УДК 621.39:623.624+623.77

ОБҐРУНТУВАННЯ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЇ ЩОДО ЇЇ ЗАХИЩЕНОСТІ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Іванченко Сергій
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України "Київський політехнічний інститут"

A GROUND OF RISK OF SAFETY OF INFORMATION IS ON HER SECURITY FROM SOURCE TECHNICAL CHANNELS

Ivanchenko Serhey
Institute of the special connection and defence of information
National technical university of Ukraine "Kyiv polytechnic institute"

Анотація: **Обґрунтовано зв'язок ризику безпеки інформації щодо її захищеності від витоку технічними каналами з енергетичними показниками, що мають місце в середовищі поширення небезпечних сигналів. Отримано співвідношення, які дозволяють оцінювання цього ризику відносно пропускної спроможності каналу, його імовірності помилки та відношення сигналу до завади. Ці співвідношення відрізняються від раніше відомих тим, що враховують дисбаланс даних на виході джерела витоку, який є допустимим на практиці. Отримані співвідношення дозволяють автоматизований аналіз цього ризику в реальні масштаби часу з використанням сучасних інформаційних систем та технологій.**
Ключові слова: **Інформація, безпека, ризик, виток інформації, технічний канал витоку.**
Annotation: **The article examines the communication of risk information security with respect to its protection against leakage by technical channels with the energy indicators in the environment the spread of dangerous signals. Relations are obtained that allow the assessment of risk in relation to the bandwidth of the channel, its error probability and the signal-to-noise. These ratios differ from the previously known fact that take into account the imbalance of the data at the output of the source of the leak, which is acceptable in practice. The obtained relations allow automated analysis of this risk in real time scale with the use of modern information systems and technologies**.
Keywords: **Information security risk to leak information, technical channel leakage.**

Вступ

Одним з питань управління інформаційною безпекою [1], що визначено циклом Шухарта-Демінга, є аналіз ризику цієї безпеки, в тому числі і ризику порушення захищеності інформації від витоку технічними каналами. Відомо, що робота технічних засобів та систем обробки та передачі інформації практично завжди супроводжується низкою побічних ефектів [2] – [4]. Ними є небажані випромінювання в навколишнє середовище електромагнітних полів, наведення та просочування у відвідні провідники електричних струмів. Зазначені носії можуть виникати від інформаційних джерел та неконтрольовано поширювати небезпечні сигнали за межі контрольованої зони.

Як відомо, критерієм захищеності є умова неможливості добування смислового змісту з перехопленого повідомлення [1], [5], яка в точці перехоплення визначається деякими енергетичними умовами – нормою на відношення сигналу до завади. В свою чергу норма цієї кількісної міри має бути обґрунтованою та достовірно забезпечувати зазначений вище ризик.

На теперішній час сучасна техніка обробки та передачі є високорозвиненою цифровою технікою з можливістю використання ефективних обчислювальних технологій. Це техніка, що побудована на електронній елементній базі з високим ступенем інтеграції, де сусідніми електричними колами може циркулювати закрита і відкрита інформація. Це техніка, яка досить швидко розвивається та надає все більші і більші можливості не тільки в обробці та передачі інформації, а й в її перехопленні технічними каналами витоку з ефективною обробкою перехопленої суміші. Так, наприклад, порядок частот роботи

сучасної техніки дозволяє сканувати сигнали з досить малим інтервалом зчитування – порядку 10^{-10} с. А це, в свою чергу, для ряду сигналів з низькою частотою Найквіста може дозволити не тільки обробку негауссівських завад, а й мінімізацію маскувальної дії гауссівських за рахунок кореляційних зв'язків їх відліків.

Очевидно, що все це має бути врахованим в нормах на енергетичні показники захищеності, які забезпечують допустимий ризик безпеки. Також очевидно, що окрім зазначеного, на захищеність також мають впливати і статистичні властивості джерела витоку, і використана форма представлення інформаційних даних. Вони також мають бути відповідним чином врахованими.

