету. Наукові інтереси: застосування інтелектуальних технологій в кібербезпеці. Адреса: Україна, 21021, Вінниця, вул. Хмельницьке шосе, 95, кімн. 2424, e-mail: kupershtein@vntu.edu.ua

Войтович Олеся, канд. техн. наук, доцент кафедри захисту інформації Вінницького національного технічного університету. Наукові інтереси: кібербезпека. Адреса: Україна, 21021, Вінниця, вул. Хмельницьке шосе, 95, кімн. 2424, e-mail: voytovych.olesya@vntu.edu.ua

Остапенко-Боженова Аліна, асистент кафедри захисту інформації Вінницького національного технічного університету. Наукові інтереси: застосування криптографічного захисту інформації. Адреса: Україна, 21021, Вінниця, вул. Хмельницьке шосе, 95, кімн. 2424, e-mail: asja87@gmail.com

Прокопчук Сергій, магістр з кібербезпеки. Наукові інтереси: безпека ОС Android. Адреса: Україна, 21021, Вінниця, вул. Хмельницьке шосе, 95, кімн. 2424, e-mail: prokopchukserhii@gmail.com

Kupershtein Leonid, PhD, associated professor of the information protection department, Vinnytsya National Technical University. Scientific interests: intellectual technology applications in cyber security. Address: 95 Khmelnytske shose, Vinnytsya, 21021, Ukraine, e-mail: kupershtein@vntu.edu.ua

Voitovych Olesia, PhD, associated professor of the information protection department, Vinnytsya National Technical University. Scientific interests: cyber security. Address 95 Khmelnytske shose, Vinnytsya, 21021, Ukraine, e-mail: voytovych.olesya@vntu.edu.ua

Ostapenko-Bozhenova Alina, assistant of the information protection department, Vinnytsya National Technical University. Scientific interests – cryptography. Address 95 Khmelnytske shose, Vinnytsya, 21021, Ukraine, e-mail: asja87@gmail.com

Prokopchuk Serhii, master of cybersecurity, Vinnytsya National Technical University. Scientific interests: Android OS protection. Address 95 Khmelnytske shose, Vinnytsya, 21021, Ukraine, e-mail: prokopchukserhii@gmail.com

Prokopchuk Serhii, master of cybersecurity, Vinnytsya National Technical University. Scientific interests – Android OS protection. Address 95 Khmelnytske shose, Vinnytsya, 21021, Ukraine, e-mail: prokopchukserhii@gmail.com

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 621.397

РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОПЕРАТИВНОЇ ТА КОНФІДЕНЦІЙНОЇ ДОСТАВКИ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ В СИСТЕМІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

БАРАННІК В.В., ГАВРИЛОВ Д.С., СОРОКУН А.Д.

Розробляється інформаційна технологія оперативної та конфіденційної доставки відеоінформаційного ресурсу в системі критичної інфраструктури шляхом захисту блоків, що містять контурну інформацію. Виявляється контурна інформація за допомогою аналізу блоку розробленою метрикою. Показується можливість класифікації блоків за контурною насиченістю з метою подальшої обробки.

Ключові слова: інформаційна технологія, оперативність, конфіденційність, метрика, контурна інформація.

1. Вступ

З суцільною інформатизацією та впровадженням новітніх технологій в життя людини по всьому світу, особливо в розвинутих країнах, які додержуються концепції Інтернету Речей, гостро постало питання контролю як внутрішніх процесів, так і зовнішніх проявів стану справ різного масштабу. Дослідження в області психофізіології за критерієм рівня сприйняття інформації залежно від методу доведення (візуально, за допомогою звуків (слова) чи кінестетично) показало, що візуальне доведення інформації про зовнішній прояв справ є найбільш ефективним.

При цьому на рівень сприйняття інформації, представленої у вигляді фото – та/чи відеоматеріалів, впливає рівень яскравості, контрасту та роздільна здатність.

Варто відзначити, що відеоінформаціний ресурс збирається, обробляється та передається як на рівні людина-людина, так і на рівні держава-держава, цивілізація-цивілізація. Подібні відомості, як правило, містять конфіденційну інформацію, тож потребують криптографічного захисту. Найбільш помітним на зображенні є об’єкт, що виділяється (контрастує) на фоні, тобто елемент зображення, який має чіткий контур.

Отже, для забезпечення необхідного рівня захисту необхідною і достатньою умовою є криптографічний захист блоків, що містять контурну інформацію. При цьому критичним є час на обробку та передачу даних.

Таким чином, метою дослідження є підвищення оперативності передачі захищених відеоданих, що є *актуальною науково-прикладною* задачею.

В свою чергу, завданням дослідження є розробка інформаційної технології оперативної та конфіденційної доставки відеоінформаційного ресурсу в системі критичної інфраструктури.

Дослідження пропонується проводити на основі алгоритму обробки даних JPEG у зв’язку з широкою популярністю та високою ефективністю даної інформаційної технології.

2. Основна частина дослідження

Аналіз інформаційної технології JPEG показав, що даний алгоритм дозволяє зменшити об’єм вхідних даних за рахунок того, що усувається психовізуальна, спектральна та структурна надлишковість.

Першою усувається психовізуальна надлишковість за рахунок психофізіологічної особливості зору людини, який реагує на зміни яскравості більше, ніж на зміни кольору. Маємо на увазі етап перетворення з колірного простору RGB в колірний простір YCrCb [9]. Слід зауважити, що найбільш важливою є компонента яскравості Y, аналіз якої вказав на можливість виявлення контурної інформації.

Розроблено метрику виявлення контурної інформації:

$$K = \log_2\left(\prod_{i=1}^{8} b_i\right);\ \ b_i = \max A(i) - \min A(i),$$

де K – метрика, що визначає наявність контурної інформації в блоці; $\max A(i)$ – максимальний елемент і-го рядка блоку А; $\min A(i)$ – мінімальний елемент і-го рядка блоку А; b_i – різниця максимального та мінімального елемента і-го рядка, при цьому: $B = \sum_{i=1}^{8} b_i$.

Приклад роботи даної метрики:

$$A = \begin{vmatrix} 136 & 136 & 136 & 136 & 237 & 237 & 237 & 0 \\ 136 & 136 & 136 & 136 & 136 & 237 & 0 & 237 \\ 136 & 136 & 136 & 136 & 136 & 0 & 237 & 237 \\ 136 & 136 & 136 & 0 & 0 & 136 & 136 & 237 \\ 237 & 136 & 0 & 136 & 136 & 136 & 136 & 136 \\ 237 & 0 & 136 & 136 & 136 & 136 & 136 & 136 \\ 0 & 237 & 237 & 136 & 136 & 136 & 136 & 136 \\ 237 & 237 & 237 & 237 & 136 & 136 & 136 & 136 \end{vmatrix}$$

$$\max A(i) = \begin{vmatrix} 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \end{vmatrix} \qquad \min A(i) = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix}$$

$$B = \begin{vmatrix} 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \\ 237 \end{vmatrix}$$

$$\prod_{i=1}^{8} b_i = 9.9537;$$

$$K = 63.1099.$$

В ході дослідження якості розробленої інформаційної технології встановлено можливість визначення класу блоку 8x8 (табл. 1-3). Виявлена особливість дає змогу проводити уточнюючий та/чи додатковий аналіз фото - та/чи відеоматеріалу на наступних етапах обробки на основі JPEG-платформи. Виділено такі класи блоків:

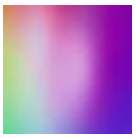
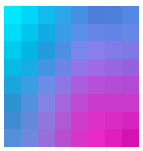
– блок без контурної інформації;

Таблиця 1

	max A(i)	min A(i)	$\prod_{i=1}^{8} b_i$	K
	34 34 34 34 34 34 34 34	34 34 34 34 34 34 34 34	0	0
	255 255 255 255 255 255 255 255	255 255 255 255 255 255 255 255	0	0

– блок з поступовим переходом кольору;

Таблиця 2

	max A(i)	min A(i)	$\prod_{i=1}^{8} b_i$	K
	219 219 219 219 214 207 193 163	126 129 126 120 112 102 93 86	6.35512	52.496
	59 120 161 194 222 248 255 255	0 1 0 0 0 0 34 52	5.4165	58.910

– блок з контурною інформацією.

Таблиця 3

	max A(i)	min A(i)	$\prod_{i=1}^{8} b_i$	K
	249 237 239 231 236 222 224 241	29 23 24 25 21 19 0 0	4.91294	62.0913
	255 255 255 255 249 252 255 255	14 0 77 0 1 66 36 3	7.10111	62.6228

Приклад вихідного та захищеного зображення представлено на рис. 1, 2.

Рис. 1. Вихідне зображення

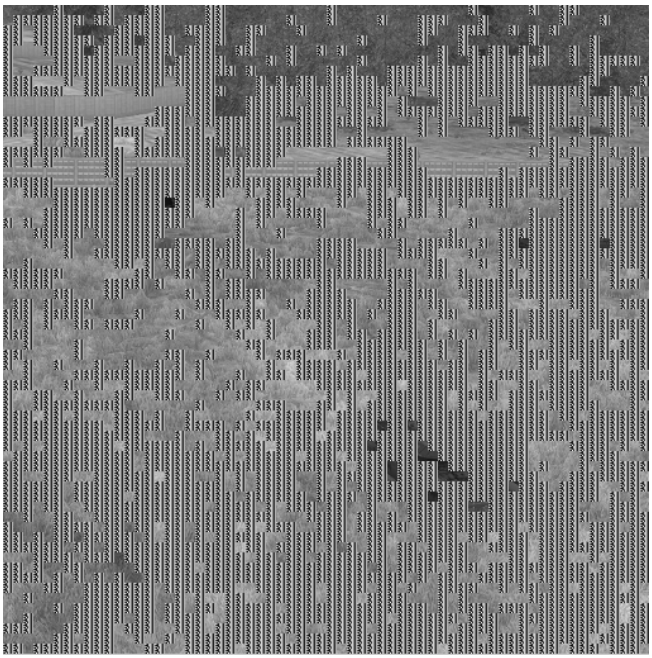


Рис. 2. Зображення, захищене розробленою інформаційною технологією

Аналіз рис. 2 вказав на можливість розробленої інформаційної технології виконувати поставлене завдання по оперативній, захищеній передачі даних з необхідною якістю.

3. Висновки

Розроблено інформаційну технологію оперативної та конфіденційної доставки відеоінформаційного ресурсу в системі критичної інфраструктури шляхом захисту блоків, що містять контурну інформацію.

Наукова новизна. Виявлення контурної інформації відбувається за допомогою аналізу блоку розробленою метрикою. Виявлена можливість класифікації блоків за контурною насиченістю з метою подальшої обробки.

Вирішена *актуальна науково-прикладна задача* підвищення оперативності передачі захищених відеоданих.

Литература: 1. *Баранник В.В.* Метод повышения информационной безопасности в системах видеомониторинга кризисных ситуаций / В.В. Баранник, Ю.Н. Рябуха, О.С. // Монография. Черкассы, 2015. 143 с. 2. *Баранник В.В.* Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку / А.В. Власов, В.В. Бараннік, Р.В.Тарнополов // Наукоємні технології. 2014. № 1 (21). С. 55 – 60. 3. *Баранник В.В.* Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов, С.А. Сидченко, А.Э. Бекиров // Информационно-управляющие системы на ЖД транспорте. 2014. №3. С. 24 – 31. 4. *Баранник В.В.* Селективний метод шифрування відеопотоку в телекомунікаційних системах на основі приховування базового І-кадру / В.В. Баранник, Д.І. Комолов, Ю.М. Рябуха // Наукоємні технології. № 2. 2015. С. 14 – 23. 5. *Barannik V.V.* The model of avalanche-relating effect in the process of images reconstruction in the combined cryptosemantic systems on the polyadic presentation / V.V. Barannik V.V. Larin, S.A. Sidchenko // Наукоємні технології. 2010. № 1(5). С. 68 – 70. 6. *Гаврилов Д.С.* Метод захисту низькочастотних складових в алгоритмі кодування JPEG./ Ларин В.В., Комолов Д.С., Ялівець К.В., Гаврилов Д.С. // Системи обробки інформації. 2015. № 9 (134). С. 121 – 123. 7. *Гаврилов Д.С.* Метод забезпечення безпеки відеоінформаційного ресурсу на основі багаторівневої селективної обробки в телекомунікаційних системах./ О.Г. Оксіюк, Д.С. Гаврилов, П.М. Гуржій, Б.О. Демідов// Наука і техніка Повітряних Сил Збройних Сил України. 2017 № 1 С. 46 - 48. 8. *Gavrulov D.* The analysis of template method of video processing./ Larin V., Krasnikov P., Gavrulov D. // Proceedings of 2015 1st International Conference on Advanced Information and Communication Technologies-2015 (AICT'2015), Lviv, Ukraine, October 29 – November 1, 2015. P. 87 – 89. 9. *Ватолин Д.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Рятушняк, М. Смирнов, В. Юкин // Учебно-справочное издание. М.: ДИАЛОГ – МИФИ. 2003. 384с. 10. *Гонсалес Р.,* Цифровая обработка изображений / Гонсалес Р., Вудс Р. // М.: Техносфера, 2005. С.812-850 11. *Яне Б.* Цифровая обработка изображений. М.: Техносфера. 2007. С.331-356. 12. *Сойфера В.А.* Методы компьютерной обработки изображений. – М.: Физматлит, – 2003. – С.192-203.

Transliterated bibliography:

1. *Barannik V.V.* Metod povyshenija informacionnoj bezopasnosti v sistemah videomonitoringa krizisnyh situacij

/ V.V. Barannik, Ju.N. Rjabuha, O.S. // Monografija. Cherkassy, 2015. 143 s.

2. *Barannyk V.V.* Model' zagroz bezpeky videoinformacijnogo resursu system videokonferenczv'-jazku. / A.V. Vlasov, V.V. Barannik, R.V.Tarnopolov // Naukojemni tehnologii'. 2014. - № 1 (21). S. 55 – 60.

3. *Barannik V.V.* Obosnovanie znachimyh ugroz bezopasnosti videoinformacionnogo resursa sistem videokonferencsvjazi profil'nyh sistem upravlenija / V.V. Barannik, A.V. Vlasov, S.A. Sidchenko, A.Je. Bekirov // Informacionno-upravljajushhie sistemy na ZhD transporte. 2014. №3. S. 24 – 31.

4. *Barannyk V.V.* Selektyvnyj metod shyfruvannja vydeopotiku v telekomunykacijnyh systemah na osnovi pryhovuvannja bazovogo I-kadru / V.V. Barannyk, D.I. Komolov, Ju.M. Rjabuha // Naukojemni tehnologii'. № 2. 2015. S. 14 - 23.

5. *Barannik V.V.* The model of avalanche-relating effect in the process of images reconstruction in the combined cryptosemantic systems on the polyadic presentation / V.V. Barannik V.V. Larin, S.A. Sidchenko // Наукоємні технології. 2010. № 1(5). С. 68 – 70.

6. *Gavrylov D.S.* Metod zahystu nyz'kochastotnyh skladovyh v algorytmi koduvannja JPEG./ Laryn V.V., Komo-lov D.S., Jalivec' K.V., Gavrylov D.S. // Systemy obrobky informacii'. 2015. № 9 (134). S. 121 – 123.

7. *Gavrylov D.S.* Metod zabezpechennja bezpeky videoinformacijnogo resursu na osnovi bagatorivnevoi' selektyvnoi' obrobky v telekomunikacijnyh systemah./ O.G. Oksijuk, D.S. Gavrylov, P.M. Gurzhij, B.O. Demidov // Nauka i tehnika Povitrjanyh Syl Zbrojnyh Syl Ukrai'ny. № 1. 2017. S. 46 - 48.

8. *Gavrulov D.* The analysis of template method of video processing / Larin V., Krasnikov P., Gavrulov D. // Proceedings of 2015 1st International Conference on Advanced Information and Communication Technologies-2015 (AICT'2015), Lviv, Ukraine, October 29 – November 1, 2015. P. 87 – 89.

9. *Vatolin D.* Metody szhatija dannyh. Ustrojstvo arhivatorov, szhatie izobrazhenij i video. / D. Vatolin, A. Rjatushnjak, M. Smirnov, V. Jukin // Uchebno-spravochnoe izdanie. M.: DIALOG – MIFI, 2003. 384s.

10. *Gonsales R.*, Cifrovaja obrabotka izobrazhenij. /. Gonsales R., Vuds R. // M.: Tehnosfera, 2005. S.812-850

11. *Jane B.* Cifrovaja obrabotka izobrazhenij. – M.: Tehnosfera, 2007. S.331-356.

12. *Sojfera V.A.* Metody komp'juternoj obrabotki izobrazhenij. M.: Fizmatlit, 2003. S.192-203.

Надійшла до редколегії 28.05.2018

Рецензент: д-р техн. наук, проф. Безрук В.М.

Бараннік Володимир Вікторович, д-р техн. наук, професор, начальник кафедри бойового застосування та експлуатації АСУ Харківського національного університету Повітряних Сил ім. І. Кожедуба, e-mail: vvbar.off@gmail.com, orcid.org/0000-0002-2848-4524. Адреса: Україна, 61023, Харків, ул. Сумська, 77/79.

Гаврилов Дмитро Сергійович, аспірант ХНУРЕ. Наукові інтереси: системи, інформаційні технології, кодування, криптографічний захист. Адреса: Україна, 49032, Дніпро, вул. Аеродром, 10, тел. 8-066-2290463.

Сорокун Антон Дмитрович, аспірант Національного авіаційного університету. Наукові інтереси: обробка інформації. Адреса: Україна, 03058, Київ, пр. Космонавта Комарова 1, e-mail: anton.sorokun@gmail.com

Barannik Volodymyr Viktorovich, Dr. Tech. Sciences, professor, head of the military application and operation department, Kharkiv National Air University of the Air Force named after I. Kozheduba, e-mail: vvbar.off@gmail.com, orcid.org/0000-0002-2848-4524. Address: Ukraine, 61023, Kharkiv, Sumska Str., 77/79.

Havrylov Dmytro Serhiiovych, postgraduate of Kharkov National University of Radio Electronics. Scientific interests: systems, information technologies, coding, cryptographic protection. Address: Ukraine, 49032, Dnepr, st. Aerodrom, 10, tel. 8066-2290463. E-mail: havrylov_d@ukr.net.

Anton D. Sorokun, PhD student of the National Aviation University. Scientific interests: information processing. Address: Ukraine, 03058, Kiev, Cosmonaut Komarov Ave. 1, e-mail: anton.sorokun@gmail.com

УДК 004.771

ТЕХНОЛОГІЯ АВТЕНТИФІКАЦІЇ ВИБОРЦІВ У ВІДКРИТІЙ СИСТЕМІ ІНТЕРНЕТ ГОЛОСУВАННЯ

МАЧАЛІН І.О., ВИШНЯКОВ В.М., КОМАРНИЦЬКИЙ О.О.

Пропонується технологія дистанційної автентифікації виборців у відкритій системі Інтернет голосування з використанням біологічних або інших додаткових ознак, що усуває можливість передачі права голосу іншій особі і дозволяє позбутися обов'язкової очної перевірки осіб виборців перед кожним актом волевиявлення, що особливо важливо у разі тривалих відряджень виборців. При цьому зберігаються усі позитивні якості відкритої системи, включаючи повну контрольованість процесів на сервері Інтернет голосування в режимі реального часу.

Ключові слова: Інтернет голосування, дистанційна автентифікація, збереження таємниці голосів, відкрита система голосування, забезпечення довіри виборців.

1. Вступ

Дистанційне голосування через Інтернет (надалі ІГ) надає суттєві переваги виборцям щодо зручності, мобільності та економії часу. Крім того, скорочуються витрати на друк бюлетенів. Але суттєвим стримуючим фактором на шляху розвитку систем ІГ є недовіра виборців через неможливість впевнитись у тому, що в електронних засобах для голосування не закладено можливостей для розкриття таємниці голосів та/або викривлення результатів волевиявлення [1, 2]. Відомо, що для подолання недовіри треба надавати широкі можливості для контролю всіх тих об'єктів і процесів, які викликають сумніви. При цьому від повноти можливостей контролю залежить рівень довіри. Зрозуміло, що для беззаперечної довіри необхідно надати усім бажаючим можливість контролювати усі складові системи протягом усього часу її функціонування. Саме такий підхід запропоновано в роботі [3], де описані принципи побудови відкритої системи таємного голосування, у якій надається можливість масового дистанційного контролю з боку необмеженої кількості будь-яких осіб щодо усіх програмних засобів та процесів в режимі реального часу функціонування системи ІГ. У роботі [4] розвинуто цей підхід і доведено, що після проведення такого контролю не залишається підстав для недовіри, бо всі елементи системи і дії обслуговуючого персоналу, які можуть бути потенційно небезпечними, є відкритими для масового спостереження. Іншими словами, будь-яка спроба вчинення зловмисної дії у такій системі може бути виявлена та зафіксована контролюючими особами. При цьому забезпечується збереження таємниці голосів і неможливість викривлення результатів волевиявлення. Фактично тільки такі системи можуть претендувати на беззаперечну довіру виборців, бо наявність хоч однієї закритої частини завжди буде породжувати підозри щодо фальсифікації. В роботі [5] показана можливість протидії незаконному впливу на виборців (підкупом, залякуванням або силовим тиском) в умовах повністю контрольованої системи. Але, крім описаних переваг відкритих систем ІГ, слід відмітити, що залишається без відповіді питання дистанційної автентифікації особи виборця. Оскільки однією з відомих вимог до систем голосування є заборона передачі свого права голосу іншій особі, то можна вважати актуальною задачу дистанційного підтвердження особи виборця (або автентифікацію) в умовах повної відкритості (прозорості) системи ІГ з метою усунення очної перевірки особи в період уточнення списків голосуючих перед кожним актом волевиявлення. Це має особливе значення у випадках тривалих відряджень виборців.

2. Аналіз відомих рішень і постановка завдання

Для дистанційного підтвердження особи може використовуватись низка відомих ознак. Наприклад, в Естонії, де було вперше впроваджено ІГ на виборах державного масштабу [6], для підтвердження особи виборця використовують персональну електронну картку, яка є заміною паспорту. Одним з недоліків такого методу підтвердження є потреба у спеціальному пристрої для зчитування інформації з електронної картки. Крім того, як показано в роботі [5], такий метод автентифікації не захищає виборця від незаконного впливу. В Україні з 1 січня 2016 року також розпочато впровадження пластикових ID-карток замість паспортів. Але слід зауважити, що неможливо за допомогою будь-якої картки досягти беззаперечної гарантії того, що проголосувала саме та, а не якась інша особа. Це багаторазово продемонстровано голосуючими у ВР України. Тільки у тих випадках, коли ознаку неможливо відокремити від особи виборця, може бути досягнута беззаперечна гарантія того, що проголосувала саме та, а не якась інша особа. Такими властивостями у тій чи іншій мірі наділені біологічні ознаки людини. Серед цих ознак, крім широко відомих відбитків пальців, в останні десятиріччя використовують сітківку ока, райдужну оболонку ока, геометрію обличчя, термограму обличчя, геометрію руки, голос та динаміку почерку [7-10]. Найбільш придатною з перелічених ознак для дистанційної автентифікації можна вважати голос, бо майже все обладнання для доступу до мережі Інтернет має вбудований мікрофон, а у разі його відсутності можна скористатись окре-

мим телефоном. В роботі [10] щодо розпізнавання по голосу вказано на високу імовірність помилок другого роду. Такі помилки у разі зміни голосу через хворобу або з інших причин можуть унеможливити здійснення виборцем акту волевиявлення, що неприпустимо для системи голосування. Слід зауважити, що вплив помилок першого роду щодо розпізнавання голосу можна компенсувати шляхом використання комбінації голосу з паролем. При цьому для того, щоб проголосувати за когось іншого, треба крім знання паролю ще й мати такий самий або у достатній мірі схожий голос. Результати експериментальних досліджень, що наведені в роботі [9] і представлені у таблиці, свідчать про існування суттєвої залежності кількості помилок розпізнавання особи від варіанту прочитаного тексту.

Варіант тексту	Процент помилок
«шиншилла шила шубу»	18,7
«Клара украла коралі»	1,2
«витівка олігарха»	3,8

Бачимо з наведених у таблиці значень, що шиплячі звуки негативно впливають на якість розпізнавання особи, а обираючи тексти з переважною більшістю дзвінких звуків, можна значно підвищити цю якість. Дослідження в напрямку поліпшення розпізнавання по голосу тривають, а існуючі результати свідчать про можливість за допомогою біологічних ознак отримувати дані для уточнення особи виборця. В роботі [11] для автентифікації особи виборців обрано електронний цифровий підпис (ЕЦП), який може використовуватись в інших цілях, що не пов'язані з виборами, і тому не може бути переданий іншій особі. Але для того, щоб використовувати будь-яке уточнення особи у відкритих системах дистанційного голосування, слід розробити технологію, яка б дозволяла підключати додаткові засоби розпізнавання, не втрачаючи жодної з описаних вище переваг та включаючи прозорість і контрольованість. Розробка саме такої технології і є завданням даного дослідження.

3. Основна частина дослідження

В роботі [4] представлено логічну модель відкритої системи дистанційного голосування , яку зображено на рис. 1, де все, що знаходиться в середині зовнішнього кола, відповідає множині об'єктів сервера ІГ.

