УДК 621.372 **Скрыпник Л.В, Ковальчук Л.В.**

ВЕРХНИЕ ОЦЕНКИ СРЕДНИХ ВЕРОЯТНОСТЕЙ ДИФФЕРЕНЦИАЛОВ БУЛЕВЫХ ОТОБРАЖЕНИЙ

Вступление

В большинстве работ, посвященных исследованию стойкости блочных шифров относительно линейного и дифференциального криптоанализа, изучаются SPN-шифры и шифры Фейстеля, единственными нелинейными преобразованиями в которых являются *s*-блоки, а ключевой сумматор реализует операцию побитового булевого сложения двоичных векторов. В работах [1-5] и других разработан и развит математический аппарат для оценки стойкости таких шифров к указанным методам криптоанализа.

Вместе с тем некоторые современные шифры (например [6,7]) имеют другой принцип построения; в частности, ключевой сумматор реализует операции сложения по модулям 2^{16} и 2^{32}. Известные методы оценки стойкости классических блочных шифров [1-5] оказываются, вообще говоря, не применимыми к анализу стойкости шифров, описанных в [6,7].

В [8] введены новые числовые параметры, зависящие от *s*-блоков, для шифров Фейстеля типа ГОСТ 28147-89, в терминах которых получены аналитические выражения для верхних оценок средних вероятностей дифференциальных и линейных характеристик шифра.

В данной работе получен ряд новых верхних границ средних вероятностей дифференциалов для отображений на множестве $\{0,1\}^m$, представляющих собой композицию ключевого сумматора, реализующего сложение по модулю 2^m, и блока подстановки (для различных вариантов задания групповых операций на области определения и множестве значений таких отображений).

1. Оценки средних вероятностей дифференциалов для композиции сумматора по модулю 2^m и блока подстановки

Далее будем использовать обозначения

$$V_m = \{0,1\}^m, \quad m \in N;$$

$$f_k(x) = \varphi(x+k), \quad x, k \in \mathrm{V_m}, \tag{1}$$

где под операцией сложения понимается сложение по модулю 2^m, а функция $\phi: V^m \to V^m$ обладает следующим свойством:

$$\varphi(x_2, x_1) = 2^{m-t}\varphi_2(x_2) + \varphi_1(x_1), \tag{2}$$

где $x_2 \in V_t$, $x_1 \in V_{m-t}$, $\varphi_1 : V_{m-t} \to V_{m-t}$, $\varphi_2 : V_t \to V_t$ − биекции; сложение выполняется по модулю 2^m. Примером такой функции является блок подстановки в алгоритме ГОСТ 28147-89.

Рассмотрим следующие величины:

$$d_{f_r}(\alpha, \beta) = 2^{-m} \sum_{x \in V_m} \delta\left(f_k(x \circ \alpha) \bullet f_k^*(x); \beta\right), \tag{3}$$

$$D_f(\alpha, \beta) = 2^{-m} \sum_{k \in V_m} d_{f_k}(\alpha, \beta), \tag{4}$$

где символ δ является символом Кронекера, под операциями “о” и “•” понимаются некоторые групповые операции, определённые на V_m, $f_k^*(x)$ означает элемент, обратный к $f_k(x)$ относительно операции “•”. Эти символы являются обобщениями (на случай произвольно выбранных на V_m операций, относительно которых рассматриваются входная и выходная разности) вероятности того, что разность α перейдёт в разность β и средней (по ключам) вероятности этого события, соответственно.

Также будем использовать обозначения “+” (“-”) и “$\oplus$”, означающие, соответственно, операции сложения (вычитания) по модулю 2^l, где значение l будет ясно из контекста, и побитовое сложение двоичных векторов.

Далее мы будем строить верхние оценки для $D_f(\alpha,\beta)$ и $\max\limits_{\alpha,\beta\neq 0} D_f(\alpha,\beta)$ при различном выборе операций “ o” и “$\bullet$”.

Теорема 1.

