УДК 681.3.06

А. И. ШУМОВ

МЕТОДЫ ОЦЕНКИ НЕЛИНЕЙНОСТИ БУЛЕВЫХ ФУНКЦИЙ

В современных информационных системах важная роль отводится криптографическим методам защиты информации, среди которых одно из основных мест занимает блочное и поточное шифрование.

В настоящее время в Украине отсутствует стандарт поточного шифрования, а в качестве стандарта блочного шифрования используется ГОСТ 28147-89, разработанный и введенный в действие в конце 80-х годов прошлого века. Очевидно, что в нынешних условиях Украине необходима разработка и ввод в действие национальных стандартов симметричного блочного и поточного шифрования, обеспечивающих высокий уровень безопасности.

Для обеспечения стойкости будущих алгоритмов необходимо применение криптографически стойких нелинейных преобразований (таблиц подстановок), которые, как правило, строятся на основе булевых функций нелинейного типа. Однако следует отметить, что в открытой литературе практически отсутствуют отечественные публикации по методике оценки нелинейности и криптографической стойкости булевых функций. Среди зарубежных публикаций можно отметить работу Уэбстера и Тавареса [1], где впервые вводится концепция строгого лавинного критерия (СЛК); работы [2 – 5], в которых проводится обобщение и сведение к единой концепции критерия распространения; в [6, 7] описывается техника построения криптографически сильных функций, удовлетворяющих критериям сбалансированности, высокой нелинейности и критерию распространения высокой степени, разработанная Себери, Чжанем и Чженем.

Одним из подходов к построению нелинейных преобразований вида $GF(2)^n \to GF(2)^m$ (S-блоков) является использование критериев нелинейности булевых функций $f:GF(2)^n \to GF(2)$, когда использование булевых функций с хорошими криптографическими свойствами необходимо для обеспечения аналогичных свойств всего S-блока. Кроме того широко используется понятие линейной структуры S–блоков: $S:GF(2)^n \to GF(2)^m$ имеет линейную структуру, если существует ненулевой вектор $a \in GF(2)^n$ совместно с нетривиальным отображением $LS:GF(2)^n \to GF(2)$ таким, что $LS(x+a)+LS(x)$ принимает одно и то же значение (0 или 1) для всех $x \in GF(2)^m$.

Структура S может быть описана булевыми функциями в алгебраической нормальной форме

$$f^q(x_1, x_2 \cdots, x_n) = a_0 + \sum a_i x_i + \sum a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \cdots x_n, \; 0 \le q \le m-1. \qquad (1)$$

Функция f^q является нелинейной (или не аффинной), если ее алгебраическая нормальная форма (многочлен Жегалкина) содержит в себе термы степени выше первой.

В данной статье основное внимание уделяется обзору известных подходов к оценке показателей нелинейности булевых функций, таких как расстояние до аффинных функций, расстояние до линейных структур и порядок нелинейности.

Расстояние до аффинных функций

Расстояние до ближайшей аффинной функции [9] определяется как расстояние от f до множества A(n), в виде

$$\delta(f) = \min_{L \in A(n)} d(f, L), \qquad (2)$$

где $d(f,L)$ есть расстояние Хэмминга между f и L, а $A(n)$ – множество всех аффинных функций $L(x_1,...,x_n) = a_0 + a_1 x_1 + ... + a_n x_n$. Таким образом, $\delta(f)$ есть расстояние от f до множества A(n). Для дальнейшего изложения свойств показателя δ необходимо введение нескольких дополнительных понятий.

Пусть $\Omega(n)$ означает группу всех обратимых преобразований пространства $GF(2)^n$, и пусть $AGL(n)$ означает подгруппу всех аффинных преобразований. Известно, что элементы $AGL(n)$ могут быть описаны как функция $\alpha(x) = A(x) + a$, где A есть невырожденная матрица $n \times n$ и $a \in GF(2)^n$. Для представления пары (α,f) $f \in \Phi(n)$ и $\alpha \in \Omega(n)$ принято использовать обозначение $\alpha \bullet f$. В этих терминах операция группы $\Omega(n)$ над множеством $\Phi(n) = \{f : [GF(2)]^n \to GF(2)\}$ определяется в виде

$$\alpha \bullet f(x) = f(\alpha(x)). \tag{3}$$

Более общим является описание свойств нелинейности с помощью оценочной функции D

$$D : \Phi(n) \to W, \tag{4}$$

которая принимает значения из множества W. Функция f должна быть выбрана из $D(f)$, $D(f) \in W_1$, где множество $W_1 \subset W$, в свою очередь, содержит булевы функции с необходимыми криптографическими свойствами.

