УДК 004.056.53: 534.8: 621.391.8

Ю. І. Касьянов, С. М. Нужний
Національний університет кораблебудування,
кафедра електрообладнання суден та інформаційної безпеки

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ГЕНЕРАТОРА РЕАЛЬНОЇ МОВОПОДІБНОЇ ЗАВАДИ ЗА КРИТЕРІЄМ РОЗБІРЛИВОСТІ МОВИ

Використано критерії розбірливості мови для оцінки ефективності використання генератора реальної мовоподібної завади та захищеності мовної інформації. Наведено результати дослідження генератора за цим критерієм.

Ключові слова: технічний захист мовної інформації, оцінка захищеності, віброакустичний канал, мовоподібна завада, розбірливість мови.

The article focuses on the use of intelligibility criterion to evaluate effectiveness of real speech-like interference generator and speech information protection. The research results of interference generator are given.

Key words: technical protection of speech information, security evaluation, vibroacoustic channel, speech-like interference, speech intelligibility.

Вступ

Мовна інформація є об’єктом особливої уваги зловмисників, які бажають оперативно отримати свіжі відомості про діяльність державних установ, різних підприємств і організацій, приватних осіб. Тому захист мовної інформації від витоку по технічних каналах завжди був і залишається актуальною проблемою, що підтверджено на державному рівні у новій редакції “Ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації…” та наказів Адміністрації ДССЗЗІ № 023 від 19.06.2015 та № 08 від 09.03.2016. Вирішення вказаної проблеми можливе тільки під час комплексного виконання триєдиного завдання: створення спеціалізованих технічних засобів протидії витоку інформації, розроблення методик оцінки захищеності інформації у нових умовах та впровадження нових нормативно-правових документів.

Найефективнішим є активний спосіб захисту, оскільки він оперативно дає можливість змінити рівень завади і пристосуватись до зміни ситуації. Наразі існує багато сертифікованих ДССЗЗІ України (“РІАС”, “МАРС-ТЗО-4-2”, “Топаз” і т.д.) та несертифікованих генераторів завад, які певною мірою відповідають вимогам нормативних параметрів у сфері ТЗІ. Але розвиток засобів знімання інформації та методів її обробки вимагає створення нових, ефективніших засобів зашумлення, якими є генератори мовоподібних завад. Впровадження у практику таких генераторів потребує нових підходів до критеріїв і методів оцінки їх ефективності та нормування захищеності мовної інформації.

Мета роботи – визначити основні принципи оцінювання ефективності використання генераторів реальних мовоподібних завад за критерієм розбірливості мови та їх апробація під час дослідження генератора ОССА-1, розробленого на кафедрі електрообладнання суден та інформаційної безпеки Національного університету кораблебудування.

Доцільність оцінювання за критерієм розбірливості мови

Оскільки завдання як пасивного, так і активного захисту мовної інформації від витоку акустичним каналом полягає у забезпеченні у точках можливого знімання інформації (контрольних точках) такого співвідношення між мовним сигналом і завадою, за якого знімання інформації певною мірою, що залежить від необхідного ступеня захисту, є неможливим, то загальноприйнятим критерієм захищеності наразі є відповідність відношення сигнал/шум, виміряного у контрольних

точках значенням, встановленим нормативними документами. Причому вимоги нормативних документів традиційно прив'язані до завади типу "білий шум" [1] і не враховують впливу виду завади на ефективність захисту мовної інформації.

У той самий час первинною мірою зрозумілості прийнятої мовної інформації є розбірливість мови, яка визначається як відносна кількість правильно розпізнаних елементів мови. І саме цей критерій вже давно використовується для оцінювання якості каналів мовного зв'язку та акустики приміщень [2–5].

Розбірливість мови переважно залежить від відношення сигнал/шум у точці прослуховування, на чому побудовано формантний та багато інших об'єктивних методів визначення розбірливості мови [2, 6]. Але ця залежність неоднозначна.

Проведено багато досліджень [6, 7] з використанням формантного методу, де отримано залежності словесної розбірливості мови від інтегрального відношення сигнал/шум за різних типів шумових завад, які показують, що різні завади по-різному впливають на сприйняття мовної інформації (за однакових відношень сигнал/шум матимемо різну розбірливість мови). Ці залежності показують, що ефективність зашумлення "рожевим" та мовоподібним шумом (шумом, який отриманий з "білого" і має обвідну спектра довготривалої мови) вищу, ніж "білим".

