УДК 621.3.06

Е. В. ПОПОВИЧ, А. В. ПОТИЙ, канд. техн. наук

МЕТОДИКА ОПЕРАТИВНОГО СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ БОЛЬШОЙ ДЛИНЫ

Шифры с одноразовой гаммой, как единственные теоретически стойкие шифры, всегда привлекали внимание разработчиков. Теоретическая стойкость таких шифров была доказана Шенноном [1], однако сложность их практической реализации сдерживает их активное использование на практике. Рассматривая особенности данных систем, следует отметить, что их стойкость полностью определяется качеством одноразовой гаммы [2].

Достижения в технологиях хранения данных большого объема и использование их в современных информационных технологиях несколько облегчает решение практических проблем реализации схем типа шифр Вернама. Однако остается нерешенной задача получения доказательств «качества» одноразовой гаммы большой длинны, записанной на носитель.

На практике возникает проблема создания качественного ключа – случайной гаммы заданного качества. Если учитывать значительный объем гаммы (десятки и сотни мегабайт), то наиболее очевидны такие проблемы:

1. Каково максимально допустимое время тестирования последовательности?
2. Какие статистические тесты должны применяться для тестирования?
3. Сколько тестов необходимо применить для получения валидной оценки?

Ответы на эти вопросы позволяют уточнить технические характеристики систем защиты: пропускную способность, период смены ключей, количество ключей, необходимое для поддержки заданной конфигурации сети.

Сегодня уже предложен ряд пакетов статистического тестирования псевдослучайных последовательностей (ПСП). Это пакеты NIST STS, DIEHARD, RIPE, Crypt-X, которые предлагают достаточно обоснованные методику и набор статистических тестов. Однако, они ориентированы прежде всего на, если так можно выразиться, аттестацию источника псевдослучайной последовательности. Проведенный авторами поиск позволил сделать вывод о том, что средств и методик проверки качества отдельно взятой ПСП большого периода (более 10^9 бит) на сегодняшний день не существует. Необходимость в ряде случаев практической реализации систем, подобных системе Вернама, делает задачу создания таких методик достаточно актуальной.

В данной работе предлагается методика оперативного статистического тестирования ПСП большой длинны. Методика основана на использовании стандартного пакета тестов NIST STS. Для выбора минимально необходимого набора тестов предлагается новый показатель оценки результатов тестирования – коэффициент крутизны статистической характеристики.

1 Этапы жизненного цикла формирования ПСП большого периода

В процессах формирования случайных последовательностей большой длины (СПБД) можно выделить четыре основных этапа:

1. Проектирование и создание генератора (источника) СПБД.
2. Приемка разработанных (оценка существующих) генераторов и постановка на эксплуатацию.
3. Получение случайной последовательности и оперативное тестирование работоспособности генератора во время эксплуатации.
4. Периодическое, детальное тестирование генератора.

Каждый из этих этапов характеризуется перечнем основных решаемых задач и требований к порядку и условиям их решения.

1. Проектирование и создание генераторов. Основная задача – создание генератора. Характеризуется отсутствием жестких требований к временным параметрам. Это дает возможность использовать большое (неограниченное) количество разнообразных тестов. Набор тестов и методика тестирования (дальше методика тестирования) должны давать детальную (инструментальную) картину генератора, а также позволять детально сравнивать несколько результатов тестирования с целью выявления изменений в ходе разработки.

2. Приемка разработанных (оценка существующих) генераторов и постановка на эксплуатацию. Основная задача – определить, отвечает ли генератор заданным требованиям. Характеризуется отсутствием жестких требований к временным характеристикам, что дает возможность использовать большое количество тестов. В отличие от первого этапа, методика тестирования должна дать оценку генератора, по которой принимается решение о пригодности.

3. Получение заданной последовательности и оперативное тестирование работоспособности генератора во время эксплуатации. Основная задача – получить случайную последовательность с заданными параметрами. Вторая задача – осуществление оперативного контроля работоспособности и исправности генератора. Характеризуется, как правило, жесткими временными ограничениями. На данном этапе вступают в противоречие требования по скорости получения случайной последовательности и ее качеству. Методика тестирования должна обеспечить отбраковку последовательностей, не удовлетворяющих заданным требованиям. При изменении количества брака принимается решение о работоспособности генератора – выходе генератора из строя.

