

ОЦЕНКА ЗАЩИЩЕННОСТИ И КОНТРОЛЯ РЕЧЕВОГО СИГНАЛА ПО СПЕКТРАЛЬНОЙ СОСТАВЛЯЮЩЕЙ ЕГО ОГИБАЮЩЕЙ

¹Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк Республика Беларусь

Актуальность разработки методов оценки защищенности речевых сигналов (РС) в каналах утечки информации (КУИ) заключается в отсутствии единой однозначной модели восприятия речи, а существующие методы оценки обладают такими недостатками, как значительные погрешности и ограниченное применение [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 электромагнитный (ЭМ) канал утечки в составе излучения усилителя. Другим способом образования КУИ РС является цифро-аналоговое преобразование (ЦАП), порождающее побочные излучения, которые содержат информацию об исходном сигнале [4].

Известно, что 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 и инфранизких частот, которая отражает скорость смены фонем речи. В данной работе предлагается метод оценки защищенности КУИ на основе анализа огибающей измерительного речевого сигнала в точке наблюдения.

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), фазы и частоты исходного колебания, что применимо и к реальным сигналам.

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

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

Набор значений мгновенной амплитуды соответствует понятию огибающей сигнала, которой оперируют при обработке амплитудно-модулированных (АМ) сигналов.

При оценке защищенности РС требуется установить взаимосвязь между сигналами в точке излучения и точке наблюдения – в канале утечки. В качестве меры схожести последовательностей предлагается использовать значение коэффициента корреляции Пирсона (3), обозначаемого как R [7], и который отражает то, насколько изменение одной величины влияет на изменение другой.

$$R = M[(s(t) - M(s(t))) \times (u(t) - M(u(t)))] / (\sigma_{s(t)} \times \sigma_{u(t)}) \quad (3)$$

где M – математическое ожидание; σ – стандартное отклонение.

Метод оценки защищенности РС КУИ на основе взаимно-корреляционного анализа заключается в генерации и излучении измерительного сигнала (ИС), огибающая которого сравнивается с огибающей в точке наблюдения. Алгоритм (рисунок 1) включает шаги:

1. Генерация измерительного АМ-сигнала $s_{тест}(t)$ в речевом диапазоне частот. При этом модулируемое многочастотное колебание $s_{несущ,тест}(t)$ должно включать набор кратных гармоник основного тона $f_i = i \times f_1$, который лежит в области 100-200 Гц, а модулирующее колебание $s_{мод,тест}(t)$ должно иметь квазипериодическую структуру в области до 30 Гц.

2. Выделение огибающей $u_{тест}(t)$ из измерительного АМ-сигнала.

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

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

5. Обработка $u_{тест}(t)$ и $u_{КУИ}(t)$ взаимно-корреляционным способом (3).

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

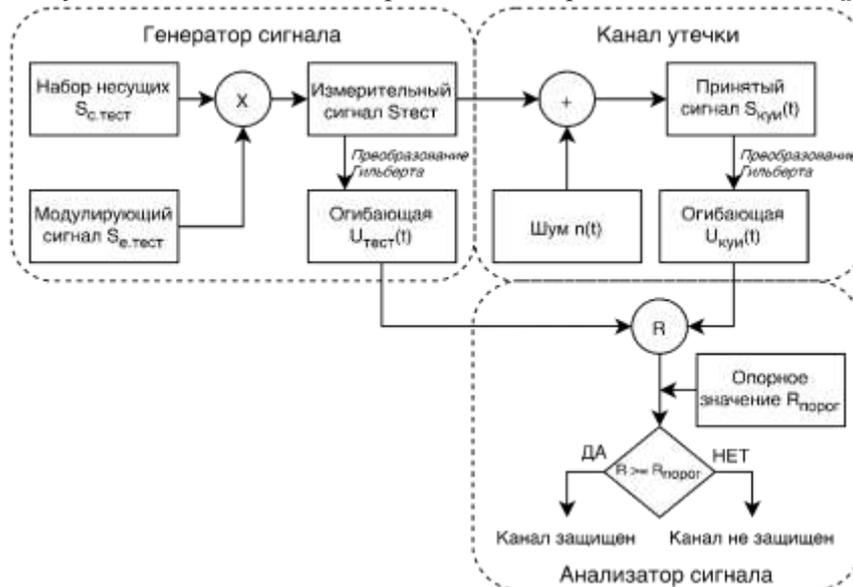


Рисунок 1 – Алгоритм имитационной модели метода оценки

Имитационное моделирование 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 $m_{\text{куи}}$.

