УДК 004.056.5
DOI https://doi.org/10.32782/2521-6643-2023.1-65.9

Тарасенко Ю. С., кандидат фізико-математичних наук,
доцент, доцент кафедри кібербезпеки
та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-4226-5707

Савченко Ю. В., кандидат технічних наук,
доцент кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-7177-6311

РИЗИК-ОРІЄНТОВАНІ ПРОЦЕСИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті представлено огляд досліджень, присвячених ухваленню рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури. В умовах підвищеної інтенсивності регіонально-галузевих інформаційних війн, їхнього неухильного розширення і впливу, насамперед на значущі сфери сучасного соціуму, дедалі гостріше набуває тенденція несумлінного протиборства новітніх інформаційних технологій, які доходять до кібершпигунства, кіберзлочинності та кібертероризму з використанням інформаційної зброї, які спрямовані на злом безпеки існуючих об'єктів критичної інфраструктури. Сенс інформаційної безпеки полягає в неможливості нанесення шкоди штатному функціонуванню та властивостей цих об'єктів або їх структурним складовим. Побудована структурно-лінгвістична схеми підтримки ухвалення рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури. Як оціночний позитивний приклад доказово викладено конкретний метод реалізації фізичної безпеки сукупності об'єктів критичної інфраструктури. Виконано аналіз методологічної побудови структурно-лінгвістичної схеми вибору засобів захисту сукупності об'єктів критичної інфраструктури з позиції зниження ризику. Показано, що вона має універсальну структуру та фактично може бути використана в будь-якій організованій сфері діяльності соціуму незалежно від виду галузі, розмірів організації, виділених матеріальних засобів та інтелектуального рівня штатного персоналу, відповідального за дану сферу безпеки та захисту. Обґрунтовано частина структурно-лінгвістичної схеми з позицій риск- орієнтованих процесів забезпечення безпеки об'єктів критичної інфраструктури, в якої відображені: організаційні та фізичні засоби захисту загального застосування; специфічні засоби захисту інформаційної системи; засоби захисту відповідно до проблем (від утрат конфіденційності; цілісності; доступності; спостережності; автентичності та надійності) та загроз у межах забезпечення їх безпеки.

На прикладі виявлення несанкціонованих повітряних атак зловмисників, які використовують дрони, продемонстровано доцільність і можливість виявлення потенційної атаки порушником або зловмисником, які застосовують дрони, використовуючи радіофізичні системи як засоби вимірювання навколишнього середовища у вигляді схемотехнічної реалізації кореляційних радіолокаційних пристроїв ближньої взаємодії, які використовують шумоподібний безперервний надвисокочастотний зондувальний сигнал з амплітудною модуляцією. При цьому показано, що оптимальність вибору зондувального сигналу, з одного боку, залежить від результату апріорного аналізу сигнальної функції конкретної зондувальної пачки та відповідного їй об'ємного тіла невизначеності, а з іншого боку, – забезпечує прихованість самого процесу виявлення дронів з високою роздільною здатністю безпосередньо за двома параметрами – його дальністю та швидкістю.

Ключові слова: *ризик, об'єкт критичної інфраструктури, структурно-лінгвістична схема, безпека, радіолокаційні пристрої ближньої взаємодії.*

Tarasenko Yu. S., Savchenko Iu. V. Risk-based processes for ensuring the security of critical infrastructure facilities

The article presents a review of research on decision-making from the perspective of risk-information security of a set of critical infrastructure facilities. In the context of increased intensity of regional and sectoral information wars, their steady expansion and impact, primarily on significant areas of modern society, the trend of unscrupulous confrontation of the latest information technologies, which reach cyber espionage, cybercrime and cyberterrorism with the use of information weapons aimed at breaking the security of existing critical infrastructure facilities, is becoming increasingly acute. The meaning of information security is the impossibility of harming the normal functioning and properties of these objects or their structural components. The article builds a structural and linguistic scheme for supporting decision-making from the standpoint of risk-information security of a set of critical infrastructure facilities. As an evaluative positive example, a specific method of implementing the physical security of a set of critical infrastructure facilities is evidently presented. The author analyses the methodological construction of the structural and linguistic scheme for selecting means of protection of a set of critical infrastructure facilities from the perspective of risk reduction. It is shown that it has a universal structure and can actually be used in any organised sphere of society, regardless of the type of industry, size of the organisation, allocated material resources and intellectual level of the staff responsible for this area of security and protection. The author substantiates a part of the structural and linguistic scheme from the standpoint of risk-oriented processes of ensuring the security of critical infrastructure facilities, which reflects: organisational and physical means of protection of general application; specific means of protection of an information system;

means of protection in accordance with the problems (against loss of confidentiality, integrity, availability, observability, authenticity and reliability) and threats within the framework of ensuring their security.

Using the example of detecting unauthorised aerial attacks by intruders using drones, the article demonstrates the feasibility and possibility of detecting a potential attack by an intruder or intruder using drones using radio physical systems as environmental measurement tools in the form of a circuitry implementation of correlation radar devices of close interaction using a noise-like continuous ultra-high frequency sensing signal with amplitude modulation. It is shown that the optimal choice of the sensing signal, on the one hand, depends on the result of an a priori analysis of the signal function of a particular sensing bundle and its corresponding uncertainty volume, and on the other hand, ensures the concealment of the process of detecting high-resolution drones directly by two parameters – its range and speed.