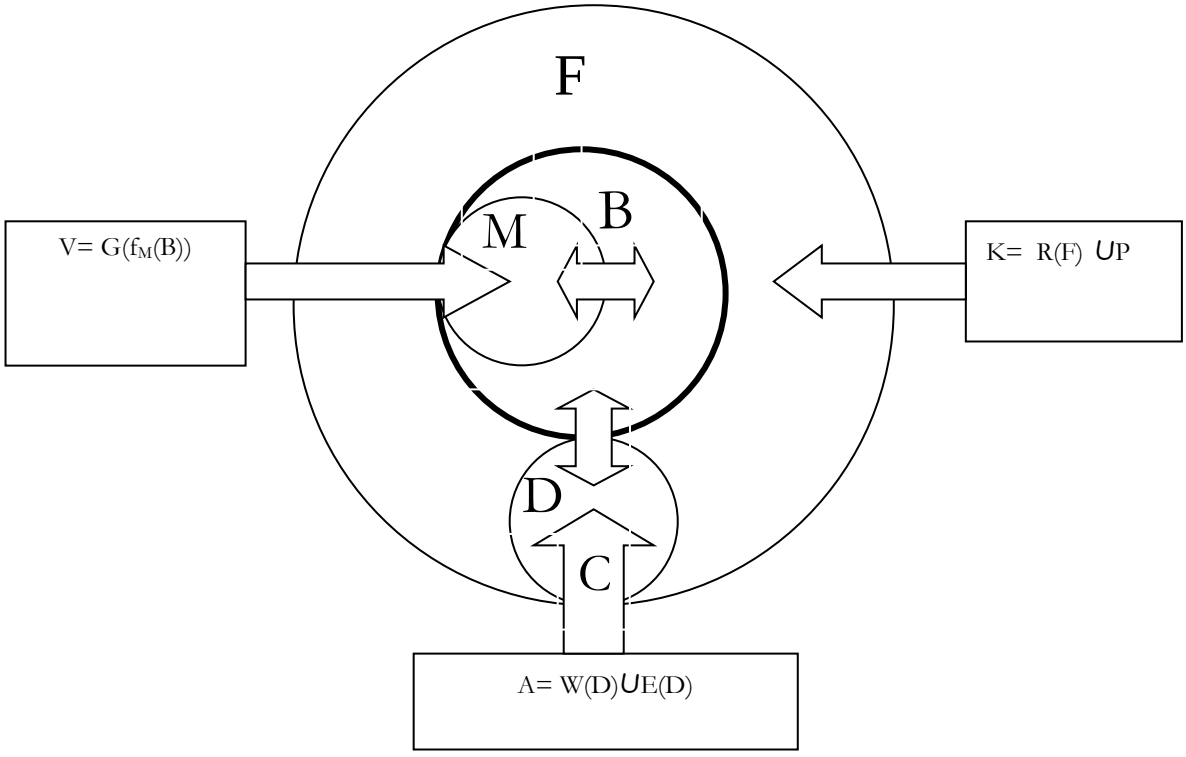


Рис. 1. Логічна модель відкритої системи дистанційного голосування

У цій моделі передбачено, що операційна система сервера ІГ (після певних процедур налаштування) дозволяє виконувати користувачам ті і тільки ті дії, що є елементами множини Q, де Q - об'єднання множин дій голосуючих виборців, адміністратора сервера ІГ та контролерів, які в сукупності складають повну групу можливих дій користувачів:

$$Q=V\cup A\cup K$$

де V – множина дій голосуючих виборців (ця множина у разі потреби може доповнюватись діями осіб для виконання спеціалізованих наперед відомих дій, що повинні бути відображені у заздалегідь відкритій прикладній програмі); A – множина можливих (штатних і нештатних) дій адміністратора сервера; K – множина дій контролюючих осіб.

Слід зауважити, що всі некоректні і помилкові дії тут не розглядаються, бо вони не сприймаються сервером.

Повна множина об'єктів, над якими можуть виконуватись дії користувачів, складається з таких множин: F – множина даних, що розміщені у файловій системі сервера, включаючи файли з програмами, готовими до виконання, а також з історією команд адміністратора; C – множина відображень команд адміністратора сервера, причому $C \subset F$, $f: C \to A$, де f – функція відображення; D – множина файлів у тій директорії, до якої має доступ адміністратор, причому $D \subset F$; B – множина даних в оперативній пам'яті прикладної програми сервера, причому $B \subset F$; M – множина даних для моніторингу звернень виборців (ці дані використовує прикладна програма для авторизації голосуючих виборців), причому $M \subset B$ (множина M у разі необхідності може доповнюватись діями осіб для виконання спеціалізованих наперед відомих процедур, що повинні бути відображені у заздалегідь відкритій прикладній програмі).

Множини дій користувачів над переліченими об'єктами описують такі вирази:

$$V = \{G_1(f_M(B)), \ldots, G_i(f_M(B)), \ldots, G_n(f_M(B))\},$$

де G_i – функція, яка відповідає і-му варіанту запиту виборця до сервера, $i = \overline{1, n}$; n – кількість варіантів запитів виборця до сервера (наприклад: голосування, отримання довідки про хід голосування тощо); f_M – функція моніторингу звернень голосуючих виборців до сервера;

$$A = W(D) \cup E(D),$$

тут W – функція, яка відповідає множині дій адміністратора (команді запису) для приєднання файлів до множини D; E – функція, яка відповідає діям адміністратора (команді) щодо запуску на виконання файлів (програм) з множини D;

$$K = R(F) \cup P,$$

де R – функція, яка відповідає множині дій щодо доступу контролерів для ознайомлення з об'єктами множини F, причому $C \subset F$, $D \subset F$; P – множина дій (команд) контролера щодо перевірки статусу процесів на сервері та отримання інших відомостей, які можуть свідчити про порушення політики безпеки.

Єдиний користувач, який має можливість виконання небезпечних дій на сервері, це – адміністратор сервера, бо будь-які дії виборців і контролерів не здатні утворити загрозу штатній роботі сервера. Тому, для запобігання можливим несанкціонованим діям, адміністратору дозволено виконувати тільки дві дії, а саме: заносити файли в свою директорію і запускати на виконання (тільки один раз) програму з цієї директорії. При цьому будь-яка нештатна дія адміністратора може бути зафіксована контролерами. Не існує таких дій, які можна було б приховати від контролерів. Представлена модель (див. рис. 1) за умов повної відкритості програмного забезпечення, включаючи операційну систему, дозволяє забезпечити досконалий захист критичних даних при обміні через середовище Інтернет, а також гарантує збереження таємниці голосів та неможливість фальсифікації результатів волевиявлення за умови повної недовіри до усіх без винятку користувачів системи. Крім того, як показано в роботі [5], така модель дозволяє застосовування методу протидії незаконному впливу на виборців. Головним досягненням відкритих систем дистанційного голосування є можливість їх повноцінного контролю з боку необмеженої кількості будь-яких осіб, а саме такого контролю, після проведення якого не повинно залишитись жодних підстав для недовіри щодо дійсності результатів волевиявлення і збереження таємниці голосів. З метою збереження досягнень відкритої системи не можна розміщувати на сервері для дистанційного голосування файли, які не є відкритими для ознайомлення, бо це позбавляє систему прозорості. А встановлення на цьому сервері додаткового програмного забезпечення для автентифікації осіб виборців буде ускладнювати процедуру спостереження за роботою сервера та перешкоджатиме проведенню повноцінного контролю. Тому розміщення на сервері дистанційного голосування додаткових засобів для розпізнавання осіб виборців є неприпустимим. Навпаки, слід максимально обмежувати функціональність цього сервера, видаляючи з нього усі зайві файли, з метою забезпечення прозорості для повноцінного контролю з боку спостерігачів. Таким чином, розміщення додаткових засобів для розпізнавання осіб виборців потребує додаткового сервера, який повинен сприймати ознаки виборців і обмінюватись даними з сервером для голосування.

Розглянемо технологічний цикл функціонування системи дистанційного голосування, зображений на рис. 2, з метою визначення часових інтервалів, у яких доцільно розпізнавання осіб виборців з використанням біологічних або інших додаткових ознак.

Рис. 2. Технологічний цикл функціонування системи голосування

На рис. 2 сірим тоном виділені процеси, які відбуваються на сервері ІГ, і прийнято такі скорочення назв періодів технологічного циклу: ППД – період підготовки даних про претендентів на дистанційне голосування; ППС – період підготовки сервера ІГ (встановлення ОС та програм загального користування); ППЗ – прикладне програмне забезпечення для дистанційного голосування; ПВЕБ – період введення електронних бюлетенів (в цей період запити виборців сервером не обслуговуються, а в дільничних списках виборців помічають тих, хто голосуватиме дистанційно, щоб не видавати їм паперові бюлетені). Проаналізуємо кожний з періодів технологічного циклу з метою визначення тих періодів, де є потреба у додаткових засобах розпізнавання осіб виборців.

В період підготовки даних про претендентів на дистанційне голосування необхідна особиста присутність виборців з паспортами. В цей період відбувається очна перевірка осіб виборців і занесення в базу даних відомостей про них та ознак, що необхідні для ідентифікації та автентифікації. Для зберігання цих даних використовується окремий сервер, який працює незалежно від сервера ІГ і може зберігати дані протягом багатьох голосувань.

В період підготовки сервера ІГ, крім встановлення ОС *OpenBSD* і пакетів *Node.js*, які забезпечують виконання програми на мові *Java Script*, створюють користувача *kontrol* з правами спостерігача (без права на внесення будь-яких змін на сервері), а також користувача *admin* з правами роботи виключно у директорії *home/admin* і блокують користувача *root* з повними правами. Після цього сервер буде працювати автоматично в режимі обмеженої функціональності, що дозволяє уникнути будь-яких спроб щодо зловмисного втручання в роботу сервера.

В період встановлення ППЗ адміністратор повинен занести в директорію *home/admin* такі три файли:

– файл з серверною програмою на мові *Java Script*;

– файл з клієнтською програмою на мовах *HTML* та *Java Script*;

– файл з даними, який формується по запиту адміністратора на окремому сервері для кожного голосування. Конфіденційні дані у цьому файлі знаходяться у зашифрованому вигляді.

З початку цього періоду кожен користувач мережі може отримати права на спостереження за усіма файлами і параметрами процесів на сервері ІГ. Це надає можливість впевнитись у тому, що все програмне забезпечення сервера ІГ є штатним, а потрібні дії адміністратора виконуються точно за графіком. Слід зауважити, що цей графік, а також все програмне забезпечення заздалегідь відкриті для проведення будь-яких експертиз.

В період введення паролів для дистанційного голосування виборці повинні пройти процедуру автентифікації. Слід зауважити, що в цей період згідно з виборчим законодавством [12] на основі Державного реєстру виборців (ДРВ) складаються, а потім уточнюються списки виборців. Тривалість підготовчого періоду зазвичай вкладається в 15 днів до виборів, бо раніше за законом можуть бути ще не створені дільничні комісії. Період введення паролів недоцільно розпочинати до створення виборчих дільниць, а оскільки збільшення цього періоду розширює інтервал часу для обрання виборцями зручного моменту проходження автентифікації, то зменшувати цей період теж недоцільно. В роботі [3] для введення паролю запропоновано приймати виборців у відділах ДРВ, де й проводити очну перевірку. Але завдяки дистанційній автентифікації не

обов'язковою стає очна перевірка, що особливо доцільно у разі тривалих відряджень виборців. Таким чином, саме в період введення паролів для дистанційного голосування існує потреба у додаткових засобах розпізнавання осіб виборців, щоб уникнути можливої підміни особи голосуючого.

В період введення електронних бюлетенів запити не обслуговуються, тому залишається проаналізувати тільки період голосування. В цей час виконуються найбільш відповідальні дії, але за допомогою нейтралізації незаконного впливу на виборців, як запропоновано в роботі [5], шансів примусити виборця голосувати всупереч власному розсуду не існує. Це може статись тільки тоді, коли сам виборець передасть свій вірний пароль для голосування іншій особі, при цьому виборець захищений тим, що має можливість передати зловмиснику помилковий пароль, бо система однаково реагує як на вірний, так і на помилковий пароль. Оскільки цей пароль вводять у відкритому вигляді, то сам виборець завжди побачить і виправить помилку. Через відкрите введення паролю не виникає небезпеки, бо пароль діє лише один раз і ним не можна скористатись вдруге. У разі виникнення сумнівів у виборця щодо точності пароля можна багато разів голосувати з різними паролями, але зараховано буде тільки один голос з вірним паролем.

Технологію отримання пароля для голосування у спеціалізованому пункті представлено на рис. 3.

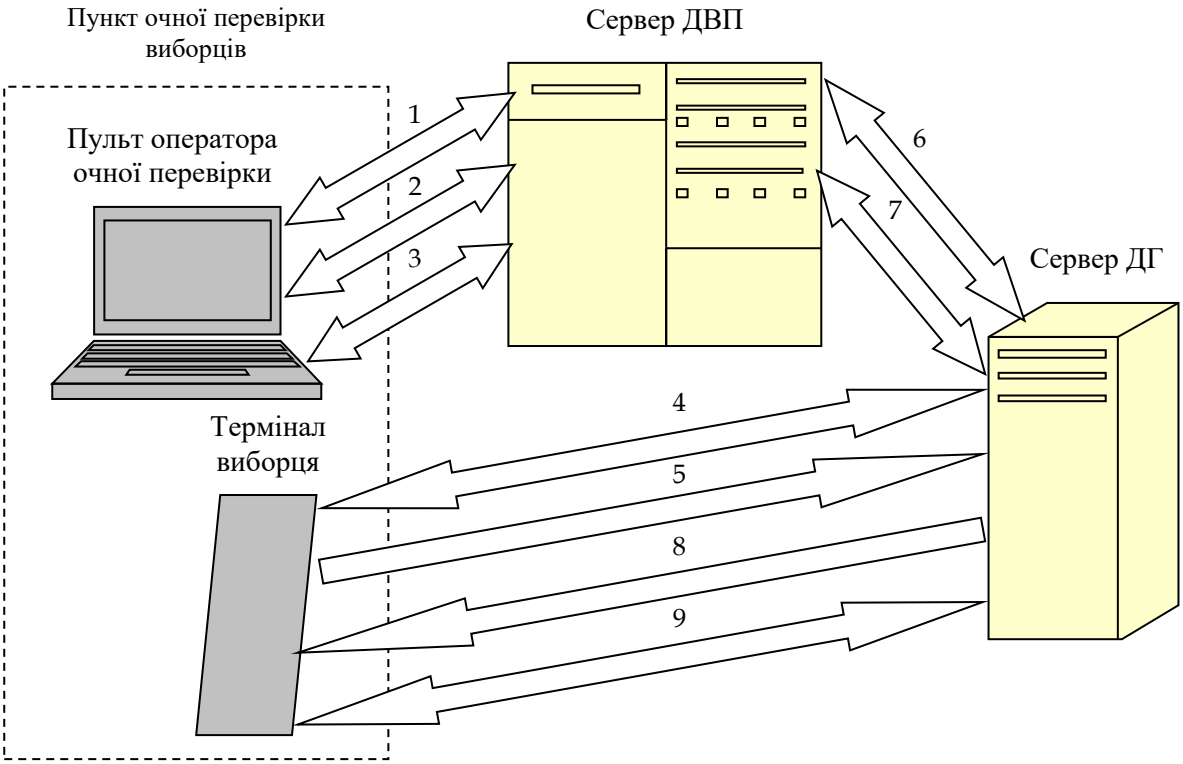


Рис. 3. Технологія отримання пароля для голосування у спеціалізованому пункті, де Сервер ДВП – сервер дозволу введення паролю

Ця технологія передбачає прибуття виборця з паспортом і, можливо, зі своїм мобільним терміналом до спеціалізованого пункту. Замість свого терміналу виборець може скористатись будь-яким іншим, наприклад, тим, що призначений для загального користування, але своєму він більше довірятиме. Після очної перевірки особи виконується така послідовність дій:

1. Оператор відправляє на сервер ДВП запит для утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
2. Оператор авторизується через захищене з'єднання та отримує дозвіл на відправку ідентифікатора виборця.
3. Оператор відправляє на сервер ДВП ідентифікатор виборця (після очної перевірки) і отримує повідомлення про надання 10 хвилин для введення паролю.
4. Виборець відправляє на сервер ДГ запит на утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
5. Виборець авторизується через захищене з'єднання на сервері ДГ і очікує дозвіл на відправку пароля.

6. Сервер ДГ утворює захищене з'єднання з сервером ДВП (через обмін ключами за алгоритмом Діффі-Геллмана).
7. Сервер ДГ відправляє на сервер ДВП запит з ідентифікатором виборця і, якщо момент запиту вкладається у виділені 10 хвилин, отримує відповідь з цим самим ідентифікатором.
8. Сервер ДГ відправляє на термінал виборця дозвіл для введення паролю.
9. Виборець відправляє на сервер пароль для голосування і отримує відповідь про успішне завершення процедури.

У разі, коли момент запиту (див. дію 7) не вкладається у виділені 10 хвилин, відповідь сервера ДВП замість ідентифікатора заповнюється нулями. При цьому виборцю замість дозволу для введення паролю відправляється відмова.

Введення сервера ДВП дозволяє при повному збереженні прозорості сервера ІГ доповнювати систему додатковими засобами дистанційного розпізнавання осіб виборців по голосу, по ЕЦП. Ці засоби встановлюються на сервері ДВП, який не потребує повної контрольованості (прозорості) в режимі реального часу, бо в період голосування, а тільки в цей період на сервері ІГ з'являється інформація, яка потребує абсолютного захисту, ніякої взаємодії між серверами ІГ і ДВП не відбувається. Тому на сервері ДВП можуть використовуватись традиційні засоби захисту інформації. Оскільки між обома серверами для кожного сеансу обміну даними утворюється спеціальний захищений канал зв'язку, то це дозволяє розміщувати їх незалежно один від одного в довільному місці мережі Інтернет. Запропонований в даній роботі розподіл дій між серверами ІГ і ДВП дозволяє виборцям отримувати пароль для голосування без обов'язкової очної перевірки. Кількість обраних виборцями додаткових ознак для автентифікації залежить тільки від можливостей придбання ними тих чи інших засобів для введення цих ознак. Запропонована технологія представлена на рис. 4.

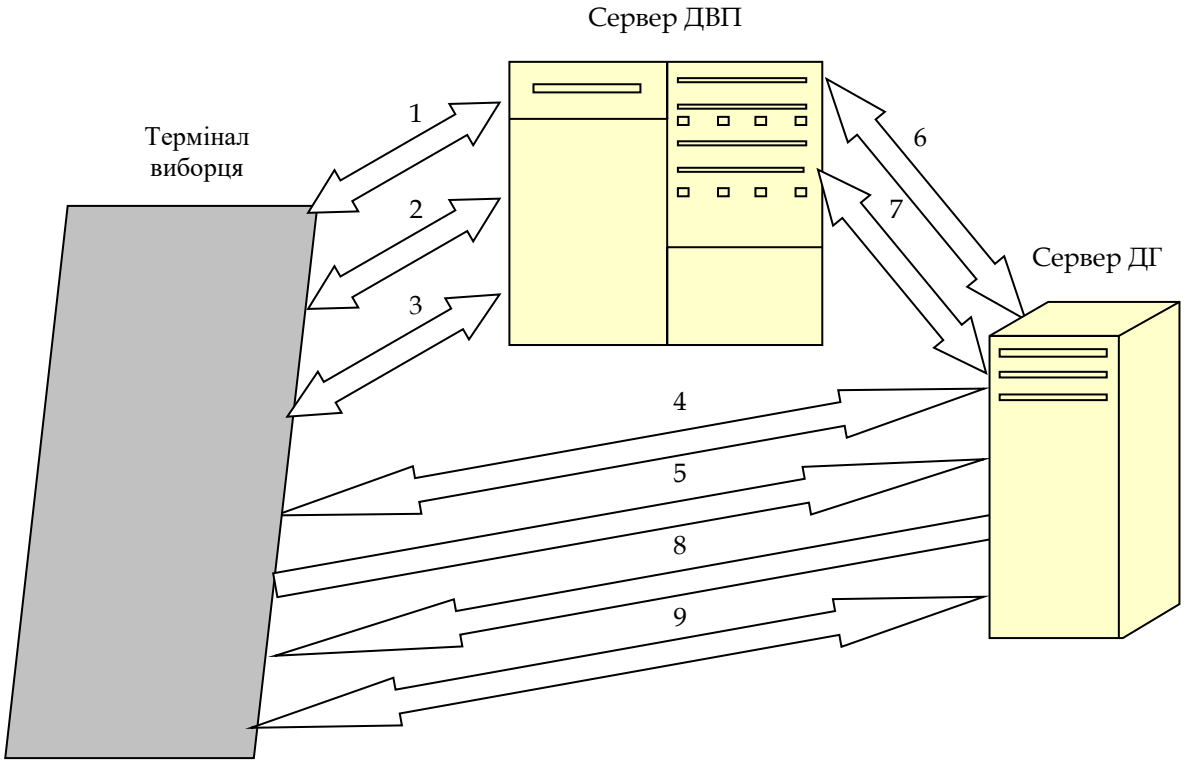


Рис. 4. Технологія отримання пароля для голосування без очної перевірки

Ця технологія передбачає наявність на сервері ДВП біологічних та/або інших ознак виборців, які заздалегідь повинні бути занесені в базу даних. Крім того, на сервері ДВП повинно бути встановлено програмне забезпечення для розпізнавання осіб виборців за цими ознаками в дистанційному режимі. При цьому для отримання пароля виконується така послідовність дій:

1. Виборець відправляє на сервер ДВП запит для утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
2. Виборець авторизується через захищене з'єднання та отримує запит на введення біологічних або інших додаткових ознак своєї особи.
3. Виборець виконує запит сервера ДВП щодо введення додаткових ознак та отримує повідомлення про вдалу автентифікацію і надання 10 хвилин для введення пароля. У разі невдалої

автентифікації виборець отримає запрошення на повторну спробу введення додаткових ознак. Слід зауважити, що кількість додаткових ознак може бути якою завгодно.

Дії 4 – 9 в точності збігаються з відповідними діями технології, розглянутої вище.

Таким чином, запропонована технологія автентифікації виборців у відкритій системі ІГ, за рахунок доповнення системи сервером ДВП, у якому розміщені засоби розпізнавання осіб виборців за додатковими біологічними або іншими ознаками, дозволяє створити більш зручні умови для виборців, не вимагаючи від них проходження обов'язкової очної перевірки перед кожним голосуванням, що особливо доцільно у разі тривалих відряджень виборців.

4. Висновки

1. Запропоновано технологію дистанційної автентифікації виборців для відкритої системи таємного голосування в мережі Інтернет, яка надає можливість позбутися обов'язкової очної перевірки осіб виборців перед кожним актом волевиявлення, що особливо доцільно у разі тривалих відряджень виборців. При цьому збережено усі позитивні якості відкритої системи, включаючи повну контрольованість процесів на сервері Інтернет голосування в режимі реального часу, що усуває будь-які підстави для недовіри з боку виборців щодо збереження таємниці голосів або точності підрахунку.

2. Визначено найбільш доцільний період технологічного циклу виборчого процесу щодо дистанційної автентифікації осіб виборців з використанням біологічних (або інших) особистих ознак, а саме під час введення паролів для дистанційного голосування, що позбавляє можливості забороненої передачі свого права голосу іншій особі.

3. З метою захисту від будь-якого негативного впливу процесів, що пов'язані з автентифікацією, на роботу сервера Інтернет голосування, запропоновано для виконання цих процесів ввести окремий сервер дозволу введення пароля. При цьому між обома цими серверами для кожного сеансу обміну даними утворюється спеціальний захищений канал зв'язку, що дозволяє розміщувати їх незалежно один від одного в довільному місці мережі Інтернет.

4. Запропонована технологія надає можливість виборцям гнучкого вибору методів автентифікації, не позбавляючи їх можливості користуватись також і очною перевіркою. Обрання виборцями додаткових ознак для автентифікації залежить тільки від можливостей придбання ними тих чи інших засобів для введення обраних ознак.

Література: 1. http://e-lected.blogspot.com/search?updated-min=2014-01-01 T0 0:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00& max-results=50 2. http://www.electronic-vote.org 3. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування // Управління розвитком складних систем. 2014. Вип. 20. С. 110-115. 4. Чуприн В.М. Захист операційного середовища систем Інтернет голосування./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // Захист інформації. 2017. Т. 19, №1 – С. 56-66. 5. Чуприн В.М. Метод протидії незаконному впливу на виборців у системі Інтернет голосування / В.М. Чуприн, В.М. Вишняков, М.П. Пригара // Безпека інформації. – 2017. Т. 19, №1. С. 7-14. 6. https://github.com/vvk-ehk/evalimine 7. Брагина Е.К., Соколов С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития. // Вестник АГТУ. 2016. № 61. С. 40–45. 8. Daugman J.Information Theory and the Iris-Code. IEEE Trans. Info.Foren.Sec 11(2), 2015. – P. 400-409. 9. Тассов К. Л., Дятлов Р. А. Метод идентификации человека по голосу. Инженерный журнал: наука и инновации, 2013, Вып. 6. 10 с. 10. Матвеев Ю. Н . Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». 2012. С. 46-61. 11. Назарук В.Д. Технології обміну даними дистанційних електронних виборів / В.Д. Назарук, О.А. Хоменчук // Захист інформації. 2016. Т. 18, №4. С. 10-15. 12. Постанова Центральної виборчої комісії від 25 вересня 2015 року № 370 «Про Роз'яснення щодо складання та уточнення списків виборців для підготовки і проведення голосування з місцевих виборів».

Transliterated bibliography:

1. http://e-lected.blogspot.com/search?updated-min=2014-01-01 T0 0:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00& max-results=50

2. http://www.electronic-vote.org

3. *Vy`shnyakov V.M., Pry`gara M.P., Voronin O.V.* Vidkry`ta sy`stema tayemnogo golosuvannya // Upravlinnya rozvy`tkom skladny`x sy`stem. 2014. Vy`p. 20. S. 110-115.

4. *Chupry`n V.M.* Zaxy`st operacijnogo seredovy`shha sy`stem Internet golosuvannya / V.M. Chupry`n, V.M. Vy`shnyakov, M.P. Pry`gara // Zaxy`st informaciyi. 2017. T. 19, #1. S. 56-66.

5. *Chupry`n V.M.* Metod proty`diyi nezakonnomu vply`vu na vy`borciv u sy`stemi Internet golosuvannya / V.M. Chupry`n, V.M. Vy`shnyakov, M.P. Pry`gara // Bezpeka informaciyi. 2017. T. 19, #1. S. 7-14. 6. https://github.com/vvk-ehk/evalimine

7. *Bragina E.K., Sokolov S.S.* Sovremennye metody biometricheskoj autentifikacii: obzor, analiz i opredelenie perspektiv razvitija // Vestnik AGTU. 2016. № 61. S. 40–45.

8. *Daugman J.* Information Theory and the Iris-Code. IEEE Trans. Info.Foren.Sec 11(2), 2015. P. 400-409.

9. *Tassov K.L., Djatlov R.A.* Metod identifikacii cheloveka po golosu // Inzhenernyj zhurnal: nauka i innovacii. 2013, Vyp. 6. 10 c. DOI: 10.18698/2308-6033-2013-6-1103

10. *Matveev Ju.N.* Tehnologii biometricheskoj identifikacii lichnosti po golosu i drugim modal'nostjam // Vestnik MGTU im. N. Je. Baumana. Ser. «Priborostroenie». 2012. S. 46-61.

11. *Nazaruk V.D.* Texnologiyi obminu dany`my` dy`stancijny`x elektronny`x vy`boriv / V.D. Nazaruk, O.A. Xomenchuk // Zaxy`st informaciyi. 2016. T. 18, #4. S. 10-15.
12. *Postanova* Central`noyi vy`borchoyi komisiyi vid 25 veresnya 2015 roku # 370 «Pro Roz'yasnennya shhodo skladannya ta utochnennya spy`skiv vy`borciv dlya pidgotovky` i provedennya golosuvannya z miscevy`x vy`boriv».

Надійшла до редколегії 12.05.2018
Рецензент: д-р техн. наук, проф. Бараннік В.В.

