УДК 004.056.5

ПРИНЦИПЫ ЗАЩИТЫ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ, ОЦЕНКА ИХ ЗАЩИЩЕННОСТИ И КОНТРОЛЯ

В.К. ЖЕЛЕЗНЯК[1], А.Г. ФИЛИПОВИЧ[2], К.Я. РАХАНОВ[1], М.М. БАРАНОВСКИЙ[2]

[1]Учреждение образования «Полоцкий университет имени Евфросинии Полоцкой», ул. Блохина, 29, Новополоцк, 211440, Беларусь

[2]Оперативно-аналитический центр при Президенте Республики Беларусь, ул. Кирова, 49, Минск, 220030, Беларусь

Поступила в редакцию 23 декабря 2022

Рассматривается обработка результатов измерений дискретно-преобразованных речевых сигналов статически математическими принципами, основанными на теореме П.Л. Чебышева. Это значительно повышает точность результатов обработки, снижает порог чувствительности обнаружения сигнала и тем самым достоверно устанавливает наличие либо отсутствие сигнала в канале утечки.

Ключевые слова: точечная оценка, интервальные оценки, правила обработки, результаты измерений, истинное значение.

Введение. Техническая защита информации – научное направление информатики, формирующее принципиально новые свойства защищенности объектов информатизации, информационных систем с дискретной формой представления сигналов, обработки результатов измерений с высокими точностными показателями параметров сигналов в виде периодической последовательности импульсов треугольной формы и сигналов шума квантования в виде периодической последовательности импульсов пилообразной формы с использованием современных микроэлектронных средств. Оптимальное управление снижает порог обнаружения широкополосной высококачественной образованной ступенчатой функцией с нелинейной амплитудной характеристикой аналоговых речевых сигналов в реальном масштабе времени.

Сложность задач, решаемых информационными системами, разнообразие помеховых воздействий на сигналы обусловили общую проблему их защиты, оценку защищенности и контроля.

Основная часть. Частными задачами являются выбор помехоустойчивых измерительных сигналов (ИС) для передачи и оптимальной обработки принимаемых сигналов [1, 2]. Обработка ИС сводится к восстановлению полезной измерительной информации с наилучшими параметрами после обработки [2, 3, 4] в соответствии с принятым критерием. Оценка защищенности аналоговых и дискретно-квантованных речевых сигналов должна выполняться по единому критерию. Идеальным квантующим устройством дискретно-квантованного преобразования является ступенчатая функция [2]. Систематической ошибкой, присущей идеальной ступенчатой функции, является пилообразная функция с максимальным значением $\frac{\Delta}{2}$, среднеквадратическое значение $\sigma^2 = \frac{\Delta}{\sqrt{12}}$, плотность вероятности ошибки квантования составляет $\frac{1}{\Delta}$ [2].

В табл. 1 приведены значения дисперсии σ_e^2 в зависимости от шага квантования, из которого следуют весьма малые значения дисперсии для ее оценки в каналах утечки информации

[1]. Значения рассчитываются по формуле $\sigma_e^2 = 10\lg\left(\frac{\Delta^2}{12}\right) = 10\lg\left(\frac{2^{-2b}}{12}\right) = -(6,02b + 10,79)$ дБ. Здесь $\Delta = 2^{-b}$ – шаг квантования.

Таблица 1

Разрядность b	8	10	12	14	16	18	20
Шаг квантования Δ	2^{-8}	2^{-10}	2^{-12}	2^{-14}	2^{-16}	2^{-18}	2^{-20}
Дисперсия σ_e^2, дБ	–59	–71	–83	–95	–107	–119	–131

Качественные улучшения метрологических и информационных характеристик процесса исследования (улучшение точности, определение неучитываемых характеристик, увеличение объема обрабатываемой информации) основаны на определении точечных характеристик и параметров математических моделей [3].

Переход к оптимальным системам сводится к задаче оптимизации выбора структуры и параметров системы, при которой свойства последней оптимальны, т. е. к выбору лучшего варианта из числа возможных [4, 5].

