Нелинейность на измеряемой частоте в пределах динамического диапазона, дБ, не более	± 1 дБ в диапазоне 0,02-10кГц	± 1 дБ в диапазоне 0,7-400 кГц	± 1 дБ в диапазоне 0,1-30МГц
Наибольшая измеряемая напряженность поля ρН, дБ мкВ/м	163	151,5	145
Тип (класс, разряд) эталонов, использованных во время аттестации	УОМП-11, $\delta_o = \pm 4{,}5\%$	УОМП-11, $\delta_o = \pm 4{,}5\%$	–

Достигнутая неравномерность АЧХ для антенны АИМ 0,005 в диапазоне частот 5 Гц … 10 кГц не превышает ± 1,25 % (вне зоны режекции). Коэффициент калибровки антенны вне зоны режекции: **k = 28** дБ м$^{-1}$ при Rвх=1 МОм и **k = 51** дБ м$^{-1}$ при Rвх=50 Ом.

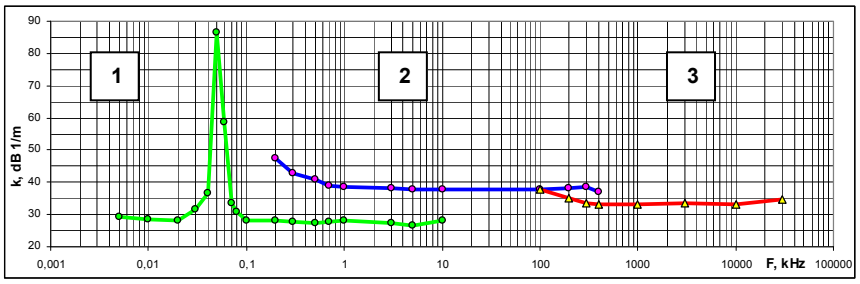

Рисунок 5 – Зависимость коэффициента калибровки точечных антенн АИМ 0,005 (с включенным режекторным фильтром 50 Гц); АИМ НЧ 200 и АИМ ВЧ 0,1-30 в частотном диапазоне 5 Гц … 30 МГц

Литература: ***1.*** *Яремчук А. А. Исследования влияния неионизирующего электромагнитного излучения. Сборник «Мониторинг и прогнозирование генетического риска в Украине». 1998, Киев, изд. Реформа, стр. 249 – 273.* ***2.*** *В. Галанский, А. Лаврентьев, М. Прокофьев. Мониторинг низкочастотного магнитного поля. Сборник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", №2, 2001, с. 91-95.* ***3.*** *В. Галанский, А. Лаврентьев, М. Прокофьев. Измеритель низкочастотных магнитных полей. Сборник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", №4, 2002, с. 161-166.* ***4.*** *В. Галанский, М. Прокофьев. Низкочастотные магнитные поля: проблемы, влияние, мониторинг. Сборник докладов восьмой российской научно-технической конференции по электромагнитной совместимости и электромагнитной безопасности. Санкт-Петербург, 2004, с. 543-547.* ***5.*** *Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, ДСанПІН 3.3.2.007-98.* ***6.*** *М. Прокофьев. Портативный дозиметр низкочастотных магнитных полей. Сборник докладов девятой российской научно-технической конференции по электромагнитной совместимости и электромагнитной безопасности. Санкт-Петербург, 2006, с. 662-664.*

УДК 621.055.5

АНАЛИЗ ИНФОРМАЦИОННЫХ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК СИГНАЛОВ МАСКИРОВАНИЯ РЕЧИ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Владимир Журавлев
НТУУ "КПИ"

Анотація: **Проаналізовано інформаційні параметри і характеристики сигналів маскування мови. Визначена науково-технічна проблема, як протиріччя між методами ідентифікації інформаційних параметрів і характеристик сигналу маскування та мовного сигналу у точці несанкціонованого доступу технічної розвідки супротивника.**

Summary: **The analyses of masking speech signals information parameters and characteristics the identification methods of masking speech signals information parameters and characteristics in the point of**

illegal access of enemy technical reconnaissance is determined.
Ключевые слова: **Защита информации, речевой сигнал, сигнал маскирования речи.**

