ISSN 0002-3566 (print)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

INFORMATION TECHNOLOGIES AND SYSTEMS

УДК 621.372.037.372

Поступила в редакцию 30.08.2016
Received 30.08.2016

В. К. Железняк, И. Б. Бураченок, Д. С. Рябенко

Полоцкий государственный университет, Новополоцк, Беларусь

КРИТЕРИИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОТ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ

Обоснован метод оценки нормативного показателя защищенности речевого сигнала по критерию разборчивости речи в полосах равной разборчивости речи в шумах высокого уровня сложным измерительным сигналом с большой базой. Показано преимущество сложного измерительного сигнала с большой базой перед гармоническим измерительным сигналом при оценке защищенности каналов утечки речевой информации.

Наряду с аналоговой формой речевого сигнала широко используются речевые сигналы в цифровой форме. Для речевых сигналов в цифровой форме необходимо установить математическую зависимость между вероятностью ошибочного приема бита и величиной разборчивости речи. Для сложных сигналов с большой базой по аналогии с речевыми сигналами в цифровой форме необходимо установить математическую зависимость с гармоническим измерительным сигналом. Целью работы является определение нормативного показателя защищенности речевых сигналов в каналах утечки информации на основании установленных математических зависимостей. Данные математические зависимости позволят реализовать автоматизированную измерительную систему для комплексной оценки защищенности конфиденциальной информации, обрабатываемой в аналоговой и цифровой форме, в технических каналах ее утечки.

Ключевые слова: речевой сигнал, разборчивость речи, измерительный сигнал, технический канал утечки информации, нормированный показатель, аналоговая и цифровая форма сигнала.

V.K. Zheleznyak, I.B. Burachenok, D.S. Rabenka

Polotsk State University, Novopolotsk, Belarus

ASSESSMENT CRITERIA OF VOICE SIGNAL LEAKAGE PROTECTION

A method of assessing of normative protection indicator of speech signal by the criterion of speech intelligibility at high noise level in the band of speech signal, equal to intelligibility, by means of complex measuring signal with a large base, is substaniated. The advantage of the complex measuring signal with a large base over harmonic measuring signal when assessing protection of speech data leakage channels is shown.

Voice signals in digital form along with voice signals in analog form are widely used. It is necessary to find mathematical relation between bit-error probability and speech intelligibility for voice signals in digital form. It is also necessary to establish mathematical relation between compound signal with large base and harmonic measuring signal. The main purpose of the study is to establish a normative characteristic of leakage protection of voice signals on the base of determined mathematical relations. The given mathematical relations will allow realizing the automated measuring system for estimation of security of the confidential information transformed into the analog and digital form, in channels of its leak.

Keywords: voice signal, speech intelligibility, measuring signal, technical information leakage channel, normalized index, analog and digital waveform.

Введение. Стандарт СТБ 34.101.29-2011 устанавливает требования к измерительным сигналам для оценки защищенности речевых сигналов (РС) по техническим каналам утечки (ТКУ). С целью установления степени защищенности в ТКУ РС широко применяется гармонический измерительный сигнал (ГИС), обоснованный корреляционной теорией разборчивости речи и обладающий рядом преимуществ по сравнению с другими сигналами [1].

Основная часть. С целью обоснования сложного измерительного сигнала с большой базой (СИС ББ) [2] установим математическую зависимость между нормированным показателем защищенности ГИС и показателем, устанавливающим защищенность СИС ББ. Для оценки используем k СИС ББ в k-полосах равной разборчивости. Исходными данными измерительных сигналов являются постоянные значения длительности $T_{\text{с}}$ и девиации частоты $\pm\Delta f_k$, перекрывающей каждую из k-полос равной разборчивости [3] ($k = \overline{1, n}$, где k – порядковый номер полосы равной разборчивости, n – количество полос равной разборчивости).