Существенно, чтобы значения D оставались инвариантными над преобразованиями из $\Omega(n)$, которые являются криптографически слабыми [9]. Обычно $\Omega(n)$ содержит все аффинные преобразования.

Для определения критерия нелинейности рассматривается максимальная из подгрупп $I(D) \subseteq \Omega(n)$, которая оставляет D инвариантным, т.е.

$$I(D) = \{\alpha \in \Omega(n) | D(\alpha \bullet f) = D(f) \text{ для } \forall f \in \Phi(n)\} \tag{5}$$

В этом случае $I(D)$ называется группой симметрий D. Критерии нелинейности связаны с описанием группы симметрий.

Пусть H будет подмножеством $\Phi(n)$ и для всех $f \in \Phi(n)$ выполняется равенство $d_H(f) = \min_{h \in H} d(f,H)$. Для δ это будет множество $A(n)$ всех аффинных функций. Кроме того, пусть $\Omega(n)^H$ будет подгруппой группы $\Omega(n)$, состоящей из элементов, удовлетворяющих условию

$$\Omega(n)^H = \{\alpha \in \Omega(n) | \alpha \bullet h \in H \text{ для всех } h \in H\}. \tag{6}$$

Эта подгруппа называется группой симметрий множества H. Она обладает следующим свойством [9]:

Для любого подмножества $H \subset \Phi(n)$ группа симметрий d_H совпадает с группой симметрий H, то есть

$$I(d_H) = \Omega(n)^H, \tag{7}$$

откуда следует, что группа симметрий $I(\delta)$ для минимума расстояний δ до множества аффинных функций L есть аффинная группа $AGL(n)$.

Поскольку множество аналитических атак используют аффинные свойства криптографических преобразований, то для обеспечения стойкости S-блоков необходимо использование множества булевых функций W_1, которые имеют максимум минимального расстояния до множества аффинных функций, причём критерий отбора функций в W_1 должен оставаться инвариантным для множества $\Omega(n)$, содержащего все аффинные преобразования.

Расстояние до линейных структур

Линейная структура булевой функции $f:GF(2)^n \to GF(2)$ определяется существованием вектора $a \in GF(2)^n$ такого, что выражение

$$f(x+a)+f(x) \tag{8}$$

принимает одно и то же значение (0 или 1) для всех $x \in GF(2)^n$. Пусть $LS(n)$ - множество булевых функций, имеющих линейную структуру. Заметим, что множество $A(n)$ всех аффинных функций содержит в себе $LS(n)$. Для булевой функции f расстояние до линейных структур определяется как расстояние от f до множества $LS(n)$:

$$\sigma(f) = d(f, LS(n)) = \min_{S \in LS(n)} d(f,s). \tag{9}$$

Расстояние до линейных структур может служить в качестве показателя нелинейности булевой функции, что вытекает из (7). Оттуда же следует, что группа симметрий $I(\sigma)$ содержит в себе аффинную группу $AGL(n)$, то есть имеет место включение $I(\sigma) \subset AGL(n)$ [8, 9].

Так как множество $A(n)$ всех аффинных функций содержит в себе $LS(n)$, то для отбора булевых функций с необходимыми криптографическими свойствами с учётом расстояния до линейных структур достаточно применения критериев, анализирующих аффинные свойства булевых функций.

Порядок нелинейности

Пусть для булевой функции $f \in \Phi(n)$ значение $O(f)$ будет степенью наивысшего порядка в алгебраической нормальной форме. В этом случае величина $O(f)$ называется порядком нелинейности f. Использование порядка нелинейности, определяемого функцией $O:\Phi(n) \to \{0,...,k,...,n\}$, удовлетворяет требованиям критерия нелинейности в силу следующего свойства: группа симметрий $I(O)$ функции O совпадает с аффинной группой $AGL(n)$ [8].

Показано [9], что другой критерий нелинейности, называемый расстоянием σ_k к функции с порядком нелинейности ограниченным k, также остается инвариантным над операцией из $AGL(n)$.

Для булевых функций, используемых в криптографических приложениях, должно выполняться условие $O(f) \geq 2$.