Мачалін Ігор Олексійович, д-р техн. наук, проф., директор Навчально-наукового інституту Аеронавігації, електроніки та телекомунікацій Національного авіаційного університету, Наукові інтереси: експлуатація та проектування інформаційно-телекомунікаційних систем. Хобі: музика. Адреса: Україна, 03054, Київ, пр. Космонавта Комарова, 1,
e-mail: igor.machalin@ukr.net
Вишняков Володимир Михайлович, канд. техн. наук, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури. Наукові інтереси: захист інформації в комп'ютерних мережах, криптографія. Хобі: Інтернет. Адреса: Україна, 03037, Київ, пр. Повітрофлотський, 31,
e-mail: volodymyr.vyshniakov@gmail.com
Комарницький Олег Олександрович, головний спеціаліст, Департамент інформаційно-комунікаційних технологій Київської міської державної адміністрації. Наукові інтереси: Інтернет технології. Хобі: спорт. Адреса: Україна, 01044, Київ, Хрещатик, 36, e-mail: komarnitskiy2012@gmail.com
Machalin Igor Alekseevich, Dr. Sc. (Ing), Prof., Director of the Educational and Scientific Institute of Aeronavigation, Electronics and Telecommunications of the National Aviation University, Research interests: operation and design of information and telecommunication systems. Khobi: music. Address: Ukraine, 03054, Kyiv, Cosmonaut Komarov Ave., 1,
e-mail: igor.machalin@ukr.net
Vyshniakov Volodymyr Mykhailovych, PhD in engineering, associate professor, Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture. Research interests: data protection. Khobi: Internet. Address: Ukraine, 03037, Kyiv, Povitroflotski Ave., 1,
e-mail: volodymyr.vyshniakov@gmail.com
Komarnitskiy Oleg Oleksandrovich, Chief Specialist, Department of Information and Communication Technologies of Kyiv City State Administration. Research interests: Internet technologes. Khobi: sport. Address: Ukraine, 01044, Kyiv, Xreshhaty`k., 36,
e-mail: komarnitskiy2012@gmail.com

УДК 519.713

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ІДЕНТИФІКАЦІЇ АУДІОСИГНАЛІВ В УМОВАХ ВПЛИВУ ХАОТИЧНИХ ІМПУЛЬСНИХ ЗАВАД

ЮДІН О.К., ЗЮБІНА Р.В.

Оцінюється ефективність розроблених методів ефективної ширини спектра та найбільшої інформаційної ваги основного тону в задачі ідентифікації диктора при наявних завадах. Визначено, що в результаті впливу хаотичних імпульсних завад можливість ідентифікації диктора в бігатоальтернативних задачах прийняття рішення різко знижується при збіганні частоти основного тону мовленнєвого сигналу і початкової частоти імпульсної завади для методу найбільшої інформаційної ваги основного тону. Метод ефективної ширини спектра забезпечує високі показники ідентифікації в умовах впливу такого типу завад для текстозалежної ідентифікації.

Ключові слова: частота основного тону, методи ідентифікації, хаотичні імпульсні завади, ймовірність ідентифікації.

Key words: frequency of the main tone, identification methods, chaotic impulse noise, probability of identification.

1. Вступ

Стрімкий розвиток інформаційних технологій вимагає розробки нових систем обробки, зберігання, відображення та реєстрації критичних інформаційних ресурсів. Впровадження сучасних інформаційних систем ідентифікації користувача в об'єктах інформаційної діяльності стає необхідним елементом забезпечення інформаційної безпеки підприємства та особистості.

Розроблені методи ефективної ширини спектра [1, 2] та найбільшої інформаційної ваги основного тону дозволяють проводити ідентифікацію диктора в умовах високого рівня завад. Однак для визначення якісних показників розроблених методів дослідження проводились при моделюванні завад за законом Гаусівського розподілу [3]. Використання такого шуму класичне в системах обробки мовленнєвих сигналів, однак зважаючи на те, що в основі розроблених методів лежать частотні характеристики формування мовленнєвого сигналу, доцільним було б врахувати можливу наявність завад іншого характеру. Відмінним видом завад є хаотичні імпульсні завади, які формуються з урахуванням початкової частоти. Використання хаотичної імпульсної завади з заданою частотою f_0 може вплинути на якість роботи методів ідентифікації та верифікації у випадку, коли вона точно збігається з частотою основного тону голосу диктора, який підлягає обробці. Таким чином отримаємо задачу оцінки якості розроблених методів в умовах наявності хаотичних імпульсних завад з частотою, що майже точно збігається з частотою основного тону голосу диктора $f_0 \approx f_{ЧОТ}$.

2. Основна частина

Математична модель хаотичної імпульсної завади має вигляд:

$$HIN = \sum_{k=0}^{N_n-1}\sum_{n=0}^{N_u-1} f\left[\begin{array}{l} t_з + \frac{T_n}{N_u}\cdot n + P\cdot k \le t_i < t_з + \frac{T_n}{N_u}\cdot(n+1) + P\cdot k, \\ f\left\{\begin{array}{l} rnd(1) \ge 0.5, \\ Sm\cdot A\cos\left[2\pi f_0 t_j + \varphi_n\big|_{\varphi_n = X_n norm(N,M,D)}\right], \\ 0 \end{array}\right\} \\ 0 \end{array}\right]$$

де $t_з$ – інтервал затримки кодової конструкції; N_u – кількість імпульсів; T_n – тривалість кодової конструкції; N_n – кількість конструкцій; P – період повторень конструкцій; φ_n – випадковий фазовий зсув, який генерується випадковим чином [4].

В результаті маємо часове представлення згенерованих хаотичних імпульсів, які будуть виступати як завади.

Результатом додавання інформаційного сигналу $Sh02$ та створеної послідовності завад стала адитивна суміш $Sh01$ (рис.2.)

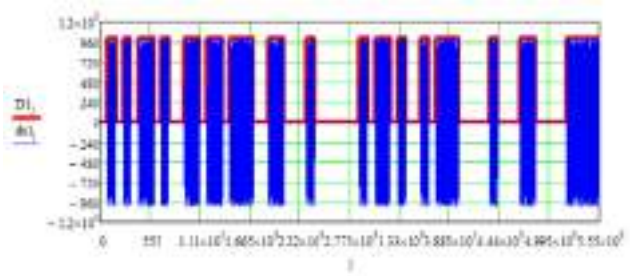


Рис.1. Часове представлення згенерованої послідовності випадкових імпульсних завад

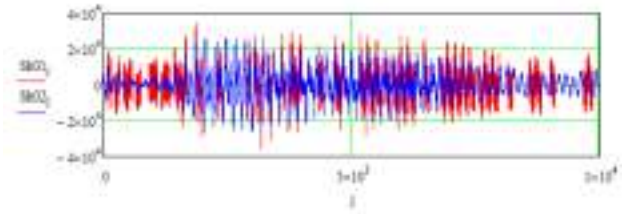


Рис. 2. Часове представлення адитивної суміші $Sh01$ та інформаційного сигналу $Sh02$

Для оцінки якості розроблених методів ефективної ширини спектра та найбільшої інформаційної ваги частоти основного тону було обрано показники співвідношення SNR, які обраховувались для оцінки ефективності розроблених методів при використанні білого шуму (табл. 1, 2).

Таблиця 1

Визначення ймовірності вірної ідентифікації диктора в багатоальтернативних задачах підтримки прийняття рішення при $H = 8$

SNR, дБ	Метод ефективної ширини спектра		Метод найбільшої інформаційної ваги основного тону	
	Текстозалежна ідентифікація	Текстонезалежна ідентифікація	Текстозалежна ідентифікація	Текстонезалежна ідентифікація
– 2,9	1	0,22	0,34	0,079
– 5,23	1	0,275	0,335	0,127
– 6,67	0,99	0,25	0,3	0,05
– 7,88	0,99	0,22	0,29	0,14
– 8,9	0,99	0,216	0,258	0,15
– 10,18	0,96	0,109	0,25	0,14
– 11,52	0,94	0,22	0,202	0,08
– 12,65	0,79	0,16	0,205	0,12
– 14,6	0,63	0,12	0,185	0,12
– 16,15	0,57	0,094	0,18	0,12

Таблиця 2

Визначення ймовірності вірної ідентифікації диктора в багатоальтернативних задачах підтримки прийняття рішення при $H = 6$

SNR, дБ	Метод ефективної ширини спектра		Метод найбільшої інформаційної ваги основного тону	
	Текстозалежна ідентифікація	Текстонезалежна ідентифікація	Текстозалежна ідентифікація	Текстонезалежна ідентифікація
– 2,9	1	0,139	0,18	0,15
– 5,23	1	0,25	0,23	0,25
– 6,67	0,99	0,35	0,24	0,26
– 7,88	0,99	0,33	0,35	0,18
– 8,9	0,99	0,304	0,325	0,21
– 10,18	0,98	0,27	0,36	0,315
– 11,519	0,84	0,114	0,32	0,17
– 12,65	0,84	0,19	0,23	0,17
– 14,6	0,47	0,07	0,197	0,114
– 16,15	0,37	0,1	0,226	0,18

У випадку, коли у експерименті бере участь 8 гіпотез, показники вірної ідентифікації свідчать про високі результати при використанні методу ефективної ширини спектра (МЕСШ), так як порівняння гіпотез проходить шляхом аналізу і послідовного перебору всіх інформативних складових спектра, і тільки для текстозалежної ідентифікації.

У випадку методу найбільшої інформаційної ваги основного тону (МНІВОТ) при такій кількості гіпотез метод не справляється з поставленою задачею. Основною причиною таких результатів є залежність від частоти основного тону $f_{ЧОТ}$, яка у даному випадку приблизно дорівнює f_0.

Таким чином, використання методу найбільної інформаційної ваги основного тону не є ефективним для ідентифікації диктора в умовах наявності хаотичних імпульсних завад в інформаційній системі надання ІТ послуг.

Наглядний результат роботи розроблених методів для $H = 8$ представлено на рис. 3.

Використання розроблених методів для багатоальтернативної задачі ідентифікації диктора в умовах наявних хаотичних імпульсних завад при $H = 6$ (рис. 4) показало, що як і в попередньому експерименті високі показники дає метод ефективної ширини спектра для текстозалежної ідентифікації, а у випадку методу найбільшої інформаційної ваги основного тону ідентифікація залишається малоймовірною в зв'язку із значним впливом завади на частоту основного тону.

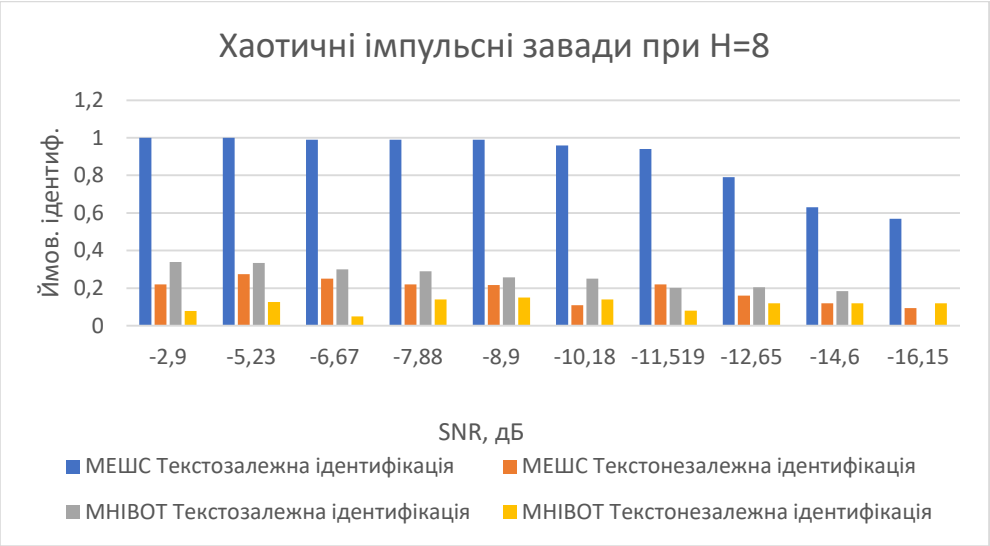


Рис. 3. Показники ймовірності вірної ідентифікації диктора при хаотичних імпульсних завадах розробленими методами при $H = 8$

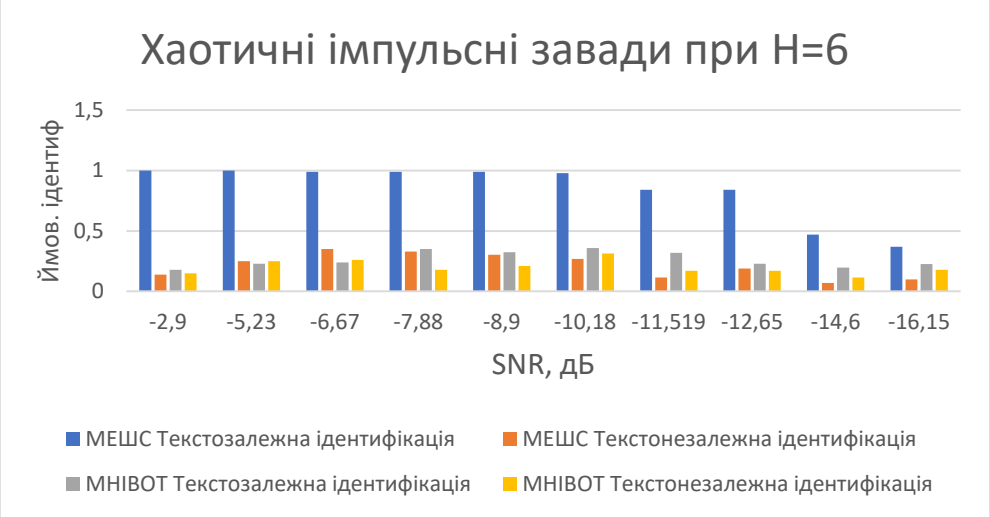


Рис. 4. Показники ймовірності вірної ідентифікації диктора при хаотичних імпульсних завадах розробленими методами при $H = 6$

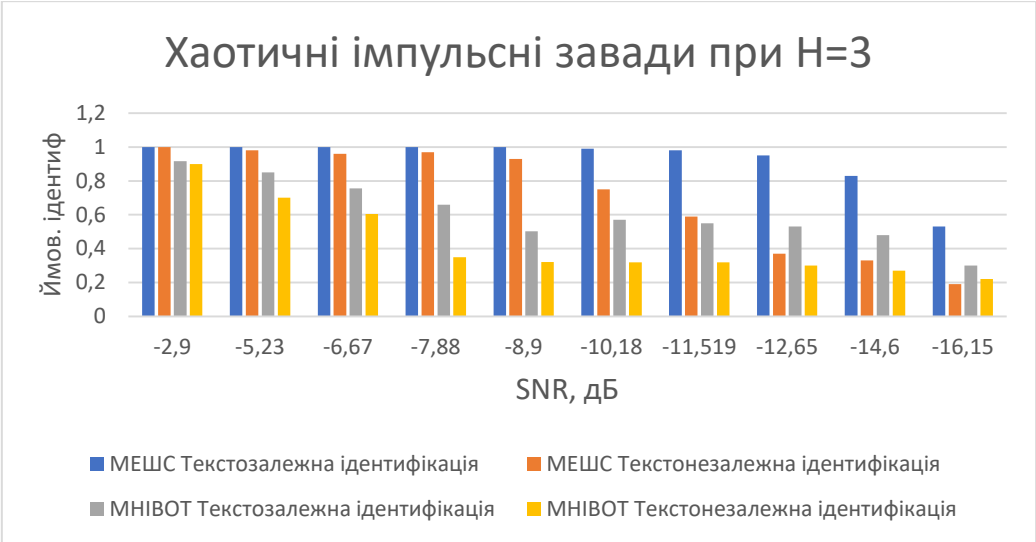


Рис. 5. Показники ймовірності вірної ідентифікації диктора при хаотичних імпульсних завадах розробленими методами при $H = 3$

Що стосується визначення ймовірності вірної ідентифікації диктора в багатоальтернативних задачах підтримки прийняття рішення при $H = 3$ (табл. 3), то в даному випадку методи дають можливість проводити точну ідентифікацію в умовах, коли $SNR = -10{,}18$ дБ для текстозалежної і при $SNR = -2{,}9$ дБ для текстоненезалежної ідентифікації методом ефективної ширини спектру. Для методу найбільшої інформаційної ваги основного тону показник $SNR = -2{,}9$ дБ дає можливість провести ідентифікацію з точністю 90% для текстонезалежної та з точністю 91% для текстозалежної ідентифікації (рис. 5).

Таблиця 3

Визначення ймовірності вірної ідентифікації диктора в багатоальтернативних задачах підтримки прийняття рішення при $H = 3$

SNR, дБ	Метод ефективної ширини спектра		Метод найбільшої інформаційної ваги основного тону	
	Текстозалежна ідентифікація	Текстонезалежна ідентифікація	Текстозалежна ідентифікація	Текстонезалежна ідентифікація
– 2,9	1	1	0,917	0,9
– 5,23	1	0,98	0,85	0,7
– 6,67	1	0,96	0,755	0,604
– 7,88	1	0,97	0,66	0,35
– 8,9	1	0,93	0,502	0,321
– 10,18	0,99	0,75	0,57	0,32
– 11,519	0,98	0,59	0,55	0,32
– 12,65	0,95	0,37	0,53	0,3
– 14,6	0,83	0,33	0,48	0,27
– 16,15	0,53	0,19	0,3	0,22

3. Висновок

Проведена оцінка ефективності розроблених методів дає можливість зробити висновок, що високі показники ідентифікації аудіосигналів у багатоальтернативних задачах підтримки прийняття рішення в інформаційних системах забезпечуються особливостями обраного простору ознак для певних видів завад. Наявність Гаусівського шуму в каналі зв'язку дає можливість текстозалежної ідентифікації з ймовірністю 98% при $H = 8$ та $H = 6$ навіть у випадку, коли шум перевищує сигнал у 1,67 разів, а для текстозалежної – у 1,1 разу. Метод найбільшої інформаційної ваги основного тону дає такі показники для $H = 8$ та $H = 6$ у випадку, коли шум перевищує сигнал у 1,43 разу для текстонезалежної ідентифікації, а для текстозалежної ймовірність 96% вірної ідентифікації забезпечується, коли сигнал перевищує шум в 1,1 разу. Звичайно, особливість формування хаотичних імпульсних завад значно впливає на показники ідентифікації диктора шляхом використання розроблених методів, так як з простору ознак мовленнєвого сигналу було обрано саме частоту основного тону, а збігання її з початковою частотою формування імпульсів значно змінює інформаційні складові спектрального представлення сигналу, в тому числі і амплітуди обертонів мовленнєвого сигналу. Однак, незважаючи на такий вплив, методи продемонстрували високу ефективність при $H = 3$ і дали можливість ідентифікувати мовленнєвий сигнал з ймовірністю більше 90% як для текстозалежного, так і для текстонезалежного випадку при перевищенні шумом використаного сигналу в 0,83 разу.

Література: 1. *Юдін О. К.,* Зюбіна Р. В. Метод ефективної ширини спектру //Наукоємні технології. 2018. Т. 37. №. 1. С. 55– 60. **2.** *Юдін О. К.,* Зюбіна Р. В. Класифікація методів ідентифікації частоти основного тону //Наукоємні технології 2017. Т. 33, №. 1. С. 13-21. **3.** *Юдін О. К.,* Зюбіна Р. В. Оцінка ефективності методів ефективної ширини спектру та найбільшої інформаційної ваги основного тону в задачах ідентифікації та автентифікації аудіо сигналів // Наукоємні технології 2017. Т. 35. №. 3. С. 209-214. **4.** *Антипенский Р.* Разработка моделей преднамеренных помех сигналам с дискретной модуляцией // Компоненты и технологии. 2007. №. 75. С. 138– 143.

Транслітерований список літератури.

1. *Judin O. K.,* Ziubina R. V. Metod efektyvnoi' shyryny spektru // Naukojemni tehnologii' 2018. T. 37, №. 1. S. 55– 60.

2. *Judin O. K.,* Ziubina R. V. Klasyfikacija metodiv identyfikacii' chastoty osnovnogo tonu // Naukojemni tehnologii' 2017. T. 33, №. 1. S. 13-21.

3. *Judin O. K.,* Ziubina R. V. Ocinka efektyvnosti metodiv efektyvnoi' shyryny spektru ta najbil'shoi' informacijnoi' vagy osnovnogo tonu v zadachah identyfikacii' ta avtentyfikacii' audio sygnaliv // Naukojemni tehnologii'. 2017. T. 35, №. 3. S. 209-214.

4. *Antypenskyj R.* Razrabotka modelej prednamerennыh pomeh sygnalam s dyskretnoj moduljacyej // Komponentы y tehnologyy. 2007. №.75. S. 138– 143.

Надійшла до редколегії 24.05.2018

Рецензент: д-р техн. наук, проф. Бараннік В.В.

Юдін Олександр Костянтинович, д-р техн. наук, проф., директор Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету. Наукові інтереси: інформаційні технології, інформаційна безпека. Адреса: м. Київ, пр. Космонавта Комарова, 1, тел. 406-70-08.

Зюбіна Руслана Віталіївна, ст. викладач кафедри комп'ютеризованих систем захисту інформацій Національного авіаційного університету. Наукові інтереси: інформаційні технології, інформаційна безпека. Адреса: м. Київ, пр. Космонавта Комарова 1, тел. 406-70-08.

Yudin Oleksandr K., Dr of Sc, Prof., Director of the Educational and Scientific Institute of Computer Information Technologies at the National Aviation University. Information technologies, information security. Address: Kyiv, 1 Kosmonavta Komarova av., tel. 406-70-08.

Ziubina Ruslana V., Senior Lecturer at the Department of Computerized Systems of Information Security at the National Aviation University. Information technologies, information security. Address: Kyiv, 1 Kosmonavta Komarova av., tel. 406-70-08.

УДК 658:512.011:681.326:519.713

АРХІТЕКТУРИ ТА МЕТОДИ КУБІТНОГО ЛОГІЧНОГО МОДЕЛЮВАННЯ КІБЕРСОЦІАЛЬНИХ ПРОЦЕСІВ

СОКЛАКОВА Т.І., АБДУЛЛАЄВ В.Г., ХАХАНОВ В.І.

Пропонуються моделі, структури даних, архітектури та методи логічного аналізу соціальних процесів, пов'язаних з підвищенням якості життя, збереженням екології планети і усуненням соціальних колізій. Вводяться кубітні структури даних, які описують багатозначні змінні, необхідні для створення еталонних зразків логічних архітектур, які задають поведінку громадян і соціальних груп. Пропонується квантовий метод кубітного моделювання інформаційних потоків для пошуку деструктивних процесів і явищ в соціальних мережах за ключовими словами і фразами. Розглядаються архітектури кіберфізичного соціального комп'ютингу на основі монторінгу контенту в соціальних мережах, моделювання даних на еталонних логічних схемах деструктивної поведінки людини з метою запобігання соціальних колізій за рахунок актюаторного управління поведінкою громадян. Архітектури, методи і засоби кубітного цифрового моделювання протестовані на реальних прикладах аналізу контенту, взятого з соціальних мереж. Показані можливі напрямки розвитку отриманих результатів, пов'язаних зі створенням кібермедичного, кіберюридичного, кібертранспортного комп'ютингу.

1. Вступ

Cyber social computing is the right decision making based on humanity history experience and nature laws. Фізичний світ з розвитком кіберпростору перетворюється з пануючого в підлеглий. Всі фізичні процеси і явища сьогодні мають власні цифрові образи, які поступово трансформуються в прообрази, а реальний світ стає все більш залежним від віртуального. Хто панує в кіберпросторі, той править і фізичним світом. Кіберфізичний світ позитивно з'єднує всіх жителів планети один з одним без посередників, завдяки соціальним мережам, хмарним сервісам і Edge Computing. Однак комп'ютингові технології роблять кіберфізичний світ уразливим з боку технічно і технологічно освічених громадян, у яких виникає намір здійснити протиправну дію. Позитивне в цьому випадку використання соціальних мереж для вичерпного моніторингу деструктивних намірів і дій громадян, які залишають кібервідбитки у віртуальному світі, що допомагають вирішити задачу ідентифікації кіберобразу протиправного процесу або явища за прийнятний час. Для цього необхідно створювати online cyber social computing з метою моніторингу та управління намірами громадян, а також профілактики і запобігання деструктивних дій по відношенню до людей і/або екосистеми планети. При цьому орієнтація на використання активного (квантового) соціального online комп'ютингу має за мету: 1) Створення паралельних квантових алгоритмів для метричного аналізу кубітних структур великих даних в процесі моніторингу кібервідбитків деструктивних намірів або дій громадян. 2) Актюаторне управління громадянами для профілактики і запобігання протизаконних акцій. 3) Запобігання терористичним актам, вбивствам, суїцидам на основі моніторингу та актюаторних впливів, включаючи залучення правоохоронних органів і спецслужб. 4) Запобігання варварським актам забруднення планети і локальних територій на основі моніторингу потенційно нечесних громадян і організацій. 5) Запобігання несанкціонованим мітингам, соціальним заворушенням, незаконним захопленням влади, революціям на основі моніторингу радикально налаштованих громадян і угруповань. 6) Формування соціального імунітету у вигляді кіберфізичного морального соціального комп'ютингу метричного вичерпного моніторингу всіх процесів і явищ для цифрового human-free управління громадянами на основі моделювання і передбачення наслідків від прийняття рішень. При цьому соціальні віруси: корупція, злодійство, тероризм, забруднення планети, народні хвилювання, революції, війни. 7) Розгляд інших видів комп'ютингу для актюаторного вирішення соцальних проблем. Кібермедичний комп'ютинг (КМК) – довічний моніторинг душевного і фізичного здоров'я кожної людини з моменту її народження з метою активного управління її поведінкою в форматі 24/7 для запобігання хворобам шляхом створення цифрового асистента, який допомагає приймати оптимальні рішення по стратегії і тактиці поведінки для забезпечення високої якості життя. КМК є альтенативою до стратегії сучасної медицини, що полягає в лікуванні хвороб, отриманих в результаті неправильного вибору повсякденних і довготривалих рішень, пов'язаних з незнанням функціональних особливостей свого організму та впливу на нього навколишньої дійсності. Запобігати хворобам шляхом моделювання можливих варіантів поведінки, а не передбачати їх (хвороби), забезпечувати якість життя, а не якість лікування на основі перманентного метричного моніторингу стану душі, тіла і навколишнього середовища з метою цифрового оптимального управління поведінкою людини. При цьому корекція природних помилок і отриманих травм є лише корисним доповненням до засобів забезпечення якості життя людини.

Бібліотека IEEE Xplore практично не має публікацій у напрямку Cyber Social Computing,

проте видавництво Springer має 13358 книг. При цьому IEEE Social Computing має 25342 роботи, а Springer представлений 41733 монографіями. Природно, що поєднання двох ринково-орієнтованих наукових напрямків може дати істотний практичний результат для підвищення якості життя і збереження екології планети. Існує тільки одна Springer-книга (Control of Cyber-Physical Systems), що побічно зачіпає питання активного кіберфізичного соціального комп'ютингу, пов'язаного з актюаторним управлінням соціальними процесами і явищами. Ринок поки по-старому використовує «дідівські настінні» системи відображення інформації, призначені для очей людини, якій властиві функції прийняття помилкових актюаторних рішень, що призводять до соціальних колізій, катастроф і воєн. Позбавлення людини від непосильної функції управління людством і передача її кіберфізичному соціальному комп'ютингу є найголовнішою організаційною проблемою морального креативного світу, від вирішення якої залежить існування людства і планети. Людина не здатна керувати навіть сама собою, забуваючи свій історичний досвід, вона постійно наступає на «граблі» помилок минулого. Тому громадянин, соціальна група, держава і людство потребують створення масштабованого аватару у форматі Gartner-computing: «virtual assistent – digital twin – smart robot», який позбавить їх від невірних рішень, що призводять до небажаних наслідків для душі і тіла кожного громадянина.

