В режимі зміни параметрів програма забезпечує користувачеві додатковий сервіс в його роботі. Наприклад, вибір поточного каталогу дозволяє реалізувати швидкий доступ до файлів з даними для розрахунку. Для розрахунку декількох файлів у програмі передбачено режим пакетного вводу даних.

Технічні переваги комплексу

- наявність можливості запису спектру сигналу для подальшої обробки;
- більш достовірні результати виявлення сигналів завдяки спеціальному алгоритму управління, особливо в умовах складної радіозавадної обстановки та при наявності коротких радіосигналів;
- організація конвеєрного принципу спецдосліджень шляхом розділення процесів підготовки, вимірювань і обробки результатів на програмному і апаратурному рівні;
- повноцінне функціонування комплексу в багатозадачному режимі Windows, що надає можливість одночасно проводити вимірювання і підготовку звітних документів та ін.;
- можливість формування звітних документів в даних шаблонах, наприклад, “Акт инструментальной проверки защищенности объекта ЭВТ” і “Предписание на эксплуатацию” (відповідно до вимог нормативних документів);
- можливість використання модифікованого комплексу для вирішення інших спеціальних задач (електромагнітна сумісність, пошук закладних пристроїв, оцінка спектру радіовипромінювань, виявлення надкоротких передач та ін.).

Організаційні переваги комплексу

- відкритість методики проведення розрахунків, наявність доступу до проміжних результатів розрахунків, можливість корегування даних;
- наявність тестового програмного забезпечення з відкритим вихідним текстом програми;
- наявність лінійного режиму вимірювань, завдяки чому збільшується точність вимірювань;
- можливість постійної модернізації програмного забезпечення відповідно до вимог замовника.

Порівняльні випробування комплексу

За базу для порівняння беремо комплекс “Навигатор” (Росія) – єдиний зарубіжний комплекс подібного класу, який використовується в Україні на даний час. Вітчизняних аналогів немає.

Порівняльні випробовування вищеназваних комплексів, а також контрольні розрахунки результатів досліджень показали, що імовірність виявлення каналів витоку інформації при використанні комплексу “АСТРА” в середньому на 10% більша. Причиною цього є те, що при використанні комплексу “Навигатор” 1) рівень сигналу, який вимірюється, перевищував верхню межу аналізатора; 2) при виявленні широкосмугового сигналу можлива втрата сигналу; 3) неможливо вимірювати низькочастотні сигнали (від 10 Гц до 9 кГц); 4) мають місце недоліки в методиці верифікації та ін.

При виконанні розрахунків потенційних загроз ручним методом числові значення, одержані при дослідженні, необхідно перерахувати, користуючись графіками. Якщо значення попадає між двома лініями, оператор повинен або інтуїтивно, або інтерполяцією вибрати конкретне числове значення. В подальшому оператор повинен внести корегуючі коефіцієнти, які також визначаються з графіків. Таким чином, незалежно від кваліфікації і бажання оператора при розрахунках виникає інструментальна помилка.

Крім цього, при ручних розрахунках можуть виникати помилки, обумовлені людським фактором.

Експериментальні дослідження показали, що при ручному методі розрахунку помилка в середньому з’являється у 25% випадків.

УДК 681.325.59:519.6

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОРРЕКТИРУЮЩИХ СВОЙСТВ ПЕРЕКЛЮЧАТЕЛЬНЫХ ФУНКЦИЙ

Оксана Тарасенко-Клятченко
НТУУ "КПИ"

Анотація: **Запропоновано характеристики абсолютної та відносної автокоригуючої властивості перемикальних функцій та методика їх отримання для оцінки та порівняння ступеня розвитку автокоригувальних властивостей перемикальних функцій. Наведені приклади.**

Summary: **The characteristics of absolute and relative self-correction ability of switching functions are offered and a technique of their reception for an estimation and comparison of a self-correction properties level of switching functions are developed. Examples are given.**
Ключевые слова: **Автокоррекция, *k*-значная функция.**

I Введение

Защита информации в компьютерных системах и сетях как комплексное направление научного поиска [1] наряду со многими другими его составными частями включает исследования, развивающие и конкретизирующие общетехнические задачи анализа и синтеза относительно таких качеств информации, как ее целостность и достоверность.

