несанкционированных действий. По этой причине некорректность преобразований, вызванная использованием кофактора, для системы критичной не является.

Очевидно, при качественных криптографических преобразованиях, задействованных для реализации протокола, можно считать, что его корректное завершение практически достоверно свидетельствует об использовании истинного значения кофактора. Иными словами, по отношению к кофактору абонент *B* обладает некоторым проверочным соотношением *T*. Таким образом, корректность криптопротокола взаимно однозначно зависит от глобального (несекретного) параметра *c*. Исходя из этого, скрытую передачу сообщения *M** от *A* к *B* (*t* битов информации) можно осуществить следующим образом.

Абоненты заранее согласовывают долговременный ключ *Y* (случайное число, не превосходящее *n*), а также стеганографический параметр *W*, состоящий из *t* чисел, указывающих на номера различных разрядов в двоичной записи *c* (необходимого размера). Для передачи данных абонент *A* поразрядно сложением по модулю два модифицирует соответствующими битами сообщения *M** разряды кофактора *c*, перечисленные в списке *W*. Затем результат умножается на *Y*. В итоге получается модифицированный кофактор $c_1=Y(c\oplus M^*(W)) \bmod n$. Далее при использовании протокола пересылки ключа *K* абонент *A* действует стандартно, за исключением того, что использует модифицированный кофактор вместо исходного.

Абонент *B*, обнаруживая нарушение корректности преобразований в ходе протокола, строит модифицированный кофактор перебором с критерием истинности *T*. Затем вычисляет $Y^{-1}c_1\oplus c=M^*(W) \bmod n$.

Очевидно, реальные значения $t\approx 30$, т. е. *t* пренебрежимо мало по сравнению с *n*, следовательно, ключ *K* может быть принят абонентом *B* практически с исходной надежностью.

Заметим также, что аутентичность информации, передаваемой по скрытому каналу, в принципе, может быть обеспечена стандартными методами.

IV Выводы

В работе рассмотрена возможность скрытой передачи данных в криптопротоколах, основанных на свойствах эллиптических кривых. Показано, что механизмы цифровых подписей типа Эль Гамаля и механизмы пересылки ключей, внедряемые в настоящее время, допускают организацию скрытых каналов передачи информации, в том числе новых. Таким образом, существует угроза внедрения скрытых каналов связи в распространенные средства криптографической защиты информации. Качество скрытых каналов зависит от вычислительных ресурсов абонентов.

Литература: 1. Simmons G. J. Subliminal Communication is Easy Using the DSA // Advances in Cryptology. Proceedings of EUROCRYPT'93. – Springer-Verlag, 1995. – P. 219–232. 2. Simmons G. J. The Subliminal Channel and Digital SignaturesDSA // Advances in Cryptology. Proceedings of EUROCRYPT'84. – Springer-Verlag, 1985. – P. 364–378. 3. Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer, 1986, – 400 p. 4. Кочубинский А. И. Эллиптические кривые в криптографии. // Безопасность информации. – 2, – 2000. с.18–31.

УДК 681.3.067:681.3.016

МЕТОДИКА ВЫЯВЛЕНИЯ В ДВОИЧНЫХ ВЕРОЯТНОСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ДЕТЕРМИНИРОВАННЫХ СОСТАВЛЯЮЩИХ НА ОСНОВЕ МЕТОДА БИНОМИАЛЬНОГО ПРЕОБРАЗОВАНИЯ

Виктор Куценко, Тарас Левченко
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **При помощи известного метода биномиального преобразования проведен анализ двоичной вероятностной последовательности (ДВП) после наложения на нее трех типов детерминированных составляющих. Предложена методика выявления в ДВП детерминированных составляющих. Методика дает необходимые доказательства наличия в ДВП детерминированной составляющей и может быть применена как составная часть системы информационной безопасности.**

Summary: **The analysis of a binary probabilistic sequence (BPS) after queued superposition of three types of determined components made using of known method of binomial transformation. The technique is**

offered for detection in BPS determined components. The technique give necessary improvements of presenting in BPS determined components can be applied as a component of information security system.
Ключевые слова: **Информационная безопасность, двоичные вероятностные последовательности, детерминированная составляющая, биномиальное преобразование.**

