показателями производительности формирования развернутого ключа и большой гибкостью при реализации на платформах с различной разрядностью.

Литература: ***1.*** *NESSIE Call for Cryptographic Primitives, Version 2.2, 8 March 2000: http://cryptonessie.org.* ***2.*** *L. R. Knudsen. Practically secure Feistel ciphers. In R. Anderson, editor, Fast Software Encryption 1993, Cambridge Security Workshop (FSE1), Volume 809 of Lecture Notes in Computer Science, pp. 211, 1994. Springer-Verlag.* ***3.*** *J. Kelsey, B.Schneier, D. Wgner "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and 3-DES" //CRYPTO'96, Springer-Verlag, 1996, pp. 237 – 251.* ***4.*** *Гловашич С. А., Горбенко И. Д. Алгоритм блочного симметричного шифрования «Торнадо». Спецификация преобразования. //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2003. Вып. 134. С.155–190.* ***5.*** *Иванов М. А. «Криптографические методы защиты информации в компьютерных системах и сетях». Москва «Кудиц-образ», 2001.– 363 с.* ***6.*** *Головашич С. А. Безопасность режимов блочного шифрования //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2001. Вып. 119. С.135–145.* ***7.*** *Лепеха А. Н. Алгоритм формирования псевдослучайной последовательности. //конференция «Актуальные проблемы и перспективы развития финансово-кредитной системы Украины», Харьков.– 2002.– с. 339.* ***8.*** *Лепеха А. Н., Головашич С. А. Статистический анализ БСШ «Торнадо» //Радиотехника: Всеукр межвед. науч.-техн. сб.– 2003. Вып. 134. С. 89 – 96.* ***9.*** *Потий А. В., Орлова С. Ю. и др. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS. //Радиотехника: Всеукр межвед. науч.-техн. сб. 2000. Вып. 114. С. 14.* ***10.*** *Фомичев В. М. «Дискретная математика и криптология». М.: «Диалог МИФИ», 2003.– 397 с.* ***11.*** *Philip Hawkes, Gregory Rose "Primitive Specification For SOBER-128" Qualcomm, Australia, 2003.* ***12.*** *R. Lorentzen, R. Nilsen "Application of linear programming to the optimal difference triangle set problem". IEEE Trans. Inform. Theory, vol IT-37, 1991, pp 1486-1488.*

УДК 681.3.06: 519.248.681

МЕТОДИКА ОЦЕНКИ ЭФЕКТИВНОСТИ ПОТОЧНЫХ ШИФРОВ

Светлана Орлова

Харьковский национальный университет радиоэлектроники

Анотація: **Наводиться удосконалена система критеріїв і показників ефективності функціонування схем потокового шифрування, яка дозволяє відібрати допустимі параметри шифру таким чином, щоб відповідати вимогам криптографічної стійкості, оптимальності та адаптивності. На основі цієї системи пропонується методика дослідження ефективності потокових шифрів, призначена безпосередньо для оцінювання нових та відомих шифрів і проведення їх порівняльного аналізу.**

Summary: **In this paper the improved system of criteria and metrics of operation efficiency of the stream encryption schemes, that allow to select valid parameters of the cipher so that to satisfy the requirement of cryptographic security, optimality and adaptivity is proposed. On the basis of this system the technique of research of efficiency of the stream ciphers intended directly for estimation of the new and known ciphers and for making the comparative analysis of their is offered.**

Ключові слова: **Потоковий шифр, оцінка ефективності, криптографічна стійкість.**

Введение

Стремительное развитие информационных технологий обуславливает необходимость применения систем защиты информации, обеспечивающих высокий уровень информационной безопасности наравне с высокой скоростью передачи данных по каналам связи. В основе таких систем используются поточные шифры (ПШ). Однако на сегодняшний день в этой области не существует стандартов, удовлетворяющих требованиям надёжности, ни в Украине, ни за рубежом. Это объясняется тем фактом, что большинство используемых на практике схем поточного шифрования либо запатентованы, либо конфиденциальны [1]. Однако опыт показывает, что засекречивание применяемых в системе алгоритмов не обеспечивает их практической стойкости. Так, например, согласно политике безопасности системы мобильной связи GSM [2], используемые алгоритмы долгое время были засекречены, однако это не помешало осуществлению многочисленных случаев её компрометации [3 – 5]. Единственная гарантия надёжности криптографических алгоритмов – это их открытость, которая позволяет широкой общественности изучать алгоритмы и находить в них слабые места. Согласно этому принципу с 2000 по 2003 год проходил масштабный Европейский проект NESSIE [6], основной задачей которого было создание набора криптографических примитивов с последующим внедрением его в международные органы стандартизации. Среди претендентов на стандарт впервые рассматривались и схемы поточного шифрования. И хотя для поточных шифров проект закончился

неудачей, криптографы не оставили попыток разработать надёжную схему. В начале 2004 года начал работу очередной масштабный сетевой проект ECRYPT [7], целью которого является объединить усилия ведущих европейских исследователей для решения открытых проблем в области защиты информации. Одной из основных задач данного проекта является разработка скоростного поточного шифра. Однако отсутствие единой методики, которая позволила бы адекватно оценить основные свойства исследуемых схем, значительно осложняет и затягивает этот процесс. В предыдущих проектах, которые брались за решение схожих задач (AES [8], NESSIE [6]), оценка сводилась к субъективному решению экспертов относительно надёжности представленных криптоалгоритмов. Одна из первых попыток разработать методику высокого уровня оценки примитивов была предпринята специалистами в рамках проекта NESSIE. В результате был предложен перечень критериев и методологических проблем, которые необходимо учитывать при анализе криптоалгоритмов [9], однако, как отмечают сами разработчики, этот список обширный, но не завершенный и требует дальнейшего совершенствования.

Таким образом, для успешного проведения сравнительного анализа и исследования основных свойств поточных шифров необходимо, в первую очередь, обосновать и выбрать систему критериев и показателей оценки исследуемых схем, а также разработать методы и создать научно-методический аппарат, который, учитывая современные тенденции проектирования схем, позволил бы выделить наиболее предпочтительные из них, что и является целью данной статьи.

I Система критериев и показателей оценки

Проблему оценки эффективности схем поточного шифрования можно решить при комплексном учёте различных по своей природе факторов. Методологическим основанием подготовки и обоснования решений относительно возможности применения исследуемых криптосистем является системный анализ [10]. Привлечение методологических средств системного анализа обусловлено, прежде всего, тем, что решения приходится принимать в условиях неопределённости, вызванной наличием факторов, не поддающихся строгой количественной оценке. Приёмы и методы системного анализа направлены на выдвижение альтернативных вариантов решения данной проблемы, выявление масштабов неопределённости по каждому варианту и сопоставление вариантов по их эффективности [10]. Очевидно, что такой подход будет действенным и при разработке систем поточного шифрования.

