

41¹⁹/₂₋₉

Промышленные Контроллеры

ACS 7.2013

ISSN: 1561-1531

Industrial Automatic Control Systems and Controllers

PPC-3120 / 3100 Безвентиляторный панельный компьютер с процессором Intel® Atom™ D2550 Спроектировано для машиностроения



PPC-3120/3100 12.1"/10.4"-дюймовый безвентиляторный

панельный компьютер с процессором Intel® Atom™ D2550

- * Процессор Intel Atom D2550 с низким энергопотреблением
- * Поддержка питания DC 12~30V input support
- * Безвентиляторное исполнение с диапазоном рабочих температур 0~50 °C
- * Встроенный интерфейс mSATA, 4 COM порта, 4 порта USB



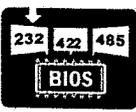
Легкодоступные порты ввода-вывода
Порты ввода/вывода сзади, легкий монтаж в панель, ничто не мешает.



Автоматическая регулировка яркости
Светодиодный дисплей с автоматической регулировкой яркости, два режима работы, устанавливаемые BIOS или ПО.



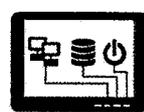
Питание через COM-порт
Последовательный порт с возможностью подачи 5V/12V, выбираемой через BIOS, повышает эффективность системной интеграции.



Управление портами в BIOS
Режимы RS-232/422/485 выбираются в BIOS.



Широкий диапазон напряжений питания
Поддерживает питание 12-30V для надежной работы в промышленных средах.



Светодиодные индикаторы
Светодиодный индикатор на передней панели отображает состояние системы включая наличие питания, доступ к накопителю и сети.



<http://www.advantech.ru/applied-computing-systems/panel-pc/>

ADVANTECH

Enabling an Intelligent Planet

Advantech Россия
Ул. Профсоюзная, 108, 6 этаж, оф. 648
Москва, 117437, Россия
Тел.: +7 (495) 232-16-92
Email: info@advantech.com
Web: www.advantech.ru



Промышленные АСУ Контроллеры 7/2013

ООО ИЗДАТЕЛЬСТВО «НАУЧТЕХЛИТИЗДАТ» ISSN 1561-1531

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ПРОИЗВОДСТВЕННЫЙ ЖУРНАЛ

СОДЕРЖАНИЕ

РОССИЙСКАЯ
ГОСУДАРСТВЕННАЯ
БИБЛИОТЕКА

АСУ ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ	
Морозова Т.Ю. Разработка автоматизированной системы управления потоками данных на предприятии (2 часть)	3
Перминов Д.А. Алгоритм работы системы управления аппаратом для сушки нити	13
НОВЫЕ ТЕНДЕНЦИИ И ТЕХНОЛОГИИ В ЭФФЕКТИВНОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ	
Карташев М.И., Николаев А.Б., Остроух А.В., Строганов В.Ю., Строганов Д.В. Инструментальная среда интеграции программных приложений для организации обучения персонала предприятий	17
НОВОСТИ СИСТЕМОСТРОЕНИЯ	26
МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ	
Лось А.Б. Об оценке суммы конечно-зависимых случайных величин в связи с исследованием алгоритмов защиты информации	31
<i>Интеллектуальные системы</i>	
Боголюбов Д.П., Бухаров О.Е., Мизикин А.А. Разработка оболочки системы поддержки принятия решений с использованием эволюционных алгоритмов	37
Игнатов А.С., Круг П.Г. Автоматизация настройки нечеткого алгоритма управления автомобильными потоками на перекрестках с различной конфигурацией	46
<i>Программное обеспечение</i>	
Обходский А.В., Овчинников А.В., Голобоков Ю.Н., Москалев В.А., Чучалин И.П., Егорова О.С. Программный комплекс обработки и хранения экспериментальных данных с исследовательских электрофизических установок	50
ТЕХНИЧЕСКИЕ СРЕДСТВА АСУТП	
<i>Сетевые многофункциональные контроллеры</i>	
Глебов Р.С., Бондаренко А.Г. Моделирование системы управления в реальном времени	56
<i>Оборудование для измерений и автоматизации производства</i>	
Нестеренко Т.Г., Барбин Е.С., Коледа А.Н. Моделирование влияния технологических дефектов на характеристики упругих подвесов микроэлектромеханических систем	60
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	
Нижегородов А.В., Закалкин П.В., Стародубцев П.Ю., Кабанов А.С. Роль мониторинга в системе обнаружения, предупреждения и ликвидации последствий компьютерных атак	67
ХРОНИКА	72

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ ЖУРНАЛА
ООО «САТАГЕ»
ООО Издательство
«НАУЧТЕХЛИТИЗДАТ»

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций
Свидетельство о регистрации ПИ № 77-1141
Подписной индекс 79216

