

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОГО СИГНАЛА В КАНАЛЕ УТЕЧКИ ИНФОРМАЦИИ

д-р техн. наук, проф. В. К. ЖЕЛЕЗНЯК, Е. Р. АДАМОВСКИЙ

*(Полоцкий государственный университет
имени Евфросинии Полоцкой)*

Предложен метод оценки защищенности канала утечки информации на основе анализа огибающей измерительного сигнала в речевом диапазоне частот. Алгоритм включает генерацию измерительного сигнала и выделение его огибающей, излучение и измерение в канале утечки, выделение огибающей результирующего сигнала, вычисление коэффициента корреляции между исходной и полученной огибающими, сравнение с пороговым значением. Выполнено имитационное моделирование метода. Полученные результаты демонстрируют преимущество речевых сигналов перед гармоническими сигналами в качестве измерительных для оценки защищенности канала утечки информации.

Ключевые слова: *канал утечки информации, огибающая речевого сигнала, взаимная корреляция, техническая защита информации.*

Введение. Актуальность разработки методов оценки защищенности речевых сигналов (РС) в каналах утечки информации (КУИ) заключается в отсутствии единой модели восприятия речи [1, 2].

Питание усилителей, в том числе – аудиосистем, осуществляется через сеть переменного тока. Изменение потребления тока нагрузки приводит к нестабильности по току на входе стабилизатора [3]. Таким путем, РС из питаемой микрофонной системы способен проникать в КУИ в составе излучения усилителя. Другим способом образования КУИ РС является цифро-аналоговое преобразование (ЦАП), порождающее побочные излучения, которые содержат информацию об исходном сигнале [4].

РС характеризуется спектром сложной формы в широком диапазоне от 90 до 10–13 кГц [5]. Во временной области для РС может быть вычислена огибающая в узкой и заранее известной полосе низких частот, которая отражает скорость смены фонем речи.

Подобная предсказуемость открывает возможности для повышения точности оценки защищенности РС. Поэтому в данной работе предлагается метод оценки защищенности речевой информации КУИ на основе анализа огибающей измерительного речевого сигнала в точках излучения и наблюдения.

Методология исследования. Рассмотрим аналитический сигнал $s(t)$, реальная $s_{re}(t)$ и мнимая $s_{im}(t)$ части которого связаны преобразованием Гильберта [6]. Практическая значимость соотношения (1) заключается в возможности выделения из его частей мгновенной амплитуды $u(t)$ (2), что применимо и к реальным сигналам:

$$s_{im}(t) = \int_{-\infty}^{\infty} s_{re}(\tau) / \pi(t - \tau) d\tau, \quad (1)$$

$$u(t) = \sqrt{s_{re}^2(t) + s_{im}^2(t)}. \quad (2)$$

Значения мгновенной амплитуды соответствуют понятию огибающей сигнала, которой оперируют при обработке амплитудно-модулированных (АМ) сигналов.

При оценке защищенности РС в КУИ требуется установить взаимосвязь между сигналами в точке излучения и точке наблюдения – в канале утечки. В качестве меры их схожести предлагается значение коэффициента корреляции Пирсона, который вычисляется согласно формуле (3), и обозначаемого как R [7]. Коэффициент отражает, насколько изменение амплитуды одного сигнала влияет на изменение амплитуды другого сигнала.

$$R = \frac{M\left[\left(s(t) - M[s(t)]\right) \times \left(u(t) - M[u(t)]\right)\right]}{\sigma_{s(t)} \times \sigma_{u(t)}}, \quad (3)$$

где M – математическое ожидание;

σ – среднеквадратическое отклонение.

Предлагается метод оценки защищенности РС КУИ на основе взаимно-корреляционного анализа, заключающийся в генерации и излучении измерительного РС, огибающая которого сравнивается с огибающей в точке наблюдения. Оптимизация метода заключается в использовании сигнала, который был бы наиболее устойчив к шумам в КУИ за счет структурных свойств. Алгоритм (рисунок 1) включает шаги:

1. Генерация измерительного сигнала $s_{\text{тест}}(t)$ в речевом диапазоне частот в аналитической форме согласно формуле (1).

2. Выделение огибающей $u_{\text{тест}}(t)$ из измерительного сигнала $s_{\text{тест}}(t)$ согласно формуле (2).

3. Излучение измерительного сигнала $s_{\text{КУИ}}(t)$ в КУИ и его измерение в точке наблюдения как $s_{\text{КУИ}}(t)$, который в простейшей модели КУИ может быть представлен как аддитивная смесь с шумом в КУИ $w(t)$.

4. Выделение из $s_{\text{КУИ}}(t)$ огибающей $u_{\text{КУИ}}(t)$ аналогично п. 2.

5. Обработка $u_{\text{тест}}(t)$ и $u_{\text{куи}}(t)$ взаимно-корреляционным способом, получение значения коэффициента корреляции R согласно формуле (3).