Согласно такому подходу, под эффективностью системы поточного шифрования будем понимать степень соответствия полученного результата функционирования схемы Y требуемому $Y^{тр}$:

$$W = \rho(Y, Y^{mp}), \tag{1}$$

где W – показатель эффективности, мера степени соответствия реального результата функционирования системы требуемому; ρ – функция соответствия, показывающая степень достижения требуемого результата функционирования системы, введенная на множестве возможных результатов.

Главной задачей при разработке и реализации систем поточного шифрования является обеспечение функции конфиденциальности информации при помощи используемого алгоритма шифрования, следовательно требуемым результатом функционирования системы $Y^{тр}$ является обеспечение данной функции. Тогда полученным результатом функционирования системы Y является реальный уровень обеспечения конфиденциальности.

Как видно из формулы (1), оценка эффективности осуществляется при помощи показателя W, отражающего степень выполнения схемой функциональной задачи. Поскольку обеспечение функции конфиденциальности достигается лишь при выполнении множества различных требований, выдвигаемых как к системе поточного шифрования в целом, так и к отдельным её компонентам, и решением нескольких задач (например, инициализация шифра, генерация выходной последовательности, шифрование), то результат функционирования системы Y описывается множеством величин y, а показатель эффективности является векторным, то есть содержит множество значений W_i частных показателей эффективности, а именно,

$$W = |W_1, W_2, \ldots, W_m|, \tag{2}$$

где W_i, $i = 1, \ldots, m$ определяется по формуле (1) с подстановкой вместо Y и $Y^{тр}$ величин y_i и $y_i^{тр}$ частных характеристик результата.

Одна из первых попыток создать систематизированное множество показателей, которые могли бы охарактеризовать эффективность функционирования схем поточного шифрования, была предпринята в работе [11], в которой также использовались векторные показатели эффективности. Однако система, предложенная в указанной работе, не удовлетворяет требованиям минимальности числа частных показателей и полноты. Тем не менее, она была взята за основу при разработке системы показателей и критериев

эффективности в данной статье, расширена за счёт введения дополнительных критериев и показателей, в некоторые из них внесены поправки, предложена другая классификация.

Согласно теории эффективности [10] критерии оценки вводятся на основе одной из трёх концепций рационального поведения систем: пригодности, оптимизации и адаптивизации. Если рассматривать эти концепции в рамках криптографической защиты информации, то все критерии (и, следовательно, показатели) эффективности систем поточного шифрования можно разделить на три группы: критерии криптографической стойкости, реализационные критерии и критерии адаптивности.

Критерии криптографической стойкости – правила, позволяющие оценить и выбрать показатели W_{CT}, характеризующие криптографическую стойкость схем поточного шифрования согласно требуемому уровню надёжности. Данная группа критериев соответствует концепции пригодности и является основной, поскольку целесообразность применения любых криптосхем основана, прежде всего, на оценке её стойкости к известным на сегодняшний день атакам, применимым к исследуемому классу схем.

Реализационные критерии – правила, позволяющие оценить и выбрать показатели W_{P}, характеризующие эффективность программной и/или аппаратной реализации. Этот тип критериев описывает оптимальность, то есть обеспечивает максимальный эффект функционирования исследуемой криптосхемы. Так, например, схема может обладать высокой стойкостью к различного рода методам анализа, но иметь ограничения на практическое использование из-за высокой стоимости аппаратной реализации, низкого быстродействия и т. п. Одним из важнейших преимуществ методов поточного шифрования информации, благодаря которому они получили широкое распространение, является высокая скорость преобразования информации. Как следствие, схемы, имеющие высокие показатели эффективности реализации, с наибольшей вероятностью будут отобраны для практических приложений.

Критерии адаптивности – правила, позволяющие оценить и выбрать показатели W_{A}, характеризующие способы изменения во времени как параметров схемы, так и её структуры с целью достижения или сохранения требуемого уровня надёжности при изменяющемся комплексе условий её применения. Система показателей адаптивности включает показатели, характеризующие прозрачность конструкции, перспективность схем, запас их стойкости и другие и, как следствие, описывает степень доверия пользователей.

Таким образом, согласно (2), показатель эффективности функционирования системы поточного шифрования содержит множество значений показателей стойкости, адаптивности и реализационных показателей

$$W = |W_{\text{CT}},\ W_{\text{P}},\ W_{\text{A}}|. \tag{3}$$

В выражении (3) каждый показатель, W_{CT}, W_{P}, W_{A}, оценивает степень соответствия реальной криптостойкости, эффективности реализации и адаптивности шифра, соответственно, требуемым характеристикам. Показатель криптографической стойкости, в свою очередь, является векторным и включает значения частных показателей, а именно,

$$W_{\text{CT}} = |W_{\text{R}},\ W_f,\ W_K,\ W_{\text{T}}|, \tag{4}$$

где W_{R} – показатель, характеризующий стойкость регистров сдвига;

W_f – показатель стойкости нелинейной функции;

W_K – показатель стойкости процедуры загрузки ключа;

W_{T} – показатель соответствия общих характеристик схемы шифрования требуемым.

Для достижения максимального значения W_{CT} необходимо, чтобы каждый частный показатель, входящий в выражение (4), принимал наибольшее значение. С этой целью выбирать параметры шифра рекомендуется в соответствии с критериями, которые можно разделить на такие группы: критерии отбора параметров регистров сдвига, критерии стойкости нелинейной функции, критерии стойкости процедуры загрузки ключа и критерии соответствия общих характеристик шифра требуемым. Согласно этим критериям оцениваются и выбираются частные характеристики соответствующего показателя.

На основе анализа основных методов криптоанализа ПШ [12], для схем, построенных на основе линейных рекуррентных регистров (ЛРР) и нелинейной функции, определим такие **критерии криптографической стойкости**.

1. ***Критерии выбора параметров ЛРР***, согласно которым подбираются параметры регистров сдвига.

– *Длина регистра* определяется степенью характеристического полинома m.

Анализ работ [12–15], посвященных исследованию корреляционных атак – наиболее мощного класса криптоатак на поточные шифры, показывает, что сложность таких методов значительно повышается с увеличением длины ЛРР. Согласно [13], если длина регистра равна 128 битам, то сложность корреляционных атак будет значительно превышать сложность полного перебора, следовательно, длина ЛРР m (а в случае, если шифрообразующее устройство комбинирует выходы нескольких ЛРР, то длина каждого регистра) должна быть больше 128 бит.

Тогда критерием отбора будем полагать $m \geq 128$.