При этом аналитический аспект таких исследований состоит из трех основных субаспектов:

1) установление эффективной и полной системы численных и функциональных характеристик целостности информации и ее достоверности;

2) прогнозирование изменения таких характеристик в зависимости от действия дестабилизирующих факторов;

3) прогнозирование последствий нарушения указанных качеств информации.

Синтетический же аспект (разработка, проектирование) таких исследований имеет целью создание методов и средств обеспечения необходимого уровня качеств целостности и достоверности информации.

Нарушение целостности и достоверности информации может быть умышленным и неумышленным, то есть, может быть антропогенным или техногенным. Нарушения технического происхождения как правило вызываются неисправностями, отказами или сбоями в работе технического и программного обеспечения компьютерных систем и сетей.

В технических средствах действие этих факторов проявляется в искажении управляющих и информационных сигналов. Вообще эти сигналы могут относиться к разным иерархическим уровням процесса обработки информации в компьютерных системах и сетях. Поэтому и исследования влияния их искажения на показатели целостности и достоверности информации целесообразно проводить, ориентируясь на общепринятое разделение как процесса обработки информации, так и собственно технических средств на иерархические уровни. В последовательности этих уровней логический уровень обычно [2] называется вторым (после физического уровня – электрического), и отвечает канальному уровню процесса передачи информации [3].

II Постановка задачи

В работе [4] показано, что комбинационные схемы, работающие в k-значном алфавите ($k\geq 2$) в большей или меньшей степени обладают свойством формировать правильные значения выходных сигналов в случаях, когда на их входах действуют сигналы с однократными детерминированными искажениями. Это свойство было названо автокоррекцией и обусловлено естественной избыточностью переключательных функций, описывающих работу комбинационных схем. Если функция принимает одинаковые значения на некоторых двух наборах аргументов, то тем самым она становится нечувствительной к искажениям, переводящим один набор аргументов в другой. Автокоррекция не свойственна только функциям, которые при $k=2$ на любой паре соседних (по Квайну) наборов принимают разные значения. Для $k=2$ это будут функции с равными количествами нулей и единиц в их таблицах истинности, которые, кроме того, должны быть еще размещены в "шахматном" порядке, а именно: функция суммы по модулю 2 и ее отрицание. Если же при $k=2$ количества единиц и нулей в таблице истинности не равны, то функция обязательно обладает автокорректирующими свойствами.

В связи с изложенным представляет интерес разработка методики оценки и сравнения автокорректирующих свойств переключательных функций различных типов, определенных при любых значностях k структурного алфавита и произвольном числе аргументов n.

III Основная часть

Далее будем считать, что переключательная функция $f(X)$, где $X=(x_1, x_2, ..., x_n)$, принимает значение $\alpha \in E_k = \{0,1,...,k-1\}$ на фиксированном наборе аргументов $A=(a_1, a_2, ..., a_n)$, $a_i \in E_k, i=\overline{1,n}$, то есть, когда $x_1=a_1$, $x_2=a_2$, …, $x_n=a_n$. Будем называть соседними два набора значений аргументов $A=(a_1, a_2, ..., a_n)$ и $B=(b_1, b_2, ..., b_n)$, которые отличаются по некоторой i-й компоненте, причем $a_i=b_i\pm 1 \ (mod\ k)$. Очевидно, что этому определению соседних наборов полностью соответствует определение соседства по Квайну [2] для двузначных функций. Заметим, что формально определенному свойству логического соседства наборов A и B обычно соответствует физическое соседство состояний носителя информации, отображающих a_i и b_i

