https://doi.org/10.31891/2219-9365-2023-74-3
УДК 621.396.969.1

СТЕПАНОВ Михайло
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0001-6376-4268
e-mail: 2m.stepanov@gmail.com
БОЙКО Юлій
Хмельницький національний університет
https://orcid.org/0000-0003-0603-7827
e-mail: boiko_julius@ukr.net
ПАВЛЕНКО Євген
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0002-0451-3861
e-mail: sl1mvsshady@gmail.com

ВИЗНАЧЕННЯ НЕОБХІДНОГО РІВНЯ СИГНАЛУ ТА МАСКУЮЧОГО ШУМУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ЇЇ ПЕРЕХОПЛЕННЯ ТЕХНІЧНИМИ ЗАСОБАМИ

В даній роботі розглядаються потенційні способи захисту сигналу на базі існуючої математичної моделі каналу витоку інформації в умовах радіотехнічної розвідки. Використана в дослідженні математична модель, при різних модифікаціях функції правдоподібності, яка по суті представляє собою математичний запис теореми Байєса, показує яким чином із апріорних даних і результатів аналізу прийнятого коливання формуються апріорні значення. Розглянута оптимальна схема виявлення детермінованого сигналу на фоні шуму, а також чотири можливих випадки виявлення сигналу, що порівнюються с встановленим порогом H і завжди супроводжуються помилками двох видів – неправильне рішення про наявність сигналу та помилкове рішення про його відсутність. На базі першого і третього випадків запропоновані потенційні варіанти захисту вихідного сигналу.

Ключові слова: технічний захист інформації, радіотехнічна розвідка, маскувальний шум, перехоплення сигналу, контрольована зона

STEPANOV Mykhailo
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
BOIKO Juliy
Khmelnytskyi National University
PAVLENKO Yevhen
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

DETERMINING THE REQUIRED SIGNAL LEVEL AND MASKING NOISE TO PROTECT INFORMATION IN THE CONDITIONS OF ITS INTERCEPTION BY TECHNICAL MEANS

This paper discusses potential ways to protect the signal based on the existing mathematical model of the information leakage channel in the conditions of electronic intelligence. The mathematical model used in the study, with various modifications of the likelihood function, which is essentially a mathematical representation of Bayes' theorem, shows how a priori values are formed from a priori data and the results of the analysis of the received fluctuation. An optimal scheme for detecting a deterministic signal against a noise background is considered, as well as four possible cases of signal detection, which are compared with the set threshold H and are always accompanied by two types of errors - an incorrect decision about the presence of a signal and an erroneous decision about its absence. Based on the first and third cases, potential options for protecting the output signal are proposed. The first part of the work presents a possible way to protect the output signal, when, with a known distance from the transmitter to the receiver and the maximum gain of the receiver antenna, a dependence is presented for calculating the signal value, which is sufficient for reception within the controlled zone, but insufficient for interception by technical means outside the controlled area. The second part considers the possibility of preventing the interception of information by means of technical intelligence by masking signals that go beyond the controlled zone with specially generated noise. A block diagram of the interception of the output signal by means of technical intelligence using masking noise is presented. One of the important steps in building the technical protection of an information system is to identify possible channels for leaking confidential information. The modeling of such technical channels makes it possible to identify and structure possible risks and dangers, as well as to suggest ways to counteract such dangers. In the context of this topic, modern methods of protecting information from sources by technical channels, as well as ways to reduce the likelihood of its interception by technical means, were considered. Based on the results of the research, conclusions were drawn about the proposed methods for protecting information based on the existing model by calculating the required level and masking the output signal, and their expediency in the tasks of preventing the interception of information by technical means was substantiated.

Keywords: technical protection of information, radio technical intelligence, masking noise, signal overshooting, controlled zone

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Одним із важливих етапів побудови технічного захисту інформаційної системи являється виявлення можливих каналів витоку конфіденційної інформації. Моделювання таких технічних каналів дозволяє визначити та структурувати можливі ризики та небезпеки, а також запропонувати шляхи протидії таким небезпекам. Обґрунтована необхідність даного дослідження полягає в розширенні та вдосконаленні існуючих способів та методів захисту інформації в задачах протидії засобам технічної розвідки.