Совершенно нелинейные функции

Булеву функцию $f:GF(2)^n \to GF(2)$ называют совершенно нелинейной, если для каждого ненулевого вектора $a \in GF(2)^n$ значения функций $f(x+a)$ и $f(x)$ совпадают точно для половины аргументов $x \in GF(2)^n$.

Показано [8], что совершенно нелинейные функции достигают оптимума расстояния σ до линейных структур.

Для произвольной функции $f:GF(2)^n \to GF(2)$ расстояние до линейных структур вычисляется следующим образом. Пусть $a \in GF(2)^n$ есть ненулевой вектор. Тогда пространство $GF(2)^n$ может быть разбито на 2^{n-1} пар вида $(x, x+a)$. Через n_0 обозначают число элемен-

тов множества W_0 пар вида $(x, x+a)$, для которых $f(x)=f(x+a)$, а через n_1 – число элементов множества W_1 пар вида $(x, x+a)$, для которых $f(x)\neq f(x+a)$.

Любая булева функция может быть получена из произвольной булевой функции f путем изменения множества выходных значений. Таким образом, f может быть преобразована в функцию с линейной структурой изменением выходного значения либо x, либо $x+a$ для пары $(x, x+a)\in W_0$, или изменением соответствующего значения x или $x+a$ для пары $(x, x+a)\in W_1$. Отсюда для получения функции g с линейной структурой, такой, что $g(x)\neq g(x+a)$ для всех x должно быть изменено n_0 значений, и n_1 значений, чтобы получить функцию g с линейной структурой со свойством $g(x)\neq g(x+a)$ для всех x. Для генерации любой другой функции с такой же линейной структурой необходимо произвести, по крайней мере, $min(n_0,n_1)$ модификаций. Следовательно, $n=min(n_0,n_1)$ есть расстояние от функции f к ближайшим функциям с линейной структурой a. Заметим, что n зависит от вектора a, то есть $n=n_f(a)= min(n_0(a),n_1(a))$. Отсюда, расстояние от f до линейных структур определяется как

$$\sigma(f)=\min_{a\neq 0} n_f(a). \tag{10}$$

Поскольку $n_0(a)+n_1(a)=2^{n-1}$, то из (10) вытекает, что $n_f(a)\le 2^{n-2}$ для всех $a\neq 0$. Максимум расстояния достигается совершенно нелинейными функциями, так как они характеризуются равенством $n_0(a)=n_1(a)=2^{n-2}$ для $a\neq 0$ или, что эквивалентно, $\sigma(f)=2^{n-2}$. Это определяет существование следующего свойства [8].

Класс $\pi(n)$ совершенно нелинейных функций совпадает с классом функций с максимальным расстоянием 2^{n-2} к линейным структурам. Ниже описан класс функций, являющихся совершенно нелинейными.

Бент-функции

Рассмотрим зависимость между совершенно нелинейными функциями и бент-функциями. Поскольку эта зависимость выражается в терминах преобразования Уолша, то все булевы функции рассматриваются со значениями +1 и –1 (то есть значения $f(x)\in\{0,1\}$ заменяются на $(-1)^{f(x)}$).

Преобразование Уолша определено следующим образом:

$$F(W)=\sum_{x\in GF(2)^n} f(x)(-1)^{X\bullet W}, \tag{11}$$

где $W\in GF(2)^n$ и $X\bullet W$ – скалярное произведение в $GF(2)$.

Для булевой функции $f: GF(2)^n\to\{+1,-1\}$ и любого ненулевого вектора $a\in GF(2)^n$ имеет место равенство

$$\sum_{x\in GF(2)^n} f(x)f(x+a)=0. \tag{12}$$

Таким образом, ± 1 – значная функция f является совершенно нелинейной тогда и только тогда, когда для каждого ненулевого вектора $a\in GF(2)^n$, то есть тогда и только тогда, когда $f\bullet f$ является σ - функцией. В [9] отмечается, что функция $f\bullet f$ преобразуется в F^2 и σ -функция преобразуется в константу. Следовательно, ± 1 – значная булевая функция f является совершенно нелинейной, тогда и только тогда, когда $F(W)$ является константой для всех w. Так как $f\bullet f(O)=2^n$, то эта константа есть

$$F(w) = 2^{n/2}. \qquad (13)$$

Это свойство определяет совпадение класса совершенно нелинейных функций $\pi(n)$ и класса бент-функций.

