УДК 681.3.06

А.А. КУЗНЕЦОВ[1], И.В. МОСКОВЧЕНКО[2]

[1] *Харьковский университет Воздушных Сил им. И. Кожедуба, Украина*
[2] *Факультет военной подготовки НТУ «ХПІ», Украина*

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОВЕРШЕНСТВОВАНИЮ СИММЕТРИЧНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПЕРСПЕКТИВНОЙ СИСТЕМЫ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Предложена математическая модель нелинейных блоков замен, представлены вычислительные алгоритмы формирования нелинейных узлов для поточных и блочных криптоалгоритмов. Выработаны практические рекомендации по совершенствованию существующих и применяемых на Украине симметричных средств защиты информации, а также международных стандартизированных симметричных криптографических средств, рекомендуемых к использованию для защиты информации в информационно-телекоммуникационных системах критического применения.

Ключевые слова: *нелинейный узел замен, нелинейность, сбалансированность, автокорреляция, корреляционный иммунитет, критерий распространения.*

Введение

Обеспечение безопасности информации в современных информационно-телекоммуникационных системах критического применения возлагается на симметричные средства защиты информации [1 – 5]. Их построение основывается на развитом математическом аппарате булевой алгебры [8 – 11]. В то же время опыт практического использования существующих средств защиты информации показывает, что применяемые на практике системы не обеспечивают современных требований по безопасности информации. Это сопряжено, в первую очередь, с уязвимостью нелинейных узлов замен (блоков усложнения) существующих средств защиты информации к современным методам криптоанализа [6, 7]. Таким образом, актуальной задачей является разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения путем разработки новых подходов и способов построения нелинейных узлов замен с улучшенными свойствами.

Целью данной статьи является разработка метода построения нелинейных узлов замен с улучшенными свойствами, обоснование предложений по совершенствованию симметричных средств защиты информации.

1. Разработка математической модели нелинейных узлов замен для симметричных средств защиты информации

Нелинейные узлы замен блочных симметричных средств защиты информации могут быть представлены в виде устройства преобразования, реализуемого с помощью двух коммутаторов (рис. 1.). При этом один коммутатор преобразует набор из n бит $(a_1, a_2, ..., a_n)$ в одну цифру по основанию 2^n, другой коммутатор выполняет обратное преобразование, т.е. образует набор из n бит $(b_1, b_2, ..., b_n)$. Такое устройство потенциально может заменить любой входной набор данных $(a_1, a_2, ..., a_n)$ на любой выходной набор $(b_1, b_2, ..., b_n)$.

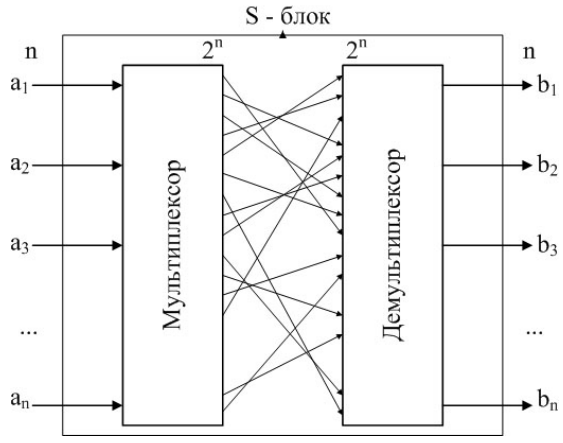

Рис. 1. Схема преобразования данных в нелинейном узле замены

Нелинейный узел замены (S - блок), схема преобразования данных в котором представлена на рис. 1, содержит 2^n внутренних состояний коммутаторов, которые могут быть выполнены $2^n!$ различными способами. Это означает, что существует $2^n!$ различных вариантов соответствующих таблиц замен. Формализуем процесс преобразования данных

в нелинейном узле замен с помощью математической модели, позволяющей описать его внутреннюю структуру.

Как видно из рис. 1, преобразования данных в нелинейном узле замен в общем случае процесс можно представить в виде некоторого отображения

$$\varphi : A \to B, \qquad (1)$$

где A – множество возможных наборов $(a_1,...,a_n)$ на входе; B – множество возможных наборов $(b_1,...,b_n)$ на выходе блока преобразования.