У роботі вирішуються питання, пов'язані зі створенням елементів кубітної теорії і архітектур кіберсоціального комп'ютингу для метричного моніторингу активності громадян і подальшого кубітного моделювання великих даних на логічних структурах з метою морального цифрового управління соціальними процесами, забезпечення якості життя і збереження екології планети.

Визначення. *Комп'ютинг* – галузь знань, яка займається розвитком теорії і практики надійного метричного управління віртуальними, фізичними і соціальними процесами і явищами на основі використання комп'ютерних дата-центрів і мереж, великих даних і цифрового моніторингу кіберфізичного простору за допомогою інтелектуальних пошуково-аналітичних сервісів, персональних гаджетів і розумних датчиків.

Комп'ютинг (рис. 1) – процес моніторингу (5) і актюації (6) метричних відношень (2) в інфраструктурі управління (3) і виконання (4) для досягнення і візуалізації (8) мети – продукції (1) при заданих ресурсах (7).

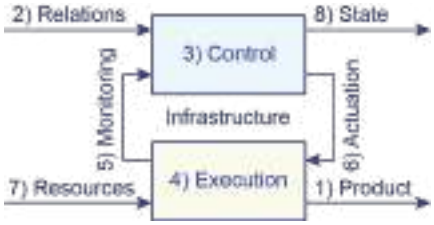


Рис. 1. Комп'ютинг

Метричне визначення комп'ютингу за допомогою восьми взаємопов'язаних компонентів надає теоретичну фундаментальну основу для формального і фактичного створення будь-якого процесу в заданій сфері людської або природної діяльності. Види комп'ютингу за введеною метрикою на окремих прикладах: космологічний, людський, біологічний, флористичний фізичний, віртуальний, квантовий, соціальний, державний, медичний, транспортний, інфраструктурний, науковий, освітній, виробничий, спортивний, відпочинку, подорожей, розваг.

Процес – взаємодія системних компонентів в часі і просторі для досягнення мети.

Явище – компонент процесу, що сприймається рецепторами, почуттями або розумом.

Процес – спостережувана взаємодія механізмів управління та виконання у часі і просторі на основі моніторингу та актюації метричних відносин для досягнення мети у вигляді продукції або сервісів при заданих ресурсах.

Аксіоми практично корисні для розуміння і використання комп'ютингу: 1) Комп'ютинг є процес розвитку явищ. 2) Всі є комп'ютинг і нічого крім нього. 3) Найпростіші два види комп'ютингу, доступні для розуміння і реалізації: read-write, speaking-listening. 4) Світ в процесах є детермінованим і цілеспрямованим. 5) Первинними є процеси, а не явища. Питання первинності курки чи яйця має однозначну відповідь: первинний процес або комп'ютинг взаємодії курки і яйця. 6) Будь-яке явище (курка, яйце) є продуктом комп'ютингу як процесу. 7) Хаос і ймовірність, як явище, є продукт нашого некомпетентного комп'ютингу (за Ейнштейном – фіговий листок на голому тілі нашого невігластва). 8) Еволюція за Дарвіном є комп'ютинг природних явищ у часі і просторі. 9) Первинними, за Кантором, є відносини, які породжують елементи. Елементів без відносин не існує. 10) Соціальний комп'ютинг є процес розвитку суспільних відносин в часі і просторі для досягнення цілей, поставлених політичною елітою.

Кіберсоціальний комп'ютинг (CSC) являє собою теорію і практику оцифрованих моральних, соціальних відносин для точного управління віртуальними, соціальними процесами і явищами на основі їх метричного онлайн-моніторингу з метою поліпшення якості життя людини і збереження екології планети.

Кіберсоціальний процес (CSP) є взаємодія в просторі і часі соціальних, фізичних і віртуальних компонентів, орієнторованих на досягнення поставленої мети.

Кіберсоціальна функціональність (CSF) являє собою структуру взаємопов'язаних логіч-них компонентів (елементів), яка забезпечує цифрову реалізацію еталонної поведінки об'єкта на заданій множині багатозначних змінних.

Кіберсоціальна (багатозначна) змінна (CSpA) являє собою повну і впорядковану множину примітивних значень, яка формує одну з проекцій поведінки об'єкта на векторі змінних, що формують процес або явище.

Кіберсоціальний (логічний) елемент (CSL) являє собою еталонну реалізацію багатозначної змінної в формі кубітного вектора, заданого {1,0} координатами на впорядкованій множині примітивних значень.

Значення (CSV) змінної – унікальна примітивна властивість об'єкта, що має пустий перетин з іншими примітивами, який в суперпозиції з ними становить універсум.

Таким чином, проглядається структурована ієрархія введених понять (рис. 2):

(CSC – CSP – CSF – CspA – CSL – CSV),

яка формує можливі архітектурні рішення кіберсоціального комп'ютингу.

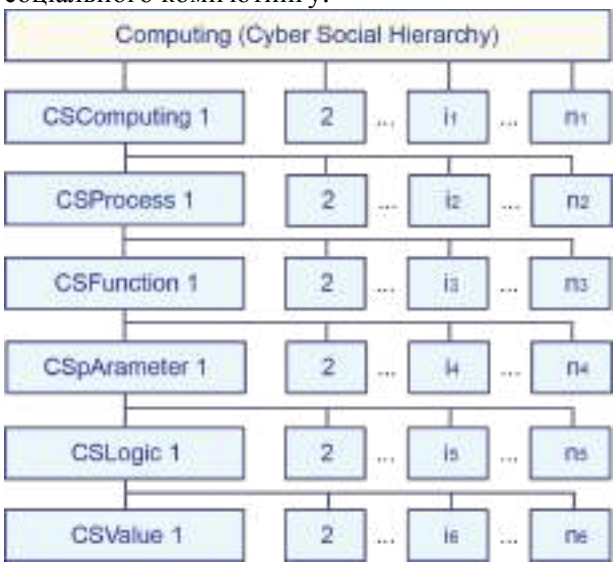


Рис. 2. Кіберсоціальний комп'ютинг, ієрархія

CSL-рівень архітектури характеризується синтезом логічної схеми, де кожен елемент має одну багатозначну змінну, яка фактично представлена кубітним вектором, де число одиничних значень може бути більше одиниці. Дана властивість кубіта дає можливість створювати компактні структури даних для їх паралельної обробки. Для виконання методу квантового моделювання на кубітних сруктурах даних необхідно унітарно закодувати вхідні вербальні дані за допомогою таблиць істинності універсумів примітивів, які відповідають кожній змінній.

Остання ототожнюється з ключовим словом, яке найбільш часто зустрічається у вхідному контенті. Набір таких keywords створює непересічну множину змінних в соціальному процесі, де їх значення представлені синонімами ключових слів, які формують багатозначність змінної як клас еквівалентності. Сукупність останніх створює простір кіберсоціального процесу, в якому визначаються еталонні, практично орієнтовані, функціональності кіберсоціального комп'ютингу у вигляді логічних кубітних схем для моделювання вхідних потоків даних із соціальних мереж або інших джерел.

Далі для спрощення і скорочення обсягу тексту вводиться абревіатура «С-», що означає кіберсоціальність процесу або явища.

Мета дослідження – розробка структур кіберфізичного соціального комп'ютингу, що використовує кубітні логічні моделі і методи аналізу великих даних, отриманих шляхом метричного моніторингу активності громадян, для морального цифрового управління соціальними процесами, забезпечення якості життя і збереження екології планети.

Задачі дослідження орієнтовані на створення моделей, методів і архітектур кіберсоціального комп'ютингу, спрямованого на автоматичний синтез і аналіз кубітних логічних схем для моделювання, моніторингу і управління соціальними процесами і явищами, а саме: 1) Архітектура memory-driven кіберфізичного комп'ютингу для синтезу та аналізу логічних секвенсорів, що моделюють соціальні процеси і явища з метою моніторингу та управління. 2) Кубітно-векторні моделі опису багатозначних логічних змінних для синтезу логічних секвенсорів, орієнтованих на аналіз кіберсоціальних процесів. 3) Кубітний метод синтезу логічних схем для моделювання кіберсоціальних процесів на основі унітарного кодування значень багатозначних змінних. 4) Кубітний метод аналізу кіберсоціальних процесів на основі використання еталонних логічних елементів з унітарним кодуванням багатозначних змінних. 5) Кубітно-регістровий метод моделювання кіберсоціальних процесів на основі логічних елементів з векторною формою унітарних кодів багатозначних змінних. 6) Тестування і верифікація кубітних моделей і методів кіберфізичного комп'ютингу на прикладах соціальних процесів, пов'язаних з наукою, освітою і поведінкою громадян.

2. Тенденції світової кіберкультури соціального комп'ютингу

Gartner тенденції світової кіберкультури [1-12] (рис. 3) формують технологічну основу для створення глобального кіберфізичного комп'ютингу в рамках технологічного укладу Internet of Things.

При цьому квантовий ком'пютинг розглядається як енергозберігаюче майбутнє цифрового світу, створюваного для підвищення якості життя і збереження екології планети. Зокрема, квантовий паралельний комп'ютинг і кубітні структури даних дозволяють спростити алгоритми в області cyber social computing і підвищити швидкодію програмних продуктів на класичних комп'ютерах.

Стратегічні тенденції в області цифрових технологій [1-5] протягом 2018 року приведуть до суттєвих дизрапцій, що надасть нові можливості розробникам корпоративної архітектури і конструктивних інновацій для створення конкурентних переваг при використанні нових трендів кіберкультури (рис. 4): 1) Автономні фізичні і віртуальні інтелектуальні та координовані речі. 2) Розширена (доповнена кіберпростором) соціальна аналітика прав і можливостей громадянина для вироблення актюаторних впливів. 3) AI-керованим проектування, розширений (доповнений – augmented) і автоматичний розробник. 4) Цифрові близнюки; цифровий образ організації або компанії. 5) Спроможні, взаємодоповнюючі один одного Edge Computing and Cloud Computing. Роль 5G у комунікаціях між кінцевими пристроями. 6) Досвід занурення у цифрову дійсність. Сприйняття змін в цифровому світі. Virtual and Augmented Reality підвищують продуктивність праці. Майбутнє залежить від охоплюючого досвіду сьогодення. 7) Використання Blockchain в соціальній схемі. 8) Smart Spaces. Розумні міські простори створення шляху. Інтелектуальний простір створення карти, а не напряму. 9) Цифрова етика і конфіденційність особистого життя. 10) Квантові обчислення; квантова безпека; розвиток і становлення квантового комп'ютингу. Застереження – поважайте QC, працюйте з обережністю.

В аналітиці експертів компанії Гартнер фігурують 35 параметрів, серед них майже половина - 16 трендів безпосередньо формує соціальну спрямованість комп'ютингових технологій. Цей факт свідчить про зміну напряму досліджень вчених-комп'ютерників у бік інженерного підходу до вирішення соціальних проблем, пов'язаних з моральним управлінням державами, соціальними групами, кожною людиною, зокрема, з метою усунення соціальних пороків, конфліктів, колізій, державних переворотів, війн і коорупції. Очевидно, що людина недосконала навіть при управлінні власною поведінкою. Практично будь-який керівник є концентрацію помилкових рішень, що призводять до соціальних і глобальних катастроф. Людину легко перепрограмувати на негативний бік поведінки (на ненависть, руйнування, грабунки, корупцію, вбивства) за наявності масових каналів прямого доступу до мозку індивідуума і відсутності фільтрів морального виховання, соціальної гігієни 10 заповідей Божих і прищепленого батьками імунітету проти численних соціальних вірусів зрілої (?) форми людства. На жаль, Humanity, як і людина, має власний геном розвитку, який в даний час інформує нас про можливе досягнення свого Евересту – піку досконалості, коли подальший рух в будь-який бік призводить до загибелі людства.

Питання полягає лише в тому, як продовжити фазу зрілості і старості людства. З досвіду відомо, що людина при ідеальному управлінні самим собою живе 100 років, з яких відраховуються роки, як розплата за помилки вибору в молодості. Людство, на щастя, не знає або не має свого циклу в передісторії, тому важко сказати, в якій фазі ми знаходимося, молодості – хочеться вірити, чи старості, де в обох фазах соціальний імунітет дає збої. Вибір рішення, виходячи з досвіду в історії – головна перевага кіберсоціального комп'ютингу. Cyber social computing is the right decision making based on humanity history experience and nature laws.

Порівняння технологічних карт (2017 і 2018) від компанії Гартнер [1, 2] дає можливість визначити зміни, пов'язані з появою нових дизрапцій, а також з відходом з ринку тих трендів, які не витримали випробування часом. Використовуючи назви трендів як ключові слова, неважко створити універсум примітивів і побудувати еталонний функціонал, щодо якого можна метрично вимірювати кіберкультуру процесів і явищ, вченого, студента і викладача, а також технологічну актуальність навчальних планів, освітніх стандартів, університетів і держави в цілому. Природно, що інтерес представляє і створення аналогічної локальної Гартнер-кривої для освітніх дисциплін університету шляхом опитування студентів як експертів за курсами навчання. Дана тест-акція дає можливість відстежувати ставлення одних і тих же студентів до курсів і викладачів у міру їх дорослішання в рамках придбання теорії і практики, а також робити миттєві зрізи студентських оцінок освітніх дисциплін на поточний момент.

Функція мети Q визначається конволюцією в мінімум (нуль) кіберфізичного простору за метрикою Ni (i = 1, n): соціальних колізій, конфліктів, протиправних та / або кримінальних дій щодо громадян і екології, корупції, державного перевороту, революцій, терористичних актів і воєн за рахунок часових T, апаратно-програмних W і матеріальних витрат M, необхідних для вичерпного моніторингу і цифрового управління соціальними процесами і явищами. Це дає можливість підвищити якість життя людини і зберег-

ти екологію планети за рахунок отримання багаторазової економічної ефективності E, пов'язаної з елімінацією втрат від соціальних і рукотворних екологічних потрясінь:

$$Q = \min \sum_{i=1}^{n} N_i \rightarrow E = \sum_{i=1}^{n} \left[\frac{N_i \times M_i^N}{(T_i \times M_i^T) + (W_i \times M_i^W)} \right]$$

Таким чином, інвестиції часових і фінансових ресурсів в кіберсоціальний комп'ютинг дають можливість людству поліпшити якість життя і екологію планети в глобальному масштабі, за наявністю мінімального рівня кіберкультури у політичних еліт держав.

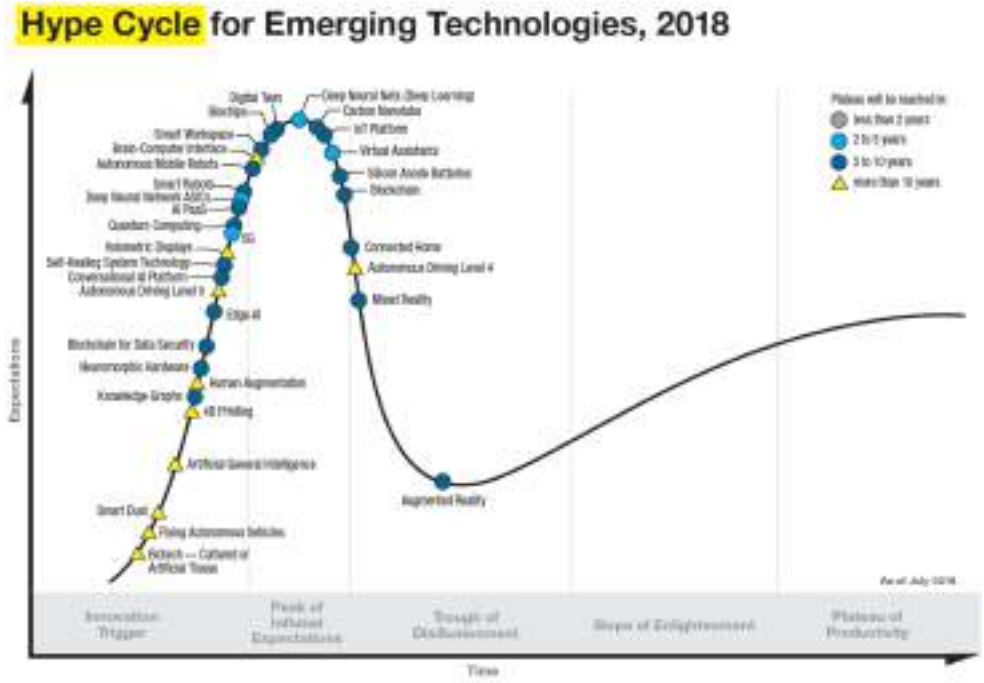


Рис. 3. Цикл компанії Gartner для дизрапторних технологій, 2018

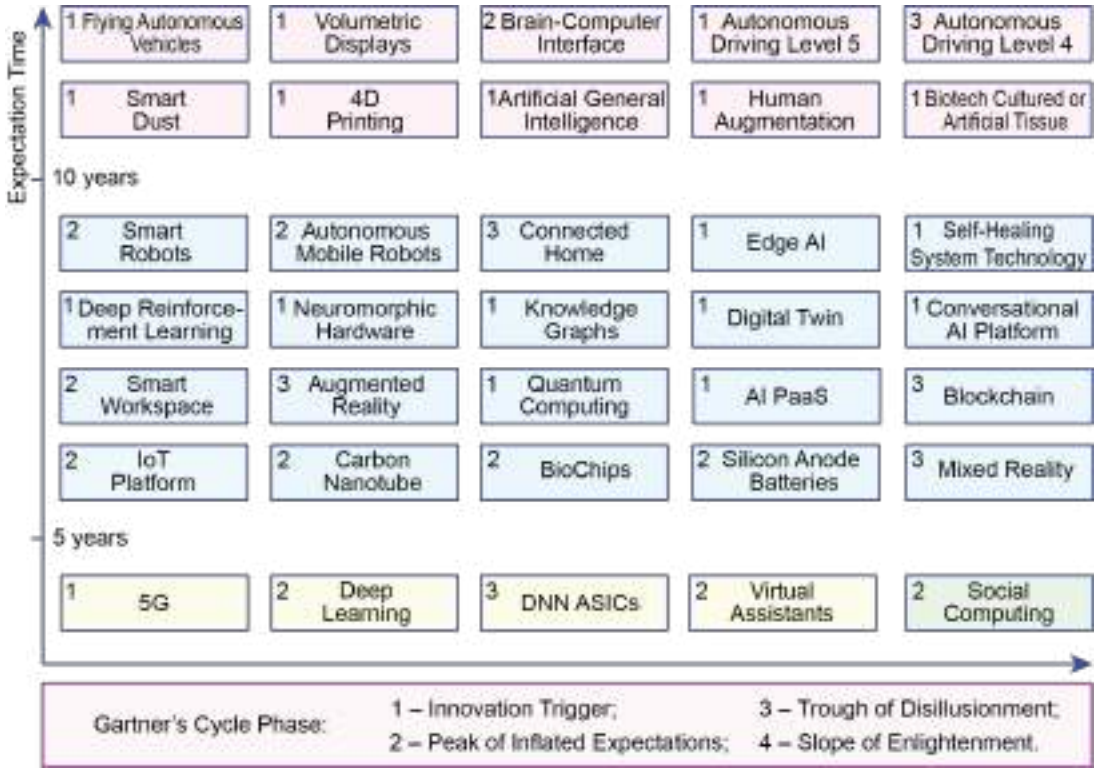


Рис. 4. 2018 Gartner's Table for Emerging Technologies

3. Кубітні моделі кіберфізичного соціального комп'ютингу

Пропонуються архітектури і класичні структури, пов'язані з кіберфізичним соціальним комп'ютингом (метричний моніторинг і цифрове управління), спрямованим на прийняття рішень, пошук і ідентифікацію великих даних, визначення функцій належності вхідних даних до заданого процесу чи явища на основі введеної метрики визначення відстаней. Всі моделі орієнтовані на схемотехнічну реалізацію методів і алгоритмів online моделювання з метою вироблення адекватних автоматичних актюаторних впливів без участі людини.

Логічні кубітні структури здатні розпізнавати вербальні повідомлення чи керування соціальними групами, що надходять на вхід комп'ютера, для досягнення поставлених цілей. Наприклад, необхідно ідентифікувати людину за метрикою параметрів: 1) Емоційність (вигуки, лайки, сміх, плач, загрози, безапеляційність, категоричність, рішучість). 2) Логічність (умовність, розсудливість, неповторюваність, послідовність, доказовість, альтернативність). 3) Креативність (уяву, парадоксальність, оригінальність, дивовижність). 4) Соціальність (дружелюбність, уважність, альтруїзм, дбайливість, чуйність). 5) Моральність (чесність, принциповість, законослухняність, самовідданість). 6) Компетентність (професіоналізм, здатність до навчання, енциклопедизм, майстерність, керованість, сила волі).

Кожен параметр може мати свою альтернативу (мультиверсність також допускається), тоді їх число подвоюється. Але можна використовувати тільки позитивні зразки, засновані на конструктивних параметрах або атрибутах. Такі образи – логічні процесори – формують еталонні якості особистостей: керівник, вчений, професор, конструктор, учитель, художник, лікар, артист.

Квантові технології паралельних обчислень використовуються для вирішення комбінаторних проблем, емулюючи обчислення на класичних комп'ютерах [13, 14]. З іншого боку, таблиці істинності або кубічні покриття для опису логічних елементів є неминучими ефективними структурами даних для вирішення проблем соціального комп'ютингу і пошуку необхідних даних [15, 16]. Автоматичний синтез кубітних покриттів функціональностей є одним з основних важко формалізованих завдань, без якого неможливо виконувати аналітику великих даних [17-20]. Для цих цілей далі вводиться аналітична модель W кубітно-логічного процесора кіберсоціального комп'ютингу, яка оперує двома матрицями: універсумів U примітивів і кубітних функциональностей Q, а також логічним примітивом L, інтегруючим функціональності в комбінаційну схему соціального процесора:

$$W = (U, Q, L),$$
$$U = (U_1, U_2, ..., U_i, ..., U_n);$$
$$\bigcup_{i-1}^{n} U_i = U;\ U_i \bigcap_{i,k=1,n}^{i\neq k} U_k = \varnothing;$$
$$Q = (Q_1, Q_2, ..., Q_i, ..., Q_n);$$
$$\bigcup_{i-1}^{n} Q_i = Q;\ Q_i \bigcap_{i,k=1,n}^{i\neq k} Q_k = \varnothing;$$
$$Q_i = (Q_{i1}, Q_{i2}, ..., Q_{ij}, ..., Q_{im});\ Q = [Q_{ij}];$$
$$U_i = (U_{i1}, U_{i2}, ..., U_{ij}, ..., U_{im});\ U = [U_{ij}];$$
$$L = f[Q] = (Q_1 \circ Q_2 \circ, ..., \circ Q_i \circ, ..., \circ Q_n)$$
$$\circ = \{\wedge, \vee, \oplus\};$$
$$U_{ij} \in U_i \in U;\ Q_{ij} \in Q_i \in Q;\ Q_i \in U_i;\ Q \in U;$$
$$Q_{ij} = 1 \leftarrow \max \mu(R, U_{ij}).$$

Метрика-універсум U тут виконує роль еталонного зразка для порівняльного аналізу з вхідним потоком даних R, що реалізується за допомогою аналізатора-компаратора, який видає максимальне значення функції належності, що трансформується в одиницю на відповідній координаті одного з кубітів $Q_{ij} = 1 \leftarrow \max \mu(R, U_{ij})$.

Архітектура метричної взаємодії U-матриці універсумів з потоком вхідних великих даних R для обчислення функцій належності μ(R, U), з метою отримання Q-матриці значень і подальшого L-об'єднання кубітів в комбінаційну схему кіберсоціального процесора, представлена на рис. 5.

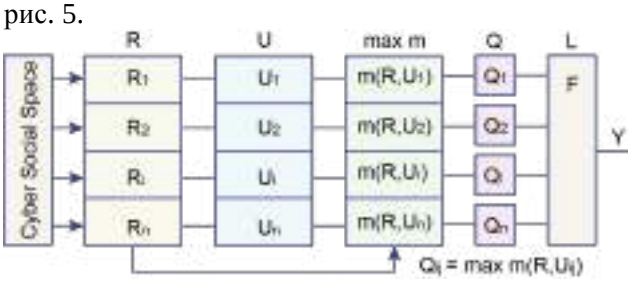


Рис. 5. Архітектура для синтезу кіберсоціального процесора

Тут вхідний потік модельованих великих даних R має такий же формат, як U-, Q-матриці і комбінаційна схема кіберсоціального процесора. Алгоритм синтезу Q-матриці полягає у визначенні максимального значення функції належності вхідного фрейму розглянутої змінної до одного з значень відповідного рядка матриці універсумів. В результаті такого порівняння по всіх координатах U-матриці формуються поодинокі координати кубітної матриці, де кожен рядок являє собою примітивну функціональність за розглянутою змінною. Всі разом рядки Q-матриці створюють комбінаційну схему логічного соціального процесора для моделювання будь-якого вхідного впливу з метою визначення його належності до даного еталону соціального процесу або явища. Наприклад, створивши за універсальною метрикою вченого конкретний

еталон-схему працівника на необхідну вакансію в університеті, шляхом моделювання можна визначити валідність кожного з претендентів у форматі заданих значень за кожним параметром (змінною). Процедура синтезу кубітів необхідна для тестування особистості, наприклад, на основі його вільного мовлення в заданому часовому інтервалі. В даному випадку всі слова надходять на входи одного або декількох універсум-елементів, що формують метрики життєдіяльності

$$U_{ij} \in U_i \in U;\ Q_{ij} \in Q_i \in Q;\ Q_i \in U_i;\ Q \in U;\ .$$

В результаті моделювання вхідного потоку великих даних формуються бінарні значення переваг індивідуума в кубітному векторі кожного логічного елемента, що відповідає одному параметру. Для цього використовується метричний вимір функції належності вербальних даних до кожного значення наперед заданого універсуму примітивів. Так, автоматично створюються кубітні вектори-зразки поведінки індивідуума. Легше це зробити вручну кожній людині при автозаповненні анкети, в якій він особисто визначає функції належності шляхом проставлення одиничок в тих полях універсуму, значення яких він вважає за краще. Формування повної множини параметрів соціального процесу або явища також пов'язано з аналітикою великих даних, спрямованою на отримання ключових понять-слів, що максимально віддалені одне від одного по метриці класів еквівалентності (кодовій відстані) і покривають всі функціональності-змінні життєдіяльності об'єкта. Слід зауважити, що універсум примітивів ототожнюється з класом непересічних еквівалентностей, що створюють всі можливі значення даної змінної-класу в той час, як множина еквівалентних класів відповідає універсуму змінних. Дані властивості використовуються при синтаксичному синтезі універсуму змінних, що покривають цифровий образ гранями, які формують заданий соціальний процес або явище.