ГЛАВНЫЙ РЕДАКТОР

Морозова Т.Ю. – д-р техн. наук

Зам. главного редактора

Рыбин В.М. – д-р техн. наук, профессор

ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ

Мазурова С.В.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Абрамов С.М. – чл.-корр. РАН, Россия
Аксенов Ю.П. – д-р техн. наук, профессор, Россия
Алексеев А.А. – канд. техн. наук, Россия
Ахремчик О.Л. – канд. техн. наук, доцент, Россия
Буланова Т.А. – д-р техн. наук, профессор, Россия
Галченко Ю. П. – д-р техн. наук, Россия
Голубятников И.В. – д-р техн. наук, профессор, Россия
Громов Ю.Ю. – д-р техн. наук, профессор, Россия
Золотарев С.В. – канд. техн. наук, Россия
Карась В.И. – д-р физ.-мат. наук, Украина;
Кохреидзе Д. – д-р техн. наук, профессор, Грузия;
Лаверов Н.П. – академик РАН, Россия
Лошак Ж. – д-р физики, президент Фонда Луи де Бройля, член Парижской АН, Франция
Ротач В.Я. – д-р техн. наук, профессор, Россия
Самхарадзе Т.Г. – д-р техн. наук, профессор, Россия
Самосадный В.Г. – д-р техн. наук, профессор, Россия
Толмаская И.И. – канд. техн. наук, Россия
Уваров А.В. – канд. техн. наук, Россия
Федик И.И. – чл. корр. РАН, Россия
Фролов С.В. – д-р техн. наук, профессор, Россия
Харазов В.Г. – д-р техн. наук, профессор, Россия
Чебышов С.Б. – д-р техн. наук, профессор, Россия
Щербаков Н.С. – д-р техн. наук, профессор, Россия
Шкабардия М.С. – д-р техн. наук, профессор, Россия
Штейнберг Ш.Е. – д-р техн. наук, профессор, Россия

ОФОРМЛЕНИЕ, ВЕРСТКА, ДИЗАЙН

Шабловская И.Ю.

Статьи, поступающие в редакцию, рецензируются. Публикация статей бесплатна. Правом внеочередной публикации пользуются аспиранты и докторанты. Материалы, опубликованные в настоящем журнале, не могут быть полностью или частично воспроизведены, тиражированы и распространены без письменного разрешения редакции. При перепечатке отдельных частей статей ссылка обязательна.

Подписано в печать 26.06.2013.
Формат 60×88 1/8. Бумага кн.-журн. Печать офсетная.
Усл.-печ. л. 8,7. Усл. кр.-отт. 13,74. Уч.-изд. л. 13,48. Зак. 534.
Тираж 5400 экз.

Адрес редакции: Москва, 107258, Алымов переулок, дом 17, строение 2. Тел.: +7(499) 168-23-28, +7(916) 008-23-28.
E-mail: promasu@mail.ru www.tgizd.ru

По вопросам приобретения журнала обращаться в бухгалтерию издательства по тел.:
Тел./факс: +7 (499) 168-13-69. E-mail: buchnauch@mail.ru

Оригинал-макет и электронная версия подготовлены ООО Издательство «Научтехлитиздат»
Отпечатано в ООО Издательство «Научтехлитиздат». 107258, Москва, Алымов пер., д. 17, стр. 2

Математическое обеспечение АСУ

А.Б. Лось

канд. техн. наук, доцент

E-mail: alos@hse.ru

(Московский институт электроники
и математики Национального исследовательского
университета "Высшая школа экономики")
Москва, Российская Федерация

Об оценке суммы конечно-зависимых
случайных величин в связи
с исследованием алгоритмов
защиты информации

В работе исследуется распределение суммы конечно-зависимых случайных величин, необходимость изучения которого возникает в ряде задач защиты информации. Одной из таких задач является исследование свойств выходной последовательности фильтрующего генератора, входящего в состав ряда отечественных и зарубежных алгоритмов защиты информации. Полученные в статье оценки близости исследуемого распределения к распределению суммы независимых случайных величин позволяют сделать вывод о качестве преобразования, реализуемого данным генератором.

Ключевые слова: конечно-зависимые величины; аппроксимирующая сумма; расстояние по вариации.

A.B. Los

Cand. of Techn. Sciences, Associate Professor

E-mail: alos@hse.ru

(Moscow Institute of Electronics and Mathematics
National Research University
"Higher School of Economics")
Moscow, Russian Federation

On the Assessment of the Amount
of Course-dependent Random Variables
in Connection with the Study
of Algorithms Information Protection

In this paper, we investigate the distribution of the sum of finitely dependent random variables, the need to examine which arises in a number of tasks of the information security. One such task is the study of the properties of the output sequence of a filtering generator, which is included in the number of domestic and foreign algorithms information security. Received in article assessment proximity of the investigated the distribution of the distribution of the sum of independent random variables allow to make a conclusion about the quality of the conversion, implemented by the generator.

Keywords: finite-dependent random variables; approximating the amount; the distance in variation.

Постановка задачи

Многие отечественные и зарубежные алгоритмы защиты информации [1...5], в том числе и стандарты шифрования, имеют в своем составе такие преобразования, как регистры сдвига, перестановки и функции усложнения.

Указанные преобразования реализуются, в частности, в фильтрующем генераторе [1, 4], схема которого приведена на рисунке 1.

Фильтрующий генератор вырабатывает последовательность символов $\eta_i = f_i(X_{i+1}, X_{i+2}, \dots, X_{i+n}) \in Z$, где $X_{i+1}, X_{i+2}, \dots, X_{i+n}$ – промежуточное заполнение регистра, f_i – функции усложнения, Z – некоторая подгруппа.