I Введение. Постановка задачи

В соответствии с законом Украины об информации [1] целью информационной защиты являются предотвращение утечки, хищения, утраты, искажения и подделки (имитации) информации. Головным критерием обеспечения разведзащищенности при анализе системных методов исследования информационных параметров и характеристик качества маскирования речевого сигнала (РС) на объектах информационной деятельности (ОИД) будем считать семантическую адекватность сигнала в точке несанкционированного доступа (НСД) технической разведки противника (ТРП). Под термином семантической адекватности будем понимать значение логического параметра $SeA(t)$ информационной разведзащищенности, который определяет соответствие артикулируемых диктором и получаемых ТРП смысловых образов. Семантическая адекватность как структурний параметр будет характеризоваться изменением энтропии ТРП $Hti(t)$ относительно энтропии диктора $Hi(t)$ на интервале времени Tc акустической передачи информационного образа (слова).

$$SeA(t) = \frac{\Delta Hti(\Delta t)}{\Delta Hi(\Delta t)}, \Delta t \in (0, Tc). \quad (1)$$

Формулировка задачи. Провести анализ методов идентификации информационных параметров и характеристик сигналов маскирования речевых сигналов на ОИД по критерию семантической адекватности.

II Основная часть

Язык представляет собой [2] многокомпонентную систему, которая, с одной стороны, обеспечивает процессы порождения информации, а с другой стороны, процессы восприятия и понимания этой информации. Деятельность диктора предполагает воплощение в РС, адресованных аудитору, своих знаний с изменением параметра $\Delta Hi(\Delta t)$. Деятельность ТРП заключается в извлечении из речевого сигнала диктора передаваемой информации и уменьшения своей энтропии $\Delta Hti(\Delta t)$. Таким образом, под основным параметром информационной эффективности $\Gamma(t)$ систем сокрытия РС на ОИД будем понимать обеспечение постоянства первой производной параметра семантической адекватности (1).

$$\Gamma(t) = \frac{dStA(t)}{dt} = const \quad (2)$$

В случае, если значение выражения (2) будет больше нуля, происходит утечка информации РС, если меньше нуля, то в речевой канал НСД поступает дезинформация.

Проведем анализ существующих в настоящее время информационных параметров и характеристик РС $Si(t)$ и маскирующего сигнала $Sn(t)$ в части возможности оценки изменения параметра (2) в точке НСД на границе зоны безопасности.

Обзор и анализ основных параметров и характеристик речевых сигналов.

Речь как процесс генерации РС по общему мнению [3] является квазишумовым квазистационарным сигналом с неустойчивыми параметрами и характеристиками составляющих ее элементов. В разных словах одни и те же звуки могут произноситься по-разному, а частотные характеристики речеобразующего тракта изменяются в зависимости от возраста и психологического состояния человека. В общем случае РС можно анализировать как шумоподобный акустический сигнал [4], имеющий информационную амплитудную (параметр A_i), частотную (параметр ω_i) и фазовую (параметр φ_i) модуляцию несущих *n* элементарных гармонических сигналов:

$$Si(t) = \sum_{i=1}^{n} A_i \cos[\omega_i t + \varphi_i(t)]. \quad (3)$$

Источниками генерации информационных акустических элементарных гармонических сигналов $Si(t)$ в речеобразующем тракте являются:

– периодическая модуляция воздушного потока, исходящего из лёгких, посредством колеблющихся диафрагмы и голосовых связок (голосовой источник сигналов основного тона (ОТ));

– турбулентные завихрения воздушного потока в сужениях речеобразующего тракта (шумовой источник);

– скачкообразное изменение давления воздуха в речеобразующем тракте при резком коротком прерывании истечения воздуха (импульсный источник).

Считается [5], что элементарные гармонические сигналы артикулируются (модулируются) по амплитуде и фазе в акустическом фильтре, который образуют активные и пассивные артикуляционные органы и система акустических резонаторов. В результате его работы отдельные составляющие РС усиливаются или ослабляются.