В наших обозначениях справедливы следующие неравенства (в зависимости от выбора операций на V_m):

1) $D_f(\alpha,\beta)\le W^{\varphi_2}(\alpha_2,\beta_2)D_{\varphi_1}(\alpha_1,\beta_1)$,

где “ o” и “$\bullet$” – операции сложения по модулю 2^m;

$$W^{\varphi_2}(\alpha_2,\beta_2)=2^{-t}\max_{\eta,\nu\in V_1}\left\{\sum_{x_2\in V_t}\delta(\varphi_2(x_2+\alpha_2+\nu)-\varphi_2(x_2)-\eta;\beta_2)\right\},$$

$$\alpha=(\alpha_2,\alpha_1),\quad \beta=(\beta_2,\beta_1),\quad \alpha_1,\beta_1\in V_{m-t},\quad \alpha_2,\beta_2\in V_t.$$

2) $D_f(\alpha,\beta)\le U^{\varphi_2}(\alpha_2,\beta_2)D_{\varphi_1}(\alpha_1,\beta_1)$,

где “ o” - операция сложения по модулю 2^m, “$\bullet$” – операция сложения по модулю 2;

$$U^{\varphi_2}(\alpha_2,\beta_2)=2^{-t}\max_{\nu\in V_1}\left\{\sum_{x_2\in V_t}\delta(\varphi_2(x_2+\alpha_2+\nu)\oplus\varphi_2(x_2);\beta_2)\right\},$$

$$\alpha=(\alpha_2,\alpha_1),\quad \beta=(\beta_2,\beta_1),\quad \alpha_1,\beta_1\in V_{m-t},\quad \alpha_2,\beta_2\in V_t.$$

3) $D_f(\alpha,\beta)\le V^{\varphi_2}(\alpha_2,\beta_2)D_{\varphi_1}(\alpha_1,\beta_1)$,

где “ o” - операция сложения по модулю 2, “$\bullet$” – операция сложения по модулю 2^m;

$$V^{\varphi_2}(\alpha_2,\beta_2)=2^{-2t}\max_{\nu,\mu,\eta\in V_1}\left\{\sum_{x_2,k_2\in V_t}\delta(\varphi_2((x_2\oplus\alpha_2)+k_2+\mu)-\varphi_2(x_2+k_2+\nu)-\eta;\beta_2)\right\}$$

$$\alpha=(\alpha_2,\alpha_1),\quad \beta=(\beta_2,\beta_1),\quad \alpha_1,\beta_1\in V_{m-t},\quad \alpha_2,\beta_2\in V_t.$$

4) $D_f(\alpha,\beta)\le Y^{\varphi_2}(\alpha_2,\beta_2)D_{\varphi_1}(\alpha_1,\beta_1)$,

где “ o” и “$\bullet$” – операции сложения по модулю 2;

$$Y^{\varphi_2}(\alpha_2,\beta_2)=2^{-2t}\max_{\nu,\eta\in V_1}\left\{\sum_{x_2,k_2\in V_t}\delta(\varphi_2((x_2\oplus\alpha_2)+k_2+\nu)\oplus\varphi_2(x_2+k_2+\eta);\beta_2)\right\}$$

$$\alpha=(\alpha_2,\alpha_1),\quad \beta=(\beta_2,\beta_1),\quad \alpha_1,\beta_1\in V_{m-t},\quad \alpha_2,\beta_2\in V_t.$$

Доказательство:

1) Заметим, что в условиях п.1 переменную k в (3) и (4) можно исключить путём замены переменной; следовательно, $d_{f_r}(\alpha,\beta)$ не будет зависеть от k и $D_f(\alpha,\beta)=d_{f_k}(\alpha,\beta)\quad\forall k$. Далее, в нащих обозначениях

$$\varphi(x+\alpha)=\varphi(x_2+\alpha_2+\nu(x_1,\alpha_1),x_1+\alpha_1),$$

где $\nu(x_1,\alpha_1)$ – бит переноса в t-й разряд при обычном сложении чисел x_1,α_1, представленных в двоичном виде. Вследствие условия (2),

$$\varphi(x+\alpha)=(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1)),\varphi_1(x_1+\alpha_1)).$$

Аналогично, $\varphi(x)=(\varphi_2(x_2),\varphi_1(x))$. Следовательно,

$$\varphi(x+\alpha)-\varphi(x)=((\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))-\varphi_2(x_2-\eta(x_1,\alpha_1;\varphi_1));\ \varphi_1(x_1+\alpha_1)-\varphi_1(x_1)),$$

