3. Бабков, В. Ю. Передача информации в системах подвижной связи / В. Ю. Бабков [и др.]. – СПб. : СПбГУТ, 1999. – 152 с.

4. Лавров, С. В. Оценка защищенности каналов утечки высокоскоростной передачи речевых сигналов в цифровой форме / С. В. Лавров, В. К. Железняк, Д. С. Рябенко // Комплексная защита информации: материалы XXIV науч.-практ. конф. / г. Витебск (21–23 мая 2019 г.). – С. 74–77.

5. Васильев, Д. В. Радиотехнические цепи и сигналы: учеб. пособие для вузов / Д. В. Васильев, М. Р. Витоль, Ю. Н. Горшенков и др.; под ред. К.А. Самойло. – М. : Радио и связь, 1982. – 528 с.

В.К.ЖЕЛЕЗНЯК[1], А.Г.ФИЛИППОВИЧ[2], К.Я.РАХАНОВ[3], М.М.БАРАНОВСКИЙ[4]

ОБРАБОТКА ДАННЫХ ОЦЕНКИ ЗАЩИЩЕННОСТИ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

[1]Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь, заведующий научной лабораторией технической защиты информации, доктор технических наук, профессор

[2]Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь, главный специалист

[3]Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь, доцент, кандидат технических наук

[4]Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь, ведущий специалист

Техническая защита информации – это 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 (РС) в реальном масштабе времени. Сложность задач, решаемых информационными системами, разнообразие помеховых воздействий на сигналы обусловили общую проблему их защиты, оценку защищенности и контроля.

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

В таблице 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 (КУИ) [1] по формуле $\sigma_e^2 = -(6{,}02b + 10{,}79)$ дБ. Здесь $\Delta = 2^{-b}$ – шаг квантования.

Таблица 1 – Значения дисперсии в зависимости от разрядности квантователя

Разрядность b, бит	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 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 [4, 5]. Численные методы статистических испытаний реализуются с помощью средств вычислительной техники (СВТ) с первичными измерительными преобразователями, программным обеспечением (ПО) в автоматизированном режиме. Обработку ИС 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 которого является возможность выполнения эффективных количественных и качественных 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 КУИ, 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 РС 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 значения 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].

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 истинное значение погрешности результата измерений [10]. Доверительные границы погрешности результата измерений – верхняя и нижняя границы доверительного интервала погрешности результата измерений [10]. Доверительные границы в случае нормального закона распределения вычисляются как $\pm tS$, где S – среднеквадратическая погрешность измерения, t – коэффициент, зависящий от доверительной вероятности P и числа измерений n [10].

Оценка истинного значения [8, 9] 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 $m_x^* = \overline{X}$ [6, 11], а с помощью статической дисперсии S_x^2 разброс измеряемой величины. Сигнал в КУИ (сигнал + шум) равен сумме $X(t)$ и $n(t)$. Маскирующий шум в КУИ подчиняется нормальному закону распределения.

Если даны значения X_1, X_2, …, X_n из n независимых опытов случайной величины X с неизвестным математическим ожиданием m_x (МО) M_x и дисперсией D_x, то для определения этих параметров следует пользоваться приближенными значениями. Несмещенной оценкой дисперсии является величина $D_x = S_x^2$ [9]. Вычисление среднеквадратического отклонения производится по следующей формуле [10]:

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

где x_i – результат i измерения величины X_i.

При увеличении числа независимых измерений n оценка среднего арифметического значения должна сходиться по вероятности к МО случайной величины. Такая оценка называется

состоятельной и должна сходиться по вероятности к истинному значению величины при неограниченном увеличении независимых измерений n [9]:

$$\lim P\left(\left|m_x - m_x^*\right| < e\right), \tag{2}$$

где e – положительная величина;

P – доверительная вероятность.

Действительное значение физической величины [9] – значение физической величины, найденное экспериментальным путем и настолько близко к истинному значению, что для поставленной 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].

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

$$S = \sqrt{\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2 \Big/ (n-1)}, \tag{3}$$

Средняя арифметическая погрешность единичного измерения в ряду измерений [10] – обобщенная характеристика рассеивания n измерений, вычисляемая по формуле:

$$X = \sum_{i=1}^{n}\left|x_i - \overline{X}\right| \Big/ n, \tag{4}$$

где X – среднее арифметическое *i* погрешностей, присущих ряду измерений;

$\left|x_i - \overline{X}\right|$ – абсолютное значение погрешности измерения.

Среднеквадратическая погрешность результата измерений [10] – это характеристика случайной погрешности среднего арифметического значения результата одной и той же величины в ряду измерений, вычисляемая как $S_{\overline{x}} = S/\sqrt{n}$.

