УДК 621.391:519.2

А. Н. Алексейчук
Институт специальной связи и защиты информации НТУУ «КПИ»
ул. Московская, 45/1, 01011 Киев, Украина

Оптимальные уравновешенные отображения в конструкциях генераторов гаммы с неравномерным движением и протоколов передачи ключей по каналу связи с отводом

Получены аналитические выражения и оценки надежности статистических процедур восстановления значений комбинирующей функции генератора гаммы с неравномерным движением линейных регистров сдвига. Показано, что эти аналитические выражения позволяют распространить на рассматриваемый класс генераторов гаммы ряд утверждений о стойкости защиты сообщений в системах передачи информации по каналу связи с отводом.

Ключевые слова: *криптографический анализ, генератор гаммы с неравномерным движением, канал с отводом, случайное кодирование.*

В современных поточных шифросистемах широко используются генераторы псевдослучайных последовательностей (генераторы гаммы), состоящие из линейных регистров сдвига (ЛРС) и узлов усложнения [1]. Одним из общих способов повышения криптографической стойкости таких генераторов является введение неравномерности в процесс движения ЛРС. Известно, например, что неравномерность закона движения регистров сдвига комбинирующего генератора гаммы (КГГ) при определенных условиях существенно улучшает его криптографические свойства, в частности, повышает его практическую стойкость относительно корреляционных атак [2, 3].

Хорошо известным примером КГГ с неравномерным движением является генератор гаммы шифра A5/1, алгоритм корреляционного криптоанализа которого предложен в [4] и впоследствии усовершенствован в [5, 6]. В работах [7, 8] описан общий метод восстановления начального состояния (НС) комбинирующего генератора гаммы с неравномерным движением, функционирующего в так называемом режиме реинициализации. Метод основан на вероятностном описании функционирования генератора гаммы, позволяющем свести задачу восстановления его начального состояния к различению нескольких статистических гипотез.

Настоящая статья посвящена исследованию вероятностной модели более общего класса КГГ с неравномерным движением, преобразующих n входных в k выходных последовательностей над произвольным конечным алфавитом F, $1 \le k < n$. Стойкость таких генераторов гаммы относительно статистических атак, аналогичных описанным в [4, 7, 8], характеризуется определенным набором условных вероятностей, для которых получены явные аналитические выражения. Эти выражения позволяют установить тесную связь между двумя криптоаналитическими задачами: восстановлением значений комбинирующей функции генератора гаммы с неравномерным движением ЛРС (в рассматриваемой модели его функционирования) и восстановлением сообщений, искаженных при передаче по каналу связи вероятностно-криптографической системы (ВКС) с равномерным случайным кодированием [9–11]. Наличие указанной связи позволяет распространить на рассматриваемый класс генераторов гаммы ряд утверждений [10, 11] о стойкости защиты сообщений в системах передачи информации по каналу связи с отводом. В частности, получено общее достаточное условие оптимальности (по критерию минимума надежности восстановления значений) комбинирующей функции КГГ с неравномерным движением над алфавитом F. Для проверки применимости полученных результатов к решению задач криптоанализа ряда генераторов гаммы современных поточных шифросистем проведены вычислительные эксперименты, результаты которых согласуются с теоретическими выводами.

Далее в статье свободно используются терминология и обозначения, принятые в [10, 11]. Доказательства теорем, выходящие за рамки статьи, опущены.

Пусть F — конечная абелева группа порядка $q > 1$, $\sigma : F^n \to F^k$ — уравновешенное отображение (то есть такое, что $|\sigma^{-1}(s)| = q^{n-k}$ для любого $s \in F^k$), $1 \le k < n$. Зафиксируем изоморфизм $a \mapsto \chi_a$, $a \in F^n$ группы F^n в группу комплексных характеров $\hat{F}^n = \mathrm{Hom}(F^n, \mathbf{C}^*)$ такой, что $\chi_a(x) = \chi_x(a)$ для любых $a, x \in F^n$. Обозначим $\mathbf{C}(F^n)$ множество всех комплекснозначных функций на группе F^n. Отметим, что множество $\mathbf{C}(F^n)$ является унитарным векторным пространством относительно скалярного произведения $(f, g) = \sum_{x \in F^n} f(x)\overline{g(x)}$, где $\overline{g(x)}$ — число, комплексно-сопряженное к числу $g(x)$. Преобразование Фурье $\hat{f}$ функции $f \in \mathbf{C}(F^n)$ определяется по формуле $\hat{f}(a) = \sum_{x \in F^n} \chi_a(x) f(x)$, $a \in F^n$; обратное преобразование имеет вид: $f(x) = q^{-n} \sum_{a \in F^n} \overline{\chi_a(x)}\, \hat{f}(a)$, $x \in F^n$.