Свойства отображения (1) задаются внутренней структурой узла замены, т.е. набором конкретных коммутаций (соединений) выходов мультиплексора и входов демультиплексора.

Для формального аналитического описания внутренней структуры и оценки свойств нелинейного узла замен предлагается математическая модель, состоящая из следующих элементов:

1. Множество A входных векторов $a = (a_1,...,a_m)$, $a \in A$, где $a_i \in GF(2)$, $|A| = 2^m$.

2. Множество B выходных векторов $b = (b_1,...,b_m)$, $b \in B$, где $b_i \in GF(2)$, $|B| = 2^m$.

3. Конечное поле $GF(2^m)$ с арифметикой над кольцом многочленов по модулю произвольного неприводимого многочлена.

4. Множество нелинейных булевых функций $F = \{f_1, f_2,..., f_m\}$, представимых в алгебраической нормальной форме:

$$\begin{cases} f_1(x_1,...,x_m) = c_{1,0} \oplus \overset{m}{\underset{i=1}{\oplus}} c_{1,i}x_i \oplus \underset{1\le i<j\le m}{\oplus} c_{1,ij}x_ix_j \oplus ... \\ ... \oplus c_{1,12...m}x_1x_2...x_m; \\ f_2(x_1,...,x_m) = c_{2,0} \oplus \overset{m}{\underset{i=1}{\oplus}} c_{2,i}x_i \oplus \underset{1\le i<j\le m}{\oplus} c_{2,ij}x_ix_j \oplus ... \\ ... \oplus c_{2,12...m}x_1x_2...x_m; \\ ... \\ f_m(x_1,...,x_m) = c_{m,0} \oplus \overset{m}{\underset{i=1}{\oplus}} c_{m,i}x_i \oplus \underset{1\le i<j\le m}{\oplus} c_{m,ij}x_ix_j \oplus \\ ... \oplus c_{m,12...m}x_1x_2...x_m. \end{cases}$$

Система ограничений:

$$\begin{Bmatrix} Сб_f \\ N_f \ge N_{тр} \\ КИ_f(k_1) \\ КР_f(k_2) \\ AC_f \le AC_{тр} \end{Bmatrix}, \qquad (2)$$

где $Сб_f$ – требование сбалансированности функции f; N_f – значение нелинейности преобразующей функции f; $КИ_f(k_1)$ – степень корреляционного иммунитета преобразующей функции f; $КР_f(k_2)$ – степень критерия распространения преобразующей функции f; AC_f – значение автокорреляция преобразующей функции f; $N_{тр}$ – требуемое значение нелинейности; k_1 – требуемая степень корреляционного иммунитета; k_2 – требуемая степень критерия распространения; $AC_{тр}$ – требуемое значение автокорреляции.

Все функции из множества $F = \{f_1, f_2,..., f_m\}$ удовлетворяют системе ограничений (2).

Узлы замен в соответствии с предложенной моделью задаются значениями функций из множества $F = \{f_1, f_2,..., f_m\}$. Любая функция $\overline{f_\varsigma}(x_1,...,x_m)$, полученная линейной комбинацией функций из множества $F = \{f_1, f_2,..., f_m\}$:

$$\begin{aligned} &\bar{f}_\varsigma(x_1,x_2,...,x_m) = f_i(x_1,x_2,...,x_m) \oplus \\ &\oplus f_j(x_1,x_2,...,x_m) \oplus ... \oplus f_l(x_1,x_2,...,x_m), \\ &f_i(x_1,x_2,...,x_m), f_j(x_1,x_2,...,x_m), ... \\ &..., f_l(x_1,x_2,...,x_m) \in F \end{aligned},$$

удовлетворяет системе ограничений (2) с возможно другими граничными значениями.

Обозначим множество отличных от нуля нелинейных булевых функций $\overline{f_\varsigma}(x_1,x_2,...,x_m)$, $\varsigma = 1, 2, ..., 2^m - 1$:

$$\begin{cases} \bar{f}1(x_1,...,x_m) = f_1(x_1,x_2,...,x_m); \\ \bar{f}2(x_1,...,x_m) = f_2(x_1,x_2,...,x_m); \\ . \qquad .. \\ \bar{f}m(x_1,...,x_m) = f_m(x_1,x_2,...,x_m); \\ \bar{f}m{+}1(x_1,...,x_m) = f_1(x_1,...,x_m) \oplus f_2(x_1,...,x_m); \\ . \qquad .. \\ \bar{f}2^m{-}1(x_1,...,x_m) = f_1(x_1,x_2,...,x_m) \oplus \\ \oplus f_2(x_1,x_2,...,x_m) \oplus ... f_m(x_1,x_2,...,x_m). \end{cases}$$

