12. Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в мережах Wi-MAX та методів їх усунення // Защита информации: Зб. науч. трудов: Випуск 18. − К.:НАУ, 2011. − С. 39 − 44.
13. Офіційний сайт Лабораторії Касперського // www.kaspersky.ru
14. Удалённые сетевые атаки // http://ru.wikipedia.org/

Надійшла: 22.10.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 681.391

Архипов А.Е, Архипова Е.А.

АНАЛИЗ И ОБРАБОТКА ДАННЫХ АРТИКУЛЯЦИОННЫХ ИСПЫТАНИЙ

В статье рассмотрен вопрос обработки результатов экспертного оценивания словесной разборчивости для украинского языка при проведении артикуляционных испытаний, имитирующих распознавание речевых сообщений в условиях воздействия на речевой сигнал маскирующей акустической помехи. Получены графики зависимости словесной разборчивости от отношения сигнал/помеха, которые могут быть использованы для решения задач защиты речевой информации. Подтверждено большую эффективность цветной помехи по сравнению с белым шумом. Предложена описательная модель, которая на качественном уровне позволяет объяснить процесс формирования ошибок восприятия аудитором аудиообраза (речевой фрагмент + маскирующая помеха), отличия результатов артикуляционных испытаний при маскировке цветным и белым шумом, особенности распределения погрешности оценивания разборчивости при разных уровнях маскирующей помехи.

Ключевые слова: артикуляционные испытания, словесная разборчивость, речевой сигнал, математическая модель, аудиообраз.

Вступление. Из практического опыта известно [1], что нельзя составить подробной справки о содержании перехваченного разговора при словесной разборчивости менее 70-80%, а короткой справки-аннотации – при словесной разборчивости менее 40-60%. При словесной разборчивости менее 20-40 % наблюдаются значительные трудности для определения даже предмета разговора, а при словесной разборчивости менее 10-20% – это практически невозможно. При словесной разборчивости менее 10% в перехваченном разговоре осложнено определение признаков речи.

Приведенные сведения позволяют оценить эффективность возможных вариантов построения защиты информации от утечки по техническим каналам и выбрать наилучший. При этом для определения словесной разборчивости рекомендуется использовать инструментально-расчетный метод [1], который, как и другие инструментальные методы, не позволяет ответить на два вопроса: 1) как отражается наличие семантической составляющей речевого сообщения на понимании его содержания в условиях искажения речевого сообщения воздействием акустических помех, 2) как влияют (в случае применения средств активной защиты речевой информации от прослушивания) спектральные характеристики маскирующего сигнала на уровень разборчивости речи. Ответ на эти вопросы можно получить путем проведения артикуляционных испытаний, в ходе которых аудитору (артикулятору, слушателю) предлагаются для распознания записи фрагментов речевой информации (произнесенных слов) с аддитивно наложенным на них шумом, имитирующим влияние маскирующей помехи.

Ниже рассматриваются некоторые аспекты организации и проведения артикуляционных испытаний, а также обработки полученных в них результатов.

Проведение артикуляционных испытаний. Для проведения артикуляционных испытаний было осуществлено начитывание тестового материала (десяти украинских артикуляционных таблиц слов, по 50 слов в каждой [2, 3]) профессиональным диктором

Вячеславом Кумейко. Способ представления тестового материала в виде словесных таблиц выбран потому, что слово является наименьшей речевой единицей, которая несет смысл о явлении, событии или предмете. Чтение слов осуществлялось диктором ровным голосом при нормальном темпе речи, средней громкости и интервале между словами 3 ± 0,3 с. Диктор выдерживал ровный темп на протяжении всего чтения таблиц. Материалы записывались на электронный носитель с частотой дискретизации 44100 Гц.

Записи обрабатывались на компьютере, где к тестовому сигналу во временной области аддитивно добавлялись сигналы помехи с отношением сигнал/помеха (S/N), равным: 0; - 2,5; - 5; - 7,5; - 10 дБ, что имитирует условия активной маскировки речевого сигнала помехами. Данные точки отношений сигнал/помеха были выбраны в связи с тем, что в этом диапазоне происходит наиболее крутой спад показателя словесной разборчивости.

В качестве сигналов маскирования использовались два случайных процесса: со спектральной плотностью мощности "белого шума", сформированного стандартной процедурой пакета MatLab, и сигнал промышленного генератора типа "ANG 2200". Их часовые диаграммы и амплитудные спектры приведены на рис. 1. Записи прослушивались бригадой из семи аудиторов без выраженных дефектов слуха – одной женщины и шестерых мужчин в возрасте от 20 до 28 лет, которые не проходили специальной тренировки.