(уровней сигналов, их частот, фаз, длительностей и др.). При k=2 понятия физического и логического соседства, по существу, совпадают. Однако в случае k>2 свойство соседства более сложное, чем в двузначном случае, так как здесь есть "соседство сверху", когда, например, $a_i=\gamma$, $b_i=\gamma+1$, $\gamma \in E_k$, и "соседство снизу", когда $a_i=\gamma$, $b_i=\gamma-1$. Кроме того, здесь необходимо принять гипотезу о логическом соседстве значений *0* и $k-1$. Известные способы физического отображения букв структурного алфавита [5, 6] характеризуются как наличием физического соседства состояний носителя информации, соответствующих *0* и *k–1* (пространственный, фазо-импульсный, время-импульсный или таймерный способы), так и отсутствием такого соседства (уровневый и частотный способы). Поэтому далее будем считать, что значения $a_i=0$, $b_i=k-1$ являются соседними. Нетрудно проверить, что приведенное выше формальное определение не противоречит этой гипотезе.

В случае k=2 число наборов, соседних заданному набору, для функции n аргументов равно n. Если функция *f(X)* принимает одно и то же значение α на всех соседних к заданному набору A наборах аргументов, то это означает, что любое одиночное искажение набора A не приводит к утрате правильности значения функции *f(X)*, так как любое одиночное искажение набора A означает переход к соседнему набору.

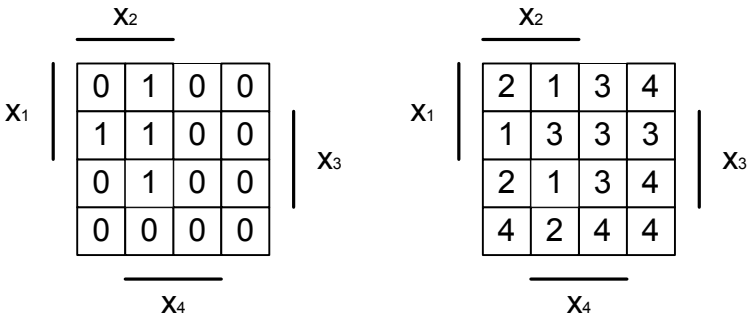
Для k-значной функции *f(X)*, где k>2, число наборов, соседних заданному набору A, составляет $2n$ вследствие отмеченного ранее соседства "сверху" и "снизу".

При оговоренных выше допущениях полную информацию о степени развития автокорректирующих свойств переключательной функции *f(X)* может дать характеристическая таблица, входная часть которой аналогична входной части таблицы истинности (возможно, в форме диаграммы Вейча или карты Карно), а в выходной части характеристической таблицы указывается число *m(A)* искажений набора A, к которым нечувствительна функция *f(X)* на данном наборе. Интегральной количественной характеристикой автокорректирующих свойств функции *f(X)* в таком случае может быть число M всех искажений наборов аргументов функции, к которым она нечувствительна, то есть

$$M = \sum_{\text{по всем } A} m(A) \qquad (1)$$

Далее число M будем называть абсолютной автокорректирующей способностью функции *f(X)*.

В качестве примера на рис. 1,а показана таблица булевой функции "три из четырех" (в форме диаграммы Вейча), а на рис.1,б – характеристическая таблица той же функции. Очевидно, что для функции "три из четырех" M=44. На рис. 2,а приведена таблица функции $min(x_1, x_2, x_3)$, а на рис. 2,б ее характеристическая таблица, где M=246.



а **б**

Рисунок 1 – Таблицы функции "Три из четырех"

Относительной количественной характеристикой автокорректирующих свойств переключательной функции *f(x)*, позволяющей производить сравнение различных функций, может служить отношение L числа автокорректируемых искажений к общему числу всех возможных искажений, которое при k=2 составляет $2^n n$, а при k>2 – $k^n 2n$. Например, для функции на рис. 1 L=44/64=11/16 а для функции на рис. 2 L=246/384=41/64 Далее L будем называть относительной автокорректирующей способностью функции *f(X)*.