6. Сравнение полученной величины R с нормативным значением $R_{\text{порог}}$.

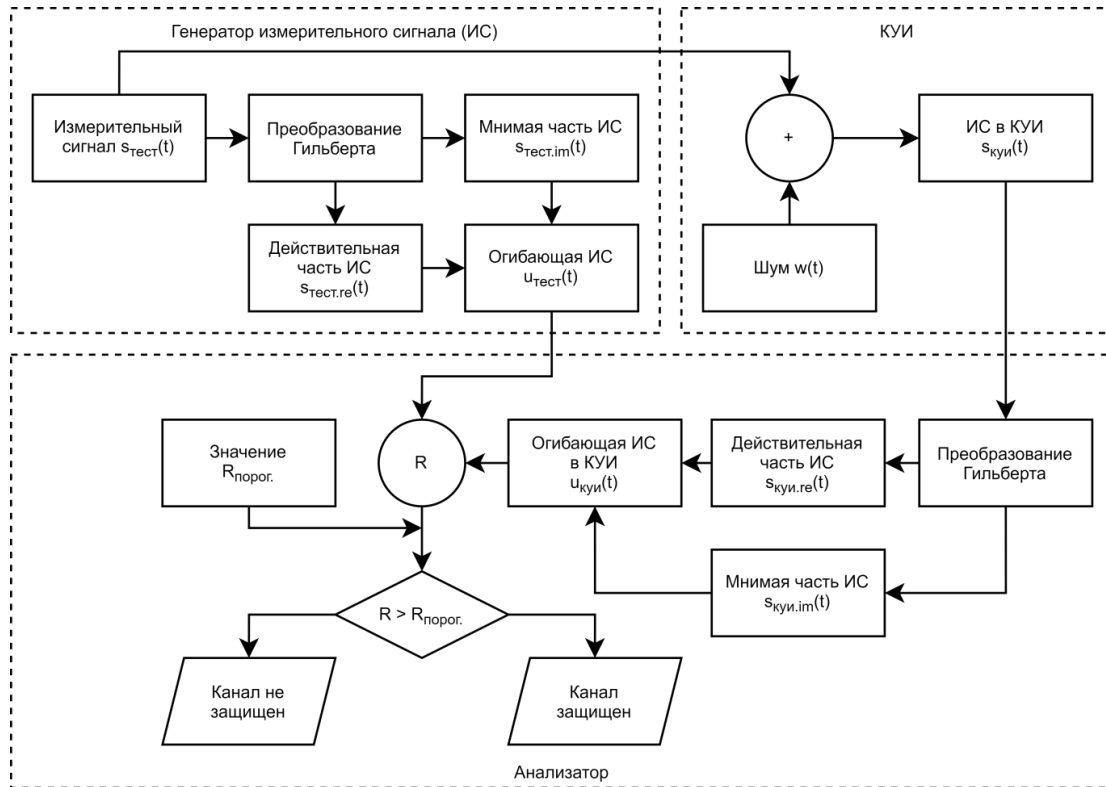


Рисунок 1. – Алгоритм имитационной модели метода оценки

Следует отметить, что результаты взаимно-корреляционного анализа могут быть использованы только при условии синхронизации обоих сигналов относительно друг друга.

Результаты и их обсуждение. Имитационное моделирование метода реализовано в программной среде MatLab, на рисунке 2 показаны его результаты: значения коэффициентов R и модуляции m измерительных сигналов как среднее арифметическое 10 измерений согласно представленному алгоритму.

В качестве измерительных сигналов был использован РС $s_{\text{речь}}(t)$ – озвученная на русском языке фраза-панграмма; выделенная огибающая $u_{\text{речь}}(t)$; гармонический АМ-сигнал $s_{\text{гарм.АМ}}(t)$ при $m = 1$; выделенная огибающая $u_{\text{гарм.АМ}}(t)$. Исходные РС подвергались зашумлению с различными отношениями сигнал/шум (ОСШ). В результате были получены сигналы $s_{\text{речь.куи}}(t)$, $u_{\text{речь.куи}}(t)$, $s_{\text{гарм.АМ.куи}}(t)$ и $u_{\text{гарм.АМ.куи}}(t)$ соответственно. Огибающие ограничивались по частоте до 30 Гц. Измерено соотношение исходного m и полученного $m_{30\text{Гц.куи}}$ коэффициента модуляции.

Дополнительно для сигналов $u_{\text{речь}}(t)$ и $u_{\text{речь.куи}}(t)$ был реализован вариант без ограничения по частоте для исследования влияния высокочастотной (ВЧ) составляющей на результаты моделирования, значение $m_{\text{куи}}$.