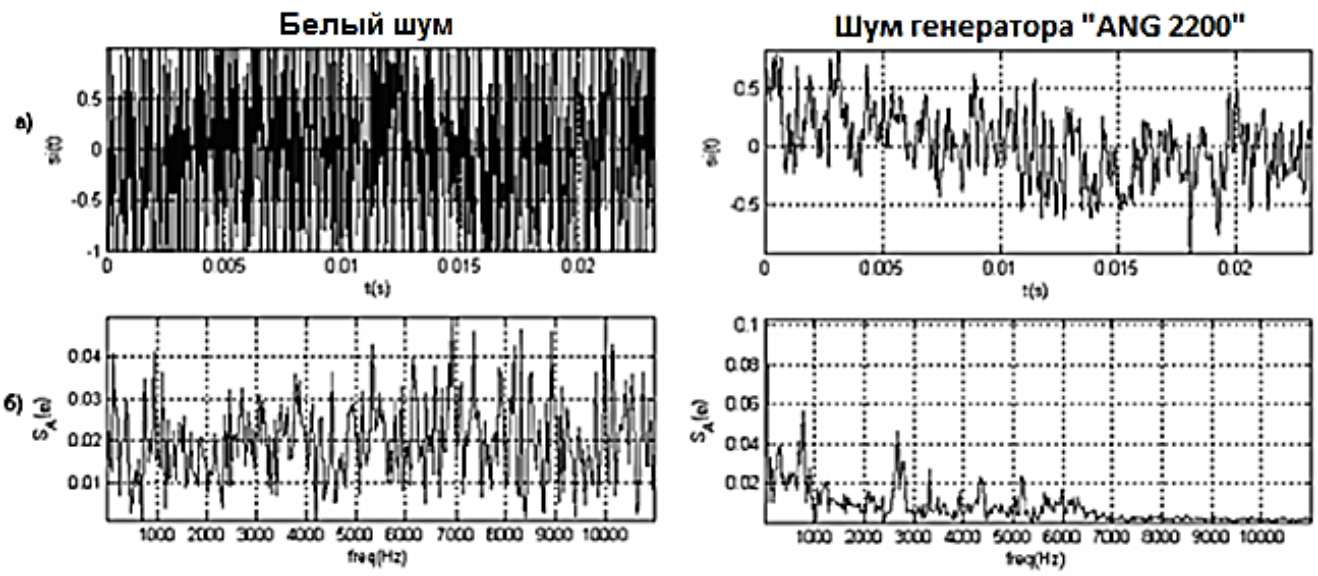

Рис. 1. Часовые диаграммы (а) и амплитудные спектры (б) двух сигналов маскирования: "белого шума" и помехи промышленного генератора "ANG2200"

При проведении испытаний тестовый сигнал воссоздавался через звуковые колонки компьютера, при этом громкость записи устанавливалась на комфортном для прослушивания уровне (около 70 дБ). После прослушивания текста аудитор записывал прослушанные слова в специальный бланк, если слово не было понятным, аудитор ставил в соответствующей слову графе прочерк. Все аудиторы прослушивали по 150 слов для каждой точки измерений. Достаточно большие объемы измерений усредняли влияние случайных факторов и субъективных особенностей отдельных аудиторов. Это позволяет предположить, что в ходе артикуляционных испытаний получены статистически стойкие и объективные данные.

В таблице 1 приведенные результаты артикуляционных испытаний по каждому аудитору для двух сигналов помех.

По результатам обработки табличных данных построены графики зависимости словесной разборчивости W от отношения S/N для украинского языка, которые можно сравнить с аналогичными данными для русского языка (рис. 2, 3.)

Таблица 1

Результаты артикуляционных испытаний для двух сигналов помех

Белый шум	Словесная разборчивость W, %				
№ аудитора	S/N=0 дБ	S/N=-2,5 дБ	S/N=-5 дБ	S/N=-7,5 дБ	S/N=-10 дБ
1	74	62,00	51,33	40,67	21,33
2	94,67	79,33	79,33	65,33	42
3	60,67	48,67	38	27,33	15,33
4	86	76,67	73,33	57,33	32
5	88	66,67	51,33	38,67	22,67
6	82	67	49,33	39,33	35,33
7	74,67	60,67	58	47,33	32
среднее	80,00	65,90	57,24	45,14	28,67
ANG 2200	Словесная разборчивость W, %				
№ аудитора	S/N=0 дБ	S/N=-2,5 дБ	S/N=-5 дБ	S/N=-7,5 дБ	S/N=-10 дБ
1	64,00	49,33	39,33	26,67	8
2	78,67	63,33	49,33	18,00	0
3	68,00	45,33	21,33	11	6,67
4	78,67	58,67	37,33	26,67	6,67
5	84,67	50,67	38,67	40,67	3,33
6	77,33	43,33	38,67	38	0
7	77,33	60,67	44	3,33	0
среднее	75,52	53,05	38,38	23,48	3,52

