би робити оцінки і прогнози, відпрацьовувати методику, перш за все, по попередженню кібезлочинності. Однак на даний час органи, які займаються питаннями попередження комп'ютерних злочинів, володіють розрізненими і несистематизованими даними про комп'ютерну злочинність, а законодавча і виконавча влади не мають реального уявлення про масштаби розповсюдження цього виду злочинності в країні, внаслідок чого держава втрачає можливість адекватного реагування на її динаміку. Ці функції зміг би вирішувати, наприклад, вже існуючий при Раді національної безпеки і оборони України Міжвідомчий науково-дослідний центр.

**Список літератури**

1. *Плещивцева Т.* Червяк в паутине // "Эксперт" Украинский деловой журнал, № 12 (110), 26.03.2007. – с 21.

2. *James N. Rosenau and J.P. Singh.* Information Technologies and Global Politics: the changing scope of power and governance. Published by State University of New York Press, 2002, p.265.

3. *Аспекти інформаційної безпеки аналізуються, зокрема, в працях:* Білорус. О.Г., Скаленко О.К. Інформаційна безпека як фактор соціально-економічного розвитку: Глобальні трансформації і стратегії розвитку. – К., 1998. – С. 361-373; Зубок Микола Іванович. Інформаційна безпека. — К. : КНТЕУ, 2005. — 133 с; Карпенко В. О. Інформаційна політика та безпека: Підручник. — К. : Нора-Друк, 2006. — 320 с. та ін.

4. *Зернецька О.В.* Проблеми інформаційної безпеки в масово-комунікаційній сфері // Колективна монографія „Глобалізація і безпека розвитку", за ред. Білоруса О.В – К.: КНЕУ, 2001. – С. 675-684.

5. *http://www.washprofile.org* - Інформаційне агентство Washington ProFile.

6. *Луков В.В.* Интернет как инструмент политических технологий в США // США v Канада: экономика, политика, культура. 2005. - № 5 (425). – С 91-107.

7. *http://www.cybersecurity.ru/net/23759.html* - сайт новин високих технологій "Cyber Security".

8. *http://www.pandasoftware.es/virus_info/pandalabs* - сайт компанії Panda Software.

9. http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0 - Tunis Commitment, Second Phase of the WSIS (16-18 November 2005, Tunis) // „Туніське зобов'язання" Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства (16-18 листопада 2005 року, Туніс).

*Надійшла 17.05.2007 р.*

**УДК 621.391: 519.2**

**Алексейчук А. Н.**

## АНАЛИТИЧЕСКИЕ ОЦЕНКИ ТЕОРЕТИЧЕСКОЙ СТОЙКОСТИ РАНДОМИЗИРОВАННЫХ БЛОЧНЫХ СИСТЕМ ШИФРОВАНИЯ ОТНОСИТЕЛЬНО МЕТОДА РАЗНОСТНОГО КРИПТОАНАЛИЗА

Одним из общих подходов к повышению стойкости криптографических систем является применение рандомизации или случайного кодирования источника сообщений, при котором каждому фиксированному открытому сообщению отвечают различные кодовые слова, выбираемые в соответствии с некоторыми распределениями вероятностей из заданных попарно непересекающихся множеств шифруемых слов [1, 2]. В настоящее время известно немало работ, посвященных исследованию теоретической стойкости так называемых

рандомизированных подстановочных шифров (см., например, [1 – 6]). Вместе с тем, разработке общих методов оценки или обоснования стойкости рандомизированных симметричных систем шифрования относительно современных методов криптоанализа уделяется мало внимания в доступных публикациях.

В [7] предложен способ построения рандомизированных блочных систем шифрования (РБСШ) на основе гомоморфизмов групповой структуры на множестве шифруемых сообщений в конечные абелевы группы и получены аналитические оценки параметров, характеризующих их теоретическую стойкость относительно метода разностного криптоанализа. Более общий класс рандомизированных систем шифрования исследован в [8], где получены достаточные условия стойкости указанных шифрсистем относительно алгебраических атак, основанных на коммутативных диаграммах [9].

Настоящая статья посвящена исследованию теоретической стойкости РБСШ, описанных в [8], относительно метода разностного криптоанализа. Основная задача, решаемая а статье, состоит в построении аналитических оценок основного параметра (максимума средних значений вероятностей раундовых дифференциалов), характеризующего теоретическую стойкость рандомизированных блочных систем шифрования относительно разностного криптоанализа. Изложенные в статье результаты усиливают и обобщают ранее известные оценки стойкости рандомизированных блочных шифров с гомоморфным случайным кодированием [7] и могут быть непосредственно использованы при оценке или обосновании стойкости РБСШ рассматриваемого вида относительно разностных атак.