В роботі представлений можливий спосіб захисту вихідного сигналу коли при відомій відстані від передавача до приймача та максимального коефіцієнту підсилення антени приймача. Представлена залежність для розрахунку величини сигналу яка достатня для прийому в межах контрольованої зони але недостатня для перехоплення технічними засобами за межами контрольованої зони. Розглядається можливість запобігання перехопленню інформації засобами технічної розвідки шляхом маскування сигналів, що виходять за межі контрольованої зони, спеціально сформованим шумом. Представлена структурна схема перехоплення вихідного сигналу засобами технічної розвідки з використанням маскувального шуму.

Аналіз досліджень та публікацій

В контексті даної тематики, були розглянуті сучасні методи захисту інформації від витоків технічними каналами, а також способи зниження ймовірності її перехоплення технічними засобами. Так, в роботі [1], в області військового зв'язку представлені експериментальні результати для захисту радіопристроїв від перехоплень шляхом передачі потужних завад на базі представленого «радіозахисного екрану». В статті [2], на основі розрахунку ефективності екранування випромінювання ІТ-обладнання, мінімізується ризик прослуховування інформації шляхом перехоплення електромагнітного випромінювання, а в роботі [3], розглянутий метод маскування для захисту інформаційно-технічного обладнання від витоків інформації шляхом перехоплення електромагнітного випромінювання, в результаті якого можна значно знизити як захисну відстань так і відношення сигнал-шум на боці приймача перехоплювача. В статті [4], для захисту мережі когнітивного радіо і погіршення якості сигналу перехоплення пропонується використовувати штучний шум, а в роботі [5] пропонується метод формування комбінованих маскувальних сигналів для систем захисту від витоків голосової інформації акустичними каналами. В статті [6], за допомогою математичного моделювання процесів, були підтверджені теоретичні результати, що дозволяють виявляти випадкові радіосигнали в найбільш надійний спосіб, який дозволяє перекрити канал витоку інформації та більш ефективно здійснювати превентивні заходи щодо запобігання його виникненню. В роботі [7], для зниження ймовірності перехоплення сигналу був запропонований метод маскування, який в результаті шумоподібного моделювання дозволяє отримати сигнал схожий на шум, тим самим збільшуючи його конфіденційність у разі перехоплення, а в роботі [8] представлений метод для генерації сигналу, який забезпечує більшу маскувальну здатність в порівнянні з білим шумом, що підвищує складність отримання корисної голосової інформації у разі її перехоплення.

Виклад основного матеріалу

Використана в дослідженні модель [9] включає три основних блоки:

1) блок розрахунку відношення сигнал/шум на вході розвід. приймача при розвідці радіоелектронного пристрою в заданих умовах;

2) блок описання процесу перетворення прийнятого вхідного сигналу елементами радіоприймача;

3) блок розрахунку інформаційного показника, що характеризує ефективність роботи радіоприймача в процесі розвідки.

Коротко проілюструємо основний зміст використаної моделі.

Представлена оптимальна схема виявлення сигналу, який носить детермінований характер [10], а невідомий параметр λ може приймати тільки одне з двох значень $\lambda = 1$ (в прийнятому коливанні присутній сигнал); $\lambda = 0$ (в прийнятому коливанні відсутній сигнал).

Нехай прийняте коливання $\xi(t)$ представляє суму:

$$\xi(t) = \lambda s(t) + n(t), \quad 0 \le t \le T \tag{1}$$

де $n(t)$ – білий нормальний шум;

$s(t)$ – корисний сигнал відомої форми (детермінований сигнал), повністю розташований в інтервалі спостереження.

Що стосується апріорних відомостей параметра λ, то будемо вважати, що апріорні ймовірності наявності і відсутності сигналів $W_{pr}(1)$, $W_{pr}(0)$ відомі.