Энергетический спектр W СИС ББ представляют выражением [4]:

$$W = \frac{\pi U_0^2}{2\mu} = \frac{\pi U_0^2 T_{\text{с}}}{2\pi\Delta f} = \frac{U_0^2 T_{\text{с}}^2}{2\Delta f T_{\text{с}}} = \frac{U_0^2 T_{\text{с}}^2}{B}, \tag{1}$$

где U_0 – амплитуда сигнала, $\mu = \Delta\omega / T_{\text{с}}$ – скорость нарастания частоты СИС ББ, а B – база сигнала $B = 2\Delta f T_{\text{с}}$.

Так как из [5] для любого детерминированного сигнала отношение сигнал/шум (ОСШ) в диапазоне $0 \le t \le T_{\text{с}}$ определяют как $q^2 = \frac{2E}{N_0}$, где N_0 – спектральная плотность мощности шума [5], а E – энергия сигнала, то ОСШ для СИС ББ можно представить:

$$q^2_{\text{вых\_сл}} = \frac{2U_0^2 T_{\text{с}}^2}{BN_0} 2\Delta f = \frac{2U_0^2 T_{\text{с}}^2 2\Delta f}{T_{\text{с}} 2\Delta f N_0} = \frac{2U_0^2 B}{2\Delta f N_0} = \frac{P_{\text{с}}}{P_{\text{ш}}} 2B, \tag{2}$$

где $P_{\text{ш}} = N_0 2\Delta f$ – мощность шума в заданной полосе равной разборчивости $2\Delta f$, а $P_{\text{с}} = U_0^2$ – мощность сигнала.

Таким образом, ОСШ на выходе приемника $q^2_{\text{вых\_сл}}$ связано с ОСШ на входе приемника $\rho^2_{\text{вх\_сл}} = \frac{P_{\text{с}}}{P_{\text{ш}}}$:

$$q^2_{\text{вых\_сл}} = 2B\rho^2_{\text{вх\_сл}}. \tag{3}$$

ОСШ на выходе $q^2_{\text{вых\_сл}}$ определяет рабочие характеристики приема СИС ББ, а ОСШ на входе $\rho^2_{\text{вх\_сл}}$ – энергетику сигнала и шума. Величина $q^2_{\text{вых\_сл}}$ может быть получена, даже если $\rho^2_{\text{вх\_сл}} \ll 1$. Для этого достаточно выбрать СИС ББ B, удовлетворяющей (3) [2]. Как видно из (2), прием СИС ББ сопровождается усилением сигнала (или подавлением помехи) на выходе. Таким образом, чем больше база сложного сигнала, тем меньше ОСШ на входе приемника можно допустить при заданной надежности обнаружения.

Для нашего случая, когда каждая полоса имеет постоянное значение девиации частоты $\pm\Delta f_k$, при увеличении длительности $T_{\text{с}}$ исходного сигнала можно увеличивать значение размера базы и тем самым улучшать ОСШ на выходе приемника. Исходя из того, что в широкополосных системах связи прием информации характеризуется отношением ОСШ $h_0^2 = \frac{q^2}{2}$ [2], то есть $h_0^2 = B\rho^2_{\text{вх\_сл}}$, то зависимость полученного ОСШ СИС ББ на выходе приемника от ОСШ на входе приемника можно представить, как показано на рис. 1.

Однако увеличение длительности СИС ББ приводит к увеличению времени оценки защищенности ТКУ РС, что в нашем случае является критичным.

Так как ГИС относится к классу простых сигналов, у которых величина базы всегда равна единице $B = 1$ [2], то для такого сигнала на выходе ОСШ можно представить

$$q^2_{\text{гар}} = \frac{2E}{N_0} = \frac{P_{\text{с}} T_{\text{с}}}{N_0} \frac{2\Delta f}{2\Delta f} = \frac{P_{\text{с}}}{N_0} \frac{B}{2\Delta f} = \frac{P_{\text{с}}}{N_0}$$

или

$$q^2_{\text{вых\_гар}} = \frac{2E}{N_0} = \frac{P_{\text{с}}}{P_{\text{ш}}}, \tag{4}$$

