УДК 004.056.55

О СЕТЯХ PES16–4, PES16–2 И PES16–1, СОЗДАННЫХ НА ОСНОВЕ СЕТИ PES16–8

Гулом Туйчиев

В статье на основе сети PES16–8 разработаны сети PES16–4, PES16–2 и PES16–1 состоящие из четырех, двух и одной раундовых функций. Основное преимущество предложенных сетей в том, что при зашифровании и расшифровании используется один и тот же алгоритм, а также в качестве раундовых функций можно использовать любые преобразования. В разработанных сетях длина подблоков равна 8, 16 и 32 битам и на основе этой сети можно создать алгоритм шифрования длиной блока 128, 256 и 512 битам. Кроме этого, алгебраические операции являются переменными, в качестве этих операции можно использовать операции сложения и умножения по модулю и XOR.

Ключевые слова: *сеть Фейстеля, схема Лай–Мэсси, раундовая функция, зашифрование, расшифрование, мультипликативная инверсия, аддитивная инверсия.*

Введение. Преимуществом сети Фейстеля является то, что при зашифрования и расшифровании используется один и тот же алгоритм и в качестве раундовой функции можно использовать любые преобразования. В алгоритмах шифрования PES [16], IDEA [17] при зашифрования и расшифровании используется один и тот же алгоритм, но раундовая функция не используется, вместо него применены МА преобразования. В работе [1–8] авторами на основе структуры алгоритма шифрования PES, IDEA разработаны сети под названием PES4–2, IDEA4–2, PES8–4, IDEA8–4, PES16–8, IDEA16–8, IDEA32–16, PES32–16, состоящие из двух, четырех, восьми и шестнадцати раундовых функций. В разработанных сетях при зашифрования и расшифровании используется один и тот же алгоритм и в качестве раундовой функции можно использовать любые преобразования.

В сетях [1–8] раундовые функции имеют по одному входному и выходному блоку. Функции, имеющие один входной и выходной блок, дают ограничения в разработке блочных алгоритмов шифрования. Кроме этого, в блочных шифрах применяются раундовые функции, имеющие несколько входных и выходных блоков.

Кроме этого, на основе сети IDEA8–4 разработаны:

– сеть IDEA8–2, состоящая из двух раундовых функции, в которой раундовые функции имеют по два входных и выходных блоков,

– сеть IDEA8–1, состоящая из одной раундовой функции, в которой раундовая функция имеет по четыре входных и выходных блоков,

– сеть RFWKIDEA8–4 (round function without key IDEA8–4), т.е., раундовые функции примененные без ключа сеть IDEA8–4, состоящая из четырех раундовых функции, в которой раундовые функции имеют по одному входному и выходному блоку,

– сеть RFWKIDEA8–2, состоящая из двух раундовых функций, в которой раундовые функции имеют по два входных и выходных блоков,

– сеть RFWKIDEA8–1, состоящая из одной раундовой функции, в которой раундовые функции имеют по четыре входных и выходных блоков [9].

Аналогичным образом, на основе сети IDEA16–8 разработаны:

– сеть IDEA16–4, состоящая из четырех раундовых функции, в которой раундовые функции имеют по два входных и выходных блоков,

– сеть IDEA16–2, состоящая из двух раундовых функции, в которой раундовые функции имеют по четыре входных и выходных блоков,

– сеть IDEA16–1, состоящая из одной раундовой функции, в которой раундовые функции имеют по восемь входных и выходных блоков [10].

Таким же образом, на основе сети IDEA32–16 разработаны сети IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, на основе сети PES8–4 разработаны сети PES8–2, PES8–1, RFWKPES8–4, RFWKPES8–2, RFWKPES8–1 и на основе сети PES32–16 разработаны сети PES32–8, PES32–4, PES32–2, PES32–1, RFWKPES32–16, RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1 [11-15].

В этой статье на основе сети PES16–8 разработаны:

– сеть PES16–4, состоящая из четырех раундовых функции, в которой раундовые функции имеют по два входных и выходных блоков,

– сеть PES16–2, состоящая из двух раундовых функции, в которой раундовые функции имеют по четыре входных и выходных блоков,

– сеть PES16–1, состоящая из одной раундовой функции, в которой раундовая функция имеет по восемь входных и выходных блоков.

Структура сети PES16–4. В сети PES32– 8 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей $K_{20(i-1)}$, $K_{20(i-1)+1}$, …, $K_{20(i-1)+15}$, $i=\overline{1...n+1}$, равна 32 (16, 8) битам. Длина раундовых ключей $K_{20(i-1)+16}$, $K_{20(i-1)+17}$, $K_{20(i-1)+18}$, $K_{20(i-1)+19}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Раундовые функции F_0, F_1, F_2, F_3 имеют по два входных и выходных блоков, длина которых равна 32 (16, 8) битам. Схема n-раундовой сети PES16–4 приведена на рис. 1, а процесс зашифрования приведен в (1) формуле.