Под термином *форманта* (Φ_n, n – номер форманты) понимается [6] гармонические компоненты сигналов основного тона (ОТ), выделенные и усиленные в акустическом фильтре речеобразующего тракта.

Основные дифференциальные параметры и характеристики РС на уровне формант.

Перечисленные ниже параметры и характеристики в основном определяются статистической обработкой [7] квазистационарного участка РС, который определяется как слоговый інтервал $Tc \approx$ (10 – 20 СМ.

Это, прежде всего, спектральная плотность мощности (СПМ), статистические характеристики Φ_n и сигнала ОТ.

Частотное распределение формант Φ_n следующее:

– форманты звонких звуков занимают полосы частот (150 – 900) Гц (Φ_1), (550 – 2800) Гц (Φ_2) и (1500 – 3400) Гц (Φ_3);

– форманты глухих звуков занимают полосы частот (1000 – 3500) Гц (Φ_1), (2500 – 6000) Гц (Φ_2) и (1500 – 4000) Гц (Φ_3);

– с вероятностью 0,98 частотный диапазон Φ_1 равен (200 – 850) Гц, Φ_2 равен (850 – 2550) Гц и Φ_3 равен (2100 – 3300) Гц.

Девиация медианной частоты формант характеризуется коэффициентом взаимной корреляции, равным 0,78 для Φ_1 и Φ_2, 0,82 для Φ_2 и Φ_3, и 0,95 для Φ_3 и Φ_4. Средне значение девиации частоты огибающей для формант Φ_1 и Φ_2 порядка 8 Гц [4].

Амплитуда сигнала ОТ определяет громкость РС. Частота колебаний голосовых связок, характеризующая сигнал ОТ, составляет от 70 до 180 Гц (средняя частота 129 Гц) для мужских голосов и от 180 до 330 Гц (средняя частота 240 Гц) для женских. Процесс модуляции сигналов ОТ акустическим фильтром речеобразующего тракта определяют как вокализацию элементов РС. У одного и того же диктора в зависимости от эмоционального состояния и ситуативности речи частота сигнала ОТ может изменяться.

Информационные параметры и характеристики изменения индекса фазовой модуляции (по параметру $\varphi_i(t)$ выражения (3)) статистически не определены [4].

Основные интегральные параметры РС.

Основная энергия акустических колебаний РС заключена в диапазоне (70 – 7000) Гц, причем более 95% семантической информации размещается в более узком частотном диапазоне (200 – 5000) Гц. Акустические колебания выше и ниже этого диапазона частот несут идентификационную информацию об эмоциях и личности диктора (устный почерк), которая способствует узнаваемости, и несколько повышают разборчивость РС в условиях интенсивных природных маскирующих сигналов. Динамические характеристики разговорной речи различны и во многом зависят от внешних условий, в которых находится диктор. Так, спокойный, доверительный разговор, ведущийся собеседниками, находящимися рядом друг с другом, происходит обычно с уровнем порядка 55 дБ SL (звуковое давление); выступление в зале, а нередко и разговор по телефону – около 75 дБ SL. При этом динамический диапазон РС также меняется в довольно широких пределах 25 – 45 дБ.

Распределение амплитудного состава РС показывает [6], что более 80% звуков речи имеют уровень меньше 45 дБ, и, считается, легко могут быть сокрыты сигналом маскирования (СМ). Вокализованные элементы РС имеют основную несущую частоту в пределах (80 – 2500) Гц и длительность $Tc =$ (30 – 300) СМ, в них сосредоточена основная энергия речевого сигнала.