Key words: *risk, critical infrastructure facility, structural and linguistic scheme, security, short-range radar devices.*

Вступ і постановка проблеми. В умовах підвищеної інтенсивності регіонально-галузевих інформаційних війн, їхнього неухильного розширення і впливу, насамперед на значущі сфери сучасного соціуму, дедалі гостріше набуває тенденція несумлінного протиборства новітніх інформаційних технологій, які доходять до кібершпигунства, кіберзлочинності та кібертероризму з використанням інформаційної зброї, які спрямовані на злом безпеки існуючих об'єктів критичної інфраструктури (ОКІ). Сенс інформаційної безпеки полягає в неможливості нанесення шкоди штатному функціонуванню та властивостей цих об'єктів або їх структурним складовим [1]. На державному (і не тільки) рівні вимушені створювати системи кібербезпеки, цілеспрямовані дії яких пов'язані з кіберзахистом, – сукупністю «організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [2, Стаття 1, п. 7.]. Фактично реалізується оціночний процес як за змістом (у різних галузях життєдіяльності соціуму), так і за призначенням (наприклад, у вигляді розроблення проектів, технологій, продукції тощо) з позицій забезпечення ідентифікації ризику, аналізу ризику та порівняльної його (ризику) оцінки [3. п. 6.4].

У зв'язку з викладеним поставлено завдання методологічної побудови структурно-лінгвістичної схеми (СЛС) підтримки ухвалення рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури (СОКІ). Як оціночний позитивний приклад доказово викладено конкретний метод реалізації фізичної безпеки СОКІ.

Аналіз останніх досліджень і публікацій. Згідно з [4,5], системи захисту та безпеки ОКІ завжди функціонують у царині ймовірнісних подій, що піддаються принципу невизначеності щодо ризику [6, п. 3.7.9–11]: впливу невизначеності ефективності, результативності, процесу вимірювання та інших. Отже, будь-який вплив з позиції зниження ризику [7, поз. 3.7]) вимагає чіткого уявлення про предмет дослідження та сферу його подальшого застосування. Фактично такий ризик-орієнтований вплив (РОВ) – це процес циклічних вимірювань з уточнення заключної оцінки впливу конкретної реалізації ризику на об'єкт його (ризику) впливу. При цьому, в умовах підвищених зобов'язань до надійності і безпеки засобів вимірювання (ЗВ), в умовах невизначеності вимірювань [8], вимоги забезпечення метрологічної достовірності вимірювань, також є актуальними в галузі будь-яких засобів вимірювання [9]. У підсумку отримуємо, що такий багатопрофільний процес впливів необхідно розглядати з позицій невизначеностей і мінливості як самих результатів, так і їхніх імовірностей, де поняття «погрішності результату вимірювань» зобов'язане корелювати з поняттям істинного значення, чого принципово неможливо досягти.

Результати дослідження. Викладене вище дає змогу використовувати «ризик-орієнтоване мислення» (РОМ) [10, п. 0.3.3], що, підтримуючи концепцію управління ризиками, здатне забезпечувати планування і впровадження будь-якої діяльності з управління та контролю ризиків, що впливають на штатну працездатність ОКІ з позиції ризик-інформаційної безпеки. При цьому, залежно від внутрішніх і зовнішніх чинників ризику та відповідно до поставлених цілей слід обирати як відповідну політику менеджменту ризику, так і конкретні принципи, необхідні для ефективного впровадження його менеджменту з позиції ризик-орієнтованих процесів забезпечення безпеки ОКІ.

Саме з цих позицій планування та впровадження заходів і методів, що використовуються для управління та контролю супутніх ризиків, які впливають на досягнення запланованих цілей безпеки [10], запропоновано до реалізації підсистема підтримки прийняття рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури (СОКІ) у межах ISO/IEC TR 13335-4:2000, IDT. Структурно логічну схему (СЛС) зазначеної Підсистеми наведено на рис. 1 у рамках загальної Схеми методології побудови розширеної системи захисту та безпеки ОКІ [4; 5], де її (підсистеми) працездатність забезпечується за рахунок «Радіофізичних та/або кіберфізичних систем», використовуючи «Систему управління та зв'язку». З їхньою допомогою, спираючись на РЗМ, можна реалізовувати безпосередню оцінку вибору як за методами забезпечення власної безпеки, так і за способами їхнього здійснення, передусім стосовно конфіденційності, цілісності, повноти та доступності використовуваної (одержуваної) інформації. Причому методологію її побудови виконано відповідно до законодавства країни щодо менеджменту ризику, що використовує зворотні зв'язки під час реалізації коригувальних впливів, адекватних вище озвученим аспектам. Саме з цих позицій аналізу безпеки СОКІ в табл. 1 наведено впорядковані дані щодо вибору апріорних засобів захисту в межах ISO/IEC TR 13335-4:2000, IDT, включно з безпекою супутніх інформаційних технологій.

