



[DOI 10.28925/2663-4023.2022.15.164174](https://doi.org/10.28925/2663-4023.2022.15.164174)

УДК 004.056

Бржевська Зореслава Михайлівна

доктор філософії

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0002-7029-9525

z.brzhevskaya@kubg.edu.ua

Киричок Роман Васильович

доктор філософії

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0002-9919-9691

r.kyrychok@kubg.edu.ua

Платоненко Артем Вадимович

кандидат технічних наук

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0002-2962-5667

a.platonenko@kubg.edu.ua

Гулак Геннадій Миколайович

доктор технічних наук, доцент

професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0001-9131-9233

h.hulak@kubg.edu.ua

ОЦІНКА ПЕРЕДУМОВ ФОРМУВАННЯ МЕТОДИКИ ОЦІНКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ

Анотація. Концептуальна модель достовірності інформації включає: інформаційні ресурси, джерела інформації, фактори інформаційного протиборства, джерела факторів інформаційного протиборства (загроз достовірності), цілі зловмисників, функції, методи та засоби забезпечення достовірності, показники достовірності. Достовірність інформації (ступінь довіри до даних), яка міститься в інформаційних ресурсах багато в чому визначається якістю джерел та можливістю індивідів впливати на інформаційні процеси. При цьому поняття достовірності інформації часто пов'язується з категоріями цілісності та доступності інформаційних ресурсів. Все це повинно бути забезпечено при функціонуванні інформаційного простору в умовах випадкових чи навмисних інформаційних впливів. Необхідною умовою досягнення необхідного рівня достовірності інформації є побудова комплексної системи забезпечення достовірності інформації. Інформаційний простір підприємств існують в системі товарно-грошових відносин, в основі якої лежить поняття економічної ефективності, і не можуть собі дозволити безконтрольно і безпідставно витрачати матеріальні ресурси на проведення будь-яких заходів. Внаслідок цього оцінка рівня достовірності інформації і прийняття рішень щодо проведення заходів для його підвищення піднімають сукупно завдання оцінки економічного ефекту від їх проведення.

Ключові слова: достовірність інформації, інформаційний простір, інформаційні ресурси, засоби масової інформації

ВСТУП

Забезпечення необхідного рівня достовірності інформації, що циркулює в інформаційному просторі (ІП), неможливо без оцінки поточного рівня, який визначають



безліч різних чинників. Методика оцінки поточного рівня достовірності інформації як ймовірності збереження її незмінності в інформаційному потоці в умовах інформаційних впливів вимагає дослідження наступних критеріїв [1-6]:

- відносні частоти виникнення дестабілізуючих факторів – факторів інформаційного протиборства (ФІП) (загроз достовірності) $P_{ФІП}$,
- можливості порушення достовірності інформації $P_{НД}$.
- ймовірності виявлення спроб порушення достовірності $P_{В}$.

Відповідно, підвищення рівня достовірності в умовах інформаційних впливів можливо роботою в трьох напрямках [7]:

- зміна структури ІП з метою зменшення кількості вразливостей/структурно-функціональних недоліків (СУ), призводять до виникнення ФІП;
- підвищення якості системи забезпечення достовірності інформації (СЗДІ).

Необхідною умовою досягнення необхідного рівня достовірності інформації (ДІ) є побудова комплексної СЗДІ. ІП підприємств існують в системі товарно-грошових відносин, в основі якої лежить поняття економічної ефективності, і не можуть собі дозволити безконтрольно і безпідставно витратити матеріальні ресурси на проведення будь-яких заходів. Внаслідок цього оцінка рівня ДІ і прийняття рішень щодо проведення заходів для його підвищення піднімають супутню завдання оцінки економічного ефекту від їх проведення.

Отже, в загальний метод оцінки достовірності необхідно включити такі додаткові критерії:

- вартість інформаційних ресурсів (ІР) $S_{ІР}$,
- вартість засобів обробки інформації $S_{ОІ}$,
- вартість системи забезпечення достовірності $S_{СЗДІ}$,
- сумарний ризик інформації $R_{ІР}$,
- сумарний ризик засобів обробки інформації $R_{ОІ}$,
- сумарний ризик системи забезпечення достовірності $R_{СЗДІ}$.