– *Примитивность характеристического полинома*. Примитивный многочлен над полем $GF(2)$ степени m – это неприводимый многочлен (не имеет нетривиальных делителей), который делит $2^q - 1$, если $q = 2^m - 1$, и не делит $2^q - 1$, если q делит $2^m - 1$ [16]. Только регистры, использующие в качестве полинома обратной связи примитивный полином, генерируют последовательности максимального периода (проходят через все возможные $2^m - 1$ состояний).

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Попарно взаимно простые степени характеристических полиномов* (для шифрующих устройств (ШУ), комбинирующих выходы нескольких ЛРР). При выборе полиномов обратной связи, их степени должны быть попарно взаимно простыми, в этом случае значения линейной сложности и периода генерируемой ключевой последовательности будут максимальными [12].

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Плотность характеристического полинома* определяется количеством ненулевых коэффициентов. Для противостояния определённым корреляционным атакам [11, 15], количество ненулевых коэффициентов, равное количеству точек съёма ξ регистра, должно быть не меньше половины его длины m.

Критерием отбора будем полагать $\xi \geq m/2$.

– *Соответствие множества точек обратных связей T регистра полному множеству положительных разностей $\Delta(T)$*, то есть все положительные разности между элементами множества T различны. Требуемое соответствие обеспечивает противостояние аналитическим атакам [12].

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Наибольший общий делитель двух парных (соседних) элементов множества точек обратных связей T должен быть равен* 1 [12].

Критерием отбора является логическая переменная «Истина» \ «Ложь».

2. ***Критерии стойкости нелинейной функции***, согласно которым осуществляется выбор нелинейной функции и её параметров.

– *Количество точек съёма нелинейной функции*. Согласно [17], для противостояния криптосхемы инверсионным атакам количество точек съёма нелинейной функции τ следует выбирать достаточно большим, предпочтительно близким к максимально возможному значению $m - 1$.

Критерием отбора будем полагать $\tau \to m - 1$.

– *Соответствие множества точек съема для нелинейной функции Γ полному множеству положительных разностей* $\Delta(\Gamma)$ (для фильтр-генераторов). Требуемое соответствие обеспечивает противостояние аналитическим атакам [12].

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Наибольший общий делитель двух парных (соседних) элементов множества точек съёма нелинейной функции Γ должен быть равен* 1 [11 – 12].

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Коэффициент пересечения*. Количество элементов I множества $|B| = \Delta(T) \cap \Delta(\Gamma)$, называемое коэффициентом пересечения, должно быть минимальным во избежание информационного просачивания, в частности, для противостояния инверсионным атакам [17] и атакам «предполагай и определяй» [18].

Критерием отбора будем полагать $I = \min\limits_{I_i} \{I_{1,\ \ldots,\ } I_{m\text{-}1}\}$, где I_i – коэффициент пересечения i-й функции, $i = 1, \ldots, m–1$.

– *Минимальный предел алгебраической степени*. Если выходная последовательность ШУ зависит от D бит состояния ЛРР, то в целях увеличения сложности атак, основанных на линейной аппроксимации нелинейных функций [19], алгебраическая степень d нелинейной функции должна быть не менее $D/2$.

Критерием отбора является условие $d \geq D/2$.

– *Алгебраическая степень функции*. Алгебраической степенью d называется максимальное количество переменных-сомножителей, встречающееся в любом из слагаемых (термов) булевой функции f, представленной в алгебраической нормальной форме [16]. Высокая алгебраическая степень позволяет противостоять различным аналитическим атакам, основанным на методах линейной аппроксимации [19].

Критерием отбора является $d = \max\limits_{d_i} \{d_{1,\ \ldots,\ } d_\tau\}$, где d_i – алгебраическая степень i-й функции, $i = 1, \ldots, \tau$.

– *Порядок корреляционного иммунитета* [1] κ функции f должен быть максимальным при заданных значениях алгебраической степени d и количества точек съёма τ.

Критерием отбора будем полагать $\kappa = \max\limits_{\kappa_i} \{\kappa_{1,\ \ldots,\ } \kappa_{d\text{-}\tau}\}$, где κ_i – порядок корреляционного иммунитета i-й

функции, $i = 1, \ldots, d-\tau$.

– *Сбалансированность*. Функция f называется сбалансированной [1], если её таблица истинности содержит одинаковое число 0 и 1, т.е.

$$\#\left\{x \in GF\left(2^n\right) \middle| f(x) = 0\right\} = \#\left\{x \in GF\left(2^n\right) \middle| f(x) = 1\right\} = 2^{n-1}.$$

Сбалансированность функции является показателем, отражающим стойкость гаммы к статистическим атакам.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Степень нелинейности функции*. Функция f называется аффинной, если принимает вид $f(x) = a_1x_1 \oplus \ldots \oplus a_mx_m \oplus c$, где $a_i,\ c \in GF(2)$. В частности, f именуется линейной, если $c = 0$. Расстояние Хэмминга между функциями f и g, принадлежащих полю $GF(2^n)$, определяется как количество позиций, в которых различаются их таблицы истинности [16]. *Нелинейность* функции f, обозначаемая как N_f – это минимальное расстояние Хэмминга между f и всеми аффинными функциями, принадлежащими полю $GF(2^n)$. Для сбалансированной функции f над $GF(2^n)$ ($n \geq 3$) нелинейность N_f может достигать [20]

$$N_f \leq \begin{cases} r = 2^{n-1} - 2^{n/2-1} - 2, & n = 2k \\ r = \left\lfloor\!\left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor\!\right\rfloor, & n = 2k+1 \end{cases},$$

где $\left\lfloor\!\left\lfloor x \right\rfloor\!\right\rfloor$ – максимальное четное целое, меньшее либо равное x.

Критерием отбора является $N_f = \max\limits_{N_{f_i}} \left\{N_{f_1}, \ldots, N_{f_r}\right\}$, где N_{f_i} – нелинейность i-й функции, $i = 1, \ldots, r$.

– *Степень критерия распространения*. Булева функция f от τ переменных удовлетворяет критерию распространения степени k, если любой выходной бит изменяется с вероятностью строго ½ при комплементарной замене k входных бит [21], то есть, если

$$(\forall \boldsymbol{a}: 1 \leq W_H(\boldsymbol{a}) \leq k) \quad P(f(\mathrm{X}) = f(\mathrm{X} \oplus \boldsymbol{a})) = ½,$$

где $\boldsymbol{a}$ – двоичный вектор, принадлежащий $GF(2^\tau)$;

$W_H(\boldsymbol{a})$ – вес Хэмминга, количество не нулевых элементов в векторе $\boldsymbol{a} \in GF(2^\tau)$;

X – случайная величина, принимающая значения $x \in GF(2^\tau)$.

