УДК: 004.56:530.192 DOI 10.33111/mise.102.2

Батечко Н.Г., д.пед.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

Чугаєва О.В., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

Batechko N.H., Doctor of Pedagogical Sciences,
Professor of the Department of Computer Mathematics
and Information Security,
KNEU named after Vadym Hetman

Chugayeva O.V., Senior lecturer at the Department of Computer Mathematics
and Information Security,
KNEU named after Vadym Hetman

АНАЛІЗ СИНЕРГЕТИЧНИХ ЕФЕКТІВ В УМОВАХ ІНФОРМАЦІЙНИХ ТА КІБЕРЗАГРОЗ

ANALYSIS OF SYNERGISTIC EFFECTS IN THE CONDITIONS OF INFORMATION AND CYBER THREATS

Анотація. *У статті проаналізовано функціонування інформаційних систем із застосуванням системного та синергетичного підходів. Останнє зумовлене умовами невизначеності, хаосу глибоких суспільних трансформацій та кібервійн у сучасному інформаційному просторі. Висвітлено новітні наукові розвідки в галузі методології інформаційної безпеки та місце в ній синергетичного підходу. Розглянуто основні методологічні принципи синергетики як міждисциплінарного наукового напряму: самоорганізація, біфуркація, флуктуація, нелінійність, дисипація, атрактори. Синергічні ефекти були виділені як міждисциплінарні утворення, які пояснюють формування та самоорганізацію моделей і структур у відкритих системах. Досліджено синергетичні ефекти, властиві інформаційним системам як складному системному об'єкту. Система захисту інформації розглядається як цілісна, багатофункціональна, динамічна, відкрита структура з притаманними їй особливостями. Доведено, що традиційні погляди на дослідження функціонування таких систем наразі неефективні, оскільки вони характеризуються постійною стохастичністю та мінливістю. Як альтернативу класичним методам у дослідженні таких систем запропоновано використовувати явище інформаційної ентропії. Моніторинг зміни ентропії є необхідним та доцільним для підтримки стійкості та безпеки функціонування інформаційних систем загалом. Запропоновано моделювання процесу захисту інформації з урахуванням ентропії системи. Варто зауважити, що система забезпечення інформаційної безпеки є підсистемою національної*

безпеки України загалом, тому аналіз її функціонування в сучасних умовах війни проти російської агресії та постійних кіберзагроз ворога набуває стратегічного значення.
Ключові слова: *інформаційна безпека, процес забезпечення інформаційної безпеки, синергетичний підхід, ентропія, інформаційна ентропія, дисипативна структура.*

Abstract. *The article analyzes the functioning of information systems using systemic and synergistic approaches. The latter is caused by the conditions of uncertainty, chaos of deep social transformations and cyberwars in the modern information space. The latest scientific intelligence in the field of information security methodology and the place of a synergistic approach in it have been highlighted. The main methodological principles of synergetics as an interdisciplinary scientific area have been considered: self-organization, bifurcation, fluctuation, nonlinearity, dissipation, attractors. Synergistic effects have been highlighted as interdisciplinary formations which explain the formation and self-organization of models and structures in open systems. The synergistic effects inherent in information systems as a complex system entity have been studied. The information security system has been considered as a complete, multifunctional, dynamic, open structure with its inherent features. It has been proven that traditional views on the study of the functioning of such systems are currently ineffective, as they are characterized by constant stochasticity and variability. As an alternative to classical methods, it has been proposed to use the phenomenon of information entropy in the study of such systems. Modeling of the information security process taking into account the entropy of the system has been suggested. It is worth noting that the information security system is a subsystem of the national security of Ukraine in general, therefore, the analysis of its functioning in the modern conditions of the war against Russian aggression and constant cyber threats of the enemy acquires strategic importance.*
Keywords: *information security, the process of ensuring information security, synergistic approach, entropy, information entropy, dissipative structure.*

Постановка проблеми. У сучасних умовах інформаційних та кіберзагроз проблема забезпечення інформаційної безпеки є предметом дослідження як на рівні спеціальних установ (інститутів, центрів), так і у локальних дослідженнях окремих науковців.