I Введение

Двоичные вероятностные последовательности (ДВП)

$$\{b_N b_{N-1} \mathrm{K}\, b_1 b_0\}, \tag{1}$$

где

$$b_i = \begin{cases} 1, \ p_1 = 0.5, \\ 0, \ p_0 = 0.5, \end{cases} \tag{2}$$

- некоррелированный бит в позиции номер i с дискретной плотностью распределения p, находят широкое применение для кодирования передаваемой информации при защите информационных ресурсов в сетях передачи данных [1]. Для получения ДВП обычно используют различные методы генерации последовательностей нулей и единиц [2–8]. Критерием использования генератора является отсутствие детерминированной составляющей и неповторяемость фрагментов определенной длины при достаточно большом N.

Для определения наличия в ДВП детерминированной составляющей одним из авторов разработан теоретико-числовой метод биномиального преобразования [9], в котором используется известное свойство [10] биномиального распределения с дискретной функцией распределения вероятностей

$$p_k = C_n^k \theta^k (1-\theta)^{n-k}, \tag{3}$$

где C_n^k – биномиальный коэффициент, равной вероятности того, что сумма n случайных величин, принимающих значение 0 или 1 с вероятностями соответственно θ и $1-\theta$, равна точно k.

Если считать ДВП набором из n случайных величин с дискретной функцией распределения (2), то очевидно, что случайная величина

$$B_j = \sum_{i=Vj}^{Vj+V-1} b_l, \tag{4}$$

где смещение V=const, является некоррелированной и имеет биномиальное распределение

$$p_k = C_n^k 2^{-n}. \tag{5}$$

Цель работы – разработка методики выявления детерминированной составляющей в ДВП.

II Основная часть

Для достижения поставленной цели авторами исследована обратная задача – изучено влияние на статистические характеристики случайной величины (4) детерминированной составляющей в ДВП.

В качестве исходной ДВП была выбрана одна из реализаций выходной последовательности линейного конгруэнтного генератора Borland C++, принимающая значения 0 либо 1. Детерминированной составляющей служили следующие последовательности:

1. Повторяющаяся с интервалом T группа шириной в $N1$ единиц.
2. Повторяющаяся с интервалом T группа шириной $N0$ нулей.
3. Повторяющаяся с интервалом T группа из последовательности $N1$ единиц и $N0$ нулей в разных сочетаниях при выполнении неизменного условия $N1=N0$.

Процесс исследования состоял в изменении T при неизменных $N1$ и $N0$, изменении $N1$ и $N0$ при неизменном T, расчете массива значений случайной величины (4) при V=128 и числе усреднений 10, а также определении гистограммы усредненной случайной величины. Проверка статистической гипотезы о соответствии реальных h_k и теоретических p_k оценок случайности распределения усредненной случайной величины (4) распределению Пуассона производилась по критерию χ^2 распределения с r–1 степенью свободы

