УДК 681.3.067

А.В. ПОТИЙ, канд. техн. наук, А.К. ПЕСТЕРЕВ

ПРИНЦИПЫ СИСТЕМНОГО ПОДХОДА К СЕРТИФИКАЦИИ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Многочисленные факты указывают на то, что опасность несанкционированных злоумышленных действий в системах обработки и передачи информации весьма велика, а проблема обеспечения безопасности в каналах телекоммуникаций становится все более актуальной [1]. Поэтому вопросам оценки эффективности функционирования таких сложных систем, как системы защиты информации (ЗИ), повсеместно уделяется большое внимание. Ряд солидных международных организаций разрабатывает критерии оценки эффективности данных систем. Не менее важной является и разработка подходов к оценке эффективности функционирования отдельных подсистем системы ЗИ, в частности генераторов псевдослучайных чисел (ГПСЧ) и построенных на их основе устройств формирования специальных данных (ключей, параметров алгоритмов, начальных приближений и т.п.). В большинстве своем имеющиеся на сегодняшний день публикации отражают отдельные вопросы разработки, тестирования и эксплуатации подобного рода устройств. В предлагаемой работе сделана попытка системного подхода к сертификации ГПСЧ.

Под ГПСЧ далее понимается устройство (программное или аппаратное), применяемое в системе ЗИ в целях формирования специальных данных, которые необходимы для функционирования этой системы и отвечают определенному множеству специфических требований [3–5].

Под сертификацией понимается процесс оценки эффективности функционирования ГПСЧ и принятия решения о возможности использования того или иного разработанного генератора в системе ЗИ, т.е. выдачи некоего рода «сертификата качества».

Сфера системных исследований в этой области довольно обширна, поэтому авторы не претендуют на полный охват всех положений и приложений системного подхода к средствам обеспечения безопасности вообще и к методам формирования специальных данных в частности.

Подход к решению задачи сертификации ГПСЧ, имеющий место в настоящее время, можно охарактеризовать как досистемный. Такой подход приводит к удовлетворительным результатам только в частных случаях, когда сравниваются две системы и одна из них явно лучше другой. Однако уже возникла необходимость в обобщенной оценке ГПСЧ в виде некоторой численной величины (скалярной или вектор-

ной), характеризующей его эффективность. Проводимые исследования позволили сделать следующий вывод: на данном этапе фактически лишь сформулирован ряд требований, предъявляемых к ГПСЧ [3–5], причем многие из них носят абстрактный, качественный характер. Основная теоретическая предпосылка при разработке этих требований заключается в том, что любой ГПСЧ в системах ЗИ в первую очередь должен противостоять криптоанализу и, следовательно, должен обладать высокой стойкостью.

Согласно принципам теории исследования операций и практическому опыту любая количественная оценка эффективности должна [2]:

— достаточно полно характеризовать систему в целом;
— обладать необходимой гибкостью и универсальностью;
— быть конструктивной при анализе и синтезе систем;
— отличаться достаточной простотой вычисления и использования;
— иметь ясный физический смысл.

Сущность системного подхода к оценкам эффективности ГПСЧ состоит в конструировании оценок в такой форме, которая охватывала бы все основные параметры генератора и отражала его способность решать различные функциональные задачи на соответствующем иерархическом уровне [2]. При этом под функциональными понимаются задачи по обеспечению отдельных качеств генератора.

Проведенные исследования позволяют выделить функциональные задачи и подзадачи для ГПСЧ (рис. 1). Наличие отдельных функциональных задач, сформулированных с учетом предъявленных к ГПСЧ требований, дает возможность разработать множество параметров системы $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, из которых затем можно выделить группы параметров, отражающие выполнение соответствующих функциональных задач.

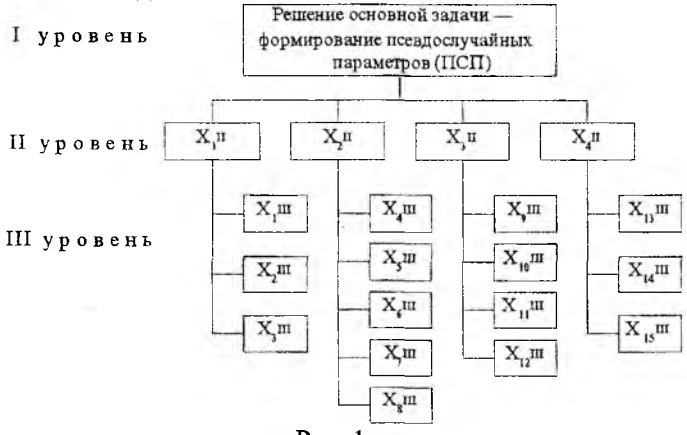

Рис. 1

На рис. 1 схематично отражены следующие задачи и подзадачи:

X_1^{II} – получение теоретически доказуемого большого периода ПСП;

X_2^{II} – обеспечение удовлетворительных статистических и корреляционных свойств ПСП;

X_3^{II} – реализация высокого уровня структурной скрытности (сложности, непредсказуемости, вычислительной неразличимости, скрытности) ПСП;

X_4^{II} – обеспечение высокой производительности ГПСЧ и приемлемой сложности реализации;

X_1^{III} – осуществление произвольной инициализации ГПСЧ по данным пользователя;

X_2^{III} – теоретическое обоснование параметров ГПСЧ, гарантирующих формирование ПСП с требуемой длиной периода и исключение вырожденных ПСП;

X_3^{III} – формирование большого объема специальных данных, инициализирующих работу ГПСЧ;

X_4^{III} – обеспечение равномерности распределения ПСЧ;

X_5^{III} – обеспечение независимости генерируемых ПСЧ;

X_6^{III} – обеспечение однородности генерируемых ПСП;

X_7^{III} – обеспечение случайности генерируемых ПСП;

X_8^{III} – реализация требуемых статистических параметров (математическое ожидание, дисперсия, эксцесс, асимметрия);

X_9^{III} – получение требуемого безопасного времени $t_б$;

X_{10}^{III} – обеспечение требуемой эквивалентной линейной сложности;

X_{11}^{III} – реализация требуемого уровня независимости (сложности по Лемпелю — Зиву);

X_{12}^{III} – обеспечение требуемой вероятности перекрытия;

X_{13}^{III} – поддержание требуемой скорости формирования ПСЧ;

X_{14}^{III} – обеспечение требуемого объема программного обеспечения или аппаратных средств;

X_{15}^{III} – осуществление функционирования на базе целочисленной арифметики.

Далее разрабатываются показатели, характеризующие степень выполнения (а следовательно, достижения цели) каждой из подзадач III уровня. Таким образом получаются частные оценки эффективности $Э_{ij}^{III}$, где i – i-я подзадача III уровня; j – соответствующая задача II уровня.

Показатель, характеризующий степень выполнения каждой из задач II уровня, строится путем композиций частных оценок $Э_{ij}^{III}$, с учетом их вклада в общую эффективность выполнения задачи II уровня. В результате находится частная оценка эффективности

$$Э_j^{II} = \sum_{i=1}^{n} \rho_{ij} Э_{ij}^{III} . \qquad (1)$$

Здесь n – количество показателей, характеризующих выполнение соответствующих подзадач III уровня; ρ_{ij} – весовой коэффициент частной оценки эффективности $Э_{ij}^{III}$.

И наконец, обобщенная оценка эффективности ГПСЧ строится путем композиции частных оценок эффективности $Э_j^{II}$ с соответствующими весовыми коэффициентами:

$$Э = \sum_{j=1}^{m} \rho_j Э_j^{II} . \qquad (2)$$

Данный подход вполне оправдал себя при построении обобщенных оценок эффективности систем связи [2]. Применение такого подхода позволяет сравнивать различные ГПСЧ как в целом (т.е. с использованием обобщенной оценки эффективности (2)), так и по каждой функциональной задаче.

Рассмотрим более подробно возможные показатели, характеризующие степень выполнения тех или иных задач или подзадач.

Функциональная задача X_1^{II} (см. рис.1) разбивается на три подзадачи $X_1^{III}, X_2^{III}, X_3^{III}$. Здесь анализируются следующие количественные показатели :

– мощность (объем) N алфавита, порождаемого генератором;

– минимальная длина периода L_{min} формируемой последовательности;

– мощность (объем) M инициализационных значений (начальных приближений) генератора.

Представляется естественным использование обобщенных показателей, объединяющих исходные. По нашему мнению, целесообразно производить такие объединения:

1. Мощность N и длина периода L_{min} представляются одним показателем — удельной мощностью формируемых ПСП

$$L_y = N/L_{min}. \qquad (3)$$

Показатель L_y характеризует эффективность использования генератором порождаемого алфавита при формировании ПСП. Чем меньше L_y, тем эффективнее генератор.