За останні кілька років у вітчизняній та зарубіжній науці накопичено чималий доробок у цій галузі, який стосується властивостей інформатизації як об'єктивної характеристики розвитку суспільства, сумісних і змістовних основ інформаційної безпеки, технічних та гуманітарних проблем цього процесу.

Серед численних наукових статей полемічного характеру можна також виділити праці, що стосуються методологічного підходу до досліджуваного феномену. Таке бачення дозволяє комплексно підійти до інформаційної безпеки, відшукати внутрішні механізми її регулювання, виявляти недоліки в системі наявних знань, в основі яких варто першочергово виокремити описовість її структури та елементів.

Сучасні інформаційні та кіберзагрози, які ми спостерігаємо майже щодня, спростовують усталені уявлення про функціону-

вання інформаційної безпеки як системи в цілому і спонукають до радикально нових підходів, які б уможливили функціонування інформаційної безпеки в умовах невизначеності, хаосу, глибоких глобальних трансформацій та кібервійн.

Виходячи з цього, на нашу думку, інформаційна безпека як система може бути досліджена в межах синергетичного підходу, поєднуючи його з системним, структурно-функціональним та іншими методологічними підходами.

Аналіз останніх досліджень і публікацій. Серед останніх публікацій про застосування синергетичного підходу до проблем інформаційної безпеки, слід виокремити житомирську наукову школу І. Г. Грабара. Відома монографія «Безпекова синергетика: кібернетичний та інформаційний аспекти (2019) [2] розкриває теоретичні та практичні основи забезпечення інформаційної безпеки людини, суспільства, держави у кібернетичному та інформаційному просторах з використанням синергетичного підходу.

Методологічний контекст проблем інформаційної безпеки досліджують О. П. Дзюбань, О. Ю. Панфілов, Р. А. Чимчикаленко [4], де обґрунтовується доцільність застосування до них діалектичного, структурно-функціонального, синергетичного, системного та інших підходів.

Слід виокремити і досягнення харківської наукової школи проф. С. П. Євсеєва, зокрема, «The synergetic approach for providing bank information security: the problem formulation» [7], в якій зазначено, що на сучасному етапі розвитку науки і техніки забезпечення інформаційної безпеки повинно базуватися на новому підході — синергетичному. Його реалізація, як зазначають автори, уможливить синергетичний ефект взаємодії обраних профілів безпеки і як наслідок — продемонструє якісно нові і невідомі раніше емерджентні властивості системи безпеки.

Заслуговує на увагу дослідження групи одеських науковців Н. М. Баландіної, М. Д. Василенко та ін. стосовно доведення необхідності нового методологічного підходу до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу [1]. Авторами запропоновано синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

Серед іноземних дослідників варто вказати на результати М. Ульеру [10], в яких авторка інтерпретує кіберпростір як самоорганізуючу систему та володіє властивостями емерджентності. М. Ульеру вважає, що такий підхід уможливить підґрунтя для

управління інформацією і ризиками в глобальних віртуальних організаціях.

Інтернаціональний колектив науковців на чолі з О. Писарчуком у праці «Bifurcation Prediction Method for the Emergence and Development Dynamics of Information Conflicts in Cybernetic Space» (2019) аналіз інформаційних загроз розглядає як багатофакторний прогрес, що відображає всі сфери життєдіяльності суспільства.

Синергетика та синергетичні ефекти в міждисциплінарних дослідженнях. Зауважимо, що терміни «синергія» та «синергетичні ефекти» останнім часом стали часто з'являтися в наукових дослідженнях, особливо міждисциплінарних. Вивченням цих феноменів займається така галузь знань, як синергетика. Як напрям міждисциплінарних досліджень, синергетика розглядає процеси самоорганізації у складних відкритих системах різної природи. Синергетика спроможна визначати загальні принципи розвитку таких систем за межами їх предметної належності. Виходячи саме із законів синергетики можна побудувати загальний методологічний каркас, який не лише розвиває загальний міждисциплінарний погляд на знання, а й допомагає під час вивчення окремих сфер наукових досліджень.