Рассмотрим вероятностную модель функционирования однотактного узла усложнения генератора гаммы с неравномерным движением ЛРС и комбинирующим отображением σ. Эта модель определяется как упорядоченная пара независимых случайных векторов (СВ) $X = (X_j(i) : j \in \overline{1, n},\ i \in \overline{0, L-1})$ и $\delta = (\delta_1, ..., \delta_n)$, принимающих значения во множествах F^{nL} и $D \subseteq \{0, 1, ..., L-1\}^n$ соответственно,

$L \in \mathbf{N}$. При этом СВ X имеет равномерное распределение вероятностей на множестве F^{nL}, а СВ δ — произвольное распределение, сосредоточенное на множестве D. Знак выходной последовательности узла усложнения определяется по формуле:

$$\gamma = \sigma(X_1(\delta_1),..., X_n(\delta_n)) \tag{1}$$

(см. работы [7, 8], посвященные исследованию вероятностных моделей двоичных генераторов гаммы указанного вида).

Пусть задан вектор $a = (a_1, ..., a_n) \in D$. Требуется разработать статистическую процедуру и оценить вероятность правильного восстановления значения случайной величины $\sigma(X_1(a_1),..., X_n(a_n))$ по наблюдаемому знаку (1). Для решения поставленной задачи рассмотрим условные вероятности

$$p(s\,|\,\gamma) = \mathbf{P}\big(X(a) = s \,|\, \sigma\big(X_1(\delta_1),..., X_n(\delta_n)\big) = \gamma\big),\ s \in G^n,\ \gamma \in G^k, \tag{2}$$

где $X(a) = (X_1(a_1),..., X_n(a_n))$. Обозначим символом $I_{\sigma,\gamma}$ индикатор множества $\sigma^{-1}(\gamma)$, а символом $\hat{I}_{\sigma,\gamma}$ — преобразование Фурье функции $I_{\sigma,\gamma}$, $\gamma \in F^k$. Для любого множества $A = \{i_1,..., i_l\} \subseteq \{1, 2, ..., n\}$, где $1 \le i_1 < ... < i_l \le n$, и произвольного вектора $x = (x_1,..., x_n)$ обозначим x_A и $\mathrm{supp}(x)$ соответственно подвектор $(x_{i_1},..., x_{i_l})$ и носитель (множество номеров ненулевых координат) вектора x.

Справедлива следующая теорема, устанавливающая явные выражения вероятностей (2).

Теорема 1. Для любых $s \in F^n$, $\gamma \in F^k$, выполняется равенство:

$$p(s\,|\,\gamma) = q^{-n}\left(1 + q^{-(n-k)} \sum_{y \in F^n \setminus \{0\}} \hat{I}_{\sigma,\gamma}(y)\overline{\chi_s(y)}\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}\right). \tag{3}$$

Пусть теперь $g : F^k \to F^k$ — произвольное отображение (декодер или решающая процедура) для восстановления значения $\sigma(X(a)) = \sigma(X_1(a_1),..., X_n(a_n))$. Обозначим $\lambda(\sigma; g) = \mathbf{P}\{g(\sigma(X_1(\delta_1),..., X_n(\delta_n))) = \sigma(X(a))\}$ вероятность правильного восстановления указанного значения, которую назовем *надежностью процедуры* g. Для любых $\alpha, \gamma \in F^k$ положим

$$\pi_\sigma(s,\ \gamma) = \sum_{s \in F^n : \sigma(s) = \alpha} p(s\,|\,\gamma) = \mathbf{P}\big(\sigma\big(X(a)\big) = \alpha \,|\, \sigma\big(X_1(\delta_1),..., X_n(\delta_n)\big) = \gamma\big). \tag{4}$$

Отметим, что на основании формулы полной вероятности справедливо следующее равенство:

$$\lambda(\sigma; g) = q^{-k} \sum_{\gamma \in F^k} \pi_\sigma(g(\gamma), \gamma). \qquad (5)$$