2. По аналогии с (3) объединяются мощности N и M в удельную мощность инициализационного алфавита

$$M_y = N/M, \qquad (4)$$

характеризующую эффективность использования порождаемого алфавита при инициализации генератора. Очевидно, что чем выше показатель, тем эффективнее ГПСЧ.

Решение функциональной задачи X_2^{II} может быть обеспечено при решении пяти ($X_4^{III} - X_8^{III}$) подзадач. Разработка показателей для них связана с рассмотрением вопросов статистической оценки тех или иных свойств ПСП.

Проверка статистической гипотезы о равномерности распределения генерируемых ПСЧ (подзадача X_4^{III}) осуществляется с использованием критериев Пирсона χ^2, Колмогорова $D_n\sqrt{n}$ и Мизеса ω^2 [6].

Не вдаваясь в подробности эксперимента, приведем пример расчета частной оценки эффективности ГПСЧ, показывающей, насколько успешно генерируемые последовательности проходят известные тесты.

Исследовалось две системы — аппаратный ГСЧ и программный ГПСЧ, реализованный по схеме ЛРР+random. В качестве параметров были определены следующие величины: α_{41}, α_{42}, α_{43} — проценты последовательностей, прошедших проверку по критериям Пирсона, Колмогорова и Мизеса соответственно; α_{44}, α_{45}, α_{46} — результаты проверок согласия эмпирических законов распределения случайных величин χ^2, $D_n\sqrt{n}$, ω^2 с соответствующими теоретическими распределениями. Все три проверки осуществлялись с использованием критерия Колмогорова.

В таблице сведены результаты тестирования генераторов. В ней $\alpha_i^{(1)}$ — параметры идеальной системы, т.е. максимально достижимые значения перечисленных выше параметров; $\alpha_i^{(2)}$, $\alpha_i^{(3)}$ — параметры аппаратного датчика и программного ГПСЧ;

$\eta_i^{(k)} = \dfrac{\alpha_i^{(k)}}{\alpha_i^{(1)}}$ — нормированные значения параметров;

$\Delta\eta = \dfrac{1}{3}\sum_{k=1}^{3}\left|\eta_i^{(k)} - \eta_i^{(1)}\right|$ — среднее значение разброса параметров;

$\rho_i = \dfrac{\Delta\eta}{\alpha_i^{(1)} + \alpha_i^{(2)} + \alpha_i^{(3)}}$ — значения весовых коэффициентов параметров.

№ п/п	$\alpha_i^{(1)}$	$\alpha_i^{(2)}$	$\alpha_i^{(3)}$	α_{max} (эталон)	$\eta_i^{(1)}$	$\eta_i^{(2)}$	$\eta_i^{(3)}$	$\Delta\eta$	ρ
1	100	90,7	90,7	100	1	0,907	0,902	0,064	0,0767
2	100	89,5	90,8	100	1	0,805	0,908	0,066	0,0789
3	100	93,3	94,5	100	1	0,933	0,945	0,041	0,4880
4	1	0,266	0,538	1	1	0,266	0,538	0,398	0,4790
5	1	0,905	0,514	1	1	0,905	0,511	0,194	0,2330
6	1	0,989	0,805	1	1	0,989	0,805	0,069	0,1740

Анализируя полученные данные (столбцы $\alpha_i^{(2)}$ и $\alpha_i^{(3)}$), трудно сразу определить лучший из генераторов. В одних тестах лучше зарекомендовал себя аппаратный датчик, в других — программный.

Расчет же частных показателей дал следующие результаты: $\gamma_1 = 0{,}998$ (идеальная система); $\gamma_2 = 0{,}695$ (аппаратный датчик); $\gamma_3 = 0{,}700$ (ЛРР+random).

Это означает, что оба датчика проходят тесты с «КПД» 69 и 70 %, т.е. они практически эквивалентны. Аналогичный подход реализуется и для других подзадач. Далее лишь перечислены используемые статистические критерии и предполагаемые показатели.

При проверке гипотезы о независимости генерируемых величин (подзадача X_5^{III}) используют критерий ранговой корреляции Спирмена ρ, коэффициент корреляции Пирсона r и критерий Пирсона χ^2.

Целесообразно применять следующие показатели: α_{51}, α_{52}, α_{53} — проценты последовательностей, прошедших тесты Спирмена ρ, корреляции Пирсона r и тест Пирсона.