Численные методы статистических испытаний реализуются с помощью средств вычислительной техники (СВТ) общего назначения с первичными измерительными преобразователями, программным обеспечением с высокой точностью в автоматизированном режиме. Обработка измерительного сигнала выполняет оптимальный приемник [5, 6].

При проектировании и создании сложных информационных систем, в которых информационные потоки являются вероятностными, реализуют алгоритм ее функционирования, применяя метод имитационного моделирования. Достоинством метода имитационного моделирования является возможность выполнения эффективных количественных и качественных (структурных) исследований. Автоматизированные измерительные системы (СИА) реализовывают временные факторы в обработке большого объема данных измерений при других преимуществах в массогабаритных показателях, квантовании точности. Дискретно-квантованные преобразования обусловили возникновение новых каналов утечки, необходимость повышения чувствительности и точности выделения сигналов, прошедших четные и нечетные искажения.

Обработка результатов измерений в условиях слабых сигналов в шумах высокого уровня аналогичных и дискретно-квантованных речевых сигналах выполняется с использованием закона больших чисел при выполнении ряда условий, получая новые качественные и количественные достоверные данные обработки [6, 7, 8].

Точечными значениями параметров находят действительные значение измеряемой величины при большом числе измерений. За действительные значение величины принимают точечную оценку истинного значения – среднее арифметическое значение при известном законе распределения результатов измерений [9, с. 166].

Для оценки достоверности результатов измерений и ее увеличения пользуются доверительными интервалами и доверительными вероятностями. Доверительный интервал погрешности результата измерений – интервал значений случайной погрешности, внутри которой с заданной вероятностью находится искомое (истинное) значение погрешности результата измерений [10, ф. (8.19)]. Доверительные границы погрешности результата измерений – верхняя и нижняя границы доверительного интервала погрешности результата измерений [10, ф. (8.20)]. Доверительные границы в случае нормального закона распределения вычисляются как $\pm tS$, где S – средняя квадратическая погрешность измерения, t – коэффициент, зависящий от доверительной вероятности P и числа измерений n [10].

Точечные оценки [8, 9]. Оценка истинного значения производится по данным выборки – ряда значений, принимаемых случайной величиной в процессе n независимых измерений. Основными параметрами функции распределения случайной величины x является математическое ожидание $M[X] = M_x$ и $D[X] = D_x$. Точечными оценками этих параметров (m_x^*, S_x) называются оценки, выражаемые одним числом. Чем больше выборка n, тем точнее определена функция нормального распределения измеряемой величины. Оценка истинного значения измеряемой величины определяется с помощью среднего арифметического значения m_x^*, а с помощью статической дисперсии S_x^2 – разброс измеряемой величины. Сигнал в канале утечки (сигнал + шум) равен

$$c + ш = X(t) + n(t) \text{ при } n(t) \ll X ,$$

где $X(t)$ – значение измеряемой величины; $n(t)$ – шум в канале утечки.

Маскирующий шум в канале утечки подчиняется нормальному закону распределения.

Правила обработки ограниченного по объему статических данных. Если даны значения X_1, X_2, …, X_n из n независимых опытов случайной величины X с неизвестным математическим ожиданием (МО) M_x и дисперсией D_x, то для определения этих параметров следует пользоваться приближенными значениями (оценками). Среднее арифметическое значение результата ряда наблюдений определяется [11, ф. (7.5)] как

$$m_x^* = \overline{X} = \frac{X_1 + X_2 + ... + X_n}{n} = \frac{\sum_{i=1}^{n} X_i}{n} \text{ [6, ф. (4.1.6)].}$$

Определение среднего квадратического отложения D_n по опытным данным. Несмещенной оценкой дисперсии является величина [9, ф. (7.7), 6, 6, ф. (4.3.2)]

$$D_x = S_x^2 = \frac{\sum_{i=1}^{n}\left(x_i - m_x^*\right)^2}{n-1} .$$

Вычисление среднего квадратического отклонения при конечном числе n производится по следующей формуле [10, ф. (8.17), 11, ф. (7.8)]:

$$S_x = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - m_x^*\right)^2}{n-1}} ,$$

где $m_x^* = \overline{X}$ – среднее значение; x_i – результат i-го измерения величины X_i ; n – число измерений.

