Merinovich Y., Bang A., Van Tilborg H. A Broadcast Key Distribution Scheme Based on Block Designs // Lecture Notes in Computer Science. – 1995. – № 1025. – P. 12 – 21. ***6****. Алексейчук А. Н., Паничек В. Г. Анализ стойкости ключевых сетей относительно компрометации корреспондентов // Збірник наукових праць КВІУЗ. Вип. 3. Київ. 1998. С. 76 – 83.* ***7****. Конюшок С. М. Алгоритм оцінки параметрів оптимальних ключових структур, побудованих на основі неповних урівноважених блок-схем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ: 2003. – Вип. 6. – С. 79 – 83.* ***8****. Холл М. Комбинаторика. Пер. с англ. – М.: Мир, 1970. – 427 с.* ***9****. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. – 743 с.* ***10****. Сачков В. Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.*

УДК 681.3.067:681.3.016

ОЦЕНКА СЛУЧАЙНОСТИ ПО ИЗБЫТОЧНОСТИ

Виктор Мясоедов, Виктор Куценко
Научно-технический комплекс «Импульс», г. Киев

Аннотация: **С помощью измерения избыточности информации в последовательности псевдослучайных чисел исключается гипотеза о внутренней периодичности выхода генератора Фибоначчи. Доказывается теорема об относительных частотах нечётных операндов в последовательности. Восполняется пробел в определении длины периода генератора Фибоначчи.**
Summary: **By means of measurement of redundancy of the information in sequence of random numbers the hypothesis about internal periodicity of an output of generator Fibonachchi is excluded. The theorem of relative frequencies of odd operands in sequence is proved. The blank in definition of length of the period of generator Fibonachchi is filled.**
Ключевые слова: **Псевдослучайные последовательности, оценки сложности, избыточность информации, архивирование данных, косвенный критерий.**

Введение

Применение псевдослучайных чисел для защиты данных от взлома накладывает очень высокие требования на качество и обоснованность средств оценки псевдослучайных последовательностей двоичных слов. Для оценки алгоритмов генерации псевдослучайных последовательностей используют понятие вычислительной сложности хэш-преобразований, осуществляемых этими алгоритмами, а также статистические оценки генерируемых последовательностей чисел.

В работе [1] обсуждаются возможности оценки сложности алгоритмов для получения нескольких последовательностей из последовательности длиной k, а также критикуется понятие сложной случайной последовательности по Колмогорову, относящейся к измерению конкретных последовательностей, а не к алгоритмам генерации. Однако, помимо того, что вычислительная сложность алгоритма влияет только на стоимость вычислений, имеется простая нелинейная (квазилинейная) схема генерации псевдослучайных последовательностей [2], использующая начальные разряды двух трансцендентных чисел (математических констант e и π $k = 8000$ десятичных знаков). Эта схема позволяет генерировать практически бесконечное число псевдослучайных последовательностей. Кроме того, получаемые с помощью этой схемы последовательности псевдослучайных чисел допускают теоретическое исследование их свойств, показывающее отсутствие достаточных оснований для гипотез о зависимости измеряемых свойств от конкретных случаев генерации.

Непосредственная экспериментальная статистическая оценка качества самих псевдослучайных последовательностей затруднена их дискретностью. Это сильно ограничивает средства статистического анализа [2], либо делает необходимым преобразование двоичных слов в двоичные дроби из непрерывного интервала [0,1] с соответствующим обоснованием усложнённых статистических схем [3]. Для оценки псевдослучайности последовательностей понятие количества информации по Шеннону может быть уточнено как измерение избыточности информации, содержащейся в последовательности двоичных слов. Избыточность измеряется по сжатию данных алгоритмами архивирования (ZIP, RAR и т. д.), основанных на анализе сложности последовательностей [4, 5]. Измерения относительной избыточности информации в данных дают основания для введения критерия псевдослучайности последовательностей, поскольку абсолютная случайность не совместима с избыточностью, меньшей единицы. Такие измерения легко согласуются с понятием сложности случайных последовательностей по Колмогорову [1].

В статье рассматриваются свойства последовательностей, порождаемых генератором Фибоначчи [6], в частности, с помощью критерия псевдослучайности и на основе доказываемой теоремы исключается гипотеза о «внутренней периодичности» таких последовательностей.