Из числа двузначных функций, определенных при любых n, широкое применение в технических приложениях получили дизъюнкция, конъюнкция, функции Шеффера и Пирса [2]. Для этих функций характерно то, что их таблицы истинности содержат только один 0 (дизъюнкция, функция Шеффера) или только одну 1 (конъюнкция, функция Пирса). Это, в свою очередь, обуславливает то, что эти функции хотя и отличаются видом таблиц истинности и характеристических таблиц при одном и том же n, однако имеют

одинаковые характеристики M и L. На рис. 3,а и 3,б показаны таблицы истинности и характеристическая таблица конъюнкции для n=4. В этом случае M=56, L=7/8.

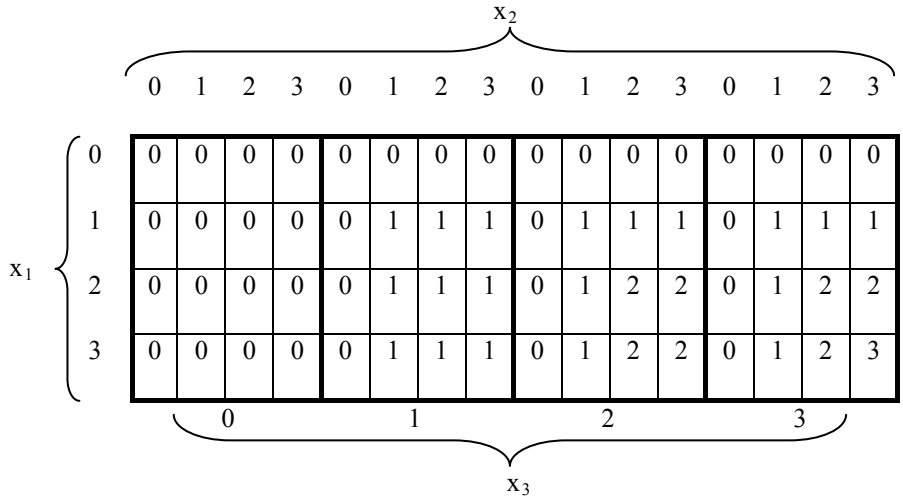


Рисунок 2, а – Таблица функции min(x_1, x_2, x_3)

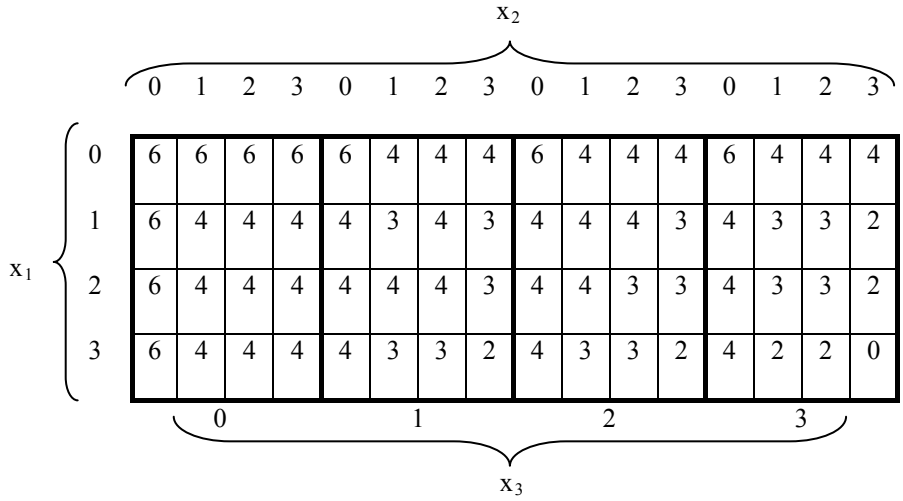


Рисунок 2, б – Характеристическая таблица функции min(x_1, x_2, x_3)