ОСНОВНА ЧАСТИНА

Імовірнісні, вартісні критерії та критерії ризиків можна назвати параметрами ІП. Залежать від них загальний коефіцієнт достовірності інформації $D_{ІР}$ і економічна ефективність E_f є показниками якості СЗДІ.

Можна виділити наступні залежності між параметрами ІП:

$$P_{ФІП} = f(S_{ІР}, S_{ОІ}),$$

$$P_{НД} = f(P_{ФІП}, S_{ІР}, S_{ОІ}, S_{СЗДІ}),$$

$$R_{ІР} = f(S_{ІР}, S_{СЗДІ}, P_{ФІП}, P_{НД}), \quad (1)$$

$$R_{ОІ} = f(S_{ОІ}, S_{СЗДІ}, P_{ФІП}, P_{НД}),$$

$$R_{СЗДІ} = f(S_{СЗДІ}, P_{ФІП}, P_{НД}).$$

Оцінка поточного рівня ДІ не є самоціллю, вона необхідна для оптимізації параметрів ІП з метою підвищення ДІ в ІП в умовах інформаційних впливів. Загальна модель контролю показників ДІ в ІП представлена на рис. 1.

Залежності (1) носять імовірнісний характер. Математична статистика і теорія ймовірностей використовують експериментальні дані, володіють точністю і

достовірністю [8, 9]. В даному випадку поняття точності і достовірності не завжди застосовні, тому що ці ймовірності залежать від «людських знань» [10]. Тому для достовірної кількісної оцінки показників якості СЗДІ необхідно використовувати теорію нечітких множин, яка оперує не поняттям «ймовірність», а поняттям «можливість», що більш адекватно відповідає рішенню важко формалізованих завдань.

Ймовірності виникнення, виявлення та усунення помилок є числовими характеристиками і можуть бути визначені статистичними методами. Але ІП складається з множини різнорідних компонентів, їх склад може вельми істотно відрізнятись. Тобто отримати статистику по достатній кількості однотипних систем майже завжди неможливо. Рішенням тут може бути експертна оцінка. Для показників достовірності та ефективності необхідно отримання кількісного результату, що істотно ускладнюється низкою факторів:

- наявність складної опосередкованої взаємозв'язку цих показників з параметрами ІП;
- необхідність обліку та формалізації ряду параметрів ІП, багато з яких спочатку задані якісними величинами і мають елементи неоднозначності;
- наявність суттєвого взаємозв'язку і взаємозалежності цих параметрів, що мають суперечливий характер;
- складність отримання вихідних даних, необхідних для оцінки, зокрема на ранніх етапах проектування СЗДІ.

Проектування, організація і застосування СЗДІ фактично пов'язані з невідомими подіями в майбутньому і тому завжди містять елементи невизначеності. Крім того, присутні й інші причини неоднозначності, такі як недостатньо повна інформація для прийняття управлінських рішень або соціально-психологічні чинники.

У процесі виконання завдання оптимізації доводиться враховувати наступне [11]:

- переважно нечіткий опис множини вихідних даних, зокрема опис стандартів, які використовуються при побудові СЗДІ і задаються у вигляді вимог;
- сама постановка завдання вибору зазвичай є нечіткою, при цьому перевагу того чи іншого показника визначається експертною інформацією;
- багатокритеріальність завдання.



Рис. 1. Загальна модель контролю показників достовірності інформації в ІП



З економічної точки зору ефективним буде такий комплекс заходів щодо підвищення достовірності інформації в ІП, при якому виконані наступні умови:

$$\begin{cases} S_{CЗД} \leq \Delta R_{IP} + \Delta R_{OI} + \Delta R_{CЗД} \\ S_{CЗД} \leq S_{IP} + S_{OI} \end{cases} \quad (2)$$

де $\Delta R_{IP} + \Delta R_{OI} + \Delta R_{CЗД}$ - загальне зниження ризиків в ІП.