Приведем определения основных понятий и сформулируем ряд вспомогательных результатов, используемых далее в статье.

Пусть $G$ – конечная абелева группа порядка $q \geq 2$, $K$ – конечное множество и $(f_k : k \in K)$ – семейство подстановок на группе $G^n$. Рассмотрим $r$-раундовый блочный шифр (БШ) $\mathfrak{Z}$ с множеством открытых (шифрованных) сообщений $G^n$, множеством раундовых ключей $K$ и функцией шифрования $F$: $G^n \times K^r \to G^n$. Согласно определению, шифрующее преобразование $F_\lambda$ открытого текста $x \in G^n$ в шифрованный текст $y \in G^n$ на ключе шифрования $\lambda = (k(1), \ldots, k(r)) \in K^r$ определяется по формуле $y = F_\lambda(x) = (f_{k(r)} \cdots f_{k(1)})(x)$, где $f_{k(r)} \cdots f_{k(1)}$ есть произведение указанных подстановок. Элементы $k(1), \ldots, k(r)$ называются раундовыми ключами, а подстановки $f_{k(1)}, \ldots, f_{k(r)}$ – раундовыми шифрующими преобразованиями шифра $\mathfrak{Z}$ в раундах шифрования с номерами $1, \ldots, r$ соотвественно. Далее предполагается, что $G$ является аддитивной группой конечного поля из $q$ элементов: $G = (\mathbf{GF}(q), +)$.

Рассмотрим класс РБСШ, которые определяются следующим образом [8]. Пусть $G^n = S + T$ – разложение группы $G^n$ в прямую сумму собственных подгрупп $S$ и $T$, где группа $S$ изоморфна группе $G^k$ для некоторого $1 < k < n$. Зафиксируем подстановку $\rho$: $G^n \to G^n$, эпиморфизм $\sigma$: $G^n \to S$, мономорфизм $\tau$: $S \to G^n$ такие, что $\mathrm{Ker}(\sigma) = T$, $\sigma(\tau(s)) = s$ для любого $s \in S$, и определим отображение $\pi$: $G^n \to G^n$, полагая $\pi(s, t) = \rho(\tau(s) + t)$, $s \in S$, $t \in T$. По указанным исходным данным построим рандомизированную систему шифрования $\mathfrak{R} = \mathfrak{R}_{\mathfrak{Z}}(S, T, \pi)$ с множеством открытых сообщений $S$, множеством ключей $K^r$, множеством шифрованных сообщений $G^n$ и функцией шифрования $\psi$: $S \times K^r \to G^n$ следующего вида:

$$\psi(s, \lambda) = F_\lambda(\pi(s, t)), s \in S, \lambda \in K^r, \qquad (1)$$

где $t$ – случайный элемент, равномерно распределенный на группе $T$.

Согласно равенству (1), зашифрование открытого сообщения $s \in S$ с помощью РБСШ $\mathfrak{R}$ осуществляется следующим образом. Вначале случайно с вероятностью $q^{-(n-k)}$ выбирается сообщение $\tau(s) + t$, принадлежащее смежному классу $\sigma^{-1}(s)$ группы $G^n$ по подгруппе $T = \mathrm{Ker}(\sigma)$. Затем это сообщение преобразуется под действием заданной подстановки $\rho$ в сообщение $x = \rho(\tau(s) + t)$, которое, в свою очередь, зашифровывается на ключе $\lambda$ шифра $\mathfrak{Z}$.

Для восстановления открытого текста $s$ по шифрованному тексту $y = F_\lambda(x)$ законный получатель находит сообщение $x = F_\lambda^{-1}(y)$ и вычисляет $s$ по формуле $s = \sigma(\rho^{-1}(x))$.

Отметим, что рассматриваемый класс РБСШ включает в себя ряд известных конструкций рандомизированных симметричных шифрсистем (см. [1]). В частности, если в приведенном выше определении подстановка $\rho$ является автоморфизмом группы $G^n$, то система шифрования $\Re_\Im(S, T, \pi)$ совпадает с так называемой рандомизацией БШ $\Im$ относительно гомоморфизма $\sigma : G^n \to G^k$ [7].

Напомним определения основных понятий теории разностного криптоанализа БШ, которые используются в дальнейшем изложении.