$$\chi^2 = K \sum_{k=1}^{r} \frac{(h_k - p_k)^2}{p_k}, \tag{6}$$

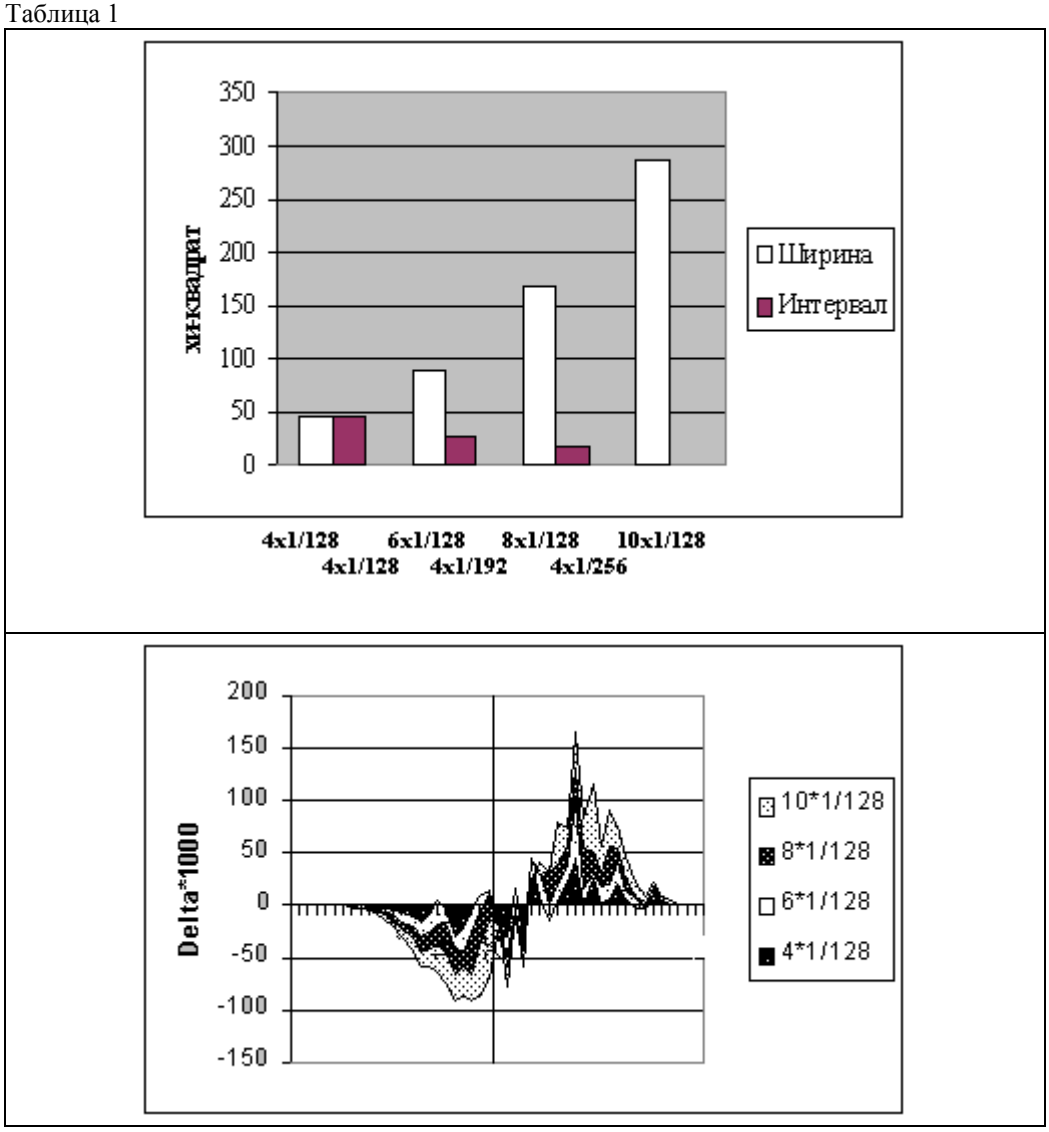
де K – число независимых наблюдений, которые отвергают теоретические оценки с уровнем значимости α при

$$\chi^2 \ \phi \ \chi^2_{1-\alpha}(r-1), \tag{7}$$

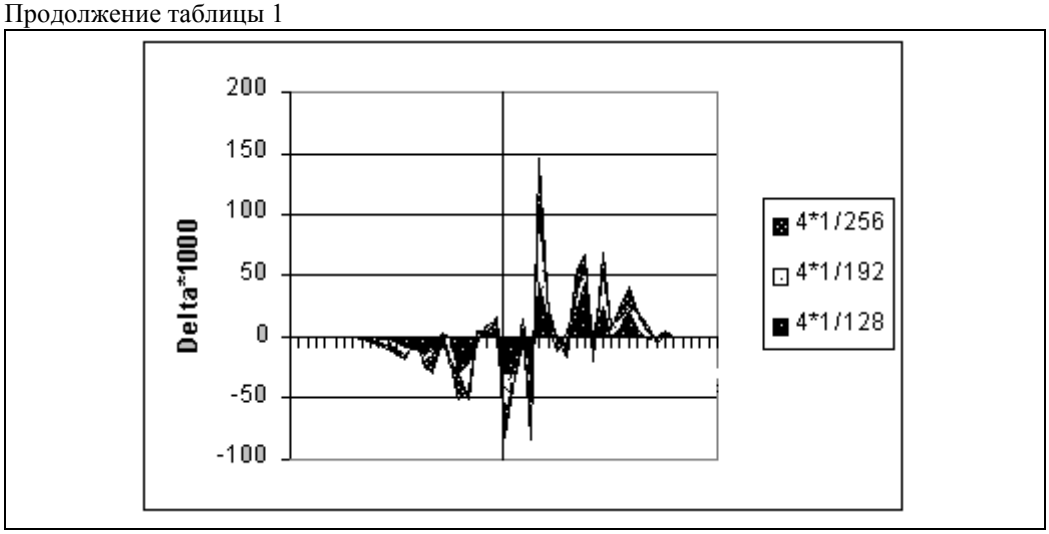
и наличию симметрии разностей Delta между k-м отсчетом гистограммы и соответствующим значением функции распределения (5).