где $\eta(x_1,\alpha_1;\varphi_1)$ – бит, который могли занимать в $\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))$ при вычитании $\varphi_1(x_1+\alpha_1)-\varphi_1(x_1)$; $\eta(x_1,\alpha_1;\varphi_1)\in\{0,1\}$. Поэтому

$$D_f(\alpha,\beta)=2^{-m}\sum_{x\in V_m}\delta(\varphi_2(x_2+\alpha_2+\nu)-\varphi_2(x_2)-\eta\,;\beta_2)\ \delta(\varphi_1(x_1+\alpha_1)-\varphi_1(x_1);\beta_1)=$$

$$=2^{-(m-t)}\times$$

$$\times\sum_{\nu,\eta\in\{0,1\}}\left\{\sum_{\substack{x_1\in V_{m-t}\\ \eta(x_1,\alpha_1,\varphi_1)=\eta\\ \nu(x_1,\alpha_1)=\nu}}\delta(\varphi_1(x_1+\alpha_1)-\varphi_1(x_1);\beta)2^{-t}\sum_{x_2\in V_t}\delta(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))-\varphi_2(x_2)-\eta(x_1,\alpha_1;\varphi_1);\beta_2)\right\}=$$

$$=2^{-(m-t)}\sum_{\nu,\eta\in\{0,1\}}\left\{\sum_{\substack{x_1\in V_{m-t}\\ \eta(x_1,\alpha_1,\varphi_1)=\eta\\ \nu(x_1,\alpha_1)=\nu}}u(x_1)v(\nu,\eta)\right\},$$

где $u(x_1)=\delta(\varphi_1(x_1+\alpha_1)-\varphi_1(x_1);\beta)$,

$$v(\nu,\eta)=\sum_{\nu,\eta\in\{0,1\}}\left\{\sum_{\substack{x_1\in V_{m-t}\\ \eta(x_1,\alpha_1,\varphi_1)=\eta\\ \nu(x_1,\alpha_1)=\nu}}\delta(\varphi_1(x_1+\alpha_1)-\varphi_1(x_1);\beta)2^{-t}\sum_{x_2\in V_t}\delta(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))-\varphi_2(x_2)-\eta(x_1,\alpha_1;\varphi_1);\beta_2)\right\}.$$

Поскольку $v(\nu,\eta)\le\max\limits_{\nu,\eta\in\{0,1\}}v(\nu,\eta)=W^{\varphi_2}(\alpha_2,\beta_2)$, то

$$D_f(\alpha,\beta)\le W^{\varphi_2}(\alpha_2,\beta_2)\,2^{-(m-t)}\sum_{\nu,\eta\in\{0,1\}}\left\{\sum_{\substack{x_1\in V_{m-t}\\ \eta(x_1,\alpha_1,\varphi_1)=\eta\\ \nu(x_1,\alpha_1)=\nu}}u(x_1)\right\}=$$

$$=W^{\varphi_2}(\alpha_2,\beta_2)\,2^{-(m-t)}\sum_{x_1\in V_{m-t}}\delta(\varphi_1(x_1+\alpha_1)-\varphi_1(x_1);\beta)=W^{\varphi_2}(\alpha_2,\beta_2)D_{\varphi_1}(\alpha_1,\beta_1).$$

2) По определению,

$$d_{f_r}(\alpha,\beta)=2^{-m}\sum_{x\in V_m}\delta(f_k(x+\alpha)\oplus f_k(x);\beta)=2^{-m}\sum_{x\in V_m}\delta(\varphi(x+\alpha+k)\oplus\varphi(x+k);\beta)=$$

$=2^{-m}\sum\limits_{x\in V_m}\delta(\varphi(x+\alpha)\oplus\varphi(x);\beta)$ посредством замены переменной.