Для данной подстановки $\rho$ на множестве $G^n$ положим

$$DP^\rho(\alpha,\beta) = q^{-n}\#\{x \in G^n : \rho(x+\alpha) - \rho(x) = \beta\},\ \alpha, \beta \in G^n. \qquad (2)$$

Далее будем считать, что раундовые ключи $k(1)$, …, $k(r)$ шифра $\Im$ являются независимыми случайными элементами, равномерно распределенными на множестве $K$. Зададим на множестве всех упорядоченных пар $(X, X')$ открытых сообщений шифра $\Im$ равномерное распределение вероятностей. Обозначим $Y(i)$ и $Y'(i)$ случайные сообщения, вырабатываемые в $i$-м раунде шифрования по открытым текстам $X$ и $X'$ соответственно, положим $\Delta Y(i) = Y'(i) - Y(i)$, $\Delta X = X' - X$ и введем в рассмотрение матрицу $D_i(\Im) = \| d_i^\Im(\alpha,\beta) \|$ вероятностей $i$-раундовых дифференциалов шифра $\Im$, полагая

$$d_i^\Im(\alpha,\beta) = \mathbf{P}\left(\Delta Y(i) = \beta \,/\, \Delta X = \alpha\right),\ \alpha, \beta \in G^n,\ i \in \overline{1,r}. \qquad (3)$$

Шифр $\Im$ называется марковским [10], если для любых $\alpha$, $\beta$, $\gamma \in G^n$, где $\alpha \neq 0$, выполняется равенство

$$\mathbf{P}\left(\Delta Y(1) = \beta \,/\, \Delta X = \alpha, X = \gamma\right) = \mathbf{P}\left(\Delta Y(1) = \beta \,/\, \Delta X = \alpha\right). \qquad (4)$$

Отметим, что равенство (4) равносильно соотношению

$$\mathbf{P}(f_K(\gamma+\alpha) - f_K(\gamma) = \beta) = q^{-n} \sum_{x \in G^n} \mathbf{P}(f_K(x+\alpha) - f_K(x) = \beta),$$

которое означает, что шифр $\Im$ является марковским в том и только в том случае, когда для любых $0 \neq \alpha, \beta, \gamma \in G^n$ вероятность $\mathbf{P}(f_K(\gamma + \alpha) - f_K(\gamma) = \beta)$ не зависит от $\gamma$. Известно [10], что для марковского шифра $\Im$ последовательность случайных величин $\Delta Y(0) = \Delta X$, $\Delta Y(1)$, … образует простую однородную цепь Маркова. Отсюда следует равенство

$$\mathbf{P}\left(\Delta Y(i) = \beta \,/\, \Delta X = \alpha, X = \gamma\right) = \mathbf{P}\left(\Delta Y(i) = \beta \,/\, \Delta X = \alpha\right), \qquad (5)$$

справедливое для всех $i \in \overline{1,r}$, $0 \neq \alpha, \beta, \gamma \in G^n$.

Алгоритмы разностного криптоанализа блочных шифров изложены в [10 – 12]. Не останавливаясь на их описании, отметим, что теоретическая стойкость БШ $\Im$ относительно классической разностной атаки характеризуется параметром

$$d_{\max}^\Im(r-1) = \max\{ d_{r-1}^\Im(\alpha,\beta) : \alpha, \beta \in G^n \setminus 0\}. \qquad (6)$$

Критерием стойкости является условие $d_{\max}^\Im(r-1) - q^{-n} < \varepsilon$, где значение положительной константы $\varepsilon$ определяется, исходя из предположений относительно вычислительных ресурсов противника, допустимого значения надежности проводимой им атаки на шифр $\Im$ и т. д.

Метод разностного криптоанализа можно распространить на рандомизированные блочные системы шифрования [7]. С целью последующего анализа стойкости РБСШ $\Re$ относительно разностного криптоанализа, определим (в предположении независимости и

равновероятности раундовых ключей $k(1)$, …, $k(r)$ и открытых сообщений $S$, $S'$) матрицу $D_i(\Re) = \| d_i^{\Re}(s,\beta) \|$ вероятностей $i$-раундовых дифференциалов РБСШ $\Re$, полагая

$$d_i^{\Re}(s,\beta) = \mathbf{P}\left( \Delta Y(i) = \beta \Big/ \Delta S = s \right), s \in G^k, \beta \in G^n, i \in \overline{1,r}, \quad (7)$$

где $\Delta Y(i) = Y'(i) - Y(i)$, $\Delta S = S' - S$, $Y(i)$ и $Y'(i)$ случайные сообщения, вырабатываемые в $i$-м раунде шифрования по открытым текстам $S$ и $S'$ соответственно. Из результатов [7, 10] вытекает, что теоретическая стойкость РБСШ $\Re$ относительно классической разностной атаки характеризуется параметром

$$d_{\max}^{\Re}(r-1) = \max\{ d_{r-1}^{\Re}(s,\beta) : s \in G^k, \beta \in G^n \setminus 0 \}. \quad (8)$$

При этом условие $d_{\max}^{\Re}(r-1) - q^{-n} < \varepsilon$, аналогичное приведенному выше неравенству $d_{\max}^{\Im}(r-1) - q^{-n} < \varepsilon$, выражает критерий теоретической стойкости РБСШ $\Re$ относительно разностного криптоанализа.