Для первого типа детерминированной составляющей при {$N1$=4, T=128}, {$N1$=6, T=128}, {$N1$=8, T=128} и {$N1$=10, T=128} в первой строке таблицы 1 белым цветом показаны соответствующие значения χ^2. Темным цветом выделены значения χ^2 для {$N1$=4, T=128}, {$N1$=4, T=192} и {$N1$=4, T=256}. В двух последующих строках изображены отклонения k-х отсчетов соответствующих гистограмм от соответствующего значения теоретической функции распределения. Вертикальной чертой показано математическое ожидание случайной величины (4), равное в рассмотренном частном случае 128/2=64. Также отметим, что значение χ^2 для исходной ДВП равно 4,46, а значение квантиля (7) для P=0,99 и r=128 равно 81,75.

Таблица 1



Продолжение таблицы 1

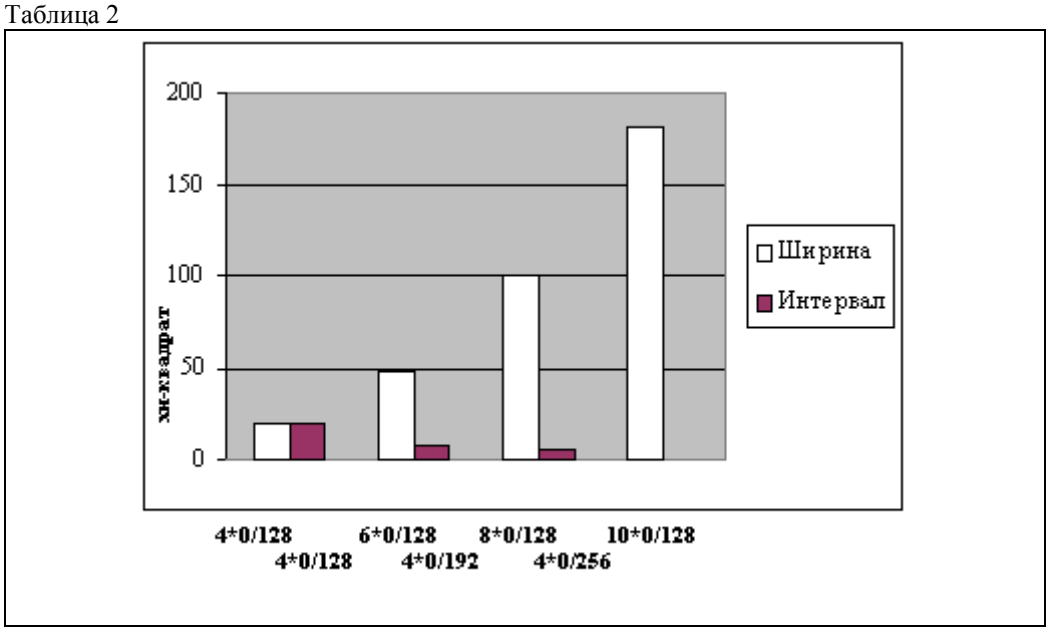


Можно отметить следующие результаты.

