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

ФОРМИРОВАНИЕ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ПРИ ОТСЧЕТНО-ДИСКРЕТНОМ ПРЕОБРАЗОВАНИИ

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

[2]Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь, исследователь

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

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

В работе [1] исследовано, что для реализации высоких требований по передаче с высокой точностью речевой информации установлены методы ее защиты в каналах утечки речевых сигналов. Амплитудная характеристика квантователя при аналого-дискретном преобразовании речи является ступенчатой функцией и представляется в виде суммы идеальной линейной и нелинейной характеристик, последняя из которых формирует искажение сигнала [2]. Характеристикой искажений является последовательность импульсов пилообразной формы. Преобразованием Фурье эта последовательность раскладывается на спектральные составляющие четной и нечетной последовательностей k = 1, 2, 3, 4, 5 … . В работе [3] показана деформация косинусоидального колебания и периодической последовательности импульсов пилообразной формы при квантовании.

Решена задача обнаружения сигналов, зависимых от конечного числа неизвестных параметров в присутствии случайных помех. Методы статистических испытаний определяют методами решения математических задач и задач исследования сложных систем при помощи моделирования сложных реализаций и имитаций случайных процессов с оценкой их вероятностных характеристик.

Ряд Котельникова записывается как

$$f(t)=\sum_{k=1}^{\infty} f(k\Delta t)\frac{\sin 2\pi F(t-k\Delta t)}{2\pi F(t-k\Delta t)}. \qquad (1)$$

Полученное выражение представляет собой разложение непрерывной функции $f(t)$ в ряд по ортогональным функциям вида $\sin x/x$. Разложим периодическую стробирующую функцию, показанную на рисунке 1, в экспоненциальный ряд Фурье и изобразим ее частотный спектр. Стробирующая функция имеет ширину (длительность импульса) t_u и период повторения T, с.

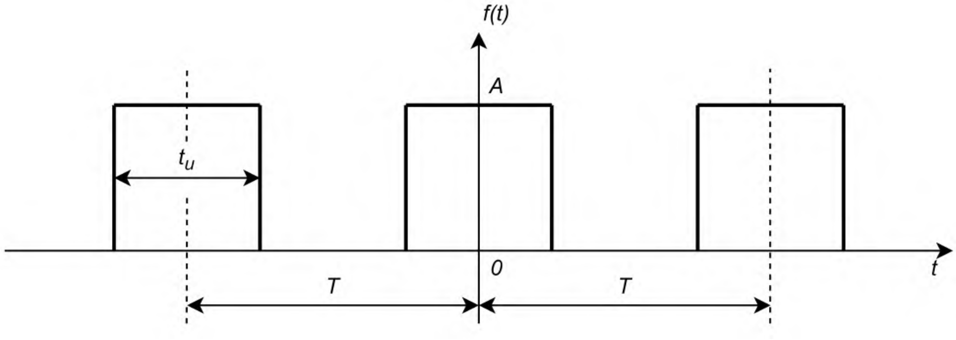


Рисунок 1 – Периодическая стробирующая функция

На интервале в один период функцию можно аналитически записать как

$$f(t)=\begin{cases} A \text{ при } \left(-\dfrac{t_{и}}{2}<t<\dfrac{t_{и}}{2}\right), \\ 0 \text{ при } \left(\dfrac{t_{и}}{2}<t<T-\dfrac{t_{и}}{2}\right). \end{cases}$$

Для удобства выберем пределы интегрирования от $-\frac{t_и}{2}$ до $T-\frac{t_и}{2}$:

$$F_n=\frac{1}{T}\int\limits_{-\frac{t_и}{2}}^{T-\frac{t_и}{2}} f(t)e^{-i n\omega_0 t}dt=\frac{1}{T}\int\limits_{-\frac{t_и}{2}}^{T-\frac{t_и}{2}} Ae^{-i n\omega_0 t}dt=\frac{-A}{-i n\omega_0 T}e^{-i n\omega_0 t}\Bigg|_{-\frac{t_и}{2}}^{\frac{t_и}{2}}=$$

$$=\frac{2A}{n\omega_0 T}\sin\left(\frac{n\omega_0 t_и}{2}\right)=\frac{At_и}{T}\left[\frac{\sin\left(\frac{n\omega_0 t_и}{2}\right)}{\frac{n\omega_0 t_и}{2}}\right]. \qquad (2)$$

Заключенная в скобки функция имеет форму $sin\, x/x$ и называется функцией отсчетов. В дальнейшем эта функция обозначается как

$$Sa(x)=\frac{\sin x}{x}. \qquad (3)$$

Функция отсчетов показана на рисунке 2.