Якщо перша умова очевидно: отриманий ефект не повинен бути менше вартості коштів і заходів, тобто витрат, то друге не настільки очевидно. І тим не менше, дійсно велика частина витрат підприємства спрямована на виконання його основної діяльності, а не на реалізацію функцій СЗДІ.

З функціональної точки зору, яка визначена загальним коефіцієнтом достовірності, якість системи визначають умови, показують відповідність деякому мінімального порогу, наприклад, так:

$$D_i \geq D_{i,min}, \forall i = \overline{1, z} \quad (3)$$

Умови (2) і (3), очевидно, суперечливі: підвищення рівня ДІ в ІП на певному етапі можливо тільки при збільшенні інвестицій в СЗДІ. З цього випливає постановка задачі оптимізації:

$$\begin{cases} D_{IP} \rightarrow \max \\ D_i \geq D_{i,min}, \forall i = \overline{1, z}, \\ S_{CЗД} \leq \Delta R_{IP} + \Delta R_{OI} + \Delta R_{CЗД} \\ S_{CЗД} \leq S_{IP} + S_{OI} \end{cases} \quad (4)$$

Модель контролю показників достовірності інформації в ІП, представлена на рис. 1, є спільною, відображає структуру взаємозв'язків параметрів ІП, а також порядок їх оцінки. Характер взаємозв'язків можна описати моделлю, представленою на рис. 2.

Область ФІП T являє собою список всіх можливих ФІП для даної ОТС, кожен ФІП характеризується відносною частотою виникнення.

Множина СУ V являє собою перелік всіх існуючих вразливостей в даній ОТС, основними характеристиками яких є значимість і доступність для зловмисника. В сукупності множини ФІП та СУ і їх взаємозв'язку утворюють перелік способів досягнення мети - інформаційний вплив на ІП організації.

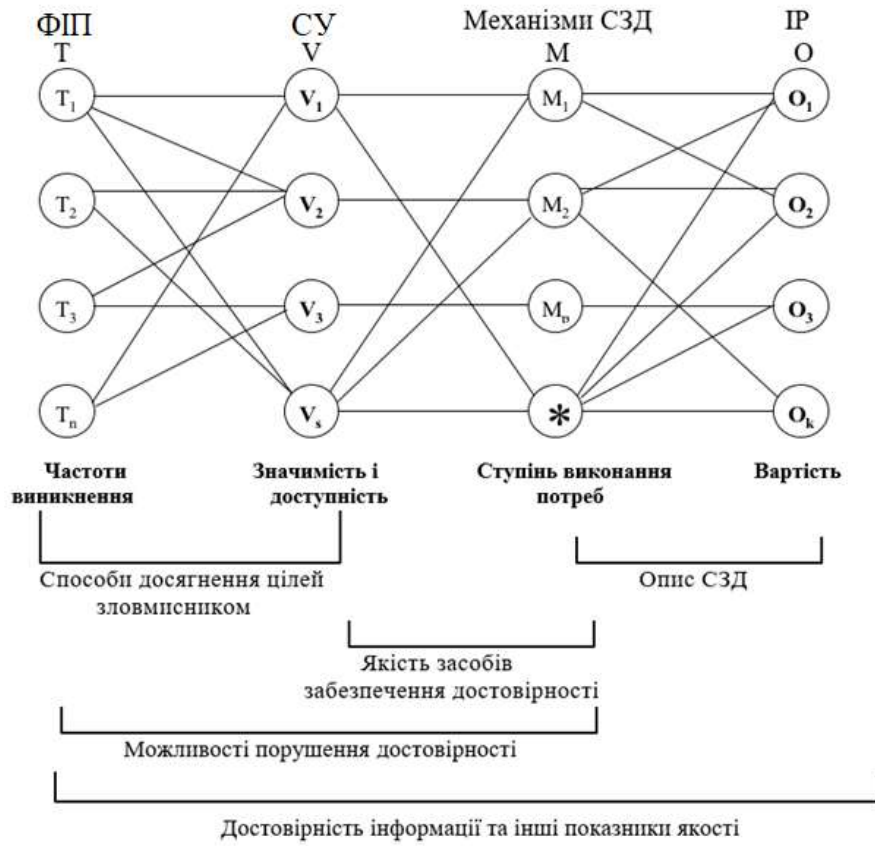


Рис. 2. Модель, що описує характер взаємозв'язку параметрів ІП і показників якості СЗД