При проверке гипотезы об однородности распределения (подзадача X_6^{III}) используют критерии Пирсона χ^2, Колмогорова $D_n\sqrt{n}$, Мизеса ω^2 [6]. В связи с этим анализируются показатели α_{61}, α_{62}, α_{63} – проценты последовательностей, прошедших тесты по критериям Пирсона, Колмогорова и Мизеса.

При проверке гипотезы о случайности генерируемых величин (подзадача X_7^{III}) употребляются показатели α_{71}, α_{72}, α_{73}, α_{74} – проценты последовательностей, прошедших тесты серий, инверсий, покер-тест и энтропийный тест.

При проверке статистических характеристик генерируемых ПСП (подзадача X_8^{III}) вычисляются показатели α_{81}, α_{82}, α_{83}, α_{84} – проценты последовательностей, прошедших тесты на математическое ожидание, дисперсию, тесты по корреляционным функциям и по коэффициенту корреляции Пирсона.

Рассмотрим функциональную задачу X_3^{II}, решение которой обусловлено решением подзадач X_9^{III} — X_{12}^{III}.

Здесь целесообразно анализировать такие показатели: 1) безопасное время $t_б$ ГПСЧ (подзадача X_9^{III}),

$$t_б = P_д \frac{M_0}{3{,}154 \cdot 10^7 \gamma},$$

где $P_д$ — допустимая вероятность решения задачи криптоанализа; M_0 — количество операций, необходимых для проведения вычислений; γ — быстродействие вычислительной системы, используемой криптоаналитиком; 2) линейную эквивалентную сложность формируемых ПСП (подзадача X_{10}^{III}); 3) степень сжатия ξ формируемых ПСП (подзадача X_{11}^{III}); 4) вероятность перекрытия (подзадача X_{12}^{III}), т.е. вероятность события, состоящего в том, что найдется любая пара выходных ПСП длиной r (сформированных из общего числа m), которые являются сегментами ПСП с периодом $l > r$ и отличаются друг от друга сдвигом на r–1 тактов.

Верхняя граница вероятности перекрытия

$$P_n \le C_m^2 (r-1)/l.$$

Рассмотренные показатели после расчета объединяются в обобщенный показатель $Э_3^{II}$ согласно выражению (1).

Обеспечение выполнения функциональной задачи X_4^{II} можно оценить с помощью общеизвестных методов, применяемых при проектировании средств вычислительной техники и разработке ПО [2; 6].

И наконец, имея все частные показатели эффективности $Э_j^{II}$, можно согласно выражению (2) вычислить обобщенную оценку эффективности ГПСЧ.

Для получения более объективной оценки эффективности необходимо обосновать и рассчитать весовые коэффициенты каждого показателя, отражающие вклад решения каждой подзадачи в общую оценку эффективности. Данные весовые коэффициенты могут быть

получены на основе методов экспертных оценок [7] и являются предметом дальнейших исследований.

Рассмотрим вопросы реализации процесса оценки эффективности функционирования ГПСЧ.

Последний, как и любая программная или техническая система, имеет свой жизненный цикл, который можно разбить на этапы проектирования, внедрения, эксплуатации и уничтожения (утилизации). Соответственно и весь процесс оценки и контроля эффективности функционирования ГПСЧ следует привязать к жизненному циклу генератора.

На этапе проектирования и внедрения ГПСЧ необходимо проводить глубокие и всеобъемлющие исследования эффективности функционирования ГПСЧ. На этом этапе характерно отсутствие жестких временных рамок при проведении проверок различных свойств и характеристик генератора. Важно получить как можно более полную и исчерпывающую информацию о функционировании ГПСЧ, которая нужна для принятия решения о возможности использования генератора в проектируемой системе ЗИ, а на этапе внедрения системы в целом позволяет выдать «сертификат качества» на генератор.

Данная задача может быть решена с помощью разработанного программно-технического комплекса (системы) тестирования, осуществляющего комплексную оценку эффективности генератора (комплексный контроль).

Целью комплексного контроля являются оценка эффективности функционирования ГПСЧ, исследование свойств ПСП и измерение всех ранее рассмотренных характеристик и показателей ГПСЧ с целью предоставить сертификат (разрешение), позволяющий использовать оцениваемый генератор в системе ЗИ.

На этапе эксплуатации системы ЗИ (и ГПСЧ как ее составляющей) необходимо осуществлять оперативный и текущий контроль за исправностью ГПСЧ. С этой целью в систему ЗИ встраиваются средства оперативного и текущего контроля эффективности функционирования ГПСЧ.

Цель оперативного контроля – оперативное (даже сиюминутное) контролирование состояния системы генерации псевдослучайных векторов (параметров) и «качества» формируемых ПСП.