ISSN 2219-9365

При неперервній обробці прийнятої реалізації апостеріорна ймовірність наявності детермінованого сигнала *(λ = 1)* визначається формулою:

$$W_{ps}(1) = kW_{pr}(1)\exp\left\{-\frac{1}{N_0}\int_0^T [\xi(t) - s(t)]^2\, dt\right\} \tag{2}$$

Апостеріорна ймовірність відсутності сигналу ($\lambda = 0$), очевидно, рівна:

$$W_{ps}(0) = kW_{pr}(0)\exp\left\{-\frac{1}{N_0}\int_0^T \xi^2(t)dt\right\}, \tag{3}$$

причому:

$$W_{pr}(0) + W_{pr}(1) = 1. \tag{4}$$

Далі представлено чотири реалізації випадкового коливання: перші дві зображають шум на виході узгодженого фільтра $q_п$, а дві інші - суму сигналу та шуму $q=q(1)$. Нехай встановлено деякий поріг H. Для конкретних реалізацій, наведених на рис. 1 можна побачити, що шум у першій реалізації не перевищує порога. У другій реалізації сигналу немає, проте значення шуму перевищує поріг. У третій реалізації сума сигналу і шуму перевищує поріг, а в четвертій реалізації видно, що незважаючи на наявність сигналу, поріг не досягається:

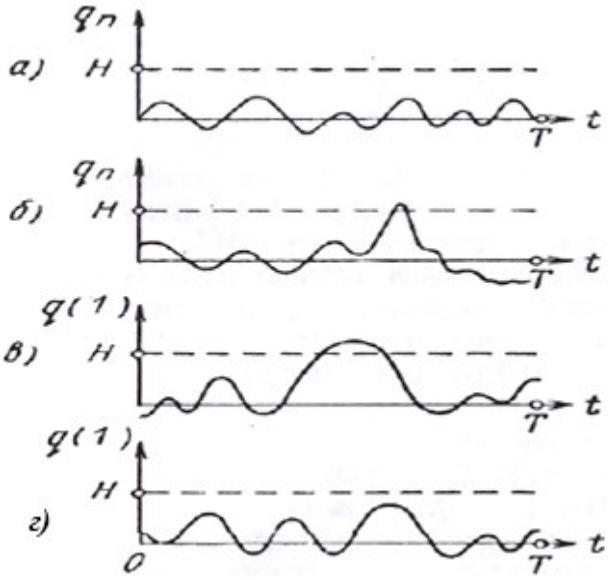

Рис. 1. Чотири можливих випадки при виявленні сигналу на фоні шуму

З розглянутих чотирьох випадків у двох випадках (першому та третьому) буде прийнято правильне рішення, а у двох інших (другому та четвертому) – неправильне. Якщо взяти інший поріг H, описана ситуація може змінитися.

Таким чином, можна дійти до висновку, що питання наявності чи відсутності сигналу супроводжується помилками двох видів:

1) незважаючи на відсутність сигналу, шум перевершує поріг і приймається неправильне рішення про наявність сигналу (помилка першого роду);

2) хоча сигнал присутній, але граничний рівень не перевищений приймається помилкове рішення про відсутність сигналу (помилка другого роду);

На рис. 2 наведено оптимальну схему для виявлення детермінованого сигналу на фоні шуму:

ISSN 2219-9365

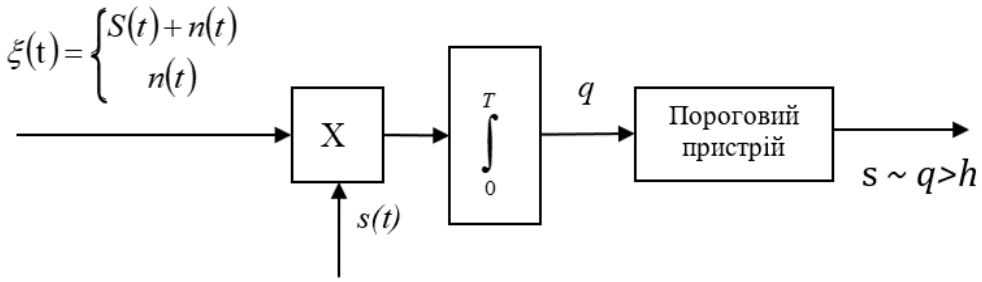

Рис. 2. Оптимальна схема для виявлення детермінованого сигналу на фоні шуму

Якщо пороговий рівень перевищений, приймається рішення про наявність сигналу. Якщо ж поріг не перевищений, то констатується відсутність сигналу.

1. Розглянемо один із можливих способів захисту вихідного сигналу. При відомій відстані від передавача до приймача та максимальному коефіцієнту підсилення антени приймача, можна розрахувати величину сигналу достатнього для прийому в межах контрольованої зони, але недостатнього для його перехоплення засобами технічної розвідки за межами контрольованої зони.