Основные криптографические показатели нелинейного узла замен (сбалансированность Сб*, нелинейность N*, степень корреляционного иммунитета КИ*, степень критерия распространения КР* и значение автокорреляции АС*) по критерию минимального риска:

$$\begin{cases} Сб^* = Сб_{\bar{f}1} \wedge Сб_{\bar{f}2} \wedge ... \wedge Сб_{\bar{f}2^m-1}; \\ N^* = \min\left\{N_{\bar{f}1}, N_{\bar{f}2}, ..., N_{\bar{f}2^m-1}\right\}; \\ КИ^*(k) = \min\left\{КИ_{\bar{f}1}(k), КИ_{\bar{f}2}(k), ..., КИ_{\bar{f}2^m-1}(k)\right\}; \\ КР^*(k) = \min\left\{КР_{\bar{f}1}(k), КР_{\bar{f}2}(k), ..., КР_{\bar{f}2^m-1}(k)\right\}; \\ AC^* = \max\left\{AC_{\bar{f}1}, AC_{\bar{f}2}, ..., AC_{\bar{f}2^m-1}\right\}, \end{cases}$$

где $Сб_{\overline{f}_\varsigma}$ – показатель сбалансированности да/нет); $N_{\overline{f}_\varsigma}$ – показатель нелинейности; $КИ_{\overline{f}_\varsigma}(k)$ – степень корреляционного иммунитета; $КР_{\overline{f}_\varsigma}(k)$ – степень критерия распространения; $АС_{\overline{f}_\varsigma}$ – значение автокорреляции булевой функции $\overline{f_\varsigma}(x_1, x_2, ..., x_m)$.

Таким образом, предложенная математическая модель нелинейных узлов замен блочных симметричных средств защиты информации, на основе аналитического описания основных структурных компонентов, накладываемой системы ограничений по нелинейности, сбалансированности, корреляционному иммунитету, критерию распространения и автокорреляции, позволяет в терминах булевой алгебры описывать внутреннюю структуру нелинейных узла замен и оценивать основные показатели их эффективности.

2. Разработка алгоритмов формирования нелинейных узлов замен для симметричных средств защиты информации

Целью данной работы есть построение нелинейных узлов замен для симметричных поточных и блочных средств защиты информации. В соответствии с поставленной задачей разработаны алгоритмы формирования нелинейных узлов, представленные на рис. 2, 3.

Алгоритм формирования нелинейных узлов замен для поточных средств защиты информации представлен на рис. 2. После определения общесистемных параметров алгоритма (размерность векторного пространства и требуемая нелинейность узлов замен), в качестве исходных данных в алгоритме рассматриваются f бент-последовательностей, построенных над полем V_n, и количество требуемых попыток h. На основе размерности векторного пространства определяется число комплементаций k, которое необходимо выполнить, а также число комплементаций n^-/n^+, которые должны привести к понижению/повышению нелинейности искомых последовательностей, причем $k = n^+ + n^-$.

Далее осуществляется последовательное понижение нелинейности n^- раз, после чего осуществляется последовательное повышение нелинейности n^- раз. Повышение/понижение нелинейности осуществляется на основе использования метода прототипа (метода градиентного подъема). В случае, если повышение/понижение нелинейности является неосуществимым, делается следующая попытка, всего h раз. Если попытка увенчалась успехом, модифицированная бент-последовательность представляется как сбалансированная последовательность, обладающая требуемой нелинейностью, после чего осуществляется восстановление полиномиальной формы булевой функции.

Приведенная процедура осуществляется для всех искомых f бент-последовательностей. Выходными данными алгоритма являются f нелинейных булевых функций с требуемыми параметрами нелинейности, представленных в полиномиальной форме.

На рис. 3 представлен алгоритм формирования нелинейных узлов замен для блочных средств защиты информации, одной из составляющих которого является вышеприведенный алгоритм.