1. Примененный к случайной величине (4) критерий χ^2 оказывается весьма чувствительным к наличию даже незначительного относительного количества (около 3%) единиц в детерминированной составляющей. Его величина при этом возрастает на порядок.
2. Критерий оказывается нечувствительным к смещению первой группы единиц относительно условного начала ДВП.
3. По мере увеличения числа единиц *N1* при *T*=const значения χ^2 увеличиваются. Отклонения гистограмм также увеличиваются и приобретают асимметричный характер с положительными приращениями в сторону увеличения значений случайной величины (4). Это происходит за счет увеличения постоянной составляющей ДВП.
4. По мере увеличения интервала *T* при *N1*=const значения χ^2 уменьшаются. Вышеуказанные отклонения гистограммы и степень ее асимметрии также уменьшаются.

Для второго типа детерминированной составляющей при {*N0*=4, *T*=128}, {*N0*=6, *T*=128}, {*N0*=8, *T*=128} и {*N0*=10, *T*=128} в первой строке таблицы 2 белым цветом показаны соответствующие значения χ^2. Темным цветом выделены значения χ^2 для {*N0*=4, *T*=128}, {*N0*=4, *T*=192} и {*N0*=4, *T*=256}. Отметим следующее.

Таблица 2



Продолжение таблицы 2

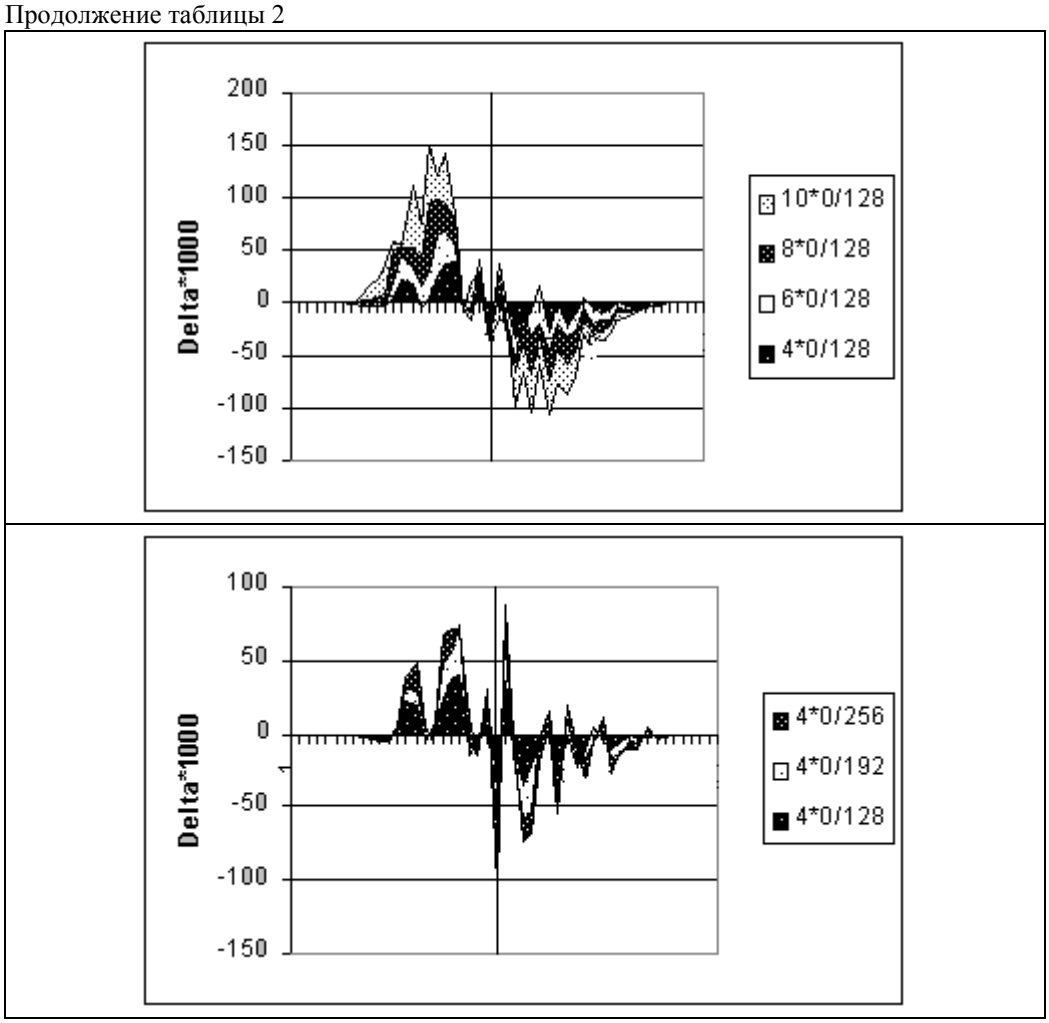
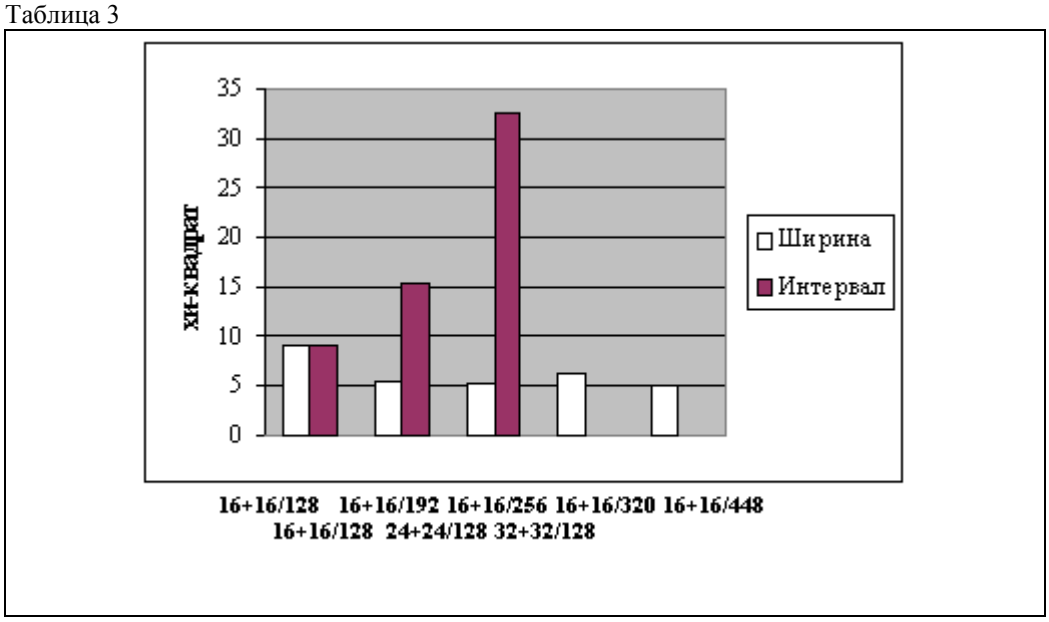
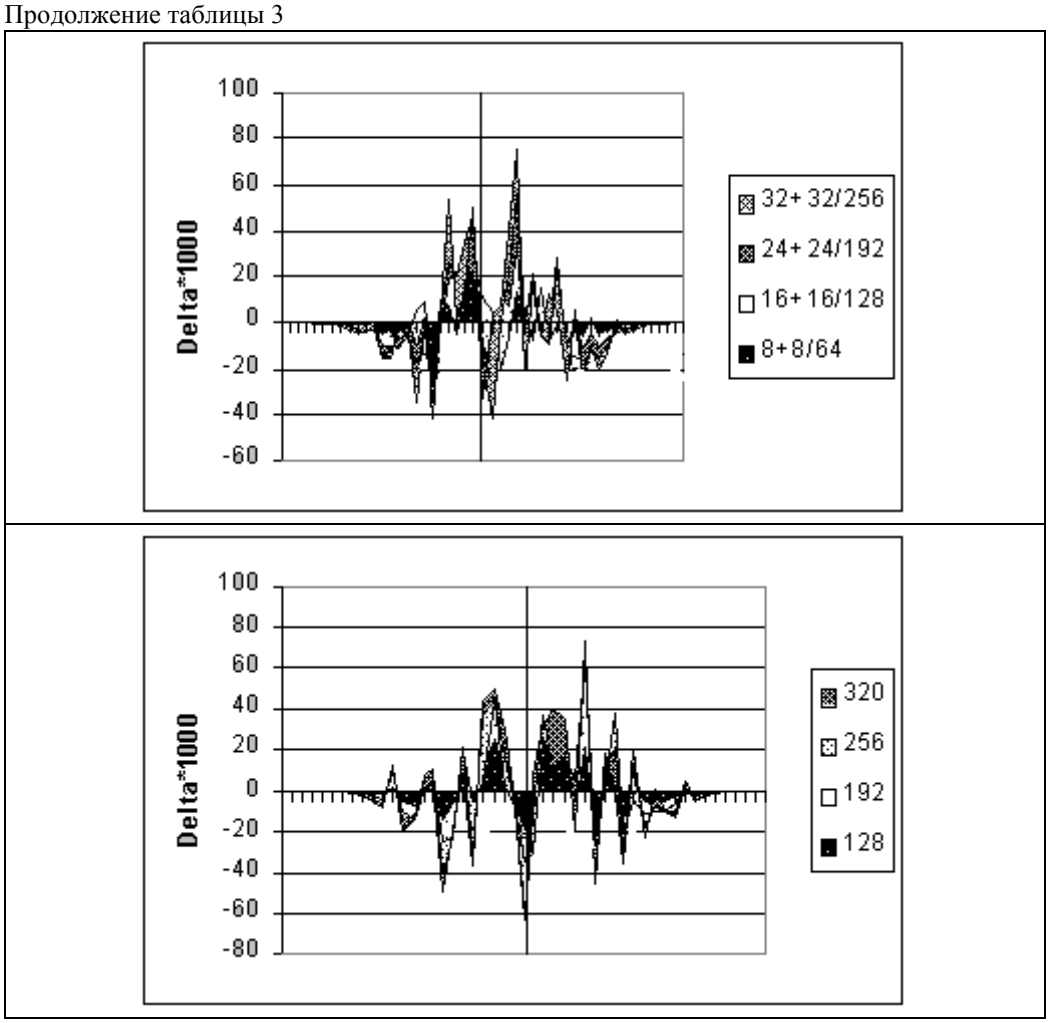