4. Периодическое, детальное тестирование генератора. Основная задача – оценить отклонения в свойствах генератора и оценить его пригодность к дальнейшей эксплуатации. Характеризуется нежесткими требованиями по времени, что дает возможность использовать расширенное количество тестов по сравнению с третьим этапом. Методика тестирования должна выявлять отклонения и сбои в работе генератора с целью принятия решения об исправности и прогнозирования линии его дальнейшего поведения.

Очевидно, что набор тестов и методик тестирования на каждом этапе должны коррелировать с назначением генератора. Следует обратить внимание на то, что методики тестирования на первом и четвертом этапах направлены на выявление технических особенностей генераторов. В то время как методики тестирования на втором и третьем этапах направлены на решение конечной задачи – получение случайных последовательностей с заданным качеством.

Анализ и практическое использование существующих пактеов и методик статистического тестирования СПБД показал, что пакеты NIST STS, DIEHARD, RIPE и Crypt-X предназначены для оценки существующих генераторов, т.е. применимы на втором этапе жизненного цикла. В американском стандарте FIPS-140-2 предложена методика для оперативного тестирования работоспособности генератора во время работы [3]. Однако методика FIPS-140-2 непригодна для тестирования СПБД, поскольку по требованиям стандарта тестированию подлежат последовательности длиной $L = 2*10^4$. Принятие решения осуществляется по интервальному критерию, который обладает недостаточной гибкостью. Это ограничивает возможности данной методики относительно формирования надежного решения о качестве СПБД.

2 Методика оперативного тестирования СПБД

Рассматривая подходы к созданию методик оперативного тестирования, можно выделить несколько основных этапов:

1. Определение требований к случайной последовательности.
2. Определение критериев принятия решения о соответствии последовательности требованиям.

3. Определение перечня тестов и порядка их использования для реализации критерия.

При построении методик оперативного тестирования необходимо учитывать, что качество последовательности определяется количеством и содержанием тестов, которым она подвергается. С другой стороны, чем больше тестов, тем больше ошибка первого рода и соответственно меньше КПД[1] генератора. Хотя ошибка второго рода в этом случае тоже уменьшается, что может являться определяющим для некоторого класса систем.

В [4] приведена оценка ошибки первого A рода в зависимости от количества независимых тестов n и уровня значимости α:

$$A = 1 - (1 - \alpha)^n. \qquad (1)$$

Исходя из (1) видно, что для пакетов NIST STS, DIEHARD, RIPE ошибка первого рода является достаточно большой, что приводит к практической неприменимости данных методик тестирования для получения последовательности с заданным качеством и оперативного тестирования работоспособности генератора во время работы. В частности для NIST STS ошибка первого рода составляет 0.85. Результаты практических испытаний NIST STS показывают, что из генеральной выборки, состоящей из 100 последовательностей[2], все 189 тестов проходят примерно 16-18 (КПД = 16 – 18%), при этом вся генеральная выборка проходит тестирование данным пакетом.

Для снижения ошибки первого рода необходимо уменьшать количество тестов. Исходя из формулы [4]

$$n = \left[-\alpha^{-1} \cdot \ln(1 - A) \right], \qquad (2)$$

при ошибке первого рода A=0,1 и уровне значимости α = 0,01 получаем количество тестов n = 10.

Для разработки методики оперативного тестирования в качестве базового набора тестов предлагается использовать тесты NIST STS. Такой выбор сделан в связи с тем, что по сравнению с остальными пакетами для NIST STS существует доказательство независимости используемых тестов [5].