Таким чином, має місце актуальне завдання обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами, яке за сучасних можливостей перехоплення та обробки небезпечних сигналів вимагає ретельного перегляду існуючих методів аналізу та оновленого обґрунтування використаних для цього обмежень та припущень [1].

Основна частина

Нехай задано джерело витоку інформації як двійкове дискретне джерело *X*, що є найбільш поширеним в радіоелектронній техніці. Джерело виробляє послідовність знаків з алфавіту $\{x_1, x_2\}$, кожному з яких поставлено у відповідність безперервні реалізації сигналів $s_1(t)$ та $s_2(t)$ як форми представлення цих знаків у середовищі носіїв. Нехай кожна з реалізацій є фінітною та має однакову тривалість *T*. Умова рівної тривалості сигналів не є обов'язковою, але вона визначена синхронністю роботи цифрових технічних засобів та систем, а тому також є поширеною.

В середовищі поширення, що утворює канал витоку, на небезпечний сигнал діє завада, яка його спотворює та цим самим протидіє перехопленню інформації. Завади мають різний характер та різні походження: детерміновані та недетерміновані, природні та штучного походження, вузько- та широкосмугові, короткочасні та постійно діючі, нормально розподілені та інші завади.

В каналі всі завади спотворююче впливають на сигнал, всі мають маскувальну дію. Однак, слід зазначити, що не всі з них забезпечують захищеність. Так, наприклад, на етапі обробки недетерміновані завади можуть бути нескладно відфільтрованими від перехопленої суміші. Залежно від розподілу ймовірностей та статистичних дефектів, як вже зазначалося вище, частково відфільтрованими можуть бути і детерміновані завади. Тому для забезпечення захищеності інформації від витоку технічними каналами враховують лише ті завади, для яких можна цю захищеність довести та обґрунтувати. Як відомо, такими завадами є нормально розподілені шумові завади. Це є завади, які є досить поширеними в природі. Вони є довготривалими і розподіленими майже по всьому спектру частот.

Нехай в середовищі поширення небезпечного сигналу, що утворює канал витоку, діє лише завада, яку можна врахувати для оцінювання захищеності. Це ідеалізована модель нормально розподіленої шумової завади – білий шум $n(t)$. При цьому, як очевидно, інші завади, якщо вони і будуть присутніми в каналі витоку, то утворять лише запас в захищеності.

Як зазвичай, в реальному середовищі всі процеси знаходяться в адитивній суміші, тому сигнал, що з'явиться на виході каналу витоку та потрапить на приймач перехоплення для аналізу, матиме вид:

$$u(t) = \mu s_r(t-\tau) + n(t) = c_r(t) + n(t), \qquad (1)$$

де $c_r(t) = \mu s_r(t-\tau)$ – послаблений сигнал із затримкою в часі; μ – коефіцієнт передачі каналу; τ – час затримки сигналу в каналі.

Таким чином, технічний канал витоку інформації зручно представити як дискретно-неперервний канал на рис. 1. При цьому джерелом витоку є дані, що циркулюють в технічному засобі обробки та передачі, а "модулятором" – технічні рішення щодо представлення даних в цьому засобі як реалізації часу.

Завдання приймача перехоплення полягає в аналізі $u(t)$ та прийнятті рішення y_l щодо того, який знак був на виході джерела витоку інформації. Очевидно, що чим більш вірним є це рішення, тим більш ефективним стане перехоплення, тим меншою буде захищеність джерел від витоку інформації.