Таблица 3



Продолжение таблицы 3



1. Критерий χ^2 оказывается довольно чувствительным к наличию в детерминированной составляющей незначительного количества (около 3%) нулей. Его величина при этом возрастает примерно вчетверо.
2. Критерий оказывается нечувствительным к смещению первой группы нулей относительно условного начала ДВП.
3. По мере увеличения числа нулей *N0* при *T*=const значения χ^2 увеличиваются. Отклонения гистограмм также увеличиваются и приобретают асимметричный характер с положительными приращениями в сторону уменьшения значений случайной величины (4). Это происходит за счет уменьшения постоянной составляющей ДВП.
4. По мере увеличения интервала *T* при *N1*=const значения χ^2 уменьшаются. Вышеуказанные отклонения гистограммы и степень ее асимметрии также уменьшаются.
5. Сравнивая соответствующие данные таблиц 1 и 2, можно отметить, что влияние группы единиц на ДВП больше, чем влияние аналогичной группы нулей.
6. При относительно небольших (до 10%) значениях *N0/T* и, соответственно, *N1/T*, влияние величины смещения *V* на результаты расчета незначительно.

Результаты исследования влияния третьего типа детерминированной составляющей при {*N1*=8, *N0*=8, *T*=64}, {*N1*=16, *N0*=16, *T*=128}, {*N1*=24, *N0*=24, *T*=192} и {*N1*=32, *N0*=32, *T*=256}. В первой строке таблицы 3 белым цветом показаны соответствующие значения χ^2. Темным цветом выделены значения χ^2 для {*N1*=16, *N0*=16, *T*=128}, {*N1*=16, *N0*=16, *T*=192}, {*N1*=16, *N0*=16, *T*=256}, {*N1*=16, *N0*=16, *T*=320}. Отметим, что:

1. Чувствительность примененного к случайной величине (4) критерия χ^2 оказывается значительно меньше, чем при наличии детерминированной составляющей предыдущих типов. Значение критерия начинает увеличиваться примерно вдвое только при ширине группы нулей и единиц не менее V/4.