Следовательно, $D_f(\alpha,\beta)=d_{f_k}(\alpha,\beta)=d_\varphi(\alpha,\beta)$. С использованием обозначения для бита переноса, введенного в предыдущем разделе, получаем:

$\varphi(x+\alpha)=(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1)),\varphi_1(x_1+\alpha_1))$, $\varphi(x)=(\varphi_2(x_2),\varphi_1(x))$;

$\varphi(x+\alpha)\oplus\varphi(x)=(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))\oplus\varphi_2(x_2));\ \varphi_1(x_1+\alpha_1)\oplus\varphi_1(x_1))$,

поэтому

$$d_f(\alpha,\beta)=2^{-t}\sum_{x_2\in V_t}\delta(\varphi_2(x_2+\alpha_2+\nu(x_1,\alpha_1))\oplus\varphi_2(x_2);\beta_2)2^{-(m-t)}\sum_{x_1\in V_{m-t}}\delta(\varphi_1(x_1+\alpha_1)\oplus\varphi_1(x_1);\beta_1)=$$

$$=2^{-t}\max_{\nu\in\{0,1\}}\sum_{x_2\in V_t}\{\delta(\varphi_2(x_2+\alpha_2+\nu)\oplus\varphi_2(x_2);\beta_2)\}\cdot d_{\varphi_1}(\alpha_1,\beta_1).$$

3) По определению,

$$d_{f_r}(\alpha,\beta)=2^{-m}\sum_{x\in V_m}\delta(f_k(x\oplus\alpha)-f_k(x);\beta)=2^{-m}\sum_{x\in V_m}\delta(\varphi((x\oplus\alpha)+k)-\varphi(x+k);\beta).$$

Как видно, в этом случае нельзя исключить переменную k посредством замены переменной. Поскольку

$$\varphi(x+k) = (\varphi_2(x_2 + k_2 + \nu(x_1,k_1)), \varphi_1(x_1 + k_1)),$$
$$\varphi((x \oplus \alpha) + k) = (\varphi_2((x_2 \oplus \alpha_2) + k_2 + \mu(x_1,\alpha_1,k_1)); \varphi_1((x_1 \oplus \alpha_1) + k_1)),$$

то

$$\varphi((x \oplus \alpha) + k) - \varphi(x+k) =$$
$$= \varphi_2((x_2 \oplus \alpha_2) + k_2 + \mu(x_1,\alpha_1,k_1)) - \varphi_2(x_2 + k_2 + \nu(x_1,k_1)) - \eta(x_1,\alpha_1,k_1); \varphi_1((x_1 \oplus \alpha_1) + k_1) - \varphi_1(x_1 + k_1))$$

и

$$\delta(\varphi((x \oplus \alpha) + k) - \varphi(x+k), \beta) =$$
$$= \delta(\varphi_2((x_2 \oplus \alpha_2) + k_2 + \mu(x_1,\alpha_1,k_1)) - \varphi_2(x_2 + k_2 + \nu(x_1,k_1)) - \eta(x_1,\alpha_1,k_1); \beta_2) \times$$
$$\times \delta(\varphi_1((x_1 \oplus \alpha_1) + k_1) - \varphi_1(x_1 + k_1); \beta_1).$$

После несложных преобразований, аналогичных тем, которые выполнялись в предыдущих пунктах, получается утверждение 3.

Доказательство п. 4 было представлено ранее [8].

<u>Следствие.</u>

Пусть $m = pt$, $\alpha = (\alpha_1,...,\alpha_p)$, $\beta = (\beta_1,...,\beta_p)$, $\alpha_i, \beta_i \in V_t$,

$$\varphi(\alpha) = \sum_{i=1}^{p} 2^{(i-1)t} \varphi_i(\alpha_i), \quad (5)$$

где $\varphi_i : V_t \to V_t$ - биекции, $i = \overline{1,p}$, сложение в (5) выполняется по модулю 2^m. Тогда в условиях п.1-4 теоремы 1 справедливы, соответственно, следующие неравенства:

1) $D_f(\alpha,\beta) \le \prod_{i=2}^{p} W^{\varphi_i}(\alpha_i,\beta_i) D_{\varphi_1}(\alpha_1,\beta_1)$;

2) $D_f(\alpha,\beta) \le \prod_{i=2}^{p} U^{\varphi_i}(\alpha_i,\beta_i) D_{\varphi_1}(\alpha_1,\beta_1)$;

3) $D_f(\alpha,\beta) \le \prod_{i=2}^{p} V^{\varphi_i}(\alpha_i,\beta_i) D_{\varphi_1}(\alpha_1,\beta_1)$;

4) $D_f(\alpha,\beta) \le \prod_{i=2}^{p} Y^{\varphi_i}(\alpha_i,\beta_i) D_{\varphi_1}(\alpha_1,\beta_1)$.