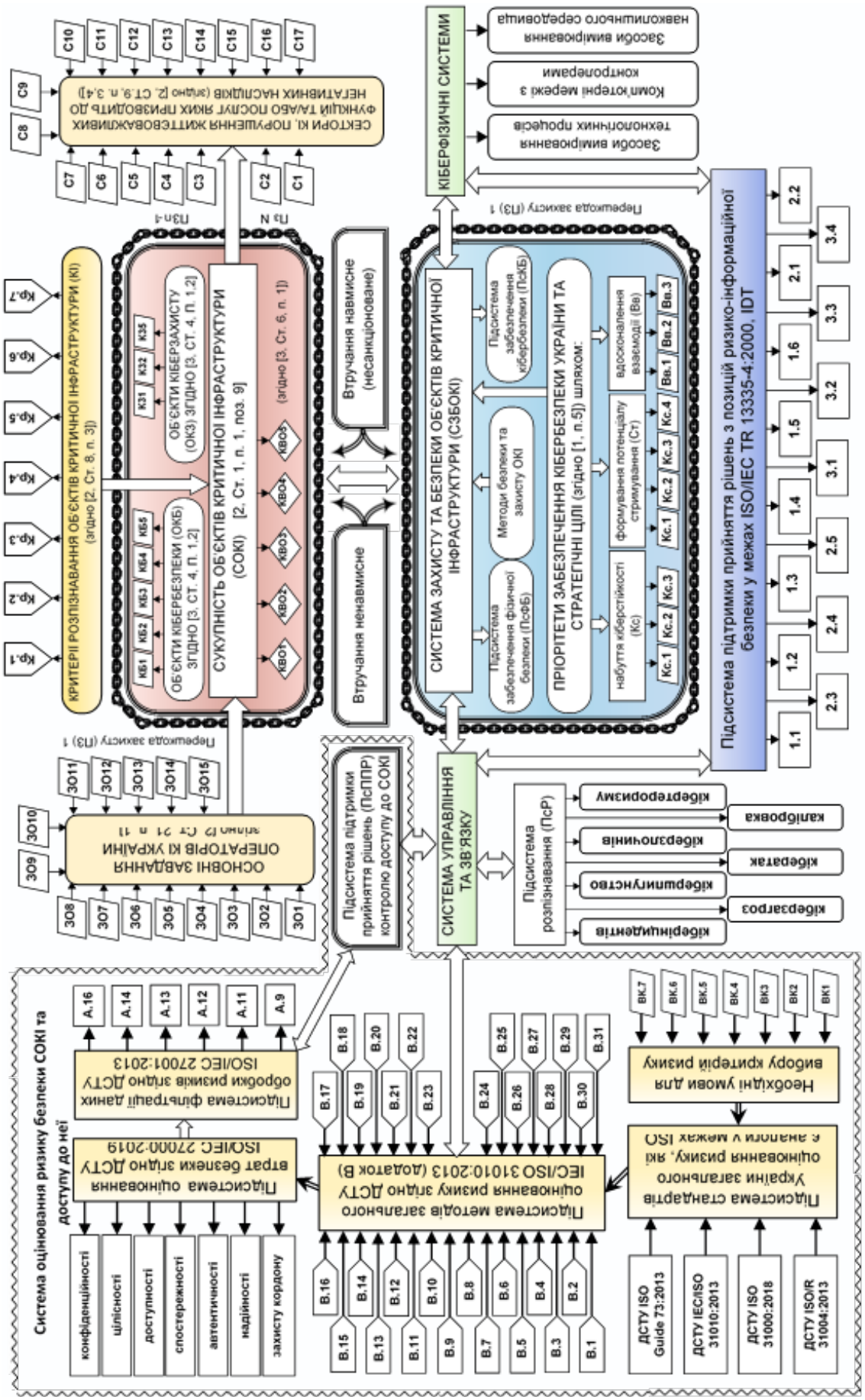

Рис. 1. Схема методології побудови розширеної системи захисту та безпеки об'єктів критичної інфраструктури

У зазначеній таблиці відображено: організаційні та фізичні засоби захисту загального застосування; специфічні засоби захисту інформаційної системи; засоби захисту відповідно до проблем (від втрат конфіденційності; цілісності; доступності; спостережності; автентичності та надійності) і загроз у межах забезпечення безпеки ОКІ. Причому, в контексті загального організаційного управління зазначимо, що концепціям безпеки (інформаційної, виробничої, технологічної тощо аж до захисту приватного життя) притаманна тенденція досконалості, а отже безперервний процес захисту та безпеки в усіх сферах життєдіяльності соціуму завжди супроводжуватиме модернізаційні тенденції на міжнародному і вітчизняному законодавчому рівні стосовно удосконалення стандартів щодо їхньої безпеки. Отже, підвищення рівня захисту СОКІ, оцінювання втрат безпеки (згідно з гіпотетичними кіберінцидентами, що мають імовірнісний характер), – це динамічний процес залучення ресурсів (методів, способів та алгоритмів) мультисервісної мережі зв'язку (криптографічних, канальних та інших) з її фільтруючими (у вигляді, наприклад, авто- та взаємо-кореляційних блоків) пристроями, реалізованими під конкретні вимоги (завдання) користувачів. Звідси, – вибір рівнів спрацьовування кінцевих порогових блоків носитиме багатопрофільний характер і залежатиме від задекларованих імовірностей правильного виявлення або пропуску кібератак чи кіберзагроз.

Таблиця 1

Позначення	**Зміст вибору засобів захисту, з позицій риск-інформаційної безпеки у межах ISO/IEC TR 13335-4:2000, IDT**
1	2
1. Організаційні та фізичні засоби захисту загального застосування:	
1.1	Керування інформаційною безпекою та політика безпеки
1.2	Перевіряння узгодженості безпеки
1.3	Реагування на порушення
1.4	Персонал та питання експлуатації
1.5	Планування неперервності бізнесу
1.6	Фізична безпека
2. Специфічні засоби захисту інформаційної системи:	
2.1	Ідентифікація та автентифікація (I&A)
2.2	Контролювання логічного доступу та аудит
2.3	Захист від зловмисного коду
2.4	Керування мережею
2.5	Криптографія
3. Засоби захисту відповідно до проблем (утрат конфіденційності; цілісності; доступності; спостережності; автентичності та надійності) **та загроз** у межах забезпечення безпеки ОКІ	
3.1 Засоби конфіденційності з позиції:	
	3.1.1. Підслуховування 3.1.2. Електромагнітне випромінення 3.1.3. Зловмисний код 3.1.4. Приховування ідентичності користувача 3.1.5. Неправильне направлення/перенаправлення повідомлень 3.1.6. Збої програмного забезпечення 3.1.7. Крадіжки 3.1.8. Несанкціонований доступ до комп'ютерів, даних, служб та програм 3.1.9. Несанкціонований доступ до носіїв даних
3.2 Засоби контролю цілісності з позиції:	
	3.2.1. Псування носіїв даних 3.2.2. Помилки обслуговування 3.2.3. Зловмисний код 3.2.4. Приховування ідентичності користувача 3.2.5. Неправильне направлення/перенаправлення повідомлень 3.2.6. Неспростовність 3.2.7. Збої програмного забезпечення 3.2..8 Збої постачання (живлення, кондиціонування повітря) 3.2.9. Технічні пошкодження 3.2.10. Помилки передавання 3.2.11. Несанкціонований доступ до комп'ютерів, даних, служб та програм 3.2.12. Використання несанкціонованих програм та даних 3.2.13. Несанкціонований доступ до носіїв даних 3.2.14. Помилки користувача