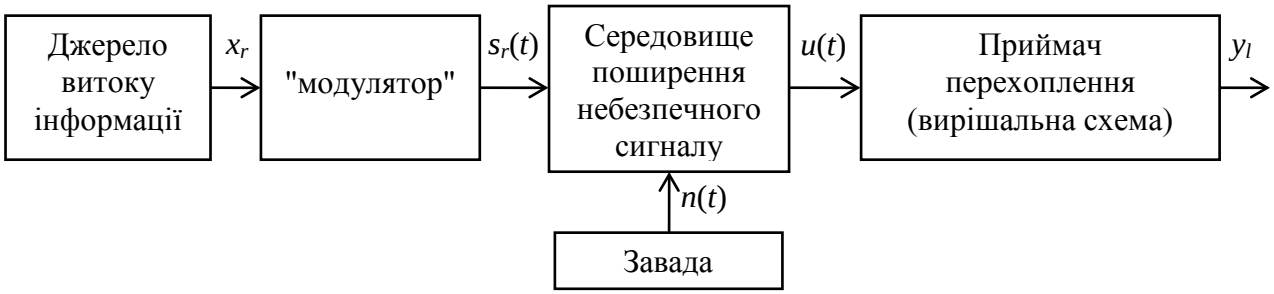

Рис. 1. Дискретно-неперервний канал як технічний канал витоку інформації

Якщо розглядати ризик безпеки інформації від витоку технічними каналами $R_{\text{ткв}}$ як кількісну міру невиконання умови захищеності, то йому можна поставити у відповідність пропускну спроможність технічного каналу витоку, виражену у вигляді її безрозмірної величини:

$$R_{\text{ткв}} \le C_{\text{ткв}} = \frac{C_{\text{кан.}}}{C_{\text{кан.max}}}, \qquad (2)$$

де для дискретного симетричного каналу з імовірністю помилки p [6]:

$$C_{\text{кан.}} = 1 + p\log_2 p + \\ +(1-p)\log_2(1-p)\ [\text{біт}], \qquad (3)$$

$$C_{\text{кан.max}} = 1\ [\text{біт}]. \qquad (4)$$

Для допустимого ризику $R_{\text{ткв доп.}}$ зазначене може бути вираженим графічно як показано на рис. 2, де $R_{\text{ткв}} \in [0, R_{\text{ткв доп.}}]$ і $R_{\text{ткв доп.}}$ є функцією від допустимої імовірності помилки $p_{\text{доп.}}$ в технічному каналі витоку.

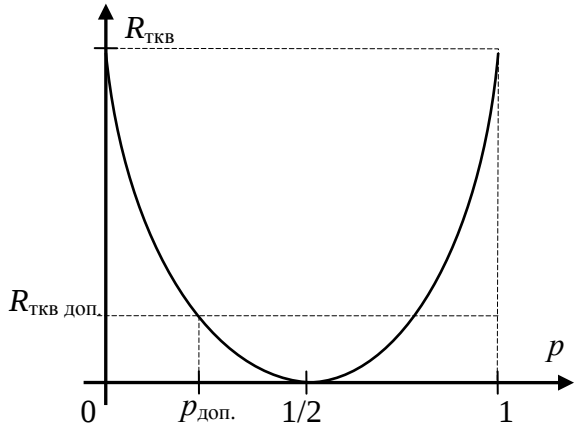

Рис. 2. Графік залежності допустимого ризику витоку інформації від імовірності помилки в ТКВ

В роботах [6, 7] показано, що для дискретно-неперервного каналу (рис. 1) при рівноймовірності знаків $p(x_1) = p(x_2)$, які виробляє джерело, відносно найкращого прийому, що обґрунтовано теорією потенційної завадостійкості, імовірність помилки визначається формулою:

$$p = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right), \qquad (5)$$

де $F(\ldots)$ – інтеграл Лапласа:

$$F(\zeta) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\zeta}\exp\left\{-\frac{\eta^2}{2}\right\}d\eta, \qquad (6)$$

P_Δ – потужність різницевого сигналу $c_\Delta(t) = c_1(t) - c_2(t)$:

$$P_\Delta = \frac{1}{T}\int_0^T c_\Delta^2(t)dt, \qquad (7)$$

N_0 – спектральна щільність шумової завади в ТКВ.

Однак для сучасної техніки обробки та передачі, яка убезпечується від витоку інформації технічними каналами, не завжди може виконуватись умова рівноймовірності інформаційних знаків, а тому формула (5) не завжди є дійсною.