Термін «синергія» (гр. *енергія сумісної дії*) передбачає співробітництво, сприяння, співучасть, і тому більшість науковців розглядають це поняття як спільне функціонування кількох структур, що досягають такого результату, який би за їх незалежної діяльності був би недосяжним. Цей факт підтверджується і в загальній теорії систем: сумісна дія елементів деякої системи перевершує ефект кожного окремого компонента у вигляді їхньої простої суми. Терміном «синергетичний ефект» дедалі більше позиціонують міждисциплінарний напрям науки, який пояснює утворення та самоорганізацію моделей і структур у відкритих системах.

Засновник теорії синергетики Г. Хакен зазначав, що її сутність розкривається у тому, що: 1) досліджувані системи складаються з декількох чи багатьох однакових чи різнорідних частин, які перебувають у взаємодії одна з одною; 2) ці системи є нелінійними; 3) у ході розгляду хімічних, фізичних та біологічних систем йдеться про відкриті системи, які далекі від теплової рівноваги; 4) ці системи перебувають під впливом внутрішніх і зовнішніх коливань; 5) системи можуть стати нестабільними; 6) відбуваються якісні зміни; 7) у цих системах виявляються емерджентні нові якості; 8) виникають просторові, часові, та просторово — часові та функціональні структури; 9) структури можуть бути

впорядкованими чи хаотичними; 10) у багатьох випадках можлива математизація [6].

Зазначене класиком синергетичної теорії Г. Хакеном розкриває: з одного боку, її сутність, а з другого — основні закономірності дослідження складних відкритих систем, які можна використовувати в їхніх дослідженнях. Узагальнюючи, можна виокремити основні аспекти дослідження відкритих складних систем: «самоорганізацію», «відкритість», «нелінійність», «нерівноваженість», «біфуркацію», «флуктуацію», «дисипативні структури», «атрактори».

Наведені поняття використовуються здебільшого в природничих науках, хоча останнім часом ними оперують науковці і в соціальних, економічних, юридичних та педагогічних дослідженнях. Застосуємо універсальну синергетичну методологію до дослідження інформаційної безпеки.

Синергетичні ефекти у досліджені інформаційної безпеки як системи. Розглянемо інформаційну безпеку як складне системне утворення та застосуємо до його дослідження основні синергетичні закони. Це доречно зробити вже з тих позицій, що ця проблема стала не лише міждисциплінарною та загальнонауковою, а й глобальною. Таке широке розуміння інформації створює підґрунтя вважати теорію інформації наукою, яка за сутністю наближається до фундаментальних.

Досліджувана система інформаційної безпеки є цілісною, поліфункціональною, динамічною, відкритою структурою з притаманними їй ознаками, ієрархічною побудовою, системоутворюючими зв'язками і спрямована на створення нової інтегративної якості (сукупності якостей) забезпечення інформаційної безпеки на всіх рівнях забезпечення життєдіяльності суспільства (рис. 1).

Варто зауважити, що система забезпечення інформаційної безпеки являє собою підсистему національної безпеки України загалом, і тому аналіз її функціонування в сучасних умовах російсько-української війни та постійних кіберзагроз ворога набуває стратегічного значення.

За таких складних умов традиційні погляди на безпекові проблеми навряд чи уможливлять певні гарантії щодо забезпечення інформаційної безпеки. Систему забезпечення інформаційної безпеки ми вважаємо відкритою у часі та просторі, яка постійно взаємодіє з навколишнім середовищем, обмінюється з ним енергією і, власне, інформацією, отже, для неї характерними є постійна стохастичність і мінливість [8].