Для оценки истинного значения измеряемой величины X используют среднее арифметическое значение, которое обозначают $\overline{X}$ или m_x^* (оценка МО m_x).

При увеличении числа независимых измерений n оценка среднего арифметического значение должна сходиться по вероятности к МО случайной величины. Такая оценка называется состоятельной. Свойство состоятельности оценки означает, что она должна сходиться по вероятности к истинному значению величины (измеряемого параметра) при неограниченном увеличении независимых измерений n [9, ф. (7.1)]:

$$\lim P\left(\left|m_x - m_x^*\right| < e\right),$$

где m_x – математическое ожидание; m_x^* – среднее арифметическое значение; e – положительная величина; P – доверительная вероятность.

Действительное значение физической величины [9, с. 166] – значение физической величины, найденное экспериментальным путем и настолько близко к истинному, что для поставленной измерительной задачи может ее заменить.

За действительное значение физической величины обычно применяется среднеарифметическое из ряда значений величин, полученных при равноточных измерениях.

Рассеивание результатов измерения – явление несовпадения результатов измерений одной и той же величины в ряду [10, ф. (8.15)].

Средняя квадратическая погрешность единичного измерения (в ряду равноточных измерений) S [10, ф. (8.17)] – обобщенная характеристика рассеивания результатов, полученных в ряду независимых равноточных измерений одной и той же физической величины вследствие влияния случайных погрешностей, вычисляемая по формуле:

$$S = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2}{n-1}}\,, \tag{1}$$

где S – средняя квадратическая погрешность единичного результата измерений, входящего в ряд из n измерений; $\overline{X}$ – среднее арифметическое из n измерений.

Средняя арифметическая погрешность единичного измерения в ряду измерений [10, ф. (8.16)] – обобщенная характеристика рассеивания из ряда n измерений, вычисляемая по формуле:

$$Ч = \frac{\sum_{i=1}^{n}\left|x_i - \overline{X}\right|}{n}\,,$$

где $Ч$ – средняя арифметическая погрешность как среднее арифметическое значение i-х погрешностей, присущих ряду измерений; $\left|x_i - \overline{X}\right|$ – абсолютное значение погрешности измерения.

Средняя квадратическая погрешность результата измерений (среднего арифметического) [10, ф. (8.18)] – характеристика случайной погрешности среднего арифметического значения результата одной и той же величины в данному ряду измерений, вычисляемая по формуле:

$$S_{\bar{x}} = \frac{S}{\sqrt{n}} = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2}{n(n-1)}}\,,$$

где $S_{\bar{x}}$ – средняя квадратическая погрешность результата измерений, полученного из ряда равноточных измерений.

Средняя квадратическая погрешность среднего арифметического в $\sqrt{n}$ раз меньше средней квадратической погрешности единичного измерения.

Точечная оценка при неизвестной дисперсии единичного измерения – оценивание с помощью доверительных интервалов (метод Ю. Неймана).

Наряду с выборочным средним $\overline{X}$ вводится выборочная дисперсия [9, ф. (7.7)] и ее несмещенная оценка для S^2:

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2 .$$

Оценивание измеряемой величины с помощью доверительных интервалов. Оценивание истинного значения производится по данным выборки – ряда значений, принимаемых случайной величиной в процессе n независимых измерений. Основными параметрами функции распределения случайной величиной X является МО m_x и дисперсия D_x . Точечными оценками этих параметров (m_x^* и S_x) называются оценки, выражаемые одним числом. Чем больше выборка n и чем точнее определена функция распределения измеряемой величины, тем точнее с помощью среднего арифметического значения m_x^* оценивается истинное значение измеряемой величины, а с помощью статистического (выборочного) дисперсии S_x^2 – разброс измеряемых значений. В этом случае (при большом числе измерений) за действительные значение измеряемой величины принимают точечную оценку истинного значения – среднее арифметическое значение m_x^* [9, с. 166].

