ISSN 2411-1031. Information Technology and Security. July-December 2016. Vol. 4. Iss. 2 (7)

UDC 004.056.53

SERHII IVANCHENKO,
VITALII BEZSHTANKO,
OLEKSII HAVRYLENKO

STATISTICAL RELIABILITY OF NOISE HINDRANCE FOR ENSURING PROTECTION AGAINST LEAKAGE OF INFORMATION THROUGH TECHNICAL CHANNELS

The statistical reliability of the noise hindrance that used to protect the information against leakage through technical channels is grounded in this paper. It is a component of technical reliability of information security system and it is defined as the probability that the statistical characteristics of the studied noise hindrance will not go beyond the permissible limits. The use of this noise hindrance in security systems will guarantee to act with an effective spectral density, which will provide the necessary probability of errors and other security indicators in channel of leakage. Assessment of the effective spectral density is carried out regarding the decisive scheme of the ideal receiver, which is built on the criterion of Kotelnikov and it includes the following steps: determination function of correlation of noise process, the verification process on stationary and ergodicity, its verification on the normal distribution and the calculation of the sought effective spectral density. Determining the function of correlation of noise process is carried out with so-called "margin" on the error for the worst case from the point of view of security. Verification of the process on the temporal homogeneity and ergodic performed using Slutsky conditions. The resulting statistical reliability of the noise hindrance is the product of the statistical reliability of the estimates at all stages. It is an indicator of the reliability guarantee and component information security system as a whole.

Keywords: information, security, risk, information leakage, technical channel of leakage, noise hindrance, statistical reliability.

One of the tasks of information security, that is identified as strategy of international standards [1, 2], is to ensure the reliability of its systems of protection, including protection of information leakage through technical channels [3-5]. The reliability of any system means: its ability to keep their properties over time and characterize it as the probability of not exceeding the system parameters in the certain limits. As a rule, the reliability of technical devices is determined by their ability to perform their functions under temperature, radiation, climate and other specified conditions of exploitation. The guarantee of non exit the technical parameters from the permissible limits is a guarantee of serviceability of equipment and the guaranteed execution task with its use.

The reliability of the information security systems, in particular, the protection provided by engineering and technical facilities, is determined not only by the reliability of an enabled or used equipment solutions, quality installation, etc. So one of its components (as it can be called) is the statistical reliability of the factors randomness which is used for protection of natural or artificially created (factors).

For example, in cryptographic systems such a factor is the random sequence [6], from which the key generated, but in systems of technical protection of information – noise process is used to mask hazardous signals in environments distribution. Obviously, under the statistical reliability of these factors it should be understood that the likelihood of, for example, a process at flow of time it will remain subordinated predetermined probability distribution law. Acceptable reliability can give possibility to calculate on the maximum permissible deviations from the desired current and a corresponding diagnosis of random processes for using them in security systems.

It is known that an idealized white noise should be used to guarantee protection of information in the best way [7-9]. This is a random process, which is subordinated to the normal law of probability distribution and has got unlimited distribution of the frequency spectrum.

Consequently, for such noise hindrance, their instantaneous values in any time intervals are statistically independent. Their use makes it relatively easy to justify energy conditions in the environment spread of dangerous signals which guarantee security.

The real noise is not white. Their probabilities distribution has the deviation from the normal law and the frequency spectrum is not proportional and infinite. As usual a limitation of the spectrum is entered by intercept receiver and creates a statistical dependence of their instantaneous values.

Obviously, this can reduce the security of information and requires appropriate consideration at its evaluation.

Thus, the main objective of the article is to justify statistical reliability of noise interference, which is used to protect information from leaking by technical channels. They must guarantee the security and reliability of the protection system.

Supposably there is the noise process *n(t)*, infinitely flowing in time. Let the noise hindrance diagnosis be carried out by the method described in paper [10]. It is to fulfill the following steps:

1. Determinations in the correlation function of the process of noise:

$$R(\tau) = \frac{1}{T}\int_0^T n(t)n(t-\tau)d\tau, \tag{1}$$

where T – determining the duration of a random process.

2. Checking the process at the stationarity and ergodicity criterion for Slutsky [8]:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T R(\tau)d\tau = 0. \tag{2}$$

3. Checking random process on the normal distribution by the criterion of statistical in goodness of fit χ^2, using a the time reading interval: $\Delta t > \tau_r$,

$$\Delta t > \tau_r, \tag{3}$$

where τ_r – is the interval at which instantaneous value of the test noise process can be regarded as not correlated. In paper [10] it is called interval correlation process.