В соответствии с методом научной абстракции для анализируемого предмета исследований информационную составляющую сигнала $Si(t)$ можно представить как сумму вокализованных частотных компонент, с определенными границами изменения параметров сигнала ОТ и сигналов первых трех формант. Представляя сигнал ОТ как нулевую форманту (Φ_0) абстрагируем выражение (3) для

информационных (в части семантической адекватности (1)) компонент сигнала $Si(t)$ в канале утечки ОИД:

$$Si(t) = \sum_{i=0}^{3} A_{\Phi i} \cos[\omega_{\Phi i} t + \varphi_{\Phi i}(t)]. \quad (4)$$

Параметр адекватности принятого ТРП информационного сигнала $Sti(t)$ оценивается разборчивостью, которая представляет собой статистическую характеристику РС $Si(t)$ принимаемой на фоне СМ $Sn(t)$. Под термином *разборчивость* понимают [8] отношение числа правильно принятых ТРП элементов РС (слогов, слов, фраз из словаря объемом Vw) к общему числу элементов, переданных диктором. В качестве показателя оценки разведзащищенности наиболее часто используют словесную разборчивость W, которая определяет семантическую адекватность (1) информации и достаточно объективно оценивает информационную эффективность (2) сокрытия РС.

До настоящего времени *не определено:*

- какие компоненты сигнала (4) определяют семантическую составляющую РС;
- аналитического выражения семантической составляющей (1) РС,

что не позволяет аналитически оценить разведзащищенность РС участников информационного общения ОИД и, по нашему мнению, является одной из составляющих актуальной научно-технической проблемы, исследование которой позволит *повысить эффективность разведзащищенности* систем защиты ОИД.

Обзор и анализ основных параметров и характеристик маскирующих сигналов.

В соответствии с нормативным документом ДСТЗИ [9] сигнал маскирования $Sn(t)$ определяется как стационарный "белый" либо "розовый шум" с нулевым средним значением и диапазоном рабочих частот не менее (180 – 5600) Гц. Под термином "розовый шум" понимается шумовой сигнал, у которого уровень СПМ падает с увеличением частоты с постоянной крутизной 6 дБ/октаву.

В связи с тем, что под термином "шум" понимаются [10] "беспорядочные звуковые колебания разной физической природы, характеризующиеся случайным изменением амплитуды, частоты и др. параметров," под термином "сигнал маскирования" будем понимать синтезированный средствами ТЗИ сигнал $Sn(t)$, предназначенный для сокрытия информационной составляющей РС и аддитивно воздействующий на сигнал $Si(t)$ в канале утечки:

$$Sni(t) = Si(t) + Sn(t), \quad (5)$$

где $Sni(t)$ суммарный сигнал в точке НСД ТРП.

Таким образом, сигнал $Sn(t)$ можно рассматривать как стационарный случайный процесс, у которого функция распределения или функция плотности вероятности инвариантна относительно операции сдвига во времени. Математические модели случайных процессов широко используются для описания различных сигналов. Наиболее известной моделью случайного процесса является гауссовский случайный процесс [11], который полностью определяется своим средним значением $\overline{m}$ и функцией автокорреляции $\hat{R}_{ss}$. Исходя из определения сигнала "розового шума", маскирующий сигнал $Sn(t)$ можно представить, как и РС, в виде конечной суммы n гармонических составляющих $Sn_i(t) = A_i \cos[\omega_i t + \varphi_i(t)]$ с собственными амплитудами A_i, частотами ω_i и фазами φ_i, которые случайно изменяются во времени, однако при этом удовлетворяются условия стационарности процесса, а также постоянства амплитудного и частотного диапазонов и корреляционных функций.

На рис. 1 приведены характеристики зависимости спектральной плотности мощности сигналов маскирования от частоты [12] применяемых в настоящее время устройств ТЗИ.