Нетрудно проверить, что для функций такого типа при произвольном n

$$M = 2n(2^{n-1} - 1) \tag{2}$$

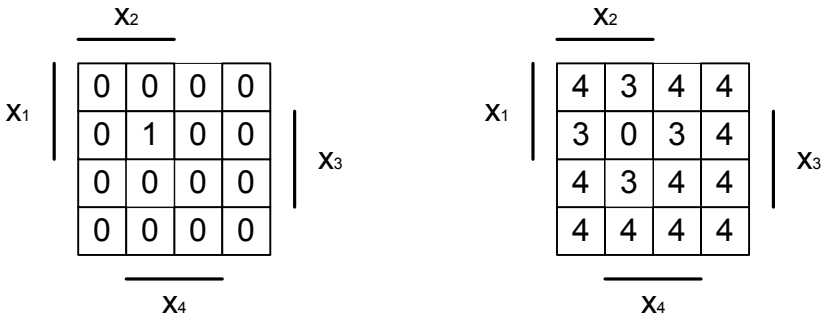


Рисунок 3 – Таблицы истинности и характеристическая таблица конъюнкции для n=4

$$L = \frac{2n(2^{n-1}-1)}{n2^n} = \frac{2^{n-1}-1}{2^{n-1}} \qquad (3)$$

Отсюда следует, что $L \to 1$ с ростом n, то есть, автокорректирующие свойства функций рассматриваемого класса усиливаются с увеличением числа их аргументов. В табл. 1 приведены результаты оценки характеристик M и L для некоторых типовых переключательных функций, определенных при различных n и k (здесь $u(x_1, x_2)$ и $p(x_1, x_2, \ldots, x_n)$ – функции переноса в старший соседний разряд при умножении и сложении по основанию k соответственно). Из таблицы следует, что определяющее значение для уровня развития автокорректирующих свойств переключательных функций имеет вид этих функций. При этом относительная автокорректирующая способность изменяется в широких пределах: от нулевой (для суммы по *mod k*) или очень низкой (для произведения по *mod k*), до значений, приближающихся к единице (для функций Шеффера, Пирса, конъюнкции и дизъюнкции при больших n).

Таблица 1 – Результаты оценки характеристик M и L для некоторых типовых переключательных функций, определенных при различных n и k

Функции	n	k			
		2	3	4	5
$Max(x_1,x_2,\ldots,x_n)$ $Min(x_1,x_2,\ldots,x_n)$	2	M=4, L=$\frac{1}{2}$	M=16, L=$\frac{4}{9}$	M=28, L=$\frac{7}{16}$	M=44, L=$\frac{11}{25}$
	3	M=18, L=$\frac{3}{4}$	M=108, L=$\frac{2}{3}$	M=246, L=$\frac{41}{64}$	
$x_1 \otimes x_2$ (mod k)	2	M=4, L=$\frac{1}{2}$	M=4k, L=$\frac{1}{k}$		
$u(x_1,x_2)$	2	Не существует	M=28, L=$\frac{7}{9}$	M=44, L=$\frac{11}{16}$	M=64, L=$\frac{16}{25}$
$p(x_1,x_2,\ldots,x_n)$	2	M=4, L=$\frac{1}{2}$	M=20, L=$\frac{5}{9}$	M=40, =$\frac{5}{8}$	M=68, =$\frac{17}{25}$
	3	M=12, L=$\frac{1}{2}$			
	4	M=32, L=$\frac{1}{2}$			
	5	M=80, L=$\frac{1}{2}$			
"3 из 4"	4	M=44, L=$\frac{11}{16}$			
Голосования (мажоритарная)	3	M=12, L=$\frac{1}{2}$			
	5	M=100, L=$\frac{5}{8}$			
Шеффера, Пирса, дизъюнкция, конъюнкция	произвольное	M=$2n(2^{n-1}-1)$ L=$\frac{2^{n-1}-1}{2^{n-1}}$			