Закінчення таблиці 1

1	2
3.3. Засоби захисту доступності з позицій протидії:	
	3.3.1. Руйнівний напад 3.3.2. Псування носіїв даних 3.3.3. Збої комунікаційного обладнання та служб 3.3.4. знищені вогнем та (або) водою Вогонь, вода 3.3.5. Помилки обслуговування 3.3.6. Зловмисний код 3.3.7. Приховування особистості користувача 3.3.8. Неправильне направлення/перенаправлення повідомлень 3.3.9. Зловживання ресурсами 3.3.10. Стихійні лиха 3.3.11. Збої програмного забезпечення 3.3.12. Збої постачання (живлення, кондиціонування повітря) 3.3.13. Технічні пошкодження 3.3.14. Крадіжки 3.3.15. Перевантаження каналів 3.3.16. Помилки передавання 3.3.17. Несанкціонований доступ до комп'ютерів, даних, служб та програм 3.3.18. Використання несанкціонованих програм та даних 3.3.19. Несанкціонований доступ до носіїв даних 3.3.20. Помилки користувача
3.4 Засоби захисту з позиції:	
	3.4.1. Спостережність 3.4.2. Автентичність 3.4.3. Надійність

Отже, успішно реалізовані ризик-орієнтовані процеси забезпечення безпеки СОКІ (або її моделі) за умови адекватної оцінки апріорних впливів (наприклад, у вигляді певної моделі порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики) є важливою складовою успішного проведення як політики ризик-менеджменту, так і супутнього зниження ризик невизначеності в процесі аналізу ризиків та визначення вимог до складу та характеристик необхідної інтегральної системи захисту. Проте, навіть в умовах багаторівневої системи перешкод, жодна пізнавальна модель не може одночасно виконувати необхідно безліч завдань захисного напрямку. Саме цьому доцільно оцінювати ефективність безпеки в конкретному (обраному) аспекті її реалізації. Зокрема, до останнього часу не приділялося достатньо серйозної уваги контролю за подоланням повітряних рубежів захисту до підриву конкретної захисної (охоронюваної) оболонки об'єкта. Тому, як приклад з виявленням несанкціонованих повітряних атак зловмисників, які використовують дрони, нижче продемонструємо можливість забезпечення штатного рівня захисту ОКІ шляхом реалізації кореляційних радіолокаційних пристроїв [11, с. 403]. Останні доцільно ототожнювати (віднести) до радіофізичних систем ближньої взаємодії як засобів вимірювання або навколишнього середовища, або технологічних процесів.

При цьому завдання загальної та параметричної ідентифікації розпізнавання потенційних атак за допомогою дослідження гіпотетичної сигнальної аналогової дії зведемо до кореляційного аналізу зондувальних та відбитих сигналів від дронів, які вторглись у повітряну область КВО, що охороняється.

Враховуючи, що найкращого розділення досягають за максимальної відмінності сигналів за параметром розділення, нескладно довести зв'язок між потенційною роздільною здатністю та автокореляційною функцією сигналу. Для цього необхідно застосувати умову, відповідно до якої середній квадрат відхилень двох сигналів, зсунутих за параметром розділення на $\Delta\xi$, повинен бути граничною величиною для всіх $\Delta\xi$ в інтервалі спостережень, крім $\Delta\xi$, близьких до нуля, де сигнали близькі один до одного, тобто

$$\int\left[U\left(\xi\right)-U\left(\xi-\Delta\xi\right)\right]^2 d\xi = max, \tag{1}$$

де ξ – параметр розділення (наприклад, для розділення за дальністю $\xi=t$, $\Delta\xi=\Delta t$).

Очевидно, що для виконання (1) потрібно одержати мінімум виразу

$$\int U\left(\xi\right)\cdot U\left(\xi-\Delta\xi\right)d\xi = min, \tag{2}$$

що являє собою аналог автокореляційної функції вхідного сигналу.

Роздільна здатність буде краща у того сигналу, який за заданого зсуву $\Delta\xi$ має найвужчу автокореляційну функцію, тобто найменше значення на рівні 0,5. Отже, оцінити потенційну роздільну здатність за координатами або швидкостями можна шляхом обчислення автокореляційної функції сигналу на рівні 0,5, причому для кутових координат сигнал має складний просторово-часовий характер [11].

Таким чином, з виразу (2) бачимо, що розділення краще у тих сигналах, автокореляційна функція яких найвужча. При цьому спільне розділення (тобто розділення одночасно за дальністю і швидкістю) цілком залежить від характеру обраного типу зондувального сигналу. Отже, з позицій риск-інформаційної безпеки у межах фізичної безпеки (Табл. 1 п. 1.6) доцільне використання взаємно-кореляційних пристроїв (ВКП). Тобто, для випадку аналогового сигналу на виході ВКП виробляється сигнал, адекватний кореляційній функції. А оскільки високочастотне заповнення радіосигналу, наприклад у радіолокації, звичайно не застосовують для одержання інформації, а піддають аналізу обвідну сигналу $K_0(\tau,\Delta\omega)$, то об'єм, зосереджений під поверхнею, є постійний і не залежить від виду зондувального сигналу. Математичним формулюванням цього положення буде рівняння

$$\int_{\tau}\int_{\Delta\omega} K_0^2\left(\tau,\Delta\omega\right)\mathrm{d}\tau\mathrm{d}\left(\Delta\omega\right)=2\pi, \tag{3}$$

або, оскільки $\Delta\omega=2\pi\Delta f$

$$\int_{\tau}\int_{\Delta\omega} K_0^2\left(\tau,\Delta\omega\right)\mathrm{d}\tau\mathrm{d}\left(\Delta f\right)=1. \tag{4}$$