Как отмечалось, в состав данного пакета входит 16 базовых тестов, некоторые из которых имеют несколько «подтестов». Общее количество проверок составляет 189. В связи с этим при разработке методики оперативного тестирования на базе NIST STS необходимо определить тесты, которые необходимо будет исключить. В качестве показателя, на основе которого будет приниматься решение об исключении того или иного теста, предлагается выбрать чувствительность каждого теста к определенным искажениям в тестируемых последовательностях. Для определения данного показателя предлагается следующая методика оценки:

1. Выбирается генеральная выборка длиной 10^8 бит, которая проходит тестирование пакетом NIST STS. В качестве параметров тестов выбираются параметры, рекомендуемые в [5].

---

[1] Под КПД генератора будем понимать отношение количества последовательностей заданной длины, прошедших тестирование N_t, к общему количеству протестированных последовательностей N_o. $КПД = \frac{N_t}{N_o} \cdot 100\%$

[2] В качестве датчика случайных чисел использовалось изделие "Гряда-31".

2. В каждую последовательность длиной 10^6 бит вносятся $I, I = \{1,10,100\}$ блоков искажений. Суммарный процент искажений составляет от 0,1 – 1%[3] с шагом 0,1%. Для испытаний, исходя из предложенного варианта криптоанализа [1], использовались два типа искажающих последовательностей:

– сплошные нули[4] 000000…;

– меандр 01010101….

3. Каждая генеральная выборка подвергается тестированию.

4. По результатам тестирования оценивается количество последовательностей N, которые прошли тестирование конкретным тестом.

Для тестов с более чем одним «подтестом» N вычислялось как среднее арифметическое.

С целью качественной оценки результатов тестирования введем коэффициент крутизны статистической характеристики K_S, который определяется согласно выражению

$$K_S = \frac{\left(N_0 - N_1\right)}{P_1}, \tag{3}$$

где: N_0 – начальное значение количества пропущенных последовательностей при отсутствии искажений;

N_1 – количество пропущенных последовательностей при одном проценте искажений;

P_1 – значение процента искажений, при котором количество пропущенных последовательностей равно нулю, в противном случае P_1=1.

В качестве порогового значения для критерия принятия решения возьмем значение $K = 100$. Т.е. значение крутизны характеристики, при котором количество последовательностей, прошедших тестирование, устанавливается равным 0 при 1% искажений.

По результатам тестирования получены данные, приведенные на рис. 1-6[5], где используются следующие сокращения для названий тестов (табл. 1):

Таблица 1

1. Frequency (monobit) Test – «Frequency».	9. Maurer's «Universal Statistical» Test – «Universal».
2. Frequency Test within a Block – «Bl. Frequency».	10. Lempel-Ziv Compression Test – «Lemp.-Ziv».
3. Runs Test – «Runs».	11. LINEAR COMPLEXITY TEST – «LIN. COMPL.».
4. Test for the Longest Run of Ones in a Block – «L. Run».	12. Serial Test – «Serial» (2).
5. Binary Matrix Rank Test – «Rank».	13. Approximate Entropy Test – «apen».
6. Discrete Fourier Transform (Spectral) Test – «fft».	14. Cumulative Sums (Cusum) Test – «Cusum» (2).
7. Non-overlapping Template Matching Test – «Non-ov.Templ.» (148).	15. Random Excursions Test – «Rnd. Exc.» (8).
8. Overlapping Template Matching Test – «Ov. Templ.».	Random Excursions Variant Test – «Rnd. Exc.V» (18).

На рисунке 1 представлены результаты, полученны для искажения типа «00000000…» и одного искаженного блока. На рисунке 2 – для искажений типа «00000000…» и 10 искаженных блоков. На рисунке 3 – для искажений типа «00000000…» и 100 искаженных блоков. На рисунке 4 – для искажений типа «01010101…» и 1 искаженного блока. На рисунке 5 – для искажений типа «01010101…» и 10 искаженных блоков. На рисунке 6 – для искажений типа «01010101…» и 100 искаженных блоков.

[3] Для последовательности длиной 10^6 бит, 1% составляет 1250 байт.

[4] При искажениях «сплошные единицы» и «сплошные нули» результаты тестирования практически совпадают.

[5] В скобках после названия указано количество проводимых тестов.