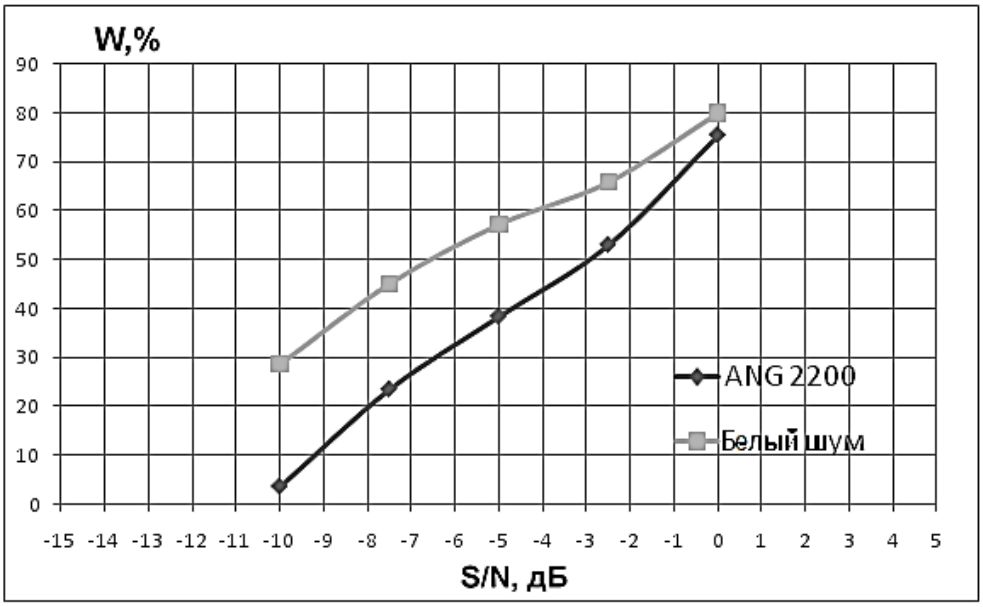

Рис. 2. Результат артикуляционных испытаний: средние значения словесной разборчивости для двух сигналов помех "белый шум" и генератора "ANG2200"

Из приведенных результатов артикуляционных испытаний следует, что использование помех промышленного генератора типа "ANG 2200" в сравнении с "белым шумом" дает более выраженный маскирующий эффект. Для "ANG 2200" значение словесной разборчивости меньше от 5% при S/N = 0 дБ, до 25% при S/N = - 10 дБ.

Используя эти данные вместе с результатами артикуляционных испытаний, можно установить необходимый минимальный уровень помех для заданного уровня защиты

выделенных помещений и каналов связи при допроектной оценке объекта или созданный уровень защиты при послепроектной оценке.