Наприклад, необхідно синтезувати віртуального асистента (virtual assistent) або цифрового двійника (digital twin), або розумного робота (smart robot), який буде реагувати на зовнішні вхідні дані як конкретна людина. Алгоритм для створення аватара містить такі кроки: 1) Синтез універсуму змінних-примітивів, що покривають всі функціональності вченого (наука, освіта, волонтерство, лідерство, моральність, спорт, музика, культура, харчування, хобі). 2) Синтез U-матриці універсумів значень-примітивів, що покривають всі можливі варіанти кожної змінної, в рамках соціального процесу або явища. 3) Синтез Q-матриці конкретних значень-примітивів у форматі кубіта-вектора кожної змінної в рамках соціального процесу або явища. 4) Перевірка отриманої U-матриці універсумів соціального процесу або явища на повноту і примітивізм змінних і значень. 5) Перевірка отриманої Q-матриці функціональностей конкретних значень-примітивів у форматі кубіта-вектора кожної змінної в рамках соціального процесу або явища. U-матриця являє собою варіант метрики вченого (табл. 1).

Використовуючи дану U-матрицю, технологічно просто отримати такі варіанти матриці функціональностей у формі кубітних рядків-векторів, де поодинокі значення ідентифікують істинність величини змінної для конкретного вченого (табл. 2).

Після синтезу кубітних векторів за всіма параметрами в Q-матриці всі значення виходів кубітних елементів надходять на входи інтегратора L, що працює по функції and (може бути і інша функція, наприклад, not-and), який видає два значення {1,0}: позитивний або негативний результат моделювання, який можна інтерпретувати як бінарну функцію належності до еталону-функціональності, формує, наприклад, властивості вченого (керівника) університету.

Таким чином, logic-процесор, синтезований на основі використання Q-матриць квантових структур даних, здатний online моделювати будь-які соціальні процеси і явища, недоступні сьогодні для класичного комп'ютингу в базисі традиційних логічних елементів, зважаючи на складність формалізації поведінки людини або соціальної групи для синтезу цифрових моделей-схем.

Наприклад, заповнена анкета на посаду керівника є вхідним потоком даних для визначення валідності претендента на позицію, наприклад, ректора. При цьому сама анкета з критеріями оцінювання по кожному параметру є U-

Таблиця 1

Змінні:	Значення матриці універсумів вченого									
наука	проекти	дісертації	книги	статті	конфер.	н.метр	H-index	аспір	магістр	IEEE
освіта	лекції	стандарти	компл.	метод.	навч.	посіб	ДЕК	бакал	с.діпл	с. публ.
волонтерство	вн.лекц	агіт.р	вч.рада	ред.кол.	PC mem	опп.діс	семінар	орг.к	ізд.ж	с.стаж.
лідерство	зав.каф	декан	проріk	ректор	кер.нш	кер.пр.	кер.конф	кер.ради	орг.комп.	орг.лаб.
моральність	чесність	етично	благор	добродій	мораль	естетик	вдячність	відповід.	непідкупн.	пристойн.
спорт	футбол	баскет.	волейб	г.лижі	плаван	л.атлет	гімнаст	шахів	теніс	карате
музика	класичні	рок муз.	популяр	шансон	heavy m	hardrock	романси	бардів	оперети	народна
культура	тол.рос.	тол.укр.	тол.правос	тол.істор	тол.мов	ру.літ	укр.літ	зар.літ	ру.муз	укр.муз
харчування	борщ	суп	м'ясо	риба	овочі	фрукти	паста	каша	тістечка	солодощі
хобі	танці	подорожі	сауна	театр	кіно	кухня	фотогр.	риболовля	полювання	спів

матрицею або метрикою керівника, щодо якої відбувається моделювання вхідного потоку даних.

Таблиця 2

Змінні:	Значення матриці функціональностей (кубітів) вченого Х									
наука	1	1	1	1	1	1	1	1	1	1
освіта	1	0	1	1	1	1	1	1	1	1
волонтерство	1	1	1	1	1	1	1	1	1	1
лідерство	0	1	1	0	1	1	1	1	1	1
моральність	1	1	1	1	1	1	1	1	1	0
спорт	1	1	1	1	1	1	1	1	1	1
музика	1	1	0	1	1	1	1	1	1	1
культура	1	1	1	1	1	1	0	1	1	1
харчування	1	1	0	1	1	1	1	1	0	0
хобі	1	1	1	1	1	1	1	1	0	1

Змінні:	Значення кубітної матриці вченого Ч									
наука	1	1	1	1	1	1	1	1	1	1
освіта	1	0	1	1	1	1	1	1	1	1
волонтерство	0	1	0	1	1	0	1	1	1	0
лідерство	1	0	0	0	0	1	0	0	1	1
моральність	1	1	1	1	1	1	1	1	1	1
спорт	0	0	0	0	1	0	1	1	0	0
музика	1	1	1	1	1	0	1	1	1	0
культура	1	1	1	1	1	1	1	1	1	1
харчування	1	1	1	1	1	1	1	1	0	0
хобі	0	1	1	1	1	1	1	1	0	0

Змінні:	Значення кубітної матриці вченого С									
наука	0	1	1	1	1	0	1	1	1	1
освіта	1	1	0	0	0	0	0	0	0	0
волонтерство	0	0	0	0	0	0	1	0	0	1
лідерство	0	0	0	0	0	0	0	0	0	1
моральність	1	1	1	1	1	1	1	1	1	1
спорт	0	0	0	1	1	1	0	0	1	0
музика	1	0	1	0	0	0	0	0	0	0
культура	1	0	0	0	1	1	0	1	0	0
харчування	0	0	1	1	1	1	0	1	0	0
хобі	1	1	1	1	1	1	1	0	0	1

Природно, все це було раніше, коли кожен претендент на вакантну позицію заповнював листок з обліку кадрів, який відповідає Q-матриці функціональностей людини. Однак головна відмінність анкети в тому, що вона є застиглим відбитком діяльності людини в минулому і не здатна моделювати вхідні впливи для передбачення поведінки співробітника в майбутньому, що архіважливо для громадянина, соціальних груп, які обирають керівника підприємства, області, країни.

Формалізм створення еталон-схеми для соціального процесу або явища полягає у визначенні числа істотних параметрів, де всередині кожного з них генерується множина значень, унітарно кодованих для синтезу кубітного вектора логічного елемента. Логічні примітиви, відповідні істотним параметрам, об'єднуються за функціями (and, or, not, xor), які регулюють взаємні відносини між параметрами для формування кінцевого результату про валідності вхідного процесу або явища по відношенню до одного чи декількох стандартів.

Далі представлена метрика для ідентифікації фахівця, студента, яка може бути використана при прийомі на роботу в компанію (табл. 3).

Технологічно також просто створювати метричні матриці універсумів негативних процесів і явищ, надзвичайно важливих для правоохоронних органів, які повинні не розбирати наслідки неправомірних вчинків, а запобігати їм шляхом вичерпного моніторингу намірів громадянина і соціальних груп в кіберфізичному просторі. Наприклад, нижче представлена матриця поведінки негативного героя (табл. 4).

Соціальний (С) комп'ютинг - кібер-фізична система інтелектуального хмарного управління С-процесами на основі точного цифрового моніторингу: розумної електронної інфраструктури; співробітників компанії, оснащених комп'ютерами та персональними гаджетами; транзакцій і процесів, заданих в часі і просторі. Структура системи С-комп'ютингу представлена трьома взаємодіючими макрокомпонентами: хмарне інтелектуальне управління, електронна С-архітектура, кіберфізичний простір (рис. 6).

Таблиця 3

Змінні:	Значення матриці універсумів фахівця, студента				
емоційність	пристрасність	гарячність	збудливість	чутливість	темпераментність
логічність	розумність	зв'язність	зрозумілість	з'ясовна	правильність
креативність	здатність	фантазія	творчість	уява	творіння
соціальність	незамкнутість	networking	контактність	товариськість	сумісність
моральність	чесність	добродіяння	етичність	благородство	моральність
компетентність	грамотність	обізнаність	ерудованість	авторитетність	досвідченість

Таблиця 4

Змінні:	Значення матриці універсумів негативного «героя»				
антилогіка	запальність	гарячність	збудливість	незв'язність	нелогічність
антикультура	паління	алкоголізм	наркотики	неспортсмен	
некреативність	здатність	фантазія	творчість	уява	творення
антисоціальність	краде	обманює	продає	стукає	зраджує
некомпетентність	НЕграмотність	обізнаність	ерудованість	ненавч.	недосвідченість

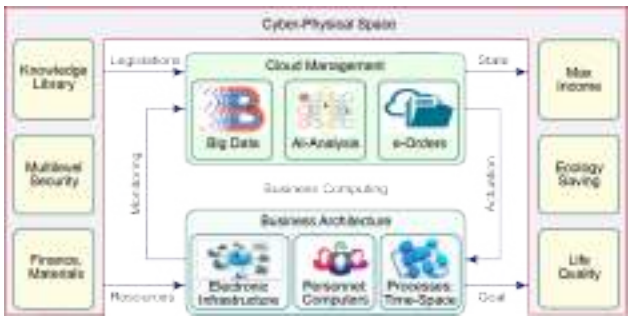


Рис. 6. С-комп'ютинг моніторингу та управління процесами

Хмарні компоненти-сервіси управління працюють за схемою: факт – оцінка – дія. Тут виконується знімання великих даних з різних розумних сенсорів і комп'ютерів, інтелектуальний аналіз даних на основі CNN, DNN, ML. Останнім компонентом хмарного сервісу є формування цифрових актюаторних впливів, орієнтованих на безпаперове управління інфраструктурами, компонентами, кадрами і кіберфізичними бізнес-процесами для досягнення мети (Goal) у вигляді отримання максимального прибутку, збереження екології планети і забезпечення високої якості життя співробітників. Вся система С-комп'ютингу безпосередньо взаємодіє з кіберпростором або інтернетом, який обов'язково є входом і виходом для створюваної структури. Крім того, входами є Legislations, які формують відносини в компанії, а також Resourses у вигляді фінансів і матеріалів, необхідних для створення продукції та / або сервісів. Важливим виходом системи є State, який ідентифікує стан розвитку бізнесу, імідж компанії у вигляді економічних і соціально-значущих показників.

С-комп'ютинг є технологією ефективного хмарного управління компанією для істотного зниження накладних непродуктивних витрат і підвищення прибутку, яка характеризується оперативним online моніторингом процесів і відділів на основі використання сучасної кіберкультури, що включає: IoT, Cyber Physical Systems, Cloud Computing, e-Infrastructure, Big Data Analytics, Artificial Intelligence, e-Dicument Circulation and Internet.

Принципи реалізації: 1) Моніторинг співробітників за допомогою впровадженого агента, в умовах інваріантності робочого місця по відношенню до геопозіції. Людина працює в подорожах, на відпочинку, в офісі. 2) Необхідно підключення всіх гаджетів і комп'ютерів працівника для створення повної картини його робочого і неробочого часу. Виникає сервіс самооцінки поведінки людини протягом доби: що він зробив, чого можна не робити, що не зроблено. 3) Моніторинг всіх пристроїв, пов'язаних з працівником, для інтелектуального аналізу і подальшого управління структурними компонентами бізнесу дає можливість оперативно приймати рішення по реконфігурації бізнес-процесів в реальному часі. 4) Моніторинг, замкнутий на online управління, без активної участі керівника. У цьому сьогодні головне і ще не вирішене завдання IoT-бізнесу. Від людського некомпетентного управління – всі біди на планеті.

Моніторинг без актюаторних впливів, що виробляються кіберфізичною соціальною системою, без участі людини, не представляє ринкового інтересу з позиції сучасної кіберкультури. Рішення проблеми цілком очевидне – створення кіберсоціальної системи моніторингу, але головне – online управління соціальними процесами на основі створення розумних алгоритмів або смарт-контрактів, що програмують легітимні відносини в компанії, університеті, державі. Програмний код реалізує тріаду соціальних подій, без участі чиновника: факт - оцінка - дія, яка модельно зводиться до кодування алгоритму обробки вхідних даних для отримання вихідних актюаторних впливів, спрямованих на компоненти кіберфізичної соціальної системи, яка виконується в рамках технологічного укладу IoT. Компонентами соціальної системи є: 1) Відносини, прийняті в компанії (державі) на основі існуючого законодавства, статуту (конституції), наказів, традицій, історії, культури. 2) Мета та / або напрямок руху компанії, зрозумілі для ринку, що мобілізують співробітників для якісного виконання завдань. 3) Цифровий менеджмент або управління компанією – секретний ключ ринкового успіху, - обов'язково використовує хмарні сервіси, які максимально виключають участь людини в моніторингу виробничих процесів і прийнятті рішень. 4) Інфраструктура підприємства, що забезпечує комфортні умови для конструктивної роботи, якісного харчування та активного відпочинку в форматі 24/7, в режимі onsite & remote online. 5) Кадри, що створюють ринкову продукцію та послуги, - головне надбання або інтелект будь-якої компанії, який оцінюється симетричною різницею компетенцій співробітників [17]:

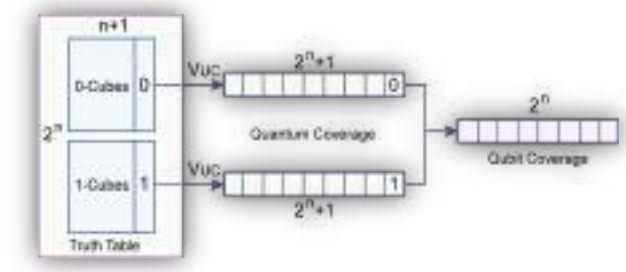
$$I = \bigoplus_{i=1}^{n} P_i = \bigcup_{i=1}^{n} P_i \leftarrow P_i \cap P_j = \varnothing;$$

$$I = \bigwedge_{i=1}^{n} P_i = \bigcap_{i=1}^{n} P_i \leftarrow P_i \underset{\forall i,j}{=} P_j.$$

4. Реалізація унітарно-кодованих структур даних

Інновація на основі сигнатурного аналізу. Інтерес представляє проблема аналізу великих даних з метою встановлення нових С-функціональностей на природному тлі вже певних. Аналогічна задача була вирішена в Лабораторії Касперського і вирішується досі засобами роботів і експертів в області malware and virus

аналітики. Тут використовується сигнатурний аналіз, адаптований до вірусної аналітики, який дозволяє мати досить компактний код-сигнатуру деструктивності з метою високопродуктивної ідентифікації в потоці даних старих вірусів. Це дає можливість акцентувати увагу робота-експерта на детальному аналізі нових деструктивностей з метою їх подальшого блокування. Перекладаючи згадану сигнатурну технологію на рішення проблем бізнес-аналітики, слід зазначити важливість отримання компактної таблиці бізнес-функціональності, інваріантної до часу. Першим кроком в цьому напрямку є мінімізація таблиці унітарного кодування С-функціональності за дозволеними логічними правилами (суперпозиція), які дають можливість отримати один стовпець, що ідентифікує С-функціональність. Структурні протиріччя при об'єднанні координат стовпців унітарно-кодованої матриці відсутні. Природно, що в результуючому стовпці-сигнатурі буде втрачена структурна інформація про порядок виконання сервісу, що є платою за компактність і швидкодію по ідентифікації стовпців С-функціональності. Однак структурна інформація не стирається і може бути затребувана в разі необхідності. Теоретичним підтвердженням і обгрунтуванням запропонованої суперпозиційної інновації зі стиснення стовпців в один є кодування будь-якої таблиці істинності двома і навіть одним кубітним вектором, отриманим за допомогою суперпозиції унітарних кодів вхідних впливів будь-якого, як завгодно складного цифрового пристрою (рис. 7).



a	b	c	Y
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

→

a	b	c	U – code	Y
0	0	0	10000000	0
0	0	1	01000000	1
0	1	0	00100000	1
0	1	1	00010000	0
1	0	0	00001000	1
1	0	1	00000100	0
1	1	0	00000010	0
1	1	1	00000001	1

→ $\bigvee_{\forall Y=1}$ $\bigvee_{\forall Y=0}$ →

0	1	1	0	1	0	0	1	1
1	0	0	1	0	1	1	0	0

Рис. 7. Конволюційний аналіз універсуму примітивів по кожній змінній

Обмеження: всі атрибути в матриці унітарного кодування, що підлягають суперпозиції по конкретних даних, повинні бути незалежними один від одного. Суперпозиція стовпців унітарної матриці дає можливість отримати покриття всіх атрибутів одиничними значеннями різноманітності даних. Якщо одиницями покриті в повному обсязі значення атрибутів, то існує некоректність в аналізі та кодуванні даних по конкретному атрибуту. У масштабах метрики значень інтегральний стовпець С-функціональності завжди буде являти собою підмножину з нульових і одиничних координат на тлі повністю одиничних значень інтегрального стовпчика універсуму $P \in R$ if $P \cap R = P$.

Суперпозіційна модель уявлення С-функціональності інваріантна до часу. Ідея класифікації полягає в порівнянні великих даних з інтегральним вектором, який виходить шляхом суперпозиції або об'єднання всіх стовпців С-функціональності

$$P = \bigcup_{i=1}^{n} P_i.$$

Процедура ідентифікації зводиться до операції перетину між стовпцем вхідних даних і інтегральним стовпцем С-функціональності: $S \in P \leftrightarrow S \cap P = S,$ яка повинна бути рівна вектору вхідних даних. Природно, виникнуть ситуації, коли не буде виконуватися наведена вище умова за всіма порівняннями за допомогою стовпців С-функціональності. Тоді слід використовувати таке правило мінімальної кодованої відстані по Хеммінгу:

$$S_i \in P_j \leftrightarrow \min(S_i \bigcap_{j=1}^{m} P_j = \varnothing), i = \overline{1,n};$$

$$S_i \in P_j \leftrightarrow \min(S_i \bigwedge_{j=1}^{m} P_j = 1), i = \overline{1,n}.$$

Для аналізу детермінованої двійкової моделі існує ефективний апарат булевих похідних, який визначає істотність і неістотність змінних щодо формування вихідного значення функціональності. Якщо зміна стану змінної-атрибута не призводить до зміни функціональності, то така змінна є несуттєвою і її можна виключити з моделі С-функціональності: При вербальному завданні моделі С-функціональності розробники використовують свій досвід і інтуїцію для формування екстра-функціональностей, дублюючих деякі істотні атрибути на моделі С-функціональності. Дана, у межі 100%-а, надмірність може бути використана також для ассерційної верифікації моделі бізнес-процесу. Сенс такої верифікації полягає в незалежному створенні і подальшому використанні-порівнянні двох моделей, де перша - максимально точна за всіма параметрами, друга - створює картину станів істотних змінних. Ассерції не несуть нової інформації про модель, але дають можливість уточнити наявність стану даних для істотних атрибутів С-функціональності в конкретному часовому фреймі.

Модельна надмірність, як правило, є корисною для прискорення обчислювальних процесів за

рахунок диверсифікації структур даних. Наприклад, просторово-часова модель С-функціональності за рахунок конволюції часу в точку може бути компактно представлена одним інтегральним стовпцем даних.

Багатозначність параметрів С-функціональності укладається в таку матричну модель:

$$P = [P_{ij}], i = \overline{1,n}; j = \overline{1,m};$$

$$P = (P_1, P_2, ..., P_i, ..., P_n);$$

$$P_i = (P_{i1}, P_{i2}, ..., P_{ij}, ..., P_{im}).$$

Тут n – число рядків матриці С-функціональності; m – кількість значень параметра Pi при її кодуванні.

Для оптимізації С-функціональності необхідно і достатньо використовувати відомі аксіоми алгебри логіки:

1) $a \vee a = a \leftrightarrow 1 \vee 1 = 1;$

2) $a \vee ab = a(1 \vee b) = a \leftrightarrow 1x \vee 11 = 1;$

3) $ab \vee a\bar{b} = a(b \vee \bar{b}) = a \leftrightarrow 11 \vee 10 = 1x = 1;$

4) $abc \vee b = b.$

Логічні аксіоми трансформуються в закони теорії множин, де фігурують елементи в форматі унітарних кодів значень вхідних змінних:

1) $a \cup a = a;\ a \cap a = a;$

2) $a \cup ab = a(1 \cup b) = a \leftrightarrow 1x \cup 11 = 1x = 1;$

3) $ab \cup a\bar{b} = a(b \cup \tilde{b}) = a \leftrightarrow 11 \cup 10 = 1x = 1;$

4) $abc \cap b = b \leftrightarrow 111 \cap 010 = 010.$

Всі вербальні значення або частини істотних (додаткових) параметрів повинні бути унітарно і єдино-метрично закодовані з метою представлення координат матриці С-функціональності двійковими векторами, які дають можливість в паралельному режимі визначати належність вхідного вектора одному або кільком стовпцям С-функціональності шляхом застосування логічної процедури:

$$a \in ab \leftrightarrow a \cap ab = a \rightarrow 10 \cap 11 = 10 \wedge 11 = 10.$$

У загальному випадку метрична взаємодія двох компонентів однієї розмірності може мати тільки п'ять випадків (рис. 8 [17]):

1) Належність чи рівність об'єктів один одному, якщо виконується умова:

$$a = b \leftrightarrow a \cap b = \{a, b\} \rightarrow 10 \cap 10 = 10 \wedge 10 = 10.$$

2) Належність першого А другому m, якщо виконується умова:

$$a \in b \leftrightarrow a \cap b = a \rightarrow 10 \cap 11 = 10 \wedge 11 = 10.$$

3) Належність другого m першому А, якщо виконується умова:

$$b \in a \leftrightarrow a \cap b = b \rightarrow 11 \cap 10 = 11 \wedge 10 = 10.$$

4) Часткова належність об'єктів один одному, якщо виконується умова:

$$a \neq b \leftrightarrow a \cap b \neq \{\varnothing, a, b\} \rightarrow 110 \cap 011 = 110 \wedge 011 = 010.$$

5) неналежність об'єктів один одному, якщо виконується умова:

$$a \neq b \leftrightarrow a \cap b = \varnothing \rightarrow 01 \cap 10 = 01 \wedge 10 = 00.$$

Структурна карта модулів комп'ютингу для аналізу С-процесів (рис. 9):

1) Синтез матриці істотних змінних.

3) Побудова унітарної матриці даних.

5) Декомпозиція унітарної матриці даних.

6) Синтез U-RPA (Robotic Process Automation) на основі застосування ML-технології до матриць С-функціональностей.

Рис. 8. Варіанти взаємодії екранів на основі and-операції

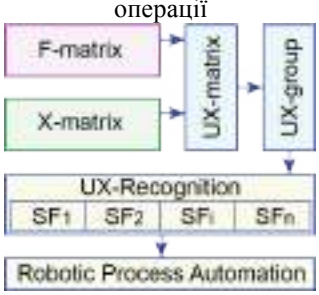


Рис. 9. Карта комп'ютингу для аналізу С-процесів

Для написання програмного коду за наведеними нижче алгоритмами слід мати доступ до структур даних існуючого програмного додатку або необхідно створювати нові моделі взаємодії вхідних, внутрішніх і вихідних даних. Слід також визначити технічні умови за часом розробки, пам'яті і швидкодії, по супроводу й тестуванню, мови, операційну систему, позиціонування, масштабування, захист, аутентифікацію, систему доступу та учасників по альфа- і бета тестуванню.

Визначення унітарної матриці істотних змінних С-процесів і кодування всіх значень.

Рішення. Організовується цикл по n істотних змінних С-функціональності, де всередині створюється цикл за значеннями змінних, де є ще один вкладений цикл, перелічує всі існуючі С-функціональності, які обробляються на предмет їх оригінальності (рис. 10). Таким чином, програмний модуль P-matrix, що містить три вкладених цикли, створює таблицю відповідності текстових значень істотних змінних їх десятковим номерам або унітарним кодам для подальшого аналізу С-процесів.

5. Модель С-процесу на основі універсуму примітивів

У загальному випадку задача формулюється як пошук і цифрова ідентифікація унікальних компонентів у текстовому фрагменті, якими можуть виступати літери, слова, пропозиції. Потім сукупність унікальних компонентів, що складають в даному випадку універсум примітивів, виступає як метрика, щоб чисельно ідентифікувати всі компоненти, але вже в масштабі текстового фрагмента цифровими (унітарними) кодами знайдених примітивів (рис. 11 [17]).

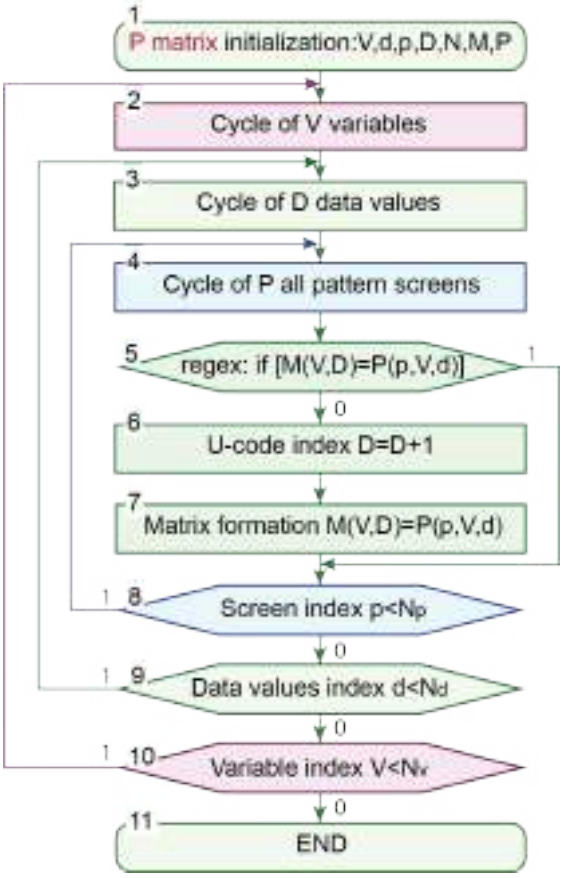


Рис. 10. Алгоритм формування матриці значень параметрів

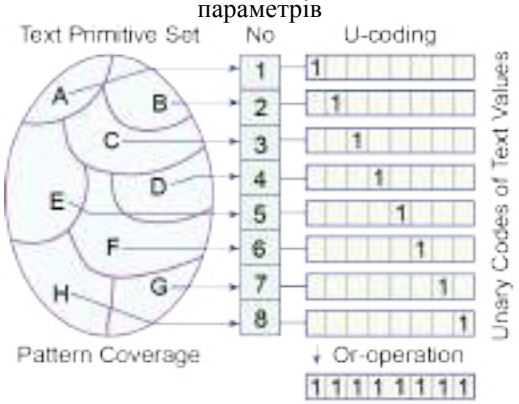


Рис. 11. Синтез унітарної моделі універсуму текстових примітивів

Таким чином, цифровізація моделі текстового фрагмента і подальший її аналіз формулюють такі завдання: 1) Визначення метрики або словникового запасу текстового фрагмента, рівного універсуму примітивних слів, що містяться в ньому. Універсум є моделлю покриття функціональності істотними компонентами, які фігурують в текстовому фрагменті. 2) Цифрове або унітарне кодування всіх метричних компонентів універсуму примітивів. 3) Ідентифікація компонентів текстового фрагмента цифровими (унітарними) кодами метричних примітивів. 4) Пошук повторень в кодованій моделі текстового фрагмента (пропозиції) з метою виключення одного представника з однакових сусідніх слів або їх заміни на синоніми, якщо вони не сусідні. 5) Пошук аналогічного текстового фрагмента в інших текстових послідовностях на основі аналізу покриття універсуму примітивів, раніше знайдених в С-функціональності. Нижче представлений результат аналізу С-функціональності, який зведений до створення таблиці, де вказані вісім унікальних значень істотних змінних, їх десяткові номери і унітарні коди:

P-value	No	U-code
A	1	1000 0000
B	2	0100 0000
C	3	0010 0000
D	4	0001 0000
E	5	0000 1000
F	6	0000 0100
G	7	0000 0010
H	8	0000 0001

Маючи таку таблицю, виконанням переборної процедури порівняння, лінійної обчислювальної складності можна знайти аналоги заданої С-функціональності в таких вхідних послідовностях: (AACFGHTDBDBE), (BACFGHTYBDBY), (DECFGHTDBDBAA). Для цього необхідно логічно об'єднати всі унітарні коди символів, що входять в кожну послідовність. В результаті об'єднання, шляхом виконання процедури Coverage, виходять покриття:

Coverage 1 (AACFGHTDBDBE) = (1111 1111),
Coverage 2 (BACFGHTYBDBY) = (1111 0111),
Coverage 3 (DECFGHTDBDBA) = (1111 1111).