Якість засобів забезпечення достовірності визначається при розгляді множини V і множини M з їх взаємозв'язками, і характеризується можливостями подолання кожного бар'єру, асоційованого з кожним СУ. Тут штучно доданий елемент (*), що показує, що ряд СУ, може бути взагалі не перекритий будь-яким бар'єром.

Область O представляє собою сукупність ІР, характеристики яких: цінність і вартість, яка визначається виходячи з фінансових втрат організації, асоційованих з відновленням ресурсу, або з упущеною вигодою, пов'язаними зі знищенням, тиражуванням, або блокуванням доступу до захищеного ресурсу.

Разом множина M , множина O в їх взаємозв'язку дають повний опис СЗДІ організації.

Ймовірності порушення достовірності в ІП визначаються, з одного боку, способами досягнення цілей, а з іншого - якістю засобів забезпечення достовірності. Загалом, достовірність інформації і інші показники якості будуть визначені при детальному розгляді всіх областей графа, при цьому ефективність характеризується співвідношенням ризиків від порушення достовірності інформації в ІП організації при відсутності і при наявності СЗДІ.

Визначення ймовірності виникнення факторів інформаційного протистояння.

Одним з методів формального визначення ймовірностей є статистична оцінка. Вона може бути адекватно застосована в тих випадках, коли є статистика для аналогічної ІП, експлуатованої з подібною специфікою діяльності, тобто коли можна говорити про наявність аналогічного набору СУ [90, 95]. Але в зв'язку з різноманіттям окремих



характеристик ІІ знайти аналог досліджуваної системи дуже непросто. Крім того, треба врахувати той факт, що отримати достовірну всеосяжну статистику по якомусь підприємству від нього буває дуже важко.

Коли така статистика недоступна, або в тому випадку, коли близьких аналогів досліджуваної ІІ немає, адекватна оцінка відносних частот виникнення ФІІ і можливостей збереження достовірності може бути проведена тільки методами експертних оцінок на основі первинної оцінки не самих ймовірностей, а множин окремих показників, від яких вони залежать. Тоді деякий відсоток помилок в загальному масиві даних не на багато знизить адекватність експертизи.

Стан ІІ характеризують не тільки можливості порушення достовірності інформації, а й відносні частоти виникнення факторів інформаційного протидіювання (ФІІ), що призводять до такого порушення.

Виникнення будь-якого ФІІ навмисного дії обумовлено, з одного боку, наявністю в ІІ СУ i , з іншого боку, зацікавленістю зловмисника у виконанні такої дії. Взаємодія двох систем: ІІ підприємства та інформаційної системи зловмисника відбувається в єдиному інформаційному просторі. З точки зору забезпечення достовірності слід розглянути множину подій в цьому інформаційному просторі $E = \{e_0, e_1, \dots, e_n\}$, де подія e_0 полягає в тому, що в даний момент часу не виник ні один з повної множини ФІІ, а події e_1, \dots, e_n полягають у виникненні l -го ФІІ, $l = \overline{1, n}$.

Множина $E = \{e_0, e_1, \dots, e_n\}$ є повною множиною незалежних і несумісних подій, тому що по-перше, виникнення одного ФІІ не залежить від виникненням будь-якого іншого ФІІ, по-друге, розглядається подія "виникнення l -го ФІІ" відбувається в нескінченно малий проміжок часу і не може збігтися з іншою подією "виникнення k -го ФІІ".