Точечная оценка при неизвестной дисперсии единичного измерения – оценивание с помощью: доверительных интервалов. Наряду с выборочным средним $\overline{X}$ вводится выборочная дисперсия [9] и ее несмещенная оценка:

$$S^2 = (1/(n-1))\sum_{i=1}^{n}\left(x_i - \overline{X}\right)^2. \tag{5}$$

Оценивание истинного значения производится по данным выборки. Основными параметрами функции распределения случайной величины являются МО и дисперсия. Точечными оценками этих параметров называются оценки, выражаемые одним числом. Чем больше выборка и чем точнее определена функция распределения измеряемой величины, тем точнее с помощью среднего арифметического значения оценивается истинное значение измеряемой величины, а с помощью дисперсии – разброс измеряемых значений. В этом случае за действительные значение измеряемой величины принимают точечную оценку истинного значения – среднее арифметическое [9].

Используем статистическую теорию ошибок, содержащую рациональные способы обработки результатов наблюдений, 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 значение погрешности.

Доверительный интервал определяется зоной $2tS_{\bar{x}}$ 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 – среднеквадратическая погрешность измерения; t – коэффициент, зависящий от доверительной вероятности P и числа измерений n [10].

Принимая точечную оценку $\overline{X} = m_x^*$ за истинное значение измеряемой величины $X_{ист}$ [11], необходимо определить ее точность. В качестве меры точности принимается интервал, определяемый доверительными границами ($-e$, $+e$), в котором рассматривается ошибка оценки e, то есть истинное значение измеряемой величины с вероятностью $P_д = 1 - q$ [6, 11] (q – уровень значимости) попадает в интервал $\overline{X} - e_x$, $\overline{X} + e_x$ [13]. Часто задают доверительный интервал от $\pm 3s$, для которого доверительная вероятность составляет 0,9973.

Вводится переменная $t = e/s$, функция $\Phi(t)$ является интегралом вероятностей и выражает вероятность попадания случайной величины t в интервале вероятности $P(-e \le t \le e) = 2\Phi(e)$, таблица 2 [13].

Интервальные оценки используют с целью увеличения достоверности результатов измерений доверительными интервалами и доверительными вероятностями. Вероятность $a = \Phi(t)$ называется доверительной вероятностью (таблица 3) [11].

Таблица 2 – Значения интеграла вероятностей $\Phi(e)$

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
0,60	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	5×10^{-4}	3,481
0,97	0,03	2,170	0,9999	1×10^{-4}	3,891
0,98	0,02	2,326	0,9999	1×10^{-5}	4,417
0,99	0,01	2,576	0,9999	1×10^{-6}	4,892
0,991	0,009	2,612	0,9999	1×10^{-7}	5,327

Находят значение e, для которого выполняется равенство $a = \Phi(t)$ [9]. При замене среднеарифметического значения истинным возникает погрешность $\pm e$ с вероятностью $a = \Phi(t)$ того, что доверительный интервал с границами ($-e$, $+e$) является истинным значением измеряемой величины. Чем шире доверительный интервал, тем выше вероятность попадания случайной погрешности измерений в этот интервал.

Принимая точечную оценку за истинное значение измеряемой величины, оценивают меру точности. В качестве меры точности рассматривают симметричный интервал ($-t$, $+t$), 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 $\Phi(t)$ (таблица 2). Выражая границу e в значениях σ , находят $t = e/\sigma_m$ и $\Phi(t) = \Phi(t/\sigma_m)$, что 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 таблице 3. На практике доверительная вероятность $\Phi(t)$ выбирается, в соответствии с таблицей 3, выше 0,9. Значение погрешности e, определяющей половину длины доверительного интервала $e = t(\sigma_x / \sqrt{n})$ [9]. Получаем:

$$m_x^* - t\left(S_x / \sqrt{n}\right) \le X_{ист} \le m_x^* + t\left(S_x / \sqrt{n}\right). \quad (6)$$

Абсолютная погрешность усредненных результатов измерений составляет $\Delta_n = \pm t\left(S_x / \sqrt{n}\right)$ [9], где t определено по значению $\Phi(t)$ (таблица 3).

Доверительное значение погрешности измерения $\Delta = \pm t\left(S_n / \sqrt{n}\right)$ [9]. Абсолютная погрешность устраненных результатов измерений $X_{ист} = m_x^* \pm t\left(S_x / \sqrt{n}\right)$ [9].

Заключение. Высокие требования к достоверности, точности результатов измерений обусловлены сложностью задач, решаемых информационными системами. Точечная и интервальная оценки значения параметров слабых сигналов в КУИ 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) КУИ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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.