Важным показателем фильтрующего генератора является структура выходной последовательности $\{\eta_i\}$, в частности, близость ее к последовательности

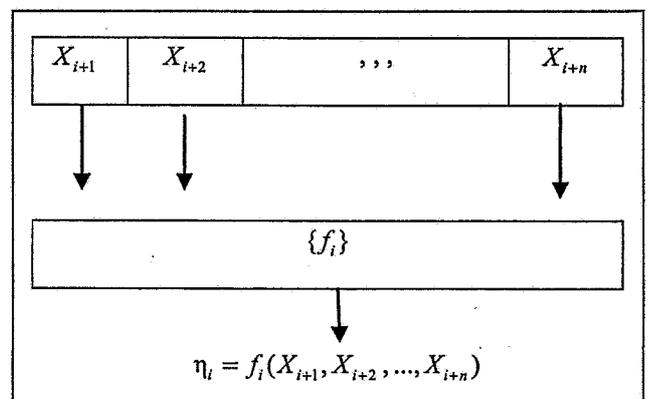


Рис. 1. Фильтрующий генератор

независимых величин. При определенном задании теоретико-вероятностной модели процесса образования величин $\{X_i\}$ величины η_i также будут случайными.

По построению величины η_i являются, вообще говоря, зависимыми случайными величинами и показателем слабости их зависимости является близость распределения их суммы $\theta_N = \eta_1 + \dots + \eta_N$ и суммы независимых случайных величин $\theta'_N = \eta'_1 + \dots + \eta'_N$, таких, что при любом i распределения η_i и η'_i совпадают.

Далее в работе будет получена оценка расстояния по вариации между распределением суммы конечно-зависимых случайных величин, принимающих значения из некоторой полугруппы, и распределением соответствующей суммы независимых случайных величин.

Оценка для распределения суммы конечно-зависимых случайных величин

В предыдущем разделе было отмечено, что ряд задач, связанных с исследованием алгоритмов защиты информации, приводит к необходимости изучения распределения случайной величины вида:

$$\theta_N = \eta_1 + \dots + \eta_N \quad (1)$$

где η_i – вообще говоря, зависимые случайные величины, принимающие значения из Z – коммутативной полугруппы по сложению, содержащей нулевой элемент 0.

Обозначим через B некоторую σ – алгебру подмножеств Z , пусть также $I_N = \{1, 2, \dots, N\}$.

Положим далее $\theta'_N = \eta'_1 + \dots + \eta'_N$, где η'_i – такие независимые случайные величины, что при любом $i \in I_N$ распределения η_i и η'_i совпадают.

Введем условие n – зависимости последовательности $\{\eta_i\}_{i=1}^N$:

1. Существует $n < N$, такое, что для любых целых величин $m, n < N$, таких, что

$$1 \leq i_1 < \dots < i_m \leq N, 1 \leq j_1 < \dots < j_k \leq N \text{ и } \min_{s,r} |i_s - j_r| > n,$$

независимы события: $\{\eta_{i_s} = 0, s = \overline{1, m}\}$ и $\{\eta_{j_l} = 0, l = \overline{1, k}\}$.

2. Существует $n < \frac{N}{2}$ такое, что при любых целых $m, k < N, i_1, \dots, i_m \in I_N, j_1, \dots, j_k \in I_N$ события $\{\eta_{i_s} = 0, s = \overline{1, m}\}$ и $\{\eta_{j_l} = 0, l = \overline{1, k}\}$ независимы, если $\min \{\rho(i_s, j_l) : s = \overline{1, m}, l = \overline{1, k}\} > n$,

где $\rho(i, j) = \min \{x > 0 : |i - j| = x \pmod{N}\}$.

Условию 1 удовлетворяют наборы n – зависимых случайных величин, расположенных на отрезке, а условию 2 – на окружности.

Без ограничения общности, далее будем считать, что если выполнено условие 1, то

$$\rho(i, j) = |i - j|.$$

В настоящей работе получена оценка для расстояния по вариации

$$\delta(\theta_N, \theta'_N) = \sup_{A \in B} |P\{\theta_N \in A\} - P\{\theta'_N \in A\}|$$

между распределением случайной величины θ_N вида (1) и распределением “аппроксимирующей” случайной величины θ'_N . Заметим, что в работе [7], для случая, когда последовательность $\{\eta_i\}$ есть последовательность индикаторов, получена оценка расстояния по вариации между распределением θ_N и соответствующим законом Пуассона.

Определим функцию $g(x)$, $x \in Z$ соотношениями:

$$g(0) = 0, g(x) = 1, x \in Z / \{0\}$$

и введем вспомогательные наборы случайных величин:

$$\{\xi_i\}_{i=1}^N \text{ и } \{\xi'_i\}_{i=1}^N,$$

где $\xi_i = g(\eta_i), \xi'_i = g(\eta'_i), i \in I_N$.