Ймовірність виникнення ФІІ залежить від зацікавленості зловмисника у виконанні несанкціонованих дій, природно, при наявності деякого СУ в ІІ. Зацікавленість зловмисника у використанні СУ виразно залежить від того, наскільки значущий даний СУ для нормального функціонування ІІ - чим більше значимість СУ, тим більше зацікавлений зловмисник в його використанні. Але на відносну частоту виникнення ФІІ також впливає ще й обізнаність зловмисника про наявність СУ.

Відносну частоту виникнення ФІІ $p_l^{\text{ФІІ}}$ можна уявити як функцію значень критеріїв "значимість СУ" і "доступність СУ" для всіх СУ (тому що один СУ може служити причиною появи декількох ФІІ, і, навпаки, множина СУ може викликати появу одного ФІІ):

$$p_l^{\text{ФІІ}} = f(\gamma_{\alpha\beta}, d_{\alpha}, \forall \alpha, \beta = \overline{1, s}). \quad (5)$$

Для обчислення кількісного значення $p_l^{\text{ФІІ}}$ необхідно:

- визначити повну скінченну множину СУ, характерних для даної ІІ;
- отримати лінгвістичні експертні оцінки $\gamma_{\alpha\beta}, d_{\alpha}, \forall \alpha, \beta = \overline{1, s}$ від кожного ε -го експерта;
- визначити причинно-наслідкові зв'язки між k -м СУ і l -м ФІІ;
- обчислити значення $p_{l\varepsilon}^{\text{ФІІ}}$ за оцінками кожного ε -експерта;
- агрегувати отримані значення $p_{l\varepsilon}^{\text{ФІІ}}$ тобто перетворити кожну нечітку множину $A(p_l^{\text{ФІІ}}) = A\{p_{l\varepsilon}^{\text{ФІІ}} / \varepsilon\}$ в чітке число $p_l^{\text{ФІІ}}$.



На першому етапі даного алгоритму експертиза повинна бути проведена у вигляді круглого столу. Її результатом буде складання повного списку всіх СУ, характерних для даної ІІ.

На другому етапі експерти представляють свої індивідуальні оцінки. Для коефіцієнтів значущості вони представлені у вигляді матриці парних порівнянь Сааті.

На третьому етапі перебування $p_l^{\text{ФІІ}}$ необхідно побудувати матриці причинно-наслідкових зв'язків між k -м СУ і l -м ФІІ

Отримаємо матрицю показників критичності СУ з розмірністю $n \times s$

$$M_{\varepsilon}^{\text{ПК}} = M_{\varepsilon}^{\text{ПНЗ}} \times M_{\varepsilon}^{\Gamma} = \begin{pmatrix} \omega_{11}^{\varepsilon} & \omega_{12}^{\varepsilon} & \dots & \omega_{1s}^{\varepsilon} \\ \omega_{21}^{\varepsilon} & \omega_{22}^{\varepsilon} & \dots & \omega_{2s}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \omega_{s1}^{\varepsilon} & \omega_{s2}^{\varepsilon} & \dots & \omega_{ss}^{\varepsilon} \end{pmatrix} \quad (6)$$

Величина $\omega_{ik}^{\varepsilon}$ показує ступінь впливу k -го СУ на появу l -го ФІІ. Величини $\omega_{ik}^{\varepsilon} \forall i = \overline{1, n}, k = \overline{1, s}$ не нормовані, але при цьому максимальне значення такої величини показує максимальну ступінь впливу.

Збереження достовірності інформації. Можливості збереження достовірності i -го ІР під впливом l -го ФІІ на думку ε -го експерта $p_{il\varepsilon}^C$ визначається тим, наскільки повно враховані якісні та кількісні вимоги до передачі, зберігання і обробці ІР:

$$p_{il\varepsilon}^C = f(x_{ilq_1}^{\text{П}\varepsilon}, x_{ilq_2}^{\text{Х}\varepsilon}, x_{ilq_3}^{\text{О}\varepsilon}, \forall q \in \overline{1, t}), \quad (7)$$

де $x_{ilq_1}^{\text{П}\varepsilon}, x_{ilq_2}^{\text{Х}\varepsilon}, x_{ilq_3}^{\text{О}\varepsilon}$ - ступеня виконання q -ї вимоги щодо функціонування відповідно механізмів передачі, зберігання або обробки i -го ІР в умовах впливу l -го ФІІ.