В [7] получены верхние границы вероятностей (7) для специального класса рандомизированных систем шифрования, определяемых по гомоморизмам группы $G^n$ в абелевы группы. Следующие теоремы, устанавливающие аналитические выражения и оценки вероятностей раундовых дифференциалов произвольной РБСШ $\Re_{\Im}(S, T, \pi)$, обобщают и усиливают указанные результаты.

**Теорема 1.** Пусть $\Re = \Re_{\Im}(S, T, \pi)$ – определенная выше рандомизированная блочная система шифрования, соответствующая БШ $\Im$. Тогда в предположении случайности, независимости и равновероятности раундовых ключей $k(1)$, …, $k(r)$ шифра $\Im$ для любых $s \in G^k$, $\beta \in G^n$, $i \in \overline{1,r}$ выполняется равенство

$$d_i^{\Re}(s,\beta) = q^{-(n-k)} \sum_{\alpha \in \sigma^{-1}(s)} \mathbf{P}\left( F_{K(i)}(\rho(Z'')) - F_{K(i)}(\rho(Z')) = \beta \Big/ Z'' - Z' = \alpha \right), \quad (9)$$

где $F_{K(i)} = f_{k(i)} \cdots f_{k(1)}$, $i \in \overline{1,r}$, $Z''$ и $Z'$ – независимые случайные элементы, равномерно распределенные на группе $G^n$. Если, кроме того, $\Im$ является марковским шифром, то

$$d_i^{\Re}(s,\beta) = q^{-(n-k)} \sum_{\alpha \in \sigma^{-1}(s)} \sum_{\gamma \in G^n} DP^{\rho}(\alpha,\gamma) d_i^{\Im}(\gamma,\beta), \quad (10)$$

где значения $DP^{\rho}(\alpha,\gamma)$ и $d_i^{\Im}(\gamma,\beta)$ определяются по формулам (2) и (3) соответственно.

**Доказательство.** Для любого $s \in G^k$ положим

$$X_s = (\sigma\rho^{-1})^{-1}(s) = \rho(\sigma^{-1}(s)). \quad (11)$$

На основании равенства (7), формулы полной вероятности и определения РБСШ $\Re$ справедливы соотношения

$$d_i^{\Re}(s,\beta) = q^k \sum_{\substack{s',s'' \in G^k : \\ s''-s'=s}} \mathbf{P}(\Delta Y(i) = \beta, S' = s', S'' = s'') =$$

$$= q^{-2n+k} \sum_{\substack{s',s'' \in G^k : x' \in X_{s'}, \\ s''-s'=s \quad x'' \in X_{s''}}} \sum \mathbf{P}(F_{K(i)}(x'') - F_{K(i)}(x') = \beta). \quad (12)$$

Заметим, что в силу равенства (11) соотношения $x' \in X_{s'}$, $x'' \in X_{s''}$ равносильны соответственно соотношениям $\rho^{-1}(x') \in \sigma^{-1}(s')$, $\rho^{-1}(x'') \in \sigma^{-1}(s'')$. Следовательно, полагая в формуле (12) $z' = \rho^{-1}(x')$, $z'' = \rho^{-1}(x'')$, получим равенство

$$d_i^{\Re}(s,\beta) = q^{-2n+k} \sum_{\substack{s',s'' \in G^k : z' \in \sigma^{-1}(s'), \\ s''-s'=s \quad z'' \in \sigma^{-1}(s'')}} \sum \mathbf{P}(F_{K(i)}(\rho(z'')) - F_{K(i)}(\rho(z')) = \beta). \quad (13)$$

Заметим теперь, что, поскольку σ является гомоморфизмом групп, то при выполнении условия $s'' - s' = s$ справедливо следующее соотношение:

$$(z' \in \sigma^{-1}(s'),\ z'' \in \sigma^{-1}(s'')) \Leftrightarrow (\sigma(z') = s',\ \sigma(z'' - z') = s).$$

Отсюда на основании равенства (13) получим, что

$$d_i^{\Re}(s,\beta) = q^{-2n+k} \sum_{\substack{z' \in G^n, \\ z'' \in z' + \sigma^{-1}(s)}} \mathbf{P}(F_{K(i)}(\rho(z'')) - F_{K(i)}(\rho(z')) = \beta) =$$

$$= q^{-2n+k} \sum_{\alpha \in \sigma^{-1}(s)} \sum_{\substack{z', z'' \in G^n: \\ z'' - z' = \alpha}} \mathbf{P}(F_{K(i)}(\rho(z'')) - F_{K(i)}(\rho(z')) = \beta) =$$

$$= q^{-(n-k)} \sum_{\alpha \in \sigma^{-1}(s)} \mathbf{P}\left( F_{K(i)}(\rho(Z'')) - F_{K(i)}(\rho(Z')) = \beta \Big/ Z'' - Z' = \alpha \right).$$

Итак, равенство (9) доказано.