Для $k = 1, 2, \dots$ положим

$$b_{i_1, \dots, i_k} = P\{\xi_{i_1} = \dots = \xi_{i_k} = 1\},$$

$$\lambda = E\theta_N = \sum_{i \in I_N} b_i,$$

$$a = \max_{i \in I_N} b_i, \alpha = [(2n+1)a \cdot e]^{-1},$$

$$T = \sum_{\substack{i, j \in I_N \\ \rho(i, j) \leq n}} b_i \cdot b_j,$$

$$S_1 = \sum_{\substack{i, j \in I_N \\ 0 < \rho(i, j) \leq n}} b_{i, j}, S_2 = \sum b_{i, j_1, j_2}.$$

В последней формуле суммирование ведется по всем значениям i, j_1, j_2 , таким, что

$$0 < \rho(i, j_1) \leq n, 0 < \rho(i, j_2) \leq n, \rho(j_1, j_2) > n.$$

Утверждение. Если последовательность $\{\eta_i\}_{i=1}^N$ удовлетворяет условию 1 или 2,

$$\sum_{i \in I_N} b_i^2 < \frac{1}{2}, \alpha > \lambda + 4,5, \text{ то}$$

$$\delta(\theta_N, \theta'_N) \leq \frac{(T + S_1) / 2 + (1 + (\lambda + 2) / \alpha + \exp\{2\lambda + 1 - \alpha\}) \cdot (S + T)}{(1 - T / 2 - s(1 + (\lambda + 2) / \alpha))_+}, \quad (2)$$

где $s = S_1 + e \cdot S_2, (x)_+ = \max(0, x)$.

Доказательство. Введем необходимые обозначения. Множеством всех возможных значений $\xi = \{\xi_i\}_{i=1}^N$ является множество:

$$H = \{h = \{h_t\}_{t=1}^N : h_t = 0 \text{ или } h_t = 1, t \in I_N\}.$$

Будем отождествлять элемент $t \in I_N$ с одноэлементным множеством $\{t\} \in I_N$ и обозначать одним и тем же символом h набор $h \in H$ и множество $h = \{t \in I_N : h_t = 1\}$, состоящее из $|h| = h_1 + \dots + h_N$ элементов.

Положим далее

$$\xi' = \{\xi'_t\}_{t=1}^N,$$

$$H_k = \{h \in H : |h| = k\},$$

$$\tilde{H}_k = \{h \in H_k : h_i \cdot h_j = 0 \text{ при } 0 < \rho(i, j) \leq n\},$$

$$\tilde{H} = \bigcup_{k=0}^{\infty} \tilde{H}_k, \bar{H} = H - \tilde{H}, p_k = p\{\xi \in \tilde{H}_k\}, k = 0, 1, \dots$$

Пусть далее

$$\nu(h) = \{i \in I_N : \min_{j \in n} \rho(i, j) \leq n\}, h \in I_N,$$

$$\lambda_h = \sum_{i \in \nu(h)} b_i,$$

$$a_k = \max_{h \in H_k} \lambda_h \leq (2n+1)k \cdot a.$$

Определим события:

$$A_0^h = \{\xi_t = 0 \text{ при любом } t \in I_N / \nu(h)\},$$

$$A_1^h = \{\xi_t = 1 \text{ при любом } t \in h\},$$

$$A_2^h = \left\{ \sum_{i \in \nu(h) \setminus h} \xi_i > 0 \right\}.$$

В силу условий 1 или 2, и определения множества $\nu(h)$, при любом $h \in I_N$ события A_0^h и A_1^h независимы. Кроме того, если $h \in \tilde{H}$, то $p\{A_1^h\} = \prod_{i \in h} b_i$. Доказательство теоремы основано на использовании соотношения:

$$A_0^h \cdot A_1^h / A_2^h \leq \{\xi = h\} \leq A_0^h A_1^h, h \in H,$$

из которого следует, что

$$p\{A_0^h\} \cdot p\{A_1^h\} - p\{A_0^h A_1^h A_2^h\} = p\{\xi = h\} \leq p\{A_0^h\} \cdot p\{A_1^h\}. \quad (3)$$

Далее нам потребуется несколько утверждений, доказательство которых приведено в работе [6].

Лемма 1. Если $h \in H_k$, то при любом $m = 1, 2, \dots$

$$p_0 \leq p\{A_0^h\} \leq p_0 \left\{ 1 + \lambda_n \cdot \sum_{i=0}^{m-1} \prod_{j=1}^i a_{k+j} \right\} + \lambda_h \cdot \prod_{j=1}^m a_{k+j} \quad (4)$$

(произведение по j от 1 до 0 считается равным 1).

Лемма 2. При любом $k = 1, 2, \dots$

$$\frac{\lambda^k}{k!} \cdot \left(1 - \binom{k}{2} \cdot T / \lambda^2 \right) \leq \sum_{h \in H_k} p\{A_0^h\} \leq \frac{\lambda^k}{k!}, \quad (5)$$

$$\sum_{h \in H_k} p\{A_1^h\} \cdot \lambda_h \leq \frac{\lambda^{k+1}}{(k+1)!} \cdot T, \quad (6)$$

$$\sum_{h \in H_k} p\{A_0^h A_1^h A_2^h\} \leq \left\{ p_0 \sum_{i=0}^{m-1} \prod_{j=1}^i a_{k+j} + \prod_{j=1}^m a_{k+j} \right\} \times \frac{\lambda^{k-1}}{(k-1)!} (S_1 + (k-1)S_2 / \lambda). \quad (7)$$

Лемма 3. При любых $m = 1, 2, \dots, v = 0, 1, \dots$

$$\frac{e^{-\lambda} (1 - S_1 / 2) - T \cdot f_{\lambda}(m)}{1 + T \cdot F_{\lambda}(m)} \leq p_0 \leq \frac{e^{-\lambda} + s \cdot f_{\lambda}(m)}{(1 - T / 2 - s \cdot F_{\lambda}(m))_i}, \quad (8)$$

$$\sum_{k=0}^{\infty} \frac{\lambda^k}{k!} \prod_{j=1}^m a_{k+\nu+j} \leq e^{\lambda} f_{\lambda+\nu-1}(m), \quad (9)$$

где $f_{\lambda+\nu-1}(m) = ((m + \nu + \lambda)(2n + 1)a)^m$,

$$F_{\lambda+\nu-1}(m) = \sum_{j=0}^{m-1} f_{\lambda+\nu-1}(j).$$

Дальнейшее доказательство разобьем на 2 леммы.