4. Calculation in the required effective spectral density is fulfilled according formula:

$$N_{0e} = N_0 \lim_{k\to\infty}\frac{\left|\mathbf{r}^k\right|^{\frac{1}{2}}}{\left|\mathbf{r}^{k-1}\right|^{\frac{1}{2}}}, \tag{4}$$

where $|\boldsymbol{r}^k|$ – is determinant of the matrix $\boldsymbol{r}^k$ the correlation coefficients:

$$\mathbf{r}^k = \begin{bmatrix} 1 & r_1 & r_2 & ... & r_{k-1} & r_k \\ r_1 & 1 & r_1 & .... & ... & r_{k-1} \\ r_2 & r_1 & 1 & .... & r_2 & ... \\ ... & .... & .... & .... & r_1 & r_2 \\ r_{k-1} & ... & r_2 & r_1 & 1 & r_1 \\ r_k & r_{k-1} & ... & r_2 & r_1 & 1 \end{bmatrix}, \tag{5}$$

where k – the maximum number of sequentially selected correlated instantaneous values.
It is defined by:

$$k = \left\lfloor \frac{\tau_r}{\Delta t} \right\rfloor \tag{6}$$

where r_i – is the correlation coefficient;

σ_r^2 – the standard deviation. For ergodic process it coincides with power.

Let us justify the statistical reliability of the investigated noise interference with its effective spectral density, which guarantees providing the desired probability of error in the technical leakage channel in any way dangerous signal processing.

1. Regarding, the first diagnosis stage, whereon the correlation function of the noise process is determined, as obviously, the statistical reliability is determined by error in measurement r and the duration of the studied process. This accounting error of, will provide either with an accurate measurement of the instantaneous values of physical media, or with the so-called "margin". If the accounting error of inaccuracy is carried out for the worst case from the point of view of protection, the function of correlation can be expressed by the formula:

$$R(\tau) = \frac{1}{T}\int_0^T [n'(t) \pm \rho_n n'(t)][n'(t-\tau) \pm \rho_n n'(t-\tau)]d\tau = \frac{1}{T}\int_0^T n'(t)n'(t-\tau)d\tau \pm (2\rho_n \pm \rho_n{}^2)\frac{1}{T}\int_0^T n'(t)n'(t-\tau)d\tau \quad (7)$$

where $n'(t)$ – is practically measured value,

ρ_n – relative error of measurement that is determined by the formula:

$$n(t) = n'(t) \pm \Delta n'(t) = (1 \pm p_n)n'(t), \quad (8)$$

where $\Delta n'(t)$ – measurement error,

τ – is interval between instantaneous values, which are measured.

When you enter a designation $\rho_r = 2\rho_n \pm \rho_n{}^2$ formula (6) takes the form:

$$R(\tau) = R'(\tau) \pm \rho_r R'(\tau). \quad (9)$$

For practical use, in view of this approach, the final form of the amendments measured by correlation function has the form:

$$R(\tau) = R'(\tau) + \rho_{r\max} R'(\tau) = (1 + \rho_{n\max})^2 R'(\tau). \quad (10)$$

The duration of the investigated noise process also affects the accuracy of the investigated correlation values. However, as shown in paper [8], increasing of this duration of has a certain limit, after which on average measurement and calculation accuracy. For use in practical investigations the indicated boundary may be found experimentally. In this case, obviously, the statistical reliability of the estimated correlation function is completely determined by the degree of trust to the acceptable errors of measuring instruments q_r which are used.

2. Obviously, in the second stage of noise hindrance diagnosis, where checks for stationarity and ergodicity are fulfilled, results of a study of the first stage can be used. Determination of the required duration of the process to enable its study is almost identical to a test for stationarity by Slutsky and therefore it can be carried out simultaneously. Therefore, the statistical reliability, which is determined in the first phase, includes the statistical reliability of the test at the second stage.

It should be noted that in electronics correlation it is considered absent, if it does not exceed 10% dispersions (power) [8] by module. According to the task of this article and calculations in the first stage of research the absence of correlation can be determined by the formula:

$$R(\tau) < \rho_r R(\tau = 0), \quad (11)$$

where $R(\tau = 0)$ – is the dispersion (power)of the studied process. Provided its ergodicity of $R(\tau = 0) = \sigma^2$.