Показано, что бент-функции существуют только для четных чисел аргументов и их порядок нелинейности не превосходит $\frac{n}{2}$ [10].

Для четного числа аргументов $n=2m$ бент-функции могут быть построены следующим образом [8]:

1) пусть $n=2m$. Тогда функция вида $f(x_1,..,x_n)=g(x_1,...,x_m)+x_1x_{m+1}+x_2x_{m+2}+...+x_{mn}$ является бент-функцией, где $g(x_1,...,x_m)$ – произвольная функция m-переменных.

2) пусть $x=(x_1,...,x_n)$ и пусть $a(x),b(x)$ и $c(x)$ будут бент функциями, такими что $a(x)+b(x)+c(x)$ есть также бент-функция. Тогда функция

$$f(x,x_{n+1},x_{n+2})=a(x)b(x)+b(x)c(x)+c(x)a(x)+[a(x)+b(x)]x_{n+1}+[a(x)+c(x)]x_{n+2}+x_{n+1}x_{n+2}$$

есть бент-функция. Требование, чтобы $a(x)+b(x)+c(x)$ являлось бент-функцией, легко удовлетворить, если взять $a(x),b(x)$ и $c(x)$ из п.1 или выбрать $a(x)=b(x)$ или $b(x)=c(x)$.

Правило п.1 описывает точные конструкции бент-функций, тогда как п.2 ведет к генерации новых совершенно нелинейных функций на основе произвольной совершенно нелинейной функции. Эта процедура может быть скомбинирована с линейными операциями на заданной совершенно нелинейной функции. Действительно, класс совершенно нелинейных функций является инвариантным над операцией аффинной группы $AGL(n)$. Кроме того, прибавление произвольной аффинной функции не влияет на совершенную нелинейность. Поэтому назначение к $f \in \Phi(n)$ функции $x \to f(\alpha(x)) + L(x)$ определяет операцию $AGL(n) \times A(n)$ на $\Phi(n)$, которая оставляет $\pi(n)$ инвариантным. В результате может быть построен рекуррентный алгоритм формирования совершенно нелинейных функций:

1. Для $n=2$ берется класс *(C2),* состоящий из всех функций с порядком нелинейности 2.

2. Для $n>2$ берутся любые функции a,b,c в $C(n-2)$ такие, что их сумма есть также в $C(n-2)$ и применяется конструкция п.2. Это определяет класс $C`(n)$ совершенно нелинейных функций. Класс $C`(n)$ является расширением класса $C(n)$, разрешая операции целой группы $G = AGL(n) \times A_n$ на $C(n)$.

Отметим, что п.1 предполагает существование по крайней мере $2^{2^{n/2}}$ совершенно нелинейных функций из всех 2^{2^n} булевых функций. Таким образом, только малая часть всех булевых функций является совершенно нелинейными, что значительно усложняет их нахождение. Уже для $n=6$ (то есть для *S*-блоков DES) поиск совершенно нелинейных функций при помощи полного перебора является фактически невозможным.

Однако совершенно нелинейные функции не являются сбалансированными, то есть $\left|\{f(x_0,...,x_n)=0 \,|\, x_0,...,x_n \in GF(2)\}\right| \neq \left|\{f(x_0,...,x_n)=1 \,|\, x_0,...,x_n \in GF(2)\}\right|$. Это означает, что если распределение элементов входной последовательности согласовано с равномерным законом распределения, для выходной последовательности функции такого согласования не будет. Это определяет невозможность использования совершенно нелинейных булевых функций в криптографических преобразованиях в чистом виде, однако применяемые функции должны быть максимально приближены по своим свойствам к совершенно нелинейным функциям.

Расстояние до аффинных функций и корреляция

Здесь мы приводим основные соображения, приведенные в [9]. Пусть $L_w(x) = w \bullet x$ означает произвольную линейную функцию. Тогда $(-1)^{w \bullet x}$ есть соответствующая ± 1- значная функция, которую также обозначим $L_w(x)$. Из определения Уолша [10] следует

$$F(w)=\left|\{x:f(x)=L_w(x)\}\right|-\left|\{x:f(x)\neq L_w(x)\}\right|=2^n-2d(f,L_w)\Big| \ ,$$