Знайдемо імовірність помилки в дискретно-неперервному каналі за умови $p(x1) \ne p(x2)$.

Нехай приймачем перехоплення є оптимальний приймач, вирішальна схема якого побудована з критерієм Котельникова – максимуму апостеріорної імовірності.

$$p(y_l / u) = \max_{r=1\div 2} p(x_r / u). \qquad (8)$$

де *yl* – вірне рішення, яке має прийняти вирішальна схема приймача.

Апостеріорна імовірність може бути вираженою формулою Байеса:

$$p(x_r / u) = \frac{p(x_r)\omega_k(u / x_r)}{\omega_k(u)}. \qquad (9)$$

де ω*k*(*u*/*xr*) = ω*k*(*u*1, *u*2, *u*3,…, *uk*,/*xr*) – умовна *k*-мірна щільність розподілу відліків зчитування приймачем, ω*k*(*u*) – безумовна *k*-мірна щільність розподілу відліків *u*(*t*):

$$\omega_k(u) = \sum_{r=1}^{2} p(x_r)\omega_k(u / x_r). \qquad (10)$$

З врахуванням (9) та (10) порівняння ймовірностей (8) зводитиметься до перевірки нерівності

$$\frac{\omega_k(u / x_l)}{\omega_k(u / x_r)} = \lambda_{kl/r}(u) > \frac{p(x_r)}{p(x_l)}, \qquad (11)$$

де $\lambda_{kl/r}(u) = \lambda_{l/r}(u_1, u_2, ..., u_k)$ – *k*-мірне відношення правдоподібності.

Якщо ввести нульову реалізацію *c*0(*t*), наприклад, реалізацію на виході каналу, якщо на його вхід нічого не потрапляє, то нерівність (11) прийме вид:

$$\lambda_{l/r}(u) = \frac{\lambda_{l/0}(u)}{\lambda_{r/0}(u)} > \frac{p(x_r)}{p(x_l)}, \text{ або}$$
$$\frac{\lambda_{l/0}(u)}{p(x_r)} > \frac{\lambda_{r/0}(u)}{p(x_l)}. \qquad (12)$$

Якщо спектр частот реалізацій знаків фінітний та повністю зосереджений в смузі частот *F*, то за теоремою Котельникова кількість відліків зчитування може обмежитись числом *k* = 2*FT*, а тому:

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \frac{\omega(u_1, u_2, ..., u_{2FT} / x_r)}{\omega(u_1, u_2, ..., u_{2FT} / 0)}. \qquad (13)$$

Для білого шуму як завади, виходячи зі статистичної незалежності його відліків зчитування, 2*FT*-мірна умовна щільність розподілу за умови нульової реалізації виражатиметься як добуток одномірних щільностей нормального закону розподілу:

$$\omega(u_1, u_2, ..., u_{2FT} / 0) = \prod_{i=1}^{2FT} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{u_i^2}{2\sigma^2}} = \frac{1}{(\sigma\sqrt{2\pi})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT} u_i^2\right\}, \qquad (14)$$

а за умови *r*-тої реалізації –

$$\omega(u_1, u_2, ..., u_{2FT} / x_r) = \omega(u_1 - c_{r1}, u_2 - c_{r2}, ..., u_{2FT} - c_{r2FT} / 0) = \frac{1}{(\sigma\sqrt{2\pi})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\right\} \qquad (15)$$

Розділивши (15) на (16), знайдемо відношення правдоподібності для *xr* за заданою вибіркою *u*(*t*):

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \exp\left\{\frac{1}{2\sigma^2}\sum_{i=1}^{2FT} u_i^2\right\} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\right\} \qquad (16)$$

За умови ергодичності завади її дисперсія може бути прирівняною до потужності, вираженою через спектральну щільність *N*0 в смузі частот пропускання *F*:

$$\sigma^2 = P_з = N_0 F. \qquad (17)$$

З врахуванням останнього для двійкового джерела прийняття рішення вирішальною схемою оптимального приймача зводитиметься до перевірки нерівності:

$$\frac{1}{T}\int_0^T c_\Delta(t) n(t) dt > -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}. \qquad (18)$$

Тобто, якщо виконується нерівність (18), то вирішальна схема приймає рішення, що на виході джерела витоку інформації з'явився знак *x*1, а якщо ні, то – *x*2.