3. The test noise which process normality of distribution, that takes place on third stage of diagnosis, it is advisable to carry on the statistical criterion χ^2, where first of all the permissible level of trust is q_N. It is the probability with which the process can be considered normally distributed, and hence the probability with which a noise process study, in the part of compliance with normal distribution law, provide protection condition, that is – reliability.

Check carried out as follows. Suppose that the actual noise $n(t)$ process is similar to the white noise, for example, which can have a deflection characteristic. Sampling noise process is carried out fairly large number of independent counting's which were taken at a time interval Δt ($\Delta t > \tau_r$) throughout the duration of the process [11].

Selective values are converted to numerical form and arranged in ascending order. Value range is divided into intervals of equal length Δn so that the values of counting's that fall into the range, rounded to one number – quantile and their number determines the frequency of quantile. The dependence of the values obtained from the frequency of their occurrence, is an approximate function of the density distribution of a continuous random variable.

Based on the obtained frequencies values it will appreciate the proximity of the real law of the distribution of the test noise process to normal. Herewith the level of trust q_N to such closeness. Let there is the sampling of N independent observations random variable n with distribution density $\omega(n)$. Let's group the N observations of K intervals Δn groups so that they in aggregate form a histogram of frequencies. So, the number of observations, which has got to i – interval, is the observation i interval – f_i. The number of observations that could get into the i – interval, if a true density of the random variable n was $\omega_0(n)$, is the expected i frequency of the interval – F_i.

Obviously, the difference between observed and expected frequencies in each i-interval is determined by the difference $|f_i - F_i|$.

The total difference of all intervals can be found by valuation differences on the expected frequency and their summation:

$$X^2 = \sum_{i=1}^{K} \frac{(f_i - F_i)}{F_i}. \quad (12)$$

After selecting the stages of degrees of freedom, which is taken as $L = K - 3$ [11] values X^2, the hypothesis checking as to normal distribution of the studies random process. Grouping the sampled values n in i intervals, $i = 1, 2, ...n, K$ and calculating the observed and expected frequencies, we can find the meaning X^2 using the formula (12). Since, each deviation $\omega(n)$ from $\omega_0(n)$ value X^2 only grow, it is expedient to use a one-sided criterion at the upper boundary.

Namely, hypothesis about normal distribution is accepted only if:

$$X^2 \le \chi^2_{L,\alpha}, \quad (13)$$

where $\chi^2_{L,\alpha}$ – value is from table χ^2-distribution of the degrees of freedom L and a level of significance α.

If $X^2 > \chi^2_{L,\alpha}$, with significance level α hypothesis $\omega(n) = \omega_0(n)$ is discarded. If $X^2 > \chi^2_{L,\alpha}$, hypothesis taken with the same level of significance.

To check the normality, by criterion consent χ^2, as a rule, equal length intervals are used. If the standard deviation of the sampled data equals s, it is recommended to take the interval length grouping to $\Delta n \approx 0{,}4s$. Moreover, the expected frequencies for each interval Δn have to be enough large. So, when choosing Δn it is recommended to fulfill the condition $F_i > 3$, for all intervals. In the implementation of verification of normality, when the frequency of the boundary meanings decrease rapidly, it is recommended that F_1 and $F_K > 3$.

Obviously, the level of confidence in such test of real noise interference for normal distribution is a level of significance: $q_N = \alpha$.

4. The fourth phase focuses on the calculation of effective spectral density using the formula (4), therefore its statistical reliability is determined by the reliability of the statistical value of N_0, which is across the dispersion σ_r. So the correlation coefficients for the formula (4) in the matrix (5), as already noted, are taken for $i = 1, 2, 3, ...$ with "margin" as a worst case, from the point of view of security:

$$r_i = r(i\Delta t) = R_i'(i\Delta t)\frac{1+\rho_r}{\sigma_r^2}; \quad (14)$$

Let us justify the reliability statistical variance σ_r, which will coincide with the statistical reliability of the spectral density N_0.