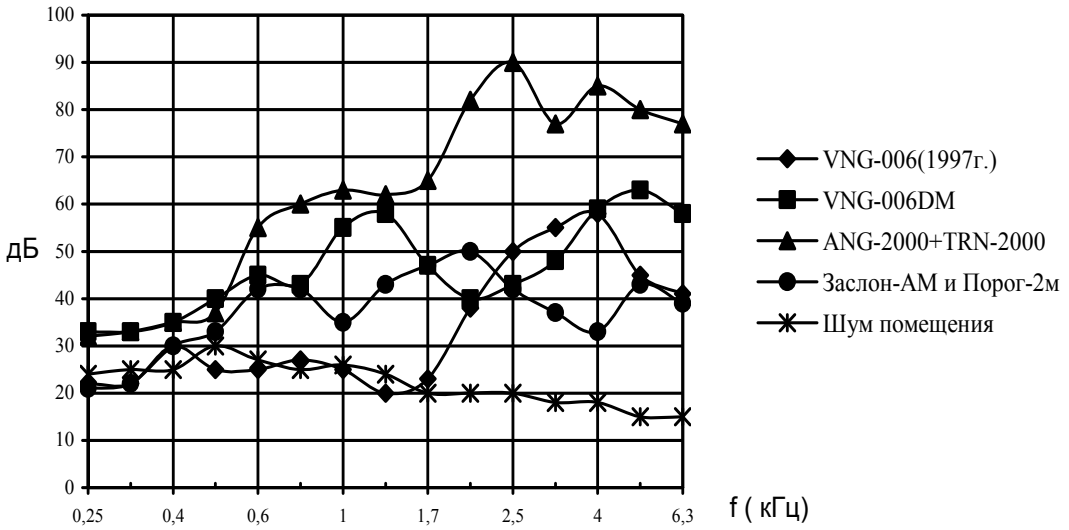

Рисунок 1 – Зависимость спектральной плотности мощности от частоты маскирующих сигналов устройств ТЗИ [12]

Анализ приведенных характеристик спектров СМ показывает, что ни одно техническое средство не обеспечивает требований к параметрам "белого" либо "розового" шума, изложенных в стандарте ДСТЗИ. Однако, декорреляционные свойства применяемых в настоящее время сигналов маскирования по отношению к РС обеспечивают, судя по наличию у них лицензии Гостехкомиссии России, необходимые параметры разведзащищенности и категорирования ОИД.

Анализ основных интегральных параметров СМ.

Судя по результатам артикуляционных исследований [13, 14], наиболее перспективным, с позиции оценки параметра информационной защищенности, оказалось применение в системах ТЗИ речеподобных сигналов (РПС) маскирования, синтез которых возможен тремя методами суммирования:

– из случайных фрагментов речи трех (или более) дикторов радиовещательных станций при примерно равных интегральных уровнях смешиваемых сигналов;

– из одного доминирующего речевого сигнала или музыкального фрагмента и смеси случайных фрагментов радиопередач с шумом;

– из случайных фрагментов скрываемого речевого сигнала при многократном их наложении с различными уровнями (т. н. "фонемный клон" [14]).

Анализ опубликованных результатов исследований [13] показал, что наименьшей семантической адекватностью (1) из всех вышеприведенных сигналов обладает адаптивный сигнал маскирования, синтезированный по третьему методу. Зависимость коэффициента словесной разборчивости речи W, взятого авторами в качестве параметра эффективности сигнала, от общепринятого параметра отношения "сигнал/помеха" S/N для третьего метода синтеза свидетельствует о возможности значительного (на 6 – 10 дБ), по отношению к другим сигналам маскирования, снижения требуемого уровня сигнала в точке НСД ТРП для достижения нормы информационной разведзащищенности. Предложен способ [14] формирования РПС, коррелированного по уровню, спектру и времени излучения с РС, заключающийся в специальном преобразовании РС за счет сложной инверсии спектра, акустической псевдореверберации путем умножения и деления его частотных составляющих, а также многократного суммирования принимаемых отраженных реверберационных акустических сигналов. Аналитических исследований и математической модели предложенного сигнала маскирования нами не обнаружено, что позволяет предположить об эмпирическом характере полученного положительного результата минимальной семантической адекватности. Исходя из потенциальной возможности применения ТРП метода многолучевого приема, вероятным становится факт извлечения из аддитивного сигнала $Sni(t)$ в точке НСД огибающей амплитудного спектра ОТ (т. н. "мелодики ОТ") РС, являющейся его информационной характеристикой, что отрицательно влияет на параметр семантической адекватности.

Аналитического выражения адаптивного РПС маскирования нами не обнаружены.