Назовем *оптимальной процедурой* восстановления значения $\sigma(X(a))$ произвольное отображение $g^*: F^k \to F^k$, удовлетворяющее условию $\lambda(\sigma; g^*) \geq \lambda(\sigma; g)$ для любого отображения $g: F^k \to F^k$. Надежность оптимальной процедуры обозначим символом $\lambda^*(\sigma)$. Заметим, что на основании формулы (5) оптимальной является байесовская статистическая процедура [12], в соответствии с которой наблюдаемому знаку γ вида (1) ставится в соответствие оценка $g^*(\gamma)$ значения $\sigma(X(a))$, определяемая по формуле:

$$\pi_\sigma(g^*(\gamma), \gamma) = \max_{\alpha \in F^k} \pi_\sigma(\alpha, \gamma), \ \gamma \in F^k. \qquad (6)$$

Непосредственно из равенств (3)–(5) вытекает следующая теорема.

Теорема 2. Пусть $g: F^k \to F^k$ — произвольное отображение. Тогда надежность восстановления значения $\sigma(X(a))$ по наблюдаемому знаку (1) с использованием процедуры g определяется по формуле:

$$\lambda(\sigma; g) = q^{-k}\left(1 + q^{-2(n-k)} \sum_{\gamma \in F^k} \sum_{y \in F^n \setminus \{0\}} \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} \hat{I}_{\sigma,\gamma}(y) \overline{\hat{I}_{\sigma,g(\gamma)}(y)}\right). \qquad (7)$$

Обратим внимание на сходство аналитического выражения в правой части равенства (7) с выражением вероятности правильного приема сообщений в канале связи вероятностно-криптографической системы с равномерным случайным кодированием (см. формулу (13) в статье [10]). Это сходство показывает, что, по крайней мере, на формальном уровне, существует тесная связь между задачей оценки надежности восстановления значений комбинирующей функции генератора гаммы с неравномерным движением ЛРС (в рассматриваемой модели его функционирования) и задачей оценки вероятности правильного восстановления сообщений в канале ВКС с равномерным случайным кодированием. Аналогия между указанными аналитическими выражениями позволяет перенести (с незначительными изменениями в доказательствах) большую часть результатов, полученных для вероятностно-криптографических систем [10, 11], на рассматриваемый класс генераторов гаммы с неравномерным движением и установить общее достаточное условие оптимальности комбинирующей функции σ генератора (по критерию минимума надежности $\lambda^*(\sigma)$) в классе всех уравновешенных отображений группы F^n в группу F^k.

Сформулируем полученные результаты в виде нескольких теорем.

Теорема 3. Справедливы следующие утверждения.

1. Если g — подстановка на группе F^k, $\iota: F^k \to F^k$ — тождественное отображение, то

$$\lambda(\sigma; g) \le \lambda(\sigma; \iota); \tag{8}$$

другими словами, тождественное отображение является оптимальной среди всех биективных процедур $g: F^k \to F^k$ восстановления значения $\sigma(X(a))$.

2. Если $\sigma: F^n \to F^k$ — эпиморфизм групп, то отображение ι есть оптимальная процедура восстановления значения $\sigma(X(a))$ и

$$\lambda^*(\sigma) = q^{-k}\left(1 + \sum_{y \in G^\perp \setminus \{0\}} \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}\right), \tag{9}$$

где G — ядро эпиморфизма σ; $G^\perp = \{x \in F^n \mid \forall a \in G: \chi_x(a) = 1\}$ — группа, дуальная к G.

3. Пусть $q = 2$, $k = 1$. Тогда для любой уравновешенной функции $\sigma: V_n \to \{0, 1\}$ выполняется равенство

$$\lambda^*(\sigma) = \frac{1}{2}\left(1 + 2^{-2n} \sum_{y \in V_n \setminus \{0\}} |W_\sigma(y)|^2 \, \mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\}\right), \tag{10}$$

где $W_\sigma(y) = \sum_{x \in V_n} (-1)^{\sigma(x) \oplus xy}$, $y \in V_n$, есть преобразование Уолша-Адамара функции σ. При этом минимум значений (10) по всем уравновешенным функциям $\sigma: V_n \to \{0, 1\}$ достигается на линейной функции $\sigma_0(x_1, ..., x_n) = x_1 \oplus \cdots \oplus x_n$, $(x_1, ..., x_n) \in V_n$.