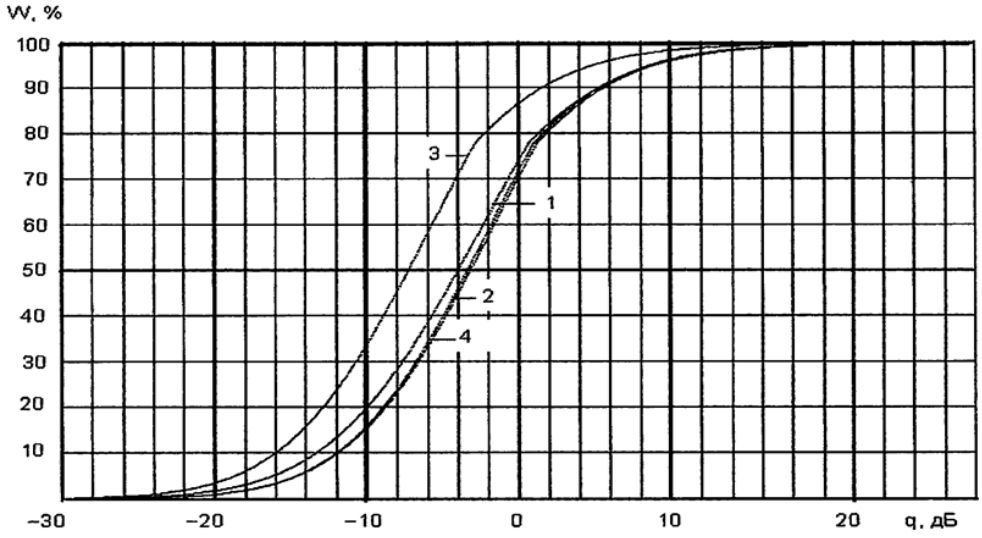

Рис. 3. Зависимость словесной разборчивости от интегрального отношения сигнал/помеха q: 1 – "белый шум"; 2 – "розовый шум" (шум со спадом спектральной плотности 3 дБ на октаву в сторону высоких частот); 3 – шум со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот; 4 – шумовая речеподобная помеха [4]

В целом полученные результаты могут быть полезными для решения задач защиты речевой информации в выделенных помещениях и каналах связи, при разработке методик проведения артикуляционных испытаний, которые бы учитывали особенности звучания украинского языка, для совершенствования методик специальных акустических исследований.

Кроме того, со стороны фонетики перспективным и интересным представляется анализ уровней разборчивости различных слов. В таблице 2 приведены примеры слов с высокой (W=91-100%), средней (W=43-52%) и низкой (W=0-5%) разборчивостями.

Таблиця 2

Примеры слов с высокой, средней и низкой словесными разборчивостями (W,%)

W, %	91-100%	43-52%	0-5%
1	снігуронька	дозвілля	беркут
2	вона	ртуть	згодом
3	морозиво	дідусь	однина
4	автомобіль	саджанець	заміс
5	жіночка	іржа	свист
6	мимоволі	заєць	скандал
7	золото	воєвода	ціннісний
8	телевізор	техніка	плодоніжки
9	політика	узбіччя	типовий
10	прохолода	шуміти	зацікавленість

Хорошо разборчивые слова в основном имеют в своем составе много гласных, звонких согласных (взрывные "б", "д", "г", фрикативное (щелевое) "в"), состоят по крайней мере из трех слогов (кроме слова "вона").

Слова с низким уровнем разборчивости более короткие, имеют относительно больше согласных, содержат глухие согласные "с", "т", "к", "п" и невокализированные "н", "ц", "л" и т. д.

Обработка данных артикуляционных испытаний. Основная задача обработки данных, полученных в ходе проведения артикуляционных испытаний, – определение зависимости уровня разборчивости от отношения сигнал/помеха S/N и оценивание степени достоверности полученных результатов. Количественно словесная разборчивость W оценивается процентным соотношением:

$$W\left(\frac{S}{N}\right) = \frac{n_1}{n}100\%, \quad (1)$$

где n – общее количество произнесенных диктором слов, n_1 – количество правильно воспринятых аудитором слов. При этом в i-ой контрольной точке (для определенного уровня отношения S/N_i) каждого j-ого аудитора рассчитывается частная разборчивость W_{ij}. Усреднение частных разборчивостей W_{ij}, $j = \overline{1,7}$ дает оценку разборчивости $\overline{W_i}$ в i-ой контрольной точке $i = \overline{1,5}$. Очевидно, что хотя исходными данными для расчета значений W_{ij} являются числа натурального ряда и 0, получаемые оценки $\overline{W_i}$ будут представлены значениями непрерывной случайной величины. Одной из основных задач обработки результатов артикуляционных испытаний является определение достоверности расчетных значений $\overline{W_i}$. Для решения этой задачи необходимо проанализировать погрешности определения оценок значений разборчивости, в частности, построить модель их формирования.