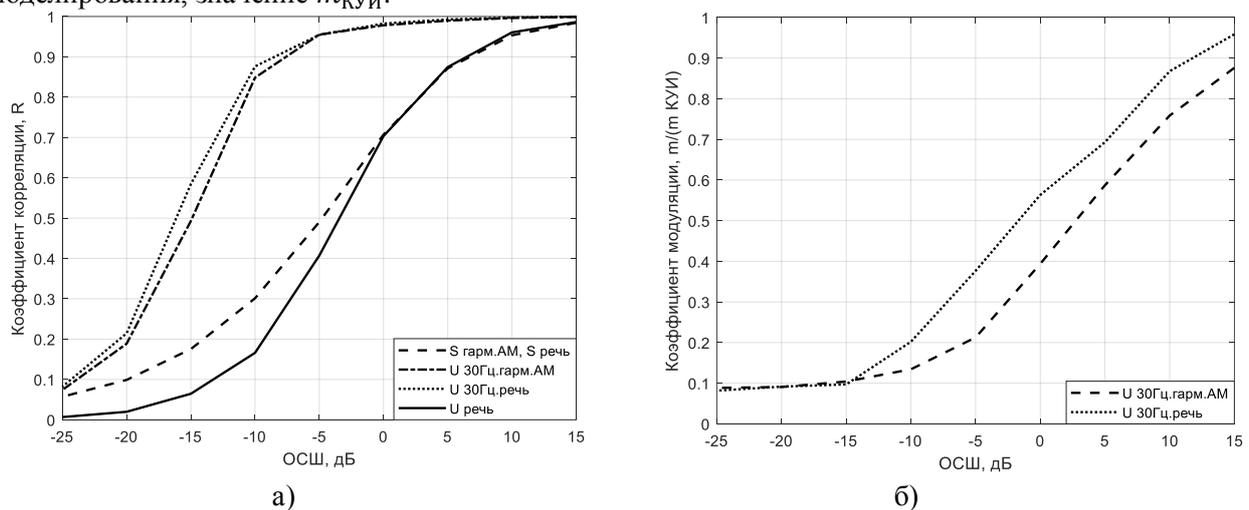


Рисунок 2 – Результаты моделирования при различных уровнях шума, сравнение: а) R ; б) m

Из рисунка 2а 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 2б демонстрирует характер падения коэффициента модуляции $m_{30\text{Гц.куи}}$, вычисленного по огибающим сигналов. Показано, что модуляция речевого сигнала более устойчива к шуму, чем гармонического модулированного сигнала.

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.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Анохин В.В., Герасименко Е.А., Кондратьев А.В. Рассмотрение критериев защищенности речи на основе словесной и смысловой разборчивости. *Специальная техника*. 2016; 6: – С. 22–28.
2. Гавриленко А.В., Дидковский В.С., Продеус А.Н. Сравнительный анализ некоторых методов оценки разборчивости речи /Акустический симпозиум «Консонанс-2007». Тезисы доклада, 25–27 июля 2007. – Киев, 2007. – С. 54–65.
3. Костиков В.Г., Парфенов Е.М., Шахнов В.А. Источники электропитания электронных средств. Схемотехника и конструирование. Горячая линия–Телеком. 2001: 344.
4. Адамовский, Е. Р. Излучение цифро-аналогового преобразователя при обработке тестовых сигналов / Е. Р. Адамовский [и др.] // Современные средства связи : материалы XXVI Междунар. науч.-техн. конф., г. Минск, 21–22 окт. 2021 г. / Белорусская государственная академия связи ; редкол. : А. О. Зеневич [и др.]. – Минск, 2021. – С. 124–126.
5. Трушин В.А., Иванов А.В., Рева И.Л. О корректировке методики оценки защищенности речевой информации от утечки по техническим каналам. *Специальная техника*. 2016; 6: – С. 22–30.
6. Бутырский, Е. Ю. Преобразование гильберта и его обобщение. *Научное приборостроение*. 2014; 24(4): – С. 30–37.
7. Рябенко Д.С., Лавров С.В., Боровкова Е.С. Приложение сигнальных графов и матричного анализа для математического моделирования каналов утечки информации. *Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки*. 2018; 4: – С. 56–60.

А.А.БАТУРА¹, А.В.БУДНИК², С.М.БОРОВИКОВ¹

НОВЫЙ ПОДХОД К ОЦЕНКЕ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ЭЛЕКТРОННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОКОММУНИКАЦИЙ

¹*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

²*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь*

Методы, используемые в отечественной [1, 2] и мировой [3–5] практике для расчета надежности электронных систем обеспечения безопасности, функционирующих на объектах любого назначения, в том числе выполняющих прием, хранение и передачу информации, принимают во внимание возникновение устойчивых отказов функциональных частей электронных систем безопасности. Эти отказы вызывают техническую неисправность функциональной части системы безопасности, что, в свою очередь, либо снижает вероятность защиты объекта (при наличии резервирования функциональной части), либо приводит к полной потере системой работоспособности (при отсутствии резервирования). В случае таких отказов восстановление работоспособности системы и/или обеспечение необходимой вероятности защиты объекта могут быть достигнуты путем ремонта и/или замены отказавшей функциональной части системы.

Практика использования электронных систем безопасности на объектах различного функционального назначения показывает, что для обеспечения защиты объектов принципиальными являются также временные отказы функциональных частей системы, которые, согласно новому ГОСТу в области надежности технических изделий [5], называют сбоями. Временный отказ (сбой) это самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора. Англоязычный термин этого отказа – *en interruption*. Причинами появления временного отказа являются естественные и искусственные воздействия факторов окружающей среды: молния, раскаты грома, сильный ветер, включение мощной электромагнитной промышленной установки и т.д. Возникновение временного отказа может приводить к тому, что например, датчик электронной системы безопасности, будучи технически