

**МЕТОДОЛОГИЯ ОЦЕНКИ ПО ЕДИНОМУ КРИТЕРИЮ ЗАЩИЩЕННОСТИ
ОТ УТЕЧКИ АНАЛОГОВОГО И ДИСКРЕТИЗОВАННОГО РЕЧЕВОГО СИГНАЛА
В ШИРОКОПОЛОСНЫХ КАНАЛАХ ПЕРЕДАЧИ**

***В.К. Железняк, д-р техн. наук, проф.¹, К.Я. Раханов², С.В. Лавров¹,
А.Г. Филиппович², М.М. Барановский², С.В. Харченко¹***

*¹Полоцкий государственный университет имени Евфросинии Полоцкой,
Новополоцк, Беларусь*

*²Оперативно-аналитический центр при Президенте Республики Беларусь,
Минск, Беларусь*

Достоинства цифровых методов представления, обработки передачи и хранения информации, бурное развитие цифровой элементной базы, а это способствует тому, что цифровые методы обработки и передачи информации стали основным направлением систем передач (связи, телевидения и других коммуникационных систем). Проблемы цифровой обработки и передачи речи в системах различного назначения, принципы построения, характеристики и особенности функционирования, алгоритмы, протоколы, методы построения, характеристики и реализация элементной базы, и другие вопросы рассмотрены в работе [1].

Ключевые слова: критерий защищенности, речевой сигнал (РС), утечка сигнала.

Введение. Достоинством метода имитационного моделирования, включающие модели отдельных элементов сложной системы и систему взаимного соединения, модели входных и возмущающих случайных воздействий, а также средства анализа результатов моделирования является возможность проведения эффективной количественной и качественной (структурной) оптимизации сложной системы, а также неограниченная степень приближения модели к реальному объекту [2].

Исследования современного развития в области технической защиты информации (ТЗИ) от утечки по техническим каналам аналоговых и дискретизованных речевых сигналов (РС) в широкополосных каналах передачи являются актуальными. Впервые установлены каналы утечки РС в низкочастотном и высокочастотном диапазоне частот методом имитационного моделирования в шумах высокого уровня.

Это позволило по единому критерию установить требования к критерию защищенности аналогового и дискретизованного РС. Обеспечена высокая точность и достоверность обработки результатов при многообразии преобразования измерительного сигнала.

Значительные успехи информатики, включающие ее научные направления – техническую защиту информации, теорию помехоустойчивости и помехозащищенности

дают дальнейшее теоретическое исследование проблемных задач комплексной защиты информации.

Снижение методической и инструментальной неопределенности (погрешности) при одновременной возможности повысить чувствительность в оценке защищенности каналов утечки информации возможно при принципиально новых разработках методов и средств технической защиты речевых сигналов при высококачественной передаче по широкополосным каналам передачи. Информатизационные технологии реализуются автоматизированными системами точной оценки функционирования.

Оценка защиты информации от утечки по техническим каналам утечки связана с измерительной информацией, информационный параметр которой с заданной степенью точности и достоверности связан с информационными параметрами сигнала и должен измеряться с достаточно высокой точностью [3].

Основная часть. В основе всякой теории лежит представление сложного объекта в виде простых объектов как суммы простых сигналов, структур, ортогональных функций [4].

Весь вопрос в том, как выбрать единый критерий для аналогового речевого сигнала (РС) со строго линейной амплитудной характеристикой передачи по каналу и для дискретизованного речевого сигнала, в канале передачи которого введена нелинейность в виде ступенчатой функции. Для аналогового речевого сигнала измерительный сигнал гостирован в виде гармонического. Амплитудная характеристика гармонического сигнала нелинейная. Известно, что признак, который по оценке (сравнению) функционирующих объектов, рассматривается как наиболее существенный [5].

Критерий оценки защищенности от аналогового РС обладает рядом положительных свойств и обладает преимуществом по сравнению с другими аналогами по простоте обработки его амплитуды и частоты.

Критерий эффективности функционирования – показатель, по численному значению которого можно судить о степени достижения поставленных целей [6].

Критерий действенности – нормирующие условия, требования и показатели, согласно с которыми оценивается корректность реализации системы технической защиты информации (ТЗИ) [7].

На рисунке 1 представлена морфологическая модель формирования защиты информации сложной системы [8], из которой следует, что сложность ТЗИ определяется многообразием ее физического представления об информационных системах.