$$\begin{cases} X_i^0 = (X_{i-1}^8(z_1)K_{20(i-1)+8}) \oplus Y_7 \\ X_i^1 = (X_{i-1}^9(z_1)K_{20(i-1)+9}) \oplus Y_6 \\ X_i^2 = (X_{i-1}^{10}(z_1)K_{20(i-1)+10}) \oplus Y_5 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^7 = (X_{i-1}^{15}(z_1)K_{20(i-1)+15}) \oplus Y_0 \\ X_i^8 = (X_{i-1}^0(z_0)K_{20(i-1)}) \oplus Y_7 \\ X_i^9 = (X_{i-1}^1(z_0)K_{20(i-1)+1}) \oplus Y_6 \\ X_i^{10} = (X_{i-1}^2(z_0)K_{20(i-1)+2}) \oplus Y_5 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{15} = (X_{i-1}^7(z_0)K_{20(i-1)+7}) \oplus Y_0 \end{cases}, \; i=\overline{1...n} \tag{1}$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{20n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{20n+1}) \\ X_{n+1}^2 = (X_n^2(z_0)K_{20n+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^7 = (X_n^7(z_0)K_{20n+7}) \\ X_{n+1}^8 = (X_n^8(z_1)K_{20n+8}) \\ X_{n+1}^9 = (X_n^9(z_1)K_{20n+9}) \\ X_{n+1}^{10} = (X_n^{10}(z_1)K_{20n+10}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{15} = (X_n^{15}(z_0)K_{20n+15}) \end{cases}, \textit{ в выходном преобразовании.}$$

Если в качестве входного блока положим $T0=[T^0,T^1]$, $T1=[T^2,T^3]$, $T2=[T^4,T^5]$, $T3=[T^6,T^7]$, и в качестве выходного блока раундовой функции берём $Y0=[Y^0,Y^1]$, $Y1=[Y^2,Y^3]$, $Y2=[Y^4,Y^5]$, $Y3=[Y^6,Y^7]$, то раундовую функцию можно представить в виде $Y0=F_0(T0,K_{20(i-1)+16})$, $Y1=F_1(T1,K_{20(i-1)+17})$, $Y2=F_2(T2,K_{20(i-1)+18})$, $Y3=F_3(T3_i,K_{20(i-1)+19})$. Здесь $T^j=(X_{i-1}^j(z_j)K_{20(i-1)+j})\oplus(X_{i-1}^{8+j}(z_{7-j})K_{20(i-1)+8+j})$, $j=\overline{0...7}$ – входные блоки раундовых функций и Y^j, $j=\overline{0...7}$ – выходные блоки раундовых функций.

Для корректности процесса зашифрования раундовую функцию $Y0=F_0(T0,K_{20(i-1)+16})$ представим в виде $Y^0=F_0^0(T^0,T^1,K_{20(i-1)+16})$, $Y^1=F_0^1(T^0,T^1,K_{20(i-1)+16})$, а раундовую функцию $Y1=F_1(T1,K_{20(i-1)+17})$ представим в виде $Y^2=F_1^0(T^2,T^3,K_{20(i-1)+17})$, $Y^3=F_1^1(T^2,T^3,K_{20(i-1)+17})$ и так далее, раундовую функцию $Y3=F_3(T3,K_{20(i-1)+19})$ представим в виде $Y^6=F_3^0(T^6,T^7,K_{20(i-1)+19})$, $Y^7=F_3^1(T^6,T^7,K_{20(i-1)+19})$.

На рис. 1 и (1) формуле в качестве операции z_0, z_1 можно выбрать операции $\otimes$ (mul), $\boxplus$ (add) и $\oplus$ (xor). Здесь $\otimes$-операция умножения целых чисел по модулю $2^{32}+1$ ($2^{16}+1$, 2^8+1), когда 32 (16, 8) – битный подблок рассматривается в качестве обычного представления целого числа по основанию два за исключением того, что подблок из всех нулей полагается равным $2^{32}+1$ ($2^{16}+1$, 2^8+1), $\boxplus$-операция сложение целых чисел по модулю 2^{32} (2^{16}, 2^8), когда 32 (16, 8) – битный рассматривается в качестве обычного представления целого числа по основанию два и $\oplus$ – операция суммирования по XOR 32 (16, 8) битных подблоков.

Генерация ключей сети PES16–4. В n-раундовой сети PES16–4 в каждом раунде применяются 20 раундовых ключей и в выходном преобразовании 16 раундовых ключей, т.е., число всех ключей равно $20n+16$. При зашифровании из ключа K генерируются $20n+16$ раундовые ключи зашифрования K_i^c. А раундовые ключи расшифрования K_i^d вычисляются на основе K_i^c.

При зашифровании вместо раундовых ключей K_i^d применяются раундовые ключи K_i^c, а при расшифровании раундовые ключи K_i^d, т.е., при зашифровании и расшифровании используется один и тот же алгоритм, меняются только раундовые ключи.

В сети PES16–4 раундовые ключи расшифрования выходного преобразования связаны с ключами зашифрования по формуле (2).