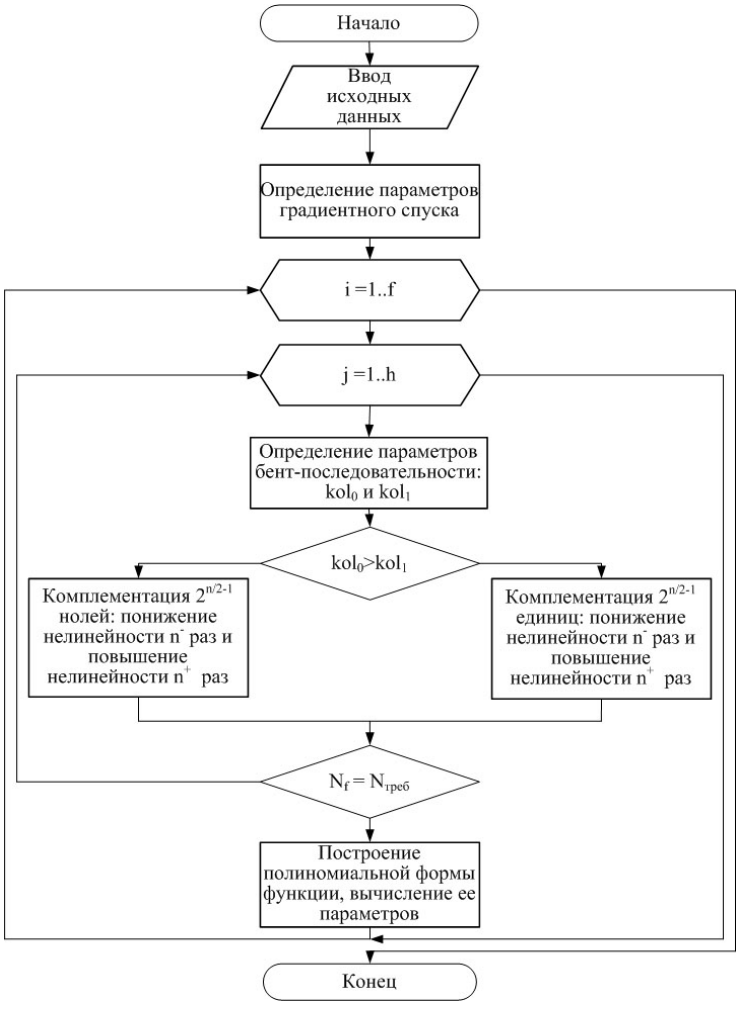

Рис. 2. Алгоритм формирования нелинейных узлов замен для поточных методов преобразования информации