Для доказательства формулы (10) запишем равенство (9) в следующем виде:

$$d_i^{\Re}(s,\beta) = q^{-2n+k} \sum_{\alpha \in \sigma^{-1}(s)} \sum_{z \in G^n} \mathbf{P}(F_{K(i)}(\rho(z+\alpha)) - F_{K(i)}(\rho(z)) = \beta). \qquad (14)$$

Сделаем во внутренней сумме в правой части равенства (14) замену переменного, полагая $x = \rho(z)$, $x \in G^n$. В результате получим, что

$$\sum_{z \in G^n} \mathbf{P}(F_{K(i)}(\rho(z+\alpha)) - F_{K(i)}(\rho(z)) = \beta) =$$

$$= \sum_{x \in G^n} \mathbf{P}(F_{K(i)}(\rho(\rho^{-1}(x)+\alpha)) - F_{K(i)}(x)) = \beta) =$$

$$= \sum_{\gamma \in G^n} \sum_{\substack{x \in G^n: \\ \rho^{-1}(x+\gamma) - \rho^{-1}(x) = \alpha}} \mathbf{P}(F_{K(i)}(x+\gamma) - F_{K(i)}(x) = \beta).$$

Заметим теперь, что так как $\Im$ является марковским шифром, то на основании равенства (5) вероятность $\mathbf{P}(F_{K(i)}(x+\gamma) - F_{K(i)}(x) = \beta)$ не зависит от $x$. Следовательно, справедливы равенства

$$\sum_{z \in G^n} \mathbf{P}(F_{K(i)}(\rho(z+\alpha)) - F_{K(i)}(\rho(z)) = \beta) =$$

$$= \sum_{\gamma \in G^n} \mathbf{P}(F_{K(i)}(x_0+\gamma) - F_{K(i)}(x_0) = \beta)\ \#\{x \in G^n : \rho^{-1}(x+\gamma) - \rho^{-1}(x) = \alpha\} =$$

$$= \sum_{\gamma \in G^n} \mathbf{P}\left( \Delta Y(i) = \beta \Big/ \Delta X = \gamma \right) \#\{x \in G^n : \rho(x+\alpha) - \rho(x) = \gamma\}. \qquad (15)$$

Подставляя выражение (15) в формулу (14) и принимая во внимание соотношения (2), (3), получим равенство (10).

Теорема доказана.

Обозначим символом $\Im^{(\rho)}$ блочный шифр, множества открытых сообщений, шифрованных сообщений и раундовых ключей которого совпадают с соответствующими множествами БШ $\Im$, а функция шифрования $F^{(\rho)}$ определяется по формуле

$$F^{(\rho)}(x, \lambda) = F_\lambda(\rho(x)),\ x \in G^n,\ \lambda \in K^r.$$

Отметим ряд следствий, вытекающих из теоремы 1.

**Следствие 1.** При выполнении условий теоремы 1 для максимальной вероятности $(r-1)$-раундовых дифференциалов РБСШ $\Re$ справедливо следующее равенство:

$$d^{\Re}_{\max}(r-1)=\max\{q^{-(n-k)}\sum_{\alpha\in\sigma^{-1}(s)}d^{\Im^{(\rho)}}_{r-1}(\alpha,\beta):s\in G^k,\beta\in G^n\setminus 0\},\qquad(16)$$

где числа $d^{\Im^{(\rho)}}_{r-1}(\alpha,\beta)$ определяются по формуле (3) (с заменой $\Im$ на $\Im^{(\rho)}$).

Соотношение (16) позволяет дать количественное описание влияния указанного выше способа рандомизации источника сообщений на стойкость блочных шифров относительно метода разностного криптоанализа. Действительно, согласно равенству (16), максимальное значение вероятностей раундовых дифференциалов РБСШ $\Re$ является средним арифметическим вероятностей определенных раундовых дифференциалов БШ $\Im^{(\rho)}$ и, следовательно, на основании равенства (10) не превосходит значения $d^{\Im}_{\max}(r-1)$, характеризующего теоретическую стойкость исходного БШ $\Im$ относительно разностного криптоанализа. Таким образом, справедливо следующее утверждение.

**Следствие 2.** При выполнении условий теоремы 1 имеет место неравенство

$$d^{\Re}_{\max}(r-1)\le d^{\Im}_{\max}(r-1),\qquad(17)$$

В частности, рандомизированная блочная система шифрования $\Re_{\Im}(S,\ T,\ \pi)$ имеет не меньшую теоретическую стойкость относительно метода разностного криптоанализа, чем исходный блочный шифр $\Im$.