Таким чином, перша і третя послідовності покривають своїми значеннями істотних змінних всі компоненти С-функціональності. Друга послідовність не формує повного покриття, тому вона не належить до С-функціональності, що задається універсумом (ABCDEFGH). Можна формувати функцію належності за ступенем покриття С-функціональності значеннями істотних змінних вхідного вектора. Тоді друга послідовність матиме якість покриття, що дорівнює Q = 7/8 = 0,875. При цьому якість покриття для першої і другої послідовності матиме оцінку Q = 1.

Висновки. Система є сукупність взаємопов'язаних в просторі і часі структурних компонентів для досягнення поставленої мети. Аналіз будь-

якої структури реалізується за допомогою пошуку універсуму примітивів, як базису системи, після чого визначаються чисельні характеристики і взаємні просторово-часові зв'язки повторюваних структурних компонентів. Інакше, щоб створити модель деякої дискретної системи, необхідно виконати її розкладання на примітиви, за допомогою яких далі синтезується просторово-часова структура, як правило, неявно задана в системі. Для цього аналізується поведінка системи в тестовому режимі або під час її функціонування шляхом зіставлення реакцій заданим вхідним впливам. Процедура аналізу використовує також навчання на основі технологій Machine Learning and Artificial Intelligence.

Маючи унітарну матрицю, що кодує текстові значення параметрів екранів вхідного бізнес-потоку recording, можна визначати істотність змінних на заданій послідовності екранів шляхом перетину (кон'юнкції) стовпців між собою, що дає можливість знаходити незмінні значення параметрів: P (essential) =∧[UMR (i)], i = 1, n. Істотність змінних для заданої C-функціональності буде ідентифікуватися одиничними значеннями координат матриці, отриманими в результаті виконання логічної операції кон'юнкції. Класичний комп'ютинг вимагає створення структур даних під існуючу реалізацію логічних операцій в кристалах кремнію: «дані для логіки». Альтернативний шлях може бути представлений реалізацією логічних операцій, які будуть впроваджуватися в хаос великих даних: «логіка для даних».

Представлення даних у вигляді компактних адрес-ідентифікаторів створює потужну технологію паралельних обчислювальних процесів, орієнтованих на високопродуктивну аналітику великих даних. Адреса даних є головною перешкодою на шляху до створення паралельних обчислювальних процесів, оскільки вона формує послідовність даних для їх завжди непаралельної обробки.

Позбавлення від адреси в структурах пам'яті приводить до комп'ютингу високої продуктивності за рахунок паралельної обробки даних.

Дивно, але факт, хаотичне невпорядковане теоретико-множинне уявлення даних в найближчому майбутньому буде представляти основу для створення сучасного високопродуктивного паралельного комп'ютингу.

Існуючі технології паралельної обробки безадресних даних включають: 1) Комбінаційні логічні схеми. 2) Регістрові логічні операції. 3) SIMD, MIMD процесори. 4) Квантові обчислення на основі операцій суперпозиції і змішування. 5) Пам'ять без адресних дешифраторів.

Пропонується address-free chaos-computing, де одним з можливих варіантів апаратної реалізації є quantum computing. The Chaos Computer Club (CCC) is Europe's largest association of hackers. Дивно, але факт, що хаос-комп'ютингом займаються хакери, які прагнуть підвищити продуктивність своїх додатків за рахунок високого паралелізму обчислень, пов'язаного з апаратною надмірністю.

На рис. 12 представлений алгоритм формування матриці значень змінних, де вирішується головна проблема ідентифікації суттєвості на тлі різноманіття атрибутів вхідного потоку даних.

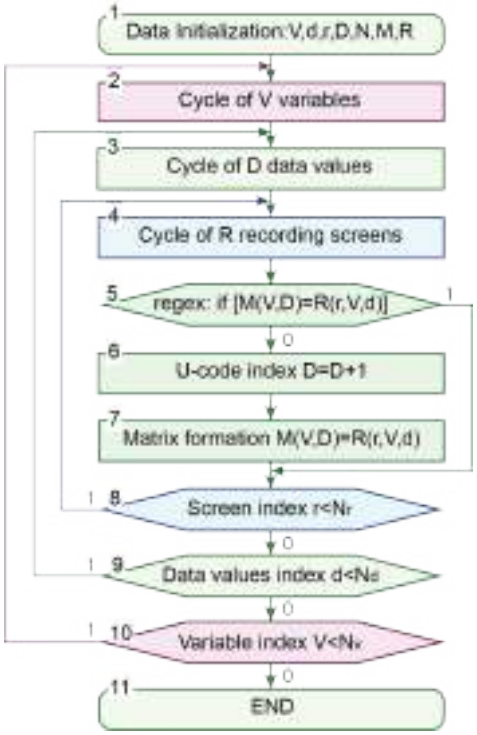


Рис. 12. Алгоритм формування матриці значень параметрів

Слово створює реальний світ і слово руйнує дійсність. Слово зберігає історію, формує дійсність і прогнозує майбутнє. Теорема Томаса (WI Thomas, 1928): якщо щось прийнято за реальність, то воно реальне в своїх наслідках. Пророцтво є причиною подальших подій. Все, що бажає людина, підкріплене волею, трапляється. Будь-яка брехня, багато разів повторена ЗМІ, стає для людини істиною. Негативні доктрини легко сприймаються людиною. Розуміння позитивних доктрин вимагає роботи мозку. Любов і творення вимагає від людини витрат, в той час як ненависть і руйнування дається їй даром. Войовниче або агресивне невігластво, зведене в ранг закону, завжди перемагає моральну компетентність. Людина програмує своє життя позитивними доктринами, якщо вона хоче бачити, або негативними, якщо її мета – руйнувати. Моральна конституція об'єднує громадян різної культури, мов, історії, релігії, традицій і програмує державу на успіх. У той же час основний закон

апріорі дискримінує громадян за згаданою метрикою, має на меті знищення державності. Успіх компанії програмується відносинами між співробітниками, які визначаються статутом, традиціями і культурою менеджменту. Цифровий світ з образу трансформується в прообраз. Якщо чогось немає в кіберпросторі, то цього немає і в фізичному світі.

Соціальний комп'ютинг гарантує і підтримує моральні відносини між людьми, вироблені людством за тисячі років його існування.

Комп'ютинг, побудований в тріаді компонентів: Memory-Address-Transaction (MAT) або Data-Address-Logic (DAL), або Logic-Address-Data (LAD), страждає від відсутності паралелізму внаслідок наявності адрес у даних, які передбачають послідовну їх обробку шляхом перебору адрес. Однак і тут інформацію можна обробляти паралельно на класичному комп'ютері, якщо скористатися апаратною надмірністю і закодувати дані унітарним кодом. Таке рішення є лише частково позитивним, оскільки воно не має перспективного майбутнього.

Десятки років вчені досить успішно поєднують два компонента (дані і логіку) в послідовність, що має виражену ієрархію, за допомогою двох можливих рішень: 1) створити комп'ютер (обчислювач, додаток, логіку) для обробки існуючих даних і 2) адаптувати дані під уже існуючий комп'ютер (обчислювач, додаток, логіку).

Дані, в частині зручності використання форматів, орієнтовані на людину і / або комп'ютер. Виходячи з цього, створюються парсери-перекладачі даних, які будують всі можливі пари: (людина-людина), (людина-комп'ютер), (комп'ютер-людина), (комп'ютер-комп'ютер). Виникає класифікація парсерів за ступенем близькості даних до комп'ютера і / або людини, яка має вигляд: 1) Системний рівень опису. 2) Рівень регістрових передач. 3) Вентильний рівень. 4) Транзисторний або аналоговий рівень опису апаратури.

Квантовий паралелізм логіки:

1) Множина кубів таблиці істинності представляється сукупністю унітарних кодів.

2) Кількість входів і виходів примітивного логічного елемента дорівнює 2**n.

3) Формується відповідність між входами і виходами логічного елемента.

4) Значення на всіх входах логічного елемента обробляються паралельно. Одночасно можна моделювати всі вхідні значення таблиці істинності.

5) Число можливих комбінацій нулів і одиниць на входах, оброблюваних паралельно, дорівнює 2**n, де n – число входів логічного примітиву.

6) Замість багатовходового унітарного примітиву можна зображати реєстровий примітив, що має 2**n входів і 2**n виходів.

7) Для синтезу унітарної моделі примітиву необхідно створювати адресний дешифратор, що перетворює позиційний код-адресу на входах логічного примітиву в унітарний код на виходах дешифратора.

8) Альтернативне рішення – використовувати в схемній структурі тільки унітарну логіку.

6. Таблиця істинності С-функціональності

Таблиці істинності для завдання С-функціональностей формуються на основі позиційного або унітарного кодування значень істотних змінних. При цьому передбачається замкнутість значень істотних змінних в межах С-функціональності, які формують групу логічних функцій, заданих кубітними покриттями таблиць істинності. Конкретна функціональність може оперувати не більше, ніж n значеннями істотної змінної, які складають алфавіт або універсум примітивів-значень A = {A1, A2, ..., Ai, ..., An}. Наступна таблиця ілюструє два види кодування універсуму примітивів значень змінної для формування таблиць істинності трьох логічних функцій, які беруть участь у створенні С-функціональності:

A	Hash 16	P-Code	U-code	P1	P2	P3
A1	0100 ... 10	00	1000	1	0	0
A2	0100 ... 11	01	0100	1	0	1
A3	1100 ... 10	10	0010	0	1	1
A4	0101 ... 11	11	0001	0	1	0

Аналогічні таблиці істинності створюються для всіх (істотних) змінних, що в сукупності формує матрицю таблиць істинності для кожного соціального процесу або явища. За фактом, стовпець позиційного кодування P-code не використовується на практиці, але він слугує базовим компонентом для доказу застосовності класичної таблиці істинності при описі будь-яких С-процесів. Стовпці P1, P2, P3 тривіально використовуються для мінімізації кількості стовпців.

Далі пропонується матрична модель С-процесів на метриці значень змінних. Стовпці-кубіти P1, P2, P3 з попередньої таблиці трансформуються в рядки-вектори, які представляють собою суперпозицію унітарних кодів значень параметрів, що беруть участь у формуванні С-процесів: PT1 - PT3:

Pi	PT1	PT2	PT3
P1	1100	1 101	1011
P2	0011	1011	0111
P3	0110	0111	0110
P4	+1001	1011	1 101

Дуалізм інтерпретації даної таблиці формує ієрархію, яку необхідно враховувати при синтезі моделі С-процесів. 1) Отримана таблиця або матриця об'єднання унітарних кодів, розміщених

в координатах, являє собою двійкову модель С-функціональності, прив'язану до модельного часу РТ1-РТ3. Тут істотно, що кожна координата матриці є векторною або кубітною формою опису таблиці істинності. 2) Однак формат матричної моделі також адекватно створює структури даних для опису сукупного С-процесу, що має місце в компанії. При цьому кожен стовпець матриці РТі інтегрально задає С-функціональність.

7. Метод синтезу логічних схем для моделювання кіберсоціальних процесів

Модель, алгебра, структура, граф, таблиця, матриця, система, рівняння є математичними поняттями, в основу яких покладено структуру взаємопов'язаних компонентів. При цьому завжди розглядається замкнутий алфавіт чи множина примітивних компонентів, які створюють основу структури або універсум примітивів. Всі можливі зв'язки між елементами алфавіту або універсуму формують сигнатуру або базові операції алгебри. Булева алгебра на найнижчому рівні представлена алфавітом або універсумом примітивних символів {0,1}, які фігурують в значеннях булевих змінних і функції Y=f(X), де {X,Y}={0,1}. При цьому поведінка функції визначається таблицею істинності, де впорядкованій двійковій послідовності вхідних змінних ставиться у відповідність двійкове значення функції. Менш поширеною є інтерпретація таблиці істинності, де кожному двійковому коду або адресі ставиться у відповідність єдине або нульове значення функції. При цьому сукупність кодів або адрес являє собою універсум примітивних компонентів або носій алгебри, на якій вводяться базові операції. Таким чином, вводиться алгебра логіки, де багатозначні стани вхідної змінної (алфавіт) кодуються в таблиці істинності двійковими векторами, які представляють собою адреси осередків пам'яті, де зберігаються {1,0}-значення функції. Інтегрально 1-значення функції в таблиці істинності формують підмножину існуючих примітивів A = {a, c, e, f} на заданому універсуми A = {a, b, c, d, e, f, g, h}, яка суперпозіційно створює функціональність:

String	Code	Function
a	000	1
b	001	0
c	010	1
d	011	0
e	100	1
f	101	1
g	110	0
h	111	0

Кубітним покриттям даної функціональності є вектор двійкових станів вихідної змінної, розмірність якого дорівнює універсуму примітивних компонентів, що формують функцію, а число одиничних значень – підмножині примітивів з універсуму, яке бере участь у формуванні заданої функціональності. Слід зазначити, що функціональність формується значеннями суттєвої змінної у часових фреймах бізнес-процесу або бізнес-патерну. З огляду на те, що кількість істотних змінних, як правило, більше 1, то необхідно синтезувати цифрові логічні схеми з кубітних покриттів функцій, число яких дорівнює кількості істотних змінних. Таким чином, кінцева множина істотних змінних є базовими елементами для синтезу цифрових логічних схем управління С-функціональності або С-процесу. Далі представлені дві структури, які оперують кубітними покриттями примітивів, об'єднані логікою елементів: and, or (рис. 13). Логічні структури, синтезовані з кубітних форм логічних функцій значень істотних змінних, призначені для моделювання бізнес-процесів з метою визначення поведінки кіберфізичної С-архітектури комп'ютингу на заданих вхідних робочих впливах. Робочими впливами є суперпозиції унітарних кодів значень істотних змінних. Стан виходу логічної С-схеми, що дорівнює одиниці, свідчить про позитивний вплив взаємодії значень істотних змінних на хід виконання бізнес-процесу для досягнення поставленої мети (реалізація закінченої бізнес-процедури). Таким чином, замість ланцюжка даних, що ілюструє послідовність дій у С-функціональності, пропонується принципово нова форма – комбінаційна цифрова логічна схема, паралельно інтегруюча тільки істотні властивості бізнес-функціональності, основною відмінністю якої є можливість моделювання С-процесів.

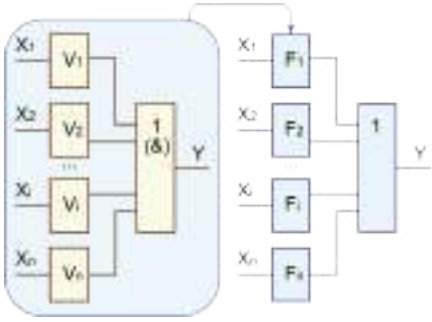


Рис.13. Structures of Logic Social Functions

Circuit формує функціональну поведінку або модель С-функціональності на основі використання кубітних покриттів змінних, інваріантних до часу. Сукупність С-функціональностей створює основу для синтезу паралельної цифрової моделі С-процесу, яка являє собою спеціалізований обчислювач, що реалізує кіберфізичний комп'ютинг для моніторингу, моделювання та управління С-процесами компанії. Ієрархія С-комп'ютингу представлена компонентами: <Значення – змінна – функціональність – процес> або <value – variable – function – process>. Приклад структурної схеми С-функціональності, що скла-

дається з логічних кубітних елементів, представлена на рис. 14.

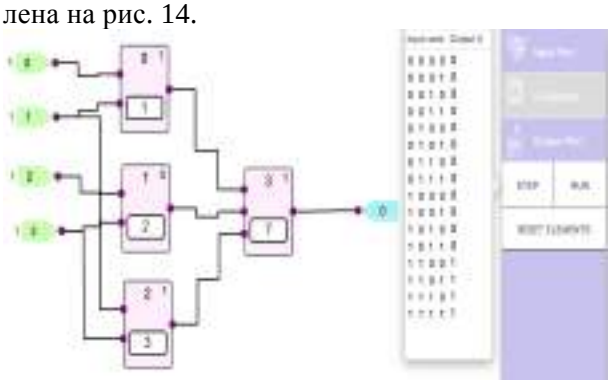


Рис. 14. С-функціональність

Дана структура (приклад) синтезована вручну шляхом використання програмного додатку QuaSim [17] на основі поєднання бібліотечних універсальних елементів, що відповідають соціальним змінним, визначеним на векторі значень-примітивів. Схема дає можливість моделювати вхідні виконавчі дії, відповідні соціальним процесам, для передбачення наслідків або ідентифікації явищ, що відбуваються в кіберфізичному просторі.

Логічна структура або С-процесор, інваріантний до часу, створює С-функціональності на основі кубітних форм таблиць істинності логічних елементів, прив'язаних до універсуму примітивних значень змінних. Переваги С-процесора полягають в компактності уявлення і високій швидкодії комбінаційної схеми С-функціональності, що визначається кубітними векторами істотних змінних, побутова розмірність яких дорівнює кількості примітивних даних кожної змінної. Кубітні структури даних інваріанті до їх hardware реалізації у вигляді логічної схеми або для імплементації в software у вигляді таблиць-матриць опису функціональностей. Кубітна двійкова форма опису С-функціональностей дає можливість технологічно моделювати як завгодно складні С-процеси шляхом впливу на схему двійковими вхідними наборами, які відповідають унітарно-кодованим даним, в цілях визначення вихідних станів С-процесора, що виконують роль класифікатора і / або актюатора. Позитивним є той факт, що кожен кубітний логічний елемент, заданий у векторному форматі кількості значень змінною, створює образ С-функціональності одиничними значеннями своїх координат. При цьому число кубітних векторів-елементів, об'єднаних в схему and (or) – елементом, дорівнює кількості істотних атрибутів (змінних), синтезується С-функціональністю. Крім того, візуалізація досить компактної логічної схеми завдання С-функціональності дає можливість користувачеві або керівнику побачити сутність С-функціональностей без прив'язки до часу, де важливим є покрити всі необхідні атрибути-елементи конструктивними діями користувача для отримання відповідних сервісів.

Недоліком процесорної С-моделі є виключення параметра часу в функціонуванні логічної моделі, що призводить до її неадекватності в разі потреби опису послідовних граф-схеми алгоритму з-функціональності. Крім того, дл моделювання даних за допомогою логічної С-схеми необхідно синтезувати препроцесор перетворення текстових даних в унітарні кубітні вектори на основі використання hash-функцій, що істотно зменшує час порівняння текстового рядка з бібліотечними даними. Необхідний також постпроцесор для інтерпретації станів виходів С-процесора користувачеві (автомату), який буде проводити наступні актюаторні дії. В сукупності препроцесор і постпроцесор займають близько 10 відсотків пам'яті і обчислювального часу обробки даних від базового варіанту, пов'язаних з синтезом і аналізом кубітних структур, що реалізують архітектуру С-схеми підприємства.

Формальний синтез логічних схем С-процесу компанії здійснюється шляхом виконання таких пунктів:

1) Формування універсуму з примітивних даних по кожному атрибуту С-процесу.

2) Заповнення вектор-кубіта примітивних даних одиничними значеннями тих координат, номери яких відповідають значенням даних, що використовуються при формуванні конкретної С-функціональності.

3) Об'єднання по and-функції всіх логічних елементів, заданих кубітами задіяних значень атрибутів, для отримання схеми С-функціональності.

4) Об'єднання всіх схем С-функціональностей для отримання логічного С-процесора компанії.

Завдання аналізу можуть бути вирішені за допомогою логічних С-схем:

1) Моделювання вхідного потоку даних в цілях їх класифікації на множині бібліотечних С-функціональностей шляхом використання вектора моделювання (покриття), який дає можливість на кожному кроці визначати стан модельованого С-процесу, а також генерувати керуючі впливу, спрямовані на отримання покриття С- функціональності, виходячи з нульових координат вектора моделювання.

2) Автоматичне генерування вхідних двійкових векторів на основі аналізу даних для їх подальшого моделювання на С-процесорі.

Для автоматичного формування С-процесора на основі використання вхідного контенту необхідно: 1) Визначення ключових слів для формування змінних С-процесу і подальшого обчислення універсумів примітивних значень даних. 2) Формування ідеї кожного С-процесу, що створює

закінчену С-функціональність у вигляді матриці кубітних покриттів, складених з унітарних кодів, які відповідають значенням з універсумів примітивів змінних. Інструментом для точного моделювання вхідних впливів на кубітних покриттях С-функціональності є функція належності, яка обчислюється шляхом визначення кодової відстані між вхідним двійковим набором, що подається на логічний елемент, і кубітним вектором останнього:

String	Input	Function	Xor	μ (I, F) =
a	1	1	0	0,75
b	0	0	0	
c	0	1	1	
d	0	0	0	
e	1	1	0	
f	1	1	0	
g	0	0	0	
h	1	0	1	

Однак належність частини С-функціональності визначається операцією логічного множення або перетину, яка повинна бути рівною вхідному вектору I∧F = I, що означає покриття логічним елементом С-функціональності значення вхідного вектора I∈F.

Отже, структури даних С-аналітики або архітектура С-комп'ютингу, зображеного на рис. 15, містить: 1) Метрику у вигляді множини U = {U1, U2, ..., Ui, ..., Un} кубітних покриттів універсумів примітивних значень, що має потужність, рівну кількості змінних n. Кожен універсум Ui = {Ui1, Ui2, ..., Uij, ..., Uim} формує повну множину примітивних значень змінної. 2) На основі даної метрики, шляхом синтаксичного порівняння, синтезуються еталонні С-функціональності P = {P1, P2, ..., Pr, ..., Pk}, де стовпчик Pr = {Pr1, Pr2, ..., Pri, ..., Prn} формує С-функціональність, а координата стовпця визначається двійковим вектором Pri = {Pri1, Pri2, ..., Prij, ..., Prim}, записаним у форматі кубітного покриття Ui = {Ui1, Ui2, ..., Uij, ..., Uim} універсуму примітивних значень змінної. При цьому Prij=1, якщо в С-функціональності присутній символьне значення змінної, рівне Uij. Кубітне покриття С-функціональності Pr = {Pr1, Pr2, ..., Pri, ..., Prn} завжди є структурною частиною кубітного покриття універсуму примітивів: Pr∈U, оскільки завжди працює аксіома Pr∧U = P. 3) Метою створення еталонних С-функциональностей є автоматичне генерування актюаторних впливів A = (A1, A2, ..., Ap, ..., Aq), які замикають цикл С-аналітики керуючими впливами, перетворюючи її в RPA-структуру.

$$\begin{bmatrix} R_1 \\ R_2 \\ \dots \\ R_p \\ \dots \\ R_q \end{bmatrix} \xrightarrow{U=f(R)} \begin{bmatrix} U_1 \\ U_2 \\ \dots \\ U_i \\ \dots \\ U_n \end{bmatrix} \xrightarrow{P=f(R,U)} \begin{bmatrix} P_{11} & P_{21} & \dots & P_{r1} & \dots & P_{k1} \\ P_{12} & P_{22} & \dots & P_{r2} & \dots & P_{k2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ P_{1i} & P_{2i} & \dots & P_{ri} & \dots & P_{ki} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ P_{1n} & P_{2n} & \dots & P_{rn} & \dots & P_{kn} \end{bmatrix} \xrightarrow{A=f(R,U,P)} \begin{bmatrix} A_1 \\ A_2 \\ \dots \\ A_p \\ \dots \\ A_q \end{bmatrix}$$

$U_i = (U_{i1}, U_{i2}, U_{ij}, U_{im}); P_{ri} = (P_{ri1}, P_{ri2}, P_{rij}, P_{rim}); \{U_{ij}, P_{rij}\} = \{0,1\}.$

Рис. 15. Матрична архітектура С-комп'ютингу

Матрична архітектура С-комп'ютингу підтримує ієрархію кубітних покриттів Rp∈Pr∈U, де Rp-вектор вхідних значень змінної не може бути більше Pri-кубіта С-змінної, який не може бути більше універсуму Ui значень змінної.

Архітектура програмного серверного додатка SoQuaSim (Social Quantum Simulation) для синтезу соціальних логічних функціональностей і подальшого моделювання на них контенту великих даних із соціальних мереж представлена на рис. 16.

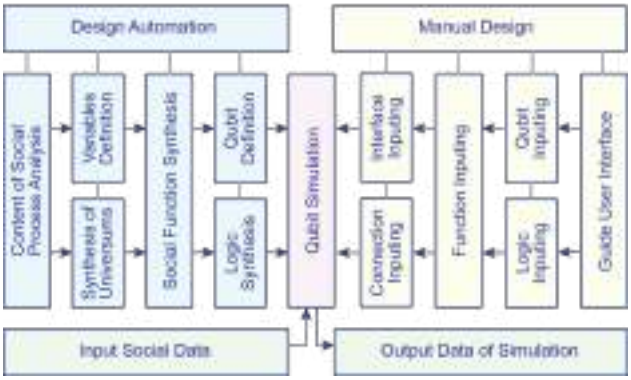


Рис. 16. Архітектура процесора SoQuaSim

Структура містить дві частини, де ліва з них призначена для автоматичного синтезу структур даних, логічних елементів і схеми в цілому. Права частина орієнтована на ручне введення схемних елементів і структури соціальної функціональності на основі використання графічного інтерфейсу. Обидві частини архітектури навантажені на блок кубітного моделювання вхідного контенту з метою визначення в ньому аналогів соціальних процесів, конструктивних і деструктивних, синтезованих раніше за інших можливостей. Результати моделювання зберігаються в бібліотеці, яка містить також і логічні еталони функціональної поведінки людини і / або соціальної групи.