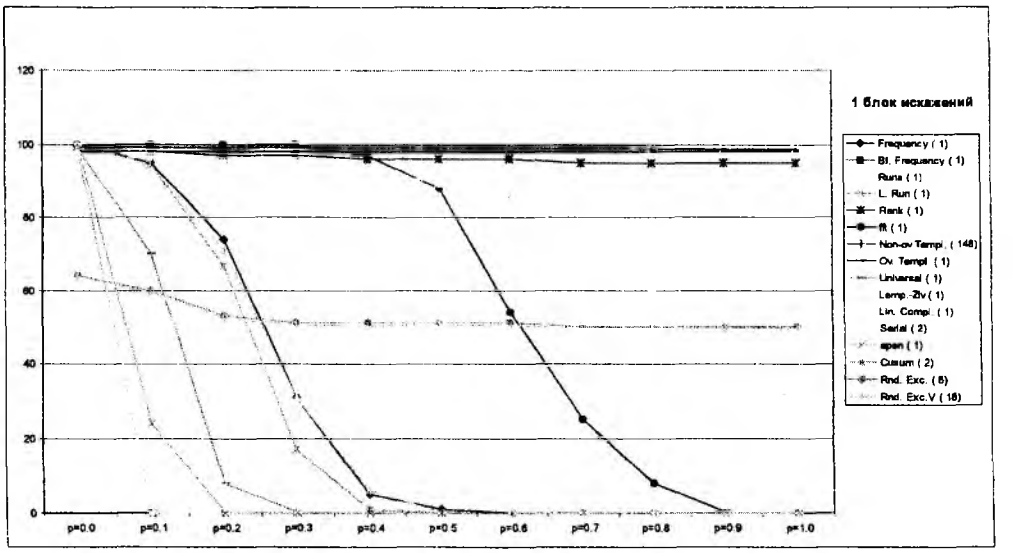

Рис. 1

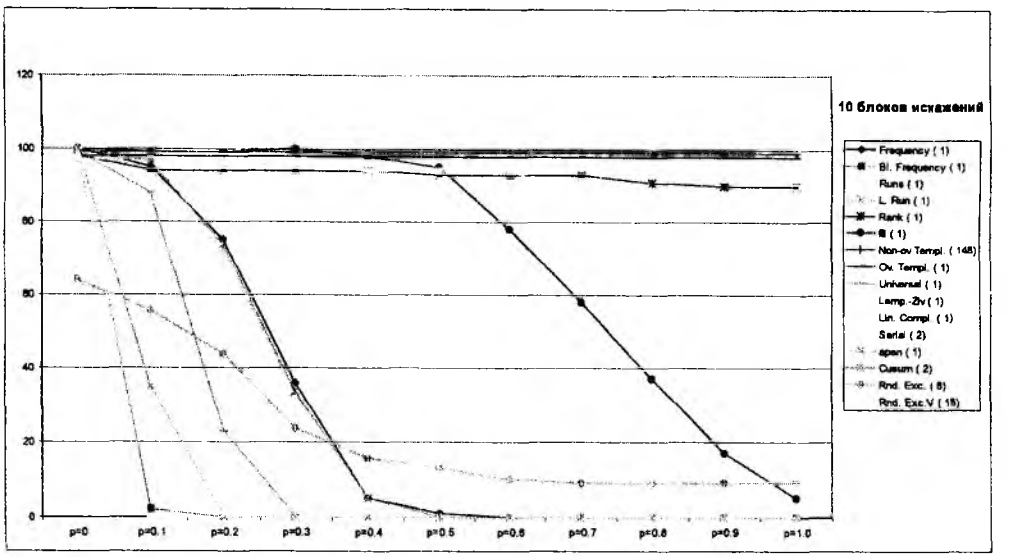

Рис. 2

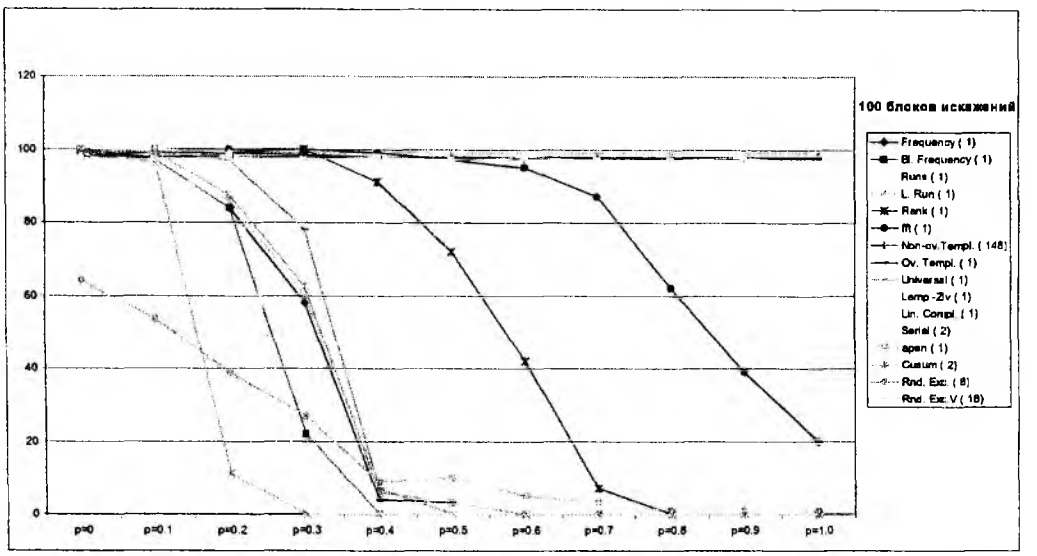