Данное следствие позволяет оценить сверху среднюю (по ключам) вероятность того, что входная разность α перейдёт в выходную разность β при прохождении через композицию ключевого сумматора и блока подстановки, где разности определяются относительно различных групповых операций на V_m. Причём для вычисления данной верхней оценки достаточно вычислить некоторые параметры, связанные с отдельными *s*-блоками, из которых состоит блок подстановки. Это позволяет суммирование (и усреднение) по всем векторам из V_m (что вычислительно нереализуемо за реальное время) заменить суммированием по всем векторам из V_t, что оказывается, как правило, вполне приемлемым (например, при *m*=32 и *t*=4).

В таблице приведены результаты статистических оценок распределений вероятностей параметров W^φ, U^φ, V^φ, Y^φ для $\varphi : V_4 \to V_4$ (как функций равновероятной подстановки φ на V_4). Как видно из таблицы, основные значения данных параметров сосредоточены на интервале от 0.15 до 0. 25.

Результаты статистической оценки распределения параметров W^{φ}, U^{φ}, V^{φ}, Y^{φ} (для 10^4 подстановок φ на V_4)

Интервал значений параметра	Количество подстановок, для которых W^{φ} находится в данном интервале	Количество подстановок, для которых U^{φ} находится в данном интервале	Количество подстановок, для которых V^{φ} находится в данном интервале	Количество подстановок, для которых Y^{φ} находится в данном интервале
0.0 – 0.05	0	0	0	0
0.05 – 0.10	0	0	0	0
0.10 – 0.15	24	0	784	0
0.15 – 0.20	3899	225	7075	325
0.20 – 0.25	4650	5627	1851	5998
0.25 – 0.30	0	0	12	0
0.30 – 0.35	1196	1360	245	1065
0.35 – 0.40	200	2423	29	2274
0.40 – 0.45	28	20	3	5
0.45 – 0.50	3	310	1	301
0.50 – 0.55	0	0	0	0
0.55 – 0.60	0	0	0	0
0.60 – 0.65	0	30	0	28
0.65 – 0.70	0	0	0	0
0.70 – 0.75	0	5	0	4
0.75 – 0.80	0	0	0	0
0.80 – 0.85	0	0	0	0
0.85 – 0.90	0	0	0	0
0.90 – 0.95	0	0	0	0
0.95 – 1.00	0	0	0	0

2. Дифференциальные аппроксимации для раундовой функции в схеме Фейстеля

Пусть $f_k(x,y) = (y, x \oplus \varphi(y+k))$, где $x,y,k \in V_m$, φ обладает свойством (2). На множестве V_{2m} введём следующие операции:

$$v\,\mathrm{o}\,u = \left(v^L \oplus u^L,\quad v^R + u^R\right),$$
$$v \bullet u = \left(v^L + u^L,\quad v^R \oplus u^R\right),$$

где $v=(v^L,v^R)$, $u=(u^L,u^R)$, $v^L,v^R,u^L,u^R \in V_m$ "+" означает сложение по модулю 2^m, "$\oplus$" - сложение по модулю 2.

Аналогично предыдущему разделу будем рассматривать величины

$$d_{f_r}(\alpha,\beta) = 2^{-2m}\sum_{x\in V_{2m}}\delta\left(f_k(x\,\mathrm{o}\,\alpha)\bullet f_k^*(x);\beta\right); \qquad (6)$$

$$D_f(\alpha,\beta) = 2^{-m}\sum_{k\in V_m} d_{f_k}(\alpha,\beta). \qquad (7)$$

Операции, определённые выше, интересны следующим своим свойством. Если рассматривать входную разность относительно операции "o", а выходную – относительно операции "$\bullet$", как в (6), то шифр ГОСТ 28147-89 является марковским [9] относительно этих операций, как будет показано в следующей лемме. Однако в этом случае возникают проблемы при соединении разностей в последовательных раундах.

Лемма.