Оперативный контроль выполняется после каждого процесса формирования псевдослучайных (случайных) параметров и последовательностей, т.е. осуществляется тестирование формируемых ключей, вставок, параметров и т.п. Отсюда вытекает необходимость укладываться в жесткие временные рамки, поскольку проведение контроля не должно существенно снижать быстродействие системы ЗИ в целом (т.е. не должна снижаться эффективность функционирования системы

ЗИ). В связи с этим подсистема оперативного контроля должна включать в себя средства быстрого статистического контроля (использование критерия серий) и различного рода заглушки (например, на ключи-близнецы, на запрещенные типы ключей). Таким образом, задача оперативного контроля — не допустить использования криптографически слабых, запрещенных параметров при шифровании, аутентификации, хешировании, наложении цифровой подписи и др.

Цель текущего контроля — оценка работоспособности системы генерации псевдослучайных векторов (параметров) и последовательности, а также своевременное выявление каких-либо нарушений в функционировании ГПСЧ. Текущий контроль выполняется ежедневно (еженедельно), например в начале рабочего дня или в другое специально отведенное время (в случае круглосуточного функционирования системы ЗИ). Он проводится с использованием более широкого набора средств, чем при оперативном контроле. В процессе текущего контроля производятся тестирование ПСП, оценка свойств ПСП (проверки на независимость, случайность), снимаются технические контрольные параметры ГПСЧ (если ГПСЧ реализован аппаратно). Но, поскольку здесь тоже приходится учитывать временные рамки, контроль осуществляется не столь глубоко (например, оценка эффективности реализуется по меньшему количеству параметров, не применяются тесты, требующие значительных временных затрат).

На рис. 2 виды контроля расположены на временной оси в соответствии с этапами жизненного цикла генератора.

Рис. 2

Таким образом, генератор охватывается тремя видами контроля (рис 3).

Проведенные исследования позволили сформулировать следующие задачи, которые предстоит решить.

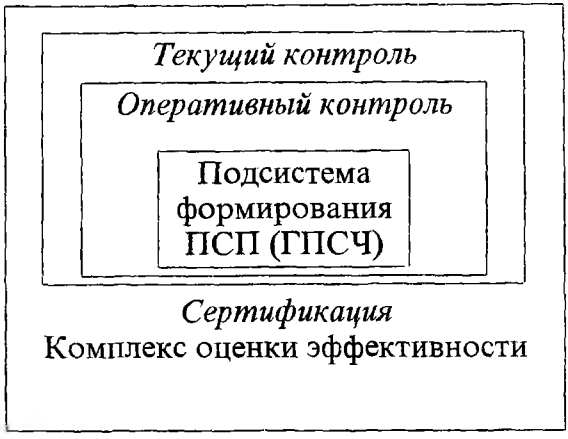

Рис. 3

1. Расчет весовых коэффициентов — как групп параметров, так и отдельных параметров. Данная задача может быть решена с использованием методов экспертного опроса.

2. Разработка методики сертификации ГПСЧ и программно-аппаратного комплекса сертификации.

3. Разработка параметров и характеристик ГПСЧ, используемых при расчетах общесистемных показателей.

Решение этих и других задач позволит получить объективную оценку эффективности функционирования ГПСЧ, что, в свою очередь, изменит подходы к оценке эффективности функционирования системы ЗИ в целом.

Список литературы: 1. *Месси Дж. Л.* Введение в современную криптологию // ТИИЭР. 1988. Т. 76, № 5. С. 24 – 42. 2. *Окунев Ю.Б., Плотников В.Г.* Принципы системного подхода к проектированию в технике связи. М.: Связь, 1976. 183 с. 3. *Ritter T.* The efficient generation of cryptographic confusion sequences // Cryptologic. 1991.Vol. XV, N 2. P. 81—139. 4. *Guefle J.E.* Computer implementation of random numbers generators // J. of computational and appl. mathematics. 1991. N 31. P. 119—125. 5. *Потий А.В.* Предложения по оценке эффективности функционирования генератора псевдослучайных чисел // Системы информационного взаимодействия. Х., 1996. С. 76—83. 6. *Большев Л.Н., Смирнов Н.В.* Таблицы математической статистики. М.: Наука, 1965. 460 с. 7. *Литвак Б.Г.* Экспертная информация. Методы получения и анализа. М.: Радио и связь, 1982. 182 с.

Харьковский государственный университет

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 19.06.97