Нехай перші h -вимоги будуть кількісними ($q = \overline{1, h}$) інші $t-h$ – якісним ($q = \overline{h+1, t}$).

Ступінь виконання кількісного вимоги визначається його ставленням до необхідного (оптимального) кількісному значенню параметра СЗДІ. Процедури отримання оцінок кількісних параметрів розглянуті в п.3.3.

Для оцінки ступеня виконання якісних вимог (а таких вимог в різних стандартах незрівнянно більше, ніж кількісних) необхідно використовувати уявлення вимоги у вигляді нечіткої множини.

Ступінь виконання кожного якісного вимоги визначається функцією приналежності ряду характеристик СЗДІ, від яких залежить виконання цієї вимоги, до їх оптимальних значень.

Нехай $G = \{g_1, g_2, \dots, g_p\}$ – універсальна множина характеристик СЗДІ. На множині G задано нечітку множину A_q , яка відбиває ступінь приналежності СЗДІ до оптимальної по q -му вимогу.

Нечітка множина A_q , визначається :

1) Множиною ступенів відповідності кожної характеристики СЗДІ виконання q -го якісного вимоги $Y_q = \{y_1, y_2, \dots, y_p\}$.

2) Множиною ступенів впливу характеристик на виконання вимоги в цілому $\Sigma_q = \{\sigma_1, \sigma_2, \dots, \sigma_p\}$.

Якщо деяка характеристика повністю задовольняє вимогу, то її ступінь відповідності дорівнює 1, якщо повністю не задовольняє, то 0.

В цілому ступінь відповідності визначається відношенням до необхідного якісного опису характеристики СЗДІ, тобто функцією приналежності. Базовими відносинами для рівня відповідності реальної характеристики системи вимогу стандарту є: «низький», «нижче середнього», «середній», «вище середнього», «високий» [106]. На множині упорядкованих описів характеристики в порядку проходження від повного невідповідності до повної відповідності стандарту будуть відносини, представлені на рис. 3.

Приклад узятий для десяти можливих описів.

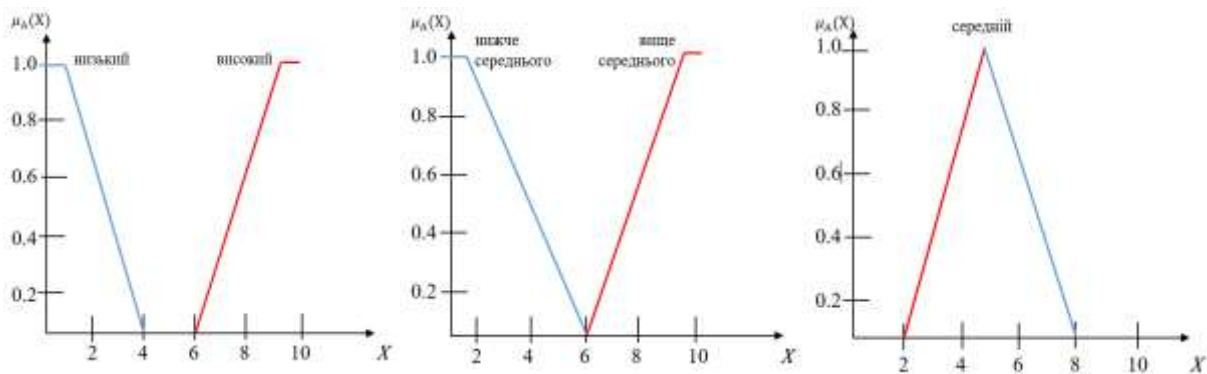


Рис. 3. Базові відносини рівня відповідності характеристики вимогу

Таблиця 1

Шкала оцінки впливу вимог на збереження достовірності [1]

Опис виду впливу	Бал
Абсолютна і постійний вплив в будь-яких умовах	5
Впливає практично у всіх умовах	3
Впливає тільки в окремих випадках (наприклад, при використанні зловмисником спецзасобів)	1
Не впливає	0

Значення 2 і 4 можуть бути взяті як проміжні.