Лемма 4. Справедлива оценка:

$$\delta(\theta_N, \theta'_N) \leq \frac{1}{2} \left\{ \sum_{h \in H} |p\{\xi = h\} - p\{\xi' = h\}| + T / 2 + S_1 / 2 \right\}.$$

Доказательство. По формуле полной вероятности, при любом $A \in B$ справедливы равенства:

$$p\{\theta_N \in A\} = p\{\theta_N \in A, \xi \in \bar{H}\} + \sum_{h \in \bar{H}} p\{\theta_N \in A, \xi = h\},$$

$$p\{\theta'_N \in A\} = p\{\theta'_N \in A, \xi' \in \bar{H}\} + \sum_{h \in \bar{H}} p\{\theta'_N \in A, \xi' = h\}.$$

По определению совокупностей случайных величин $\{\eta_t\}_{t=1}^N$ и $\{\eta'_t\}_{t=1}^N$,

при $h \in \bar{H}$ и любом $A \in B$

$$p\{\theta_N \in A / \xi = h\} = p\{\theta'_N \in A / \xi' = h\} = p(A, h).$$

Следовательно,

$$\left| p\{\theta_N \in A\} - p\{\theta'_N \in A\} \right| \leq p\{\theta_N \in A, \xi \in \bar{H}\} + p\{\theta'_N \in A, \xi \in \bar{H}\} + \sum_{h \in \bar{H}} |p\{\xi = h\} - p\{\xi' = h\}| \cdot p(A, h). \quad (10)$$

Заменяя A дополнительным событием $\bar{A} = Z/A$, получаем:

$$p\{\theta_N \in \bar{A}\} - p\{\theta'_N \in \bar{A}\} \leq p\{\theta_N \in \bar{A}, \xi \in \bar{H}\} + p\{\theta'_N \in \bar{A}, \xi' \in \bar{H}\} + \sum_{h \in \bar{H}} |p\{\xi = h\} - p\{\xi' = h\}| p(\bar{A}, h). \quad (11)$$

Далее заметим, что

$$\begin{aligned} p\{\theta_N \in A\} - p\{\theta'_N \in A\} &= |p\{\theta_N \in \bar{A}\} - p\{\theta'_N \in \bar{A}\}|, \\ p(A, h) + p(\bar{A}, h) &= 1, \\ p\{\theta_N \in A, \xi \in \bar{H}\} + p\{\theta_N \in \bar{A}, \xi \in \bar{H}\} &= p\{\xi \in \bar{H}\}, \\ p\{\theta'_N \in A, \xi' \in \bar{H}\} + p\{\theta'_N \in \bar{A}, \xi' \in \bar{H}\} &= p\{\xi' \in \bar{H}\}. \end{aligned} \quad (12)$$

Нетрудно показать, что

$$\begin{aligned} p\{\xi \in \bar{H}\} &= p\{i, j \in I_N : 0 < \rho(i, j) \leq n, \xi_i = \xi_j = 1\} \leq \\ &\leq \sum_{\substack{i, j \in I_N \\ i < j, \rho(i, j) \leq n}} b_{i, j} = S_1 / 2, \end{aligned} \quad (13)$$

$$p\{\xi' \in \bar{H}\} \leq \sum_{\substack{i, j \in I_N \\ i < j, \rho(i, j) \leq n}} b_i \cdot b_j \leq T / 2. \quad (14)$$

Суммируя выражения (10) и (11) и учитывая (12)...(14), приходим к доказательству леммы 4.

Лемма 5. Если выполнены условия теоремы, то при любом $m = 1, 2, \dots$

$$\begin{aligned} \sum_{h \in \bar{H}} |p\{\xi = h\} - p\{\xi' = h\}| &\leq \\ &\leq \frac{(T + S_1) / 2 + 2(F_\lambda(m) + e^\lambda \cdot f_\lambda(m))(S + T)}{(1 - T / 2 - s F_\lambda(m))_+}. \end{aligned}$$

Доказательство. Из соотношения (3) следует, что

$$\begin{aligned} p\{\xi = h\} - p\{\xi' = h\} &\leq \\ &\leq p\{A_0^h, A_1^h, A_2^h\} + |p\{\xi' = h\} - p\{A_0^h\} p\{A_1^h\}|. \end{aligned} \quad (15)$$