Let purpose there is a real noise process $n(t)$, which meets the requirements for stationary and ergodicity, verifiable in a second step. Then the value of the spectral density as a function of frequency equal to:

$$N_0(f) = \frac{dP}{df} \approx \sigma_n^2 \Delta t \ . \tag{15}$$

Lets find on sample data $n_j = n(t_j)$, $t_j = t_{j-1} + \Delta t$, medium sample variance s^2 and will substantiate procedure for assessment of evolution of the confidence level to the resulting value. Suppose K samples are given, where $j = 1, 2, \ldots, K$. Then the average of the variance can be expressed as a ratio [12]:

$$s^2 = \frac{1}{K-1} \sum_{j=1}^{K} (n_j - \overline{n})^2 \tag{16}$$

where $\overline{n}$ – is the average value of the random variable n:

$$\overline{n} = \frac{1}{K} \sum_{j=1}^{K} n_j \, . \tag{17}$$

If the random variable n is normally distributed with a mean value μ_n and variance σ_n^2 (μ_n and σ_n^2 – true but unknown values, which is necessary to evaluate), then

$$\sum_{j=1}^{K} (n_j - \overline{n})^2 = \sigma_n^2 \chi_k^2 \, , \tag{18}$$

where χ_k^2 – distributed chi-square value $k = K - 1$ degrees of freedom:

$$\chi^2 = z_1^2 + z_2^2 + z_3^2 + \ldots + z_k^2 \tag{19}$$

where – $z_1^2, z_2^2, z_3^2, \ldots, z_k^2$ is independent random variables have normal law distribution value with zero mean and unit variance.

Density distribution probability χ_k^2 has the form:

$$\omega(\chi^2) = [2^{k/2} \Gamma(k/2)]^{-1} (\chi^2)^{((k/2)-1)} e^{-\chi^2/2} , \tag{20}$$

where $\Gamma(k/2)$ – is gamma function.

So, the sample mean dispersion s^2 can be found by replacing in the right side of formula (16) by formula (18):

$$s^2 = \frac{\sigma_n^2 \chi_k^2}{k} \, . \tag{21}$$

If the value s is χ^2-distribution, for the significance level $\alpha<1$ the value $\chi^2_{k,\alpha}$, a exists a, for which the probability

$$P[\frac{ks^2}{\sigma_n^2} \le \chi^2_{k,\alpha}] = 1 - \alpha \, . \tag{22}$$

Hence, the true variance of the investigated noise process will take guaranteed values not lower than:

$$\sigma_n^2 \ge \frac{ks^2}{\chi^2_{k,\alpha}} \, , \tag{23}$$

and the level of confidence:

$$q_\sigma = P[\sigma_n^2 \ge \frac{ks^2}{\chi^2_{k,\alpha}}] = 1 - \alpha \, . \tag{24}$$

It is possible to find the value of the spectral density N_{0k}, where $k = 1,2,3,\ldots N$, for frequencies f_k, that are the reciprocals value of these intervals (see fig.1) finding dispersion with different reading intervals and taking it as the pulse power correspondently.

Interpolation points will allow to receive continuous dependence specified density against the frequency.

Obviously, as a worst case in terms of ensuring protection of information leakage sources, the level of confidence of such an assessment of the spectral density of noise hindrance determined by the minimum variance estimation level over all frequencies:

$$q_{\sigma}^{2} = \min_{f,k} q_{\sigma k}^{2}, \tag{25}$$

and spectral density will be taken as the minimum value $N_0 = \min_{f} N_0(f)$.

So, reasoning of the statistical reliability components of stages diagnosing noise hindrance was held and actions on the assessment and inspections have been carried out with "margin", or with confidence levels, respectively, q_r, q_N and q_σ. These levels of confidence are the probabilities of a sequence of independent stages-events, so the probability of all the stages is compatible:

$$q_{N0e} = q_r\, q_N\, q_\sigma \tag{26}$$

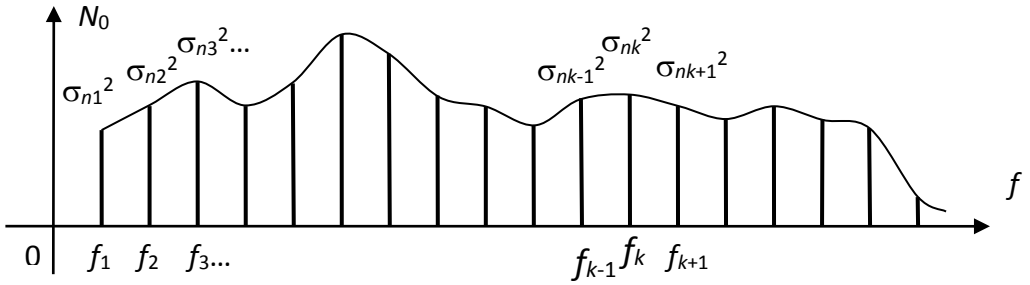

Figure1 – Graphical representation spectral density of noisy hindrance through a statistically found variance

The value q_{N0e} is a statistical reliability, which looking for, of the effective spectral density N_{0e}. The latter can be used to evaluate the probability of errors in channels of information leakage [3], and its statistical reliability can be used as part of the reliability of the entire security system.

