DOI 10.20535/2411-1031.2020.8.2.222610
УДК 004[056.53+413.4]::511.521

ВІТАЛІЙ БЕЗШТАНЬКО,
ЯРОСЛАВ ЗІНЧЕНКО

ІНТЕРПРЕТАЦІЙНА МОДЕЛЬ ОЦІНЮВАННЯ ГРАНИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Внесення змін до законодавства України дозволяє будувати, впроваджувати та проводити атестації систем захисту інформації, що є власністю держави, або вимоги щодо захисту якої встановлені Законом. При цьому рекомендується використовувати вимоги та/або настанови міжнародних практик, які передбачають використання ризик-орієнтованого підходу. Так, імплементований в Україні міжнародний стандарт ISO/IEC 27001 рекомендує обрати або розробити метод оцінювання ризиків інформаційної безпеки. Разом з тим, за результатами аналізування відкритих джерел встановлено відсутність моделей і методів кількісного оцінювання їх граничних значень. Під інформаційними будемо розуміти ризики, пов'язані з можливістю виникнення втрат в результаті порушення властивостей конфіденційності, цілісності, доступності інформації. Тому метою даної статті є розроблення інтерпретаційної моделі, яка дозволить отримувати граничні значення ризиків інформаційної безпеки. Їхні кількісні значення можливо використовувати в якості критеріїв на етапі формування вимог до комплексної системи захисту інформації та/або системи управління інформаційної безпеки. За основу для розрахунку величини граничного значення ризику взято середньоквадратичне відхилення недоотриманого організацією прибутку за визначений період. Якщо прибуток перевищує запланований, то гіпотетично за період аналізу не було інцидентів, які б впливали на організацію. Оскільки інформаційні ризики є складовою ризиків організації, то відповідно до рекомендацій ISO/IEC 27005. За ним ризик визначається як ефект невизначеності щодо досягнення цілей. У даному випадку ефект – це позитивне чи негативне відхилення від очікуваного результату. Тоді гіпотетично отримане середнє квадратичне значення відхилення можна вважати оцінкою впливу інформаційної невизначеності адитивних інформаційних ресурсів на економічні результати, а отже і оцінкою прийнятного граничного значення інформаційного ризику організації. З огляду на це, запропоновано інтерпретаційну модель оцінювання граничних ризиків інформаційної безпеки та допустимих втрат за окремими складовими загроз порушення властивостей інформації як формалізацію впливу інформаційної невизначеності на економічні наслідки. Це дозволило кількісно визначати ці оцінки на підставі наявних фактичних економічних/вартісних показників функціонування організації.

Ключові слова: аналіз ризиків, оцінка ризиків, інформаційна безпека, граничні значення ризиків, інтерпретаційна модель.

Постановка проблеми. Відповідно до [1] були внесені зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" [2]. Вони дозволятимуть будувати та впроваджувати в організації як комплексні системи захисту інформації (КСЗІ), так і системи управління інформаційної безпеки (СУІБ), а також оцінювати та підтверджувати захищеність інформації. Слід зазначити, що побудова КСЗІ та СУІБ проводиться за результатами оцінювання ризиків інформаційної безпеки [3], [4]. Прийняття зазначених змін до Закону [2] стимулює використання рекомендацій кращих міжнародних практик оцінювання ризиків, що, у свою чергу, підвищує ефективність заходів та засобів забезпечення безпеки відповідно до фактичних економічно-вартісних показників функціонування організації.

Аналіз останніх досліджень і публікацій. Кращі практики аналізу ризиків викладено в [4] - [8]. Варто наголосити, що оцінювання ризику організації як приватної, так і державної форми власності, є одним з головних завдань управління ризиками. При такому оцінюванні, за можливості, ідентифікуються всі вірогідні ризики організації, їх кількісні або якісні характеристики та граничні значення. Враховуючи визначення, викладене в [9], під граничним значенням ризику слід розуміти обґрунтоване значення величини втрат, з яким керівництво організації готове погодитися і діяти в умовах його існування.