В обозначениях (6), (7) выполнено:

$$D_f(\alpha,\beta) = d_{f_k}(\alpha,\beta) = \delta\left(\alpha^R,\beta^L\right)d_{\varphi}\left(\alpha^R,\beta^R-\alpha^L\right) \quad \forall k \in V_m,$$

где $d_{\varphi}(\alpha,\beta) = 2^{-m}\sum_{x\in V_m}\delta\left(\varphi_k(x+\alpha)-\varphi_k(x);\beta\right) = 2^{-m}\sum_{x\in V_m}\delta\left(\varphi(x+\alpha)-\varphi(x);\beta\right)$ и не зависит от k.

Доказательство:

В наших обозначениях $x \circ \alpha = \left(x^L \oplus \alpha^L, \quad x^R + \alpha^R\right)$; $f_k(x) = (x^R; x^L \oplus \varphi(x^R + k))$;

$f_k(x \circ \alpha) = \left(x^R + \alpha^R; \quad x^L \oplus \alpha^L \oplus \varphi(x^R + \alpha^R + k)\right)$.

Тогда

$f_k(x \circ \alpha) \bullet f_k^*(x) = \left(\alpha^R; \quad \varphi(x^R + \alpha^R + k) \oplus \varphi(x^R + k) \oplus \alpha^L\right)$, следовательно,

$\delta(f_k(x \circ \alpha) \bullet f_k^*(x); \beta) = \delta(\alpha^R, \beta^L)\delta\left(\varphi(x^R + \alpha^R + k) - \varphi(x^R + k), \beta^R - \alpha^L\right)$,

т.е. условие $\alpha^R = \beta^L$ является необходимым для выполнения условия $d_{f_k}(\alpha, \beta) \neq 0$; при этом

$$d_{f_k}(\alpha, \beta) = \delta(\alpha^R, \beta^L) 2^{-m} \sum_{x_1 \in V_m} \delta\left(\varphi(x^R + \alpha^R + k) - \varphi(x^R + k), \beta^R - \alpha^L\right) =$$

$$= \delta(\alpha^R, \beta^L) 2^{-m} \sum_{x_1 \in V_m} \delta\left(\varphi(x^R + \alpha^R) - \varphi(x^R), \beta^R - \alpha^L\right) = \delta(\alpha^R, \beta^L) d_\varphi(\alpha^R, \beta^R - \alpha^L),$$

для $\forall k \in V_m$. Заметим также, что в данном случае

$D_f(\alpha, \beta) = d_{f_k}(\alpha, \beta) = \delta\left(\alpha^R, \beta^L\right) d_\varphi\left(\alpha^R, \beta^R - \alpha^L\right) \quad \forall k \in V_m$ и при условии $\alpha^R = \beta^L$ выполнено равенство $D_f(\alpha, \beta) = d_\varphi\left(\alpha^R, \beta^R - \alpha^L\right) \quad \forall k \in V_m$.

На основании приведенной выше леммы и теоремы 1 получаем следующую теорему.

Теорема 2.

В обозначениях (6), (7) выполнено:

$$d_\varphi(\alpha, \beta) \leq \Delta^{\varphi_2}(\alpha_2, \beta_2) d_{\varphi_1}(\alpha_1, \beta_1),$$

где $\Delta^{\varphi_2}(\alpha_2, \beta_2) = 2^{-t} \max\limits_{\eta, \nu \in V_1} \left\{ \sum\limits_{x_2 \in V_t} \delta\left(\varphi_2(x_2 + \alpha_2 + \nu) - \varphi_2(x_2) - \eta\ ; \beta_2\right) \right\}$,

$\alpha = (\alpha_2, \alpha_1), \quad \beta = (\beta_2, \beta_1), \quad \alpha_1, \beta_1 \in V_{m-t}, \quad \alpha_2, \beta_2 \in V_t.$

Полученные результаты могут быть использованы для вычисления оценок стойкости некоторых классов блочных шифров относительно различных видов дифференциальных атак, т.е. при различных операциях, определённых на множестве V_m.