Используя оценки (7) и (9), получаем

$$\begin{aligned} \sum_{k=0}^{\infty} \sum_{h \in \bar{H}_k} p\{A_0^h, A_1^h, A_2^h\} &\leq \sum_{k=0}^{\infty} \left\{ p_0 \sum_{i=0}^{m-1} \prod_{j=0}^i a_{k+j} + \prod_{j=1}^m a_{k+j} \right\} \times \\ &\times \frac{\lambda^{k-1}}{(k-1)!} \left(S_1 + \frac{k-1}{\lambda} S_2 \right) \leq \\ &\leq e^\lambda (p_0 F_\lambda(m) (S_1 + e \cdot S_2) + f_\lambda(m) (S_1 + e \cdot S_2)) = \\ &= e^\lambda s (p_0 F_\lambda(m) + f_\lambda(m)). \end{aligned} \quad (16)$$

В последнем равенстве использовано соотношение:

$$\frac{f_{\lambda+1}(m)}{f_\lambda(m)} = \left(1 + \frac{1}{m + \lambda + 1} \right)^m \leq \exp \left\{ \frac{m}{m + \lambda + 1} \right\} < e.$$

С учетом (8) из (16) получаем:

$$\begin{aligned} \sum_{k=0}^{\infty} \sum_{h \in \bar{H}_k} p\{A_0^h, A_1^h, A_2^h\} &\leq \\ &\leq e^\lambda \cdot s \left\{ \frac{e^{-\lambda} + s \cdot f_\lambda(m)}{(1 - T / 2 - s \cdot F_\lambda(m))_+} F_\lambda(m) + f_\lambda(m) \right\} \leq \\ &\leq \frac{s(F_\lambda(m) + e^\lambda \cdot f_\lambda(m))}{(1 - T / 2 - s \cdot F_\lambda(m))_+}. \end{aligned} \quad (17)$$

Далее, при $h \in \bar{H}$

$$|p\{\xi' = h\} - p\{A_0^h\} p\{A_1^h\}| = p\{A_1^h\} \left| \prod_{i \in I_N / h} (1 - b_i) - p\{A_0^h\} \right|.$$

В силу (4) и (8), при $h \in H_k$ справедливо соотношение:

$$\begin{aligned} \frac{e^{-\lambda} (1 - S_1 / 2) - T \cdot f_\lambda(m)}{1 + T \cdot F_\lambda(m)} &\leq p\{A_0^h\} \leq \\ &\leq \frac{e^{-\lambda} + s \cdot f_\lambda(m)}{(1 - T / 2 - s \cdot F_\lambda(m))_+} \left\{ 1 + \lambda_h \sum_{i=0}^m \prod_{j=1}^i a_{k+i} \right\} + \lambda_h \prod_{j=1}^m a_{k+j}. \end{aligned} \quad (18)$$

Покажем, что при любом $h \in H$

$$\frac{e^{-\lambda}}{1 + T} \leq \prod_{i \in I_N / h} (1 - b_i) \leq e^{-\lambda} \sum_{i=0}^m \lambda_h^i + \lambda_h^{m+1}. \quad (19)$$

Вначале заметим, что из условия утверждения $\alpha > \lambda + 4, 5$ следует справедливость неравенства:

$$\max_{i \in I_N} b_i \leq \frac{1}{(2n + 1)e^{(\lambda + 4, 5)}} < \frac{1}{3}.$$

Для доказательства (19) используем справедливое при $0 \leq x \leq \frac{1}{3}, 0 \leq y \leq \frac{1}{2}$ неравенство:

$$e^{-x} (1 + y)^{-x^2/y} \leq 1 - x \leq e^{-x}, \quad (20)$$

где правая часть очевидна, а левая следует из того, что в данных условиях

$$\begin{aligned} e^x (1 - x)(1 + y)^{-x^2/y} &\geq (1 + x^2 + x^2/2)(1 - x)(1 + x^2(1 - y/2)) \geq \\ &\geq 1 + \frac{x^2}{2} (1 - y - x - x^2 - x^3) \geq 1 + \frac{x^2}{108}. \end{aligned}$$

Левая часть неравенства (20) при $y = \sum_{i \in I_N} b_i^2$ дает левую оценку в (19):

$$\prod_{i \in I_N/h} (1-b_i) \geq \prod_{i \in I_N/h} e^{-b_i} \cdot (1+y)^{-b_i/y} \geq \prod_{i \in I_N} e^{-b_i} \cdot (1+y)^{-b_i/y} = e^{-\lambda} (1+y)^{-1} \geq \frac{e^{-\lambda}}{1+T}.$$

Правая оценка в неравенстве (19) тривиальна, если $\lambda_h \geq 1$. При $\lambda_h < 1$, в силу (20) и известного неравенства $e^x \leq 1+x+x^2, 0 \leq x \leq 1$, получаем:

$$\prod_{i \in I_N/h} (1-b_i) \leq \exp \left\{ -\lambda + \sum_{i \in h} b_i \right\} \leq \exp \left\{ -\lambda + \lambda_h \right\} \leq e^{-\lambda} (1 + \lambda_h + \lambda_h^2).$$

Последнее неравенство доказывает правую оценку в (19). Сравнение (18) и (19) показывает, что при любом $h \in H$ величина

$$\left| \prod_{i \in I_N/h} (1-b_i) - p \{A_0^h\} \right|$$

не превосходит разности между левой и правой частями соотношения (18). Это соображение, с учетом соотношений (5), (6) и (9), позволяет получить оценку:

$$\sum_{k=0}^{\infty} \sum_{h \in H_k} p \{A_1^h\} \left| \prod_{i \in I_N/h} (1-b_i) - p \{A_0^h\} \right| \leq \frac{(T+S_1)/2 + (s+2 \cdot T)(F_{\lambda}(m) + e^{\lambda} f_{\lambda}(m))}{(1-T/2 - s \cdot F_{\lambda}(m))_+} \quad (21)$$

Из (15), (17) и (21) следует утверждение леммы 5.