Для независимости изложения приведём описание схемы генерации. В генераторе Фибоначчи используются обобщённые последовательности Фибоначчи F_n и алгоритм генерации этих последовательностей

$$F_{n+2} = F_{n+1} + F_n = f_{n+1} \cdot u_1 + f_n \cdot u_2,\ F_1 = u_2,\ F_2 = u_1, \tag{1}$$

где $f_{n+2} \equiv f_{n+1} + f_n,\ f_0 = 1,\ f_1 = 1$ – числа Фибоначчи, $u_1,\ u_2$ – начальные значения, не равные одновременно нулю. Поскольку свойства этих последовательностей не зависят от начальных значений u_1, u_2 [5], постольку достаточно рассмотреть свойства хэш-преобразования (1) в соотнесении с конечной длиной последовательностей псевдослучайных чисел (двоичных слов) генератора Фибоначчи

$$x_{n+2} \equiv x_{n+1} + x_n \left(\mathrm{mod}\, 2^L\right),\ x_0 = u_2',\ x_1 = u_1', \tag{2}$$

где $u_1' \equiv u_1 \left(\mathrm{mod}\, 2^L\right),\ u_2' \equiv u_2 \left(\mathrm{mod}\, 2^L\right)$. Генератор Фибоначчи порождает последовательность $\{s_n\}$ двоичных слов с длиной L_1 битов

$$s_n = \frac{x_n - \mathrm{mod}(x_n, 2^{L-L_1})}{2^{L-L_1}}. \tag{3}$$

Числа $u_1,\ u_2$ в (2) не являются одновременно чётными, что обеспечивает требуемую фактически длину операндов.

Для параллельной генерации используются независимые пары начальных значений генератора, также поставляемые генератором Фибоначчи, имеющим практически бесконечную длину периода $60 \cdot 10^{3999}$.

Постановка задачи

Структура хэш-преобразования определена преобразованиями (2), (3). Их отличие состоит в том, что преобразование (2) безусловно отображает обобщённые числа Фибоначчи в множество натуральных чисел $\{0, 1, ..., 2^L - 1\}$, а преобразование (3) отображает полученное множество в множество $\{0, 1, ..., 2^{L_1} - 1\}$ **в зависимости** от «бита переполнения» скрытой части операндов. При этом последовательность неиспользуемых явно частей операндов также получается безусловным отображением обобщённых чисел Фибоначчи в множество чисел $\{0, 1, ..., 2^{L-L_1} - 1\}$.

Периоды последовательностей $\{x_n\}$ и $\{x_{n,L-L_1}\}$ являются конечными [1], $3 \cdot 2^{L-1}$ и $3 \cdot 2^{L-L_1-1}$ соответственно, а «полезная» длина последовательности $\{s_n\}$ определяется периодом последовательности скрытых частей операндов. Уменьшение длины выходной последовательности до «полезной» продиктовано требованием исключения избыточности содержащейся в ней информации, в принципе позволяющей восстановить начальные значения генератора по «полной», $N = 3 \cdot 2^{L-1}$, последовательности $\{s_n\}$.

Дополнительной компонентой хэш-преобразования (2) – (3) является исключение из последовательности $\{s_n\}$ подпоследовательности слов, соответствующих чётным операндам x_n (каждый третий, начиная с первого чётного). Это гарантирует отсутствие *возможной* «внутренней периодичности» в последовательности двоичных слов, независимо от её проявления в оценках качества выхода генератора псевдослучайных чисел. Множеством образа хэш-преобразования в этом случае является множество нечётных чисел $\{1, 3, ..., 2^L - 1\}$, дополненное элементом «чётное число», т. е. эта компонента есть просто фильтр во множество, $Odd = \{1, 3, ..., 2^L - 1\} \bigcup \{"чётное\_число"\}$.

Требуется теоретически оценить качество последовательностей длиной N операндов $\{x_n\}$ генератора Фибоначчи и проверить наличие в них избыточной информации, несовместимой с абсолютной случайностью последовательностей двоичных слов. Требуется также проверить влияние коррелированности

последовательностей псевдослучайных битов [6] на относительную избыточность при сжатии двоичных файлов.