Используем математико-статистическую теорию ошибок, содержащую рациональные способы обработки результатов наблюдений и измерений, в основе которой одно из положений устанавливает принятие принципа арифметической середины, приводящей к тому, что измерения укладываются в нормальный закон распределения.

Ошибка измерения *E* представляет разность между результатом измерения величины *X* и истинным его значением $e = X - X_{ист}$ [12].

В широком классе задач точечная оценка действительных значений параметров определена. К недостатку оценивания относится несовпадение $X_{ист}$ с измеряемой величиной. Кроме того, необходимо знать дисперсию единичного измерения. Более совершенный способ оцениваний – способ доверительных интервалов [6, 9].

Доверительный интервал погрешности результата измерений – интервал значений случайной погрешности, внутри которого с заданной вероятностью находится искомое (истинное) значение погрешности результата измерений. Доверительный интервал определяется зоной, равной $2tS_{\bar{x}}$ для каждого измерения как среднего арифметического [9].

Доверительные границы погрешности результата измерений – верхняя и нижняя границы доверительного интервала погрешности результата измерений. Доверительные границы в случае нормального закон распределения вычисляются как $\pm tS$, где S – средняя квадратическая погрешность измерения; t – коэффициент, зависящий от доверительной вероятности *P* и числа измерений *n* [10, ф. (8.20)].

Вводят среднее выборочное [11, ф. (7.10)]:

$$m_x^* = \overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i .$$

Средняя квадратическая погрешность измерения [11, ф. (7.17); 9, с. 186]:

$$S = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2}{n-1}} .$$

Принимая точечную оценку $\overline{X} = m_x^*$ за истинное значение измеряемой величины $X_{ист}$, необходимо определить ее точность. В качестве меры точности принимается симметричный интервал, определяемый доверительными границами (–*e*, +*e*), в котором с заданной вероятностью $P_д = 1 - q$ рассматривается ошибка оценки $e_x = \overline{X} - X_{ист}$ [13, ф. (2.36)], означающей, что истинное значение измеряемой величины с вероятностью $P_д$ нападает в интервал $\overline{X} - e_x,\ \overline{X} + e_x$ [13].

$$P\left(\overline{X} - e < X_{ист} < \overline{X} + e\right) = P_д ,$$

где $P_д$ – доверительная вероятность надежности доверительного интервала, задается по интерполяционным таблицам [6, 11].

Часто задают доверительный интервал от $\pm 3\sigma$, для которого доверительная вероятность (надежность доверительного интервала) составляет 0,9973.

Интервал шириной $\overline{X} - e_x,\ \overline{X} + e_x$ и вероятностью $P_д$ называют доверительным, а коэффициент q – уровнем значимости. Вводится переменная $t = \dfrac{e}{\sigma}$, функция $\Phi(t)$ является интегралом вероятностей (интегралом Лапласа) и выражает вероятность попадания случайной величины t в интервале вероятности $P\left(-e \le t \le e\right) = 2\Phi\left(e\right)$. Значения функции приведены в табл. 2 [13].

Интервальные оценки используют с целью увеличения достоверности результатов измерений доверительными интервалами и доверительными вероятностями. Вероятность $\alpha = \Phi\left(t\right)$ называется доверительной вероятностью ($\alpha = 1 - q$, где q – уровень значимости) (α = 0,90; 0,95; 0,9973) (табл. 3) [11].

Таблица 2

Значения интеграла вероятностей $\Phi(t)$

e	$\Phi(e)$	e	$\Phi(e)$	e	$\Phi(e)$	e	$\Phi(e)$
0,00	0,000	0,70	0,516	1,40	0,839	2,25	0,976
0,10	0,080	0,80	0,576	1,50	0,866	2,50	0,988
0,20	0,159	0,90	0,632	1,60	0,890	2,75	0,994
0,30	0,236	1,00	0,683	1,70	0,911	3,00	0,9973
0,40	0,311	1,10	0,729	1,80	0,928	3,30	0,9990
0,50	0,383	1,20	0,770	1,90	0,943	3,50	0,9995
0,60	0,452	1,30	0,806	2,00	0,955	4,00	0,9999