Система защиты информации предусматривает комплексное исследование объектов, систем и их элементов, алгоритмов измерений, обоснования критерия защищенности от утечки аналогового и дискретизованного РС при заданной точности оценки параметров с предельной чувствительностью, при слабых сигналах в шумах высокого уровня. К морфологическим аспектам оценки параметров относят инструментальные, методические параметры, полученные в различных условиях оценки погрешности обработки результатов [8].

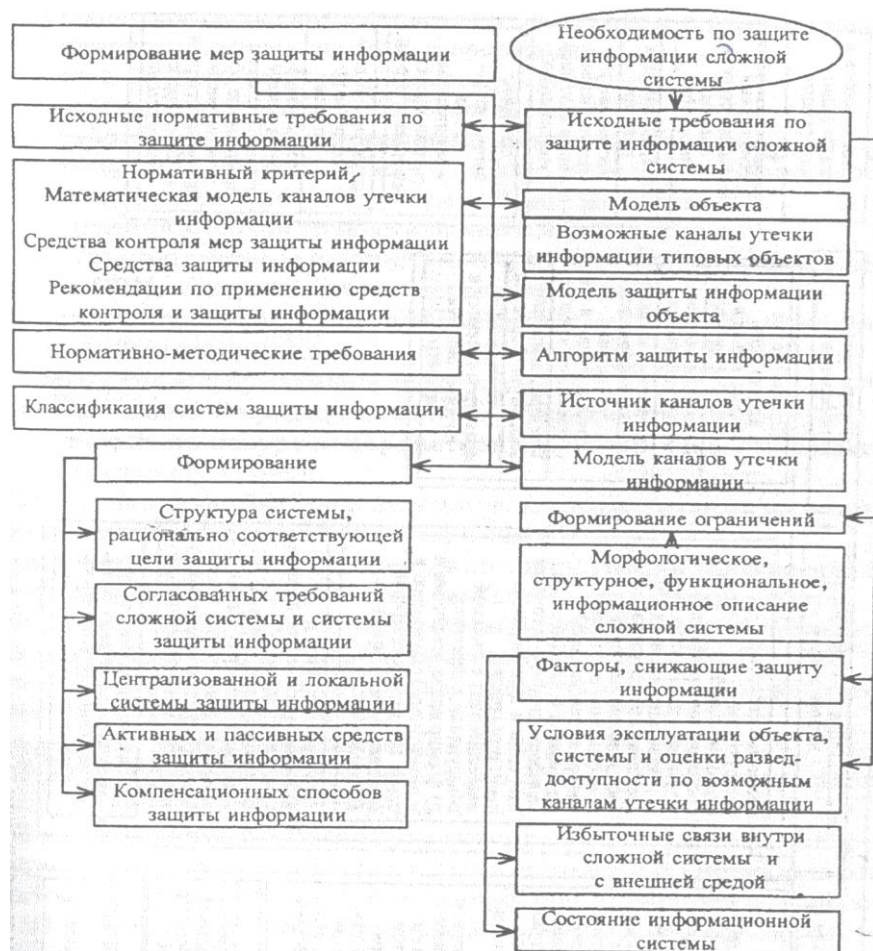


Рисунок 1. – Морфологическая модель формирования защиты информации сложной системы

Требования к контролю эффективности защиты информации представлены на рисунке 2.



Рисунок 2. – Требования к контролю эффективности защиты информации

На рисунке 3 приведена схема контроля (измерения) параметров, определяющих эффективность защиты информации.

Контроль эффективности ТЗИ устанавливает получение информации о соответствии эффективности и рациональности ТЗИ требованиям или нормам.

Эффективность ТЗИ – интегральный показатель, устанавливающий степень соответствия достигнутых результатов ТЗИ установленным нормативным требованием [8].

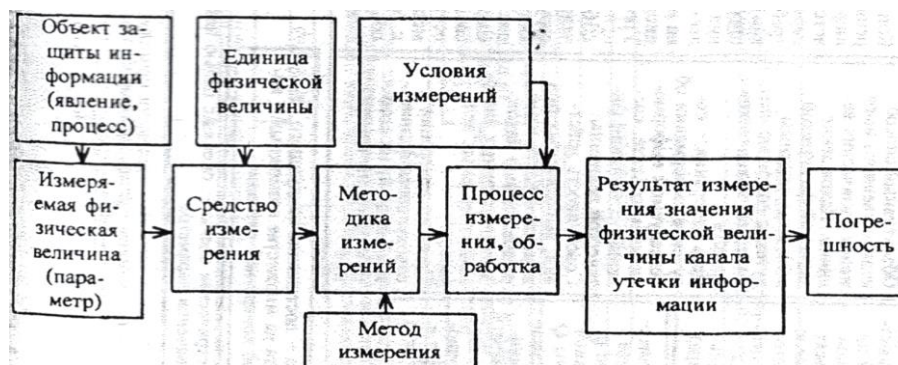


Рисунок 3. – Схема контроля (измерения) параметров, определяющих эффективность защиты информации

Результаты опыта. Определение среднеквадратического отклонения по опыт-ным данным. Несмещенной оценкой дисперсии является величина

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

Вычисление среднеквадратического отклонения при конечном числе n производится по следующей формуле

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

где m_x^* – среднее значение;

x_i – результат i -го измерения величины X_i ;

n – число измерений.