So the statistical reliability of noise interference is grounded and used to protect information from leaking by technical channels. It is supposed that the diagnosis of the noise carried out by stages: determining noise correlation function of the process, check process on stationarity and ergodicity, check process on its distribution normality; calculate the required effective noise spectral density of the process.

The resulting statistical reliability is probability that investigated noise hindrance when using it will guarantee operating with the effective spectral density N_{0e}. It is guarantee to provide probability of errors and other security indicators in the information leakage channel.

Statistical reliability of noise hindrance is an index of guaranty and a component of reliability of the all system information security.

REFERENCES

[1] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27001, Information technology. Security techniques. Information security management. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug., 28, 2016.

[2] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27002, Information technology. Security Techniques. Code of practice for information security controls.* [Online]. Available: https://www.iso.org/standard/54533.html. Accessed on: Aug., 28, 2016.

[3] G.A. Buzov, S.V. Kalinin, and A.V. Kondratev, *Protection Information Against Leakage Through Technical Channels.* Moscow, Russia: Goryachaya liniya, Telekom, 2005.

[4] S.V Lenkov, D.A. Peregudov and V.A. Khoroshko, *Methods and Means of Information Protection. Volume I.Unauthorized Receiving the Information.* Kyiv, Ukraine: Arii, 2008.

[5] G. Kuhn, *Compromising Emanations: Eavesdropping Risks of Computer Displays. Technical Report.* [Online]. Available: http://www. cl. cam. ac. uk/techreports. Accessed on: Aug., 28, 2016.

[6] Ueli M. Maurer, "A Universal Statistical Test for Random Bit Generators", *Journal of Cryptology*, vol. 5, iss. 2, pp. 89-105, January 1992. doi: 10.1007/BF00193563.

[7] S.O. Ivanchenko, "Justification Risk Security of Information From Leakage by Technical Channels", *Legal, Regulatory and Metrological Support of Information in Ukraine*, no.1 (31), pp. 9-13, 2016.
[8] S.I. Baskakov, *Radio Technical Circuits and Signals.* Moscow, Russia: Vysshaia shkola, 1988.
[9] D L Burachenko et al., *Common Theory of Communication.* Moscow, Russia: VAS, 1970.
[10] S.O Ivanchenko, V.O. Khoroshko, O.V. Ghavrylenko, and O.M. Kulinich. "The method of diagnosing noise hindrances to provide information security from leakage technical channels", *Zahist ìnformacìi: sbornyk nauchnykh trudov.* Kyiv, NAU, Release 22, p. 74-86, 2015.
[11] J. Bendat, and A. Pirsol. *Applied Analysis of Random Data.* Moscow, Russia: Mir, 1989.

The article was received 02.09.2016.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27001, Information technology. Security techniques. Information security management. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug., 28, 2016.
[2] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27002, Information technology. Security Techniques. Code of practice for information security controls.* [Online]. Available: https://www.iso.org/standard/54533.html. Accessed on: Aug., 28, 2016.
[3] Г.А. Бузов, С.В. Калинин, и А.В. Кондратьев, *Защита информации от утечки по техническим каналам.* Москва, Россия: Горячая линия, Телеком, 2005.
[4] С.В. Ленков, Д.А. Перегудов, и В.А. Хорошко, *Методы и средства защиты информации. Том I. Несанкционированное получение информации.* Киев, Украина: Арий, 2008.
[5] G. Kuhn, *Compromising Emanations: Eavesdropping Risks of Computer Displays. Technical Report.* [Online]. Available: http://www. cl. cam. ac. uk/techreports. Accessed on: Aug., 28, 2016.
[6] Ueli M. Maurer, *A Universal Statistical Test for Random Bit Generators.* Journal of Cryptology, Vol. 5, No. 2, pp. 89 – 105, 1992.
[7] С.О. Іванченко, "Обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами", *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*, № 1 (31), с. 9-13, 2016.
[8] С.И. Баскаков, *Радиотехнические цепи и сигналы*, Москва, Россия: Высшая школа, 1988.
[9] Д.Л. Бураченко, и др. *Общая теория связи.* Москва, Россия: ВАС, 1970.
[10] С.О Іванченко, В.О. Хорошко, О.В. Гавриленко, та О.М. Кулініч, "Метод діагностування шумових завад для забезпечення захищеності інформації від витоку технічними каналами", *Защита информации.* Вип. 22, с. 74-86, 2015.
[11] Дж. Бендат, и А. Пирсол, *Прикладной анализ случайных данных.* Москва, Россия: Мир, 1989.