Нехай джерело випромінювання – антена радіоелектронного засобу, що характеризується коефіцієнтом підсилення $G_{ПЕР}$, тоді густина потоку потужності на відстані D в направленні максимуму випромінювання буде визначатись як:

$$П_д = \frac{P_\Sigma G_{ПЕР}}{4\pi D^2} \tag{5}$$

де P_Σ – потужність джерела випромінювання, Вт;
$G_{ПЕР}$ – коефіцієнт направленої дії антени радіоелектронного засобу;
$4\pi D^2$ – площа сфери радіусу D, апроксимуючого фронту електромагнітної хвилі;
D – дальність від радіоелектронного засобу до приймача [11-13].

При відомій ефективній площі прийомної антени S, потужність сигналу на вході прийомної антени буде рівна:

$$P_{С\,ПР} = S \cdot П_Д \tag{6}$$

Коефіцієнт підсилення антени $G_{ПР}$ та її ефективна площа розсіювання S пов'язані співвідношенням:

$$S = \frac{\lambda^2 G_{ПР}}{4\pi} \tag{7}$$

де λ - довжина хвилі випромінювання, м.

З урахуванням (1) формулу (2) можна записати у вигляді:

$$P_{С\,ПР} = \frac{P_\Sigma \lambda^2 G_{ПР} G_{ПЕР}}{16\pi^2 D^2 K_б} \tag{8}$$

Отже, при відомих значеннях D (відстань від приймача до передавача) і $G_{пр\ max}$ (максимальний коефіцієнт підсилення антени приймача), можна розраховувати мінімальну величину сигналу, що передається за допомогою регулювання відповідного коефіцієнта $G_{пер\ min}$.

$$G_{пер\,min} = \frac{P_{с\,пр} \cdot 16П^2 D^2 K_б}{G_{пр\,max} P_\Sigma \lambda^2} \tag{9}$$

Таким чином, якщо засіб технічної розвідки буде знаходись за межами контрольованої зони, тоді значення сигналу передавача не досягне порогового рівня H засобу технічної розвідки (див. рис.1 г), що відповідно забезпечить захист даного вихідного сигналу.

Розглянемо можливість запобігання перехопленню інформації засобами технічної розвідки шляхом маскування сигналів, що виходять за межі контрольованої зони, спеціально сформованим шумом.

Найбільш оперативним та економічним вирішенням цього завдання є активне маскування голосового сигналу низькочастотним відрізком білого шуму.

Визначимо необхідний мінімальний рівень маскувальних шумів для захисту сигналу за межами контрольованої зони. Розглянемо структурну схему перехоплення вихідного сигналу засобами технічної розвідки (ЗТР), рис. 3.

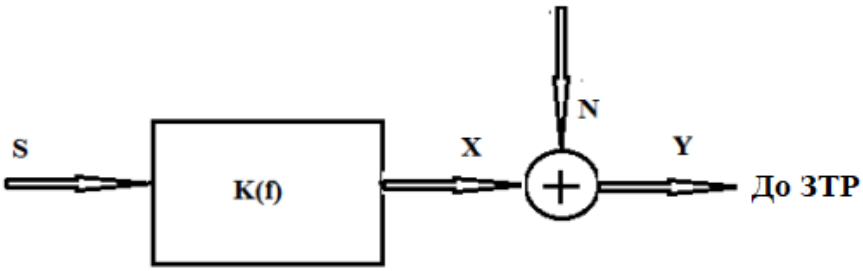

Рис. 3. Структурна схема перехоплення вихідного сигналу ЗТР: S – тестовий сигнал; Y – адитивна суміш вихідного сигналу X і зовнішнього шуму N; K(f) – комплексна частотна характеристика огороджувальної конструкції; ЗТР – засіб технічної розвідки

Якщо, маскувальний шум відсутній ($M = 0$) і на виході схеми діє адитивна суміш вихідного сигналу X із зовнішнім (фоновим) шумом N:

$$Y = \sqrt{X^2 + N^2}$$

Тоді вихідний сигнал X_i:

$$X_i = \sqrt{Y_i^2 - N_i^2} = S_i \cdot K(f_i) \tag{10}$$

Нехай на виході контрольованої зони встановлено деякий поріг $H_{iн}$ для ЗТР. Тоді розглянемо випадок, коли сигнал не захищений і перевищує поріг $H_{iн}$, тобто:

$$H_{iн} - H_i = \Delta H_i \tag{11}$$

де ΔH_i – перевищення сигналом порогового рівня ЗТР

$$H_{iн} = H_i + \Delta H_i \tag{12}$$

У цьому випадку, задача активного маскування полягає в задаванні такого мінімального рівня маскувального сигналу M_i при якому $H_{Mi} > H_{iн}$.