где d означает расстояние Хэмминга. Следовательно,

$$d(f,L_w) = 2^{n-1} - \frac{1}{2}F(w). \tag{14}$$

Известно [8], что для соответствующей аффинной функции $L_w = 1 + L_w$ расстояние d вычисляется как $d(f,L_w) = 2^{n-1} + \frac{1}{2}F(w)$. Формулу (14) предлагается использовать для нахождения лучшей аффинной аппроксимации к заданной функции нахождением w такого, чтобы $|F(w)|$ являлся максимумом, то есть

$$\delta(f) = 2^{n-1} - \frac{1}{2}\max_w |F(w)|. \tag{15}$$

Таким образом, как следует из (13), совершенно нелинейные функции всегда имеют расстояние до ближайших аффинных функций, равное

$$\delta(f) = 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{16}$$

При предположении, что f не является совершенно нелинейной, из теоремы Парсеваля следует [9]:

$$\sum_w F(w)^2 = 2^n \sum_x f(x)^2 = 2^{2n}, \tag{17}$$

где существует w с $|F(w)| > 2^{\frac{n}{2}}$. Показано, что $\delta(f) < 2^{n-1} - 2^{\frac{n}{2}-1}$ и, следовательно, f является более близкой к множеству всех аффинных функций, чем совершенно нелинейные функции. В результате делается вывод, что, совершенно нелинейные функции являются оптимальными не только в отношении к расстоянию до линейных структур, но и в отношении к расстоянию до всех аффинных функций, т.е. класс $\pi(n)$ совершенно нелинейных функций является классом функций с максимальным расстоянием $2^{n-1} - 2^{\frac{n}{2}-1}$ к аффинным функциям [8]. Показано, что этот результат может быть расширен до утверждения, что расстояние от совершенно нелинейной функции f к любой аффинной функции равно $2^{n-1} + 2^{\frac{n}{2}-1}$ или $2^{n-1} - 2^{\frac{n}{2}-1}$. Этот факт может быть точно выражен через корреляцию f к аффинным функциям. В общем случае, расстояние Хэмминга между двумя булевыми функциями $f, g : GF(2)^n \to \{+1,-1\}$ связано со взаимной корреляцией между f и g, которая определяется как

$$c(f,g)=\frac{\left|\{x:f(x)=g(x)\}\right|-\left|\{x:f(x)\neq g(x)\}\right|}{2^n}.$$

Для $g = L_w$ преобразование Уолша определяется следующим образом (смотри также (14)):

$$c(f,g)=\frac{F(w)}{2^n}. \tag{18}$$

На основе этого результата делается вывод, что абсолютная величина взаимной корреляции между совершенно нелинейной функцией и любой аффинной функцией есть константа, равная $2^{\frac{n}{2}}$. Кроме того, для функции g, которая не является совершенно нелинейной, всегда есть аффинная функция L с взаимной корреляцией $c(g,L)$ большей, чем $2^{\frac{n}{2}}$ в абсолютном значении. Совершенно нелинейные функции являются классом функций с минимальной корреляцией ко всем аффинным функциям [8].

Это свойство является противоположным по своей сути к корреляционному иммунитету [8]. Известно, что корреляционный иммунитет m-го порядка функции f удовлетворяет соотношению $F(w)=0$ для всех w с весом Хэмминга меньшим или равным m. Следовательно, для этих векторов взаимная корреляция $c(f, L_w)$ исчезает. С другой стороны, из теоремы Парсеваля следует, что для произвольной булевой функции f

$$\sum_{w \in GF(2)^n} c(f, L_w)^2 = 1. \qquad (19)$$

Это означает, что корреляция ко всем линейным (или аффинным) функциям не зависит от функции f. Таким образом, для функций с корреляционным иммунитетом исчезновение определенной взаимной корреляции неизбежно ведет к увеличению корреляции с другими аффинными функциями.

Известно, что взаимная корреляция $c(f,0)$ с нулевой функцией измеряется отклонением от ± 1-баланса булевой функции f. Как уже отмечено выше, совершенно нелинейная функция никогда не может быть сбалансированной. Вместе с тем, ее отклонение от сбалансированности, равное $2^{\frac{n}{2}}$, быстро стремится к нулю, когда n неограниченно возрастает. То же самое имеет силу для корреляции f с любой другой аффинной функцией.

Требование обеспечения минимальной корреляции входных и выходных значений противоречит требованию к сбалансированности выходных значений булевой функции. Совершенно нелинейные функции имеют минимальную корреляцию с аффинными функциями, однако являются несбалансированными. Как уже отмечено выше, необходим поиск функций, своими свойствами обеспечивающих компромисс между требованиями обеспечения сбалансированности, минимальной корреляции и нелинейности.