Известны [15] активные параметрические системы защиты, построенные на основе применения метода синтеза маскирующего сигнал $Sh(t)$, комплексно противофазного к информационному сигналу $Si(t)$ в

точке подключения средств ТРП. В результате достигается взаимная компенсация информационного $Si(t)$ и маскирующего $Sh(t)$ сигналов. Однако предложенный метод компенсации и его модификации подразумевают удовлетворение некоторым, в том числе и взаимоисключающим, требованиям:

- непрерывного заполнения точки подключения приемника ТРП и компенсирующей поверхностей соответствующими приемниками и излучателями;
- волновой "прозрачности" приемной точки и компенсирующей поверхности;
- бесконечного числа каналов связи приемник-компенсатор;
- измерения динамических параметров акустического поля, в том числе его нормальной производной в одной и той же точке пространства;
- известности и неизменности функций Грина, описывающих информационное акустическое поле.

Несмотря на привлекательность этого метода, его практическая реализация при современном уровне развития технических средств и методов обработки сигналов затруднена. При синтезе данного СМ необходимо учитывать комплексную волновую обратную связь при стохастическом изменении акустических параметров выделенного помещения, решать вопрос об оптимальной дискретизации приемной и компенсирующей поверхностей, а также удовлетворять высоким требованиям к точности настройки, быстродействию, показателям качества регулирования и устойчивости алгоритма управления системой защиты.

На основании проведенного анализа можно сделать вывод, что основными параметрами сигнала маскирования $Sn(t)$, влияющими на параметр информационной эффективности $\Gamma(t)$, являются:

- частотный диапазон, определяемый, со стороны верхней частоты ω_h, интервалом корреляции АКФ сигнала $Sn(t)$;
- неравномерность характеристики спектральной плотности мощности в октавных частотных полосах сигнала, которая определяет степень его адекватности сигналу со спектром "белого шума";
- мощность в точке подключения средств ТРП (энергетической разведзащищенностью), которая зависит от метода его синтеза: не адаптивного и адаптивного по отношению к маскируемому речевому сигналу.

Необходимо отметить, что аналитического выражения маскирующего речеподобного сигнала в открытых источниках информации нами не обнаружено, но эмпирически доказано [14], что в случае положительного коэффициента корреляции семантическая адекватность маскированного сигнала ухудшается.

На основании промежуточных выводов проведем анализ параметров РС $Si(t)$ и СМ $Sh(t)$, определяющих информационную разведзащищенность сигнала $Sti(t)$ (табл. 1).

Таблица 1 – Основные параметры информационного $Si(t)$ и маскирующего сигналов $Sn(t)$.

Параметры сигнала $Si(t)$	Параметры сигнала $Sn(t)$
1. Семантическая адекватность $SeA(t)$, эквивалентная разборчивости слов W.	1. Метод синтеза, который аналитически определен только для сигнала "белый" шум.
2. Амплитуды A_i, частоты ω_i и индексы модуляции вокализованных формантных составляющих слов.	2. Верхняя граница частотного диапазона ω_h, определяемая интервалом корреляции АКФ сигнала СМ.
3. Активная длительность вокализованных формант Tc на интервале длительности слова.	3. Неравномерность (дБ) характеристики СПМ в октавных частотных полосах сигнала.
4. Информационная разведзащищенность и динамический диапазон D по отношению к сигналу $Sn(t)$ в точке НСД ТРП.	4. Энергетическая разведзащищенность и динамический диапазон D по отношению к сигналу $Si(t)$ в точке НСД ТРП.

Анализируя параметры и характеристики, приведенные в табл.1, можно сделать вывод, что сигналы $Si(t)$ и $Sn(t)$ ***в настоящее время характеризуются различными параметрами*****,** за исключением

параметра динамического диапазона D и эффективной полосы частот ω_h, определяемой для СМ как верхняя граница частотного диапазона.