Основная часть

Решение теоретической части задачи опирается на независимость хэш-преобразований от начального момента генерации обобщённых последовательностей Фибоначчи и на иррациональность предела отношения двух последовательных чисел этих последовательностей

$$\lim_{n\to\infty}\frac{F_{n+1}}{F_n}=\frac{\sqrt{5}-1}{2}$$

Этот предел также не зависит от начальных значений u_1, u_2. Поэтому некоторые свойства последовательностей $\{s_n\}$ не изменяются с изменением начала отсчёта «дискретного времени» генерации.

Тем не менее, рассмотрение последовательности операндов по модулю восемь показывает, например, что не все возможные чётные операнды появляются в генерируемых последовательностях, причём их множество зависит от начальных значений последовательностей. В силу этого принцип трансфинитной индукции не применим в теоретических исследованиях свойств последовательностей (2), (3), и нужны независимые от него доказательства, хотя некоторые свойства и могут быть обоснованы в соответствии с этим принципом.

В полных последовательностях операндов, рассматриваемых по модулю четыре, имеются следующие последовательности остатков: …, (0), 3, 1, (0), 1, 1, (2), 3, 1, (2), 3, 1, (0), … и…, (2), 1, 3, (0), 3, 3, (2), 1, 3, (0), 3, 3, (2), … . При этом относительные частоты остатков 1 и 3 в зависимости от начальных значений составляют 1:3 или 3:1.

Теорема. При длине операндов $L>1$ все нечётные числа из множества Odd встречаются в полных последовательностях операндов либо один, либо три раза.

Для доказательства теоремы нам понадобится следующая

Лемма. Период последовательности операндов длиной $L>1$ не равен периоду последовательности с меньшей длиной операндов.

Действительно, для пары чисел Фибоначчи f_n, f_{n+1}, выбираемых в качестве начальных значений, имеет место соотношение $f_{n+m}=f_{m-1}f_n+f_m f_{n+1}$, определяющее продолжение классической последовательности Фибоначчи. Дважды применяя метод математической индукции по длине операндов l, покажем, во-первых, что число $f_{3\cdot 2^{L-1}}$ делится на 2^L, и, во-вторых, что число $f_{3\cdot 2^{L-1}+1}-1$ делясь на 2^{L-1}, не делится на 2^L. Тогда из предположения, противоречащего утверждению леммы, следовало бы в силу первого свойства, что $x_{3\cdot 2^{L-1}+1}\equiv f_{3\cdot 2^{L-1}+1}u_1\equiv u_1\equiv x_1(\mathrm{mod}\,2^L)$, $x_{3\cdot 2^{L-1}+2}\equiv f_{3\cdot 2^{L-1}+2}u_2\equiv u_2\equiv x_2(\mathrm{mod}\,2^L)$, так что числа u_1, u_2 в силу второго свойства чисел Фибоначчи были бы одновременно чётными, что исключено нетривиальностью длины операндов.

В случае $l=1$ $f_3=2$ и первое свойство очевидно. Из формулы $f_{2\cdot n}=f_n\left(f_{n-1}+f_{n+1}\right)$, где $n=3\cdot 2^l$, по предположению индукции и в силу нечётности f_{n-1} следует, что первое свойство имеет место для всех l.

В случае $l=2$ $f_7-1=12$, и второе свойство очевидно. Из формул $f_{2\cdot n+1}-1=f_n^{\,2}+f_{n+1}^{\,2}-1=f_n^{\,2}+\left(f_{n+1}-1\right)\left(f_{n+1}+1\right)$, где $n=3\cdot 2^l$, в силу первого свойства, предположения индукции и простой чётности числа $f_{n+1}+1$ следует, что второе свойство имеет место для всех $l\geq 2$. ***Лемма доказана.***

Для доказательства теоремы снова применим методом математической индукции. В случае $L=2$ имеются две периодические последовательности операндов, в которых нечётные операнды встречаются либо один, либо три раза: 1, 3, (0), 3, 3, (2) и 3, 1, (0), 1, 1, (2), где в скобках показаны чётные операнды, а начало последовательности выбрано так, чтобы первый операнд был нечётным.

Предположим, что теорема доказана для всех L, $2<L\leq l$, и докажем, что она верна при $L=l+1$.