Из лемм 4 и 5 следует, что при любом $m = 1, 2, \dots$

$$\delta(\theta_N, \theta'_N) \leq \frac{((T+S_1)/2 + F_{\lambda}(m) + e^{\lambda} \cdot f_{\lambda}(m))(s+T)}{(1-T/2 - S \cdot F_{\lambda}(m))_+} \quad (22)$$

Заметим далее, что при $\lambda \geq 0, 0 < m + \lambda + 1 \leq \alpha$,

$$\frac{d}{dm} \ln f_{\lambda}(m) = \ln(m + \lambda + 1) - (2n+1)a + \frac{m}{m + \lambda + 1} < 0,$$

$$\frac{d^2}{dm^2} \ln f_{\lambda}(m) = \frac{m}{m + \lambda + 1} + \frac{\lambda + 1}{(m + \lambda + 1)^2} > 0.$$

Так как функция $\ln f_{\lambda}(m)$ выпукла вниз и

$$f_{\lambda}(\alpha - \lambda - 1) = e^{\lambda + 1 - \alpha} > e^{\lambda - \alpha} (1 - 1/\alpha)^{\alpha} \geq ((1 - 1/\alpha)e^{-1})^{\alpha - \lambda} = f_{\lambda}(\alpha - \lambda),$$

то, обозначая через $[x]$ целую часть x , получаем,

$$f_{\lambda}([\alpha - \lambda]) \leq \max \{ f_{\lambda}(\alpha - \lambda - 1), f_{\lambda}(\alpha - \lambda) \} = e^{\lambda + 1 - \alpha}. \quad (23)$$

Далее заметим, что при

$$1 \leq m \leq [\alpha - \lambda], \beta = ([\alpha - \lambda] - 1)^{-1} \geq (\alpha - \lambda - 1)^{-1},$$

имеет место неравенство:

$$f_{\lambda}(m) \leq f_{\lambda}^{1-(m-1)\beta}(1) \cdot f_{\lambda}^{(m-1)\beta}([\alpha - \lambda]) \leq f_{\lambda}(1) \cdot [f_{\lambda}(\alpha - \lambda - 1) \cdot f_{\lambda}^{-1}(1)]^{(m-1)\beta}.$$

Из последнего соотношения следует, что

$$F_{\lambda}(m) = \sum_{j=0}^{m-1} f_{\lambda}(j) \leq 1 + f_{\lambda}(1) \left\{ 1 - [f_{\lambda}(\alpha - \lambda - 1) \cdot f_{\lambda}^{-1}(1)]^{\beta} \right\}^{-1} \leq 1 + \frac{\lambda + 2}{\alpha \cdot e} \left\{ 1 - \exp \left(\frac{1}{\alpha - \lambda - 1} - 1 + \frac{1}{\alpha} \right) \right\}^{-1} \leq 1 + \frac{\lambda + 2}{\alpha}, \quad (24)$$

поскольку $e^{-1} \cdot \left\{ 1 - \exp \left(\frac{1}{\alpha - \lambda - 1} - 1 + \frac{1}{\alpha} \right) \right\} \leq 1$ при $\alpha \geq \lambda + 4, 5$.

Подставляя в неравенство (22) $m = [\alpha - \lambda]$ и используя оценки (23) и (24), завершаем доказательство утверждения.

Список литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. *Основы криптографии*. М.: Гелиос АРВ. 2001, 479 с.
2. Бабаш А.В., Шанкин Г.П. *Криптография*. М.: Гелиос АРВ. 2007, 511 с.
3. Шангин В.Ф. *Информационная безопасность компьютерных систем и сетей*. М.: ИД "Форум"-ИНФРА-М. 2008, 415 с.
4. Панасенко С.П. *Алгоритмы шифрования*. Специальный справочник. СПб: БХВ-Петербург. 2009. 576 с.
5. Фомичев В.М. *Дискретная математика и криптология*. Курс лекций. М.: Диалог-МИФИ. 2003. 397 с.
6. Зубков А.М. Неравенства для распределения суммы функций от независимых случайных величин // *Математические заметки*. 1977, т. 22, № 5. С. 745-758.
7. Зубков А.М. Оценки для сумм конечно-зависимых индикаторов и для момента первого наступления редкого события / *Труды Математического института им. В.А. Стеклова Академии наук СССР*, 1986, т. 177. С. 33-46.

References

1. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. *Osnovy kriptografii* [Foundations of cryptography]. M.: Gelios ARV [Moscow: Publishing House "Gelios ARV"]. 2001, 479 p.
2. Babash A.V., Shankin G.P. *Kriptografiya* [Cryptography]. M.: Gelios ARV [Moscow: Publishing House "Gelios ARV"]. 2007, 511 p.
3. Shangin V.F. *Informatsionnaya bezopasnost kompyuternykh sistem i setey* [Information security of computer systems and networks]. M.: Forum-Infra-M. 2008, 415 p.