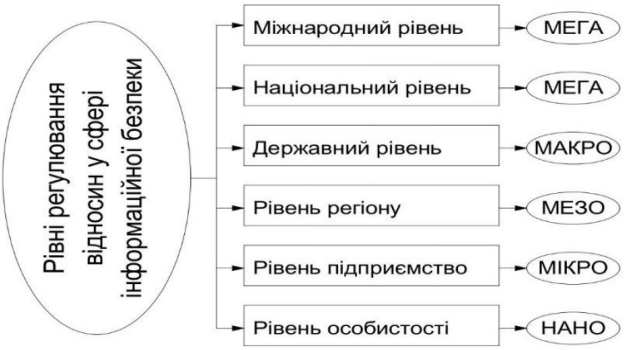


Рис. 1. Багаторівневий підхід у сфері забезпечення інформаційної безпеки

Джерело: [3].

З поняттям стохастичності тісно пов'язані явища флуктуації та біфуркації. Так, І. А. Пригожин вважає, що всі системи містять підсистеми, котрі постійно флуктуються. Іноді окрема флуктуація, або комбінація флуктуацій можуть стати настільки сильними, що попередня організація системи не витримує і руйнується. У цей переломний момент, який називають точкою біфуркації, принципово неможливо передбачити в якому напряму буде відбуватись подальший розвиток системи: чи стане ще більше хаотичним, чи перейде на новий більш високий рівень організації, який І. А. Пригожин [8] назвав дисипативною структурою.

Яскравим прикладом таких явищ слугують випадки неузгодженості складних технічних систем та інформаційних підсистем, якими вони наповнені. Іншими словами, між технологічною та інформаційною підсистемами системи безпеки в таких складних конструкціях була відсутня, як зазначається в основному принципі синергетики, взаємодія. Це часто спричиняє технічні збої та техногенні катастрофи. Останні наукові дослідження в галузі теорії синергетики стверджують, що саме синергетична концепція може стати науковим підґрунтям гармонічної взаємодії між технологічною та інформаційною підсистемами безпеки складних систем, і такою, що спроможна прогнозувати їх біфуркаційні стани, адже саме біфуркації різного виду та атрактори здебільшого призводять до катастроф та руйнування систем.

Дедалі більше науковців [5, 9] схиляються до думки, що вже саме поняття інформації тісно пов'язане з поняттям ентропії

(принцип мінімуму ентропії також основний в синергетичній теорії).

У наукових дослідженнях виокремлюється поняття — «інформаційна ентропія» — невизначеність інформаційної системи, зокрема, непередбачуваність появи деякого символу первинного алфавіту. В останньому за відсутності інформаційних втрат ентропія чисельно дорівнює кількості інформації на символ повідомлення, яке передається.

Принцип мінімуму ентропії відкритої системи (рівня її хаотичного стану) у стаціонарному стані є найважливішим результатом нерівноважної термодинаміки, оскільки пропонує цілісний критерій встановлення стаціонарного стану. Цей принцип ґрунтується, зокрема, на теорії Пригожина: у стаціонарному стані, близькому до термодинамічної рівноваги, значення швидкості продукції ентропії системи за рахунок необоротних процесів досягає відмінного від нуля постійного мінімального значення:

$$\sigma = \frac{dS}{dt} \to \min.$$

Критерієм наближення відкритої системи до стаціонарного стану слугує від'ємний знак похідної від продукції ентропії за часом.

З властивостей ентропії випливає, що вона за змістом є мірою невизначеності стану фізичної системи. Природньо, що при цьому кількість інформації можна вимірювати зменшенням ентропії системи, для уточнення стану якої і призначена власне ця інформація. Тому як об'єкт, про який передається інформація, в теорії інформації взято фізичну систему, яка має певний рівень невизначеності. Отже, інформаційна ентропія — це міра хаотичності інформації, чи міра внутрішньої невпорядкованості інформаційної системи. Ентропія збільшується у разі хаотичного розподілу інформаційних ресурсів і зменшується під час їх упорядкування. Інколи інформацію розглядають як від'ємну ентропію.