Числа x_n и F_n связаны соотношениями

$$x_1=F_1-2^{l+1}\cdot v_1=u_2-2^{l+1}\cdot v_1,$$

$$x_2 = F_2 - 2^{l+1} \cdot v_2 = u_1 - 2^{l+1} \cdot v_2,$$
$$x_3 = x_2 + x_1 - 2^{l+1} v_3 = u_1 + u_2 - 2^{l+1} \cdot (v_2 + v_1 + v_3),$$
$$x_4 = x_3 + x_2 - 2^{l+1} v_4 = 2 \cdot u_1 + u_2 - 2^{l+1} \cdot (2 \cdot v_2 + v_1 + v_3 + v_4),$$
$$\dots$$
$$x_{n+1} = x_n + x_{n-1} - 2^{l+1} v_{n+1} = f_{n+1} \cdot u_1 + f_n \cdot u_2 - 2^{l+1} \cdot (f_{n+1} \cdot v_2 + f_n v_1 + f_{n-1} \cdot v_3 + \dots + v_{n+1}),$$

где v_1, v_2 – целые части дробей $\frac{F_1}{2^{l+1}}$, $\frac{F_2}{2^{l+1}}$, v_i, $i \geq 3$, – целые части дробей $\frac{x_{i-1} + x_{i-2}}{2^{l+1}}$.

Полагая, как и в случае $L = 2$, x_1 нечётным, что не нарушает общности рассуждений, обнаруживаем, что в силу свойств чисел f_n, доказанных в лемме, равенство $x_{3 \cdot 2^l + 1} = x_1$ невозможно, так как в противном случае число x_1 было бы чётным, что противоречит выбору начального члена последовательности.

С другой стороны, последовательность остатков чисел x_n по модулю 2^l в полной последовательности операндов повторяется дважды, начиная с номера $3 \cdot 2^l + 1$. В силу предположения индукции каждое нечётное число в последовательности остатков встречается либо один, либо три раза. Если остаток первого члена последовательности x_n встречается в последовательности остатков один раз, то из доказанного неравенства $x_{3 \cdot 2^l + 1} \neq x_1$ следует, что числа x_1 и $x_{3 \cdot 2^l + 1}$ в последовательности нечётных операндов также встречаются по одному разу. Если же остаток первого члена последовательности x_n встречается в последовательности остатков три раза, то последовательно устанавливая в первом полупериоде начало последовательности на каждый из трёх членов последовательности x_n с равными остатками, находим в полном периоде шесть попарно различных нечётных чисел. Эти шесть чисел отличаются только старшими битами, поэтому среди них имеются две тройки равных чисел, т. е. в этом случае нечётные члены последовательности встречаются в полной последовательности три раза. Таким образом, относительные частоты нечётных операндов есть один и три.

В случае $L = 2$ в последовательности встречаются все нечётные числа, меньшие 2^L. Полагая по индукции, что это имеет место для всех L, $2 < L \leq l$, видим, что каждый из нечётных остатков относится к двум различным нечётным числам из последовательности операндов, то есть в последовательности x_n встречаются все нечётные числа $1, 2, \dots, 2^L - 1$ из множества Odd. ***Теорема доказана.***

Доказанная лемма восполняет пробел в определении периода последовательностей (Теорема 1 из [6]). Доказанное свойство последовательностей операндов не зависит от начальных значений последовательностей.

Заметим, что несмотря на выявленные ограничения частоты появления операндов в последовательностях, получаемых с помощью обобщённых чисел Фибоначчи, априорная неопределённость способа «расщепления» остатков в пару различных нечётных чисел и использованный в доказательстве произвол выбора начала последовательности операндов свидетельствуют о наличии «достаточного беспорядка» в таких последовательностях. Точнее, численные эксперименты с параметрами $N = 3 \cdot 2^{19}$, $L = 64, 56, \dots, 16, 8$ показывают, что сжатие «длинных» последовательностей с помощью обычных архиваторов (ZIP, RAR и т.д.) практически невозможно при длине последовательности операндов, меньшей длины периода. То же имеет место в численных экспериментах с последовательностями длины $N = 2^{20}$, состоящими только из нечётных операндов.