Получим верхние границы параметра $d^{\Re}_{\max}(r-1)$, позволяющие в ряде случаев непосредственно оценивать стойкость РБСШ $\Re$ относительно разностного криптоанализа.

Запишем равенство (10) в виде

$$d^{\Re}_{i}(s,\beta)=q^{-(n-k)}\sum_{\alpha\in\sigma^{-1}(s)}p^{(i)}(\alpha,\beta),\ s\in G^k,\beta\in G^n,\qquad(18)$$

где

$$p^{(i)}(\alpha,\beta)=\sum_{\gamma\in G^n}DP^{\rho}(\alpha,\gamma)d^{\Im}_{i}(\gamma,\beta),\qquad(19)$$

и параметры $DP^{\rho}(\alpha,\gamma)$, $d^{\Im}_{i}(\gamma,\beta)$ определяются по формулам (2), (3) соответственно, $i\in\overline{1,r}$.

Зафиксируем произвольный вектор $\beta\in G^n\setminus 0$ и рассмотрим преобразование Фурье распределения вероятностей $(p^{(r-1)}(\alpha,\beta):\alpha\in G^n)$ на группе $G^n$:

$$\pi^{(r-1)}(x,\beta)=\sum_{\alpha\in G^n}p^{(r-1)}(\alpha,\beta)\chi_{\alpha}(x),\ x\in G^n\qquad(20)$$

(здесь и далее символом $\chi_{\alpha}$ обозначается комплексный характер группы $G^n$, соответствующий элементу $\alpha\in G^n$) [13, 14]. Пусть $H=\{\alpha\in G^n:\chi_{\alpha}(x)=1,\ x\in T\}$ – дуальная к $T=\mathrm{Ker}\sigma$ подгруппа группы $G^n$. Применяя к выражению в правой части равенства (18) формулу для суммарной вероятности элементов смежного класса группы $G^n$ по подгруппе $T$ (см. лемму 1 из [15]), получим следующее выражение вероятности $(r-1)$-раундового дифференциала РБСШ $\Re$:

$$d^{\Re}_{r-1}(s,\beta)=q^{-n}+q^{-n}\sum_{x\in H\setminus 0}\pi^{(r-1)}(x,\beta)\overline{\chi}_{x}(\nu(s)),\ s\in G^k,\beta\in G^n\setminus 0,\qquad(21)$$

где $\nu(s)$ – фиксированный элемент, принадлежащий смежному классу $T_s=\sigma^{-1}(s)$, $s\in G^k$, $\overline{\chi}_{x}$ – комплексно-сопряженный к $\chi_x$ характер группы $G^n$.

Докажем следующую теорему.

**Теорема 2.** Пусть $\Im$ – марковский $r$-раундовый блочный шифр над абелевой группой $G=(\mathbf{GF}(q),+)$, $r\ge 2$. Тогда максимальная вероятность $(r-1)$-раундовых дифференциалов РБСШ $\Re=\Re_{\Im}(S,\ T,\ \pi)$ удовлетворяет следующему неравенству:

$$0 \le d^{\Re}_{\max}(r-1) - q^{-n} \le q^{k-2n} \max_{x \in H \setminus 0} \sum_{\gamma \in G^n \setminus 0} \left| \sum_{\omega \in G^n} \chi_x(\rho(\omega+\gamma) - \rho(\omega)) \right| d^{\Im}_{\max}(r-1). \qquad (22)$$

**Доказательство.** Нижняя граница (22) очевидна. Для доказательства верхней границы заметим, прежде всего, что на основании равенства (21) для любых $s \in G^k$, $\beta \in G^n \setminus 0$ справедливо неравенство

$$d^{\Re}_{r-1}(s,\beta) - q^{-n} \le q^{-n} \sum_{x \in H \setminus 0} \left| \pi^{(r-1)}(x,\beta) \right|$$

и, следовательно,

$$d^{\Re}_{\max}(r-1) - q^{-n} \le q^{k-n} \max_{\substack{x \in H \setminus 0, \\ \beta \in G^n \setminus 0}} \left| \pi^{(r-1)}(x,\beta) \right|, \qquad (22)$$

поскольку $|H| = q^n |T|^{-1} = q^k$.