Отже, критерій відношення сигнал шум під час оцінювання захищеності мовної інформації є неоднозначним щодо сприйняття інформації зловмисником за різних видів завад. Врахування ж в нормативних документах специфіки завад теж є недоцільним через їх різноманіття.

Це гальмує впровадження нових ефективніших генераторів завад, оскільки їх використання за нижчих рівнів створюваної завади, які забезпечуватимуть той самий рівень розбірливості під час покращення умов роботи у виділених приміщеннях, входить у суперечність з вимогам нормативних документів. У той самий час урахування в нормативних документах специфіки завад теж є недоцільним через їх розмаїття.

У цій ситуації доцільним є використання як критерію захищеності мовної інформації безпосередньо міри сприйняття інформації – розбірливості мови. Цей критерій зробить оцінку інваріантною до типу завади та врахує властивості мовного сигналу і слуху.

Доцільність використання цього критерію в оцінці звукоізоляційної здатності огороджувальних конструкцій наведено у [8].

Доцільність підтверджується і тим, що у багатьох зарубіжних країнах, зокрема в Росії та США, критерій розбірливості мови активно впроваджується у практику та створюються сертифіковані методики оцінки захищеності мовної інформації на його основі. У [9] наведено обґрунтування та наведено орієнтовні значення допустимої словесної розбірливості W у контрольних точках для різних ступенів захищеності мовної інформації, а також відповідні значення відношення сигнал/шум q для завади типу "білій шум" (таблиця).

Критерії захищеності виділених приміщень

Ступінь захищеності	Критерій захищеності	
	відношення сигнал/шум	словесна розбірливість
Приховування факту ведення переговорів у виділеному приміщенні	$q \le$ -14 дБ	$W \le 10$ %
Приховування предмета переговорів у виділеному приміщенні	$q \le$ -10 дБ	$W \le 20$ %
Приховування змісту переговорів у виділеному приміщенні	$q \le$ -8 дБ	$W \le 30$ %
Приховування змісту переговорів у виділеному приміщенні від ненавмисного прослуховування (без технічних засобів)	$q \le$ -6 дБ	$W \le 40$ %

Отже, актуальним завданням є розроблення ефективних методів і методик оцінювання захищеності мовної інформації за критерієм розбірливості мови та внесення на їх основі змін до нормативної бази України з технічного захисту інформації.

Основні принципи побудови генераторів реальних мовоподібних завад та оцінки їх ефективності

Розвиток спеціалізованих напрямків аналізу складних сигналів та принципів формування мовних сигналів дали змогу створити методики, які уможливлюють проводити очищення фонограм сигналів від таких "кольорових" шумів. Це зумовило розроблення та розвиток ефективніших генераторів реальних мовоподібних завад, які формуються (синтезуються) з мовних сигналів. При цьому можливе формування перешкоди як з мовних фрагментів (відрізків), які не корелюються з сигналом, що приховується, так і безпосередньо з нього [10].

Завади, які формуються з мовних фрагментів, що не корелюються з приховуваним сигналом, є завади типу "мовний хор" або "гомін (галас) натовпу". Такі завади формуються змішанням фрагментів промови кількох людей (дикторів).

Серед мовоподібних завад, що формуються з сигналу, який необхідно приховувати, можна виділити два типи:

а) реверберaційний – завада формується з фрагментів приховуваного мовного сигналу багаторазовим їх накладення з різними рівнями;

б) інверсійний – завада, що формується з приховуваного мовного сигналу за допомогою складної інверсії його спектра.

Однак і такі пристрої мають багато системних недоліків: обмеженість довжини коду формування завади (тобто він є псевдовипадковим) та можливість проведення фільтрації несанкціонованих фонограм методами виявлення нетипових фонем.

Запропоновано третій тип мовоподібної завади ("переставна"), яка у першому наближенні може розглядатися як завада комбінованого типу, що має власну розширену систему криптографічного захисту. Завада формується з приховуваного мовного сигналу поточного та попереднього тактів, складним переставлянням часових та частотних смуг з випадковими довжиною, кількістю та інверсією.

За цим принципом на кафедрі ЕОС та ІБ НУК розроблений та виготовлений експериментальний зразок генератора мовоподібної завади ОССА-1, який наразі проходить дослідницькі випробування.