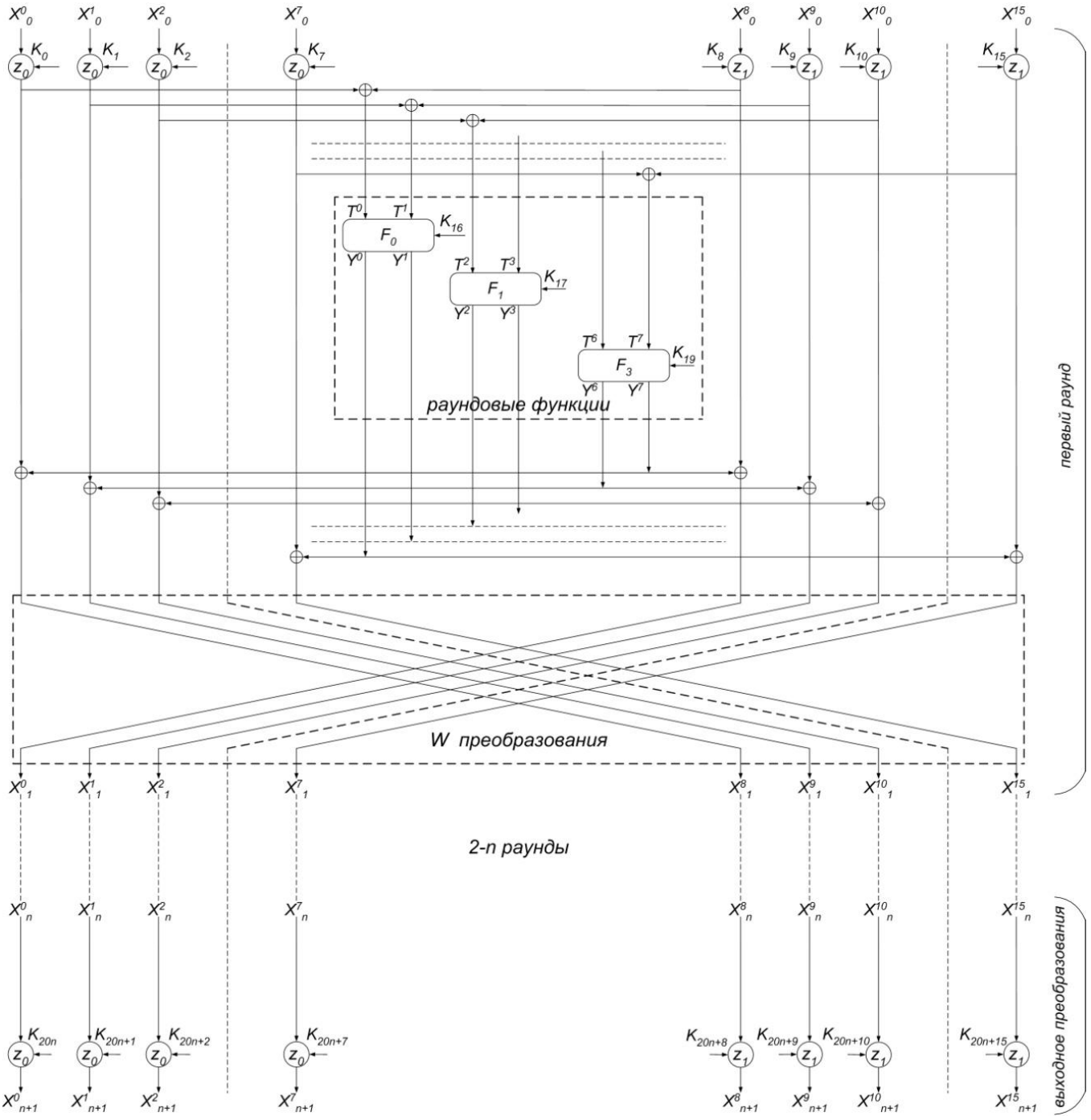

Рис. 1. Схема *n*-раундовой сети PES16–4

$$(K^d_{20n}, K^d_{20n+1}, K^d_{20n+2}, K^d_{20n+3}, K^d_{20n+4}, K^d_{20n+5}, K^d_{20n+6}, K^d_{20n+7}, K^d_{20n+8}, K^d_{20n+9}, K^d_{20n+10}, K^d_{20n+11},$$
$$K^d_{20n+12}, K^d_{20n+13}, K^d_{20n+14}, K^d_{20n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, (K^c_3)^{z_0}, (K^c_4)^{z_0}, (K^c_5)^{z_0}, (K^c_6)^{z_0}, \quad (2)$$
$$(K^c_7)^{z_0}, (K^c_8)^{z_1}, (K^c_9)^{z_1}, (K^c_{10})^{z_1}, (K^c_{11})^{z_1}, (K^c_{12})^{z_1}, (K^c_{13})^{z_1}, (K^c_{14})^{z_1}, (K^c_{15})^{z_1}).$$

Если в качестве операции z_0, z_1 применяется операция mul, тогда $K = (K)^{-1}$, если применяется операция add, тогда $K = -K$ и если применяется операция xor, тогда $K = K$. Здесь K^{-1} – мультипликативная инверсия K по модулю $2^{32}+1$ $(2^{16}+1, 2^8+1)$, $-K$ – аддитивная инверсия K по модулю 2^{32} $(2^{16}, 2^8)$. Для 32, 16 и 8 битных чисел выполняются $K \otimes K^{-1} = 1 \bmod(2^{32}+1)$, $K \otimes K^{-1} = 1 \bmod(2^{16}+1)$, $K \otimes K^{-1} = 1 \bmod(2^8+1)$ и $-K \boxplus K = 0$, $K \oplus K = 0$.

Таким же образом, раундовые ключи расшифрования первого, второго, и $n-$раунда связаны с раундовыми ключами зашифрования по формуле (3).

$$
\begin{aligned}
&(K^d_{20(i-1)}, K^d_{20(i-1)+1}, K^d_{20(i-1)+2}, K^d_{20(i-1)+3}, K^d_{20(i-1)+4}, K^d_{20(i-1)+5}, K^d_{20(i-1)+6}, K^d_{20(i-1)+7}, K^d_{20(i-1)+8},\\
&K^d_{20(i-1)+9}, K^d_{20(i-1)+10}, K^d_{20(i-1)+11}, K^d_{20(i-1)+12}, K^d_{20(i-1)+13}, K^d_{20(i-1)+14}, K^d_{20(i-1)+15}, K^d_{20(i-1)+16},\\
&K^d_{20(i-1)+17}, K^d_{20(i-1)+18}, K^d_{20(i-1)+19}) = ((K^c_{20(n-i+1)})^{z_0}, (K^c_{20(n-i+1)+1})^{z_0}, (K^c_{20(n-i+1)+2})^{z_0},\\
&(K^c_{20(n-i+1)+3})^{z_0}, (K^c_{20(n-i+1)+4})^{z_0}, (K^c_{20(n-i+1)+5})^{z_0}, (K^c_{20(n-i+1)+6})^{z_0}, (K^c_{20(n-i+1)+7})^{z_0}, (K^c_{20(n-i+1)+8})^{z_1},\\
&(K^c_{20(n-i+1)+9})^{z_1}, (K^c_{20(n-i+1)+10})^{z_1}, (K^c_{20(n-i+1)+11})^{z_1}, (K^c_{20(n-i+1)+12})^{z_1}, (K^c_{20(n-i+1)+13})^{z_1},\\
&(K^c_{20(n-i+1)+14})^{z_1}, (K^c_{20(n-i+1)+15})^{z_1}, K^c_{20(n-i)+16}, K^c_{20(n-i)+17}, K^c_{20(n-i)+18}, K^c_{20(n-i)+19}),\ i = \overline{1...n}.
\end{aligned}
\tag{3}
$$