Однією із складових ризиків організації є інформаційні ризики. Інформаційними можна назвати ризики, пов'язані з можливістю виникнення втрат в результаті порушення властивостей конфіденційності, цілісності, доступності інформації [10]. Питання про те, який ризик слід вважати прийнятним для інформації, є одними з найскладніших і важливих в практиці побудови КСЗЗІ та/або СУІБ. Рішення про прийнятність ризику приймають, як правило, керівник або відповідальний за інформаційну безпеку організації спираючись на свої знання, досвід, а часом і інтуїцію, що не завжди дозволяє отримати правильний результат. Стратегічні плани організації розробляються з розрахунку на деякі фіксовані умови або на їх більш-менш передбачуваний планомірний розвиток. На практиці внаслідок впливу на організацію загроз такі плани часто порушуються, особливо в довгостроковій перспективі. В організації завжди існує ймовірність недосягнення поставленої мети і запланованого стратегічного результату, що обумовлено недостатністю одержуваної інформації про існуючі загрози інформаційній безпеці та статистиками їх реалізації. Розбіжність отриманого результату з запланованим, тобто втрати, визначаються як ризик.

Метою роботи є розробка інтерпретаційної моделі оцінювання граничних значень ризиків інформаційної безпеки організації та допустимих втрат за окремими складовими загроз властивостям інформації (конфіденційності, цілісності, доступності), кількісні значення яких можна було б використовувати в якості критеріїв на етапі формування вимог до КСЗІ та/або СУІБ.

Виклад основного матеріалу дослідження. Для визначення оцінок граничного інформаційного ризику $R_{гр}$ пропонується застосовувати наступний підхід. Припустимо, що недоотриманий організацією дохід $P_{план.}$, тобто збиток G, можна взяти за основу для розрахунку величини граничного значення ризику $R_{гр}$ [11] - [13].

Нехай організація за певний часовий інтервал (місяць, рік) планувала отримати значення прибутку $P_{план.i}$, де i – номер часового періоду, що розглядається, $i \in (1, m)$; m – кількість розглянутих періодів часу. Реально за прийнятий для розрахунку період було отримано прибуток $P_{отр.i}$. Гіпотетично різниця між реальним значенням і прибутком, що прогнозується, є збитком організації G_i, тобто адитивним значенням інформаційних ризиків організації за прийнятий для розрахунку період.

Якщо прибуток організації перевищує запланований, то можна припустити, що інцидентів, які впливали на конфіденційність, цілісність, доступність інформації за період аналізу, не було. Якщо ж інциденти порушення властивостей інформації внаслідок яких організація зазнала збитків мали місце, то збиток G_i описується виразом:

$$G_i = P_{план.i} - P_{отр.i}.$$

Зазначимо, що аналогічні міркування застосовуються не тільки для організацій діяльність яких направлена на отримання прибутку, а й для неприбуткових. Для таких організацій слід оперувати значеннями оцінки планованих фінансових затрат і отриманого збитку G_i за часовий інтервал, що аналізувався.

За всіма часовими інтервалами, що аналізувались, та отриманими відхиленнями від запланованого організацією прибутку обчислюється середнє значення

$$G_{сер} = \frac{\sum_{i=1}^{m} G_i}{m}.$$

Окрім середнього значення $G_{сер}$ використовується показник їхнього розсіювання – середньоквадратичне відхилення σ [14]. Воно показує наскільки значення випадкової величини розсіяні (розкидані) відносно її математичного сподівання, тобто використовується для оцінювання відхилення випадкової величини відносно центру розподілу

$$\sigma = \sqrt{\frac{\sum_{i=1}^{m} (G_i - G_{ср})^2}{m-1}}. \quad (1)$$

У разі використання рекомендацій [5] ризик визначається як ефект невизначеності щодо досягнення цілей, а ефект – позитивне чи негативне відхилення від очікуваного. Гіпотетично отримане значення середнє квадратичного відхилення σ можна вважати оцінюванням впливу інформаційної невизначеності адитивних інформаційних ризиків на економічні результати діяльності організацій. Отже, й оцінкою граничного значення інформаційного ризику $R_{гр}$. Її аналітичний опис матиме такий вигляд

$$R_{гр} = \sigma. \quad (2)$$

Викладене розглянемо на прикладі. Нехай організація за чотири роки успішної діяльності оцінюється характеристиками за табл. 1.