- networks]. M.: ID "Forum" -INFRA- M [Moscow: Publishing House ID "Forum" INFRA-M]. 2008, 415 p.
4. Panasenko S.P. *Algoritmy shifrovaniya. Spetsialnyy spravochnik* [Encryption algorithms. A special handbook]. SPb: BKhV-Peterburg [St. Petersburg: Publishing House "BKhV-Peterburg"]. 2009. 576 p.
 5. Fomichev V.M. *Diskretnaya matematika i kriptologiya. Kurs lektsiy* [Discrete mathematics and cryptology. A course of lectures]. M.: Dialog-MIFI [Moscow: Publishing House "Dialog-MIFI"]. 2003. 397 p.
 6. Zubkov A.M. *Neravenstva dlya raspredeleniya summy funktsiy ot nezavisimykh sluchaynykh velichin* [Inequalities for the distribution of the sum of functions of independent random variables]. *Matematicheskie zametki* [Mathematical notes]. 1977, vol. 22, no. 5, pp. 745–758.
 7. Zubkov A.M. *Otsenki dlya summ konechno-zavisimykh indikatorov i dlya momenta pervogo nastupleniya redkogo sobytiya* [Estimates for sums of finite-dependent indicators and for the first time the occurrence of a rare event]. *Trudy Matematicheskogo instituta im. V.A. Steklova Akademii nauk SSSR* [Proceedings of the Steklov Institute of Mathematics. V.A. Steklov Academy of Sciences of the USSR]. 1986, vol. 177, pp. 33–46.

Информация об авторе

Лось Алексей Борисович, канд. техн. наук, доцент
 E-mail: alos@hse.ru
 Московский институт электроники и математики Национального исследовательского университета "Высшая школа экономики"
 109028, Москва, Российская Федерация, Трехсвятительский пер., д. 3

Information about the author

Los Aleksey Borisovich, Cand. of Techn. Sciences, Associate Professor
 E-mail: alos@hse.ru
 Moscow Institute of Electronics and Mathematics National Research University "Higher School of Economics"
 109028, Moscow, Russian Federation, Trehsvyatitelsky per., 3

Модульные встраиваемые системы между стандартами 19" и COM

Развитие миниатюризации в электронике позволяет присвоить все больше функций одной европлате. Если еще несколько лет назад требовались отдельные платы для центрального процессора, графических и запоминающих устройств, контроллера Ethernet и т. д., сегодня все эти функции размещаются на одноплатном компьютере. Поэтому для построения комплексной промышленной компьютерной системы необходимо все меньше слотов. Вместо систем с количеством слотов до 21 в настоящее время требуются системы всего с тремя, четырьмя или пятью слотами. Поэтому, в большинстве случаев система шириной 19" является слишком избыточной. Возникает потребность в корпусе с меньшими размерами, который не встраивается в 19" плоскость распределительного шкафа. Помимо классических 19" систем есть много решений с малым форм-фактором, которые, однако, довольно быстро достигают пределов по мощности, если есть потребность в высокой производительности компьютера или графических устройств, модульности, расширяемости и возможности резервирования.



Система AMC с двумя слотами для модулей AMC

Этот пробел между классическими 19" системами и решениями с малым форм-фактором восполняет компания Pentair Equipment Protection с выпуском серии новых модульных систем с малым форм-фактором. Данные системы конфигурируются из стандартных деталей в соответствии с требованиями заказчика. При специальных требованиях можно изменить стандартную систему за счет простых модификаций. Основой новых модульных систем с малым форм-фактором являются шасси AMC высотой 1 U и шириной 250 мм или компактный блочный каркас Schroff высотой 3 U, глубиной 205 мм и шириной всего 28 HP. Шасси AMC разработаны на базе шасси multipacPRO с пространством для двух устанавливаемых горизонтально сменных плат. Оба шасси позволили создать платформу для построения независимых от технологии стандартных систем — здесь можно использовать модули AMC, а также сменные платы в евроформате для VMEbus, VPX, CompactPCI, CompactPCI Serial и т. д. Размеры шасси легко адаптируются к форм-фактору AMC или к платам евроформата.

Первое изделие серии модульных систем с малым форм-фактором — система AMC с двумя слотами для установки одного или двух модулей Single Full Size или Mid Size. Для равномерного вентилирования встроенных модулей справа от них расположен блок с четырьмя вентиляторами и воздушным фильтром. В задней части находится блок питания Open Frame мощностью 120 Вт, что позволяет использовать платы AdvancedMC с мощностью до 50 Вт на модуль. Небольшие выемки в верхней крышке и панели основания предусмотрены для установки нескольких систем друг на друга. С помощью запрессованных гаек система крепится на монтажной панели.

В основе второго стандартного изделия данной серии лежит блочный каркас Schroff шириной всего 28 HP. Система комплектуется соответствующей объединительной платой, блоком питания и вентиляторным блоком, который крепится фланцами снизу. Для различных шинных систем используются блоки питания со специальными выходными напряжениями. Все блоки питания, используемые в данной серии изделий, оснащаются входом переменного или постоянного тока. Это расширяет сферу применения, охватывая промышленные приложения или, например, транспортную технику. Дополнительную информацию см. на сайте www.schroff.ru.

Компания Schroff.

<http://www.schroff.ru>