Как видно из формулы (2) при расшифровании ключи зашифрования применяются в обратном порядке, только требуется вычисление инверсии в соответствии операции z_0, z_1. При зашифровании в первом раунде ключи зашифрования K_0^c, K_1^c, …, K_0^{16} на подблоки применяются по операции z_0, z_1, то при расшифровании в выходном преобразовании требуется вычисление инверсии по операции z_0, z_1, т.е. $K^d_{20n} = (K^c_0)^{z_0}$, $K^d_{20n+1} = (K^c_1)^{z_0}$, ..., $K^d_{20n+15} = (K^c_{15})^{z_1}$.

В сети PES16–4 раундовые функции имеют два входа и два выхода. Таким же образом, на основе сети PES16–8 можно построить сети, в которых раундовые функции имеют по четыре входных и выходных блока, по восемь входных и выходных блоков. Сеть, состоящая из двух раундовых функций, в которой раундовые функции имеют по четыре входных и выходных блоков называется PES16–2. Аналогично, сеть, состоящая из одной раундовой функций, в которой раундовые функции имеют по восемь входных и выходных блоков называется PES16–1.

Структура сети PES16–2. В сети PES16–2 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей $K_{18(i-1)}$, $K_{18(i-1)+1}$, …, $K_{18(i-1)+15}$, $i = \overline{1...n+1}$, равна 32 (16, 8) битам. Длина раундовых ключей $K_{18(i-1)+16}$, $K_{18(i-1)+17}$, $i = \overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Раундовые функции F_0, F_1 имеют по четыре входных и выходных блоков, длина которых равна 32 (16, 8) битам. Схемы раундовых функций i - раунда сети PES16–2 приведены на Рис. 2, а процесс зашифрования приведен в (4) формуле.

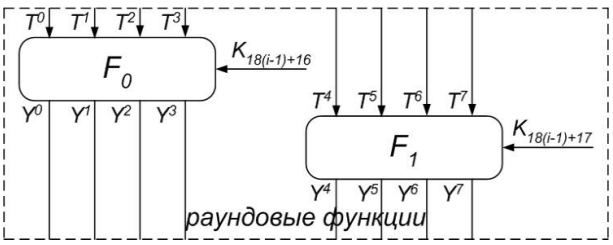

Рис. 2. Схема раундовых функций i – раунда сети PES16–2

Если в сети PES16–2 $T0 = [T^0, T^1, T^2, T^3]$, $T1 = [T^4, T^5, T^6, T^7]$ – входной блок, $Y0 = [Y^0, Y^1, Y^2, Y^3]$, $Y1 = [Y^4, Y^5, Y^6, Y^7]$ – выходной блок раундовых функции, то раундовую функцию можно представить в виде $Y0 = F_0(T0, K_{18(i-1)+16})$, $Y1 = F_1(T1, K_{18(i-1)+17})$, здесь $T^j = (X^j_{i-1}(z_j)K_{18(i-1)+j}) \oplus (X^{8+j}_{i-1}(z_{7-j})K_{18(i-1)+8+j})$, $j = \overline{0...7}$. Для корректности процесса зашифрования раундовую функцию $Y0 = F_0(T0, K_{18(i-1)+16})$ представим в виде $Y^0 = F_0^0(T^0, T^1, T^2, T^3, K_{18(i-1)+16})$, $Y^0 = F_0^1(T^0, T^1, T^2, T^3, K_{18(i-1)+16})$, ..., $Y^3 = F_0^3(T^0, T^1, T^2, T^3, K_{18(i-1)+16})$, раундовую функцию $Y1 = F_1(T1, K_{18(i-1)+17})$ представим в виде $Y^4 = F_1^0(T^4, T^5, T^6, T^7, K_{18(i-1)+17})$, $Y^5 = F_1^1(T^4, T^5, T^6, T^7, K_{18(i-1)+17})$, ..., $Y^7 = F_1^3(T^4, T^5, T^6, T^7, K_{18(i-1)+17})$.

$$
\begin{cases}
X^0_i = (X^8_{i-1}(z_1)K_{18(i-1)+8}) \oplus Y_7\\
X^1_i = (X^9_{i-1}(z_1)K_{18(i-1)+9}) \oplus Y_6\\
X^2_i = (X^{10}_{i-1}(z_1)K_{18(i-1)+10}) \oplus Y_5\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X^7_i = (X^{15}_{i-1}(z_1)K_{18(i-1)+15}) \oplus Y_0\\
X^8_i = (X^0_{i-1}(z_0)K_{18(i-1)}) \oplus Y_7\\
X^9_i = (X^1_{i-1}(z_0)K_{18(i-1)+1}) \oplus Y_6\\
X^{10}_i = (X^2_{i-1}(z_0)K_{18(i-1)+2}) \oplus Y_5\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X^{15}_i = (X^7_{i-1}(z_0)K_{18(i-1)+7}) \oplus Y_0
\end{cases},\ i = \overline{1...n}
\tag{4}
$$

$$
\begin{cases}
X^0_{n+1} = (X^0_n(z_0)K_{18n})\\
X^1_{n+1} = (X^1_n(z_0)K_{18n+1})\\
X^2_{n+1} = (X^2_n(z_0)K_{18n+2})\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X^7_{n+1} = (X^7_n(z_0)K_{18n+7})\\
X^8_{n+1} = (X^8_n(z_1)K_{18n+8})\\
X^9_{n+1} = (X^9_n(z_1)K_{18n+9})\\
X^{10}_{n+1} = (X^{10}_n(z_1)K_{18n+10})\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X^{15}_{n+1} = (X^{15}_n(z_0)K_{18n+15})
\end{cases},\ \textit{в выходном преобразовании.}
$$