Таблица 3

Значения интеграла вероятностей $\Phi(t)$

$\Phi(t)$	$1 - \Phi(t)$	t	$\Phi(t)$	$1 - \Phi(t)$	t
0,50	0,50	0,675	0,992	0,008	2,652
0,600	0,40	0,842	0,993	0,007	2,697
0,70	0,30	1,036	0,994	0,006	2,748
0,75	0,25	1,150	0,995	0,005	2,807
0,80	0,20	1,282	0,996	0,004	2,878
0,85	0,15	1,440	0,997	0,003	2,968
0,90	0,10	1,645	0,998	0,002	3,090
0,95	0,05	1,960	0,999	0,001	3,291
0,96	0,04	2,054	0,9995	$5 \cdot 10^{-4}$	3,481
0,97	0,03	2,170	0,9999	$1 \cdot 10^{-4}$	3,891
0,98	0,02	2,326	0,99999	$1 \cdot 10^{-5}$	4,417
0,99	0,01	2,576	0,999999	$1 \cdot 10^{-6}$	4,892
0,991	0,009	2,612	0,9999999	$1 \cdot 10^{-7}$	5,327

Находят значение e, для которого выполняется равенство:

$$P\left(\left|m^* - m_x\right| < e\right) = \alpha = \Phi(t) \text{ [9, ф. (7.33)].}$$

При замене среднеарифметического значения m_x^* истинным $X_{ист}$ возникает погрешность $\pm e$ с вероятностью $\alpha = \Phi(t)$.

Тогда уравнение [9, ф. (7.33)] представляется как

$$P\left(m_x^* - e < X_{ист} < m_x^* + e\right) = \alpha = \Phi(t) \text{ [9, ф. (7.34)].}$$

Доверительная вероятность α есть вероятность того, что доверительный интервал со случайными границами (–e, +e) – истинное значение измеряемой величины.

Чем шире доверительный интервал погрешностей (–e, +e), тем выше вероятность попадание случайной погрешности измерений e в этот интервал. Для вычисления вероятности e удобнее в интервале введена новая переменная $t = \dfrac{e}{\sigma}$ [9, ф. (7.36)].

Доверительная вероятность и доверительный интервал. Принимая точечную оценку за истинное значение измеряемой величины X_n, оценивают меру точности. В качестве меры точности рассматривают симметричный интервал (–t, +t) $\left(-\Delta_г, +\Delta_г\right)$, в котором с заданной вероятностью располагается $X_{ист}$.

Вероятность попадания случайной погрешности в интервале, называемом доверительным интервалом с границами $\pm e$ при нормальном распределении выражается функцией $\Phi(t)$ (табл. 2). Выражая границу e в значениях σ, находят $t=\dfrac{e}{\sigma_m}$ и $\Phi(t)=\Phi\left(\dfrac{t}{\sigma_m}\right)$.

$\Phi\left(\dfrac{t}{\sigma_m}\right)$ соответствует доверительному интервалу $\pm e$ и называется доверительной вероятностью, а значение $1-\Phi(t)$ – уровнем значимости. Значения функции $\Phi(t)$ и $1-\Phi(t)$ приведены в табл. 3. На практике доверительная вероятность $\Phi(t)$ выбирается в соответствии с табл. 3 в пределах 0,9 и выше.

Значение погрешности e, определяющей половину длины доверительного интервала [9, ф. (7.38)]:

$$e=t\frac{\sigma_x}{\sqrt{n}}.$$

Из формулы $P\left(\left|m^*-m_x\right|<e\right)=\Phi(t)$ получаем

$$m_x^*-t\frac{S_x}{\sqrt{n}}<X_{ист}<m_x^*+t\frac{S_x}{\sqrt{n}},\ \text{[9, ф. (7.39), (7.40)]},$$

где S_x – статистическое СКО,

$$S_x=\sqrt{\frac{\sum_{i=1}^{n}\left(x_i-m_x^*\right)^2}{n-1}}.$$

Абсолютная погрешность усредненных результатов измерений:

$$\Delta_n=\pm t\frac{S_n}{\sqrt{n}}\ \text{[9, с. 170]},$$

где t – определено по значению доверительной вероятности $\Phi(t)$ (табл. 3).