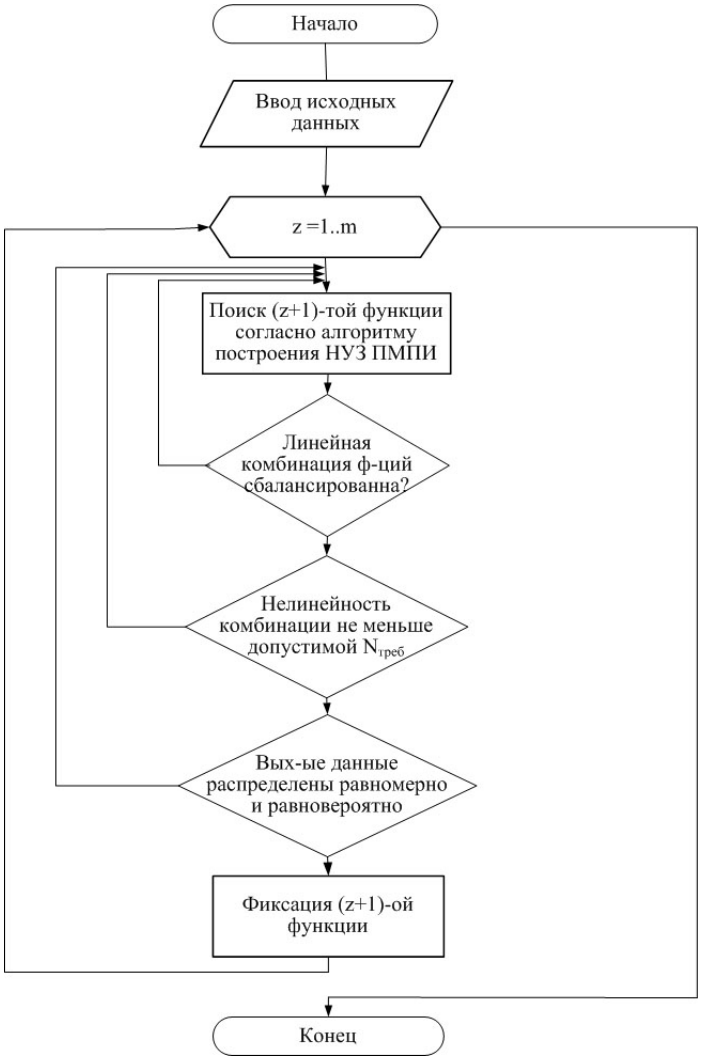

Рис. 3. Алгоритм формирования нелинейных узлов замен для блочных методов преобразования информации

Основной составляющей разработанного алгоритма формирования нелинейных узлов замен для блочных методов преобразования информации является представленный выше алгоритм формирования нелинейных узлов замен для поточных методов преобразования информации. В качестве исходных данных используются те же данные, а также требуемые размерность выходных данных (V_m) и $N_{треб}$.

Отправной точкой работы алгоритма является некоторая выбранная булева функция с требуемыми показателями стойкости. Далее в течение m – 1 итераций осуществляется поиск остальных (m–1) функций. Некоторая функция j, $j \le m$, фиксируется и считается отобранной для нелинейного узла замены, если выполняются следующие условия: 1) нелинейность j-й функции не меньше Nтреб; 2) любая линейная комбинация из найденных t функций, $t \le m$, является сбалансированной; 3) нелинейность любой линейной комбинации из найденных функций не меньше Nдопуст (опционально); 4) все возможные 2m выходные комбинации nвых от 2n входных комбинаций nвх являются равновероятно и равномерно распределенными между выходными комбинациями: nтр = nвх / nвых.

Выходными данными алгоритма являются m нелинейных булевых функций с требуемыми параметрами нелинейности, представленных в полиномиальной форме, а также их двоичные последовательности, непосредственно представляющие собой нелинейный узел замены для блочного метода преобразования информации.

В ходе проведенных исследований с использованием разработанного пакета программ сформированы 4 нелинейные булевы функции над V8, удовлетворяющие системе ограничений:

$$\left\{\begin{array}{c} \text{Сб}_f,\ N_f \ge 112,\ \text{КИ}_f(0), \\ \text{КР}_f(1),\ \text{АС}_f \le 24 \end{array}\right\}.$$

Любая функция $\overline{f_\varsigma}(x_1, x_2, ..., x_m)$, полученная линейной комбинацией функций $\{f_1, f_2, f_3, f_4\}$ также является сбалансированной и удовлетворяет системе ограничений:

$$\left\{\begin{array}{c} \text{Сб}_f,\ N_f \ge 110,\ \text{КИ}_f(0), \\ \text{КР}_f(1),\ \text{АС}_f \le 56 \end{array}\right\}.$$

Для построения блока нелинейных замен, реализующего отображение элементов из GF(28), дополнительно сформированы четыре булевы функции $\{f_5, f_6, f_7, f_8\}$ методом случайной генерации.

Нелинейные булевы функции аналитически задают узел замен, формализовано описывают его внутреннюю структуру и определяют основные показатели эффективности (4).

Представим входной вектор $a = (a_1, a_2, ..., a_8)$ в виде $a = (x, y)$, где

$$x = (a_1, a_2, a_3, a_4),\ y = (a_5, a_6, a_7, a_8).$$

Выходной вектор $b = (b_1, b_2, ..., b_8)$ представим в виде $b = (z, u)$, где

$$z = (b_1, b_2, b_3, b_4),\ u = (b_5, b_6, b_7, b_8).$$

Таблица замен сформированного нелинейного узла замен представлена в табл. 1, где каждая строка соответствует конкретному значению x, каждый столбец соответствует конкретному значению y, в ячейках таблицы указаны соответствующие значения z и u, а собственные значения x, y, z и u представлены в шестнадцатеричном формате.