Звідси в теорії інформації рівнем апріорної невизначеності системи і застосовується ентропія та відома формула

$$H(X) = -\sum_{i=1}^{n} p_i log(p_i), \qquad (1)$$

де $H(X)$ — ентропія деякої інформаційної системи X; $x_i, i = \overline{1,n}$ — скінченна множина станів, в яких система розташована ($X \approx x_i$: подія, коли система X перебуває у стані $x_i, i = \overline{1,n}$); $p_i, i = \overline{1,n}$ — імовірність події, $\sum_{i=1}^{n} p_i = 1$.

Отже, простежується тісний зв'язок між властивостями інформаційної безпеки та основними синергетичними принципами.

Моделювання процесу забезпечення інформаційної безпеки з врахуванням ентропії системи. Розглянемо інформаційну систему як дисипативну та поставимо перед собою мету — досягти стійкого функціонування та забезпечення потрібного рівня її безпеки. Як відомо, за результатами досліджень І. Пригожина [8], саме для відкритих дисипативних систем характерним буде зменшення ентропії. Очевидно, що систему забезпечення інформаційної безпеки можна розглядати як відкриту систему.

Зауважимо, що у закритих системах процес дисипації відбувається лише як процес неперервної дезорганізації, хаотизації, руйнування початково заданої структури, що свого часу й встановила класична термодинаміка, яку ще іноді називають теорією руйнування структур.

У відкритих системах за умов стійкого обміну інформацією з навколишнім середовищем зміну ентропії можна подати у вигляді суми двох доданків: $\frac{dS_1}{dt}$ та $\frac{dS_2}{dt}$. Перший із них визначає зовнішні процеси (потік ентропії), а другий обумовлений внутрішніми процесами, які відбуваються в самій системі (виробництво ентропії):

$$\frac{dS}{dt} = \frac{dS_1}{dt} + \frac{dS_2}{dt}, \qquad (2)$$

де $\frac{dS_1}{dt}$ – потік ентропії; $\frac{dS_2}{dt}$ – виробництво ентропії.

У дослідженнях І. Пригожин зазначав, що саме у відкритих системах значення ентропії може бути довільного знаку. Справді, перший доданок: $\frac{dS_1}{dt}$ може бути більше нуля $\left(\frac{dS_1}{dt} > 0\right)$ або дорівнювати нулю $\left(\frac{dS_1}{dt} = 0\right)$. Другий же доданок може набувати як додатні, так і від'ємні значення $\left(\frac{dS_2}{dt} > 0 \text{ або } \frac{dS_2}{dt} < 0\right)$.

Звідси можна зробити висновок, що у відкритій дисипативній системі саме за рахунок другого доданку у (2) загальна зміна ентропії може бути від'ємною.

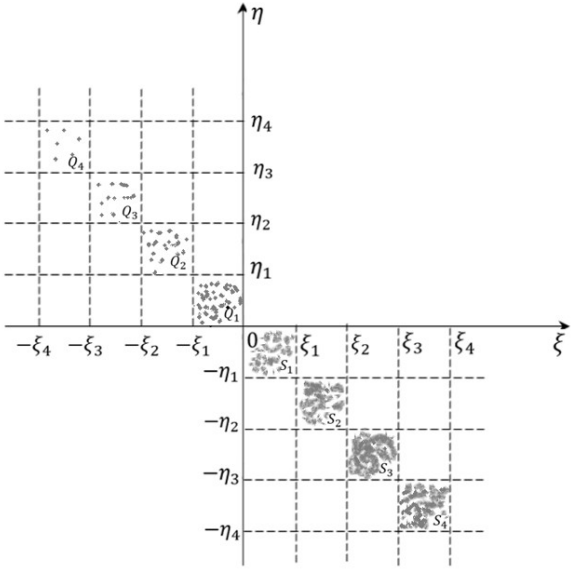
Ситуація, за якою зміна ентропії у відкритій системі $\frac{dS}{dt} < 0$, характеризує дисипативну систему.