Оцінка загального показника достовірності інформації. Оскільки різні ресурси надають різний вплив на якість функціонування ІІ, то необхідно ввести деяку величину η_i^{ε} - ($\forall i = \overline{1, z_I}$), що показує відносну цінність і-го інформаційного ресурсу. Для комерційних підприємств цінність ресурсу завжди зводиться до його грошового еквівалента, отже, вона може бути визначена з як

$$\eta_{\varepsilon i} = \frac{S_{\varepsilon IP, i}}{S_{\varepsilon IP}}, (\forall i = \overline{1, z_I}). \quad (8)$$

Тоді загальний показник достовірності достовірність інформації в ІІ за оцінкою ε -го експерта визначимо наступним чином:



$$D_{\varepsilon} = \sum_{i=1}^{z_1} \frac{S_{\varepsilon_{IP,i}}}{S_{\varepsilon_{IP}}} * D_{\varepsilon_i} \quad (9)$$

ВИСНОВКИ

Методика оцінки поточного рівня достовірності інформації як ймовірності збереження її незмінності в інформаційному потоці в умовах інформаційних впливів вимагає врахування: частоти виникнення факторів інформаційного протиборства, можливості порушення достовірності, ймовірності виявлення спроб порушення достовірності інформації. Інформаційний простір організації, підприємства, держави дуже часто складається з множини різнорідних компонентів, що не дає можливості одержувати числові компоненти статистичними методами. Відтак, найбільш доцільними тут є методи експертного оцінювання.

Таким чином, у разі відсутності статистики адекватна оцінка відносних частот виникнення факторів інформаційного протиборства та можливостей збереження достовірності інформації може бути проведена методами експертних оцінок на основі первинної оцінки множини початкових показників. У загальному випадку ймовірність виникнення фактора інформаційного протиборства залежить від зацікавленості зловмисника у виконанні несанкціонованих дій при наявності деяких уразливостей в інформаційному просторі організації. На основі експертного оцінювання кількісних та якісних вимог, у тому числі з нечіткими змінними, досягається можливість оцінки загального показника достовірності інформації у вигляді комбінації окремих показників достовірності окремих інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1 ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414
- 2 ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413
- 3 Остапенко, Г.А., Паринова, Л.В., Белоножкин, В.И., Батаронов, И.Л. (2013). *Информационные риски в социальных сетях. Монография*. ООО "Издательство "Научная книга".
- 4 Борзенкова, С.Ю., Казарина, Е.Е. (2020). Анализ методов уровня защищенности информационных систем в процессе их эксплуатации. *Известия ТулГУ. Технические науки*, 5, 93-97
- 5 Полянский, Д.А., Монахов, М.Ю. (2012). Модель оценки факторов изменения достоверности информации в корпоративной сети передачи данных. *Изв. ВУЗов. Приборостроение*, 55(8), 39-43
- 6 Sergienko, I. V. (2012). *Methods of Optimization and Systems Analysis for Problems of Transcomputational Complexity*. Springer.
- 7 Behrendt, S., Richter, A., Trier, M. (2014). Mixed methods analysis of enterprise social networks. *Computer Networks*, 75, 560–577. <https://doi.org/10.1016/j.comnet.2014.08.025>
- 8 Вентцель, Е.С. (2018). *Теория вероятностей*. Высшая школа.
- 9 Семенова, И.И. (2014). Управление процессом обеспечения достоверности информации в интеллектуальных системах поддержки принятия решений. *Одиннадцатый Международный симпозиум "Интеллектуальные системы"*, 310-314
- 10 Иванова, Н.В., Коробулина, О.Ю. (2011). *Аудит информационной безопасности. Учеб. Пособие*. ПГУПС.
- 11 Butko, T., Prokhorchenko, A., Muzykin, M. (2016). An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. *Eastern-European Journal of Enterprise Technologies*, 5(3 (83)), 47–55. <https://doi.org/10.15587/1729-4061.2016.80471>