Высокая степень критерия распространения повышает сложность определённых аналитических атак.

Критерием отбора будем полагать $k = \max\limits_{k_i} \{k_1, \ldots, k_\tau\}$, где k_i – степень критерия распространения i-й функции, $i = 1, \ldots, \tau$.

3. ***Критерии стойкости процедуры загрузки ключа***, согласно которым подбирается, либо уточняется алгоритм инициализции/переинициализации шифра.

– *Вероятность нулевого заполнения*. Пусть $S_0 = \{s_0, s_1, \ldots, s_m\}$ обозначает начальное состояния шифра после выполнения процедуры загрузки ключа, тогда вероятность того, что $s_i = 0$, для всех $i = 0, \ldots, m$, должна быть полностью исключена.

Критерием отбора будем полагать $P(S_0 = 0) = 0$.

– *Нелинейность операций ключевой загрузки*. Нелинейность операций повышает стойкость к методам анализа, основанным на использовании частой инициализации (переинициализации) шифра.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Каждый бит инициализированного регистра является результатом нелинейных преобразований всех бит ключа*. В таком случае, знание вводимого ключа исключает знание инициализированного ключа (при гарантированной стойкости нелинейных преобразований).

Критерием отбора является логическая переменная «Истина» \ «Ложь».

4. ***Критерии соответствия общих характеристик шифра требуемым***. Выполнение данных критериев гарантирует увеличение сложности методов анализа общего типа.

– *Период ключевой последовательности*. Периодом ключевой последовательности, T, называется количество бит до того момента, когда последовательность начнет повторяться [1]. Поскольку ЛРР длиной m бит может находиться в одном из $2^m - 1$ внутренних состояний, то теоретически ключевая последовательность может иметь период длиной $2^m - 1$. Обеспечение большого периода шифрпоследовательности снижает эффективность атак периодичности и методов анализа линейной сложности, поскольку любая последовательность, имеющая конечный период, имеет конечную линейную сложность [22]. Согласно [11 – 12] одним из необходимых условий абсолютной стойкости шифра является невозможность повторного использования одного и того же ключа. Но любая последовательность, сгенерированная детерминированным алгоритмом, имеет конечный период [16].

Тогда критерием отбора будем полагать $T = \max\limits_{T_i} \{T_1, \ldots, T_r\}$, где T_i – период i-й схемы, $i = 1, \ldots, r$.

– *Линейная сложность ключевой последовательности*. Значение линейной сложности $\Lambda(s^n)$ показывает, насколько сложно воспроизвести символы исследуемой последовательности на основе её фрагмента, по сути, оно отражает непредсказуемость шифрпоследовательности [22]. Высокая линейная сложность гарантирует увеличение сложности алгоритма Берлекампа-Мэсси [23], основной целью которого является нахождение кратчайшего ЛРР, способного сгенерировать заданную последовательность. Концепция линейной сложности впервые была предложена Рюппелем в работе «Линейная сложность и случайные последовательности» [22], в которой автор предположил, а впоследствии это доказали другие исследователи [22], что значение линейной сложности случайной периодической последовательности близко к периоду, т. е. $\Lambda(s^n) \to T$. Однако, учитывая, что современные поточные шифры обеспечивают огромные длины периодов, рассчитать соответствующие значения линейной сложности практически невозможно. Тем не менее, Рюппель показал, что для двоичных независимых и равномерно распределённых последовательностей s^i, какими предполагаются шифрпоследовательности, значение линейной сложности $\Lambda_j(s^n)$ подпоследовательности s^n из их профиля становится случайной величиной [22], и вывел формулы для расчёта матожидания и дисперсии. Следовательно, оценить линейную сложность можно при помощи статистического теста: линейная сложность выходной последовательности криптографически стойкого ШУ неотличима от линейной сложности случайной последовательности. Подробное описание теста линейной сложности можно найти в работе [24]. Согласно той же работе [24], критериями отбора будем полагать статистические критерии: правило 1 – правило доверительного интервала, в который должно попадать количество последовательностей, прошедших статистический тест, и правило 2, согласно которому «общее» значение вероятности $\boldsymbol{P}_{j<o>}$, вычисляемое в процессе тестирования, должно превышать значение 0,0001.

Критерии отбора: $r_{\min} < r_j < r_{\max}$; $\boldsymbol{P}_{j<o>} \geq 0{,}0001$.

– *Длина ключей*. Длина секретного ключа l определяет сложность атак прямого перебора. В настоящее время для обеспечения минимального уровня надёжности криптосистемы необходимо использовать секретные ключи длиной не менее 128 бит [9].

Критерием отбора является $l \geq 128$.

– *Внутренняя память генератора*. Согласно [25], для противостояния атакам компромисса время-память размер внутреннего состояния ШУ M должен быть, по меньшей мере, в два раза больше длины ключа l.

Критерием отбора будем полагать $M \geq 2l$.

– *Максимальная длина ключевой последовательности, сгенерированной на одном и том же ключе*. С целью достижения максимального периода и высокой линейной сложности выходных последовательностей ШУ предполагаемая в приложениях (максимальная) длина ключевой последовательности $N_{\max}$ не должна превышать значение $\binom{m}{d}$, где m – длина регистра, d – алгебраическая степень нелинейной функции. Кроме того, выполнение этого условия повысит сложность атак на различимость и корреляционных атак [12].

Критерием отбора будем полагать $N_{\max} < \binom{m}{d}$.

– *Статистические критерии*.

Статистические свойства ключевой последовательности являются основными характеристиками, определяющими стойкость схемы шифрования. Криптографическая стойкость схемы поточного шифрования в большой степени зависит от того, насколько близко она аппроксимирует генератор случайных чисел, т.е. насколько шифрпоследовательность будет вычислительно непредсказуемой и неотличимой от истинно случайной последовательности. По результатам анализа, проведенного в работе [24], наиболее эффективной методикой статистического анализа ШУ на сегодняшний день является методика, предложенная NIST. Согласно данной методике первым критерием отбора является коэффициент прохождения тестов последовательностями r_j; он должен находится внутри доверительного интервала $[r_{\min}, r_{\max}]$, т. е. $r_{\min} < r_j < r_{\max}$.

Вторым критерием является правило 2, согласно которому должно выполняться условие $\boldsymbol{P}_{j<o>} \geq 0{,}0001$.

Согласно выражению (3), на общий показатель эффективности влияет также значение реализационного показателя, характеризующего оптимальность исследуемой схемы. С целью повышения этого значения введем следующие **реализационные критерии**, в соответствии с которыми оцениваются частные характеристики показателя $W_{\text{р}}$, большие значения которых увеличивают общее значение данного показателя, и, как следствие, обеспечивают максимальный эффект функционирования криптосхемы.