2. Критерий оказывается нечувствительным к очередности распределения нулей и единиц внутри группы, а также расположения начала группы относительно условного начала ДВП.

3. По мере увеличения ширины группы при T=const значения χ^2 увеличиваются. Отклонения гистограмм также увеличиваются, но их асимметричный характер не нарушается.

4. По мере увеличения интервала T при неизменной ширине группы значения χ^2 почти не изменяются.

Таким образом, методика выявления в ДВП детерминированной составляющей должна содержать следующие операции.

Операция 1. Составление из исходной ДВП (1) в соответствии с (4) массива значений случайной величины *B*.

Операция 2. Расчет осредненной гистограммы случайной величины *B,* определение направления ее асимметрии относительно теоретической плотности распределения (5).

Операция 3. Установление по полученной асимметрии типа детерминированной составляющей: если асимметрия характеризуется положительными приращениями в сторону уменьшения значений случайной величины, то детерминированная составляющая состоит из единиц, в противном случае – из нулей.

Операция 4. Вычисление критерия χ^2 для осредненной гистограммы и сравнение его с табличным значением для заданного объема выборки и числа степеней свободы. Отклонение полученного значения от теоретического более чем в 2 раза, особенно при наличии определенной на операции 2 асимметрии, является необходимым условием наличия в исходной ДВП детерминированной составляющей.

III Выводы

1. Предложена методика выявления в ДВП детерминированных составляющих, основанная на известном методе биномиального преобразования.

2. Методика дает необходимые доказательства наличия в ДВП детерминированных составляющих и может быть применена как составная часть системы информационной безопасности.

Литература: 1.Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с., ил. 2. Д. Кнут. Искусство программирования для ЭВМ.– Т. 2. – Получисленные алгоритмы. – М.: Мир. – 1977. – 482 с. 3. P. L'Ecuyer. Uniform random number generation.// Annals of Operations Research. – 1994. – V. 53. – pp. 77-120. 4. H. Niederreiter. Pseudo-random numbers and optimal coefficients. // Advances in Mathematics. – 1977. – V. 26. – pp. 99-181. 5. S. K. Park and K. W. Miller. Random number generators: good ones are hard to find. // Communs of the ACM. – 1988. – V. 31. – pp. 1192-1201. 6. N. S. Altman. Bit-wise behavior of random number generators.// SIAM Journal of Sci. Stat. Computing. – 1988. – V9(5). – pp. 941-949. 7. J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. // International Statistical Review. – 1992. – V. 60. – pp. 167-176. 8. J. Walker. HotBits: Genuine random numbers, generated by radioactive decay. // http://www.fourmilab.ch/hotbits/ 9. Т. Левченко. Тестирование двоичных вероятностных последовательностей методом биномиального преобразования. – В сб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Науково-технічний збірник. – Випуск 2. – К.:НДЦ "Тезіс" НТУУ "КПІ". – 2001. – 273с.– С. 152. 10. Справочник по математике (для научных работников и инженеров). – Г. Корн, Т. Корн. – Изд. 4.– М.: Наука, 1978.– 831 с.

УДК 681.3.067:681.3.016

ВЫЯВЛЕНИЕ В ДВОИЧНЫХ ВЕРОЯТНОСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ДЕТЕРМИНИРОВАННЫХ СОСТАВЛЯЮЩИХ С ИСПОЛЬЗОВАНИЕМ ЛИНЕЙНОГО БУЛЕВА ПРОГРАММИРОВАНИЯ

Тарас Левченко

Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Двоичная вероятностная последовательность (ДВП) разбивается на фрагменты длиной *m* бит, рассматриваемых как совокупность из *n* образцов, обладающих некоторым числом признаков из заданного множества *m* признаков. Показано, что периодическую компоненту можно выявить в результате решения задачи покрытия методом линейного булева программирования. Приведен алгоритм выявления.**

Summary: **Binary probabilistic sequence (BPS) is fragmented in *n* patterns by *m* bits length, each one**