Следующие две теоремы устанавливают аналитические оценки и достаточные условия минимальности параметра $\lambda^*(\sigma)$ при дополнительном ограничении на закон распределения случайного вектора δ.

Теорема 4. Пусть для данного вектора $a = (a_1, ..., a_n)$ существует функция $\varphi_a: [0, +\infty) \to [0, 1]$, убывающая и строго выпуклая вниз на множестве $[0, +\infty)$ такая, что

$$\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} = \varphi_a(\|y\|), \; y \in F^n \setminus \{0\}. \tag{11}$$

Тогда для любого уравновешенного отображения $\sigma: F^n \to F^k$ выполняются неравенства

$$\lambda^*(\sigma) \ge \lambda(\sigma; \iota) \ge q^{-k} + \frac{q^k - 1}{q^k} \varphi_a(f), \tag{12}$$

где $f = n\dfrac{q^k - q^{k-1}}{q^k - 1}$. Если, кроме того, σ является t-устойчивым отображением (см. [13]), то

$$\lambda(\sigma;\iota) \le q^{-k} + \frac{q^k - 1}{q^k}\varphi_a(t+1). \tag{13}$$

В частности, справедливо неравенство $t \le f - 1$, которое обращается в равенство тогда и только тогда, когда $\lambda(\sigma;\iota) = q^{-k} + \dfrac{q^k - 1}{q^k}\varphi_a(f)$.

Теорема 5. Пусть в условиях предыдущей теоремы существует отображение $\sigma_0 : F^n \to F^k$, имеющее максимальный порядок устойчивости, равный $f - 1$. Тогда для любого уравновешенного отображения $\sigma : F^n \to F^k$ выполняется неравенство:

$$\lambda^*(\sigma) \ge \lambda^*(\sigma_0) = \lambda(\sigma_0;\iota). \tag{14}$$

В [11] приведены примеры отображений σ_0, удовлетворяющих условиям последней теоремы. Подчеркнем, что эти отображения обеспечивают наименьшую надежность восстановления значения комбинирующей функции генератора гаммы в (неизвестной) точке $X(a)$ по наблюдаемому знаку его выходной последовательности (1) среди всех уравновешенных отображений $\sigma : F^n \to F^k$.

Приведем примеры законов распределения случайного вектора $\delta = (\delta_1, ..., \delta_n)$, удовлетворяющих условиям теоремы 4.

Пусть $\delta_1, ..., \delta_n$ — независимые СВ с одинаковым распределением на конечном множестве $N \subseteq \mathbf{N}_0$ (это условие характеризует генераторы гаммы, регистры которых сдвигаются независимо друг от друга в каждом такте). Предположим, что $a_1 = ... = a_n \in N$. Обозначим $\Delta = \mathbf{P}\{\delta_1 = a_1\}$; в этом случае $\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} = \Delta^{\|y\|}$, $y \in F^n \setminus \{0\}$, и равенство (11) выполняется для функции $\varphi_a(x) = \Delta^x$, $x \in [0, +\infty)$.

Рассмотрим несколько более общий пример. Пусть p_i — распределение вероятностей на конечном множестве $N \subseteq \mathbf{N}_0$, $i \in \overline{1,m}$,

$$\mathbf{P}\{\delta_1 = u_1, ..., \delta_n = u_n\} = \sum_{i=1}^{m} q_i p_i(u_1) \cdots p_i(u_n), \tag{15}$$

где $u_1, ..., u_n \in N$, $q_i \ge 0$, $i \in \overline{1,m}$, $\sum\limits_{i=1}^{m} q_i = 1$. Предположим, что $a_1 = ... = a_n \in N$. То-

гда на основании равенства (15) $\mathbf{P}\{\delta_{\mathrm{supp}(y)} = a_{\mathrm{supp}(y)}\} = \sum_{i=1}^{m} q_i\big(p_i(a)\big)^{\|y\|}$ для любого $y \in F^n \setminus \{0\}$, и формула (11) справедлива, если $\varphi_a(x) = \sum_{i=1}^{m} q_i\big(p_i(a)\big)^x$, $x \in [0, +\infty)$. Заметим, что здесь $\delta_1,...,\delta_n$ является симметрично зависимыми случайными величинами (см. [14], стр. 265). В частности, при $m = 1$ получаем предыдущий пример.