Таблиця 1 – Характеристики діяльності організації

Розглядуваний період часу m, років	2017	2018	2019	2020
Запланований прибуток, $P_{план.i}$, тис. грн.	200	210	215	220
Отриманий прибуток $P_{отр.i}$, тис. грн.	180	195	210	210
Збиток G_i, тис. грн.	20	15	5	10

За всіма періодами часу, а також за відомим відхиленням знайдемо середнє значення збитку $G_{ср}$ у тис. грн

$$G_{ср} = \frac{\sum_{i=1}^{4} G_i}{4} = \frac{G_1 + G_2 + G_3 + G_4}{4} = \frac{20+15+5+10}{4} = 12,5.$$

Відповідно до (1) визначається середнє квадратичне відхилення σ:

$$\sigma = \sqrt{\frac{(20-12,5)^2 + (15-12,5)^2 + (20-12,5)^2 + (10-12,5)^2}{4-1}} = 6,45.$$

Якщо розглядати інформаційні ризики організації, наприклад, порушення властивостей розміщеної на веб сайті організації інформації r_1, витік інформації в результаті допущення помилки персоналом r_2 та інші r_k, то їх адитивне значення не повинне перевищувати $R_{гр}$.

Тоді

$$r_1 + r_2 + ... + r_k \le R_{гр}. \quad (3)$$

З урахуванням (2) і (3) для даного прикладу рекомендується вибрати значення граничного ризику

$$R_{гр} \le 6,45. \quad (4)$$

Умовами (3) та (4) визначаються множина наборів граничних значень ризиків інформаційної безпеки, якими забезпечується неперевищення заданого рівня адитивного ризику $R_{гр}$ інформаційної безпеки організації. Загалом, цим формується інтерпретаційна модель оцінювання граничних ризиків інформаційної безпеки організації.

Якщо керуватись визначенням, викладеним у [4], то для окремого ризику інформаційної безпеки буде правильним твердження, що це такий стан інформації про окремий ресурс організації, в якому вона знаходиться під впливом джерел загроз. Тоді ризик інформаційної безпеки окремого ресурсу організації r_k, записаний аналітично, матиме вигляд

$$a_k p_k = r_k, \tag{5}$$

де a_k – величина витрат для відновлення окремого інформаційного ресурсу внаслідок впливу загрози;

p_k – імовірність реалізації загрози.

Оскільки загрози безпеці інформації направленні на порушення її властивостей конфіденційності, цілісності та доступності, то вплив загроз на інформацію призводить до часткової або повної втрати однієї з її властивостей. Варто зазначити, що в переважній більшості випадків джерела загроз впливають на властивості інформації незалежно один від одного. Тоді співвідношення (5) можна записати так:

$$a_к p_к + a_ц p_ц + a_д p_д = r_k, \tag{6}$$

де $p_к, p_ц, p_д$ – імовірності реалізації загроз конфіденційності, цілісності та доступності інформації.

Якщо для загрози, що розглядається стосовно властивостей інформації, існують доступні статистики ймовірностей виникнення втрат, то цей стан впливу можна віднести до категорії реальних загроз. Відповідно, загрозу, для якої не існує або така статистика є недоступною, можна відносити до категорії загроз, які можуть або мають з'явитися за певних умов, але її в реальності не існує. Отже, можна зробити висновок про те, що загрози, які реально не існують, можна виключити з розгляду при оцінюванні ризиків інформаційної безпеки окремих ресурсів. Для існуючих загроз статистика значень імовірності виникнення втрат зібрана й існує. Загрози, статистики за якими немає, можуть бути віднесені до категорій рідкісних або малозначущих.