Рис. 3

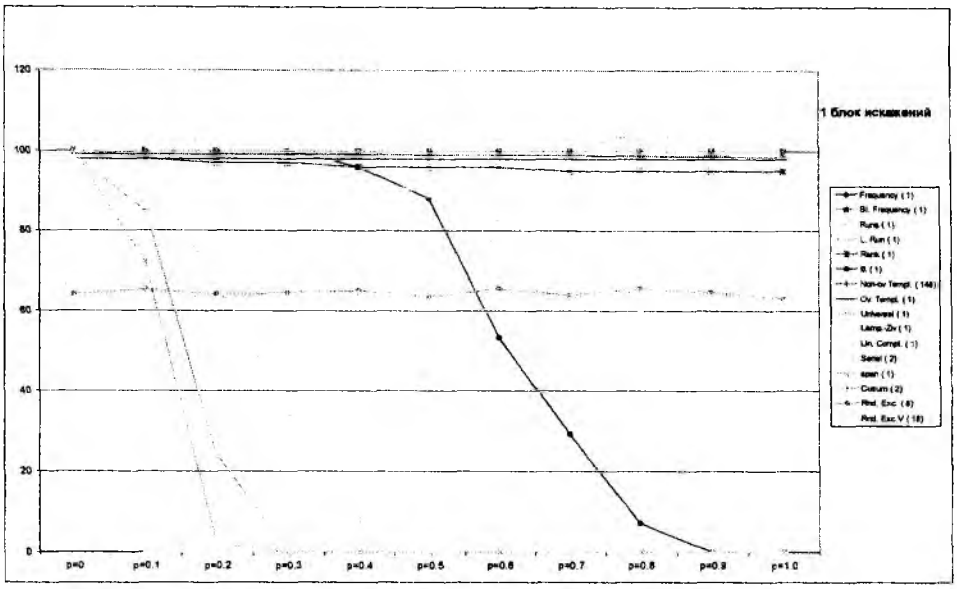

Рис. 4

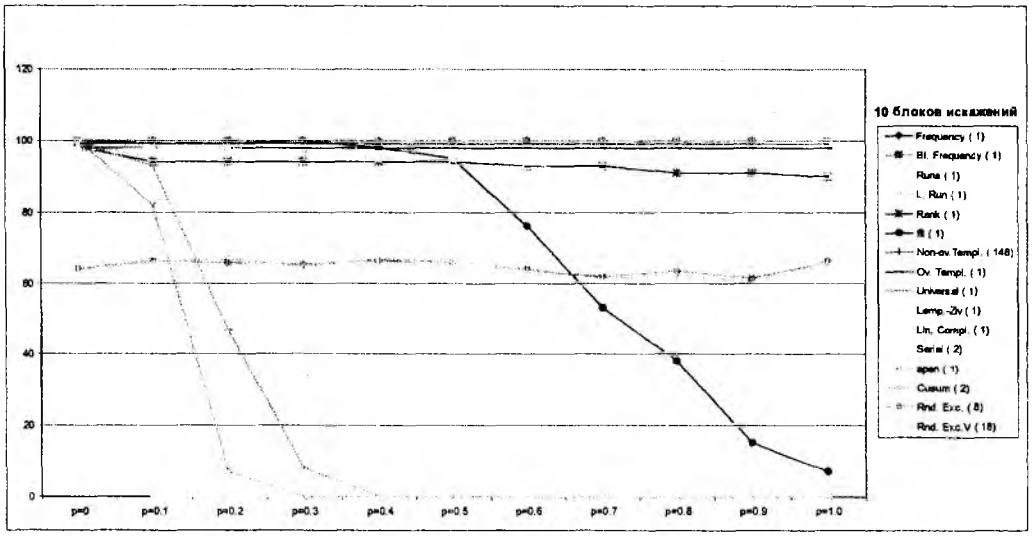

Рис. 5

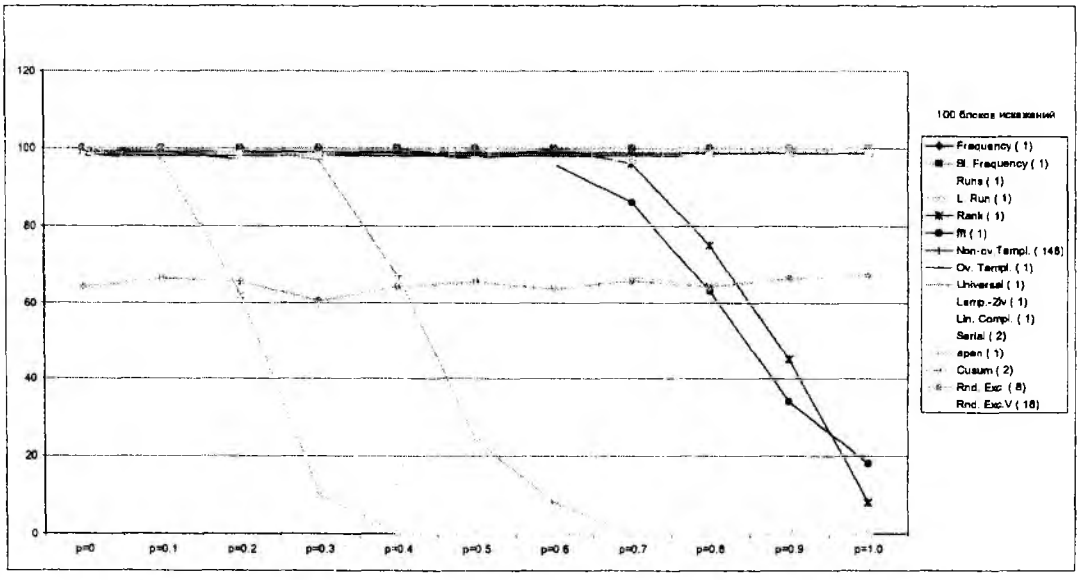

Рис. 6

Обобщенные результаты тестирования коэффициента крутизны статистической характеристики K_S сведены в табл. 2.