Изложенные выше результаты позволяют дать исчерпывающее описание оптимальных статистических процедур и установить аналитические выражения надежности восстановления значений комбинирующих функций двоичных генераторов гаммы с неравномерным движением ($q = 2$, $k = 1$). С целью проверки применимости указанных процедур к решению задач криптоанализа комбинирующих генераторов гаммы ряда поточных шифрсистем были проведены вычислительные эксперименты. Исследования проводились для генераторов с различными комбинирующими функциями и законами движения ЛРС, при различном выборе моментов наблюдения знаков их выходных последовательностей и векторов a. В качестве примера, иллюстрирующего типичные результаты экспериментальных исследований, опишем вычислительный эксперимент, проведенный со следующими двумя генераторами гаммы.

Оба КГГ состоят из $n = 3$ ЛРС с примитивными многочленами обратной связи и, за исключением комбинирующих функций, имеют одинаковые параметры криптосхем, совпадающие с соответствующими параметрами криптосхемы генератора гаммы шифра A5/1. В частности, предполагается, что блок управления движением каждого генератора вырабатывает за первые i тактов случайный вектор $\delta(i) = (\delta_1(i), \delta_2(i), \delta_3(i))$, распределенный по закону

$$\mathbf{P}\{\delta(i) = a\} = 4^{-i} \frac{i!}{(i-a_1)!(i-a_2)!(i-a_3)!(a_1+a_2+a_3-2i)!}, \qquad (16)$$

где $a_1, a_2, a_3 \in \overline{0, i}$, $a_1 + a_2 + a_3 \geq 2i$ [4]. Комбинирующие функции генераторов гаммы равны $\sigma_1(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ и $\sigma_2(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$ соответственно. Отметим, что порядки устойчивости этих функций равны $\mathrm{cor}(\sigma_1) = 2$, $\mathrm{cor}(\sigma_2) = 0$.

Ниже в таблице приведены результаты статистического оценивания надежности оптимальных процедур восстановления значений $\sigma_\nu(X(a))$ по наблюдаемым знакам $\gamma_{\nu,i} = \sigma_\nu(X_1(\delta_1(i)), X_2(\delta_2(i)), X_3(\delta_3(i)))$, $\nu = 1, 2$, для различных тактов i и векторов $a = (a_1, a_2, a_3)$. Данные в таблице получены с использованием программы для ЭВМ типа Sempron 2200 MHz, 256 Mb ОЗУ, в ходе следующего вычислительного эксперимента. Сначала по Урновой схеме с возвращением генерируется 10^4 начальных состояний первого (второго) КГГ, для каждого из которых вырабатывается отрезок $\{\gamma_{1,i} : i \in \overline{0, 164}\}$ ($\{\gamma_{2,i} : i \in \overline{0, 164}\}$). Затем для каждой пары (a, i), указанной в таблице, с использованием формул (3)–(6) принимается реше-

ние относительно значения величины $\sigma_1(X(a))$ ($\sigma_2(X(a))$) и полученный результат сравнивается с фактическим значением этой величины, которое вычисляется по известному НС первого (второго) КГГ.

В таблице указаны относительные частоты $N^{(1)}$ и $N^{(2)}$ совпадений (из 10^4 сгенерированных) символов вида $\sigma_1(X(a))$ и $\sigma_2(X(a))$ соответственно с их оценками. Для сравнения приведены также теоретические значения $N^{(1)}_{\text{Teop}}$, $N^{(2)}_{\text{Teop}}$ надежностей восстановления этих символов, рассчитанные по формуле (10) с использованием равенства (16). Как видно из таблицы, для каждого из двух генераторов гаммы полученные значения надежности приближаются к 0,5 с ростом параметра $\min\{a_1, a_2, a_3\}$. При этом для второго КГГ указанное приближение имеет регулярный (монотонно убывающий) характер и является более медленным, чем для первого. Так, оценка $N^{(2)}$ в среднем на 4–10 % выше по сравнению с оценкой $N^{(1)}$, что согласуется с зависимостью надежности восстановления значений комбинирующей функции генератора гаммы от порядка ее устойчивости (см. равенство (10)).