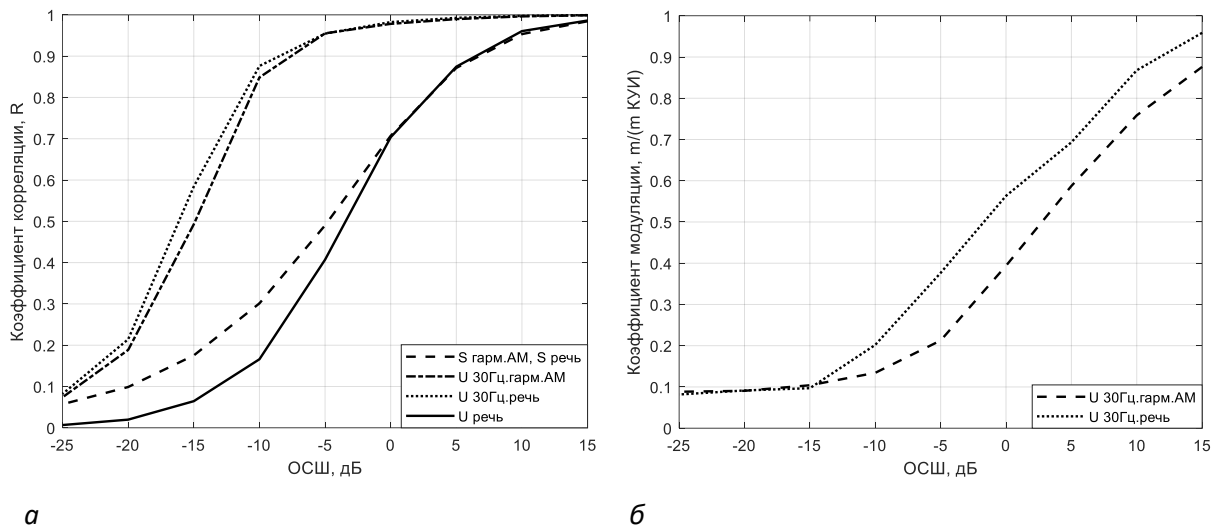


Рисунок 2. – Результаты имитационного моделирования метода при различных уровнях шума, сравнение полученных значений: коэффициентов взаимной корреляции R (а); коэффициентов модуляции m (б)

Из рисунка 2, а следует, что оценка корреляционных свойств сигналов во всей доступной частотной полосе дает низкие значения, поскольку влияние широкополосного шума снижает величину схожести. Это подтверждается быстрым спадом не ограниченных по частоте кривых. Рисунок 2, б демонстрирует характер падения коэффициента модуляции $m_{30\text{Гц.куи}}$, вычисленного по огибающим сигналов.

Заключение. Представлен метод оценки защищенности канала утечки информации на основе взаимно-корреляционного анализа огибающей измерительного сигнала в речевом диапазоне частот и результаты имитационного моделирования метода. Произведен сравнительный анализ результатов для огибающей речевого сигнала, исходного речевого сигнала и гармонического амплитудно-модулированного сигнала. Показаны преимущества использования огибающей речевого сигнала для оценки защищенности канала утечки информации, поскольку в этом случае достигаются большие значения коэффициента корреляции в шумах высокого уровня, следовательно использование огибающей РС оптимально.

ЛИТЕРАТУРА

1. Анохин, В. В. Рассмотрение критериев защищенности речи на основе словесной и смысловой разборчивости / В. В. Анохин, Е. А. Герасименко, А. В. Кондратьев // Специальная техника. – 2016. – № 6. – С. 22–28.
2. Железняк, В. К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В. К. Железняк, Ю. К. Макаров, А. А. Хорев // Специальная техника. – 2000. – № 4. – С. 39.

3. Костиков, В. Г. Источники электропитания электронных средств. Схемотехника и конструирование : учеб. для вузов / В. Г. Костиков, Е. М. Парфенов, В. А. Шахнов. – Второе издание. – Москва : Научно-техническое издательство "Горячая линия-Телеком", 2001. – 344 с.
4. Адамовский, Е. Р. Излучение цифро-аналогового преобразователя при обработке тестовых сигналов / В. К. Железняк [и др.] // Современные средства связи : материалы XXVI междунар. науч.-техн. конф., Минск, 22–23 окт. 2021 г. / Белорусская государственная академия связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2021. – С. 124–126.
5. Рева, И. Л. О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам / И. Л. Рева, В. А. Трушин, А. В. Иванов // Специальная техника. – 2016. – № 6. – С. 29–35.
6. Бутырский, Е. Ю. Преобразование Гильберта и его обобщение / Е. Ю. Бутырский // Научное приборостроение. – 2014. – Т. 24. – № 4. – С. 30–37.
7. Железняк, В. К. Защита информации от утечки по техническим каналам : учеб. пособие / В. К. Железняк ; Федеральное агентство по образованию, Государственное образовательное учреждение высшего профессионального образования Санкт-Петербургский государственный университет аэрокосмического приборостроения. – СПб. : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2006. – 187 с.