IV Выводы

Как правило, зависимость относительной автокорректирующей способности L от n неубывающая, что обусловлено пропорциональным увеличением числа соседних наборов с ростом n. Зависимость же L от k, как показывают рассмотренные примеры, имеет более сложный характер. Однако если функция принимает $k>2$

значений и хотя бы на двух соседних наборах ее значения совпадают (в этом случае M=2), то ее относительная автокорректирующая способность не ниже $\frac{2}{k^n 2n} = \frac{1}{k^n n}$. При k=2, $n \geq 2$ и минимальном, но не равном нулю количестве соседних наборов с одинаковыми значениями функции, абсолютная автокорректирующая способность равна $2n$ и поэтому для этого случая $L = \frac{2n}{2^n n} = 2^{-n+1}$.

Таким образом, предложенные выше характеристики абсолютной и относительной автокорректирующей способности переключательных функций и методика их получения позволяют оценивать и проводить сравнение степени развития автокорректирующих свойств переключательных функций.

Литература: 1. Збитнев С., Коновалов И., Меалковский Д., Поляков А. Контроль и восстановление целостности информации в автоматизированных системах / К.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2002, № 4. – с. 119–128. 2. Самофалов К. Г., Корнейчук В. И., Тарасенко В. П. Цифровые ЭВМ. Теория и проектирование. – К.: Вища школа, 1989. – 424 с. 3. Тарасенко В., Коваль С. Імітаційне моделювання функціонування на канальному рівні відкритих мереж передачі даних в умовах загроз / К.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2001, № 3. – с. 219–221. 4. Тарасенко В. П., Тарасенко-Клятченко О. В. Автокоригуючі властивості логічних операцій / Хмельницький, Вимірювальна та обчислювальна техніка в технологіних процесах, 2001, № 8. – с. 334–337. 5. Самофалов К. Г., Корнейчук В. И., Романкевич А. М., Тарасенко В. П. Цифровые многозначные элементы и структуры. – К., "Вища школа", 1974, 168 с. 6. Tarasenko V. P. Logical Models of Elementary Automats in k-valued Alphabet. Engineering Simulation, Amsterdam, 1997, Vol. 14, p. p. 747–752.

УДК 621.96

ВОПРОСЫ ПОСТРОЕНИЯ КОМПЬЮТЕРОВ, ЗАЩИЩЕННЫХ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Сергей Чеховский
ООО «ЭПОС»

Аннотация: **Приведены основные положения построения защищенных компьютеров для работы как в автономном режиме, так и в составе локальной сети. Рассмотрены особенности мер технической защиты для различных применений.**
Summary: **In this paper are considered the basic principles of concept of building of TEMPEST computers intended for operation in autonomous mode as well as in local area networks. The measures on technical protection of information for different applications are considered.**
Ключевые слова: **Информация, информационная безопасность, техническая защита информации.**

Проблема защиты компьютеров от утечки информации по каналам побочных излучений известна уже давно. На западе широко применяется известная аббревиатура TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions).

История возникновения TEMPEST уходит своими корнями в далекий 1918 год, когда Herbert Yardley со своей командой был привлечен Вооруженными Силами США для исследования методов обнаружения, перехвата и анализа сигналов военных телефонов и радиостанций. Исследования показали, что оборудование имеет различные демаскирующие излучения, которые могут быть использованы для перехвата секретной информации, что серьезно обеспокоило Правительство США.

Однако, сама аббревиатура TEMPEST появилась только в конце 60-х начале 70-х годов, как секретная программа Министерства Обороны США по разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования.

Долгое время все, связанное с понятием TEMPEST, было окутано завесой секретности. Первое сообщение, появившееся в открытой печати, принадлежит голландскому инженеру Wim van Eck, опубликовавшему в 1985 году статью "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?". Статья посвящена потенциальным методам перехвата сигнала видеомониторов. В марте 1985 года на