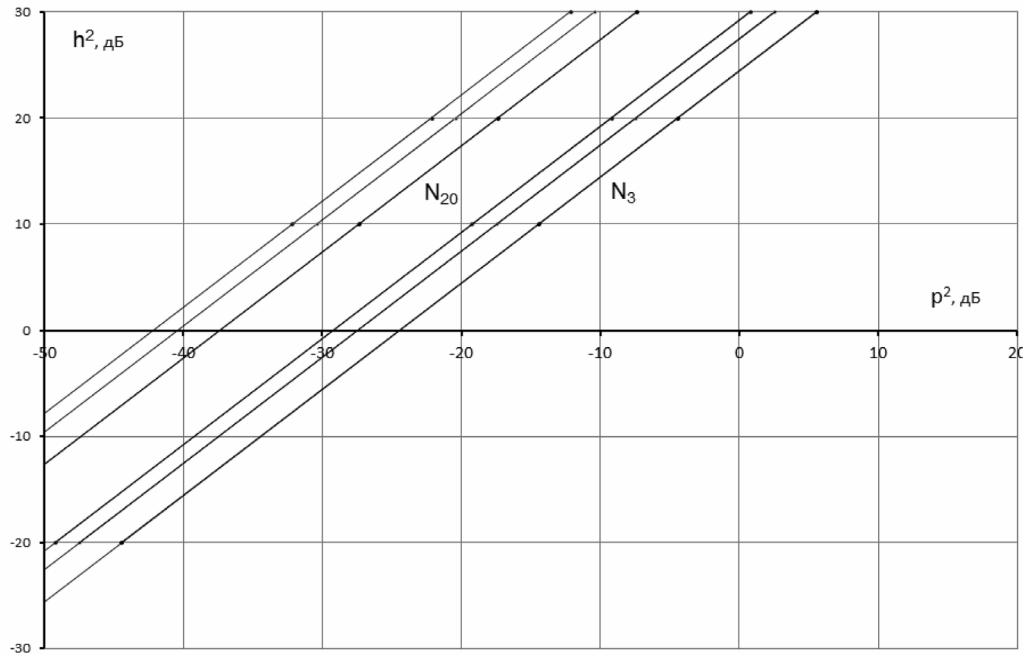

Рис. 1. Зависимость ОСШ СИС ББ на выходе приемника от ОСШ на входе приемника при T_c = 2, 4, 6 с в N_3 и N_{20} полосах равной разборчивости

Fig. 1. Dependence of the signal-to-noise ratio of complex measuring signal with a large base at the exit of the receiver from the signal-to-noise ratio on a receiver input at T_c = 2, 4, 6 second in N_3 and N_{20} in the band of equal to intelligibility

Нормативный показатель, устанавливающий математическую зависимость между нормированным показателем защищенности ГИС и показателем защищенности СИС ББ, определяют как ОСШ на выходе, оцененное при помощи СИС ББ $q^2_{\text{вых\_сл}}$ к нормативному показателю $q^2_{\text{вых\_гар}}$ защищенности РС в виде численного значения ОСШ ГИС:

$$\delta_{\text{сл}} = \frac{q^2_{\text{вых\_сл}}}{q^2_{\text{вых\_гар}}}. \tag{5}$$

Если нормативный показатель защищенности РС ГИС определяется как $q^2_{\text{вых\_гар}} = \left(\frac{P_c}{P_ш}\right)_{\text{норм}}$, то при равенстве ОСШ выходных ГИС и СИС ББ $(P_c / P_ш)_{\text{сл}} = (P_c / P_ш)_{\text{норм}}$ имеем:

$$\delta = \frac{q^2_{\text{вых\_сл}}}{(P_c / P_ш)_{\text{норм}}} = \frac{B(P_c / P_ш)_{\text{сл}}}{(P_c / P_ш)_{\text{норм}}} = B. \tag{6}$$