Для исключения чётных операндов использован следующий фильтр (дополнительная компонента полного хэш-преобразования)

$$r_1 \equiv u_0 \pmod 2, \; r_2 \equiv u_1 \pmod 2,$$
$$t_1 = 1 - r_1, \; t_2 = 3 - r_1 - r_2,$$
$$x'_{2i} = x_{3i + t_1}, \; x'_{2i+1} = x_{3i + t_2}.$$

Легко видеть, что этот фильтр выделяет нечётные операнды независимо от начальных значений последовательности.

Зависимость отношения длин файлов (исходного и сжатого архиватором RAR), от длины операндов показана в таблице.

Таблица – Выявление избыточности при архивировании

		Длины операндов (байты)						
		7	6	5	4	3	2	1
		Длина файлов						
Все операнды	Исх.	11010062	9437196	7864330	6291464	4718598	3145732	1572866
	Сжат.	11010062	9437196	7864330	6291464	4710918	195983	1257
Нечётные операнды	Исх.	7340032	6251456	5242880	4194304	3145728	2097152	1048576
	Сжат.	7340032	6251456	5242880	4194304	3127695	10499	852

Обращает на себя внимание поведение этой зависимости в окрестности длины операндов $L=16$ (два байта), где нарушено неравенство $N<3\cdot 2^{L-1}$, гарантирующее отсутствие «массовых» повторов (частичных симметрий) в целой последовательности. При длине операндов большей трёх байтов сжатия сплошной последовательности практически не наблюдается. Это явление уточняется в экспериментах с фиксированной длиной операндов и изменяющейся длиной последовательностей. Из рисунка видно, что коэффициент сжатия не фильтрованной последовательности увеличивается пропорционально длине части последовательности, находящейся за пределами полного периода.

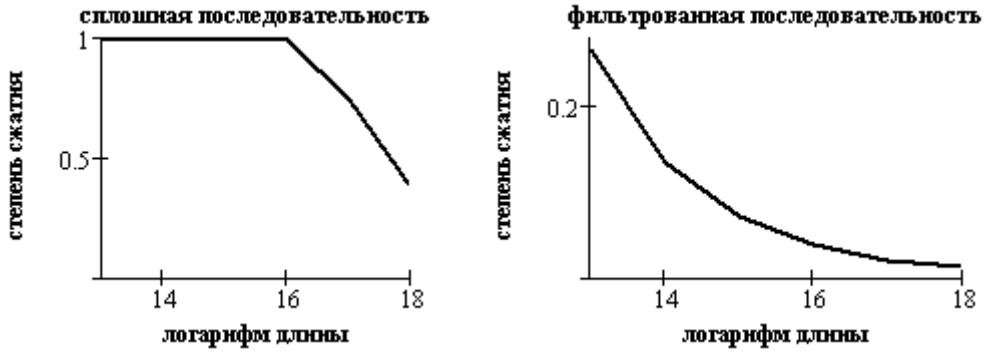

Рисунок – Сжимаемость двухбайтовых последовательностей малой длины $N=2^{13}\ldots 2^{18}$

Из этого рисунка видно также, что избыточность подпоследовательности нечётных операндов намного выше, чем избыточность сплошной последовательности. Подробный анализ этих зависимостей требует учёта деталей архивирования, что выходит за рамки статьи.

Таким образом, фильтрованная последовательность операндов является «намного» менее сложной, чем сплошная последовательность, так что гипотеза о «внутренней периодичности» может быть отброшена.

Разумеется, специфическое сжатие последовательности операндов возможно при задании двух начальных членов. Однако для последовательностей двоичных слов, в которых $L_1>0$, это уже невозможно в силу абсолютной стойкости алгоритма получения двоичных слов к попыткам определения начальных значений генератора Фибоначчи по известной последовательности двоичных слов из полезной части периода, $N\le 3\cdot 2^{L-L_1-1}$. Для доказательства абсолютной стойкости достаточно заметить, что изменение всех битов скрытой части одного из операндов, кроме первого бита, «гладко», т. е. через один такт генерации, изменяет всю последующую выходную последовательность двоичных слов, и нет никаких данных в пределах полезной части периода (см. конструкцию из доказательства Теоремы 1 в [6]), кроме неизвестных по условию начальных значений генератора, чтобы обнаружить такую подмену.