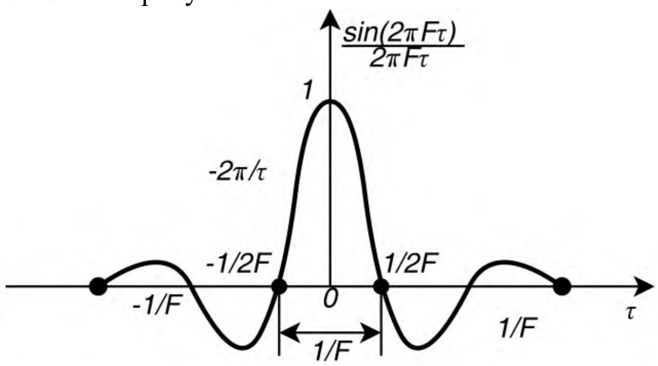


Рисунок 2 – Функция отсчетов $Sa(x)$

Заметим, что она осциллирует с периодом 2π, спадая по амплитуде с увеличением x и переходя через нуль в точках $x = \pm\pi, \pm 2\pi, \pm 3\pi$ и т.д. Из формулы (2) следует, что

$$F_n=\frac{At_и}{T}Sa\left(\frac{n\omega_0 t_и}{2}\right).$$

Поскольку $\omega_0=\frac{2\pi}{T}$, $\frac{n\omega_0 t_и}{2}=\frac{n\pi t_и}{T}$, получаем

$$F_n=\frac{At_и}{T}Sa\left(\frac{n\pi t_и}{T}\right), \qquad (4)$$

$$f(t)=\frac{At_и}{T}\sum_{n=-\infty}^{\infty}Sa\left(\frac{n\pi t_и}{T}\right)e^{i n\omega_0 t}. \qquad (5)$$

Из формул (4), (5) следует, что F_n – действительная величина, поэтому для частного представления достаточно одного спектра.

Величины $f(k\Delta t)$ называются отсчетами функции $f(t)$. Они определяют значения исходной функции $f(t)$ в дискретные моменты времени $k\Delta t$. Множитель $\frac{\sin 2\pi F(t-k\Delta t)}{2\pi F(t-k\Delta t)}$ называется функцией отсчетов.

Если обозначить $\tau = t - k\Delta t$, то функция отсчетов примет вид:

$$\psi[\tau] = \frac{\sin 2\pi F\tau}{2\pi F\tau}. \qquad (6)$$

Функция отсчетов принимает наибольшее значение, равное единице, в моменты времени $t = k\Delta t\ (\tau = 0)$ и обращается в нуль в моменты времени $t = (k \pm m)\Delta t$, где m = 1, 2, 3 … . Ширина главного лепестка функции отсчетов на нулевом уровне равна $1/F$. Спектр функции отсчетов является равномерным в полосе ($-F$, F) и равен нулю вне этой полосы. Действительно,

$$S(i\omega) = \int_{-\infty}^{\infty} \frac{\sin 2\pi F(t - k\Delta t)}{2\pi F(t - k\Delta t)} e^{i n\omega_0 t} dt = \begin{cases} \frac{1}{2F} e^{i k\Delta t\omega} & \text{при } |\omega| < 2\pi F, \\ 0 & \text{при } |\omega| > 2\pi F. \end{cases}$$

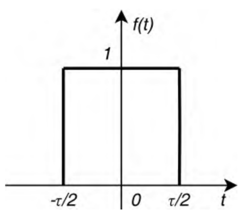
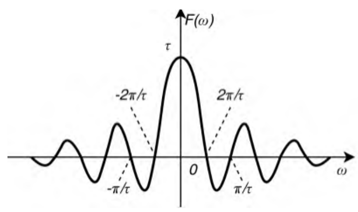
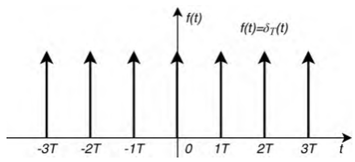
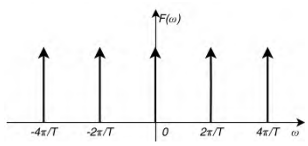
Модуль спектра $S(\omega) = \frac{1}{2F}$. Энергия сигнала через отсчетные значения выражается следующим образом:

$$E = \int_{-\infty}^{\infty} f^2(t)\,dt = \frac{1}{2F} \sum_{k=-\infty}^{\infty} f^2(k\Delta t). \qquad (7)$$

Если полоса частот сигнала $f(t)$ расширяется (таблица 1, п. 1), то Δt будет уменьшаться, и в пределе $F \to \infty$ функция отсчетов стремится к дельта-функции $t_{и}(t - t_k)$ (таблица 1, п. 2), а ряд Котельникова (1) превращается в интеграл:

$$f(t) = \int_{-\infty}^{\infty} f(t)\, t_{и}(t - t_k)\,dt. \qquad (8)$$

Таблица 1 – Некоторые сигналы и их преобразования Фурье

1. Стробирующая функция $f(t) = G_\tau(t) = \begin{cases} 1 \text{ при } \lvert t\rvert < \frac{\tau}{2}, \\ 0 \text{ при } \lvert t\rvert > \frac{\tau}{2}. \end{cases}$		$F(\omega) = \tau Sa\left(\frac{\omega\tau}{2}\right)$	
2. Последовательность дельта-функций $f(t) = \delta_T(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT)$		$F(\omega) = \omega_0 \delta_{\omega_0}(\omega) = \omega_0 \sum_{k=-\infty}^{\infty} \delta(\omega - k\omega_0)$, $\omega_0 = 2\pi/T$	