СЕРГІЙ ІВАНЧЕНКО,
ВІТАЛІЙ БЕЗШТАНЬКО,
ОЛЕКСІЙ ГАВРИЛЕНКО.

СТАТИСТИЧНА НАДІЙНІСТЬ ШУМОВИХ ЗАВАД ДЛЯ ГАРАНТУВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Обґрунтовано статистичну надійність шумових завад, що використовуються для захисту інформації від витоку технічними каналами. Передбачається, що діагностування шуму здійснюється за етапами: визначення функції кореляції шумового процесу, перевірки процесу на стаціонарність та ергодичність, перевірки процесу на нормальність його

розподілу; розрахунку шуканої ефективної спектральної щільності шумового процесу. Отримана статистична надійність є імовірністю того, що досліджена шумова завада при її використанні гарантовано діятиме зі спектральною щільністю та забезпечуватиме в каналі витоку ймовірність помилки й інші показники захищеності. Вона гарантовано забезпечуватиме в каналі витоку імовірність помилки та інші показники захищеності. Статистична надійність шумової завади є показником гарантування та складовою надійності системи захисту інформації в цілому.

Ключові слова: інформація, безпека, ризик, виток інформації, технічний канал витоку, шумова завада, статистична надійність.

СЕРГЕЙ ИВАНЧЕНКО
ВИТАЛИЙ БЕЗШТАНЬКО,
АЛЕКСЕЙ ГАВРИЛЕНКО.

СТАТИСТИЧЕСКАЯ НАДЕЖНОСТЬ ШУМОВЫХ ПОМЕХ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Обоснованно статистическую надежность шумовых помех, используемые для защиты информации от утечки по техническим каналам. Предполагается, что диагностирование шума осуществляется по этапам: определение функции корреляции шумового процесса, проверки процесса на стационарность и эргодичность, проверки процесса на нормальность его распределения; расчета искомой эффективной спектральной плотности шумового процесса. Полученная статистическая надежность является вероятностью того, что исследована шумовая помеха при ее использовании гарантированно будет действовать со спектральной плотностью и обеспечивать в канале утечки вероятность ошибки и другие показатели защищенности. Она гарантированно обеспечивает в канале утечки вероятность ошибки и другие показатели защищенности. Статистическая надежность шумовой помехи является показателем обеспечения и составляющей надежности системы защиты информации в целом.

Ключевые слова: информация, безопасность, риск, утечка информации, технический канал утечки, шумовая помеха, статистическая надежность.

Serhii Ivanchenko, doctor of technical sciences, associate professor, professor at the security of government information resources academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.
E-mail: soivanch@ukr.net.
Vitalii Bezshtanko, candidate of technical sciences, head of laboratory, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.
E-mail: v.bezshtanko@gmail.com.
Oleksii Havrylenko, candidate of technical sciences, associate professor at the IT-security academic department, National Aviation University, Kyiv, Ukraine.
E-mail: gavrylav@gmail.com.

Сергій Олександрович Іванченко, доктор технічних наук, доцент, професор кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний університет імені Ігоря Сікорського”, Київ, Україна.
Віталій Михайлович Безштанько, кандидат технічних наук, начальник лабораторії, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний університет імені Ігоря Сікорського”, Київ, Україна.
Гавриленко Олексій Вадимович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.

Сергей Александрович Иванченко, доктор технических наук, доцент, профессор кафедры безопасности государственных информационных ресурсов, Институт специальной связи и защиты информации национального технического университета Украины “Киевский политехнический университет имени Игоря Сикорского”, Киев, Украина.

Виталий Михайлович Безштанько, кандидат технических наук, начальник лаборатории, Институт специальной связи и защиты информации национального технического университета Украины “Киевский политехнический университет имени Игоря Сикорского”, Киев, Украина.

Гавриленко Алексей Вадимович, кандидат технических наук, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.