С помощью математической модели (6), фиксирующей однозначную связь метода оценки разборчивости речи СИС ББ с методом ГИС оценки разборчивости речи, установлено преимущество первого метода перед вторым, определяемое величиной базы первого сигнала, которое равно произведению времени существования сигнала на удвоенную девиацию частоты в пределах полосы равной разборчивости. Из (6) следует, что увеличение (выигрыш) ОСШ на выходе ТКУ при использовании СИС ББ по сравнению с ОСШ на его выходе при использовании ГИС зависит от размера базы сложного сигнала. На рис. 2 приведен график нормированных значений коэффициента разборчивости речи K_p на выходе ТКУ для ГИС и СИС ББ.

Из графика следует, что чем больше база СИС ББ, тем выше возможность обнаружения этого сигнала на фоне помех относительно ГИС. Таким образом, преимуществом СИС ББ является то, что с помощью такого сигнала можно получить большие значения ОСШ на выходе ТКУ РС.

При несомненном преимуществе качества РС в цифровой форме его защита от утечки по ТКУ сдерживается отсутствием единого критерия защищенности аналоговой и цифровой рече-

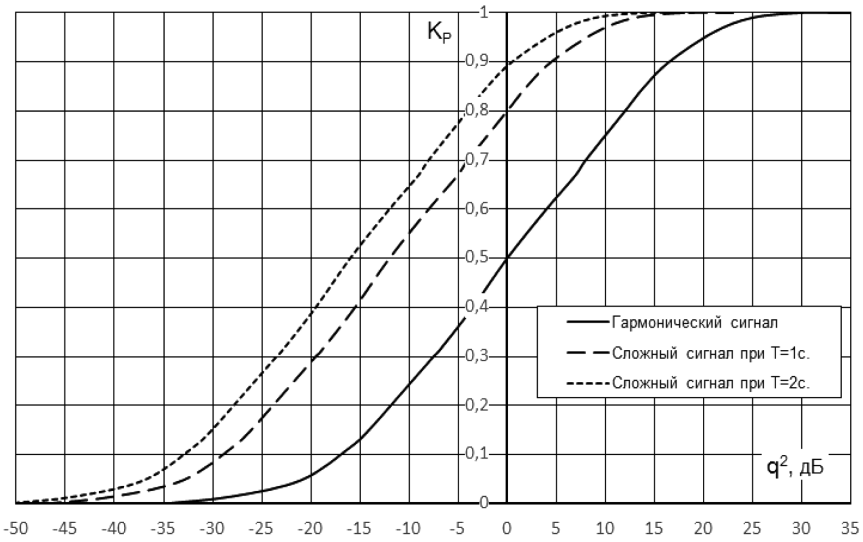

Рис. 2. Зависимость коэффициента разборчивости речи $K_{\text{р}}$ от ОСШ на выходе ТКУ для ГИС и СИС ББ

Fig. 2. Dependence of coefficient of speech legibility on the signal-to-noise ratio at the exit of the technical channel of leak for a harmonic measuring signal and a complex measuring signal with a large base

вой информации и требует дальнейшего развития. Это в первую очередь относится к установлению нормативного показателя защищенности от утечки РС в цифровой форме. Преобразования РС из аналоговой формы в цифровую и наоборот обусловливают необходимость предложить и научно обосновать единый критерий оценки защищенности. В качестве критерия оценки качества РС в цифровой форме используют вероятность ошибочного приема бита. Необходимо исследовать и установить взаимосвязь между величиной разборчивости речи и вероятностью ошибочного приема бита. Важно определить численное значение показателя защищенности РС в цифровой форме в зависимости от численного значения нормированного показателя защиты аналогового РС.

По формуле Шеннона для нормированного численного значения ОСШ по мощности устанавливают пропускную способность аналогового РС [6]:

$$C_{\text{а}} = F \log\left(1 + P_{\text{с}} / P_{\text{ш}}\right), \text{ бит/с.} \tag{7}$$

Данное отношение определено в зависимости от нормированной величины разборчивости речи [1, 7]. Важным параметром, устанавливающим свойства каналов и сигналов, является пропускная способность C. Именно этот параметр предложен в качестве связующего звена между параметрами аналоговых РС и РС в цифровой форме.