Список литературы

1. *Biham E, Shamir A.* Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.
2. *Matsui M.* Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer Verlag, 1994. – P. 386 – 397.
3. *Knudsen L.R.* Practically secure Feistel cipher // Fast Software Encryption. – FSE'94, Proceedings. – Springer Verlag, 1994. – P. 211 – 221.
4. *Kanda M.* Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. – SAC 2000, Proceedings. – Springer Verlag, 2001. – P. 324 – 338.
5. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. of Cryptology. – 2003. – V. 16. – № 4. – P. 249 – 286.
6. Государственный стандарт 28147-89. Криптографическая защита систем обработки данных. Государственный комитет СССР по стандартам, 1989.
7. *Lai X., Massey J.L., Murphy S.* Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.
8. *Алексейчук А., Ковальчук Л.* Линейный и дифференциальный криптоанализ шифров, содержащих сумматор по модулю 2^m // Международная конференция "Современные проблемы и новые течения в теории вероятностей", Черновцы, 19-26 июня 2005 г., с. 9-10.

9. *Vaudenay S.* On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.

Поступила 22.03.2006

УДК 621.372 **Корченко О. Г., Ануфрієнко К.П.**

КЛАСИФІКАЦІЯ УРАЗЛИВОСТЕЙ В ПОЧАТКОВИХ КОДАХ

Наприкінці минулого століття на ринку програмних засобів забезпечення безпеки відбувся значний сплеск: з'явились та набули поширення різноманітні антивірусні програми, міжмережеві екрани, криптографічні та інші програмні засоби. Проте після багатьох років використання цих засобів кількість атак на ресурси комп'ютерних систем (КС) продовжує зростати [1]. Інциденти з безпекою на прикладному рівні взаємодії комп'ютерних систем посідають чільне місце серед найбільш значних проблем безпеки інформаційних технологій. Традиційні методи та засоби захисту інформаційних технологій в основному зосереджені на мережевому й периметровому захисті, лишаючи поза увагою проблему захищеності програмного забезпечення (ПЗ). В результаті ПЗ виявляється зазвичай слабкою ланкою в системі захисту. Так, за даними Національного інституту стандартів і технологій США, 93% уразливостей, які знаходять, – це уразливості в ПЗ [2].

У зв'язку зі специфікою розробки ПЗ, уразливості у ньому виникають в основному в процесі розробки під час написання початкового коду. Кількість уразливостей в початкових кодах невпинно зростає. Згідно з даними CERT Coordination Center за 1998 р. було зафіксовано 262 уразливості, тоді як за 2002 р. – 4131 уразливість [3].

І в той час, як більшість розроблювачів оцінюють функціональні можливості, продуктивність і здатність до інтеграції додатків, відсутність перевірки їх захищеності під час процесу розробки може мати серйозні наслідки. Помилка в коді програми може призвести до таких катастрофічних збитків, як втрата інтелектуальної власності, коштів або важливих даних.

Проблема аналізу захищеності ПЗ, вибору ефективних методів і засобів розробки захищеного ПЗ (ЗПЗ) та розробки систем виявлення уразливостей в початкових кодах значною мірою залежить від організації життєвого циклу зазначеного забезпечення, мови програмування, конкретних реалізацій алгоритмів обробки вхідних даних, можливостей порушень характеристик безпеки та інших чинників. Ефективність її розв'язання в першу чергу пов'язана із визначенням того, на які класи уразливостей розраховані ті чи інші методи та засоби їх виявлення.

Проблема уразливостей і їх виявлення досліджується досить давно. У роботах [1-9] різними авторами розглядається використання уразливостей в початкових кодах для здійснення атак, а також методи та засоби виявлення цих уразливостей чи запобігання їх появі. Наведені у цих роботах декілька варіантів класифікацій уразливостей не охоплюють широкого спектра ознак і не характеризуються системним узагальнюючим підходом, що можна було б використати при розв'язанні зазначеної проблеми. Крім того, деякі класифікації дещо звужені, наприклад, до таких об'єктів, як операційні системи (класифікація уразливостей Т. Аслама (T. Aslam) в операційній системі Unix [4]). Найновіший структурований підхід до класифікації уразливостей [5] полягає у тому, що уразливості як об'єкти мають властивості (початковий код, компоненти ПЗ, версію програми, проломи, властивості експлойту та ін.) – атрибути (некоректна довжина, вплив, наслідки, розташування коду експлойту тощо) із певним значенням. Класифікація здійснюється шляхом призначення уразливості набору атрибутів із конкретними значеннями. В результаті різні уразливості мають відмінний набір ознак. Такий підхід нагадує більше