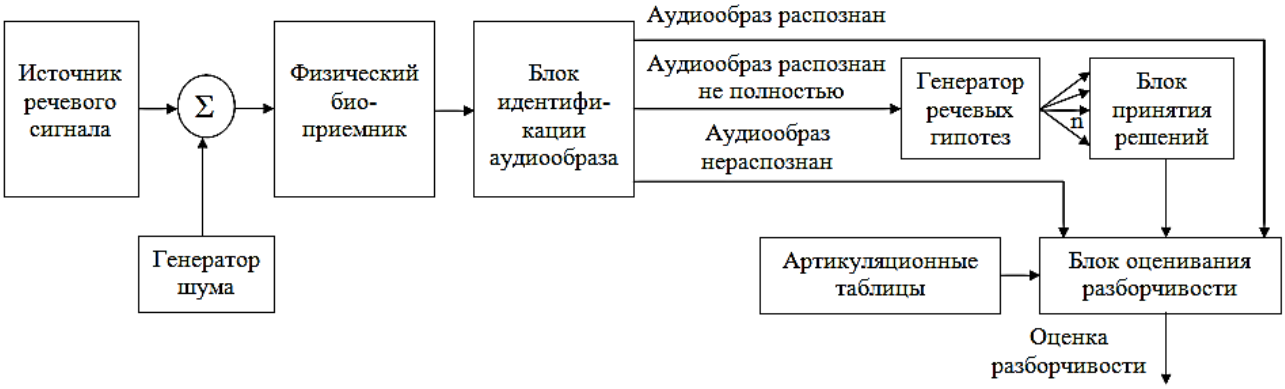

Рис. 4. Блок-схема преобразования информации
в процессе выполнения артикуляционных испытаний

Будем рассматривать бригаду аудиторов как некий преобразователь, на вход которого подается акустический сигнал (речь диктора + шум), а выходом является информация о проценте правильно распознанных элементов артикуляционных таблиц (см. рис. 4). Отличия индивидуального восприятия аудиторами общего входного сигнала приводят к различиям в оценках частных разборчивостей по каждой из таблиц и обуславливают случайный характер этих оценок. Назовем оценкой погрешности частной разборчивости разность

$$z_{ijk} = W_{ijk} - \overline{W_i},\ i = \overline{1,5},\ j = \overline{1,7}, \quad (2)$$

где W_{ijk} – разборчивость, рассчитанная по k-ой артикуляционной таблице по данным j-ого аудитора, $k = \overline{1,3}$.

Обычной практикой является принятие предположения о нормальности распределения $F(z_{ijk})$, что позволяет ограничиться лишь вычислением его выборочных характеристик. Однако гистограммный анализ совокупности оценок погрешностей частных разборчивостей, рассчитанных для контрольных точек отношения сигнал/помеха, показал, что в большинстве случаев распределения $F(z_{ijk})$ лучше аппроксимируются двусторонним симметричным экспоненциальным распределением (распределение Лапласа).

Сходная ситуация исследовалась в [5] при анализе распределения ошибок экспертов в данных, полученных при проведении многообъектной экспертизы. Было показано, что в каждой отдельно проводимой экспертизе ошибки эксперта распределяются по нормальному закону, но дисперсия этого распределения меняется случайным образом от экспертизы к экспертизе. При достаточно общих условиях справедливо предположение о распределении случайной дисперсии по закону Релея, тогда ошибки эксперта на множестве экспертиз (случайной многообъектной экспертизы) подчиняются распределению Лапласа [5,6], причем параметры этого распределения неизменны на протяжении всей многообъектной экспертизы. Однако в артикуляционных испытаниях параметры распределений $F(z_{ijk})$, $i = \overline{1,5}$ меняются с изменением значений отношения S/N_i. На рис. 5 приведены зависимости среднеквадратического отклонения σ_{zi} распределений $F(z_{ijk})$ от значений W_i, расчитанные для шумовых сигналов типа «белый шум» и «цветной шум» (сигнал генератора «ANG 2200"). По своей структуре обе зависимости сходны, одномодальны, их максимумы (15,5 и 16,21) достаточно близки.