Доверительное значение погрешности измерения:

$$\Delta=\pm t\frac{S_n}{\sqrt{n}}\ \text{[9, ф. (7.41)]}.$$

Абсолютная погрешность устраненных результатов измерений [9, с. 170]:

$$m_x^*\pm t\frac{S_n}{\sqrt{n}}=X_{ист}.$$

Заключение. Высокие требования к достоверности, точности результатов измерений обусловлены сложностью задач, решаемых информационными системами.

Точечная и интервальная оценки значения параметров слабых сигналов в каналах утечки информации в условиях высоких уровней шумов снижают порог чувствительности, статистической обработкой – разброс измеренных значений, что характеризует качество измерений и свойство измеряемой величины, доверительные интервалы и достоверные вероятности от конкретных условий достоверно устанавливать наличие (отсутствие) каналов утечки информации.

RATIONAL PRINCIPLES FOR PROTECTION OF VOICE DATA LEAKAGE CHANNELS, ASSESSMENT OF THEIR SECURITY

V.K. ZHELEZNJAK, A.G. FILIPOVICH, K.Ya. RAKHANAU, M.M. BARANOUSKI

Abstract

The processing of measurement results of discretely converted speech signals by statically mathematical principles based on P.L. Chebyshev. This significantly improves the accuracy

of the processing results, lowers the signal detection sensitivity threshold, and thus reliably establishes the presence or absence of a signal in the leak channel.

Список литературы

1. Гольденберг, Л. М. Цифровая обработка сигналов : справ. / Л. М. Гольденберт, Б. Д. Матюшкин, М. Н. Поляк. – М. : Радио и связь, 1986. – 312 с.
2. Бартон, Д. Справочник по радиолокационным измерениям / Д. Бартон, Г. Вард ; пер с англ. под ред. М. М. Вейсбейна. – М., 1976. – 392 с.
3. Вентцель, Е. С. Теория вероятностей / Е. С. Вентцель. – М. : Наука, 1984. – 576 с.
4. Тихонов, В. И. Оптимальный прием сигналов / В. И. Тихонов. – М. : Радио и связь, 1993. – 320 с.
5. Володарский, Е. Т. Планирование и организация измерительного эксперимента / Е. Т. Володарский, Б. Н. Малиновский, Ю. М. Туз. – Киев : Вища школа, 1997. – 280 с.
6. Линник, Ю. В. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений / Ю. В. Линник. – Изд. второе, испр. и доп. – Л. : Физматгиз, 1962. – 352 с.
7. Цыпкин, Я. З. Основы теории автоматических систем / Я. З. Цыпкин. – М. : Наука, 1977. – 560 с.
8. Левин, Б. Р. Теоретические основы статистической радиотехники / Б. Р. Левин. –М. : Сов. радио, 1968. – 584 с.
9. Кузнецов, В. А. Общая метрология / В. А. Кузнецов, Г. В. Ялунина. – М. : ИПК Изд-во стандартов, 2001. – 272 с.
10. Юдин, М. Я. Основные термины в области метрологии : слов.-справ. / М. Я. Юдин, М. Н. Селиванов, О. Ф. Тищенко, А. С. Скороходов ; под ред Ю. В. Гарбеева. – М. : Изд-во стандартов, 1989. – 113 с.
11. Тюрин, Н. Н. Введение в метрологию : учеб. пособие / Н. Н. Тюрин. – М. : Изд-во стандартов, 1989. – 248 с.
12. Венецкий, И. Г. Основные математико-статистические понятия и формы в экономическом анализе / И. Г. Венецкий, В. И. Венецкая. – М. : Статистика, 1974. – 279 с.
13. Электрорадиоизмерения : учеб. / В. И. Нефедов [и др.] ; под ред. проф. А. С. Сигова. – М. : Форум : Инфра, 2004. – 184 с.