Для виконання умови (12), сформуємо активну шумову заваду M. Дана завада відрізняється від зовнішнього фонового шуму відносно стабільною інтенсивністю її формування на протязі всього часу життєвого циклу вихідного сигналу. Представимо відношення сигнал/шум в кінематичній формі для двох значень активної шумової завади $M = 0$ і $M \neq 0$.

Якщо $M = 0$:

$$q_i = \frac{(S_i \cdot K(f_i))^2}{N_i^2},$$

Якщо $M \neq 0$:

$$q_{M_i} = \frac{(S_i \cdot K(f_i))^2}{N_i^2 + M_i^2},$$

де q_i, q_{Mi} - відношення сигнал/шум при відсутності активної маскувальної завади і при наявності активної шумової завади відповідно.

Представимо відношення виду:

$$\frac{q_i}{q_{M_i}} = 1 + \frac{M_i^2}{N_i^2} = \delta Q_i \qquad (13)$$

де δQ_i – кінематичне значення перевищення сигналом порогового рівня ЗТР.

Із виразу (13), кінематичний параметр маскувальної завади, який забезпечує рівність (12) і являється мінімально необхідним рівнем інтенсивності маскувальної завади може бути представлений наступним виразом:

$$M_i = N_i \sqrt{\frac{q_i}{q_{M_i}} - 1} = N_i \cdot \sqrt{\delta Q_i - 1} \qquad (14)$$

Таким чином, структурна схема перехоплення вихідного сигналу ЗТР буде мати наступний вигляд:

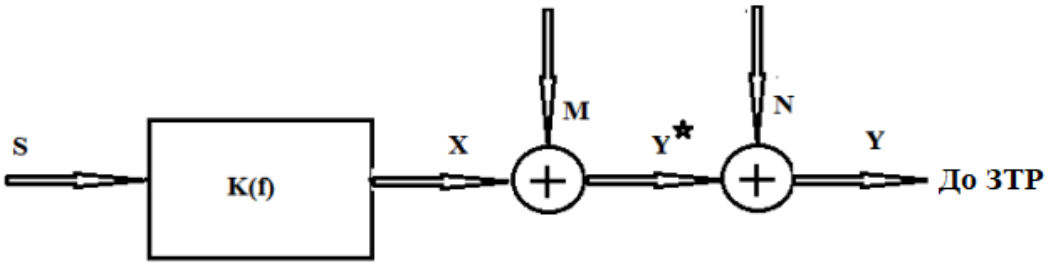

Рис. 4. Структурна схема перехоплення вихідного сигналу ЗТР з використанням маскувального шуму М: Y* – адитивна суміш вихідного сигналу X з маскувальним шумом M; Y – адитивна суміш вихідного сигналу X з маскувальним шумом M і зовнішнім шумом N.

Висновки з даного дослідження і перспективи подальшого розвитку у даному напрямі

1. В ході дослідження, була проаналізована математична модель каналу витоку інформації в умовах радіотехнічної розвідки в якій представлена оптимальна схема виявлення сигналу, що носить детермінований характер (рис. 2). За результатами аналізу були розглянуті чотири можливих випадки виявлення сигналу на фоні шуму (рис. 1), на базі двох з яких (рис. 1 б, г) були представлені можливі варіанти захисту вихідного сигналу.

2. За результатами дослідження була отримана залежність (9), для розрахунку величини вихідного сигналу, достатнього для прийому в межах контрольованої зони, але недостатнього для перехоплення технічними засобами за її межами.

Таким чином, якщо засіб технічної розвідки буде знаходись за межами контрольованої зони, тоді значення сигналу передавача не досягне порогового рівня H засобу технічної розвідки, що відповідно забезпечить захист даного вихідного сигналу.

3. За результатами дослідження була отримана залежність (14), для визначення мінімально необхідного рівня інтенсивності маскувальної завади, яка відрізняється від зовнішнього фонового шуму відносно стабільною інтенсивністю її формування на протязі всього часу життєвого циклу вихідного сигналу.