При увеличении числа n оценка среднего арифметического значения должна сходиться к M_x случайной величины. Такая оценка называется состоятельной.

Отклонения результатов (погрешность) измерений от действительного значения измеряемой величины X_d определяются по формуле

$$\Delta X_{\text{изм}} = X_{\text{изм}} - X_d,$$

где $\Delta X_{\text{изм}}$ – погрешность измерения.

Действительное значение физической величины – значение, найденное экспериментальным путем и настолько близко к истинному значению, что для поставленной измерительной задачи может ее заменить.

Рассеивание результатов измерения – явление несовпадения результатов измерений одной и той же величины в ряду.

Средняя квадратическая погрешность единичного измерения S – обобщенная характеристика результатов, полученных в ряду независимых измерений физической величины вследствие влияния случайных погрешностей

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

Средняя арифметическая погрешность единичного измерения в ряду измерений вычисляется по формуле

$$\varphi = \frac{\sum_{i=1}^n |x_i - \bar{X}|}{n},$$

где $|x_i - \bar{X}|$ – абсолютное значение погрешности измерения.

Средняя квадратическая погрешность результата измерений – характеристика случайной погрешности среднего значения результата величины

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

Точечная оценка при действительной оценке приближается к истинному значению $X_{\text{ист}}$:

$$\bar{X} \in N\left(X_{\text{ист}}, \frac{\sigma}{\sqrt{n}}\right).$$

При большом числе наблюдений n и отклонении более $\frac{3\sigma}{\sqrt{n}}$ вероятность оценки составляет около 0,0027. В ряде задач такие результаты точечных оценок вполне удовлетворительны [9].

Заключение.

1. Предложен единый для аналогового измерительный сигнал периодической последовательности импульсов треугольной формы, из которого путем обработки выделяется гармонический сигнал, по которому оценка защищенности аналогового и дискретно-квантованного речевого сигнала оценивается по единому критерию измерительным гармоничным сигналом аналогового и дискретно-квантованного речевого сигнала.

2. Обоснован критерий оценки защищенности речевого сигнала в аналоговой форме и при дискретно-квантованном преобразовании в КУИ.

3. Обоснованы оптимальные методы обработки слабых сигналов в шумах сигналов, шумов квантования в точке наблюдения в шумах высокого уровня.

4. Для оценки точности результатов предложено использовать элементы теории больших чисел.

ЛИТЕРАТУРА

1. Шелухин О.И., Лукьянцев Н.Ф. Цифровая обработка и передача речи / под ред. О.И. Шелухина. – М.: Радио и связь, 2000. – 456 с.
2. Четвериков В.Н., Баканович Э.А., Меньков А.В. Вычислительная техника для статистического моделирования / под ред. В.Н. Четверикова. – М.: Сов. Радио, 1978. – 312 с.
3. Комплексная защита информации: материалы XXIX науч.-практ. конф., 15–17 мая 2024 г. – М.: Авангард, 2024. – 292 с.
4. Трахман А.М. Введение в обобщенную спектральную теорию сигналов. – М.: Сов. Радио, 1972. – 352 с.
5. Толковый словарь математических терминов / О.В. Мантуров, О.В. Солнцев, Ю.И. Соркин и др. – М.: Просвещение, 1965. – 539 с.
6. Перишков В.И., Савинков В.М. Толковый словарь по информатике. – М.: Финансы и статистика, 1991. – 543 с.
7. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевский, Г.В. Кузнецов, В. О. Хорошко та інш.; за ред. проф. В.О. Хорошко. – К.: ДУІКТ, 2007. – 315 с.
8. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие / ГУАП. – СПб., 2006. – 188 с.: ил.
9. Основные термины в области метрологии: Словарь-справочник / М.Ф. Юдин, М.Н. Селиванов, О. Ф. Тищенко и др.; под ред. Ю. В. Тарбеева. – М.: Изд-во стандартов, 1989. – 113 с.