Таблица 1

Таблица замен сформированного нелинейного узла

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	f0	4a	ed	f4	d1	db	bc	67	7d	f7	a0	fb	6c	d6	51	ba
	1	eb	7f	46	c3	aa	ef	e7	02	f6	72	ab	3e	37	52	3b	4e
	2	3f	15	ec	85	5a	a4	4d	66	03	39	30	b9	ca	78	91	0a
	3	54	11	e3	82	fd	f1	b6	13	48	2c	2b	6e	f9	ac	7b	2e
	4	5f	b5	f2	69	71	cb	4c	97	92	e8	ff	25	dc	96	79	ea
	5	14	60	99	0c	6a	be	d7	c2	89	6d	40	c1	bf	12	7a	ae
	6	70	c8	93	d8	ee	94	2d	a6	cc	76	6f	b4	e2	a8	81	3a
	7	6b	9f	58	3d	65	01	16	63	a7	53	64	41	09	1c	8a	ce
	8	a1	bb	cd	b3	08	da	ad	36	d2	88	9d	24	33	e9	1f	f5
	9	4b	af	e6	d3	2a	0e	b7	32	28	8c	95	c0	c9	5c	84	b0
	A	7e	d4	8d	26	2f	05	7c	07	3c	56	8f	d0	1d	df	8e	c5
	B	04	90	55	b2	45	31	86	5b	06	62	d5	10	27	a2	c4	50
	C	9e	74	43	68	b1	1a	dd	fe	bd	87	00	9b	f3	29	1e	75
	D	34	20	a9	18	9a	de	77	22	c7	73	38	cf	d9	fc	44	e0
	E	e1	1b	42	49	4f	a5	9c	47	23	19	80	0b	0d	57	5e	e5
	F	35	21	c6	a3	8b	0f	98	5d	17	83	e4	61	59	b8	fa	f8

Как следует из данных, приведенных в табл. 1, сформированный нелинейный узел замен реализует биективное отображение и может быть использован при построении криптографических средств защиты информации. Таблица замен и соответствующий нелинейный узел сформированы с использованием разработанного метода формирования криптографических булевых функций, его основные криптографические свойства соответствуют приведенной системе ограничений.

3. Обоснование предложений по совершенствованию симметричных средств защиты информации

Разработанный подход позволяет формировать блоки нелинейной подстановки, свойства которых не уступают лучшим известным мировым аналогам, а по некоторым показателям (нелинейность и автокорреляция) могут превосходить известные результаты. Таким образом, разработанный метод целесообразно использовать для совершенствования симметричных криптографических средств защиты информации.

На сегодняшний день в Украине действует стандарт блочного симметричного криптографического преобразования информации ГОСТ-28147-89, вместе с тем, в виду стремительного развития новейших информационных технологий, появления новых форм и способов обработки и передачи информации, алгоритм не удовлетворяет современным требованиям. Это относится, прежде всего, к следующим положениям.

1. Резкое увеличение объемов обрабатываемой и передаваемой информации в современных информационно-телекоммуникационных системах привело к повышению требований к быстродействию криптографических средств защиты информации. Алгоритм ГОСТ-28147-89 не удовлетворяет современным требованиям, сложность его реализации неприемлемо высока.

2. Размер блока современных симметричных криптоалгоритмов должен составлять не менее 128 бит с возможностью расширения до 256 и 512 бит. Размер блока алгоритма ГОСТ-28147-89 равен 64 битам, что не удовлетворяет современным требованиям в виду возможности осуществления тотального перебора всех блоков данных на современной вычислительной технике.

3. Одним из необходимых требований к современным алгоритмам шифрования является «прозрачность» используемого математического аппарата, отсутствие скрытых «лазеек». В то же время правила формирования блоков нелинейных замен (S-блоков) алгоритма ГОСТ-28147-89 являются государственной тайной Российской Федерации. Следовательно, использование произвольных S-блоков может привести к образованию скрытой «лазейки», чем могут воспользоваться соответствующие службы или злоумышленники. Закрытость математического аппарата и алгоритмов формирования S-блоков алгоритма ГОСТ-28147-89 является существенным ограничением на пути широкого практического использования в Украине.

4. Размер S-блоков современных симметричных блочных криптоалгоритмов доложен быть достаточным для устойчивости против алгебраических и других атак. Алгоритм ГОСТ-28147-89 построен по структуре цепи Файстеля (по примеру американского алгоритма шифрования DES) и оперирует сравнительно небольшими S-блоками, осуществляющими отображения 4-х битных слов в 4-х битные слова. Число возможных состояний (возможных вариантов подстановок) такого размера S-блока не превышает $2^n! = 2^4! = 20\,922\,789\ \ 888\,000 \approx 10^{13}$, что на сегодняшний день является неудовлетворительным по причине возможного полного перебора всех возможных состояний S-блока и слабой устойчивости к алгебраическим методам криптоанализа.