Тим самим, виконується задача запобігання перехопленню інформації засобами технічної розвідки шляхом маскування сигналів, що виходять за межі контрольованої зони спеціально сформованим шумом.

Перспективи подальшого розвитку у даному напрямі, за результатами проведених досліджень, ґрунтуються на запропонованих способах захисту інформації з використанням базової існуючої моделі і спрямовані на розрахунок необхідного рівня та маскування вихідного сигналу, обґрунтування їх доцільності в задачах запобігання перехопленню інформації технічними засобами.

Література

1. Riihonen T. Military Full-Duplex Radio Shield for Protection Against Adversary Receivers / T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmaki, M. Valkama, R. Wichman // 2019 International Conference on Military Communications and Information Systems (ICMCIS), (Budva, Montenegro, 14-15 May 2019). – Budva : IEEE, 2019. – P. 1-6.

2. Nowosielski L. Shielding effectiveness required for IT equipment enclosures / L. Nowosielski, J. Michalak // 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL), (Singapore, 19-22 November 2017). – Singapore : IEEE, 2017. – P. pp. 427-431.

3. Tajima K. Effect evaluation of countermeasure method for image information leakage by electromagnetic radiation from ITE / K. Tajima, Y. Suzuki, R. Ishikawa, H. Nobata, Tetsuya T., J. Kato // 2019 International Symposium

on Electromagnetic Compatibility - EMC EUROPE, (Barcelona, Spain, 02-06 September 2019). – Barcelona : IEEE, 2019. – P. 394-397.

4. Wu Y. Secure beamforming for cognitive radio networks with artificial noise / Y. Wu, X. Chen, X. Chen // 2015 International Conference on Wireless Communications & Signal Processing (WCSP), (Nanjing, China, 15-17 October 2015). – Nanjing : IEEE, 2015. – P. 1-5.

5. Seitkulov Y. Rationale for the method of formation of the combined speech masking signals / Y. Seitkulov, S. Boranbayev, B. Yergaliyeva, G. Davydov, A. Patapoviche // 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), (Astana, Kazakhstan, 15-17 October 2014). – Astana : IEEE, 2014. – P. 1-4.

6. Lukova-Chuiko N. The Method Detection of Radio Signals by Estimating the Parameters Signals of Eversible Gaussian Propagation / N. Lukova-Chuiko, O. Herasymenko, S. Toliupa, S. Laptiev, T. Laptieva, O. Laptiev // 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), (Kyiv, Ukraine, 15-17 December 2021). – Kyiv : IEEE, 2021. – P. 67-70.

7. Wu Y. The Noise-like Disguised Scheme for Physical Layer Security Using Phase Rotation And Wavelet Transform / Y. Wu, C. Chen // 2018 5th International Conference on Systems and Informatics (ICSAI), (Nanjing, China, 10-12 November 2018). – Nanjing : IEEE, 2018. – P. 823-827.

8. Jingsai J. Adaptive acoustic masking based on spectral envelope / Jiang Jingsai, Li Ye, Zhang Peng, Hao Qiuyun, Ma Xiaofeng, Fan Yanhong // 2016 International Conference on Audio, Language and Image Processing (ICALIP), (Shanghai, China, 11-12 July 2016). – Shanghai : IEEE, 2016. – P. 442-446.

9. Сягаева О.О Дослідження та розробка математичної моделі джерела небезпечного сигналу втрати інформації в банківських системах : магістерська атестаційна робота : 8.05090202 – Автоматизовані комплекси радіоелектронних виробництв / О. О. Сягаева ; ХНУРЕ. – Харків, 2012. – 90 с.

10. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. – Київ : Логос, 2018. – 227 с.

11. Бойко Ю. SAML: дефініція та принцип роботи через VPN тунель у захищених інформаційних мережах / Ю. Бойко, Б. Білявець // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2022 - № 4. С. 41–48.

12. Бойко Ю. Особливості формування кодової надлишковості у каналах передачі інформації / Ю. Бойко, А. Семенко, І. П'ятін, // Інфокомунікаційні та комп'ютерні технології. – 2022 - Т.2, №04. - С. 12-25.

13. Boiko J., Pyatin I., Eromenko O., Stepanov M. Method of the adaptive decoding of self-orthogonal codes in telecommunication //Indonesian Journal of Electrical Engineering and Computer Science (IJEECS). – 2020. – Т. 19. – №. 3. – С. 1287-1296.