Співвідношення (3) та (4) називають принципом невизначеності, який встановлює, що незалежно від типу сигналу об'єм, що має назву тіла невизначеності (ТН), залишається незмінним. Але шляхом підбору виду сигналу можна усе ж таки перерозподілити об'єм так, щоб досягти необхідного розділення в будь-якій частині площини $(\tau,\Delta\omega)$. Таким чином, розглядаючи розділення за дальністю або швидкістю, а також спільне розділення за цими параметрами, необхідно визначати нормовану автокореляційну функцію за часом (уважаючи $\Delta\omega = 0$) або за частотою ($\Delta\tau = 0$) або змішану автокореляційну функцію вхідного сигналу й обчислювати її ширину на рівні 0,5. Застосовуючи формули, що визначають дальність цілі через часову затримку сигналу, а швидкість через допплерівській частотний зсув, нескладно оцінити потенційну роздільну здатність за дальністю, швидкістю, а також спільне розділення залежно від характеру обраного типу зондувального сигналу. При цьому СЛС дозволу, розпізнавання і забезпечення приналежності до різних класів кіберінциндентів також доцільно реалізовувати за допомогою кореляційних схемотехнічних рішень. Більш того, усі ці структурно-логічні схеми отримання, доставки, зберігання і безпосереднього захисту задіяної інформації мають бути укомплектовані відповідними функціональними підсистемами підтримки прийняття рішень, що носять характер апріорного порогу спрацьовування, тобто мінімально допустимого рівня, перевищення якого вимагає прийняття усіх заздалегідь передбачених засобів захисту, кількісний і якісних характер яких залежить від можливостей реалізації гіпотетичних кіберінциндентів. Тому, з метою забезпечення фізичного захисту КВО від мобільних, наприклад у вигляді дронів, засобів розвідки, доцільно в даному випадку виявлення ворожої атаки здійснювати шляхом попереднього оптимального вибору зондуючого сигналу з наступною його автокореляційною обробкою прийнятого сигналу (за допомогою ВКУ), аналізуючи їх (сигналів) об'ємне тіло невизначеності (ТН).

Достовірність сказаного продемонструємо аналізом результатів комп'ютерного моделювання (див. рис. 2, 3, 4) об'ємного ТН сигналу, наприклад, у вигляді пакету з N когерентних імпульсів гаусової форми (КІГФ) однакової амплітуди, модуль змішаної автокореляційної функції якої [11, с. 375] є:

$$K_{0\mathrm{N}}(\tau',\Delta\omega)=\frac{\sin\left[0{,}5\Delta\omega T_{\mathrm{i}}(N-|p|)\right]}{N\sin(0{,}5\Delta\omega T_{\mathrm{i}})}\exp\left(-0{,}5\gamma^2\tau^2\right)\exp\left(-\frac{\Delta\omega^2}{8\gamma^2}\right) \tag{5}$$

де $\tau'=p\cdot T_{\mathrm{i}}\pm\tau_{\mathrm{i}}$; $p=0,\pm1,\pm2,...,\pm N$;

T_{i} – постійний період надходження елементарних сигналів;

γ – коефіцієнт, обернено пропорційний тривалості імпульсу, відрахованій на рівні 0,5 від максимуму, що дорівнює значенню ефективної ширини спектру $\Delta f_{\text{сп}}$ і характеризує швидкість зміни обвідної $M(f)$.

Причому відповідна роздільна здатність за дальністю та швидкістю, яку визначають за найбільшими розмірами перерізу центрального піка, складає

$$\delta(D)_{\text{пот}}=0{,}66\cdot c\cdot\tau_{\mathrm{i}}; \tag{6}$$

$$\delta(V_{\mathrm{p}})_{\text{пот}}=\pi\cdot c/(\omega NT_{\mathrm{i}})=0{,}5\lambda/NT_{\mathrm{i}}. \tag{7}$$

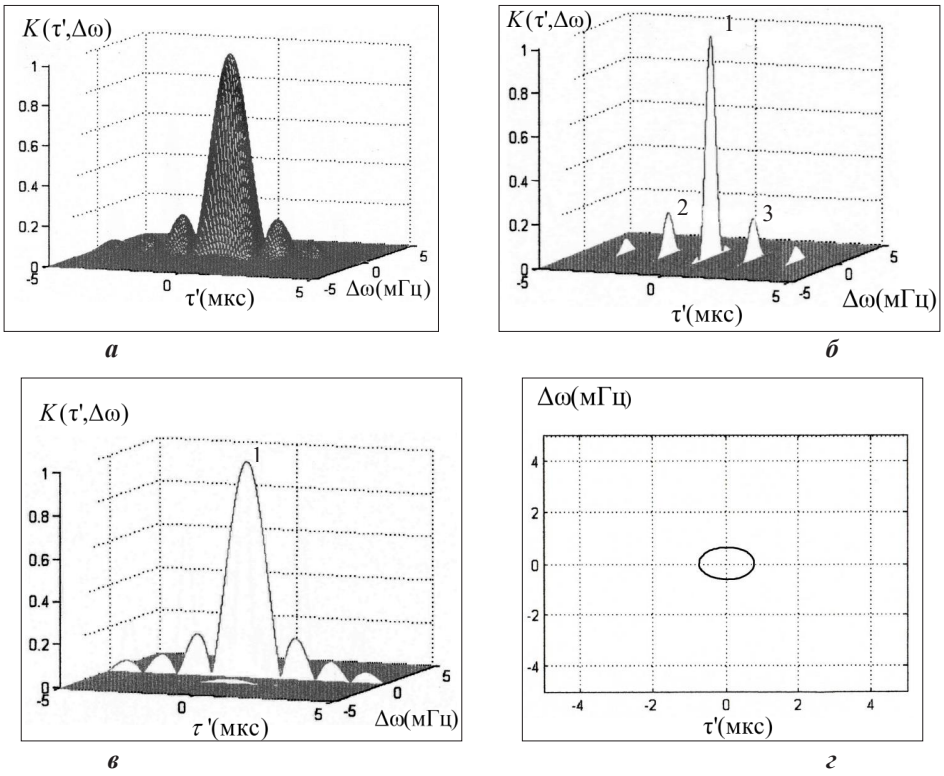

Рис. 2. Від ТН сигналу у вигляду пакета КІГФ і однакової амплітуди,

де:

а) ТН пачки ($N = 5$) імпульсів з $\tau_i = 0{,}4$ мкс, $\Delta T = 10^{-3}$ с;

б) за $\Delta\omega = \text{const}$, $|\tau_2| > |\tau_2|$: $1 \Rightarrow K(0, \Delta\omega)$; $2 \Rightarrow K(-\tau, \Delta\omega)$; $3 \Rightarrow K(\tau_1, \Delta\omega)$;

в) за $\tau = \text{const}$: $1 \Rightarrow K(\tau, 0)$;

г) $K(\tau, \Delta\omega) = 0{,}5$ за $\tau_i = 0{,}4$ мкс, $\Delta T = 10^{-3}$ с.

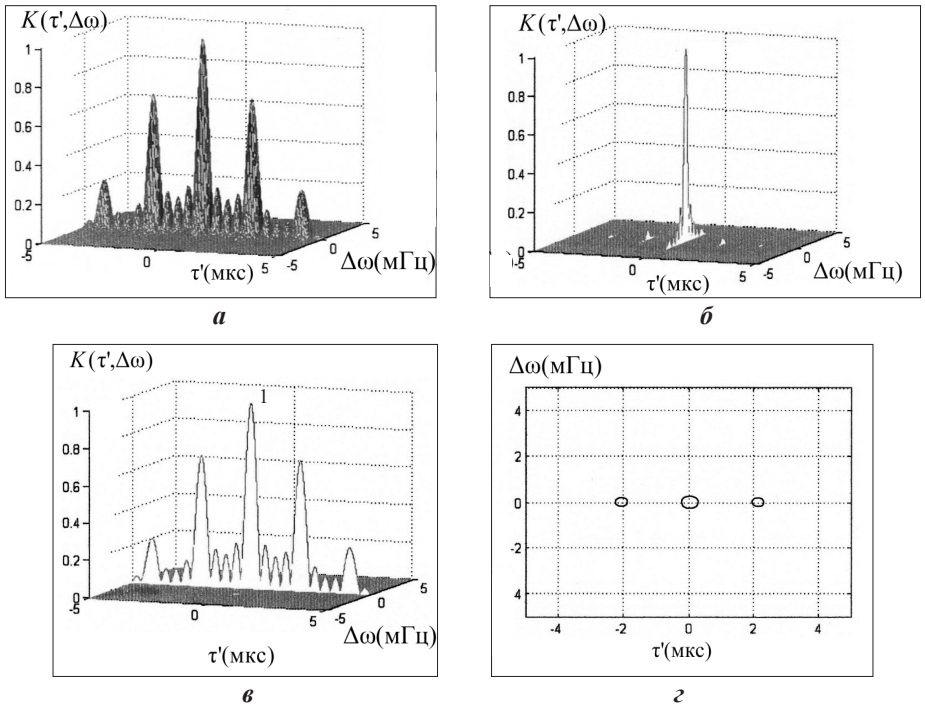

Рис. 3. Від ТН сигналу у вигляду пакета з N когерентних імпульсів гауссової форми й однакової амплітуди,

де:

а) ТН пачки ($N = 5$) імпульсів з $\tau_i = 0{,}4$ мкс, $\Delta T = 3 \cdot 10^{-3}$ с;

б) за $\Delta\omega = \text{const}$: $1 \Rightarrow K(0, \Delta\omega)$;

в) за $\tau = \text{const}$: $1 \Rightarrow K(\tau, 0)$;

г) $K(\tau, \Delta\omega) = 0{,}5$ за $\tau_i = 0{,}4$ мкс, $\Delta T = 10^{-3}$ с.

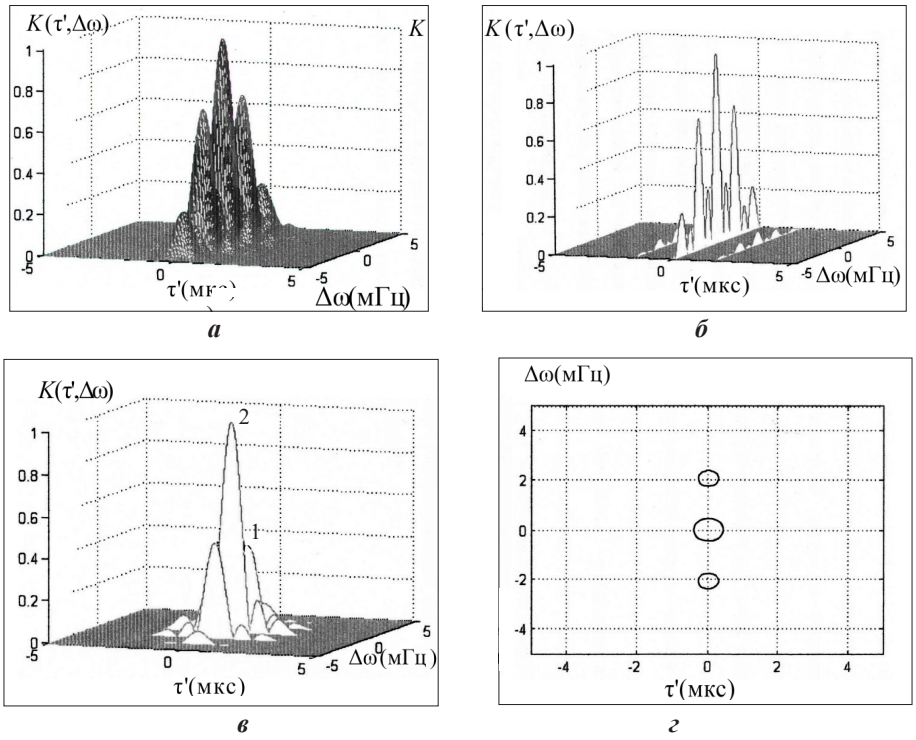

Рис. 4. Від ТН сигналу у вигляду пакета з N когерентних імпульсів гауссової форми й однакової амплітуди, де:

а) ТН пачки ($N = 5$) імпульсів з τі = 1,2 мкс, $\Delta T = 3 \cdot 10^{-3}$ с;

б) за Δω = const : 1 ⇒ K (0, Δω);

в) за τ = const : 1 ⇒ K (τ, $-\Delta\omega_1$); 2 ⇒ K (τ, 0); 3 ⇒ K (τ, $\Delta\omega_1$);

г) K (τ, Δω) = 0,5 за τ_i = 1,2 мкс, $\Delta T = 10^{-3}$ с;

Однак наявність декількох піків функції K_{0N}, звужує діапазон однозначного вимірювання дальності та швидкості, який складає величину $0{,}5cT_i$ та $\pi c/\omega T_i$ відповідно. Крім того, як бачимо (див. рис. 2–4) [11, с. 389–392], для різних пачок імпульсів на площині (τ',Δω) об'ємне ТН (K_{0N}) має вигляд послідовності піків, висоти яких зменшуються в процесі віддалення від початку координат. При цьому кожен еліпс невизначеності поодинокого сигналу розпадається на ряд еліпсів, довжина яких зменшена за віссю частот приблизно в NT_i/τ_i разів. Крім того, функція має періодичну структуру за обома (за годиною – дальністю та частотою – швидкістю) напрямками.

Періодичність за часом вказує на неоднозначність відліку дальності, що виникає в таких випадках, коли дальність цілі ΔТ (у одиницях часу) перевищує період повторюваності імпульсів.

Тому в разі вибору щодо сигналу, якій зондує, його період звичайно беруть настільки великий, щоб уникнути неоднозначності за максимальної дальності. Періодичність (неоднозначність) за частотою також добрі відома в системах із селекцією рухомих цілей. Ця неоднозначність пов'язана з так званими «сліпими» швидкостями цілей. Якщо період повторення та несуча частота обрані так, що в межах передбаченого діапазону дальність та швидкість неоднозначність не проявляється, то точність і роздільну здатність визначає тільки центральний пік функції K_0(τ,Δω).

Очевидно, що площа цього піка значно менша, ніж для поодинокого імпульсу, тому когерентна пачка має певні переваги. Однак, застосувавши пачку замість поодинокого імпульсу, також не уникаємо загальної невизначеності вимірювання, а лише перерозподіляємо її, оскільки одержали безліч неоднозначних відліків, кожен із яких виконується з більш високою точністю.

Отже, оптимальність вибору зондувального сигналу, з одного боку, доцільно забезпечувати шляхом реалізації апріорного аналізу сигнальної функції конкретної зондувальної пачки та відповідного їй об'ємного тіла невизначеності. З іншого боку, за аналогією з шумоподібним сигналом, використання складних (відносно поодинокого імпульсу) сигналів дає змогу покращувати прихованість самого процесу виявлення (у даному випадку дронів) з високою супутньою роздільною здатністю безпосередньо за двома параметрами – його (дрона) локальною дальністю та швидкістю.

Висновки. Виконано аналіз методологічної побудови структурно-лінгвістичної схеми вибору засобів захисту сукупності об'єктів критичної інфраструктури з позиції зниження ризику. Показано, що вона має універсальну структуру та фактично може бути використана в будь-якій організованій сфері діяльності

соціуму незалежно від виду галузі, розмірів організації, виділених матеріальних засобів та інтелектуального рівня штатного персоналу, відповідального за дану сферу безпеки та захисту.

Обґрунтовано додана частина структурно-лінгвістичної схеми з позицій риск- орієнтованих процесів забезпечення безпеки ОКІ, в якої відображені: організаційні та фізичні засоби захисту загального застосування; специфічні засоби захисту інформаційної системи; засоби захисту відповідно до проблем (від утрат конфіденційності; цілісності; доступності; спостережності; автентичності та надійності) та загроз у межах забезпечення їх безпеки.

На прикладі виявлення несанкціонованих повітряних атак зловмисників, які використовують дрони, продемонстровано доцільність і можливість виявлення потенційної атаки порушником або зловмисником, які застосовують дрони, використовуючи радіофізичні системи як засоби вимірювання навколишнього середовища у вигляді схемотехнічної реалізації кореляційних радіолокаційних пристроїв ближньої взаємодії, які використовують шумоподібний безперервний надвисокочастотний зондувальний сигнал з амплітудною модуляцією у вигляді пачки з N когерентних імпульсів гаусової форми. При цьому показано, що оптимальність вибору зондувального сигналу, з одного боку, залежить від результату апріорного аналізу сигнальної функції конкретної зондувальної пачки та відповідного їй об'ємного тіла невизначеності, а з іншого боку, – забезпечує прихованість самого процесу виявлення (у цьому разі дронів) з високою роздільною здатністю безпосередньо за двома параметрами – його дальністю та швидкістю.