Генерация ключей сети PES16–2. В n – раундовой сети PES16–2 в каждом раунде применяются 18 раундовых ключей и в выходном преобразовании 16 раундовых ключей, т.е., число всех ключей равно $18n+16$. Ключи расшифрования сетей вычисляются аналогично сети PES16–4, только в сети PES16–2 вместо индекса ключа 20 ставится 18.

Раундовые ключи расшифрования первого, второго, и n-раунда сети PES32–2 связаны с раундовыми ключами зашифрования по формуле (5).

Раундовые ключи расшифрования выходного преобразования связаны с раундовыми ключами зашифрования по формуле (6).

$$\begin{aligned}&(K^d_{18(i-1)}, K^d_{18(i-1)+1}, K^d_{18(i-1)+2}, K^d_{18(i-1)+3}, K^d_{18(i-1)+4}, K^d_{18(i-1)+5}, K^d_{18(i-1)+6}, K^d_{18(i-1)+7}, K^d_{18(i-1)+8},\\ &K^d_{18(i-1)+9}, K^d_{18(i-1)+10}, K^d_{18(i-1)+11}, K^d_{18(i-1)+12}, K^d_{18(i-1)+13}, K^d_{18(i-1)+14}, K^d_{18(i-1)+15}, K^d_{18(i-1)+16},\\ &K^d_{18(i-1)+17}) = ((K^c_{18(n-i+1)})^{z_0}, (K^c_{18(n-i+1)+1})^{z_0}, (K^c_{18(n-i+1)+2})^{z_0}, (K^c_{18(n-i+1)+3})^{z_0}, (K^c_{18(n-i+1)+4})^{z_0},\\ &(K^c_{18(n-i+1)+5})^{z_0}, (K^c_{18(n-i+1)+6})^{z_0}, (K^c_{18(n-i+1)+7})^{z_0}, (K^c_{18(n-i+1)+8})^{z_1}, (K^c_{18(n-i+1)+9})^{z_1}, (K^c_{18(n-i+1)+10})^{z_1},\\ &(K^c_{18(n-i+1)+11})^{z_1}, (K^c_{18(n-i+1)+12})^{z_1}, (K^c_{18(n-i+1)+13})^{z_1}, (K^c_{18(n-i+1)+14})^{z_1}, (K^c_{18(n-i+1)+15})^{z_1},\\ &K^c_{18(n-i)+16}, K^c_{18(n-i)+17}),\ i=\overline{1...n}.\end{aligned} \tag{5}$$

$$\begin{aligned}&(K^d_{18n}, K^d_{18n+1}, K^d_{18n+2}, K^d_{18n+3}, K^d_{18n+4}, K^d_{18n+5}, K^d_{18n+6}, K^d_{18n+7}, K^d_{18n+8}, K^d_{18n+9}, K^d_{18n+10}, K^d_{18n+11},\\ &K^d_{18n+12}, K^{\mathrm{d}}_{18n+13}, K^d_{18n+14}, K^d_{18n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, (K^c_3)^{z_0}, (K^c_4)^{z_0}, (K^c_5)^{z_0}, (K^c_6)^{z_0},\\ &(K^c_7)^{z_0}, (K^c_8)^{z_1}, (K^c_9)^{z_1}, (K^c_{10})^{z_1}, (K^c_{11})^{z_1}, (K^c_{12})^{z_1}, (K^c_{13})^{z_1}, (K^c_{14})^{z_1}, (K^c_{15})^{z_1}).\end{aligned} \tag{6}$$

Структура сети PES16–1. В сети PES16–1 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей $K_{17(i-1)}$, $K_{17(i-1)+1}$, …, $K_{17(i-1)+15}$, $i=\overline{1...n+1}$, равна 32 (16, 8) бит. Длина раундового ключа $K_{17(i-1)+16}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Раундовая функция F имеет восемь входных и выходных блоков, длина которых равна 32 (16, 8) битам. Схемы раундовых функций i – раунда сети PES16–1 приведены на Рис. 3, а процесс зашифрования приведен в (7) формуле.

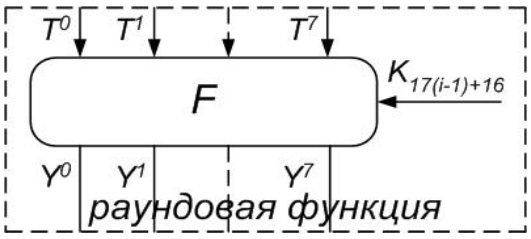

Рис. 3. Схема раундовых функций i – раунда сети PES16–1

Если в сети PES16–1 $T0=[T^0,T^1,T^2,...,T^7]$ – входной блок и $Y0=[Y^0,Y^1,Y^2,...,Y^7]$ – выходной блок раундовой функции, то раундовую функцию можно представить в виде $Y0=F(T0,K_{17(i-1)+16})$, здесь $T^j=(X^j_{i-1}(z_j)K_{17(i-1)+j})\oplus(X^{8+j}_{i-1}(z_{7-j})K_{17(i-1)+16+j})$, $j=\overline{0...7}$. Для корректности процесса зашифрования, раундовую функцию $Y0=F(T0,K_{17(i-1)+16})$ представим в виде

$$Y^0=F^0(T^0,T^1,...,T^7,K_{17(i-1)+16}),$$
$$Y^1=F^1(T^0,T^1,...,T^7,K_{17(i-1)+16}),...,$$
$$Y^7=F^7(T^0,T^1,...,T^7,K_{17(i-1)+16}).$$