5. Одним из непременных требований к вновь разрабатываемым методам симметричного шифрования является математическое обоснование стойкости криптоалгоритма к наиболее известным видам атак, например к дифференциальному и линейному криптоанализу. С этой целью при обосновании стойкости шифра RijnDael, ставшим впоследствии национальным шифром США, использованы понятия ветвей рассеивания, дифференциального и ли-

нейного следов. Стандарт ГОСТ-28147-89 не содержит сведений о математической оценке стойкости и по причине использования перестановочных преобразований (вместо слоев линейного рассеивания как в RijnDael) не предполагает оценку стойкости по числу ветвей рассеивания и соответствующим методикам.

Таким образом, применяемый в Украине стандарт шифрования ГОСТ-28147-89 в современных условиях, на наш взгляд, нуждается в усовершенствовании или замене. По указанным выше причинам (п.4) разработка новых (с тем же размером) S-блоков для алгоритма ГОСТ-28147-89 также является нецелесообразной. Увеличение размерности блоков замен приведет к необходимости внесения значительных структурных изменений в сам алгоритм шифрования и пересмотру его криптографических свойств.

Одним из самых эффективных симметричных шифров на сегодняшний день является национальный алгоритм шифрования США FIPS-197 (AES). Он построен по структуре классического подстановочно-перестановочного шифра (по SPN структуре) и отвечает практически всем современным требованиям. Перечисленные выше недостатки ГОСТ-28147-89 не присущи алгоритму AES, кроме того, по своему быстродействию как в программной, так и в аппаратной реализации алгоритм шифрования FIPS-197(AES) является одним из наиболее эффективных. Единственным недостатком данного алгоритма, отмечаемым в последнее время, является относительная простота алгебраической структуры используемого нелинейного узла замен. Данный подход построения нелинейных узлов замен имеет следующие недостатки:

1. Функциональное преобразование, задающее нелинейное отображение и, непосредственно, сам вид таблицы замен не предполагает обсуждение таких показателей эффективности, как корреляционный иммунитет, степень критерия распространения, спектральные и корреляционные характеристики преобразующих функций.

2. Построение нелинейных узлов замен предполагает очень ограниченный диапазон возможных нетривиальных таблиц. При формировании таблицы замен вариативность может быть достигнута только посредством изменения неприводимого многочлена $m(x)$ и/или соответствующих значений констант, применяемых в алгоритме. В то же время, замена $m(x)$ приводит к взаимооднозначному функциональному соответствию элементов образованных конечных полей, т.е. к их изоморфизму. Изменение значений констант приведет к новой таблице замен, линейно эквивалентной исходной матрице.

3. По нашему мнению, алгебраическая структура нелинейных узлов замен может привести к появлению вычислительно эффективных криптоатак, основанных, например, на алгебраических методах криптоанализа.

Указанные конструктивные недостатки снижают научно-прикладное значение данного подхода. В соответствии со спецификацией AES разработчики алгоритма рассматривают возможность применения и других нелинейных подстановок.

Естественным развитием (модификацией) алгоритма AES является замена алгебраически сконструированных блоков замен на S-блоки, построенные с использованием математического аппарата булевой алгебры, например, с использованием предложенного в данной работе метода. Соответствующая таблица замен может быть представлена, например, в виде табл. 1, или любой другой таблицы, заполненной в соответствии с таблицей истинности комплементарных булевых функций, сформированных в соответствии с предложенным методом. При этом указанные выше недостатки алгебраически сконструированных нелинейных узлов замен AES будут устранены.

Выводы

В результате проведенных исследований выработаны практические рекомендации по совершенствованию существующих и применяемых на Украине симметричных средств защиты информации, а также международных стандартизированных симметричных криптографических средств, рекомендуемых к использованию для защиты информации в информационно-телекоммуникационных системах критического применения.

Показано, что усовершенствованные схемы за счет применения сформированных в соответствии с разработанным методом узлов нелинейных замен обеспечивают лучшие показатели безопасности.