– *Скорость шифрования* $S_{\text{ш}}$, Гбайт/с. Высокая скорость шифрования – одно из основных требований

выдвигаемых к схемам поточного преобразования информации, выделяющее их среди остальных криптопримитивов.

Критерием отбора будем полагать $S_{\text{ш}} = \max\limits_{S_{\text{ш}_i}}\{S_{\text{ш}_1}, \text{K}, S_{\text{ш}_r}\}$, где $S_{\text{ш}_i}$ – скорость шифрования *i*-й схемы, Гбайт/с, $i = 1, \ldots, r$.

– *Время загрузки ключа* t_u, с. Данный параметр характеризует скорость выполнения процедуры инициализации (переинициализации) шифра. Как показано в работе [11], перспективные схемы поточного шифрования отличаются использованием быстрых процедур загрузки ключа.

Критерием отбора будем полагать $t_u = \min\limits_{t_{u_i}}\{t_{u_1}, \text{K}, t_{u_r}\}$, где t_{u_i} – время инициализации *i*-й схемы, с, $i = 1, \ldots, r$.

– *Объём используемой памяти* v_{mem}, байт. Отображает размер используемой памяти, ОЗУ и ПЗУ.

Критерием отбора является $v_{\text{mem}} = \min\limits_{v_{\text{mem}_i}}\{v_{\text{mem}_1}, \text{K}, v_{\text{mem}_r}\}$, где v_{mem_i} – объём памяти, используемой *i*-й схемой, $i = 1, \ldots, r$.

– *Количество используемых различных арифметических операций* N_O. Данный параметр характеризует уязвимость схемы к атакам на реализацию, как, например, временные атаки и анализ энергопотребления.

Критерием отбора является $N_{O_i} = \min\limits_{N_{O_i}}\{N_{O_1}, \text{K}, N_{O_r}\}$, где N_{O_i} – количество используемых различных арифметических операций *i*-й схемой, $i = 1, \ldots, r$.

– *Возможность генерации ключевой последовательности с любой точки*. Обеспечение быстрого поиска произвольных элементов ключевой последовательности гарантирует возможность выполнения эффективной синхронизации и её восстановления в случае потери. Обозначим данную характеристику как *C*.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Обеспечение целостности передаваемых сообщений*. Использование эффективных методов обеспечения целостности шифруемых данных является одним из отличительных особенностей эффективного поточного шифра. Данный параметр обозначим как f_{MAC}.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

Как известно [10], эффективность выполнения любой операции может изменяться во времени. Следовательно, множество допустимых параметров схемы шифрования также может видоизменяться при изменении условий её применения. Учитывая этот факт, определим множество **критериев адаптивности**.

– *Прозрачность П.* Данный параметр характеризует возможность проведения сравнительного анализа схем и осуществления контроля над внедрением «закладок».

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Переносимость* $P_{p\text{-}h}$. Параметр, характеризующий возможность реализации схемы программной и/или аппаратной.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Изменяемая длина ключа* $\bar{l}$. Данный параметр характеризует возможность применения схемы для различных уровней надёжности.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Запас стойкости* R_s.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

– *Перспективность* P_A.

Критерием отбора является логическая переменная «Истина» \ «Ложь».

Приведенные параметры достаточно полно характеризуют конкретную схему поточного шифрования. Введенные критерии эффективности в совокупности с методиками оценки позволят осуществить сравнение различных схем поточного шифрования. Использование векторных показателей приводит к снижению неопределенности эксперта относительно оцениваемой схемы. В целом, предложенная система показателей и критериев эффективности позволит построить эффективный инструментарий оценки схем поточного шифрования.

II Методика оценки эффективности схем поточного шифрования

Практическая направленность исследования эффективности криптографических систем заключается в выработке решений на рациональное использование средств шифрования при обеспечении конфиденциальности информации в разных условиях применения шифра или на целесообразный вариант проектируемой схемы. Таким образом, главной задачей таких исследований является выработка научно

обоснованных решений, связанных с созданием и применением криптосистем. В нашем случае, решение, независимо от его конкретного содержания и характера, – это результат сознательного выбора одного (рационального) способа или некоторого их подмножества из множества возможных обеспечения конфиденциальности информации. Такой выбор осуществляет лицо, принимающее решения (ЛПР), которое наделено определёнными правами и полномочиями и несет всю полноту ответственности за последствия принимаемых решений.

Основная цель применения схем поточного шифрования – обеспечение конфиденциальности, может быть достигнута различными способами (разными схемами с разным набором основных элементов). Допустимые способы (в смысле наложенных ограничений) образуют множество стратегий (альтернатив).

Каждая из допустимых альтернатив, как правило, обеспечивает различный уровень решения поставленной задачи. Указать, какая лучше из них, может лишь конкретное ЛПР применительно к понимаемой именно им данной задаче [10]. Рассмотрим общую схему процесса выработки решений.

На первом этапе ЛПР, опираясь на свою систему предпочтений, последовательно формирует множество A стратегий (альтернатив), которое образуют допустимые способы достижения цели, в нашем случае, обеспечения конфиденциальности информации, и множество Ψ факторов, влияющих на успешное проведение операции шифрования. Аналогично на основе системы предпочтений выбираются численные характеристики Y исхода выполнения операций шифрования и формируется величина требуемого результата $Y^{\text{тр}}$ шифрования. Далее по информации Y, $Y^{\text{тр}}$ с учётом предпочтений о виде показателя эффективности устанавливается один из возможных видов метрики $\rho(Y, Y^{\text{тр}})$ и формируется некоторая модель Θ «результат – показатель», задающая отображение значений полученных результатов в значение показателя эффективности, при этом, если показатель эффективности является векторным, то определяется вид функции свертки частных значений этого показателя. Одновременно формируется критерий K по информации о предпочтении формирования его в виде решающего правила. На основе суждения о степени соответствия функции конфиденциальности требуемому уровню безопасности осуществляется выбор альтернативы из подмножества «наилучших» с точки зрения ЛПР стратегий $A^* \in A$.

Все введенные в предыдущем подразделе данной статьи показатели эффективности являются векторными, следовательно, модель Θ задаёт отображение вида

$$\Theta: Y \to (\rho_1(y_1,\ y_1^{\text{ТР}}),\ \rho_2(y_2,\ y_2^{\text{ТР}}),\ \ldots,\rho_m(y_m,\ y_m^{\text{ТР}})), \tag{5}$$

где y_i, $y_i^{\text{ТР}}$ – детерминированные скалярные характеристики исхода и требуемого результата ($i = \overline{1,m}$). Функция Θ ставит в соответствие каждой стратегии $a \in A$ значение векторного показателя $W(a) = (W_1(a), W_2(a), \ldots, W_m(a))$.