Рассмотренные показатели отражают современные подходы к оценке нелинейности булевых функций при построении симметричных криптографических алгоритмов. Для обеспечения стойкости преобразований булевы функции должны быть на максимальном расстоянии от множества аффинных функций и множества линейных структур, иметь высокий порядок нелинейности, обладать корреляционным иммунитетом, удовлетворять лавинному критерию и критерию распространения. Класс совершенно нелинейных функций имеет максимум минимального расстояния до аффинных функций и линейных структур, и совпадает с известным классом бент-функций. Однако совершенная нелинейность не может быть достигнута в сочетании со сбалансированностью или высоким порядком нелинейности.

Следует отметить, что для построения таблиц подстановок, применяемых в блочных и поточных алгоритмах шифрования, использования только критериев нелинейности булевых функций недостаточно. Например, в [13] предлагаются критерии построения узлов замены ГОСТ 28147-89 на основе применения булевых функций с заданными криптографическими свойствами, однако в [14] показано, что алгоритм шифрования с такими подстановками может быть уязвимым для дифференциального криптоанализа. Поэтому при построении блоков нелинейного преобразования для симметричных шифров наряду с критериями нелинейности булевых функций необходимо использовать и дополнительные критерии, анализирующие свойства всей подстановки в целом.

Список литературы: 1. *A.F.Webster and S.E. Tavares.* On the design of S-boxes. In Lecture Notes in Computer Science *218*; Advances in Cryptology: Proc. Crypto'*85*, H.C. Williams, Ed., Santa Barbara, CA, Aug. *18-22*, *1985*, pp. 523 – 534. Springer-Verlag, 1986. 2. *R. Forre.* The strict avalanche criterion: Special properties of boolean functions and an extended definition. In Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto'88, pp. 450 – 468. Berlin: Springer-Verlag, 1990. 3. *C.M. Adams and S.E. Tavares.* The use of bent sequences to achieve higher-order strict avalanche criterion. Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990. 4. *B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle.* Propagation characteristics of boolean functions. In Lecture Notes in Computer Science 473; Advances in Cryptology: Proc. Crypto'90, I. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 161 – 173. Berlin: Springer-Verlag. 5. *B. Preneel, R. Govaerts, and J. Vandewalle.* Boolean functions satisfying higher order propagation criteria. In Lecture Notes in Computer Science 547; Advances in Cryptology: Proc. Crypto'91, 1991, pp. 141 – 152. Berlin: Springer-Verlag. 6. *J. Seberry, X. M. Zhang, and Y. Zheng.* Nonlinearity balanced Boolean function and their propagation characteristics. In D.R. Stinson, editor, Advances in Cryptology – Crypto '93, pp. 49 – 60, Springler-Verlag, New York, 1994. 7. *J. Seberry, X.-M. Zhang, and Y. Zheng.* Nonlinearity and propagation Characteristics of Balanced Boolean Functions. Information and Computation, Vol. 119, No 1, pp. 1 – 13, 1995. 8. *W. Meier and O. Staffelbach.* Nonlinearity criteria for cryptographic functions. In Lecture Notes in Computer Science 434; Advanced in Cryptology; Proc. Eurocrypt'89, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 549 – 562. Berlin: Springer-Verlag, 1990. 9. *А.В. Бабаш, Г.П. Шанкин.* Криптография. М.: СОЛОН-Р, 2002. 10. *O.S. Rothaus.* On bent functions. Journal of Combinatorial Theory (A), Vol. 20, pp. 300 – 305, 1976. 11. *C.E. Shannon.* Communications theory of secrecy systems. Bell Sys. Tech. Journal, Vol. 28, pp. 656 – 715, Oct. 1949. 12. *Донской В.И.* Дискретная математика. Симферополь: Изд. «СОНАТ», 2000. 13. *Холоша А.А.* Об одном подходе к анализу качества блока подстановки битовых векторов // Збірник наукових праць інституту проблем моделювання в енергетиці НАНУ. 1998. Вип. 2. С. 59 – 74. 14. *Р. Олейников, И. Лисицкая, А. Шумов.* Исследование свойств подстановок ГОСТ 28147-89, построенных на основе анализа свойств координатных функций. Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. К.: ИВЦ «Политехника», 2002. Вып. 5.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 12.05.2003