Аналогичные результаты имеют место в численных экспериментах с последовательностями двоичных слов, образованных из одного, двух, …, семи старших байтов операндов генератора Фибоначчи, с той лишь

разницей, что для длинных последовательностей никакое сжатие не наблюдается – независимо от соотношения фактической длины последовательности с периодом. Так же, как и для последовательностей двоичных слов генератора Фибоначчи, не наблюдается сжатие двухбайтовых псевдослучайных последовательностей ($N = 3 \cdot 2^{19}$), источником которых был датчик из Mathcad 2003. Это свидетельствует о том, что период датчика $runif$ из Mathcad 2003 очень большой.

Проведенные эксперименты показывают, что последовательности нечётных операндов малой длины (по отношению к длине периода) в некотором смысле симметричны, в частности, остатки этих операндов по модулю четыре повторяются с периодом 4. Представляет интерес исследование асимметрии последовательностей двоичных слов, $L_1 > 0$, содержащих как чётные, так и нечётные числа.

Выводы

Не фильтрованные последовательности операндов, в отличие от подпоследовательностей нечётных операндов, являются достаточно сложными случайными последовательностями. Эти последовательности могут быть приняты в качестве псевдослучайных последовательностей для генерации псевдослучайных чисел (двоичных слов) в силу измерений относительной избыточности, используемых в косвенном критерии оценки псевдослучайности.

*Литература: **1.** O. Goldreich, S. Goldwasser, S. Micali. How to construct random functions//Journal of the ACM, vol.33, E4, Oct 1986, pp.792-807.- kiev-security_org_ua-Криптография_Как построить случайные функции.htm. **2.** В. Мясоедов, В. Куценко, Т. Левченко, Равномерность распределения в шкале наименований. В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник.-Вип. 7.-К.:НДЦ "Тезіс" НТУУ "КПІ".-2003.- 224с. - С.179. **3.** В. Мясоедов, В. Куценко, Особенности генерации псевдослучайных чисел. В сборнике „Захист інформації” ... **4.** A. Lempel and J. Ziv, On the Complexity of Finite Sequences, IEEE Trans. on Information Theory Vol. IT -22, Jan. 1976, pp 75-81. **5.** A. K. Leung and S. E. Tavares, Sequence Complexity as a Test for Cryptographic Systems, Advances in Cryptology ’84, pp.75-81. **6.** В. В. Мясоедов, Золотое сечение в шифровании данных. В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник.-Вип. 4 .-К.:НДЦ "Тезіс" НТУУ "КПІ".-2002.- 214с. - С. 105.*

УДК 681.5.015: 004.056.57

СИСТЕМА С РАССЕЯННЫМИ ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В УСЛОВИЯХ АТАКИ ФИЛЬТРАЦИЕЙ И АДДИТИВНЫМ ШУМОМ

Ирина Маракова
Одесский национальный политехнический университет

Анотація: **Розглянуто систему с прихованими розсіяними цифровими водяними знаками (ВЗ) з використанням зображень у вигляді головного покриваючого повідомлення в умовах атаки фільтрацією та адитивним шумом. Одержані формули для імовірностей помилок Pm та Pfa як функцій числа елементів ВЗ, постійної перекручень, порогу. Це дозволяє оцінити число потрібних біт ВЗ для забезпечення надійності системи в певних умовах.**
Summary: **We consider private tile-based watermarking (WM) digital system at use as the cover message (CM) of images with additive noise and filtering attack The formulas for probabilities Pm and Pfa are derived as a dependence on the number of WM elements, distortion constraints, chosen threshold. It allows to find out how many bits of WM is necessary to use in order to embed reliable WM for different conditions.**
Ключевые слова: **Водяные знаки, основное покрывающее сообщение, идентификатор.**

I Введение

Основное практическое использование систем с цифровыми водяными знаками (ЦВЗ) – это скрытое или открытое погружение дополнительной идентификационной информации в основное покрывающее сообщение (ОПС) [1, 2]. В простейшем случае декодер такой системы принимает решение о наличии или отсутствии ЦВЗ в ОПС. При этом декодер фактически является обнаружителем (детектором) и система