Поскольку стойкость шифра играет определяющую роль при вынесении суждения о применимости исследуемой схемы в криптографических приложениях (т. е. цель операции шифрования состоит в достижении требуемого результата), то для введенного показателя стойкости $W_{\text{СТ}}$ функция соответствия ρ будет иметь вид:

$$\rho\left(y, y^{\text{ТР}}\right) = \begin{cases} 1, \text{ если } y \geq y^{\text{ТР}}; \\ 0, \text{ если } y < y^{\text{ТР}}, \end{cases} \tag{6}$$

В этом случае невыполнение соответствующего условия приводит к тому, что значение частного показателя стойкости системы шифрования будет равно нулю.

Для показателей адаптивности $W_{\text{А}}$ и реализационного $W_{\text{Р}}$ определим следующую функцию соответствия:

$$\rho(y, y^{\text{ТР}}) = y. \tag{7}$$

Такая функция соответствует ситуации, когда при выполнении операции необходимо достигнуть наибольшего эффекта.

Решая задачу выбора, стоящую перед ЛПР, необходимо, прежде всего, ориентироваться на достижение цели операции, а следовательно, задаваться определенным видом критерия эффективности. В случае, если оценивается криптографическая стойкость системы (при этом, учитывая выражение (6), показатель $W_{\text{СТ}}$ может принимать только два значения), то критерием вынесения окончательного суждения относительно стойкости исследуемой схемы может послужить такой, согласно которому принимается любая стратегия (набор параметров шифра), приводящая к желаемому результату.

При оценивании оптимальности и адаптивности схемы необходимо достичь максимума результата, т. е. бóльшие значения показателей $W_{\text{А}}$ и $W_{\text{Р}}$ будут соответствовать более предпочтительным исходам операции. В данном случае выбор решения будем осуществлять с использованием критерия, согласно которому наилучшей считается та стратегия, для которой показатель достигает экстремального значения в указанном направлении:

$$a^* : \max_{a \in A} W(a), \tag{8}$$

где $W(a)$ – обобщенный показатель эффективности исследуемой схемы шифрования, полученный соотнесением разнородных частных показателей в общую оценку эффективности.

Качество принимаемых решений по заданным критериям определяется адекватностью вида свертки векторного показателя эффективности в скалярную целевую функцию.

В общем виде показатель W задаётся в виде некоторой композиции (символ композиции – $\otimes$) [10]:

$$W = W_1 \otimes W_2 \otimes \ldots \otimes W_m. \tag{9}$$

Так как значения частных показателей W_{R}, W_f, W_K и W_{T}, составляющие вектор $W_{\text{ст}}$, определяются по формуле (6), то функция (9) для обобщенного показателя стойкости будет выглядеть следующим образом:

$$W_{\text{ст}} = W_{\text{R}} \wedge W_f \wedge W_K \wedge W_{\text{T}}, \tag{10}$$

где $\wedge$ – обозначает конъюнкцию. То есть, если хотя бы один из частных показателей будет равен нулю, то исследуемая схема рассматривается как нестойкая и дальнейшие исследования по показателям адаптивности W_{A} и реализационному W_{P} не проводятся.

Как было показано выше, значения частных показателей, составляющих векторы W_{A} и W_{P}, определяются по формуле (7). Однако в большинстве случаев степень достижения результата (как например, степень перспективности или прозрачности) описывается не количественными, а качественными характеристиками. Для того, чтобы измерить предпочтительность той или иной частной характеристики показателей W_{A} и W_{P}, будем использовать способ выражения предпочтения лингвистическими переменными посредством введения некоторой функции принадлежности как способа формализации субъективного смысла этих качественных характеристик, т. е. будем осуществлять переход к нечетким отношениям.

Переход от обычного (четкого) отношения к нечеткому осуществляется так же, как и переход от обычного множества к нечеткому.

В этом случае *нечетким отношением на обычном множестве A* называется [26] нечеткое подмножество D, характеризующееся функцией принадлежности $\mu_{\text{D}} : A \to [0,1]$, которая ставит в соответствие каждому элементу $a \in A$ число $\mu_{\text{D}}(a)$ из отрезка [0,1], описывающее степень принадлежности элемента a подмножеству D.

Будем считать, что факт превосходства в важности имеет место при значениях функции принадлежности $\mu_{\text{D}}(a) \geq 0{,}5$.

Все частные характеристики реализационного показателя и показателя адаптивности имеют различную степень влияния на общий исход операции шифрования. То есть необходимо определить степень влияния изменения значения частной характеристики показателя эффективности на результат операции. В этом случае, используют форму выражения предпочтений коэффициентами важности, которые измеряют степень этого влияния, и удовлетворяют требованиям неотрицательности и нормировки (сумма их равна единице). Коэффициент важности тем больше, чем более предпочтительным для ЛПР является изменение характеристики в соответствующем направлении по вкладу в целевой эффект. Для одинаковых по предпочтительности частных характеристик показателей эффективности значения коэффициентов важности одинаковы. В дальнейшем полученные коэффициенты используются при агрегировании частных показателей в функцию эффективности (9). Определение коэффициентов важности каждой характеристики будем производить методом экспертного оценивания по следующей схеме [10].

Экспертами производится попарное сравнение элементов (характеристик) a_i, a_j, руководствуясь шкалой выражения предпочтений со следующими градациями: 1 – элементы одинаковы по предпочтительности; 3 – имеются достаточные основания считать один элемент предпочтительнее другого; 5 – один элемент безусловно предпочтительнее другого. Если эксперт колеблется в оценке предпочтительности между указанными градациями, он ставит промежуточное целое число (2, 4). Далее формируется матрица Q попарных сравнений следующим образом. Последовательно просматривая пары элементов (a_i, a_j), соответствующие строкам i ($i = \overline{1,m}$) матрицы, эксперт выделяет и оценивает в заданной шкале только те пары, в которых элемент a_i предпочтительнее a_j. Значения остальных элементов q_{ji} матрицы Q размером $m \times m$ вычисляют по правилу:

$$q_{ji} = \frac{1}{q_{ij}},$$

где q_{ij} – оценка предпочтительности элемента a_i над элементом a_j по шкале с градациями 1, 2, 3, 4, 5. Это правило соответствует попарному выражению предпочтения как доли относительной интенсивности свойства.

Для определения коэффициентов важности γ_i полученная матрица $Q = \| q_{ij} \|$, $i, j = \overline{1,m}$ обрабатывается по следующему итерационному алгоритму.

***Алгоритм* 1**. 1. Задать требуемую точность ε вычисления γ_i, $i = \overline{1,m}$.

2. Положить $t = 0$ и все $\gamma_i^{(t)} = \frac{1}{m}$, $i = \overline{1,m}$.