Ефективність генератора реальної мовоподібної завади, зокрема розробленого в НУК, може бути визначена за залежністю розбірливості мови від відношення сигнал/завада, аналогічною до отриманих в [6, 7]. Однак, оскільки завади такого типу, на відміну від шумових мовоподібних завад, які отримали на основі "білого" шуму, хоч і матимуть аналогічність з інформаційним мовним сигналом енергетичного спектра довготривалих фрагментів, але матимуть динамічний короткочасний спектр, то використаний в [6, 7] формантний метод може дати істотні похибки. Враховуючи це та з метою максимального врахування особливостей такого зашумлення, для розробки методики випробувань таких генераторів взято метод артикуляційних випробувань [2], який вже давно використовується для оцінювання якості каналів мовного зв'язку і нормований багатьма стандартами: ГОСТ 16600-72 (діє в Україні), ISO 9921:2003, ГОСТ Р 50840-95, ANSI S3.2-2009, ГОСТ Р 51061-97 тощо. Методика спирається на вказані стандарти, але враховує, що якість каналу зв'язку та захищеність інформації залежать від розбірливості мови прямо протилежно. Тому за найгіршим варіантом щодо витоку інформації в розробленій методиці, окрім таблиць слів, передбачено також використання фраз з ключовими словами або зв'язних текстів.

Характеристики залежності словесної розбірливості від відношення сигнал/шум для генератора того чи іншого типу завади під час оцінювання захищеності мовної інформації за критерієм розбірливості мови дають змогу легко визначити для цього генератора необхідний рівень сигналу завади, який забезпечить нормативне значення розбірливості для бажаного ступеня захищеності.

Дослідження генератора реальної мовоподібної завади ОССА-1

Завдання дослідження полягало в отриманні залежності словесної розбірливості від відношення сигнал/завада під час використання генератора реальної мовоподібної завади ОССА-1.

Для дослідження використовувався метод артикуляційних випробувань. Експеримент включає чотири стадії: підготовчу, інструментальну, розрахункову і аналітичну (рис. 1).

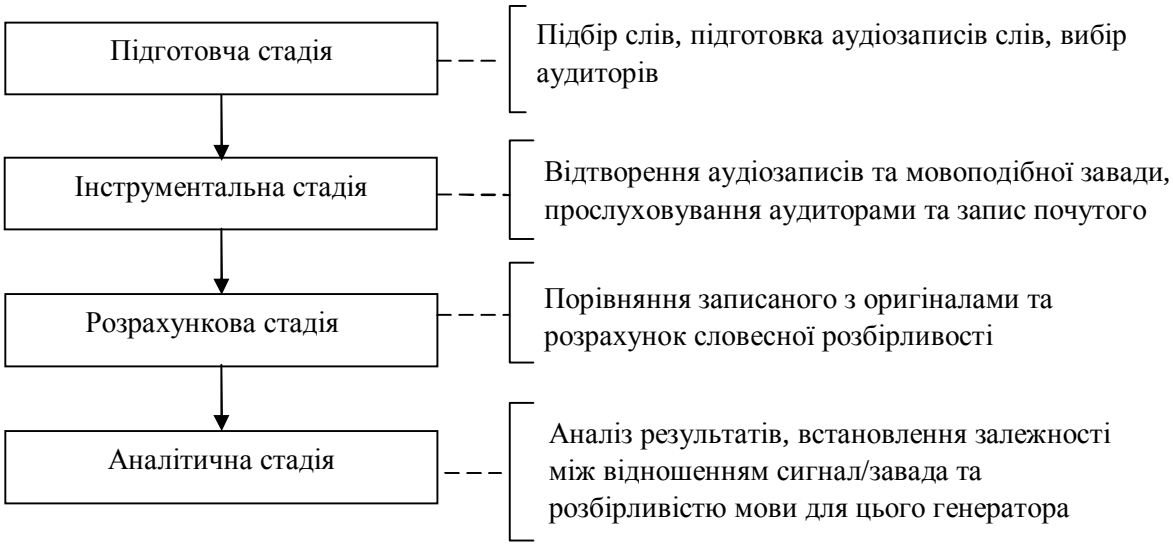

Рис. 1. Стадії експерименту

Для запису та прослуховування використано таблиці слів з чинного в Україні ГОСТ 16600-72. Слова зачитували почергово два диктори (чоловік і жінка) рівним голосом, з постійним рівнем мови, чітко без підкреслювання окремих звуків. Темп зачитування слів: 15…20 слів за хвилину з паузами між ними 2…3 секунди для їх запису аудиторами. Аудіозапис здійснювався на персональний комп'ютер стандартною програмою звукозапису Windows. Рівень запису усього текстового матеріалу однаковий. Для запису використано електродинамічний кардіоїдний мікрофон SHURE C606.