Використання програмного додатку SoQuaSim дає можливість моделювати будь-які соціальні процеси і явища, що мають практичне значення. Для цього необхідно визначити сукупність істотних змінних, де для кожної з них знайти універсум примітивних значень або метрику вимірювання параметра для заданого процесу чи явища. Наступний графік (рис. 17) демонструє моделювання спроможності вчених університету за 10 параметрами науково-освітньої метрики на

прикладі кращих з них, які претендують на роль керівників наукових шкіл.

Рис. 17. Моделювання спроможності вчених

Інший приклад, представлений на рис. 18, ілюструє факт валідності кожного вченого спільно з його кращим науковим результатом по цитованості публікації в Scopus-метриці. Графік показує спроможність кращих вчених (наукових статей) по метриці H = 10 + and Paper Citation = 20 + в університеті.

Рис. 18. Аналіз H-index and Citation вчених

Результат моделювання показує, що рівень вищих перших наукових результатів пов'язаний з апаратними технологіями і матеріалами та тільки одна публікація має відношення до IT-індустрії програмних додатків.

Для моделювання соціальних процесів всередині університету слід використовувати модифікований додаток SoQuaSim для синтезу та аналізу цифрових пристроїв. Логічна структура, синтезована в додатку SoQuaSim (рис. 19), орієнтована на пошук позитивного рішення при збігу по and-операції двох еталонів, представлених векторами, які формують значення двох багатозначних (реєстрових) змінних: Y=(01101011) and (1100011). Вхідне слово має збігатися за всіма розрядами зі значеннями кубітного вектора для вироблення одиничного значення на виході логічного елемента. Розбіжність векторів супроводжується кодовою відстанню між ними, яка формує интервальне чисельне значення функції належності m (R, F) = (0,1) вхідного слова до логічного ідеалу соціального процесу або явища.

Результати моделювання представлені у вигляді стану вектора-стовпця Out, який містить поодинокі координати, якщо вхідні претенденти збігаються по операції and (елемент 2) з двома метричними еталонами, представленими векторами (0,1)-значення, записаними в логічних елементах з номерами 0 і 1.

Схема може бути спрощена щодо числа зовнішніх входів, яке на рис. 20 дорівнює числу логічних багатозначних елементів першого рівня. Багатозначність дає користувачеві можливість оперувати тільки такими еталонами значень, які прописані як функціональні.

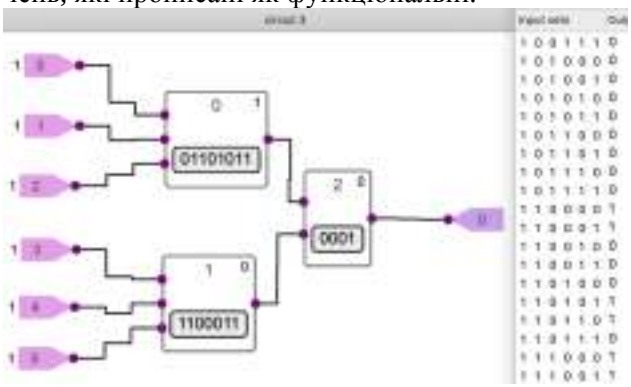


Рис. 19. Схема моделювання на співпадіння

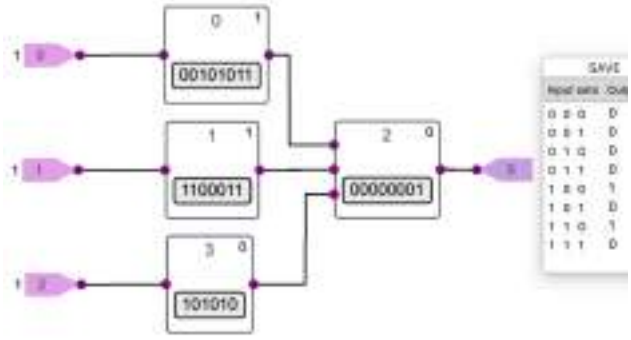
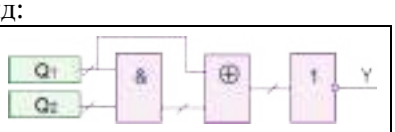


Рис. 20. Структура з багатозначними логічними входами

Багатозначні логічні елементи соціальних функціональностей. Пропонується рішення в частині синтезу логічних схем для аналізу соціальних процесів, пов'язане з використанням кубітно-регістрових змінних, які унітарно кодують множину примітивних значень з багатозначного універсуму змінної. У цьому випадку будь-яка функціональність може бути представлена логічним елементом and (or, or), який має регістрові вхідні змінні, представлені кубітними векторами. Середнє арифметичне значення на виході логічного елемента з багатозначними або векторними входами визначається збігом сигналів з кубітними векторами за всіма вхідними змінними. Для цього необхідно виконувати процедуру, пов'язану з логічним перетином (and-операція) вхідного сигналу з кубітним вектором і подальшим хог-порівнянням результату перетину з вихідним сигналом. Якщо таке порівняння дорівнює нулю за всіма координатами векторів, то формується середнє арифметичне значення виходу для однієї багатозначної змінної. При наявності одиниць на всіх виходах змінних логічного елемента and його значення буде рівним

одиниці. Аналітична модель і схемна реалізація процедури порівняння двох векторів для визначення приналежності одного з них Q1 до іншого Q2 має такий вигляд:

Y =∨[(X∧Q)⊕X]	

Схемна реалізація пристрою для моделювання соціальних процесів X шляхом порівняння з еталонними функціональностями Q представлена на рис. 21.

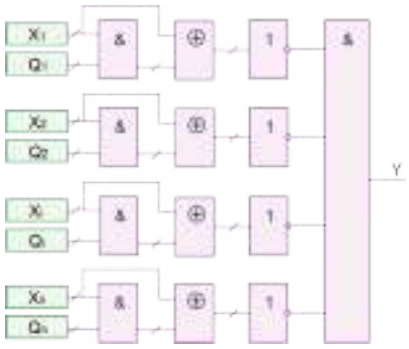


Рис. 21. Схема моніторингу і аналізу соціальних процесів

Тут порівнюються двійково-кодовані вхідні значення X з відповідними кубітними векторами еталонних значень змінних соціальних процесів. Стан вихідної змінної Y=1, якщо вхідні значення рівні кубітним векторам за усіма кординатами. Це означає, що вхідні дані в сукупності являють собою наперед задану еталонну соціальну функціональність. Кубітні вектори в сукупності формують матрицю еталонних значень соціальної функціональності. Швидкодія отримання рішення на виході схеми дорівнює п'яти структурним тактам. Слід зазначити, що в загальному випадку стан виходу схеми формується функцією належності

$$Y = m(X, Q) = 1 - d(X, Q) / n,$$

яка визначена в інтервалі (0,1) числом (розбіжностей) одиничних координат на регістровому виході логічної and-функції кожної змінної, де n – число координат Q-вектора, d (X, Q) – кодова відстань за Хеммінгом. Схема формує функцію належності елемента або підмножини до наперед заданого еталонного вектора примітивів за один автоматний цикл, завдяки векторній формі завдання підмножин однакової розмірності. Інакше, схема дає можливість відповісти на питання: чи належить вхідна двійкова послідовність X еталонній соціальний функціональності Q, також представленої в цифровому вигляді Y=1.

Можна використовувати схему (рис. 22) з нульовим позитивізмом вихідного сигналу, коли максимальна належність вхідного сигналу X до кубітного еталону Q ідентифікується 0-рівнем відмінності між двома векторами

$$Y = a(X, Q) = d(X, Q) / n.$$

Рис. 22. Схема компараторного аналізу соціальних процесів

Це істотно спрощує логічну структуру, представлену на рис. 23. Тут Y=0 означає повний збіг між вхідними даними і кубітним вектором еталонної функціональності, що дає підстави, ідентифікувати або класифікувати аналізований процес, як належить еталонному вектору. В результаті виходить, що функція збігу (match function) є інверсною по відношенню до функції належності (membership function):

$$Y=a(X, Q)=d(X,Q)/n = not[m(X, Q)=1-d(X, Q)/n].$$

Зі схеми можна прибрати шар or-елементів, пов'язаний зі згорткою регістрових змінних в логічні змінні.

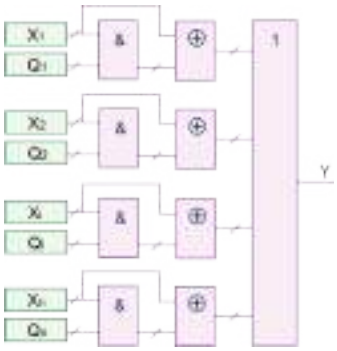


Рис. 23. Схема спрощеного компараторного аналізу соціальних процесів

Тоді стан виходу схеми формується нульовим значенням, якщо їх капітали логічних елементів-змінних рівні нулю, які ідентифікують збіг вхідних і еталонних сигналів. В іншому випадку, визначається ступінь їх розбіжності або належності, як чисельна оцінка кількості відмінностей (збігів) до загальної кількості значень на всіх змінних. Маючи логічні or-елементи, можна структурувати збіги за змінними і додатково отримувати чисельні оцінки належності вхідних сигналів еталонним.

Сигналами можуть виступати: символи, літери, слова, пропозиції, цифри, числа, відносини, структури, малюнки, фотографії, відеофільми, звукові фрагменти, процеси і явища.

UU-модель кіберсоціальних процесів і явищ для університету представлена на рис. 24.

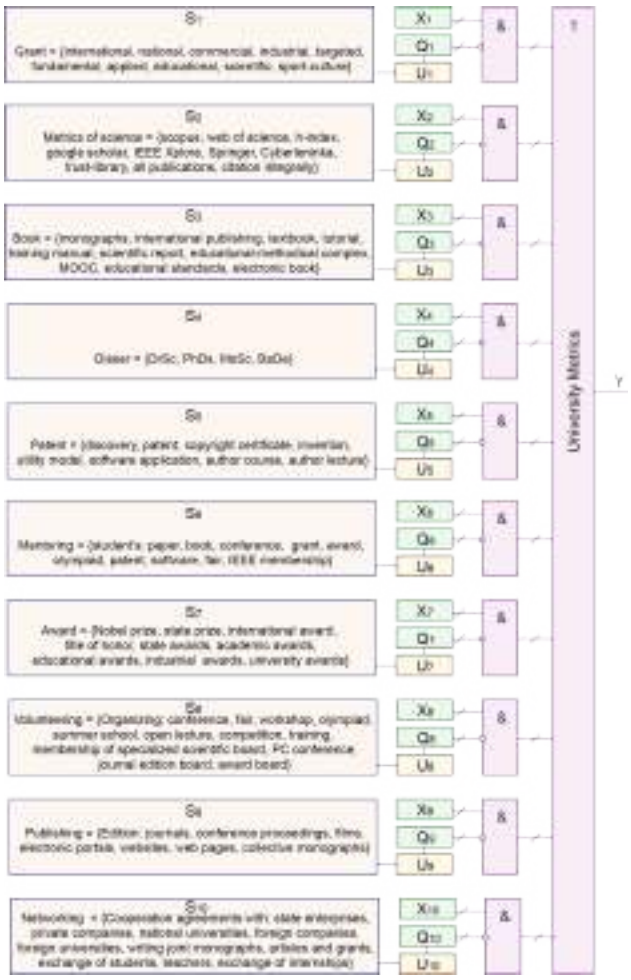


Рис. 24. Метрика університету

Універсум універсумів (UU) являє собою дворівневу модель процесу або явища, призначену для активного цифрового моделювання з метою точного розпізнавання вхідних великих даних шляхом метричного порівняння з заданими еталонами.

Вчений (студент, університет), як компонент науково-освітнього процесу, використовує UU-метрику, яка представлена десятьма найважливішими параметрами, складовими універсуму примітивів:

1) Grant – отримання вченими R & D-грантів, комерційних, державних, освітніх і наукових проектів. Grant = {international, national, commercial, industrial, targeted, fundamental, applied, educational, scientific, sport-culture}.

2) Metrics of science – наукометрія соціальної значущості праць ученого: індекс Хірша, цитованість, кількість публікацій. Metrics of science = {scopus, web of science, h-index, google scholar, IEEE Xplore, Springer, Cyberleninka, trust-library, all publications, citation integrally}.

3) Book – монографії, навчальні посібники, навчально-методичні комплекси (УМК), масові онлайн курси (MOOC). Book = {monographs, international publishing, textbook, tutorial, training manual, scientific report, educational-methodical complex, MOOC, educational standards, electronic book}.

4) Disser – дисертації, захищені під керівництвом вченого. Disser = {DrSc, PhDs, MsSc, BaDe}.

5) Patent – патенти, ринкові науково-освітні продукти і сервіси. Patent = {discovery, patent, copyright certificate, invention, utility model, software application, author course, author lecture}.

6) Mentoring – участь студентів під керівництвом професора у всіх видах екстра-активності. Mentoring={student's: paper, book, conference, grant, award, olympiad, patent, software, fair, IEEE membership}.

7) Award – нагороди, звання, премії та дипломи соціального визнання досягнень вченого. Award = {Nobel prize, state prize, international award, title of honor, state awards, academic awards, educational awards, industrial awards, university awards}.

8) Volunteering – організація і проведення конференцій, виставок і семінарів. Volunteering = {Organizing: conference, fair, workshop, olympiad, summer school, open lecture, competition, training, membership of specialized scientific board, PC conference, journal edition board, award board}.

9) Publishing – видання журналів, фільмів і праць конференцій. Publishing = {Edition: journals, conference proceedings, films, electronic portals, websites, web pages, collective monographs}.

10) Networking – укладання договорів про співпрацю з підприємствами та університетами. Networking = {Cooperation agreements with: state enterprises, private companies, national universities, foreign companies, foreign universities, writing joint monographs, articles and grants, exchange of students, teachers, exchange of internships}.

Кожен з параметрів представлений значеннями, які в сукупності складають універсум другого рівня. В результаті виходить UU-метрика функціональності еталонного вченого (студента, університету), щодо якої можна вимірювати-моделювати явище, що претендує на дану роль (рис. 25).

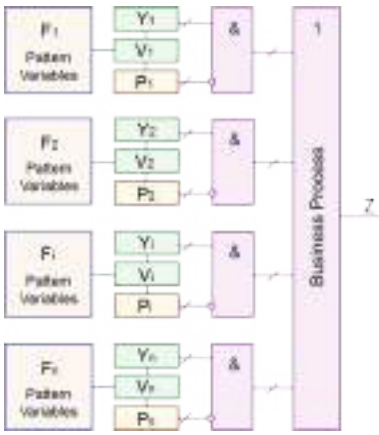


Рис. 25. Логічний кубітний секвенсор для розпізнавання або моделювання бізнес-процесів

Університет, як науково-освітня установа, також можна уявити метрично в новій активній логічній формі універсуму універсумів (об'єкт-функціональності-змінні-значення): сукупність істотних компонентів, що утворюють online комп'ютинг, де кожен з них представимо універсумом значень другого рівня (рис. 26):

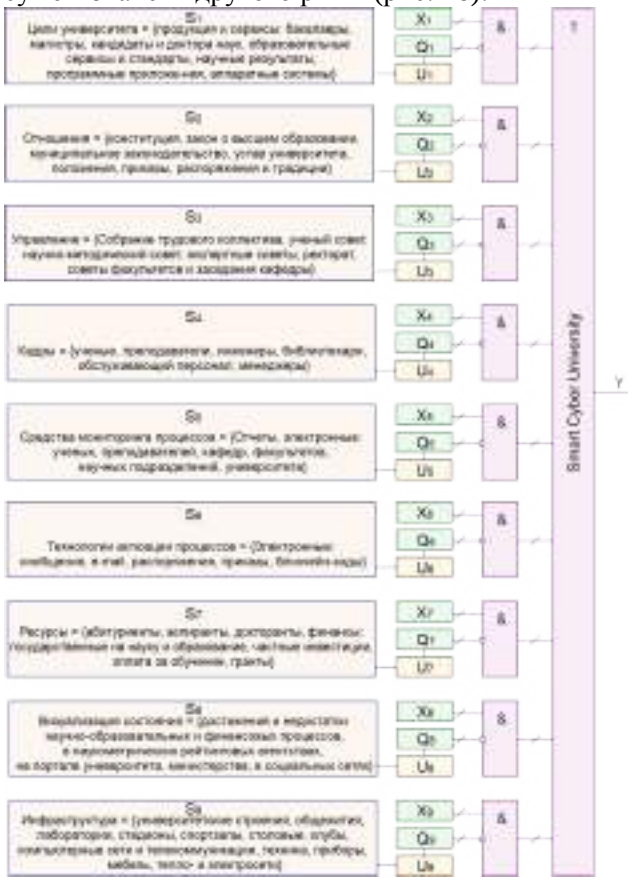


Рис. 26. Smart Cyber University

Наведені вище схеми є тільки частина соціального комп'ютингу – monitoring and analysis. Найбільш істотним і дизрапторним компонентом комп'ютингу є controlling, який створює актюаторний вплив з архітектури, симетричною щодо логічної структури моніторингу. На рис. 27 представлена логічна структура для генерування актюаторних впливів на соціальний процес, що використовують засоби моніторингу та аналізу для формування керуючих сигналів.

Рис. 27. Логічна структура управління

Тут сукупність актюаторних впливів формує універсум примітивів для кожної змінної, з яких створюються кубітні логічні функціональності для управління кіберсоціальними процесами і явищами, які використовують компараторні процедури або алгоритми для порівняння з еталонами. Універсум актюаторних примітивів дає можливість управляти змінною за допомогою синонімів, кожен з яких активує певний процес або явище. Наприклад, змінна активізації руху довільного об'єкта має такі варіанти, що становлять універсум: {поїхали, рушили, покотилися, поскакали, полетіли, помчали, потяглися, попрямували, погнали, побігли, пішли, стартанули}. Обов'язковою умовою в підборі синонімів для змінної є їх неперетинання з універсумом інших параметрів, щоб уникнути неоднозначності поведінки об'єкта. Природно, що змінні активізації своїми універсумами створюють команди для управління процесами, пов'язаними з людиною, твариною, автомобілем, роботом, дроном, комп'ютером, зброєю, технікою, будинком, робочим місцем.

Таким чином, логічна схема для аналізу соціального процесу або явища здатна верифікувати створену метрику або структуру, моделювати позитивні або негативні рішення політичної еліти, передбачати соціальні явища в майбутньому, включаючи деструктивні акції, катаклізми, колізії, злети і падіння громадян, соціальних груп і держав. Соціальний комп'ютинг, як і універсальний обчислювач, здатний визначати точні рішення за допомогою логічних схем еталонної поведінки людини, соціальної групи або держави. Проблема підлягає вирішенню в майбутньому, полягає в створенні бази алгоритмів або схем, з яких можна технологічно просто синтезувати кіберсоціальні метричні процесори для моніторингу, аналізу та актюаторного управління медициною, транспортом, наукою, освітою, державою, виробництвом, екологією, юриспруденцією, фінансами.

8. Висновок

Наукова новизна полягає в створенні моделей, методів і архітектур кіберсоціального комп'ютингу, спрямованого на автоматичний синтез і аналіз кубітних логічних схем, орієнтованих на моделювання, моніторинг і управління соціальними процесами і явищами, а саме:

1) Удосконалено архітектуру memory-driven кіберфізичного комп'ютингу, яка відрізняється паралелізмом процедур синтезу та аналізу логічних секвенсорів, призначених для моделювання соціальних процесів і явищ з метою моніторингу та управління.

2) Удосконалено кубітно-векторні моделі цифрових комбінаційних схем, які відрізняються

унітарним кодуванням багатозначних логічних змінних для синтезу секвенсорів з метою паралельного аналізу кіберсоціальних процесів.

3) Вперше запропоновано кубітний метод синтезу логічних схем, який характеризується унітарним кодуванням багатозначних змінних для паралельного моделювання кіберсоціальних процесів і явищ.

4) Вперше запропоновано кубітний метод паралельного аналізу кіберсоціальних процесів, який характеризується унітарним кодуванням багатозначних змінних, використовуваних в еталонних логічних елементах комбінаційних схем.

5) Вперше запропоновано кубітно-регістровий метод аналізу, який характеризується використанням логічних елементів з векторною формою унітарних кодів багатозначних змінних для паралельного моделювання кіберсоціальних процесів.

6) Створено сервіс-додатки SoQuaSim, виконано його тестування і верифікацію в частині кубітних моделей і методів кіберфізичного комп'ютингу на прикладах соціальних процесів, пов'язаних з поведінкою громадян.

7) Розроблені кубітні моделі, структури даних, методи синтезу та аналізу логічних схем фрагментів соціальних процесів, які дозволяють моделювати реакцію системи від прийняття конструктивних і деструктивних рішень людини, керівника, чиновника, завдяки кубітному опису еталонів поведінки, що дає можливість актюаторно управляти громадянами для уникнення деструктивних наслідків . Окремі сервіси синтезу та аналізу кубітних моделей соціальних процесів реалізовані у вигляді програмного додатка SoQuaSim і пройшли представницьку апробацію в процесі виконання проекту "Smart Cyber University". Середовище проектування: SWIFT, платформа: Macintosh OS X.

Напрями майбутніх досліджень. Так само як біологічні віруси деструктурують людину, соціальні віруси (корупція, злодійство, тероризм, забруднення планети, бунти, революції, війни) вражають організм людства в масштабах планети, несучи на той світ мільйони життів. Причиною цього завжди є аморальність і некомпетентність політичної еліти державних утворень, яка формує соціальні хвороби «брудних рук». Якщо врахувати, що зцілити політичну еліту можна шляхом тривалого процесу її «санітарної» освіти, необхідно шукати альтернативні технології боротьби проти соціальних вірусів. Одним з можливих варіантів може бути соціальний імунітет, як кіберфізичний моральний соціальний комп'ютинг метричного вичерпного моніторингу всіх процесів і явищ для цифрового human-free управління громадянами на основі моделювання і передбачення наслідків від прийняття рішень. Комп'ютинг завжди, скрізь і в усьому пояснює природу процесів і явищ, допомагає вирішувати актуальні питання гармонійного і морального розвитку людства. Ось кілька прикладів комп'ютингу. Всесвіт має гармонійний геном циклічної зміни в метриці: матерія і енергія, простір і час – Cosmological Computing. Людство також прагне до гармонійної зміни моральних відносин для досягнення соціальної справедливості шляхом цифрового моніторингу та автоматичного управління при наявності ресурсів в метриці: матерія і енергія, простір і час - Humanity Computing. Геном людини формує гармонійний напівцикл зміни шляхом зародження, розвитку, старіння і вмирання в метриці ресурсів: матерія і енергія, простір і час – Human Computing. Геном комп'ютингу також має гармонійну форму розвитку технологій, елементної бази, системних, алгоритмічних, програмних і архітектурних рішень в метриці: матерія і енергія, простір і час – HW-SW Computing. Кібермедичний комп'ютинг (КМК) – довічний моніторинг душевного і фізичного здоров'я кожної людини з моменту її народження в цілях активного управління її поведінкою в форматі 24/7 для запобіжників хвороб шляхом створення цифрового асистента, який допомагає приймати оптимальні рішення по стратегії і тактиці поведінки для забезпечення високої якості життя. КМК є альтенативою до стратегії сучасної медицини, що полягає в лікуванні хвороб, отриманих в результаті неправильного вибору повсякденних і довготривалих рішень, пов'язаних з незнанням функціональних особливостей свого організму та впливу на нього навколишньої дійсності. Запобігати хворобам шляхом моделювання можливих варіантів поведінки, а не пояснювати, чому вони сталися, забезпечувати якість життя, а не якість лікування на основі перманентного метричного моніторингу стану душі, тіла і навколишнього середовища з метою цифрового оптимального управління поведінкою людини. При цьому корекція природних помилок і отриманих травм є лише корисним доповненням до засобів забезпечення якості життя людини. Біокомп'ютинг, як моніторинг і управління біологічними процесами, є найбільш суттєвою областю в пізнанні життя (синтез і аналіз), яка найменш вивчена вченими і практиками. Адитивний комп'ютинг є безвідхідною технологією вирощування або 3 (4) D-друкування комп'ютерів і їх компонентів, технічних конструкцій, будинків, продуктів харчування, біоінженерних частин людського тіла.

Окремі висновки. Беручи до уваги дизрапторну аксіому, що комп'ютинг, як процес, є первинним

по відношенню до явищ, які він пояснює, породжує, обслуговує і використовує, можна зробити кілька істотних практично-орієнтованих висновків: 1) Замість універсального цільового критерію ефективності: час-гроші-якість вводиться вимір процесу або явища в метриці двох взаємодіючих пар: простір-час, матерія-енергія. 2) Будь-який процес спрямований на зміну явища в метриці параметрів простір-час, матерія-енергія для досягнення мети. 3) Процес реалізується, реально чи віртуально, в архітектурі або моделі комп'ютингу, який визначається вісьмома взаємодіючими компонентами: мета, відносини, візуалізація, управління, виконання, ресурси, моніторинг, актюація. 4) Будь-який соціальний процес може і повинен бути реалізований у форматі комп'ютингу, де головною відмінністю від всієї передісторії людства є цифровий моніторинг і актюаторне human-free online управління. 5) Кіберсоціальний комп'ютинг має сенс лише в разі прямої і безпосередньої взаємодії кожного громадянина з будь-якими сервісами моніторингу та управління, що усувають армію чиновників. 6) Громадянин не повинен вступати в стосунки з чиновниками при отриманні сервісів, тільки кібер-роботи-автомати обслуговують людину. 7) Кіберсоціальний комп'ютинг своєю моральністю виключає середньовічну дискримінацію громадян за расою, національністю, релігією, історією, культурою, мовою, віком, статтю та місцем народження.