Для результативної реалізації сценарію розвитку загрози необхідний збіг (резонанс) в часі і просторі активної фази життєвого циклу загрози і відповідної фази життєвого циклу інформації [15]. Тому можна припустити, що в певний момент часу на інформацію впливає лише одна загроза. Враховуючи (5) і (6) для інформаційних ризиків організації буде справедливою така нерівність

$$a_1 p_1 + a_2 p_2 + ... + a_k p_k + ... + a_n \cdot p_n \le R_{гр}, \tag{7}$$

де $k \in (1, n)$.

Для зручності умову (7) можна записати у вигляді рівняння

$$a_1 p_1 + a_2 p_2 + ... + a_k p_k + ... + a_n \cdot p_n = R_{гр}, \tag{8}$$

Рівністю (8) задається множина граничних ризиків інформаційної безпеки ресурсів організації, яку можна інтерпретувати як математичну модель визначення граничних оцінок інформаційних ризиків. У випадку "глибокої" деталізації моделі рівність (8) в лівій частині може містити n змінних, кількість яких може досягати декількох тисяч.

На практиці оцінювання витрат для відновлення інформаційного ресурсу внаслідок впливу загрози a_k здійснює власник та/або розпорядник такого ресурсу. При цьому кваліфікований спеціаліст, як правило, здійснює оцінювання з прийнятою керівництвом організації похибкою. Оцінювання імовірності p_k також відбувається на підставі висновків експертів. Однак, застосування експертних оцінок обмежене складністю накопичення статистик великого обсягу, оскільки будь-який негативний прояв ризику в сфері інформаційної безпеки вимагає негайного оброблення для запобігання його прояву у майбутньому. Це призводить до невиконання умов стаціонарності спостережень і, як

наслідок, до складності визначення імовірності виникнення граничних ризиків інформаційної безпеки організації і отримання кінцевого числа оцінок імовірностей виникнення втрат, які можуть задаватися як проектні вимоги при створенні КСЗІ та/або СУІБ.

Отже, виконання умов (3), (7) зводиться до пошуку значень імовірностей p_k. При цьому очевидно, що в загальному випадку множина рішень (8) є нескінченно-незліченною. Як наслідок, пошук наборів імовірностей граничних втрат за (8) без додаткових відомостей/обмежень є складним завданням. Тобто, модель (8) потребує трансформації до представлення з кінцевим набором рішень.

Висновки. Запропоновано інтерпретаційну модель оцінювання граничних ризиків інформаційної безпеки та допустимих втрат за окремими складовими загроз порушення властивостей інформації (конфіденційності, цілісності, доступності). Для цього формалізовано вплив інформаційної невизначеності на економічні наслідки, що дозволило кількісно визначати ці оцінки на підставі наявних, фактичних економічних/вартісних показників функціонування організації. Отримані результати можна використовувати в якості проектних вимог (критеріїв) на етапі формування вимог до КСЗІ та/або СУІБ. Цим сформовано теоретичні передумови для пошуку наборів імовірностей граничних ризиків інформаційної безпеки організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Верховна Рада України. 3 сесія. (2020, Черв. 04). *Закон № 681-IX, Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/681-20#Text. Дата звернення: Верес. 03, 2020.

[2] Верховна Рада України. I скликання. (1994, Лип. 05). *Закон № 80/94-ВР, Про захист інформації в інформаційно-телекомунікаційних системах*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80# Text. Дата звернення: Верес. 03, 2020.

[3] International organization for standardization. (2013, Sept. 25). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ru/standard/54534.html. Accessed on: Sept. 03, 2020.

[4] International organization for standardization. (2018, Jul. 09). *ISO/IEC 27005, Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/ru/standard/75281.html?browse=tc. Accessed on: Sept. 03, 2020.