3. Положить $t = t + 1$.

4. Вычислить

$$\gamma_j^{(t)} = \frac{\sum_{i=1}^{m} q_{ij} \gamma_i^{(t-1)}}{\sum_{i=1}^{m} \sum_{j=1}^{m} q_{ij} \gamma_i^{(t-1)}}, \; j = \overline{1,m}.$$

5. Проверить условие $\left| \gamma_i^{(t)} - \gamma_i^{(t-1)} \right| \le \varepsilon$, $i = \overline{1,m}$. Если условие выполняется, то перейти к п. 6, иначе – к п. 3.

6. Прекратить вычисления. Полученные $\gamma_i^{(t)}$ принять в качестве коэффициентов важности γ_i.

В алгоритме 1 критерием останова является условие п. 5. Практика показывает, что $\varepsilon = 0{,}01$. Весовые коэффициенты элементов a_i, измеренные в шкале отношений, удовлетворяют условию: $\sum_{i=1}^{m} \gamma_i = 1$.

Тогда, учитывая полученные коэффициенты важности, функция свертки (9) примет вид

$$W = W_1^{\gamma_1} \otimes W_2^{\gamma_2} \otimes \mathrm{K} \otimes W_m^{\gamma_m}. \qquad (11)$$

где γ_i – весовые коэффициенты соответствующих частных характеристик показателей W_A и W_P.

При оценке эффективности схем поточного шифрования по предлагаемой системе характеристик показателей W_A и W_P недопустимо компенсировать значения одних характеристик другими. Так, например, низкие скоростные характеристики, входящие в состав вектора W_P нельзя компенсировать наличием дополнительных функций. В нашем случае требуется обеспечить равномерное «подтягивание» всех характеристик к их наилучшему уровню. Тогда в качестве одного из возможных способов организации функции свертки рекомендуется использовать функцию вида [10]

$$W = \min \{W_1, W_2, \ldots W_m\}, \qquad (12)$$

которая соответствует вынесению суждения по «узкому месту».

Таким образом, преложенная методика оценки схем поточного шифрования в совокупности с введенной системой критериев и показателей эффективности позволяет оценить основные свойства исследуемых схем и выбрать наиболее оптимальную в случае их сравнительного анализа, либо определить целесообразный вариант проектируемой схемы при помощи развернутой методики исследований.

Обобщённый критерий стойкости определяет множество необходимых параметров, которыми должна обладать любая схема поточного шифрования. Согласно остальным критериям (реализационным и адаптивности) оценивается степень эффективности исследуемой схемы. Поэтому анализ эффективности производится в два этапа. На первом этапе схема проверяется на соответствие критерию стойкости, т. е. производится анализ пригодности алгоритма шифрования в криптографических приложениях.

Вычисляются значения частных характеристик показателей W_R, W_f, W_K и W_T и проверяется выполнение соответствующих условий. Согласно выражению (6) формируется множество значений частных характеристик каждого показателя, которые затем преобразуются в общие значения W_R, W_f, W_K и W_T по формуле (10). Показатель стойкости $W_\mathrm{ст}$ определяется по правилу (10). Суждение о криптографической надёжности исследуемой схемы поточного шифрования выносится по критерию пригодности, согласно которому алгоритм считается криптостойким в случае, если полученное значение $W_\mathrm{ст} = 1$, иначе схема считается ненадёжной и снимается с дальнейшего рассмотрения.

На втором этапе исследований эффективности рассчитываются значения реализационного показателя W_P и показателя адаптивности W_A и сравниваются с требуемым уровнем эффективности W^{TP}. Поскольку значения W_P, $W_\mathrm{A} \in [0,1]$, то «идеальная» (предельная) эффективность $W^{\mathrm{TP}} = 1$.

Таким образом, анализ эффективности схем поточного шифрования предлагается выполнять в такой последовательности.

1. Определяются численные значения характеристик частных показателей стойкости W_R, W_f, W_K и W_T по функции соответствия (6).

2. Используя функцию свертки (10), вычисляются значения частных показателей стойкости W_R, W_f, W_K и W_T.

3. Определяется значение обобщенного показателя стойкости $W_{ст}$ по правилу (10). Если $W_{ст} = 1$, то исследуемая схема удовлетворяет критерию стойкости, иначе алгоритм снимается с дальнейшего рассмотрения и принимается решение о его криптографической ненадёжности.

4. Если значение $W_{ст} = 1$, оценивается оптимальность алгоритма по реализационному показателю W_P согласно следующей схеме.

4.а. Специалистами-криптографами в результате балльного оценивания частных реализационных характеристик показателя W_P определяется их предпочтительность и осуществляется переход к нечетким множествам посредством установления функции принадлежности μ_i, $i = \overline{1, 6}$ каждой полученной оценки (факт превосходства имеет место при $\mu \geq 0{,}5$).

4.б. Производится экспертная оценка степени важности частных характеристик показателя W_P по пятибалльной шкале предпочтений, в результате которой формируется матрица попарных сравнений размером 6×6.

4.в. По алгоритму 1 рассчитываются коэффициенты важности $\gamma_{1...}\gamma_6$.

4.г. Определяется значение обобщенного реализационного показателя W_P по правилу (12) с учетом (11).

4.д. В случае, если оценивается эффективность единственной схемы, то значение W_P сравнивается с $W^{TP} = 1$. Выносится решение относительно оптимальности исследуемого алгоритма. Если производится сравнительный анализ схем, то наиболее оптимальной считается та схема, которая удовлетворяет критерию (8).

6. Если рассматриваемая схема удовлетворяет реализационному критерию, т. е. является оптимальной, то определяется степень её адаптивности посредством вычисления и оценки показателя W_A. Для этого п.п. а – д применить для W_A.

7. По результатам оценки показателей W_P и W_A выносится окончательное суждение об эффективности исследуемой схемы, либо (если их несколько) выбирается наилучшая.