Далі слід проаналізувати внутрішні зміни у системі, так щоб уможливити зменшення хаосу, спрогнозувати безпечні та стійкі

робочі режими її функціонування та на практиці досягнути потрібного рівня її безпеки загалом.

Для чіткого розуміння впливу процесів ентропії на рівень забезпечення захисту інформаційної системи подамо в умовних координатах (рис. 2): Oξ — вісь зміни ентропії інформаційної системи; Oη — вісь рівнів забезпечення інформаційної безпеки залежно від ступеня реалізації потенційних загроз.

Умовно, вісь Oη відділяє від'ємну та додатно ентропії інформаційної системи, а вісь Oξ — безпечні та небезпечні зони її функціонування. Можна вважати, що у точці O відбувається балансування системи від нестійкого до стійкого стану, тобто точка O — точка рівноваги системи.



$Q_1 - Q_2$: зона загроз, забезпечення ІБ
$Q_3 - Q_4$: зона безпеки
$S_1 - S_2$: зона небезпеки
$S_3 - S_4$: зона втрат та руйнувань

Рис. 2. Залежність рівня забезпечення інформаційної безпеки від процесів ентропії у системі

Джерело: розроблено авторами.

Проаналізуємо стан функціонування інформаційної системи в правій півплощині від осі Oη, коли ентропія додатна. На проміжну $[0; \xi_1]$ кількість ентропії ще недостатньо велика. Проте інформаційна система потрапляє до зони небезпеки (S_1). Це середовище підвищеного ризику та можливості загроз функціонування

системи. У цій зоні кількість ентропії може як збільшуватися, так і зменшуватися, тому розвиток системи має ймовірнісний характер. Так, зі збільшенням ентропії — небезпека наростає і система переходить в зону S_2. Поки що для функціонування системи немає катастрофічних наслідків і можна вжити заходи і протидіяти загрозам із приведенням самої системи до стану рівноваги.

Проте зі збільшенням ентропії система переходить до зони S_3 ($\xi \in [\xi_2; \xi_3]$) — зону руйнування і втрат. Наростання хаосу, у нашому випадку — невпорядкованої інформації, призводить до значних змін у структурі системи, за яких повернути систему до вихідного стану стає неможливим. Майже зруйнована, зі зміненою структурою система потрапляє в зону S_4 — зону кінцевого руйнування. Зауважимо, що саме тут, поряд з остаточним руйнуванням системи, цілком можливі й ефекти самоорганізації системи: прояви нових зародків її абсолютно нової організації, структури та властивостей, що стане предметом подальших наших досліджень.

Проаналізуємо стан функціонування інформаційної безпеки зліва від осі 0η, коли ентропія від'ємна. Зауважимо, що це буває лише у відкритих складних дисипативних структурах.

Наприклад, на проміжку $[-\xi_1; 0]$ ентропія вже від'ємна, однак система ще перебуває в зоні загроз, оскільки характер ентропії може змінитися в будь-який момент. Розташування у цій зоні вказує на рівень загроз на стан інформаційної безпеки загалом, які можуть вплинути за цілеспрямованих дій інших об'єктів. Саме ця зона вимагає найпильнішої уваги з боку суб'єктів безпеки, оскільки характер сучасних загроз в кіберпросторі має непередбачуваний асиметричний характер. Саме тут будуть найефективнішими стабілізаційні заходи, спрямовані на пом'якшення впливу дестабілізуючих на інформаційну систему вчинків. Проведення таких заходів напрямлене на те, щоб система інформаційної безпеки повинна мати таку структуру, щоб дозволило їй знищувати негативні прояви зовнішнього середовища: воно має або не пропускати зовнішні збурення, або відходити від них в безпечнішу зону Q_2, а потім у Q_3 — зону безпеки. Стан безпеки інформаційної системи зумовлює надійну її захищеність та збереження інформації. В цій зоні структурним елементам системи вже не загрожують дестабілізуючі впливи — усі показники перебувають у межах допустимих значень та мають стійку тенденцію до покращення.