Список використаних джерел:

1. Тарасенко Ю.С., Соляннiков В.Г., Бруй І.І. Кібербезпека: інформаційні аспекти захисту від технологій впливу. *Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах* : Матеріали міжнародної науково-практичної інтернет-конференції. Секц. «Спрямування розвитку сучасних інноваційних технологій у сфері комп'ютерних наук та кібербезпеки», Дніпро 16 квітня 2021 р. С. 424–426.
2. Закон України Про основні засади забезпечення кібербезпеки України. *Відомості Верховної Ради (ВВР)*. 2017. № 45, ст. 403. {Із змінами від 21.06.2018, від 17.06.2020, від 17.09.2020}
3. ДСТУ ISO 31000 2018. (ISO 31000:2018, IDT) Менеджмент ризиків. Принципи та настанови. Наказ від 29.11.2018 № 446. Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»). З наданням чинності від 2019-01-01.
4. Tarasenko Yu.S., Klym V.Yu. The methodology of building the cognitive model of critical infrastructure's security. Rr. 38–51. Rrospektive globale wissenschaftliche trends. European Science : monographic series. Book 11. Part 1. Karlsruhe, Germany : ScientificWorld-NetAkhatAV, 2022.
5. Tarasenko Yu.S., Klym V.Yu. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. *System technologies*. 2022. Vol. 4. № 141. Pp. 158–168.
6. Національний стандарт України ДСТУ ISO 9000:2015 (ISO 9000:2015, IDT) Системи управління якістю. Основні положення та словник термінів Видання офіційне. Київ : ДП «УкрНДНЦ», 2016. С. 51.
7. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) Дата початку дії 01.11.2019. ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») Дата прийняття 16.10.2019. Мова документа Англійська. International standard ISO/IEC 27005:2019 Information technology – Security techniques – Information secure risk management. https://www.google.com/url
8. ISO/IEC Guide 98-1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT.
9. Тарасенко Ю.С., Соляннiков В.Г. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань. *Збірник матеріалів міжнародної науково-практичної інтернет-конференції «Інноваційні технології, моделі управління кібербезпекою – "ITMK-2021",* Дніпро, 14–16 квітня 2021 р. С. 29–30.
10. ISO 9001:2015(en). Quality management systems – Requirements. Fifth edition 2015-09-15.
11. Тарасенко Ю.С. Фізичні основи радіолокації : навч. посіб. Д. : «Пороги», 2011. 487с.

References:

1. Tarasenko YU.S., Solyannikov V.H., Bruy I.I. Kiberbezpeka: informatsiyni aspekty zakhystu vid tekhnolohiy vplyvu [Cyber security: informational aspects of protection from influence technologies]. Materialy mizhnarodnoyi naukovo-praktychnoyi internet-konferentsiyi "I*nnovatsiyni rishennya v ekonomitsi, biznesi, suspilnykh komunikatsiyakh ta mizhnarodnykh vidnosynakh*" Sekts. "Spryamuvannya rozvytku suchasnykh innovatsiynykh tekhnolohiy u sferi kompyuternykh nauk ta kiberbezpeky" Dnipro 16 kvitnya 2021 r. S. 424-426.
2. Zakon Ukrayiny Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny [The Law of Ukraine On the Basic Principles of Ensuring Cyber Security of Ukraine] *Vidomosti Verkhovnoyi Rady (VVR)*, 2017, № 45, st. 403. {Iz zminamy vid 21.06.2018, vid 17.06.2020, vid 17.09.2020}
3. DSTU ISO 31000 2018. (ISO 31000:2018, IDT) Menedzhment ryzykiv. Pryntsypy ta nastanovy [Risk management. Principles and guidelines]. Nakaz vid 29.11.2018 № 446. Derzhavne pidpryyemstvo "Ukrayinskyy naukovo-doslidnyy i navchalnyy tsentr problem standartyzatsiyi, sertyfikatsiyi ta yakosti" (DP "UkrNDNTS"). Z nadannyam chynnosti vid 2019-01-01.

4. Tarasenko Yu.S., Klym V.Yu. The methodology of building the cognitive model of critical infrastructure's security. Rr. 38-51. Rrospektive globale wissenschaftliche trends. Monographic series "European Science". Book 11. Part 1. Published by: ScientificWorld-NetAkhatAV. Karlsruhe, Germany 2022.

5. Yu.S. Tarasenko, V.Yu. Klym. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. Vol. 4 No. 141 (2022): *System technologies.* Pp. 158–168.

6. Natsionalnyy standart Ukrayiny DSTU ISO 9000:2015 (ISO 9000:2015, IDT) Systemy upravlinnya yakistyu Osnovni polozhennya ta slovnyk terminiv [Quality management systems. Basic provisions and glossary of terms] Vydannya ofitsiyne Kyyiv DP "UkrNDNTS" 2016. 51 s.

7. DSTU ISO/IEC 27005:2019 Informatsiyni tekhnolohiyi. Metody zakhystu. Upravlinnya ryzykamy informatsiynoyi bezpeky [Information technology – Security techniques – Information secure risk management] (ISO/IEC 27005:2018, IDT) Data pochatku diyi 01.11.2019. DP "Ukrayinskyy naukovo-doslidnyy i navchalnyy tsentr problem standartyzatsiyi, sertyfikatsiyi ta yakosti" (DP "UkrNDNTS") Data pryynyattya 16.10.2019. Mova dokumenta Anhliyska. International standard ISO/IEC 27005:2019 Information technology – Security techniques – Information secure risk management. https://www.google.com/url.

8. ISO/IEC Guide 98-1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT.

9. Tarasenko Yu.S., Solyannikov V.H. Informatsiyni systemy z pozytsiy zabezpechennya nadiynosti ta nevyznachenosti vymiryuvan [Information systems from the standpoint of reliability and measurement uncertainty]. *Zbirnyk materialiv mizhnarodnoyi naukovo-praktychnoyi internet-konferentsiyi "Innovatsiyni tekhnolohiyi, modeli upravlinnya kiberbezpekoyu – "ITMK-2021",* Dnipro, 14–16 kvitnya 2021 r. S. 29Y30.

10. ISO 9001:2015(en). Quality management systems – Requirements. Fifth edition 2015-09-15.

11. Tarasenko. Yu.S. Fizychni osnovy radiolokatsii [Physical foundations of radar]: navch. posib. D.: "Porohy", 2011. 487 s.