Свертка дельта-функции с любой функцией $f(t)$ дает равенство:

$$\int_{-\infty}^{\infty} f(t)\, t_{и}(t - t_k)\,dt = f(t_k) \int_{-\infty}^{\infty} t_{и}(t - t_k) = f(t_k),$$

из которого видно, что интеграл (8) не изменится от замены функции $f(t)$ ее значением $f(t_k)$. Следовательно, (8) преобразовывается в интеграл Дюмеля:

$$f(t) = \int_0^t f(\tau)\, t_{и}(t - \tau)\,d\tau. \qquad (9)$$

Вернемся к выражению ряда Котельникова (1). Каждое слагаемое этого разложения по физическому смыслу представляет отклик идеального фильтра нижних частот с частотой среза F на весьма короткий импульс, приходящий в момент $t = k\Delta t$ и имеющий площадь, равную мгновенному значению функции $f(t)$ в тот же момент. Отсюда следует, что при передаче сигнала $f(t)$ с ограниченным спектром по каналу связи необходимо через равные интервалы $\Delta t = \frac{1}{2}F$ взять отсчеты мгновенных значений сигнала и передать по каналу короткие импульсы, площади которых пропорциональны этим отсчетам. На приемном конце эти импульсы пропускаются через фильтр нижних частот, а исходный сигнал $f(t)$ восстанавливается как сумма откликов фильтра. Сигнал длительности T будет определяться $\nu = \frac{T}{\Delta t} = 2TF$ отсчетами.

$$G_\tau(\omega) = \frac{\tau_и}{T}\sum_{k=-\infty}^{\infty}\frac{\sin(k\Omega\tau_и/2)}{k\Omega\tau_и/2}G_\tau(\omega - k\Omega). \qquad (10)$$

Для сигналов с конечной длительностью можно сформулировать теорему отсчетов в частотной области, аналогичную теореме отсчетов во временной области, т.е. теореме Котельникова. Такая возможность следует из симметрии преобразований Фурье относительно переменных ω и t.

Заменяя выражение (1) t на ω, ширину спектра $2\omega_m$ на длительность сигнала T_c, интервал дискретизации $T = \frac{1}{2}f_m$ на $\Omega = \frac{2\pi}{T_c}$, функцию $s(t)$ на $G(\omega)$, получим теорему отсчетов в частотной области:

$$G(\omega) = \sum_{k=-\frac{N-1}{2}}^{\frac{N-1}{2}} G(k\Omega)\frac{\sin\frac{T_c}{2}(\omega - k\Omega)}{\frac{T_c}{2}(\omega - k\Omega)}.$$

Здесь N – это число выборок (спектральных линий) функции $G(\omega)$. Суммирование происходит по значениям k от $-(\frac{N-1}{2})$ до $(\frac{N-1}{2})$, включая $k = 0$. Таким образом, спектр сигнала конечной длительности T_c полностью определяется выборками, взятыми с интервалом $\Omega = \frac{2\pi}{T_c}$.

При дискретизации сигнала в частотной области общее число спектральных линий при ширине спектра $2\omega_m$ равно:

$$\frac{2\omega_m}{\Omega} = 2T_c f_m.$$

Заключение. Величины $f(kt)$ функции $f(t)$, сдвинутые на время $T = \frac{\pi}{\omega_m} = \frac{1}{2f_m}$, формируют канал утечки информации в виде амплитудно-импульсно-модулированных сигналов.

Число выборок от $(N - 1)$ до $(N + 1)$. Суммированное число выборок $G(k\Omega)$ спектральных линий по значениям k от $-(\frac{N-1}{2})$ до $(\frac{N-1}{2})$, включая $k = 0$, взятое с интервалами $\Omega = \frac{2\pi}{T_c}$, формирует канал утечки информации в виде амплитудно-импульсных моделированных сигналов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Железняк, В. К. Способ оценки защищенности преобразованного в цифровую форму речевого сигнала в каналах утечки информации / В. К. Железняк [и др.] // Комплексная защита информации: материалы XXIV науч.-практ. конф. / г. Витебск (21–23 мая 2019 г.). – С. 53–59.

2. Железняк, В. К. Анализ ошибки равномерного квантования периодической импульсной последовательностью треугольной формы в спектральной области / В. К. Железняк [и др.] // Проблемы инфокоммуникаций. – 2022. – № 1 (15). – С. 39–45.

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 $D/2$, среднеквадратическое значение $s^2 = D/\sqrt{12}$, плотность вероятности ошибки квантования составляет $1/D$ [2].

В таблице 1 приведены значения дисперсии s_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 $s_e^2 = -(6{,}02b + 10{,}79)$ дБ. Здесь $D = 2^{-b}$ – шаг квантования.

Таблица 1 – Значения дисперсии в зависимости от разрядности квантователя

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