В інструментальній стадії брали участь п'ять аудиторів, що не мають дефектів слуху та пройшли попереднє тренування за методикою експерименту. Схему проведення інструментальної стадії показано на рис. 2.

Аудіозаписи таблиць слів відтворювались на комп'ютері за допомогою програми Windows Media. Сигнал подавався на акустичну систему та на генератор завади, де з нього формувалась мовоподібна завада, яка відтворювалась іншою акустичною системою. Були використані акустичні системи F&D H600.

Рівень корисного сигналу у місці прослуховування задавався таким, що дорівнював 70 дБ, що вимірювалось шумоміром ВШВ-003, і залишався незмінним упродовж всього експерименту. Рівень завади у місці прослуховування дискретно змінювався (85; 80; 75; 70; 65 дБ) для задання відношення сигнал/завада: -20; -15; -10; -5; 0, 5 дБ, що вимірювалось шумоміром за відсутності корисного сигналу. Перед прослуховуванням проводилась попередня адаптація аудиторів до шуму упродовж 5–10 хв. За кожного з відношень сигнал/завада аудитори прослуховували нову таблицю слів та записували почуте. Експеримент був повторений 3 рази з перервами між циклами.

Обробка результатів полягала у визначенні словесної розбірливості, як відношення розпізнаних слів до їх загальної кількості та статистичного усереднення результатів. Слова з помилками, які не змінювали їх змісту, за принципом найгіршого варіанта захищеності вважались розпізнаними.

Аналіз результатів зводився до побудови залежності усередненої словесної розбірливості від відношення сигнал/завада та порівняння отриманої характеристики з наведеними у [7] характеристиками для шумових завад (рис. 3).

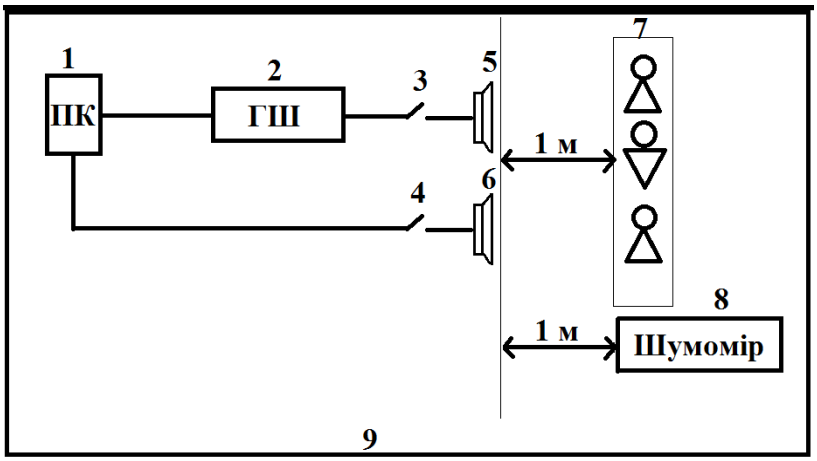

Рис. 2. Схема проведення інструментальної стадії:
1 – персональний комп'ютер;
2 – генератор мовоподібної завади ОССА-1; 3, 4 – ключі;
5, 6 – акустичні системи; 7 – аудитори;
8 – шумомір; 9 – зона експерименту