Zoreslava M. Brzhevska

PhD

Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID: 0000-0002-7029-9525

z.brzhevska@kubg.edu.ua

Roman V. Kyrychok

PhD

Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID: 0000-0002-9919-9691

r.kyrychok@kubg.edu.ua

Platonenko V. Artem

PhD in Technical Sciences, associate professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID: 0000-0002-2962-5667

a.platonenko@kubg.edu.ua

Hennadii M. Hulak

Doctor of Technical Sciences, Associate Professor

Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID: 0000-0001-9131-9233

h.hulak@kubg.edu.ua

ASSESSMENT OF THE PRECONDITIONS OF FORMATION OF THE METHODOLOGY OF ASSESSMENT OF INFORMATION RELIABILITY

Abstract. The conceptual model of information reliability includes information resources, sources of information, factors of information confrontation, sources of factors of information confrontation (threats to authenticity), goals of attackers, functions, methods and means of ensuring reliability, and reliability indicators. The reliability of information (the degree of trust in data) contained in information resources is largely determined by the quality of sources and the ability of individuals to influence information processes. However, the concept of reliability of information is often associated with the categories of integrity and availability of information resources. All this must be ensured in the functioning of the information space in conditions of accidental or intentional informational influences. A necessary condition for achieving the required level of reliability of information is the construction of a comprehensive system for ensuring the reliability of the information. Information space of enterprises exists in the system of commodity-money relations, which is based on the concept of economic efficiency and can not afford to spend uncontrollably and unreasonably material resources for any activities. As a result, the assessment of the level of reliability of information and decision-making on measures to improve it raise the concomitant task of assessing the economic effect of their implementation.

Keywords: reliability of the information, information space, information resources, mass media

REFERENCES

- 1 ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414



- 2 ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413
- 3 Ostapenko, G.A., Parinova, L.V., Belonozhkin, V.I., Bataronov, I.L. (2013). Informatsionnyye riski v sotsial'nykh setyakh. Monografiya. OOO "Izdatel'stvo "Nauchnaya kniga".
- 4 Borzenkova, S.YU., Kazarina, Ye.Ye. (2020). Analiz metodov urovnya zashchishchennosti informatsionnykh sistem v protsesse ikh ekspluatatsii. Izvestiya TulGU. Tekhnicheskiye nauki, 5, 93-97.
- 5 Polyanskiy, D.A., Monakhov, M.YU. (2012). Model' otsenki faktorov izmeneniya dostovernosti informatsii v korporativnoy seti peredachi dannykh. Izv. VUZov. Priborostroyeniye, 55(8), 39-43.
- 6 Sergienko, I. V. (2012). *Methods of Optimization and Systems Analysis for Problems of Transcomputational Complexity*. Springer.
- 7 Behrendt, S., Richter, A., Trier, M. (2014). Mixed methods analysis of enterprise social networks. *Computer Networks*, 75, 560–577. <https://doi.org/10.1016/j.comnet.2014.08.025>
- 8 Venttsel', Ye.S. (2018). Teoriya veroyatnostey. Vysshaya shkola.
- 9 Semenova, I.I. (2014). Upravleniye protsessom obespecheniya dostovernosti informatsii v intellektual'nykh sistemakh podderzhki prinyatiya resheniy. Odinnadtsatyy Mezhdunarodnyy simpozium "Intellektual'nyye sistemy", 310-314
- 10 Ivanova, N.V., Korbulina, O.YU. (2011). Audit informatsionnoy bezopasnosti. Ucheb. Posobiye. PGUPS.
- 11 Butko, T., Prokhorchenko, A., Muzykin, M. (2016). An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. *Eastern-European Journal of Enterprise Technologies*, 5(3 (83)), 47–55. <https://doi.org/10.15587/1729-4061.2016.80471>