Таким образом, в результате проведенных исследований подтверждена достоверность полученных результатов и обоснована целесообразность их практического использования.

Литература

1. Барсуков В.С. Технологии электронных коммуникаций: В 20 т. Т.20: Безопасность связи в каналах телекоммуникаций / В.С. Барсуков, С.В. Дворянкин, И.И. Шеремет. – М.: Электронные знания, 1992. – 122 с.

2. Береза А.С. Основы построения АСУ. Основы структурного анализа и синтеза АСУ / А.С. Береза. – Х.: ХВУ, 1997. – 210 с.

3. Береза А.С. Основы построения АСУ. Системотехнические основы построения АСУ / А.С. Береза. – Х.: ХВУ, 1996. – 355 с.

4. Захист інформації в комп'ютерних системах від несанкціонованого доступу / за ред. С.Г. Лаптєва. – К., 2001. – 321 с.

5. Мамаев Е. Технологии защиты информации в Интернете / Е. Мамаев. – СПб.: ИД Питер, 2001. − 848 с.

6. Потий А.В. Исследование методов криптоанализа поточных шифров / А.В. Потий, Ю.А. Избенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – ДСТСЗІ СБУ, НТУ "КПІ". – 2003. – № 6. – С. 34-49.

7. Система показателей оценки эффективности функционирования схем поточного шифрования / А.В. Потий, Ю.А. Избенко // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – 2003. – № 123. – С. 146-158.

8. Столлингс В. Компьютерные системы передачи данных / В. Столингс. – М.: Вильямс, 2002. – 928 с.

9. Шеннон К. Теория связи в секретных системах / К. Шеннон. – М.: Изд-во иностранной литературы, 1963. – С. 333-402.

10. Rueppel R.A. Analysis and Design of Stream Ciphers / R.A. Rueppel. – Berlin, Springer-Verlag, 1986.

11. Schneier B. Applied Cryptography. 2nd edition / B. Schneier. – New York: John Wiley & Sons, 1996.

Поступила в редакцию 10.06.2008

Рецензент: д-р техн. наук, с.н.с., ведущий научный сотрудник научного центра В.В. Баранник, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО УДОСКОНАЛЕННЯ СИМЕТРИЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПЕРСПЕКТИВНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ

О.О. Кузнецов, І.В. Московченко

Метою даної статті є розробка методу побудови нелінійних вузлів замін з поліпшеними властивостями, обґрунтування пропозицій щодо удосконалення симетричних засобів захисту інформації. Запропонована математична модель нелінійних вузлів замін для симетричних засобів захисту інформації. Представлені алгоритми формування нелінійних вузлів замін для потокових та блокових засобів захисту інформації. Відпрацьовані практичні рекомендації щодо удосконалення існуючих та користуємих симетричних засобів захисту інформації.

Ключові слова: нелінійних вузол замін, нелінійність, збалансованість, автокореляція, кореляційний імунітет, критерій розповсюдження.

DEVELOPMENT OF THE OFFERS ON IMPROVEMENT OF THE SYMMETRICAL MEANSES OF PROTECTION INFORMATION OF THE PERSPECTIVE SYSTEM OF THE CRITICAL USING

O.O. Kuznetsov, I.V. Moskovchenko

The purpose given article is a development of the method of the building of the nonlinear nodes of the change with perfected characteristic, motivation of the offers on improvement of the symmetrical meanses of protection information. The mathematical model of the nonlinear nodes of the change is offered for symmetrical meanses of protection information. The presented algorithms of the shaping the nonlinear nodes of the change for flow and block meanses of protection information. The practical recommendations will worked out on improvement existing and applicable symmetrical meanses of protection information.

Key words: nonlinear knot of replacements, non-linearity, balanced, autocorrelation, correlation immunity, criterion of distribution.

Кузнецов Александр Александрович – д-р техн. наук, старший научный сотрудник, начальник информационно-вычислительного центра Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина, e-mail: kuznetsov_alex@rambler.ru.

Московченко Илларион Валериевич – инженер кафедры боевого применения подразделений войск РХБ защиты подразделений гвардейского ордена Красной Звезды факультета военной подготовки имени Верховного Совета Украины Национального технического университета „Харьковский политехнический институт", Харьков, Украина, e-mail: larry_green@mail.ru.