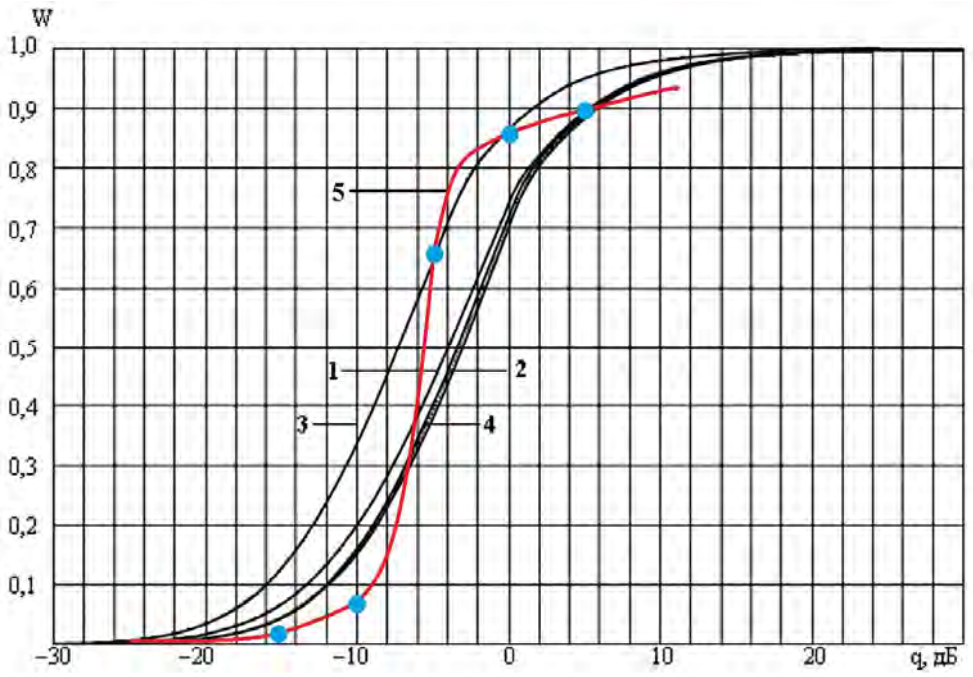

Рис. 3. Залежність словесної розбірливості W від інтегрального відношення сигнал/завада q:
1 – "білий шум"; 2 – "рожевий шум"; 3 – "коричневий шум"; 4 – мовоподібний шум;
5 – реальна мовоподібна завада, сформована генератором ОССА-1

З порівняння характеристик можна зробити висновок, що генератор ОССА-1 в діапазоні відношень сигнал/завада від -20 до -7 дБ є ефективніший, ніж генератори шумових завад, а потім його ефективність різко знижується. Це потребує певного удосконалення алгоритму формування завади. Але навіть в існуючому варіанті він є ефективніший за шумові генератори (забезпечує нижчу розбірливість мови) фактично для усіх ступенів захищеності (див. таблицю).

Висновки:

1. Впровадження для активного захисту мовної інформації нових, ефективніших генераторів завад потребує введення у практику нормування захищеності мовної інформації критерію словесної розбірливості мови, що зробить нормативні вимоги інваріантними до типу генератора і виду завади

та дасть змогу знизити рівні зашумлення у виділених приміщеннях за рахунок використання ефективних генераторів завад за незмінності нормативних вимог захищеності.

2. Характеристика залежності словесної розбірливості мови від відношення сигнал/шум повинна стати паспортною характеристикою генераторів завад, що дасть можливість порівнювати їх за ефективністю та легко визначати потрібний рівень завади для забезпечення нормативного значення словесної розбірливості.

3. Розроблений генератор реальної мовоподібної завади потребує удосконалення для підвищення ефективності в області відношень сигнал/шум $q > -8$ дБ.

1. Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації. НД ТЗІ Р-001-2000. – К.: ДССЗЗІ України, 2000. – 5 с. 2. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с. 3. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений: ГОСТ 16600-72. – М.: ИПК Издательство стандартов, 1973. – 90 с. 4. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости: ГОСТ Р 50840-95. – М.: Госстандарт Росии, 1997. 5. Ergonomics – Assessment of speech communication: ISO 9921:2003 [Электронный ресурс]. – Консорциум Кодекс: Электронный фонд правовой и нормативно-технической документации. – Режим доступу: http://docs.cntd.ru. 6. Акустическая экспертиза каналов речевой коммуникации: моногр. / В. С. Дидковский, М. В. Дидковская, А. Н. Продеус. – К.: Имэкс-ЛТД, 2008. – 420 с. 7. Хорев А. А. Методы защиты речевой информации и оценки их эффективности / А. А. Хорев, Ю. К. Макаров // Специальная техника. – 2001. – № 4. – С. 22–33. 8. Касьянов Ю. І. Визначення впливу шумової завади та звукоізоляції на розбірливість мови формантним методом / Ю. І. Касьянов // Комп'ютерні технології друкарства. – 2014. – № 31. – С. 85–93. 9. Хорев А. А. Способы и средства защиты речевой (акустической) информации от утечки по техническим каналам / А. А. Хорев // Специальная техника. – 2005. – № 5. – С. 54–59. № 6. – С. 54–62. 10. Нужний С. М. Нові напрямки в забезпеченні захищеності акустичної інформації / С. М. Нужний // Інформаційна безпека України: зб. наук. доп. та тез наук.-техн. конф. – К.: КНУ ім. Тараса Шевченка, 2015. – С. 66–67.