В сетях PES16–4, PES16–2, PES16–1 в качестве F_i^j выбран выходной $j+1$ блок раундовой функции F_i.

$$\begin{cases}X^0_i=(X^8_{i-1}(z_1)K_{17(i-1)+8})\oplus Y_7\\ X^1_i=(X^9_{i-1}(z_1)K_{17(i-1)+9})\oplus Y_6\\ X^2_i=(X^{10}_{i-1}(z_1)K_{17(i-1)+10})\oplus Y_5\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^7_i=(X^{15}_{i-1}(z_1)K_{17(i-1)+15})\oplus Y_0\\ X^8_i=(X^0_{i-1}(z_0)K_{17(i-1)})\oplus Y_7\\ X^9_i=(X^1_{i-1}(z_0)K_{17(i-1)+1})\oplus Y_6\\ X^{10}_i=(X^2_{i-1}(z_0)K_{17(i-1)+2})\oplus Y_5\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^{15}_i=(X^7_{i-1}(z_0)K_{17(i-1)+7})\oplus Y_0\end{cases},\ i=\overline{1...n}$$

$$\begin{cases}X^0_{n+1}=(X^0_n(z_0)K_{17n})\\ X^1_{n+1}=(X^1_n(z_0)K_{17n+1})\\ X^2_{n+1}=(X^2_n(z_0)K_{17n+2})\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^7_{n+1}=(X^7_n(z_0)K_{17n+7})\\ X^8_{n+1}=(X^8_n(z_1)K_{17n+8})\\ X^9_{n+1}=(X^9_n(z_1)K_{17n+9})\\ X^{10}_{n+1}=(X^{10}_n(z_1)K_{17n+10})\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^{15}_{n+1}=(X^{15}_n(z_0)K_{17n+15})\end{cases},\ \textit{в выходном преобразовании.}$$

(7)

Генерация ключей сети PES16–1. В n -раундовой сети PES16–1 в каждом раунде применяются 17 раундовых ключей и в выходном преобразовании 16 раундовых ключей, т.е., число всех ключей равно $17n+16$. Ключи расшифрования сетей вычисляются аналогично сети PES16–4, только в сети PES16–1 вместо индекса ключа 20 ставится 17.

Раундовые ключи расшифрования первого, второго, и n -раунда сети PES32–1 связаны с раундовыми ключами зашифрования по формуле (8).

$$
\begin{aligned}
&(K^d_{17(i-1)}, K^d_{17(i-1)+1}, K^d_{17(i-1)+2}, K^d_{17(i-1)+3}, K^d_{17(i-1)+4}, K^d_{17(i-1)+5}, K^d_{17(i-1)+6}, K^d_{17(i-1)+7}, K^d_{17(i-1)+8},\\
&K^d_{17(i-1)+9}, K^d_{17(i-1)+10}, K^d_{17(i-1)+11}, K^d_{17(i-1)+12}, K^d_{17(i-1)+13}, K^d_{17(i-1)+14}, K^d_{17(i-1)+15}, K^d_{17(i-1)+16}) =\\
&((K^c_{17(n-i+1)})^{z_0}, (K^c_{17(n-i+1)+1})^{z_0}, (K^c_{17(n-i+1)+2})^{z_0}, (K^c_{17(n-i+1)+3})^{z_0}, (K^c_{17(n-i+1)+4})^{z_0}, (K^c_{17(n-i+1)+5})^{z_0},\\
&(K^c_{17(n-i+1)+6})^{z_0}, (K^c_{17(n-i+1)+7})^{z_0}, (K^c_{17(n-i+1)+8})^{z_1}, (K^c_{17(n-i+1)+9})^{z_1}, (K^c_{17(n-i+1)+10})^{z_1}, (K^c_{17(n-i+1)+11})^{z_1},\\
&(K^c_{17(n-i+1)+12})^{z_1}, (K^c_{17(n-i+1)+13})^{z_1}, (K^c_{17(n-i+1)+14})^{z_1}, (K^c_{17(n-i+1)+15})^{z_1}, K^c_{17(n-i)+16}),\ i=\overline{1...n}.
\end{aligned}
\tag{8}
$$

Раундовые ключи расшифрования выходного преобразования связаны с раундовыми ключами зашифрования по формуле (9).

$$
\begin{aligned}
&(K^d_{17n}, K^d_{17n+1}, K^d_{17n+2}, K^d_{17n+3}, K^d_{17n+4}, K^d_{17n+5}, K^d_{17n+6}, K^d_{17n+7}, K^d_{17n+8}, K^d_{17n+9}, K^d_{17n+10}, K^d_{17n+11},\\
&K^d_{17n+12}, K^{\mathrm{d}}_{17n+13}, K^d_{17n+14}, K^d_{17n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, (K^c_3)^{z_0}, (K^c_4)^{z_0}, (K^c_5)^{z_0}, (K^c_6)^{z_0},\\
&(K^c_7)^{z_0}, (K^c_8)^{z_1}, (K^c_9)^{z_1}, (K^c_{10})^{z_1}, (K^c_{11})^{z_1}, (K^c_{12})^{z_1}, (K^c_{13})^{z_1}, (K^c_{14})^{z_1}, (K^c_{15})^{z_1}).
\end{aligned}
\tag{9}
$$

Полученные результаты. На основе структуры сети PES16–8 разработаны сети PES16–4, PES16–2 и PES16–1, состоящие из четырех, двух и одной раундовых функций. Аналогично сети Фейстеля, в разработанных сетях при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовых функций можно выбрать любые преобразования, потому что при расшифровании нет необходимости вычисления обратных раундовых функций. Кроме этого, в разработанных сетях в качестве раундовых функций можно выбрать функции с двумя, четырьмя и восьмью входных и выходных блоков.