References

1. Riihonen T. Military Full-Duplex Radio Shield for Protection Against Adversary Receivers / T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmaki, M. Valkama, R. Wichman // 2019 International Conference on Military Communications and Information Systems (ICMCIS), (Budva, Montenegro, 14-15 May 2019). – Budva : IEEE, 2019. – P. 1-6.

2. Nowosielski L. Shielding effectiveness required for IT equipment enclosures / L. Nowosielski, J. Michalak // 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL), (Singapore, 19-22 November 2017). – Singapore : IEEE, 2017. – P. pp. 427-431.

3. Tajima K. Effect evaluation of countermeasure method for image information leakage by electromagnetic radiation from ITE / K. Tajima, Y. Suzuki, R. Ishikawa, H. Nobata, Tetsuya T., J. Kato // 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, (Barcelona, Spain, 02-06 September 2019). – Barcelona : IEEE, 2019. – P. 394-397.

4. Wu Y. Secure beamforming for cognitive radio networks with artificial noise / Y. Wu, X. Chen, X. Chen // 2015 International Conference on Wireless Communications & Signal Processing (WCSP), (Nanjing, China, 15-17 October 2015). – Nanjing : IEEE, 2015. – P. 1-5.

5. Seitkulov Y. Rationale for the method of formation of the combined speech masking signals / Y. Seitkulov, S. Boranbayev, B. Yergaliyeva, G. Davydov, A. Patapoviche // 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), (Astana, Kazakhstan, 15-17 October 2014). – Astana : IEEE, 2014. – P. 1-4.

6. Lukova-Chuiko N. The Method Detection of Radio Signals by Estimating the Parameters Signals of Eversible Gaussian Propagation / N. Lukova-Chuiko, O. Herasymenko, S. Toliupa, S. Laptiev, T. Laptieva, O. Laptiev // 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), (Kyiv, Ukraine, 15-17 December 2021). – Kyiv : IEEE, 2021. – P. 67-70.

7. Wu Y. The Noise-like Disguised Scheme for Physical Layer Security Using Phase Rotation And Wavelet Transform / Y. Wu, C. Chen // 2018 5th International Conference on Systems and Informatics (ICSAI), (Nanjing, China, 10-12 November 2018). – Nanjing : IEEE, 2018. – P. 823-827.

8. Jingsai J. Adaptive acoustic masking based on spectral envelope / Jiang Jingsai, Li Ye, Zhang Peng, Hao Qiuyun, Ma Xiaofeng, Fan Yanhong // 2016 International Conference on Audio, Language and Image Processing (ICALIP), (Shanghai, China, 11-12 July 2016). – Shanghai : IEEE, 2016. – P. 442-446.

9. Siahaeva O.O Doslidzhennia ta rozrobka matematychnoi modeli dzherela nebezpechnoho syhnalu vtraty informatsii v bankivskykh systemakh : mahisterska atestatsiina robota : 8.05090202 – Avtomatyzovani kompleksy radioelektronnykh vyrobnytstv / O. O. Siahaeva ; KhNURE. – Kharkiv, 2012. – 90 s.

10. Boiko J.M. Teoretychni aspekty pidvyshchennia zavadostiikosti y efektyvnosti obrobky syhnaliv v radiotekhnichnykh prystroiakh ta zasobakh telekomunikatsiinykh system za naiavnosti zavad: monohrafiia / J. M. Boiko, V. A. Druzhynin, S. V. Toliupa. - Kyiv: Lohos, 2018. - 227 s.

11. Boiko J. SAML: definition and principles of operation through a VPN tunnel in secure information networks/ J. Boiko, B. Biliavets//Measuring and computing devices in technological processes. – 2022 - № 4. - P. 41–48.

12. Boiko J. Features of code redundancy formation in information transmission channels / J. Boiko, A. Semenko, I. Pyatin // Infocommunication and computer technologies. – 2022 - T.2, №04. - P. 12-25.

13. Boiko J., Pyatin I., Eromenko O., Stepanov M. Method of the adaptive decoding of self-orthogonal codes in telecommunication //Indonesian Journal of Electrical Engineering and Computer Science (IJEECS). – 2020. – V. 19. – №. 3. – P. 1287-1296.