При малом ОСШ для аналогового РС из формулы Шеннона значение пропускной способности представляется, согласно [7], как

$$C_{\text{а}} = F \log_2 e \cdot \frac{P_{\text{с}}}{N} = 1{,}443 \cdot F \cdot \frac{P_{\text{с}}}{N} = 1{,}443 \frac{P_{\text{с}}}{N_0} = 1{,}443\Delta\,, \tag{8}$$

где $C_{\text{а}}$ – пропускная способность канала для аналогового сигнала, бит/с; F – ширина полосы частот, Гц; $P_{\text{с}}/N$ – отношение мощности сигнала к мощности шума; $P_{\text{с}}/N_0 = \Delta$ – нормативное значение отношения мощности речевого сигнала $P_{\text{с}}$ к спектральной плотности мощности шума N_0.

Пропускная способность канала утечки информации должна быть минимальной и определяться пределом Шеннона. Зададим пропускную способность C такой, чтобы она соответствовала невозможности извлечения информации из ТКУ. Пропускная способность для симметричного дискретного канала C в битах на один отсчет вычисляется, согласно [7], следующим образом:

$$C = F\left[\log_2 m + p_{\text{ош}} \log_2 \frac{p_{\text{ош}}}{m-1} + \left(1 - p_{\text{ош}}\right)\log_2\left(1 - p_{\text{ош}}\right)\right], \tag{9}$$

где $p_{\text{ош}}$ – вероятность ошибочного приема многомерного сигнала.

Из формулы (9) при $m = 2$ получаем пропускную способность для цифрового сигнала $C_{ц}$ [7] для двоичного симметричного канала (ДСК) при условии, что пропускная способность C соответствует максимальной скорости передачи информации:

$$C_{ц} = 1 + p_{ош} \log_2 p_{ош} + (1 - p_{ош}) \log_2 (1 - p_{ош}). \quad (10)$$

По значению пропускной способности $C_{ц}$ и равенству $C_{ц} = C_{а}$ из формулы (10) вычисляют вероятность ошибочного приема бита $p_{ош}$. Нормативным значением оценки защищенности РС в цифровой форме следует принять величину вероятности ошибочного приема бита $p_{ош}$, соответствующую нормированному значению величины разборчивости речи.

Установив пропускную способность для аналогового РС (8), находим вероятность ошибочного приема бита по формуле (10), предварительно построив табличную и графическую зависимость между пропускной способностью и вероятностью ошибки [8]:

$$p_{ош} = \Phi\left(\sqrt{2 \cdot E_b / N_0}\right), \quad (11)$$

где E_b – энергия бита сигнала; $\Phi(x)$ – гауссов интеграл ошибок.

Из (8) при подстановке нормативного значения Δ получим предельную пропускную способность для цифрового сигнала. Полученное значение $C_{ц}$ позволяет по зависимости $C_{ц} = f(p_{ош})$ установить нормативную вероятность ошибочного приема бита $p_{ош}$ для ДСК.

По известной величине вероятности ошибочного приема бита устанавливают нормативное отношение энергии бита к спектральной плотности мощности шума E_b/N_0 либо отношения произведения мощности сигнала на длительность одного импульса к спектральной плотности мощности шума $P_{с}\tau/N_0$ в зависимости от используемого сигнала (противофазный фазоманипулированный сигнал, ортогональный частотно-манипулированный сигнал, сигнал с пассивной паузой амплитудно-манипулированный).

Критерием оценки защищенности аналогового РС является нормированное значение величины разборчивости речи [1]. Критерий защищенности РС в аналоговой форме должен адекватно соответствовать критерию РС в цифровой форме. В качестве критерия оценки защищенности от утечки РС в цифровой форме на основании формул Шеннона о пропускной способности канала предложено и научно обосновано числовое значение вероятности ошибочного приема бита информации.