На основе приведенных сетей, при длине подблоков равной 32 битам, можно построить алгоритм зашифрования длиной блока 512 бит, при длине подблоков равных 16 битам, можно построить алгоритм зашифрования длиной блока 256 бит и при длине подблоков равных 8 битам, можно построить алгоритм шифрования длиной блока 128 бит. Если выбрать в качестве операций z_0, z_1 операции mul, add и xor, все возможные варианты данного выбора равны 3^2. Характеристика сетей приведена в табл. 1.

Заключение. Преимущество разработанных сетей состоит в том, что при зашифровании и расшифровании используется один и тот же алгоритм. Это даёт удобство при создании аппаратных и программно–аппаратных средств. Кроме этого, в качестве раундовых функций используя раундовые функции существующих алгоритмов шифрования, например алгоритмы шифрования основанные на сети Фейстеля, можно перевести эти алгоритмы на основе вышеприведенных сетей.

Таблица 1

Характеристика сетей

Сеть	Число раундовых ключей	Число раундовых функций	Число раундовых ключей, примененных в раундовых функциях
PES16–8	$24n+16$	8	8
PES16–4	$20n+16$	4	4
PES16–2	$18n+16$	2	2
PES16–1	$17n+16$	1	1

ЛІТЕРАТУРА

[1]. Арипов М.М., Туйчиев Г.Н. Сеть IDEA4–2, состоящая из двух раундовых функции // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2012, №4, с. 55–59.

[2]. Арипов М.М., Туйчиев Г.Н. Сеть PES8–4, состоящая из четырех раундовых функции // Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хоразми 2012», Том № II, – Ташкент, 2012, с. 16–19.

[3]. Туйчиев Г.Н. Сеть IDEA8–4, состоящая из четырех раундовых функции // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2013, №2, с. 55–59 б.

[4]. Туйчиев Г.Н. Сеть IDEA16–8, состоящая из восьми раундовых функции // Вестник ТашГТУ. – Ташкент, 2014, №1, с. 183–187 б.

[5]. Туйчиев Г.Н. Сеть IDEA32–16, состоящая из шестнадцати раундовых функции // Вестник НУУз. – Ташкент, 2013, №4, с. 57–61.

[6]. Туйчиев Г.Н. Сеть PES4–2, состоящая из двух раундовых функции // Проблемы информатики и энергетики, – Ташкент, 2013, №5–6, с. 17–111.
[7]. Туйчиев Г.Н. О сети PES16–8, состоящей из восьми раундовых функций // Защита информация. - Киев, 2014, №3, с. 318-322.
[8]. Туйчиев Г.Н. Сеть PES32–16, состоящая из шестнадцати раундовых функции // Безпека информации. – Киев, 2014, №1, с. 43-47.
[9]. Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанные на основе сети IDEA8–4 // Узбекский математический журнал. – Ташкент, 2014, №3, с. 104-118.
[10]. Туйчиев Г.Н. О сетях IDEA16–4, IDEA16–2, IDEA16–1, созданных на основе сети IDEA16–8 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». – Ташкент, 2014.
[11]. Туйчиев Г.Н. О сетях IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, созданных на основе сети IDEA32–16 // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2014, №2, с. 45–50.
[12]. Туйчиев Г.Н. О сетях PES8-2 и PES8-1, разработанные на основе сети PES8-4 // Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хоразми 2014». Том № II, – Ташкент, 2014, с. 28–32.
[13]. Туйчиев Г.Н. О сетях RFWKPES8-4, RFWKPES8-2, RFWKPES8-1, разработанные на основе сети PES8-4 // Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хоразми 2014». Том № II, – Ташкент, 2014, с. 32–36.
[14]. Туйчиев Г.Н. О сетях PES32–8, PES32–4, PES32–2 и PES32–1, созданных на основе сети PES32–16 // Безопасность информации. - Киев, 2014, Том 20, №2, стр. 164-168.
[15]. Туйчиев Г.Н. О сетях RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1, созданных на основе сети PES32–16 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». – Ташкент, 2014.
[16]. Lai X., Massey J.L. A proposal for a new block encryption standard // Advances in Cryptology – Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991, pp. 389–404.
[17]. Lai X., Massey J.L. On the design and security of block cipher // ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.