[5] National Institute of Standards and Technology. (2012, Sept. 18). *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.* [Online]. Available: https://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/sp800-30.pdf. Accessed on: Sept. 03, 2020.

[6] International organization for standardization. (2018, Feb. 14). *ISO 31000. Risk management. Guidelines.* [Online]. Available: https://www.iso.org/ru/standard/65694.html. Accessed on: Sept. 03, 2020.

[7] International Electrotechnical Commission. (2019, Jun. 17). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/72140.html. Accessed on: Sept. 03, 2020.

[8] Bundestag Standard Institute. (2018, May 07). *BSI Standard 200-3: Risk Analysis based on IT-Grundschutz, Version 1.0.* [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2. Accessed on: Sept. 03, 2020.

[9] В. В. Мохор, и А. М. Богданов, “Постатейная интерпретация ISO GUIDE 73:2009 Risk management. Vocabulary”, *Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України,* вип. 59, с. 173-199, 2011.

[10] В. В. Мохор, и А. М. Богданов, “Изложения стандарта ISO 31000 Risk Management. Principles and Guidelines на русском языке”, *Das Management,* № 3, с. 5-18, 2011.

[11] В. И. Завгородний, “Парадигма информационных рисков” [Электронный ресурс]. Доступно: http://www.fa-kit.ru/main_dsp.php?top_id=591. Дата обращения: Сент.. 03, 2020.

[12] А. А. Иванов, С. Я. Олейников, и С. А. Бочаров, *Риск-менеджмент*. Москва, Россия: Изд. центр ЕАОИ, 2008.

[13] Е. Д. Соложенцев, *Сценарное логико-вероятносное управление риском в бизнесе и технике.* СПб, Россия: Издательский дом “Бизнес-пресса”, 2006.

[14] П. І. Бідюк, Б. П. Ткач, та Т. Харрінгон, *Математична статистика*. Київ, Україна: ДП “Вид. дім ”Персонал”, 2018.

[15] В. В. Мохор, А. М. Богданов, О. Н. Крук, и В. В. Цуркан, “Построение оценок рисков безопасности информации на основе динамического множества актуальных угроз”, *Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України,* вип. 56, с. 87-99, 2010.

Стаття надійшла до редакції 18.09.2020.

REFERENCE

[1] Verkhovna Rada of Ukraine, 3st Session. (2020, Jun. 04). *Law № 681-IX, On amendments to the Law of Ukraine “On information protection in information and telecommunication systems” to confirm the compliance of the information system with the requirements for information protection.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/681-20#Text. Accessed on: Sept. 03, 2020.

[2] Verkhovna Rada of Ukraine, I Convocation. (1994, Jul. 05). *Law № 80/94-VR, On information protection in information and telecommunication systems*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. Accessed on: Sept. 03, 2020.

[3] International organization for standardization. (2013, Sept. 25). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ru/standard/54534.html. Accessed on: Sept. 03, 2020.

[4] International organization for standardization. (2018, Jul. 09). *ISO/IEC 27005, Information technology. Security techniques. Information security risk management*. [Online]. Available: https://www.iso.org/ru/standard/75281.html?browse=tc. Accessed on: Sept. 03, 2020.

[5] National Institute of Standards and Technology. (2012, Sept. 18). *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.* [Online]. Available: https://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/sp800-30.pdf. Accessed on: Sept. 03, 2020.

[6] International organization for standardization. (2018, Feb. 14). *ISO 31000. Risk management. Guidelines.* [Online]. Available: https://www.iso.org/ru/standard/65694.html. Accessed on: Sept. 03, 2020.

[7] International Electrotechnical Commission. (2019, Jun. 17). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/72140.html. Accessed on: Sept. 03, 2020.

[8] Bundestag Standard Institute. (2018, May 07). *BSI Standard 200-3: Risk Analysis based on IT-Grundschutz, Version 1.0.* [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2. Accessed on: Sept. 03, 2020.