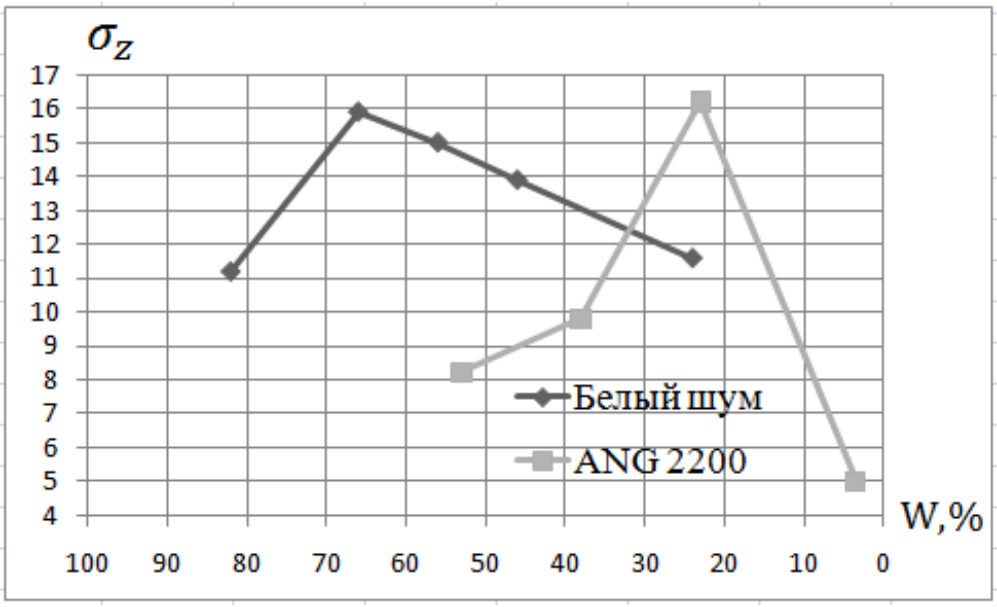

Рис. 5. Зависимости среднеквадратического отклонения σ_{zi} распределений $F(z_{ijk})$ от значений W_i, рассчитанные для шумовых сигналов типа «белый шум» и «цветной шум» (сигнал генератора "ANG 2200")

Рассмотрим возможное объяснение причин и механизма появления в результатах обработки артикуляционных испытаний данных с описанными выше особенностями.

Попробуем построить модель преобразователя входного возмущающего воздействия, которым является сигнал шума (помехи) в выходной сигнал – погрешность оценок разборчивости, вычисляемых по результатам работы бригады аудиторов. О погрешности Z известно, что это случайная величина, распределенная по закону Лапласа, плотность распределения вероятностей которой задается выражением:

$$f_i(z) = \frac{\lambda_i}{2} e^{-\lambda_i |z|}, \quad i = \overline{1,5}, \tag{3}$$

где параметр λ_i связан со средним квадратическим отклонением σ_z, оцениваемым по данным артикуляционных испытаний, соотношением $\lambda = \frac{\sqrt{2}}{\sigma_z}$.

Индекс i в выражении (3) указывает на изменение значения λ при переходе к новому соотношению сигнал/помеха.

Учитывая статичность описания выхода преобразователя, для описания его входа используем выражение плотности вероятности случайной амплитуды *Y* шума (помехи). Так как шум нормальный, получаем:

$$f(y) = \frac{1}{\sqrt{2\pi}\sigma_{yi}} e^{-\frac{y^2}{2\sigma_{yi}^2}},\ i = \overline{1,5}. \quad (4)$$

Очевидно, что исследуемый преобразователь должен выполнять преобразование плотности вероятности входного воздействия в соответствующую характеристику выходного. Задать этот оператор преобразования можно в виде некоторой случайной величины λ, взаимно независимой со случайной величиной Y и удовлетворяющей соотношению:

$$Z = \lambda Y. \quad (5)$$

Если плотность вероятностей случайной величины λ определить как $f(A)$, то с учетом взаимной независимости λ и Y справедливо выражение [6]:

$$f(z) = \int_{\infty}^{-\infty} f(A) f\left(\frac{z}{A}\right) \frac{dA}{|A|}, \quad (6)$$

$$\text{где } f\left(\frac{z}{A}\right) = f(y). \quad (7)$$

Для определения вида оператора λ (в частности, задания распределения $f(A)$) частично используем сведения, приведенные в [5, 10].

Предположим, что ошибки аудиторов, совершаемые в процессе артикуляционных испытаний, обусловлены в основном двумя причинами. Первая – невозможность распознавания исходного речевого сообщения (слова) в аудиообразе, полученном наложением помехи (шума) на исходный речевой сигнал, причем в процессе распознавания аудиообраз не ассоциируется с каким-либо словом. Назовем эту ошибку аудитора ошибкой 1-го вида. Причиной появления ошибки 2-го вида является неправильное распознавание аудиообраза. Эта ошибка возникает в случае, когда неполное (нечеткое) распознавание аудиообраза стимулирует генерацию ряда слов-гипотез, ассоциируемым с принятым аудиообразом. Выбор ложной гипотезы приводит к ошибке 2-го вида. Реальность существования описанных ошибок непосредственно подтверждается записями аудиторов в бланках артикуляционных испытаний.

Формализуем изложенное выше. Предположим, что X_1 – случайная величина, характеризующая интенсивность воздействия на аудитора фактора, приводящего к появлению ошибок 1-го вида, X_2 – аналогичная характеристика фактора, обуславливающего возникновение ошибок 2-го вида (далее в тексте могут совмещаться два понятия: «интенсивность действия фактора X_q» и «фактор X_q, приводящий к возникновению ошибок q-го вида» заменой их словосочетанием «фактор X_q»). Полагаем, что оба фактора независимы и распределены по нормальному закону:

$$f(x_q) = \frac{1}{2\pi\sigma_x} e^{-\frac{{x_q}^2}{2\sigma_x^2}}, \quad q = 1,2. \quad (8)$$

Оценим интенсивность их совместного воздействия на аудитора.