Таблица 2

Тип искажений	00000000			01010101		
Количество искаженных блоков	1	10	100	1	10	100
Frequency (1)	**166,667**	**166,667**	**166,667**	0,000	0,000	0,000
Bl. Frequency (1)	**990,000**	**495,000**	**247,500**	-1,000	-1,000	-1,000
Runs (1)	**198,000**	**198,000**	**165,000**	**165,000**	**165,000**	**141,429**
L. Run (1)	0,000	0,000	0,000	0,000	0,000	0,000
Rank (1)	3,000	8,000	**122,500**	3,000	8,000	90,000
fft (1)	**111,100**	95,000	80,000	**111,111**	93,000	82,000
Non-ov.Templ. (148)	0,595	0,074	1,601	0,576	0,094	0,621
Ov. Templ. (1)	0,000	0,000	0,000	0,000	0,000	0,000
Universal (1)	**330,000**	**330,000**	**198,000**	**330,000**	**247,500**	**141,429**
Lemp.-Ziv (1)	**1000,000**	**1000,000**	**333,333**	**1000,000**	**1000,000**	**250,000**
Lin. Compl. (1)	69,000	28,000	1,000	69,000	28,000	-1,000
Serial (2)	**328,333**	**328,333**	**246,250**	**328,333**	**328,333**	**246,250**
apen (1)	**500,000**	**500,000**	**333,333**	**333,333**	**333,333**	**250,000**
Cusum (2)	**200,000**	**200,000**	**166,667**	0,000	0,000	0,000
Rnd. Exc. (8)	14,000	55,000	63,125	1,000	-2,000	-3,125
Rnd. Exc.V (18)	13,945	54,445	62,333	0,889	-2,389	-4,333

Применив описанный выше критерий, разделим все тесты на группы в зависимости от значения K_S:

1. Тесты, для которых K_S: всегда больше 100: Apen (1), Serial (2), Lemp.-Ziv (1), Universal (1) Runs (1).
2. Тесты, для которых K_S иногда больше 100: Cusum (2) fft (1), Rank (1), Bl. Frequency (1), Frequency (1).
3. Тесты, для которых K_S всегда меньше 100: Rnd. Exc.V (18), Rnd. Exc. (8), Lin. Compl. (1), Ov. Templ. (1), Non-ov.Templ. (148), L. Run (1).

Таким образом, можно сделать вывод, что для построения методики оперативного тестирования случайных последовательностей из набора тестов NIST можно использовать следующие тесты:

1. Approximate Entropy Test.
2. Serial Test (2).
3. Lempel-Ziv Compression Test.
4. Maurer's «Universal Statistical» Test.
5. Runs Test.
6. Cumulative Sums (Cusum) Test (2).
7. Frequency Test within a Block.
8. Frequency (monobit) Test.

С учетом того, что Serial Test и Cumulative Sums (Cusum) Test реально выполняют по 2 теста, получаем общее количество тестов 10, что совпадает с оценкой, полученной по формуле (2).

Проведя тестирование данным набором тестов, получили, что из 100 тестируемых последовательностей тест прошло 95 (КПД генератора – 95%). Данное значение попадает в интервал ошибки первого рода 0,1.

Выводы

В данной статье предложена методика отбора тестов для формирования пакета оперативного тестирования, основанная на проверке чувствительности ряда независимых тестов. Предложен показатель и критерий отбора статистических тестов из пакета NIST STS. Обосновано количество и содержание тестов, отобранных по согласно предложенному показателю и критерию. Экспериментально подтверждена сходимость теоретической и эмпирической оценок необходимого количества тестов для оперативного тестирования. Использование полученных результатов позволяет построить методику оперативного тестирования, которая удовлетворяет временным ограничениям на тестирования СПБД на специализированных АРМах генерации таких последовательностей. Направлением дальнейших исследований является разработка пакета оперативного тестирования и расчет технических характеристик АРМа тестирования.

Список литературы: 1. *Шеннон К.Э.* Теория связи в секретных системах // Работы по теории информации и кибернетике (сб. статей). М.: Изд-во иностр. лит., 1963. 2. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.,* Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2001. 3. FIPS PUB 140-2 Security Requirements For Cryptographic Modules, 1999. 4. *Гулак Г.М., Ковальчук Л.В.,* Підходи до визначення випадкових послідовностей // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. 2001. Вип. 3. 5. NIST Special Publication 800-22. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

Департамент специальных телекоммуникационных систем и защиты информации
Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 15.04.2003