[9] V. V. Mokhor, and A. M. Bogdanov, "Interpretation ISO GUIDE 73:2009 Risk management – Vocabulary", *Collection of scientific works of the Institute of modeling problems in energy named after G.E. Pukhov* of National Academy Sciences of Ukraine, iss. 59, pp. 173-199, 2011.

[10] V. V. Mokhor, and A. M. Bogdanov, "Presentation of standard ISO 31000 Risk Management. Principles and Guidelines in Russian", *Das Management*, iss. 3, pp. 5-18, 2011.

[11] V. I. Zavgorodniy, "Information risk paradigm". [Online]. Available: https://studfile.net/preview/5366710. Accessed on: Sept. 03, 2020.

[12] A. A. Ivanov, S. Y. Oleynikov, and S. A. Bocharov, *Risk management.* Moscow, Russia: Izd. zentr EAOI, 2008.

[13] E. D. Sologentsev, *Scenario-based probabilistic risk management in business and technology.* Sankt-Peterburg, Russia: Izdatelskiy dom "Biznes-pressa", 2006.

[14] P. I. Biduyk, B. P. Tkach, and T. Harringon, *Mathematical statistics.* Kyiv, Ukraine: DP "Vid. dim "Personal", 2018.

[15] V. V. Mokhor, A. M. Bohdanov, O. N. Kruk, and V. V. Tsurkan, "Building a risk assessment of information security based on dynamic set of actual threats", *Collection of scientific works of the Institute of modelling problems in energy named after G.E. Pukhov* of National Academy Sciences of Ukraine, iss. 56, pp. 87-99, 2010.

VITALII BEZSHTANKO,
YAROSLAV ZINCHENKO

INTERPRETATION MODEL OF ASSESSMENTS BOUNDARY INFORMATION SECURITY RISKS

Amendments to the legislation of Ukraine allow building, implementing, and conducting certifications of information protection systems owned by the state, or the requirements for the protection of which are established by law. It is recommended to use the requirements and/or guidelines of international practices that provide for the use of a risk-oriented approach. Thus, the international standard ISO/IES 27001 implemented in Ukraine recommends choosing or developing a method for assessing information security risks. At the same time, the results of the analysis of open sources revealed the absence of models and methods for quantifying their limit values. By informational, we mean the risks associated with the possibility of losses as a result due to violations of the properties of confidentiality, integrity, availability of information. Therefore, the purpose of this article is to develop an interpretive model that will provide the limit values of information security risks. Their quantitative values could be used as criteria at the stage of formation requirements for a comprehensive information security system and / or information security management system. The basis for calculating the value of the risk limit value is the standard deviation of the uncollected profit for the period. If the profit exceeds the planned, then hypothetically during the analysis period there were no incidents that would affect resources. Information risks are a component of the organization's risks. According to the recommendations of ISO/IES 27005, where risk is the effect of uncertainty on the achievement of goals, and the effect is a positive or negative deviation from the expected, the hypothetically obtained standard deviation can be considered an assessment of the impact of information uncertainty of additive information resources on economic results. In addition, assessing the acceptable threshold of information risk of the organization. Thus, an interpretive model for estimating the marginal risks of information

security and allowable losses on individual components of threats to the information properties as a formalization of the impact of information uncertainty on financial consequences. This made it possible to quantify these estimates based on available actual economic / cost indicators of information activity in the organization.

Keywords: risk analysis, risk assessment, information security, risk limits, interpretive model.

Безштанько Віталій Михайлович, кандидат технічних наук, науковий співробітник науково-дослідної спеціальної лабораторії № 1 науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-7998-246X.

E-mail: v.bezshtanko@gmail.com.

Зінченко Ярослав Вікторович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідної спеціальної лабораторії № 1 науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-9574-3947.

E-mail: wmed75@ukr.net.

Bezshtanko Vitalii, candidate of technical sciences, researcher of research special laboratory № 1 at the research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Zinchenko Yaroslav, candidate of technical sciences, senior researcher, head of research special research laboratory № 1 at the research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.