Однак завада може бути такою, що навіть і оптимальний приймач може прийняти помилкове рішення – в каналі матиме місце помилка. Імовірність цієї

помилки можна виразити як її математичне сподівання по всіх знаках, що виробляє джерело:

$$p = p(x1)\, p(y1/x2) + p(x2)\, p(y2/x1). \qquad (19)$$

За умови вироблення джерелом знаку $x1$ імовірність помилкового рішення:

$$p(y_2 / x_1) = p\left\{\xi \le -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}\right\}, \qquad (20)$$

де $\xi = \frac{1}{T}\int_0^T c_\Delta(t)n(t)dt$ – нормально розподілена випадкова величина з математичним сподіванням $\mathrm{M}[\xi] = 0$ та дисперсією $\mathrm{D}[\xi] = \frac{N_0 P_\Delta}{T}$ [6, 7].

Звідси ця імовірність може бути вираженою:

$$p(y_2 / x_1) = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} - \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right) \qquad (21)$$

де $F(\ldots)$ – інтеграл Лапласа [8].

Аналогічним чином може бути знайдена і імовірність помилкового прийняття рішення вирішальною схемою приймача за умови вироблення джерелом знаку x_2:

$$p(y_1 / x_2) = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} + \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right) \qquad (22)$$

Підставивши співвідношення (21) та (22) в (19) можна знайти імовірність помилки в каналі для довільного розподілу ймовірностей джерела витоку інформації. При цьому слід зазначити, що якщо виконується умова $p(x1) = p(x2)$, то співвідношення (19) в сукупності з (21) та (22) повністю збігатиметься з співвідношенням оцінювання цієї ж імовірності (5).

Висновки

Таким чином, обґрунтовано зв'язок ризику безпеки інформації щодо її захищеності від витоку технічними каналами з енергетичними показниками, що мають місце в середовищі поширення небезпечних сигналів. Отримано співвідношення, які дозволяють оцінювання цього ризику відносно пропускної спроможності каналу, його імовірності помилки та відношення сигналу до завади.

Ці співвідношення відрізняються від раніше відомих тим, що враховують дисбаланс даних на виході джерела витоку, який є допустимим на практиці. Отримані співвідношення дозволяють автоматизований аналіз цього ризику в реальні масштаби часу з використанням сучасних інформаційних систем та технологій.

Перелік посилань

[1] *Information technology. Security techniques*. Information security management systems. Requirements [ISO/IEC 27001:2013].

[2] *Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"*. – [Электронный ресурс]. – Режим доступа: http://www.zakon.rada.gov.ua/go

[3] Г. А. Бузов, *Защита информации от утечки по техническим каналам* / Бузов Г. А., Калинин С. В., Кондратьев А. В. – М.: Горячая линия – Телеком, 2005. – 416 с.

[4] G. Kuhn, *Compromising emanations: eavesdropping risks of computer displays.* This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. [Электронный ресурс]. – Режим доступа: http://www. cl. cam. ac. uk/techreports.

[5] С. В. Ленков, *Методы и средства защиты информации.* Том I. Несанкционированное получение информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко – К.: Арий, 2008. – 464 с.

[6] Л. М. Финк, Теория *передачи дискретных сообщений*. Изд. 2-е, М.: Сов. Радио, 1970. – 728 с.

[7] Д. Л. Бураченко, Г. Д. Заварин, Н. И. Клюев и др. *Общая теория связи*.– Л.: ВАС, 1970. – 412 с.