Построена графическая зависимость коэффициента разборчивости $K_{р}$ аналогового РС от вероятности ошибочного приема бита $p_{ош}$ (рис. 3). Корреляционная теория разборчивости

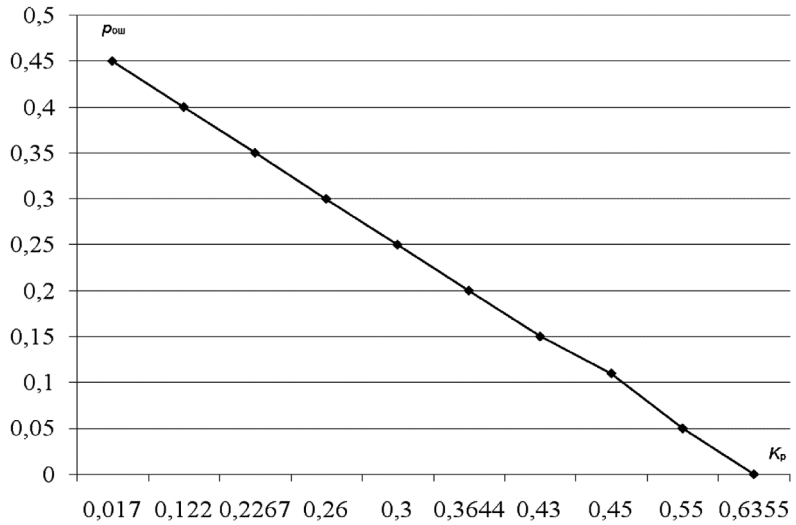

Рис. 3. Зависимость вероятности ошибочного приема бита $p_{ош}$ от коэффициента разборчивости речи $K_{р}$

Fig. 3. Dependence of bit-error probability $p_{ош}$ on coefficient of speech legibility $K_{р}$

речи по ОСШ по мощности позволяет получить расчетное численное значение величины разборчивости речи в автоматизированном режиме с применением измерительных автоматизированных систем.

Заключение. Математическая зависимость критерия оценки защищенности РС СИС ББ и критерия оценки защищенности РС ГИС позволила установить нормативное значение показателя защищенности ТКУ РС, измеренного с помощью СИС ББ.

Корреляционная теория разборчивости речи [9] по ОСШ по мощности позволяет получить расчетное численное значение величины разборчивости речи с помощью программно-аппаратного комплекса.

Таким образом, установив нормированное значение критерия защищенности РС в цифровой форме и зависимости $p_{ош} = f(K_р)$ (рис. 3), решена задача оценки в автоматизированном режиме защищенности от утечки РС в цифровой форме.

Список использованных источников

1. Железняк, В. К. Защита информации от утечки по техническим каналам / В. К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

2. Варакин, Л. Е. Теория сложных сигналов / Л. Е. Варакин. – М.: Совет. радио, 1970. – 376 с.

3. Железняк, В. К. Представление параметров широкополосного линейно-частотно-модулированного сигнала для оценки разборчивости речи в технических каналах утечки информации / В. К. Железняк, К. Я. Раханов, И. Б. Бураченок // Вестн. Полоц. гос. ун-та. Сер. С, Фундамент. науки. – 2014. – № 12. – С. 2–12.

4. Баскаков, С. И. Радиотехнические цепи и сигналы / С. И. Баскаков. – М.: Высш. шк., 1988. – 446 с.

5. Линдсей, В. С. Системы синхронизации в связи и управлении / В. С. Линдсей. – М.: Мир, 1978. – 600 с.

6. Солодов, А. В. Теория информации и ее применение к задачам автоматического управления и контроля / А. В. Солодов. – М.: Наука, 1967. – 432 с.

7. Ван Трис, Г. Теория обнаружения, оценок и модуляции : в 4 т. / Г. Ван Трис. – М.: Совет. радио, 1975. – Т. 2. – 344 с.