Література:

1. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/
2. https://www.gartner.com/doc/3891569?src Id=1-7251599992&cm_sp=swg-_-gi-_-dynamic
3. *Gupta A. and Jha R.K.* "A Survey of 5G Network: Architecture and Emerging Technologies," in IEEE Access, vol. 3, pp. 1206-1232, 2015.
4. *Zhu C., Leung VCM, Shu L. and Ngai ECH*. "Green Internet of Things for Smart World," in IEEE Access, vol. 3, pp. 2151-2162, 2015.
5. *Christidis K. and Devetsikiotis M.* "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.
6. *Blockchains*: How They Work and Why They'll Change the World IEEE Spectrum. October 2017.
7. *Zanella A., Bui N., Castellani A., Vangelista L. and Zorzi M.* "Internet of Things for Smart Cities," in IEEE IoT Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014.
8. *Frahim J.* Securing the Internet of Things: A Proposed Framework / J. Frahim // Cisco White Paper. 2015.
9. *Kharchenko V.* Green IT Engineering: Concepts, Models, Complex Systems Architectures / V. Kharchenko, Y. Kondratenko, J. Kacprzyk (Eds.) // In the book series "Studies in Systems, Decision and Control" (SSDC). Vol. 1. Berlin, Heidelberg: Springer International Publishing.- 2017.
10. *Kharchenko V.* Green IT Engineering: Components, Networks and Systems Implementation / V. Kharchenko, Y. Kondratenko, J. Kacprzyk (Eds.) // In the book series "Studies in Systems, Decision and Control" (SSDC). Vol. 2. Berlin, Heidelberg: Springer International Publishing.- 2017.
11. *Memory-Driven* Computing. [Online]. Available: https://www.labs.hpe.com/next-next/mdc
12. *Benenti G., Casati G., Strini G.* Principles of Quantum Computation and Information. Vol. 1: Basic Concepts.World Scientific. 2004. 256 p.
13. *Imai Hiroshi, Hayashi Masahito*. Quantum Computation and Information. From Theory to Experiment. Springer. 2006. 234 p.
14. *Nielsen MA, Chuang IL* Quantum Computation and Quantum Information. Cambridge University Press. 2010. 710 p.
15. *Abramovici M.* Digital System Testing and Testable Design / M. Abramovici, MA Breuer and AD Friedman.- Comp. Sc. Press. 1998. 652 p.
16. *Benso A.* Control-flow checking via regular expressions / A. Benso, S. Di Carlo, G. Di Natale, P. Prinetto, L. Tagliaferri // Proc. 10th Asian Test Symposium.- Kyoto.- 2001. P. 299-303. [Online]. Available: http://dl.acm.org/citation.cfm?id= 872025.872649
17. *Vladimir Hahanov*. Cyber Physical Computing for IoT-driven Services. New York. Springer. 2018. 279p.
18. *Hahanov V.I.* Qubit technologies for analysis and diagnosis of digital devices / VI Hahanov, T. Bani Amer, SV Chumachenko, EI Litvinova // Electronic Modeling. Vol. 37, no. 3. 2015. P. 17-40.
19. Hahanov V.I. Kubitnie strukturyi dannyih vyichislitelnyih ustroystv / V. I. Hahanov, V. Garibi, E. I. Litvinova, A. S. Shkil // Elektronnoe modelirovanie. 2015. T. 37, # 1. S. 76-99.
20. *Hahanov I.* QuaSim – Cloud Service for Digital Circuits Simulation / I. Hahanov, W. Gharibi, I. Iemelianov, T. Bani Amer // Proc. of IEEE East-West Design & Test Symposium. 2016. Yerevan, Armenia. P. 363-370.

Надійшла до редколегії 02.06.2018

Рецензент: д-р техн. наук, проф. Дрозд О.В.

Соклакова Тетяна Ігорівна, інженер кафедри АПОТ ХНУРЕ. Наукові інтереси: проектування та тестування цифрових систем. Хобі: подорожі. Адреса: Україна, 61166, Харків, пр. Науки, 14, e-mail: tetiana.soklakova@gmail.com.

Абдуллаєв Вугар Гаджимахмудович, канд. техн. наук, доцент кафедри «Комп'ютерна інженерія технології та програмування» Азербайджанської Державної Нефтяної Академії (АДНА), Інститут Кібернетики НАНА. Наукові інтереси: інформаційні технології,

веб-програмування, мобільні додатки. Захоплення: электронна комерція, B2B, B2C проекти, наукові книги, спорт. Адрес: Азербайджан, AZ1129, Баку, ул. М. Гади, 53, кв. 81, тел. (99412)5712428, (050)3325483, e-mail: abdulvugar@mail.com

Хаханов Володимир Іванович, д-р техн. наук, проф., головний науковий співробітник кафедри АПОТ ХНУРЕ. Наукові інтереси: проектування та тестування цифрових систем. Хобі: футбол, гірські лижи. Адрес: Україна, 61166, Харків, пр. Науки, 14, e-mail: hahanov@icloud.com.

Soklakova Tetyana Igorevna, engineer, Design Automation Department, NURE. Scientific interests: design and test of digital systems. Hobbies: Traveling. Address: Ukraine, 61166, Kharkiv, Nauka Ave, 14, e-mail: tetiana.soklakova@gmail.com

Abdullaev Vugar Gadzhimakhmudovich, Cand. tech. Sci., Associate Professor of Computer Engineering and Technology Programming at the Azerbaijan State Oil Academy (ASAN), Institute of Cybernetics of ANAS. Scientific interests: information technology, web programming, mobile application. Hobbies. e-commerce, B2B, B2C projects, science books, sports. Address: Azerbaijan, AZ1129, Baku, M. Gadi, 53, apt. 81, tel. (99412) 5712428, (050) 3325483, e-mail: abdulvugar@mail.com

Hahanov Vladimir Ivanovich, Dr., Prof., Chief Scientific Officer, Design Automation Department, NURE. Scientific interests: design and testing of digital systems. Hobby: football, downhill skiing. Address: Ukraine, 61166, Kharkov, Science, 14, e-mail: hahanov@icloud.com.

РЕФЕРАТИ

УДК 537.8.029.6;621.37.029.6

СВЧ сенсор швидких трансформацій властивостей біологічних рідин / Чан Лю, І.М. Бондаренко, О.Ю. Панченко, М.І. Сліпченко // Радіоелектроніка та інформатика. 2018. № 2. С. 5-10.

Проаналізована схема НВЧ сенсора, для якої можна створити сувору аналітичну модель. Розглянута задача опису полів у робочій області такого сенсора. Представлена схема допускає можливість використання математичної моделі і для тієї частини завдання, яка відноситься до трансформації властивостей досліджуваного об'єкта. Обговорені попередні результати розрахунків компонент електромагнітного поля в робочій області сенсора, дана оцінка її розмірам.

Іл. 4. Бібліогр.: 25 назв.

УДК 621.382

Технологія кодування передбачених кадрів в інфокомунікаційних системах / В.В. Хіменко // Радіоелектроніка та інформатика. 2018. №1. С. 11-16.

Розглянуто метод кодування інформативних елементів послідовності передбачених кадрів з урахуванням особливостей інформативної складової диференційно-описаної спектрограми. Запропоновано підхід, заснований на обробці ДОС за блоковим принципом. Показано, що таким чином досягається зниження інформаційної інтенсивності відеоданих без погіршення показників достовірності відеопотоку.

Бібліограф.: 20 назв.

УДК 519.713

Технологічна концепція диференційованої обробки сегментів відеокадру з урахуванням наявності ключової інформації / Д.О. Медведєв // Радіоелектроніка та інформатика. 2018. №1. С. 17-21.

Обгрунтовано підхід до формування ядра технологічної концепції диференційованої обробки сегментів відеокадру, що ураховує наявності ключової інформації. Запропонований підхід дозволяє, з одного боку, знизити складність процесів синтаксичного представлення, а з іншого боку - забезпечити заданий рівень достовірності відеоінформації, тобто, здійснювати режим обробки з контрольованою втратою якості реконструйованих відеокадрів.

Бібліограф.: 10 назв.

ABSTRACTS

UDC 537.8.029.6;621.37.029.6

Microwave sensor of fast transformations of biological liquids / Chang Liu, I.N. Bondarenko, A.Yu. Panchenko, N.I. Slichenko // Radioelectronics & Informatics. 2018. № 2. P. 5–10.

Electrodynamic measuring instruments have high speed. They make it possible to trace the process of changes in the state of the bioobject. Practical problems in the use of electrodynamic methods are due to the cumbersome process of determining the transfer function of the microwave sensor. In the paper, the microwave sensor circuit is analyzed, for which it is possible to create a rigorous analytical model. The problem of describing fields in the working area of such a sensor is considered. Preliminary results of calculations of electromagnetic field components in the working region of the sensor are discussed, and its dimensions are estimated.

Fig. 4. Ref.: 25 items.

UDC 621.382

Technology of encoding of predicted frames in infocommunication systems / V.V. Himenko // // Radioelectronics & Informatics. 2018. № 2. P. 11-16.

The method of encoding informative elements of the sequence of predicted frames with consideration of the features of the informative component of differential-described spectrograms is considered. The approach based on DOS processing for block decision is proposed. It is shown that this way the reduction of the information intensity of video data is achieved without deteriorating the reliability of the video stream.

Ref.: 10 items.

UDC 519.713

The technological concept of differentiated processing of video frame segments, taking into account the availability of key information / D.O. Medvedev // Radioelectronics & Informatics. 2018. № 2. P. 17-21.

The approach to the formation of the technological concept of differentiated processing of segments of a video frame, which takes into account the availability of key information, is substantiated. The proposed approach allows, on the one hand, to reduce the complexity of the processes of syntactic representation, and on the other hand - to provide a specified level of reliability of video information, that is, to implement a processing mode with controlled loss of quality of reconstructed video frames.

Ref.: 10 items.

УДК 004.627

Прогнозування параметрів внесених спотворень при стисненні зображень з втратами / С.С. Кривенко, М.С. Зряхов, В.В. Лукін // Радіоелектроніка та інформатика. 2018. № 2. С. 22–29.

Проаналізована залежність середньоквадратичної похибки (СКП)спотворень, що вносяться під час стиснення зображень із втратами від кроку квантування для сучасного кодеру на основі дискретного косинусного перетворення (ДКП) та схеми розбиття. Показано, что поведінка залежності визначається як ступенем складності (насиченості) зображення, так і характеристиками завад, що можуть бути присутніми на зображенні, яке стискається. Запропоновані метод та засоби прогнозування СКП, які дозволяють обирати крок квантування з урахуванням вимог до рівня спотворень, що вносяться. Прогнозування виконується значно швидше, ніж саме стиснення.

Табл. 1. Іл. 7. Бібліогр.: 17 назв.

UDC 004.627

Prediction of introduced losses parameters in in sossy image compression / S.S. Krivenko, M.S. Zriakhov, V.V. Lukin // Radioelectronics & Informatics. 2018. № 2. P. 22-29.

A dependence of of introduced losses mean square error (MSE) in lossy image compression on quantization step for modern coder based on discrete cosine transform and partition scheme is analyzed. It is shown that dependence behavior is determined by both image complexity and noise characteristics if noise is present in images to be compressed. The method and tools for MSE prediction that allow choosing quantization step taking into account acceptable level degradations. Prediction is carried out much faster than just compression.

Tab. 1. Fig. 7. Ref.: 17 items.

УДК 004.056.53

Безпека інтернет ресурсів: аналіз розповсюдженості загроз та технології захисту / О.В. Слободянюк, А.В. Хаханова, Д.І. Комолов // Радіоелектроніка та інформатика. 2018. № 2. С. 30–34.

Описані основні підходи до класифікації відомих вразливостей веб-ресурсів, проведено аналіз активності найбільш розповсюджених типів загроз на основі звітів компаній, що займаються моніторингом інцидентів порушення безпеки веб-ресурсів, а також розглянуто основні технології захисту від можливих реалізацій погроз.

Іл. 3. Бібліогр.: 10 назв.

UDC 004.056.53

Internet Security: Analysis of Distributed Threats and Security Technology / O. Slobodyanyuk, A.V. Khakhanova, D.I. Komolov // Radioelectronics & Informatics. 2018. № 2. P. 30-34.

The article describes the main approaches to classifying known vulnerabilities in web resources, analyzes the activity of the most common types of threats based on reports from companies involved in the monitoring of incidents of security of web resources, as well as the main technologies of protection against possible implementations threats.

Fig. 3. Ref.: 10 items.

УДК 658:512.011:681.326:519.713

Синтез та аналіз логічних Х-функцій / М.М. Любарський, В.Г. Абдуллаєв, В.І. Хаханов, С.В. Чумаченко, Є.І. Литвинова, І.В. Хаханов // Радіоелектроніка та інформатика. 2018. № 2. С. 35-44.

Представлені моделі і методи кубітного синтезу та аналізу логічних Х-функцій (xor, not-xor) від n змінних, які є потужним математичним засобом для вирішення завдань генерації тестів, моделювання несправностей, створення тестопригодності схем. Їх основна перевага полягає в можливості перевірки несправностей, які є інверсними по відношенню до справної поведінки логічної схеми. Це означає, що будь-який вхідний набір перевіряє 50 відсотків всіх вхідних дефектів. Дана властивість використовується тестувальниками для синтезу тестопригодності схем, дедуктивних формул моделювання несправностей.

Іл. 7. Бібліогр.: 8 назв.

UDC 658:512.011:681.326:519.713

Synthesis and analysis of logical X-Functions / M.M. Lyubarsky, V.G. Abdullaev, V.I. Khakhanov, S.V. Chumachenko, E.I. Litvinova, I.V. Khakhanov // Radioelectronics & Informatics. 2018. № 2. P. 35-44.

Models and methods of qubit synthesis and analysis of logical X-functions (xor, not-xor) of n variables are presented, which are a powerful mathematical tool for solving problems of test generation, simulation of faults, creating testable circuits. Their main advantage lies in the verifiability of faults that are inverse to the correct behavior of the logic circuit. This means that any input set checks 50 procents of all input defects. This property is used by testers to synthesize dough-like circuits, deductive fault simulation formulas.

Fig. 7. Ref.: 8 items.

УДК 004.056.53

Багаторівневий підхід до захисту від несанкціонованого використання додатків в операційній системі Android / Л.М. Куперштейн, О.П. Войтович, А.В. Остапенко-Боженова, С. А. Прокопчук // Радіоелектроніка та інформатика. 2018. № 2. С. 45–50.

Розглянуто особливості безпеки додатків у операційній системі Android, показана необхідність покращення захисних механізмів. Набула подальшого розвитку модель захисту Android-додатку від несанкціонованого використання, яка відрізняється своєю багаторівневою структурою з перекриттям загроз. Наведена загальна багаторівнева модель захисту додатку. Розроблено модель роботи віддаленого контролю додатком, яка включає функції: блокування додатку, очищення даних додатку, створення резервної копії даних, відновлення даних. Розроблено модель роботи багатофакторної автентифікації, в якій використовується апаратний токен з Bluetooth-підключенням до мобільного пристрою. На основі запропонованої багаторівневої моделі розроблено програмний модуль для захисту від несанкціонованого використання Android-додатку у вигляді бібліотеки, що дозволяє забезпечити захист від загроз конфіденційності, цілісності та доступності.

Іл. 4. Бібліогр.: 13 назв.

UDC 004.056.53

Multilevel approach to unauthorized use protecting of the Android applications / L. Kupershtein, O. Voitovych, A. Ostapenko-Bozhenova, S. Prokopchuk // Radioelectronics & Informatics. 2018. № 2. P. 45-50.

The security features of Android applications are discussed, the need to improve the protection mechanisms is shown in the article. The unauthorized use protecting model of the Android application, which is distinguished by its multi-level structure with overlapping threats, is developed. The general multi-level model for application protection is presented in the article. A model of the application remote control is developed and includes such functions: blocking the application, clearing the application data, creating a backup data, restoring data. The multi-factor authentication model which uses a hardware token with a Bluetooth connection to the mobile device is developed. Based on the proposed multi-level model, a software module of unauthorized use protection of the Android application in the library form, which allows protection against threats of confidentiality, integrity and accessibility, is proposed.

Fig. 4. Ref.: 13 items.

УДК 621.397

Розробка інформаційної технології оперативної та конфіденційної доставки відеоінформаційного ресурсу в системі критичної інфраструктури / В.В. Баранник, Д.С. Гаврилов, А.Д. Сорокун // Радіоелектроніка та інформатика. 2018. № 2. С. 51–54.

Розроблено інформаційну технологію оперативної та конфіденційної доставки відеоінформаційного ресурсу в системі критичної інфраструктури за рахунок захисту блоків, що містять контурну інформацію. Виявлення контурної інформації відбувається за допомогою аналізу блоку розробленою метрикою. Виявлена можливість класифікації блоків за контурною насиченістю з метою подальшої обробки.

Табл. 3. Іл. 2. Бібліогр.: 12 назв.

UDC 621.397

Development information technology operative and confidential delivery of a video information resource in the critical infrastructure system / V.V. Barannik, D.S. Havrylov, A.D. Sorokun // Radioelectronics & Informatics. 2018. № 2. P. 51-54.

The information technology operative and confidential delivery of a video information resource in the critical infrastructure system has been developed by protecting blocks containing contour information. The detection of contour information occurs through the analysis of the block developed by the metric. The possibility of classifying blocks by contour saturation for the purpose of further processing is revealed.

Tab. 3. Fig. 2. Ref.: 12 items.

УДК 004.771

Технологія автентифікації виборців у відкритій системі інтернет голосування / І.О. Мочалін, В.М. Вишняков, О.О. Комарницький // Радіоелектроніка та інформатика. 2018. № 2. С. 55-62.

Запропоновано технологію дистанційної автентифікації виборців у відкритій системі ІГ з використанням біологічних або інших додаткових ознак, що усуває можливість передачі права голосу іншій особі і дозволяє позбутися обов'язкової очної перевірки осіб виборців перед кожним актом волевиявлення, що особливо важливо у разі тривалих відряджень виборців. При цьому збережено усі позитивні якості відкритої системи, включаючи повну контрольованість процесів на сервері ІГ в режимі реального часу.

Іл. 4. Бібліогр.: 12 назв.

УДК 004.771

Voter Authentication Technology In The Open Internet Voting System // Radioelectronics & Informatics. 2018. № 2. P. 55-62.

This article proposes a technology for remote authentication of voters in an open IV system using biological or other additional attributes that excludes the possibility of transferring the right to vote to another person and allows to get rid of the obligatory full-time identity check of the voters before each vote, which is especially important in case of long-term business trips. At the same time, all the advantages of the open system are preserved, including the process controllability on the IV server in real time.

Fig. 4. Ref.: 12 items.

УДК 004.934:681.391

Оцінка ефективності методів ідентифікації аудіосигналів в умовах впливу хаотичних імпульсних завад / О.К. Юдін, Р.В. Зюбіна // Радіоелектроніка та інформатика. 2018. № 2. С. 63-66.

Проведено оцінку ефективності розроблених методів ефективної ширини спектру та найбільшої інформаційної ваги основного тону в задачі ідентифікації диктора при наявних завадах. Визначено, що в результаті впливу хаотичних імпульсних завад можливість ідентифікації диктора в бігатоальтернативних задачах прийняття рішення різко знижується при співпадіння частоти основного тону мовленнєвого сигналу і початкової частоти імпульсної завади для методу найбільшої інформаційної ваги основного тону. Метод ефективної ширини спектру забезпечує високі показники ідентифікації в умовах впливу такого типу завад для текстозалежної ідентифікації.

Табл. 3. Іл. 5. Бібліогр.: 4 назв.

UDC 004.934:681.391

Effectiveness evaluation of methods for the audio signals identification in terms of the chaotic impulse interference impact / O.K. Judin, R.V. Ziubina // Radioelectronics & Informatics. 2018. № 2. P. 63-66.

An estimation of efficiency of the developed methods of effective spectrum width and the greatest informational weight of the main tone in the task of the speaker identification in the presence of disturbances were carried out. It is determined that as a result of the influence of chaotic pulsed noise the possibility of speaker identification a in bi-alternative decision-making problems decreases sharply when the frequency of the main tone of the speech signal and the initial frequency pulse noise for the method of the largest information weight of the main tone were coincided. Method of effective spectrum width provides high identification rates under the influence of this type of noise for text-dependent identification.

Tab. 3. Fig. 5. Ref.: 4 items.

УДК 658:512.011:681.326:519.713

Архітектури та методи кубітного логічного моделювання кіберсоціальних процесів / Т.І. Соклакова, В.Г. Абдуллаєв, В.І. Хаханов // Радіоелектроніка та інформатика. 2018. № 2. С. 67-90.

Запропоновано моделі, структури даних, архітектури та методи логічного аналізу соціальних процесів, пов'язаних з підвищенням якості життя, збереженням екології планети і усуненням соціальних колізій. Введено кубітні структури даних, які описують багатозначні змінні, необхідні для створення еталонних зразків логічних архітектур, які задають поведінку громадян і соціальних груп. Запропоновано квантовий метод кубітного моделювання інформаційних потоків для пошуку деструктивних процесів і явищ в соціальних мережах за ключовими словами і фразами. Розглянуто архітектури кіберфізичного соціального комп'ютингу на основі монторінгу контенту в соціальних мережах, моделювання даних на еталонних логічних схемах деструктивної поведінки людини з метою запобігання соціальних колізій за рахунок актюаторного управління поведінкою громадян. Архітектури, методи і засоби кубітного цифрового моделювання протестовані на реальних прикладах аналізу контенту, взятого з соціальних мереж. Показані можливі напрямки розвитку отриманих результатів, пов'язаних зі створенням кібермедичного, кіберюридичного, кібертранспортного комп'ютингу.

Табл. 4. Іл. 27. Бібліогр.: 20 назв.

UDC 658: 512.011: 681.326: 519.713

Architecture and methods of qubit logical modeling for cyber-social processes / T.I. Soklakova, V.G. Abdullaev, VI Hakhanov // Radioelectronics & Informatics. 2018. № 2. P. 67-90.

Models, data structures, architectures and methods of logical analysis of social processes associated with improving the quality of life, conservation of the ecology of the planet and the elimination of social conflicts are proposed. Qubit data structures that describe multivalued variables are needed to create reference samples of logical architectures that set the behavior of citizens and social groups. The quantum method of qubit modeling of information flows for the search of destructive processes and phenomena in social networks by keywords and phrases is proposed. The architecture of cyberphysical social computing on the basis of content monture in social networks, modeling of data on standard logical schemes of destructive behavior of a person with the purpose of prevention of social collisions at the expense of actuator management of citizens' behavior is considered. Architecture, methods and tools of qubit digital modeling are tested on real examples of content analysis from social networks. The possible directions of development of the obtained results related to the creation of cyber-medical, cyber-legal, and cyber-transport computer are shown.

Tab. 4. Fig. 27. Ref.: 20 items.

ПРАВИЛА

оформления рукописей для авторов научно-технического журнала "Радиоэлектроника и информатика"

Тематика: радиотехника; электроника; телекоммуникации; компьютерные науки; компьютерная инженерия и техническая диагностика; системы и процессы управления; информационные технологии в науке, образовании, культуре, медицине, экономике, экологии, социологии.

Формат страницы ─ А4 (210х297 мм), все поля – 20 мм. Количество колонок – 2, интервал между ними – 5 мм. Редактор Page Maker 6.0 или Word, гарнитура Times ET, (Times New Roman Cyr), кегль – 10 пунктов, межстрочное расстояние ─ 110%, табуляция ─ 5 мм. Объем рукописи – от 2 до 7 с. (языки: русский, украинский, английский).

Согласно решению редакционной коллегии, основанному на Постановлении ВАК Украины от 15.01.2003 №7-05/1 (Бюллетень ВАК Украины, №1, 2003, с.2), текст рукописи должен быть структурирован и содержать все *основные части, характерные для научной статьи*: **введение** (отражает *актуальность*, формулирование *цели* и *задач* исследования); **сущность** (изложение основного материала исследования с описанием идеи, метода, и обоснованием полученных научных результатов); **выводы** (отражают результаты исследования, их *научную новизну* и *практическую значимость*, сравнение с лучшими аналогами, перспективы).

Оформление рукописи: УДК, заголовок, фамилия и инициалы, аннотация, текст, литература, реферат (на украинском и английском языках), сведения об авторах.

ОБРАЗЕЦ ОФОРМЛЕНИЯ

УДК 519.713

НАЗВАНИЕ РУКОПИСИ

ФАМИЛИЯ И.О.

(*Название желаемого раздела тематики*)

Аннотация (на языке статьи, абзац 5-10 строк, кегль 9) помещается в начале статьи и содержит информацию о результатах описанных исследований.

Ключевые слова (Key words) приводятся (на языке статьи и на английском языке).

Основной текст следует разделять на **подразделы 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 под иллюстрацией (вне рисунка), как показано на рис. 1.

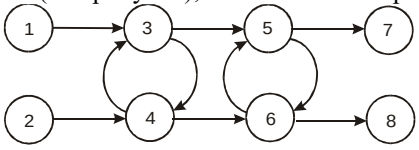


Рис. 1. Граф с контурами

Табличный заголовок располагается справа над таблицей (вне таблицы), что иллюстрируется табл.1. Редакторы: CorelDraw, Table Editor, Microsoft Excel.

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. Формулы, символы, переменные, встречающиеся в тексте, должны быть набраны как объекты Microsoft Equation. Рекомендуемая высота формульных кеглей: переменная – 10 пунктов, индекс – 8, над- и подиндекс – 8, основной (индексный) математический символ – 12(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 высоты кегля, которые рекомендуется опускать (поднимать) на 17 (33) % относительно основной строки.

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

Транслитерированный список литературы**,** в соответствии с требованиями наукометрических баз, является полным аналогом списка литературы и выполняется на основе транслитерации языка оригинала латиницей. При этом число и порядок источников в списке литературы должны оставаться неизменными. Ссылки на англоязычные источники не транслитерируются. Транслитерация украинского языка латиницей выполняется на основе Постановления Кабинета Министров Украины № 55 от 27 января 2010 (http://zakon2.rada.gov.ua/laws/show/55-2010-% D0% BF), русского – на основе ГОСТ 7.79-2000 (ISO 9-95) (http://protect.gost.ru/document.aspx?control=7&id=130715).

Рекомендуется использовать автоматические средства транслитерации (http://translit.net).

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

Литература: 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.

Транслитерированный список литературы.

Поступила в редколлегию 00.00.00

Рецензент: должность, ученая степень, фамилия, И.О.

Фамилия, имя, отчество, ученая степень, звание, должность и место работы. Научные интересы. Увлечения и хобби. Адрес, контактные телефоны.

Сведения об авторах на английском языке.

Рефераты на украинском, русском и английском языках.

УДК 000.000.00
Назва статті / Ініціали. Прізвище. // Радіоелектроніка та інформатика. 2000. № 00. С. 00–00.
Текст реферату.
Табл. 00. Іл. 00. Бібліогр.: 00 назв.

УДК 000.000.00
Название статьи / Инициалы. Фамилия. // Радиоэлектроника и информатика. 2000. № 00. С. 00–00.
Текст реферата.

UDC 000.000.00
Title of paper / Initials. Surname // Radioelektronika i informatika. 2000. N 00. P. 000-000.
Text.
Tab. 00. Fig. 00. Ref.: 00 items.

Представление материалов

Рукопись, рефераты, сведения об авторах – в одном файле, *поименованном фамилией автора*. Твердая копия материалов – для граждан Украины — в одном экземпляре: рукопись, подписанная авторами, рефераты, внешняя рецензия, подписанная доктором наук, заявление на имя главного редактора со сведениями об авторах. Материалы, не соответствующие требованиям, редколлегией не рассматриваются.

Адрес редакции: Украина, 61166, Харьков, просп. Науки, 14, ХНУРЭ, комната 321, тел. 70-21-326.
E-mail: hahanov@icloud.com

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки (протокол № 12 від 15.06.2018)

Підписано до друку 27.06.2018. Формат 60×84 1/8.

Умов. друк. арк. 10,3. Зам. № б/н . Тираж 300 прим. Ціна договірна.

Віддруковано у СПД ФО Степанов В.В.

61168, Харків, вул. Акад. Павлова, 311.