[8] И. Н. Бронштейн, К. А. Семендяев *Справочник по метематике для инженеров и учащихся вузов*. – М.: Наука, Гл. ред. физ-мат. Лит., 1986. – 544 с.

References

[1] *Information technology. Security techniques.* Information security management systems. Requirements [ISO/IEC 27001:2013].

[2] *Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh"*. – [Эlektronnыi resurs]. – Rezhym dostupa: http://www.zakon.rada. gov.ua/go

[3] H. A. Buzov, *Zashchyta ynformatsyy ot utechky po tekhnycheskym kanalam* / Buzov H. A., Kalynyn S. V., Kondratev A. V. – M.: Horiachaia lynyia – Telekom, 2005. – 416 s.

[4] G. Kuhn *Compromising emanations: eavesdropping risks of computer displays.* This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. [Эlektronnыi resurs]. – Rezhym dostupa: http://www. cl. cam. as. uk/techreports.

[5] S. V. Lenkov, *Metodu y sredstva zashchyty ynformatsyy.* Tom I. Nesanktsyonyrovannoe poluchenye ynformatsyy / S. V. Lenkov, D. A. Perehudov, V. A. Khoroshko – K.: Aryi, 2008. – 464 s.

[6] L. M. Fynk, *Teoryia peredachy dyskretnukh soobshchenyi.* Yzd. 2-e, M.: Sov. Radyo, 1970. –728 s.

[7] D. L. Burachenko, H. D.Zavaryn, N. Y. Kliuev y dr. *Obshchaia teoryia sviazy*.– L.: VAS, 1970. – 412 s.

[8] Y. N. Bronshtein, K. A. Semendiaev *Spravochnyk po metematyke dlia ynzhenerov y uchashchykhsia vuzov*. – M.: Nauka, Hl. red. fyz-mat. Lyt., 1986. – 544 s

Реферат

Іванченко Сергій

Обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами

Одним з питань управління інформаційною безпекою, що визначено циклом Шухарта-Демінга, є аналіз ризику цієї безпеки, в тому числі і ризику порушення захищеності інформації від витоку технічними каналами. Ними є небажані випромінювання в навколишнє середовище електромагнітних полів, наведення та просочування у відвідні провідники електричних струмів. Критерієм захищеності є умова неможливості добування смислового змісту з перехопленого повідомлення, яка в точці перехоплення визначається деякими енергетичними умовами – нормою на відношення сигналу до завади. В свою чергу норма цієї кількісної міри має бути обґрунтованою та достовірно забезпечувати зазначений вище ризик. На теперішній час сучасна техніка обробки та передачі є високорозвиненою цифровою технікою з можливістю використання ефективних обчислювальних технологій. Це техніка, що побудована на електронній елементній базі з високим ступенем інтеграції, де по сусіднім електричним колам може циркулювати закрита і відкрита інформації. Це техніка, яка досить швидко розвивається та надає все більші і більші можливості не тільки в обробці та передачі інформації, а й в її перехопленні через технічні канали витоку з ефективною обробкою перехопленої суміші. Окрім зазначеного, на захищеність також мають впливати і статистичні властивості джерела витоку, і використана форма представлення інформаційних даних. Все це має бути врахованим в нормах на енергетичні показники захищеності, які забезпечують допустимий ризик безпеки. В статті вирішується актуальне завдання обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами. Обґрунтовано його зв'язок з енергетичними показниками, що мають місце в середовищі поширення небезпечних сигналів. Отримано співвідношення, які дозволяють оцінювання цього ризику відносно пропускної спроможності каналу, його імовірності помилки та відношення сигналу до завади. Ці співвідношення відрізняються від раніше відомих тим, що враховують дисбаланс даних на виході джерела витоку, який є допустимим на практиці. Отримані співвідношення дозволяють автоматизований аналіз цього ризику в реальні масштаби часу з використанням сучасних інформаційних систем та технологій.