III Выводы

В результате анализа методов исследования информационных параметров и характеристик сигналов маскирования речи на ОИД можно констатировать факт ***противоречия между методами идентификации информационных параметров и характеристик при синтезе сигнала аддитивного маскирования*** $Sn(t)$ ***и информационными параметрами и характеристиками при анализе речевого сигнала*** $Si(t)$ ***в точке НСД ТРП,*** влияющего на процесс исследования и анализа разведзащищенности информационной составляющей РС.

Литература: ***1.*** *ДСТУ 3396.2-97. Державний стандарт України. Захист інформації, Технічний захист інформації. Терміни та визначення. Київ. - 1998. – с. 12.* ***2****. Психоакустические аспекты восприятия речи. Механизмы деятельности мозга / Под. ред. Н. П. Бехтеревой. — М. Наука. 1988. –с. 504.* ***3****. Фланаган Дж. Анализ, синтез и восприятие речи: Пер. с англ./ Под ред. А. А. Пирогова. – М. Связь. 1968. – с. 396.* ***4****. Вокодерная телефония. Методы и проблемы. Под ред. А. А. Пирогова – М. Связь. 1974. – с. 536.* ***5****. Назаров М. В., Прохоров Ю. Н. Методы цифровой обработки и передачи речевых сигналов. – М. Радио и связь. 1985. – с. 176.* ***6.*** *Михайлов В. Г., Златоустова Л. В. Измерение параметров речи /Под ред. М. А. Сапожкова. – М. Радио и связь. 1987. – с. 168. 7. Вемян Г. В. Передача речи по цепям электросвязи. – М. Радио и связь. - 1985. – с. 272.* ***8.*** *ГОСТ Р 50840-95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. Издание официальное. – М. Госстандарт России, 1997.* ***9****. НД ТЗІ – Р – 001 – 2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. НД ТЗІ – Р – 001 – 2000. ДСТСЗІ СБ України. – Київ. - 2000. – с. 9.* ***10****. Советский энциклопедический словарь. /Гл. ред. А. М. Прохоров. 4 – изд. – М. Сов. энциклопедия, 1989. – с. 1632.* ***11.*** *Брандт З. Статистические методы анализа наблюдений. – М. Мир. 1975. – с. 312.* ***12****. Калинин С. В. Исследование систем виброакустического зашумления. www.mascom.ru. - 2003.* ***13****. Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации//Специальная техника. – М. 2000.– № 4. С. 28 - 33.* ***14.*** *Иванов В. М., Хорев А. А. Способ и устройство формирования "речеподобных" шумовых помех// Вопросы защиты информации. – М. 1999. – № 4. С. 37 - 44.* ***15****. Shakhnov V. A., Vlasov A. I. Das Realisirungkonzept der aktiven Unterdruckung der Akustiklarme der Electronengerate.//Proceeding of 15th International Congress on Acoustics. Trondheim, Norway, 26 - 30 June 1995.*

УДК 004.31, 004.056.55, 003.26

ОЦІНКА РІВНЯ БЕЗПЕКИ ОПЕРАЦІЙ, ВИКОНУВАНИХ ЗАСОБАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Микола Карпінський, Леся Коркішко*, Тимур Коркішко**

*Університет в Бєльську-Бяла, Польща, *Тернопільський національний економічний університет, **Інститут передових технологій Самсунг Електронікс, Південна Корея*

Анотація: **Розвинуто методику оцінки рівня безпеки виконуваних засобами захисту інформації базових операцій алгоритмів криптографічних перетворень над даними у маскованому представленні.**

Summary: **A methodology for estimation of security level of basic operations execution on masked data for cryptographic transformations algorithms by information protection means was further developed.**

Ключові слова: **Масковане представлення даних, витік інформації, аналіз споживаної потужності, рівень безпеки виконання операцій, елементи пристроїв захисту інформації.**

Вступ

Для успішних практичних реалізацій алгоритмів криптографічних перетворень необхідно розв’язувати цілий комплекс задач, серед яких традиційне місце займають задачі досягнення мінімальної споживаної потужності, забезпечення малогабаритних вимог, продуктивності обчислень. Разом з тим, широке