Очевидно, что совместное влияние факторов на аудитора характеризуется положением радиус-вектора *A* произвольной точки (x_1, x_2), в декартовой системе координат X_1OX_2, при этом, как следует из [7], плотность распределения интенсивности воздействия определяется плотностью вероятности длины вектора $A = \sqrt{x_1^2 + x_2^2}$:

$$f(A) = \frac{A}{\sigma_x^2} e^{-\frac{A^2}{2\sigma_x^2}}, \quad (9)$$

соответствующей распределению Рэлея.

С физической точки зрения полученный результат с учетом выражения (5) означает, что нормально распределенные случайные значения амплитуды входного воздействия Y, проходя через нелинейный преобразователь (бригада аудиторов), умножается на его коэффициент передачи, значения которого изменяются случайным образом, подчиняясь закону Рэлея. В соответствии с [5, 6], можно предположить, что значения сигнала на выходе преобразователя будут изменяться случайным образом, подчиняясь распределению Лапласа. Проверим это, подставив в (6) выражения для $f(A)$ и $f\left(\frac{z}{A}\right) = f(y)$:

$$f(z) = \frac{1}{\sqrt{2\pi}\sigma_y\sigma_x^2}\int_0^\infty e^{-\frac{A^2}{2\sigma_x^2}-\frac{z^2}{2\sigma_y^2A^2}}\frac{dA}{A} = \frac{1}{\sqrt{2\pi}\sigma_y\sigma_x^2}\int_0^\infty e^{-\delta A^2-\frac{\beta}{A^2}}dA, \qquad (10)$$

где $\delta = \frac{1}{2\sigma_x^2}$, $\beta = \frac{z^2}{2\sigma_y^2}$.

Интеграл (10) является частным случаем табличного интеграла [9, формула 3.478.4], нахождение которого требует вычисления цилиндрических функций. Опуская промежуточные вычисления, приведем окончательный результат:

$$f(z) = \frac{1}{2\sigma_y\sigma_x}e^{-\frac{|z|}{\sigma_y\sigma_x}}. \qquad (11)$$

Введя замену $\lambda = 1/\sigma_y\sigma_x$, приходим к стандартной форме представления плотности распределения для закона Лапласа (формула (3)).

Учитывая дискретность изменения параметра σ_y входного сигнала в контрольных точках: $\{\sigma_y\}$, $i = \overline{1,5}$, получаем объяснение скачкообразного изменения среднего квадратического отклонения σ_{zi} распределений $F(z_{ijk})$ на рис. 5: $\sigma_{yi} \Rightarrow \lambda_i = \frac{1}{\sigma_{yi}\sigma_x} \Rightarrow \sigma_{zi} = \sqrt{2}/\lambda_i$, т.е. увеличение уровня шума (рост σ_y) ведет к повышению разброса оценок разборчивости (рост σ_z). Однако на практике, при достижении достаточно высокого уровня шума (а значит при существенном снижении разборчивости *W*), шумовой сигнал начинает «забивать» слуховой канал аудиторов. Это сопровождается ростом числа прочерков в аудиторских бланках: аудиторы все чаще регистрируют факты нераспознаваемости аудиообразов, генерация ложных слов-гипотез падает, что вызывает снижение разброса оценок разборчивости, σ_z уменьшается. На графике рис. 5 этому явлению соответствует излом ранее возраставшей зависимости $\sigma_z(W)$ и последующий её спадающий участок, причем для белого шума излом наступает раньше, чем для цветного.

Приведенные выше математические соотношения не дают непосредственного объяснения наблюдаемой ситуации. Это обусловлено тем, что при построении модели (11) вводились упрощающее её построение допущения, в частности о постоянстве параметра σ_x в выражении (8). Среднее квадратическое отклонение σ_x, характеризующее интенсивность действия факторов X_1, X_2 на аудиторов, предполагалось неизменным и одинаковым для обоих факторов. Действительный механизм влияния факторов X_1, X_2 на аудитора реализует сложноформализуемую зависимость его индивидуальных качеств от уровня и характеристик шумового сигнала, причем фактор X_1, инициирующий появление ошибок 1-го вида, в большей степени связан с физиологическими параметрами аудиторов, а X_2 – с их эмоционально-интеллектуальными свойствами. Перечисленные параметры и свойства по-разному влияют на интенсивность факторов X_1, X_2, а значения $\sigma_x(X_1)$ и $\sigma_x(X_2)$ в общем случае являются функциями упомянутых параметров и свойств. Идентификация этих функций составляет отдельную задачу, решение которой требует проведения специальных исследований, выходящих за рамки артикуляционных испытаний. Из аудиторских данных очевидно лишь то, что высокому уровню интенсивности фактора X_2 (большее количество слов-гипотез) соответствуют возрастающие участки зависимости $\sigma_z(W)$.