Иванченко Сергей

Обоснование риска безопасности информации по ее защищенности от утечки по техническим каналам

Одним из вопросов управления информационной безопасностью, которое определенно циклом Шухарта-Деминга, является анализ риска этой безопасности, в том числе и риска нарушения защищенности информации от утечки по техническим каналам. Ими являются нежелательные излучения в окружающую среду электромагнитных полей, наводок и просачивания в посторонние проводники электрических токов. Критерием защищенности является условие невозможности добывания смыслового содержания из перехваченного сообщения, который в точке перехвата определяется некоторыми

энергетическими условиями - нормой на отношение сигнала к помехе. В свою очередь норма этой количественной меры должна быть обоснованной и достоверно обеспечивать отмеченный выше риск. На настоящее время современная техника обработки и передачи является высокоразвитой цифровой техникой с возможностью использования эффективных вычислительных технологий. Это техника, которая построена на электронной элементной базе с высокой степенью интеграции, где по соседним электрическим кругам может циркулировать закрытая и открытая информации. Это техника, которая достаточно быстро развивается и предоставляет все большие и большие возможности не только в обработке и передаче информации, но и в ее перехвате через технические каналы утечки с эффективной обработкой перехваченной смеси. Кроме отмеченного, на защищенность также должны влиять и статистические свойства источника утечки, и использованная форма представления информационных данных. Все это должно быть учтенным в нормах на энергетические показатели защищенности, которые обеспечивают допустимый риск безопасности. В статье решается актуальное задание по обоснованию риска безопасности информации по ее защищенности от утечки по техническим каналам. Обоснована его связь с энергетическими показателями, которые имеют место в среде распространения опасных сигналов. Получены соотношения, которые позволяют оценивание этого риска относительно пропускной способности канала, его вероятности ошибки и отношения сигнала к помехе. Эти соотношения отличаются от ранее известных тем, которые учитывают дисбаланс данных на выходе источника утечки, который является допустимым на практике. Полученные соотношения позволяют автоматизированный анализ этого риска в реальные масштабы времени с использованием современных информационных систем и технологий.

Ivanchenko Serhey

A ground of risk of safety of information is on her security from source technical channels

One on questions a management informative safety, that certainly by the cycle of Shuharta-Deming, an analysis of risk of this safety is, including to the risk of violation of security of information from a source technical channels. By them are undesirable radiations in the environment of the electromagnetic fields, aiming and impregnation in discharge explorers of electric currents. The criterion of security is a condition of impossibility of getting of semantic maintenance from the intercepted report that in the point of intercept is determined by some power terms - norm on attitude of signal toward a hindrance. In turn a norm of this quantitative measure must be reasonable and for certain to provide the risk marked higher. On present tense a modern technique of treatment and transmission is a highly developed digital technique with possibility of the use of effective calculable technologies. It is a technique that is built on an electronic element base with the high degree of integration, where for can circulate nearby electric circles closed and open to information. It is a technique, that quickly enough develops and gives all greater and greater possibilities not only in treatment and information transfer but also in her intercept through the technical channels of source with effective treatment of the intercepted mixture. Except marked, on security also must influence and statistical properties of source of source, and used form of presentation of informative data. All of it must be taken into account in norms on the power indexes of security, that provide the possible risk of safety. In the article the actual task of ground to the risk of safety of information decides on her security from a source technical channels. His connection is reasonable with power indexes that take place in the environment of distribution of dangerous signals. Correlations, that allow the evaluation of this risk concerning admission ability of channel, his probability of error and relation of signal to the hindrance, are got. These correlations differ from earlier well-known those that take into account the disbalance of data-outs source of source that is possible in practice. The got correlations allow the automated analysis of this risk in the real times with the use of the modern informative systems and technologies.

Відомості про автора

Іванченко Сергій Олександрович

***Освіта*:** Київське вище військове інженерне училище зв'язку ім. М. Калініна (1992).

Місце роботи: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», професор, д.т.н. (2015).

Область знань: інформаційна безпека.

Email: *soivanch@ukr.net*