Далее, используя формулы (19), (20), получим, что для любых $x$, $\beta \in G^n \setminus 0$ выполняются равенства

$$\pi^{(r-1)}(x,\beta) = \sum_{\alpha \in G^n} p^{(r-1)}(\alpha,\beta)\chi_\alpha(x) = \sum_{\gamma \in G^n} \Big( \sum_{\alpha \in G^n} DP^{\rho}(\alpha,\gamma)\chi_\alpha(x) \Big) d^{\Im}_{r-1}(\gamma,\beta).$$

Отсюда следует, что

$$\left| \pi^{(r-1)}(x,\beta) \right| \le \sum_{\gamma \in G^n} \left| \sum_{\alpha \in G^n} DP^{\rho}(\alpha,\gamma)\chi_\alpha(x) \right| d^{\Im}_{\max}(r-1), \; x, \beta \in G^n \setminus 0. \qquad (23)$$

Наконец, согласно формуле (2),

$$\sum_{\alpha \in G^n} DP^{\rho}(\alpha,\gamma)\chi_\alpha(x) = q^{-n} \sum_{\omega \in G^n} \chi_x(\rho(\omega+\gamma) - \rho(\omega)), \; x, \gamma \in G^n \setminus 0. \qquad (24)$$

Из соотношений (22) – (24) непосредственно вытекает верхняя граница (22).

Теорема доказана.

Будем говорить, что подстановка $\rho$: $G^n \to G^n$ имеет тривиальную линейную структуру, если не существует элементов $x, \gamma \in G^n \setminus 0$ таких, что функция $\chi_x(\rho(\omega+\gamma) - \rho(\omega))$, $\omega \in G^n$ является константой.

**Следствие 3.** Пусть выполняются условия теоремы 2, и подстановка $\rho$ имеет тривиальную линейную структуру. Пусть, далее, (при отождествлении группы $G^n = (\mathbf{GF}(q)^n, +)$ с аддитивной группой поля из $q^n$ элементов) степень полинома, представляющего подстановку $\rho$ над полем $\mathbf{GF}(q^n)$, равна числу $d \ge 3$. Тогда справедливо следующее неравенство:

$$0 \le d^{\Re}_{\max}(r-1) - q^{-n} \le (d-2)\, q^{k-n/2}\, d^{\Im}_{\max}(r-1). \qquad (25)$$

**Доказательство.** Из условия тривиальности линейной структуры подстановки $\rho$ вытекает, что тригонометрическая сумма

$$S(x,\gamma) = \sum_{\omega \in G^n} \chi_x(\rho(\omega+\gamma) - \rho(\omega)), \; x, \gamma \in G^n \setminus 0, \qquad (26)$$

удовлетворяет условиям теоремы Вейля [13], в соответствии с которой для любых $x, \gamma \in G^n \setminus 0$ выполняется соотношение $|S(x,\gamma)| \le (d-2)\, q^{n/2}$. Отсюда на основании неравенств (22) следует справедливость неравенств (25), что и требовалось доказать.

**Следствие 4.** При выполнении условий следствия 3 справедливо неравенство

$$0 \le d^{\Re}_{\max}(r-1) - q^{-n} \le (d-2)\, q^{k-3n/2}. \qquad (27)$$

**Доказательство.** Заметим, что, поскольку матрица $D_{r-1}(\Im)$ является стохастической (см. [10]), то на основании неравенства (22) и соотношения

$$\pi^{(r-1)}(x,\beta)=\sum_{\gamma\in G^n}\Big(\sum_{\alpha\in G^n}DP^{\rho}(\alpha,\gamma)\chi_{\alpha}(x)\Big)d^{\Im}_{r-1}(\gamma,\beta),\ x,\beta\in G^n\setminus 0,$$

справедлива оценка

$$d^{\Re}_{\max}(r-1)-q^{-n}\le q^{k-n}\max_{\substack{x\in H\setminus 0,\\ \gamma\in G^n\setminus 0}}\left|\sum_{\alpha\in G^n}DP^{\rho}(\alpha,\gamma)\chi_{\alpha}(x)\right|.$$

Отсюда на основании соотношений (24), (26) и утверждения теоремы Вейля [13] вытекает неравенство (27). Следствие доказано.

Полученные аналитические выражения верхних границ максимума вероятностей раундовых дифференциалов РБСШ $\Re$ позволяют оценить выигрыш в теоретической стойкости системы шифрования $\Re$ по сравнению со стойкостью исходного блочного шифра $\Im$ относительно метода разностного криптоанализа. Действительно, на основании неравенства (22) отношение параметра $d^{\Im}_{\max}(r-1)$ к параметру $d^{\Re}_{\max}(r-1)-q^{-n}$ может быть рассчитано по формуле

$$w_d(\Re;\Im)=\frac{d^{\Im}_{\max}(r-1)}{d^{\Re}_{\max}(r-1)-q^{-n}}\ge q^{2n-k}\left(\max_{x\in H\setminus 0}\sum_{\gamma\in G^n\setminus 0}\left|\sum_{\omega\in G^n}\chi_x(\rho(\omega+\gamma)-\rho(\omega))\right|\right)^{-1}. \qquad (28)$$

Кроме того, если подстановка $\rho$ имеет тривиальную линейную структуру и является полиномом степени $d\ge 3$ над полем $\mathbf{GF}(q^n)$, то теоретическая стойкость РБСШ $\Re$ относительно разностного криптоанализа будет в

$$w_d(\Re;\Im)\ge(d-2)^{-1}q^{n/2-k} \qquad (29)$$

раз выше по сравнению с теоретической стойкостью исходного (марковского) блочного шифра $\Im$.