Численные оценки надежности восстановления значений комбинирующих функций генераторов гаммы с неравномерным движением ЛРС

(a_1, a_2, a_3)	i	$N^{(1)}_{\text{Teop}}$	N_1 (%)	$N^{(2)}_{\text{Teop}}$	N_2 (%)
(5, 5, 5)	7	0,52	50,5	0,54	60,4
(10, 10, 10)	13	0,51	51,6	0,53	60,1
(15, 15, 15)	20	0,51	49,9	0,53	57,4
(20, 20, 20)	27	0,50	49,9	0,52	56,6
(25, 25, 25)	33	0,50	49,6	0,52	57,1
(30, 30, 30)	40	0,50	50,2	0,52	55,8
(35, 35, 35)	47	0,50	51,1	0,52	55,5
(40, 40, 40)	53	0,50	50,1	0,52	55,3
(45, 45, 45)	60	0,50	49,6	0,51	54,7
(50, 50, 50)	67	0,50	50,8	0,51	54,7
(55, 55, 55)	73	0,50	50,1	0,51	54,3

В целом, результаты проведенных экспериментальных исследований свидетельствуют о возможности практического восстановления (с надежностью до 61 %) значений комбинирующих функций ряда двоичных КГГ с неравномерным движением по отдельным знакам их выходных последовательностей. В [7, 8] показано, что применение описанного способа восстановления значений комбинирующих функций генераторов гаммы, функционирующих в режиме реинициализации НС, приводит к практически реализуемым атакам, позволяющим восстанавливать элементы их начальных состояний с надежностью, сколь угодно близкой к 1.

Автор статьи признателен Р.В. Проскуровскому за помощь при проведении вычислительных экспериментов.

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М.: Триумф, 2002. — 816 с.

2. *Фомичев В.М.* Дискретная математика и криптология / В.М. Фомичев. — М.: ДИАЛОГ-МИФИ, 2003. — 400 с.

3. *Kholosha A.A.* Clock-Controlled Shift Registers for Key-Stream Generation / A.A. Kholosha // http://eprint.iacr.org/2001/061.

4. *Ekdahl P.* Another Attack on A5/1 / P. Ekdahl, T. Johansson // IEEE Trans. on Inform. Theory. – 2003. – Vol. IT-49, N 1. — P. 284–289.

5. *Maximov A.* An Improved Correlation Attack on A5/1 / A. Maximov, T. Johansson, S. Babbage // Selected Areas in Cryptography. — SAC 2004. — Proceedings. — Springer Verlag, 2005. — P. 1–18.

6. *Barkan E.* Cryptanalysis of Ciphers and Protocols / E. Barkan. — Ph. D. Thesis, 2006.

7. *Алексейчук А.Н.* Статистическая атака на комбинирующий генератор гаммы с неравномерным движением в режиме реинициализации начального состояния / А.Н.Алексейчук, Р.В. Проскуровский, Л.В. Скрыпник // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25–27 октября 2006 г. — М.: МЦНМО, 2007. — С. 161–167.

8. *Алексейчук А.Н.* Нижняя граница вероятности различения внутренних состояний комбинирующего генератора гаммы с неравномерным движением / А.Н. Алексейчук, Р.В. Проскуровский // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2006. — Вип. 2(13). — С. 159–169.

9. *Иванов В.А.* О методе случайного кодирования / В.А. Иванов // Дискретная математика. — 1999. — Т. 11. — Вып. 3. — С. 99–108.

10. *Алексейчук А.Н.* Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе / А.Н. Алексейчук // Захист інформації. — 2002. — № 3. — С. 7–16.

11. *Алексейчук А.Н.* Оптимальное случайное кодирование равновероятных сообщений в q-ичном симметричном канале / А.Н. Алексейчук // Захист інформації. — 2002. — № 4. — С. 49–58.

12. *Боровков А.А.* Математическая статистика / А.А. Боровков. — М.: Наука., 1984. — 472 с.

13. *Camion P.* Construction of T-Resilient Functions Over a Finite Alphabet / P. Camion, A. Canteaut // Advances in Cryptology — EUROCRYPT'96, Proceedings. — Springer Verlag, 1996. — P. 283–293.

14. *Феллер В.* Введение в теорию вероятностей и ее приложения. — Т. 2; пер. с англ. — М.: Мир, 1984. — 738 с.

Поступила в редакцию 26.03.2008