REFERENCES

[1]. Aripov M.M. Tuychiev G.N. The network IDEA4–2, consists from two round functions, Infocommunications: Networks–Technologies–Solutions., Tashkent, 2012, №4, pp. 55–59.
[2]. Aripov M.M. Tuychiev G.N. The network PES8–4, consists from four round functions, Materials of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–khorezmiy 2012». Volume № II, Tashkent, 2012, pp. 16–19.
[3]. Tuychiev G.N. The network IDEA8–4, consists from four round functions, Infocommunications: Networks–Technologies–Solutions., Tashkent. 2013, №2, pp. 55–59.
[4]. Tuychiev G.N. The network IDEA16–8, consisted of eight round functions, Acta TSTU, Tashkent, 2014, №1, pp. 183–187.
[5]. Tuychiev G.N. The network IDEA32–16, consists from sixteen round functions, Acta NUUz, Tashkent, 2013, №4. pp. 57–61.
[6]. Tuychiev G.N. The network PES4–2, consists from two round functions, Uzbek journal of the problems of informatics and energetics, Tashkent, 2013, №5–6, pp. 17–111.
[7]. Tuychiev G.N. About the network PES16–8, consisting of eight round function, Ukrainian Information Security Research Journal, 2014, № 3. pp. 318-322.
[8]. Tuychiev G.N. The network PES32–16, consisting of sixteen round functions, Ukrainian Scientific Journal of Information Security. 2014, vol. 20, issue 1, pp. 43–47.
[9]. Tuychiev G.N. About networks IDEA8–2, IDEA8–1 and RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, developed on the basis of network IDEA8–4, Uzbek mathematical journal, Tashkent, 2014, №3, pp. 104–118.
[10]. Tuychiev G.N. About networks IDEA16–4, IDEA16–2, IDEA16–1 created on the basis of network IDEA16–8, Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions», Tashkent, 2014.
[11]. Tuychiev G.N. About networks IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, created on the basis of network IDEA32–16, Infocommunications: Networks–Technologies–Solutions, Tashkent, 2014, №2, pp. 45–50.
[12]. Tuychiev G.N. About networks PES8–2 and PES8–1, developed on the basis of network PES8–4, Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012». Volume № 2,, Tashkent, 2014, pp. 28–32.
[13]. Tuychiev G.N. About networks RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, developed on the basis of network PES8–4, Transactions of the international scientific conference «Modern problems

of applied mathematics and information technologies–Al–Khorezmiy 2012». Volume № 2, Tashkent, 2014, pp. 32–36.
[14]. Tuychiev G.N. About networks PES32–8, PES32–4, PES32–2 and PES32–1, created on the basis of network PES32–16, Ukrainian Scientific Journal of Information Security. 2014, vol. 20, issue 2, p.164–168.
[15]. Tuychiev G.N. About networks RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 and RFWKPES32–1, created on the basis of network PES32–16, Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions», Tashkent, 2014.
[16]. Lai X., Massey J.L. A proposal for a new block encryption standard, Advances in Cryptology, Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991, pp. 389–404.
[17]. Lai X., Massey J.L. On the design and security of block cipher, ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.

ПРО МЕРЕЖІ PES16–4, PES16–2 І PES16–1, СТВОРЕНІ НА ОСНОВІ МЕРЕЖІ PES16–8

У статті на основі мережі PES16–8 розроблені мережі PES16–4, PES16–2 і PES16–1, які складаються з чотирьох, двох і однієї раундових функцій. Основна перевага запропонованих мереж в тому, що при зашифровані і розшифровані використовується один і той же алгоритм, а також як раундові функцій можна використовувати будь-які перетворення. В розроблених мережах довжина підблоков дорівнює 8, 16 і 32 бітам і на основі цієї мережі можна створити алгоритм шифрування довжиною блоку 128, 256 і 512 бітам. Крім цього, алгебраїчні операції є змінними, в якості цих операцій можна використовувати операції додавання і множення по модулю і XOR.

Ключові слова: мережа Фейстеля, схема Лай–Мессі, раундова функція, зашифрування, розшифрування, мультиплікативна інверсія, аддитивная інверсія.

ABOUT NETWORKS PES16–4, PES16–2 AND PES16–1, CREATED ON THE BASIS NETWORK PES16–8

In the paper on the basis of the network PES16–8 developed networks PES16–4, PES16–2 and PES16–1 consisting of four, two, and one round function. The main advantage of the proposed network that during encryption and decryption using the same algorithm as well as a round function can be any transformation. In the network PES16-8 length of subblock is 8, 16 and 32 bits and basis on the network can create the encryption algorithm a length of subblock 128, 256 and 512 bits. In a network PES16-8 algebraic operations are variable, as these operations can use the operations of addition and multiplication modulo and XOR.

Index terms: Feistel network, Lai–Massey scheme, round function, encryption, decryption, multiplicative inverse, additive inverse.

Туйчиев Гулом Нумонович, кандидат технических наук, преподаватель Национального университета Узбекистана.
E-mail: blasterjon@gmail.com.
Туйчіїв Гулом Нумович, кандидат технічних наук, викладач Національного університету Узбекистану.
Gulom Tuychiev, PhD, Associate Professor, National university of Uzbekistan.

УДК 004.056.53

РОЗШИРЕННЯ ЕКОНОМІКО-ВАРТІСНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНИХ РИЗИКІВ ЗА РАХУНОК ВИКОРИСТАННЯ СОЦІАЛЬНО-ПСИХОЛОГІЧНИХ ТИПІВ ЗЛОВМИСНИКА

Олександр Архипов, Андрій Скиба, Олена Хоріна

Розглядаються соціально-психологічні характеристики зловмисника та їх застосування з економіко-вартісними моделями з метою оцінювання інформаційних ризиків і оптимальних інвестицій в інформаційну безпеку. Для проведення адекватного оцінювання інформаційних ризиків та визначення оптимальних інвестицій у сферу захисту інформації існуючі економіко-вартісні моделі потребують розширення з урахуванням соціально-психологічних характеристик зловмисника, які істотно впливають на оцінювання ризиків. Сучасні методи оцінювання інформаційних ризиків, які спираються на існуючі нормативно-правові документи, не враховують соціально-психологічні характеристики зловмисників, що призводить до некоректного проведення оцінювання та зменшення точності отриманих оцінок. Запропоноване розширення економіко-вартісної моделі з урахуванням соціально-психологічних характеристик зловмисника дає можливість підвищити точність оцінок інформаційних ризиків та оптимізувати інвестиції в інформаційну без-