Отметим, что аналитические оценки (27), (29) не зависят от особенностей строения блочного шифра $\Im$ (в частности, от того, насколько стойким к разностному криптоанализу является этот шифр). Таким образом, полученные оценки могут быть использованы для обоснования теоретической стойкости РБСШ $\Re$ относительно метода разностного криптоанализа, в том числе, в условиях отсутствия полной информации о криптографической схеме исходного БШ $\Im$.

## Список літератури

1. *Rivest R.L., Sherman A.T.* Randomization encryption techniques // Advances in Cryptology – CRYPTO'82, Proceedings. – Springer Verlag, 1982. – P. 145 – 167.

2. *Massey J. L.* An Introduction to Contemporary Cryptology // Proc. IEEE. – 1988. – V. 76. – № 5. – P. 533 – 549.

3. *Gunter Ch.G.* A universal algorithm for homophonic coding // Advances in Cryptology – EUROCRYPT' 88, Proceedings. – Springer Verlag, 1988. – P. 405 – 414.

4. *Jendal H.N., Kuhn Y.J.B., Massey J.L.* An information-theoretic treatment of homophonic substitution // Advances in Cryptology – EUROCRYPT' 89, Proceedings. – Springer Verlag, 1989. – P. 382 – 394.

5. *Штарьков Ю.М.* Некоторые теоретико-информационные задачи защиты дискретных данных // Проблемы передачи информации. – 1994. – Т. 30. – Вып. 2. – С. 49 – 60.

6. *Штарьков Ю.М., Юхансон Т., Смитс Б.Дж.М.* О совместной стойкости защиты информации и ключа в секретных системах // Проблемы передачи информации. – 1998. – Т. 34. – Вып. 2. – С. 117 – 127.

7. *Алексейчук А.Н., Васюков И.В., Корнейко А.В.* Обоснование стойкости вероятностных моделей рандомизированных блочных шифров к методу разностного криптоанализа // Электронное моделирование. – 2004. – Т. 26. – № 4. – С. 23 – 35.

8. *Алексейчук А.Н.* Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм // Реєстрація, зберігання і обробка даних. – 2007. – Т. 9. – № 2 (в печати).

9. *Wagner D.* Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 116 – 135.

10. *Lai X., Massey J.L., Murphy S.* Markov chiphers and differential cryptoanalysis // Advances in Cryptology – EUROCRYPT' 91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.

11. *Biham E, Shamir A.* Differential cryptoanalysis of DES-like cryptosystems // J. of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.

12. *Харин Ю.С., Берник В.И., Матвеев Г.В.* Математические основы криптологии. – Минск.: Изд-во БГУ, 1999. – 319 с.

13. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.

14. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. М.: Мир, 1976. 136 с.

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

*Поступила 18.05.2007 г.*

**УДК 621.391:519.7:510.5**

**Волошин А. Л.**

## МЕТОД ПОСТРОЕНИЯ СОВЕРШЕННЫХ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ, РЕАЛИЗУЮЩИХ СЕМЕЙСТВА ИЕРАРХИЙ ДОСТУПА, ДЛЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

При разработке современных информационно-телекоммуникационных систем (ИТС) особое внимание уделяется вопросам разграничения доступа к их ресурсам [1]. Согласно принятой мировой и отечественной практике [2, 3], решение задач разграничения доступа к ресурсам ИТС возлагается на подсистему управления доступом (ПУД), которая обычно включается в состав ИТС как отдельная функциональная подсистема. Развитие информационных технологий, систем связи и средств телекоммуникаций, расширение функциональных возможностей ИТС, и, как следствие, сферы их практического применения, создание новых технологических платформ хранения и обработки данных требуют повышения надежностных и эксплуатационных характеристик современных ПУД.

Исходя из особенностей практического использования ИТС в отечественных системах электронного документооборота, на сегодняшний день наибольшее применение находят ПУД, реализующие многоуровневую политику безопасности [4]. Известно также [5, 6], что доминирующую роль при построении ПУД играют криптографические методы; при этом использование протоколов разделения секрета (ПРС) позволяет получать приемлемые