Окремо варто вказати на поведінку в системі Q_4 — близької до ідеальної. За таких умов в ній повністю відсутній хаос. Це

означає, що інформація в інформаційних джерелах відсутня повністю, наприклад, — повністю зникли записи в банківських операціях, що неможливо в реальному інформаційному просторі. Можна, за таких умов, зробити припущення, що система знову стає замкненою і процес має циклічний характер. Проте, це вже тема наступних наукових розвідок.

Отже, доходимо висновку, що наведений підхід зонування залежно від кількості та знаку ентропії є, на нашу думку, необхідним для виокремлення та специфікації безпечних та стійких робочих режимів функціонування інформаційної системи, які на практиці дозволяють забезпечити потрібний рівень безпеки. Моніторинг зміни ентропії є необхідним і доцільним для підтримки стійкості і безпеки функціонування інформаційних систем загалом.

Висновки та перспективи подальших наукових розвідок. У роботі на основі системного та синергетичного підходів розвинуто методологію функціонування інформаційної системи в сучасних умовах кіберзагроз. Представлення інформаційної безпеки як відкритої, складної і дисипативної системи уможливлює використовувати в її дослідженні теорії інформаційної ентропії та моделювати зони загроз в процесі її функціонування залежно від характеру ентропії.

Подальші наукові розвідки пов’язані з вивченням процесів самоорганізації в інформаційних системах у біфуркаційних станах і математичного моделювання їх прогнозування.

Бібліографічні посилання

1. Баландіна Н.М. Підхід до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації. *Вісник Черкаського державного технологічного університету*. *Технічні науки*. 2019. С.57-66.

2. Грабар І.Г., Грищук Р.В., Молодецька К.В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. За заг. ред. д.т.н., проф. Р. В. Грищука. Житомир: ЖНАЕУ, 2019. 280 с.

3. Джалладова І., Батечко Н., Коломієць-Людвіг Є. Системний підхід до аналізу нормативно-правового забезпечення інформаційної безпеки. *Social development & Security*. 2018. Vol. 7. Iss. 5. С. 3–20.

4. Дзьобань О.П., Панфілов О.Ю., Чемчикаленко Р.А. Методологічний контекст дослідження проблеми інформаційної безпеки. Зовнішня торгівля: економіка, фінанси, право. 2014. № 2. С. 171-180.

5. Brillouin L. Science and Information Theory. Second Edition. *Dover Publications.* 2013. July 17. 368 p.

6. Hermann Haken. Synergetics. Springer — Verlag Berlin, Heidelberg, New York*, 1978, 383p.*

7. Hryshchuk R., Yevseiev S. The synergetic approach for providing bank information security: the problem formulation. *Ukrainian Scientific Journal of Information Security*. 2016. vol. 22. issue 1. p. 64-74.

8. Prigogine I, Stengers I, Order Out of Chaos: Man's New Dialogue with Nature by Ilya Prigogine, Isabelle Stengers, Alvin Toffler (Foreword). Heinemann. London. 1984. 432 p.

9. Shannon, Claude Elwood (July 1948). A Mathematical Theory of Communi-cation. B*ell System Technical Journal*. 27(3): 379–423p.

10. Ulieru M. (2003). Emergence in Cyberspace: Towards the Evolutionary Self-Organizing Enterprise. In: Carbonell, J.G., Siekmann, J., Kowalczyk, R., Müller, J.P., Tianfield, H., Unland, R. (eds) Agent Technologies, Infrastructures, Tools, and Applications for E-Services. NODe 2002. Lecture Notes in Computer Science, vol 2592. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36559-1_3.

Статтю подано до редакції 29.11.2022