2. Рубан В.В. Цифровий маркетинг: роль та особливості використання. *Економічний вісник Запорізької державної інженерної академії*. 2017. Вип. 2–2(08). С. 20–25.

3. Агутін М. М. Математичне моделювання рекламного просування веб-проекту / Агутін М. М., Дем'яненко В. В., Потапенко С. Д. *Моделювання та інформаційні системи в економіці : зб. наук. пр.* МОН України, ДВНЗ «Київ. нац.екон. ун-т ім. Вадима Гетьмана». Київ : КНЕУ, 2020. Вип. 100. С. 29–38.

4. Simon Kingsnorth, Digital marketing strategy: an integrated approach to online marketing, Kogan Page Publishers, 2019.

Статтю подано до редакції 16.11.2020

УДК: 355.451:004.7 DOI 10.33111/mise.101.2

Батечко Н.Г. д. педаг. наук, к. фіз. – мат. наук, доцент,
професор кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»
Ващаєв С.С. к.е.н., доцент,
доцент кафедри математичного моделювання та статистики,
ДВНЗ «КНЕУ імені Вадима Гетьмана»
Лютий О.І. к.т.н., доцент,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Batechko N.G., Doctor of Sciences in Pedagogy, PhD in Mathematics,
Professor of the Department of Computer Mathematics
and Information Security,
SHEI KNEU named after V. Hetman
Vashchaiev S.S., PhD in Economics,
Associate Professor of the Economic
and Mathematical Modelling Department,
SHEI KNEU named after V. Hetman
Liutyj O.I., Candidate of Technical Sciences,
Associate Professor of the Computer Mathematics
and Information Security Department,
SHEI KNEU named after V. Hetman

МЕТОДОЛОГІЯ СИСТЕМНОГО АНАЛІЗУ ПОЛІТИКИ КІБЕРБЕЗПЕКИ В ЦИФРОВОМУ СУСПІЛЬСТВІ

METHODOLOGY OF SYSTEM ANALYSIS OF CYBER SECURITY POLICY IN DIGITAL SOCIETY

Анотація. *Сучасна безпекова ситуація як в Україні, так і у світі щороку суттєво змінюється з'являються нові загрози та виклики, які все важче долати на локальному рівні. У статті запропоновано та обґрунтовано концепцію, яка на думку авторів, для того, щоб зрозуміти та виокремити*

фактори, які зумовлюють виникнення та загострення кіберзагроз варто підійти до вивчення проблеми за допомогою системного аналізу, розглядаючи кібернетичну безпеку як складне системне утворення зі складними зовнішніми та внутрішніми зв'язками. Кібербезпека подається як системне утворення. Дослідження у сфері системного аналізу надають змогу виокремити наукові підходи щодо феномену кібербезпеки безпосередньо та поліпшити її реалізації, зокрема. Актуальним є як кібернетичний (структуралістський) підхід, коли особлива увага приділяється структурним характеристикам досліджуваної системи, так і підхід, відповідно до якого є важливими і функції, притаманні системі, як: відкритість, лінійність чи, наприклад, стаціонарність. У роботі сучасними методами системного аналізу подано методологію кібербезпеки, як багатогранного утворення, невід'ємного складника національної безпеки. Ця складова частина характеризує стан захищеності національних інтересів від зовнішніх і внутрішніх загроз в інформаційній сфері. Водночас, аналіз подано із застосуванням логіко-структурних зв`язків, що поєднують інформаційно-психологічні та інформаційно-технологічні підсистеми кібербезпеки.
Ключові слова: *кібербезпека; кібервійна; системний аналіз; цифрове суспільство; соціологія знання*

Abstract. *The process of formation of the digital society has become one of the most global processes of mankind for the entire period of its existence. The current security situation in both Ukraine and the world is changing significantly every year, new threats and challenges are emerging that are increasingly difficult to overcome at the local level. The article proposes and substantiates the concept, which according to the authors, in order to understand and identify the factors that cause the emergence and exacerbation of cyber threats should approach the study of the problem through systems analysis, considering cyber security as a complex system with complex external and internal connections. languages.*