8. Витерби, А. Д. Принципы цифровой связи и кодирования / А. Д. Витерби, Дж. К. Омура. – М.: Радио и связь, 1982. – 536 с.

9. Покровский, Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Связьиздат, 1962. – 391 с.

References

1. Zheleznyak V.K. *Protection of the information against leakage through technical channels*]. Sankt Petersburg, State University of Aerospace Instrumentation, 2006. 188 p. (In Russian).

2. Varakin L.E. *The theory of complex signals*. Moscow, Sovetskoe Radio Publ., 1970. 376 p. (In Russian).

3. Zheleznyak V.K., Rakhanov K.Ya., Burachenok I.B. Presentation parameters of broadband linear frequency-modulated signal to evaluate intelligibility of technical information leakage channels. *Vestnik Polotskogo gosudarstvennogo universiteta Seriia C. Fundamental'nye nauki* [Herald of Polotsk State University. Series C. Fundamental Sciences], 2014, no. 12, pp. 2–12. (In Russian).

4. Baskakov S.I. *Radio circuits and signals*. Moscow, Vysshaia Shkola Publ., 1988. 446 p. (In Russian).

5. Lindsey W.C. *Synchronization systems in communication and control*. N. J., Englewood Cliff, 1972.

6. Solodov A.V. *Information theory and its application to problems of automatic control and monitoring*. Moscow, Nauka Publ., 1967. 432 p. (In Russian).

7. Van Tris G. *The theory of detection, evaluation and modulation. Vol. 2*. Moscow, Sovetskoe Radio Publ., 1975. 344 p. (In Russian).

8. Viterbi A.D. *Principles of Digital Communication and Coding*. New York, McGraw-Hill, 1979. 588 p.

9. Pokrovskii N.B. *Calculation and measurement of speech intelligibility*. Moscow, Sviaz'izdat Publ., 1962. 391 p. (In Russian).

Информация об авторах

Железняк Владимир Кириллович – доктор технических наук, профессор, заведующий кафедрой радиоэлектроники, Полоцкий государственный университет (ул. Блохина, 29, 211440, Новополоцк, Республика Беларусь). E-mail: vlad@psu.by

Information about the authors

Zheleznyak Vladimir Kirillovich – D. Sc. (Engineering), Professor, Head of the Department of Radio Electronics, Polotsk State University (29, Blohin Str., 211440, Novopolotsk, Republic of Belarus). E-mail: vlad@psu.by.

Бураченок Ирина Брониславовна – старший преподаватель кафедры технологий программирования, Полоцкий государственный университет (ул. Блохина, 29, 211440, Новополоцк, Республика Беларусь). E-mail: irina.psu@gmail.com

Рябенко Денис Сергеевич – кандидат технических наук, доцент кафедры радиоэлектроники, Полоцкий государственный университет (ул. Блохина, 29, 211440, Новополоцк, Республика Беларусь). E-mail: d.rabenka@psu.by

Для цитирования

Железняк, В. К. Критерии оценки защищенности от утечки речевых сигналов / В. К. Железняк, И. Б. Бураченок, Д. С. Рябенко // Вес. Нац. акад. навук Беларусі. Сер. фіз.-тэхн. навук. – 2017. − № 1. – С. 122–128.

Burachenok Irina Bronislavovna – Senior Lecturer, Department of Programming Technologies, Polotsk State University (29, Blohin Str., 211440, Novopolotsk, Republic of Belarus). E-mail: irina.psu@gmail.com

Rabenka Denis Sergeevich – Ph. D. (Engineering), Assistant Professor of the Department of Radio Electronics, Polotsk State University (29, Blohin Str., 211440, Novopolotsk, Republic of Belarus). E-mail: d.rabenka@psu.by.

For citation

Zheleznyak V.K., Burachenok I.B., Rabenka D.S. Assessment criteria of voice signal leakage protection. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-technichnych navuk* [Proceedings of the National Academy of Sciences of Belarus. Physical-technical series], 2017, no. 1, pp. 122–128. (In Russian).