Выводы. По результатам анализа и обработки данных артикуляционных испытаний предложена описательная модель процесса возникновения ошибок аудитора при распознавании им искаженных маскирующей помехой слов артикуляционных таблиц. Модель позволяет на качественном уровне интерпретировать особенности и характеристики ошибок аудитора, объяснить форму закона распределения погрешностей оценок разборчивости и в ряде случаев может быть использована для построения аппроксимативной математической модели этого распределения.

ЛИТЕРАТУРА

1. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации / С.В. Дворянкин, Ю.К. Макаров, А.А. Хорев // Защита информации. Инсайд. – М.: 2007. - №2. – С.39-45.
2. Архипова О.О., Журавльов В.М., Кумейко В.М. Артикуляційні таблиці слів української мови / О.О. Архипова, В.М. Журавльов, В.М. Кумейко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2009. – № 2/19. – С. 13-17.
3. Архипова О.О., Журавльов В.М., Доровських А.В. Таблиці слів української мови для артикуляційних випробувань розбірливості інформації, що передається трактами зв'язку / О.О. Архипова, В.М. Журавльов, А.В. Доровських // Зв'язок. – К., 2010. – № 1 (89). – С. 9-11.
4. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки / А.А. Хорев // Специальная техника. – М.: 2009.– № 4. – С. 49– 63.
5. Архипов О.Є., Архипова С.А. Модель ошибок экспертных оценок / О.Є. Архипов, С.А. Архипова // "Сучасні проблеми управління", Матеріали IV Міжнародної наук.-практичної конференції (28-30 листопада 2007р., м.Київ). – ІВЦ Видавництво "Політехніка"– К.: 2007. – С. 65-66.
6. Мудров В.И., Кушко В.Л. Методы обработки ошибок измерений / В.И. Мудров, В.Л. Кушко – М., Советское радио, 1976. – 192 с.
7. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и её инженерные приложения / Е.С. Вентцель, Л.А. Овчаров – М.: Наука, 1988. – 480 с.
8. Пугачев В.С. Теория вероятностей и математическая статистика / В.С. Пугачев – М.: Наука, 1979. – 496 с.
9. Градштейн И.С., Рыжик И.М. Таблицы интегралов, сумм, рядов и произведений / И.С. Градштейн, И.М. Рыжик – М.: ГИФМЛ, 1971. – с.
10. Архипов А.Е. О моделировании некоторых типов случайных последовательностей / А.Е. Архипов // Вестник Киев. политехн. ин-та – Вып. 12. – К.:1988 – С. 39-44.

Надійшла: 14.11.2012 р.

Рецензент: д.т.н., професор Кваснiков В.П.

УДК 004.056.2

Василенко В.С., Дубчак О.В., Василенко М.Ю.

МАТРИЧНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ЗАДАЧАХ ЗАХИСТУ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

У статті запропоновано використання одного із видів матричних криптографічних перетворень на базі коду умовних лишків у задачах захисту цілісності інформації, що дозволяє одночасно з контролем і відновленням цілісності інформаційних об‘єктів забезпечити високий рівень їх імітостійкості.

Ключові слова: конфіденційність, цілісність інформації, криптографічні перетворення, імітостійкість.

Вступ. Система технічного захисту інформації (ТЗІ) забезпечує у разі збереження, передавання або оброблення інформації її цілісність достовірною, повною і захищеною від ненавмисних і навмисних спотворень. Одним з основних способів забезпечення цілісності інформації в автоматизованих системах є застосування засобів контролю цілісності програмних засобів та оброблюваної інформації, включаючи в деяких випадках і її відновлення.

Не зупиняючись на причинах порушення цілісності [1], слід підкреслити, що частина загроз цілісності, зокрема з боку авторизованих користувачів і випадкового впливу природних і технічних факторів, може бути виявленою, а, отже, і усуненою лише за рахунок застосування ефективних механізмів контролю і відновлення цілісності, в яких використовуються процедури захищених від підробок перетворень інформації. Це пов’язане з тим, що основним завданням засобів контролю цілісності інформаційних ресурсів є