Cybersecurity is presented as a systemic entity. Research in the field of systems analysis makes it possible to identify scientific approaches to the phenomenon of cybersecurity directly and improve its implementation, in particular. Both the cybernetic (structuralist) approach, when special attention is paid to the structural characteristics of the system under study, and the approach according to which the functions inherent in the system, such as openness, linearity or, for example, stationarity, are important, are relevant. The modern methods of system analysis present the methodology of cybersecurity as a multifaceted entity, an integral part of national security. This component characterizes the state of protection of national interests from external and internal threats in the information sphere. At the same time, the analysis is presented with the use of logical-structural connections that combine information-psychological and information-technological subsystems of cybersecurity.
Keywords: *cybersecurity; cyberwar; system analysis; didgital society; sociology of knowledge*

Вступ. Процес формування цифрового суспільства став одним із найглобальніших процесів людства за весь період його існування. Утім, небачене досі поширення інформаційно-комунікаційних технологій, окрім очевидних переваг, призвело до низки проблем, зумовлених дедалі більшою вразливістю інформаційного простору щодо стороннього впливу. Останнім часом в Україні все частіше вчиняються масштабні злочини інформаційного характеру, які загрожують сталому та безпечному функціонуванню інформаційно-комуніка-

ційних систем, а отже загрожують економічний, політичній, духовній життєдіяльності суспільства. Про високий рівень загроз у кібернетичному просторі України свідчать результати дослідження відомого німецького оператора Deutsche Telecom: Україна знаходиться на четвертій сходинці світового рейтингу — об'єктів і джерел кібернетичних атак [2]. Тому, цілком природньо постала необхідність створення надійної системи кібернетичної безпеки, яка б уможливила контроль та врегулювання відносин в інформаційному просторі та й в цифровому суспільстві загалом.

Зауважимо, що сучасна безпекова ситуація як в Україні, так і у світі щороку суттєво змінюється з'являються нові загрози та виклики, які все важче долати на локальному рівні. У результаті відсутності дієвої системи забезпечення інформаційної безпеки у національному інформаційному просторі України спостерігається велика кількість негативних явищ, які створюють реальні та приховані загрози інформаційній безпеці громадянина, суспільству та державі [1]. Тому, все більшої актуальності набуває створення ефективної кібербезпекової політики, яка б враховувала ці аспекти та уможливила б системне бачення досліджуваної проблеми.

Політика кібербезпеки держави як підсистема національної безпеки держави. Кібербезпека, як багатогранне утворення, є невід'ємним складником національної безпеки, оскільки характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх і внутрішніх загроз. Водночас, варто вказати на інформаційно-психологічні та інформаційно-технологічні системи кібербезпеки, як складові національної безпеки держави. Кібербезпека є інтегрованою складовою національної безпеки (рис. 1) поряд з політичною, економічною, екологічною, військовою, гуманітарною.

Розуміння ролі і значення кібербезпеки в системі національної безпеки України уможливить передбачення кіберзагроз, як внутрішніх, так і зовнішніх. Як влучно висловився 37-й Президент Сполучених Штатів Америки: "Один долар, вкладений в інформацію і пропаганду, цінніший, ніж 10 доларів, вкладених у створення систем зброї, бо остання навряд чи буде вжита, в той час як інформація працює щохвилинно і повсюдно".

Як стверджують фахівці корпорації Gartner: витрати на інформаційну безпеку у світі щорічно зростають приблизно на 8,2 %. За їх прогнозами у 2020 році їх обсяг мав сягнути 170 млрд дол. США [2]. Забезпечення інформаційної безпеки завдяки послідовній, грамотно сформульованій національній стратегії у свою

чергу може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військовій, соціальній, економічних та інших сферах і зможе суттєво вплинути, на нашу думку, на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів.