Заключение

При современном уровне развития информационных технологий обеспечение эффективности функционирования схем шифрования становится актуальной проблемой, поскольку основная масса предложенных до настоящего времени алгоритмов обладают явным дисбалансом между криптографической стойкостью и эффективностью. Попытки разработать криптостойкую схему шифрования приводили к значительному снижению скорости выполняемых преобразований. С другой стороны, высокая скорость шифрования достигалась за счёт ослабления надёжности. Полностью разрешить данное противоречие достаточно сложно, однако, если согласовать множество различных факторов, влияющих на выполнение операций шифрования, выявить и измерить предпочтения по каждому оцениваемому показателю рассматриваемой схемы, то можно найти некоторый компромисс при разрешении данной проблемы. Предложенная в данной работе система показателей и критериев эффективности позволяет определить множество допустимых параметров схемы на соответствие требованиям пригодности, оптимальности и адаптивности. Каждая группа векторных показателей значительно снижает неопределенность эксперта относительно оцениваемой схемы, поскольку позволяет достаточно глубоко и всесторонне описать её. В целом сформированный комплекс критериев и показателей эффективности позволил разработать методику оценки поточных шифров, при помощи которой можно получить комплексную (интегральную) оценку положительных и отрицательных свойств и частных характеристик элементов анализируемых схем, а также осуществлять их сравнительный анализ. Предложенная методика предназначена для исследования эффективности новых и известных алгоритмов поточного шифрования, а также для выработки научно обоснованных решений на целесообразный вариант проектируемой схемы.

Література: ***1.*** *Menezes A., P. van Oorschot, and Vanstone S. Handbook of Applied Cryptography. CRC Press, 1997.– 816 p.* ***2.*** *European Telecommunication Standards Institute. Group special mobile. Provisional Standard GSM 06.01, prI-ETS 300 036, ETSI.* ***3.*** *Barkan E., Biham E., Keller N., Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, in Advances in Cryptology – CRYPTO 2003, vol. 2729 of Lecture Notes in Computer Science, Springer-Verlag, 2003. pp .600-616.* ***4.*** *Biham E., Dunkelman O., Cryptanalysis of the A5/1 GSM Stream Cipher, Progres in Cryptology, proceedings of Indocrypt'00, Lecture Notes in Computer Science 1977, Springer-Verlag, pp. 43-51, 2000.* ***5.*** *Goldberg I., Wagner D., Green L., The (Real-Time) Cryptanalysus of A5/2, presented at the Rump Session of Crypto'99, 1999.* ***6.*** *NESSIE Project – New European Schemes for Signatures, Integrity and Encryption. http://cryptonessie.org.* ***7.*** *ECRYPT Project – European Network of Excellence*

for Cryptology. http://www.ecrypt.eu.org. ***8.*** *AES discussion forum: http://aes.nist.gov.* ***9.*** *Preneel B., Biryukov. A, Oswald E. and others. NESSIE security report. Public Report, Deliverable D 20. 2002. Version 1.0: http://cryptonessie.org.* ***10.*** *Надежность и эффективность в технике: Справочник: Н17 В 10 т./ Ред. совет: В.С. Авдуевский (пред.) и др. –М.: Машиностроение, 1988. – (В пер.). Т - 3, Эффективность технических систем / Под общ. В.Ф. Уткина, Ю.В.Крючкова.–328 с.* ***11.*** *Потий А .В., Избенко Ю. А. Множество показателей оценки эффективности функционирования схем поточного шифрования // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2003. – № 133.* ***12.*** *Потий А. В., Избенко Ю. А. Исследование методов криптоанализа поточных шифров // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - НТУ "КПІ", ДСТСЗІ СБУ. - 2003. - № 6. - С. 34 – 49.* ***13.*** *M. Mihaljevic, J. Golić. A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence. // In Advances in Cryptology – AUSCRYPT'90, vol.453, Lecture Notes in Computer Science, Springer-Verlag, pp.165 – 175,1990.* ***14.*** *W. Maier, O. Staffelbach. Fast correlation attacks on stream ciphers. // In Advances in Cryptology – EUROCRYPT'88, vol.330, Lecture Notes in Computer Science, Springer-Verlag, pp.301 – 314, 1988.* ***15.*** *T. Siegenthaller, Decrypting a class of stream cipher using ciphertext only // IEEE Trans. Comput.,vol. C-34, pp.81 – 85, Jan. 1985.* ***16.*** *Фомичев В. М., Дискретная математика и криптология: Курс лекций / Под ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003. 400 с.* ***17.*** *J. Dj. Golić, A. Clark, and E. Dawson. Inversion attacks and branching. // Information Security and Privacy, Fourth Australasian Conference, ACISP'99, Lecture Notes in Computer Science, vol. 1587, J. Pieprzyk, R. Savavi-Naini, J. Seberry eds., Springer-Verlag, pp. 88 – 102, 1999.* ***18.*** *J. Golić, On the security of nonlinear filter generators. In Fast Software Encryption – Third International Workshop, Cambridge, February 1996, Lecture Notes in Computer Science, vol. 1039, pp. 173 – 188, Springer-Verlag, Berlin, 1996.* ***19.*** *Courtois N. Meier W. Algebraic attacks on stream ciphers with linear feedback, Eurocrypt 2003, Warsaw, Poland, Lecture Notes in Computer Science, vol. 2656, Springer, 2003, pp. 345 – 359.* ***20.*** *J. Seberry, X.-M. Zhang and Y. Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995.* ***21.*** *B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functions," in Lecture Notes in Computer Science 473; Advances in Cryplology: Proc. Eurocrypt'90, 1. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 161-173. Berlin: Springer-Verlag.* ***22.*** *R. A. Rueppel. Linear complexity and random sequences. Advances in Cryptilogy–EUROCRYPT'85 (LNCS 219), 167 – 188, 1986.* ***23.*** *Massey J. L., Shift-Register Synthesis and BCH Decoding // IEEE Transactions on Information Theory, January 1969. Vol. IT-15, no. 1.* ***24.*** *Потий А., Орлова С., Гриненко Т., Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вып. 2. С.206-214.* ***25.*** *Babbage S. A space/time tradeoff in exhaustive search attacks on stream ciphers. In European Convention on Security and Detection, volume 408 of IEE Conference Publication, May 1995.* ***26.*** *Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. М.: Наука, 1977. 248 с.*

УДК 681.321;322:621.395

АЛГОРИТМ РОЗПОДІЛУ РЕСУРСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДОКУМЕНТАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ

Володимир Кононович, Тетяна Тардаскіна*

Академія зв'язку України, Одеський регіональний центр ТЗІ ВАТ "Укртелеком",
**Одеська національна академія зв'язку*

Анотація: **Аналізується задача оптимізації витрат на інформаційну безпеку системи документальних телекомунікацій, яка зводиться до задачі багатокритеріального вибору. Пропонується інтерактивна процедура раціонального вибору варіанту розподілу витрат.**

Summary: **The expenses optimization task of information security of the documental telecommunication systems is analyzed. Whole thing comes to multi criteria choice task. The interactive procedure of rational choice of the expenses distribution variant is offered.**

Ключові слова: **Інформаційна безпека, інформаційно-телекомунікаційні системи, телекомунікаційні мережі, передавання даних, загрози, послуги та механізми безпеки, функціональний профіль захисту.**

І Вступ

Забезпечення інформаційної безпеки документальних телекомунікацій має на меті створення перешкод