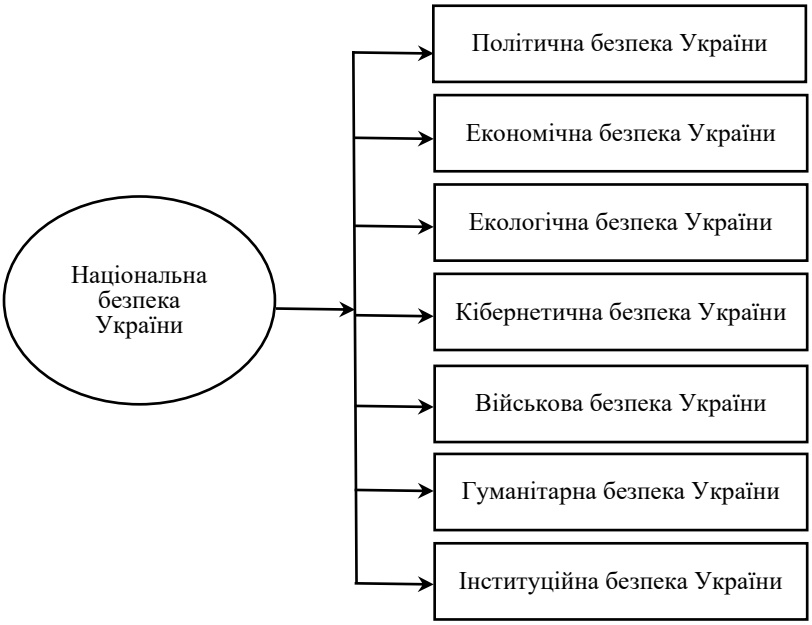


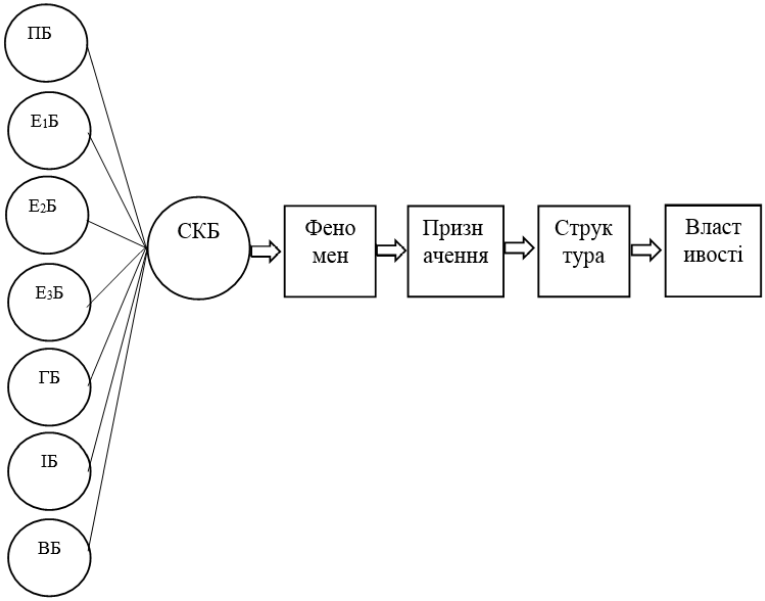
Рис. 1. Кібербезпека України
як складова національної безпеки держави

На думку авторів, для того, щоб зрозуміти та виокремити фактори, які зумовлюють виникнення та загострення кіберзагроз, варто підійти до вивчення проблеми за допомогою системного аналізу, розглядаючи кібернетичну безпеку як складне системне утворення зі складними зовнішніми та внутрішніми зв'язками.

Основні результати. Кібербезпека як системне утворення. Дослідження у сфері системного аналізу надасть змогу виокремити наукові підходи щодо феномену кібербезпеки безпосередньо та поліпшити її реалізації, зокрема. Зауважимо, що для нас буде актуальним як кібернетичний (структуалістський) підхід, коли особлива увага приділяється структурним характеристикам досліджуваної системи, так і підхід, відповідно до якого є важли-

вими і функції, притаманні системі, як от: відкритість, лінійність чи, наприклад, стаціонарність.

Використаємо основні класичні системні принципи: цілісність, структурність, ієрархічність, множинність опису, взаємозалежність системи і середовища. Оскільки кібербезпека тісно пов'язана з іншими структурними компонентами національної безпеки, то вважаємо, що саме ці зовнішні взаємозв'язки і формують феномен системи кібербезпеки, її призначення, структуру та властивості (рис. 2).



ПБ — політична безпека
E_1Б — економічна безпека
E_2Б — економічна безпека
E_3Б — енергетична безпека
ГБ — гуманітарна безпека
ІБ — інституційна безпека
ВБ — військова безпека
СКБ — система кібербезпеки

Рис. 2. Формування системи кібербезпеки

З позицій системно-структурного підходу дослідимо послідовні аспекти та закономірності створення системи кібербезпеки, які обумовлять основні принципи її подальшого функціонування. З'ясуємо спочатку феномен системи кібербезпеки, тобто її тип і внутрішню сутність.

Система кібербезпеки є відкритою, оскільки постійно мати контакт з довкіллям, іншими структурними компонентами національної безпеки (рис. 2), обмінюється з ними інформацією та енергією. У ній відбувається постійний динамічний рух, відчувається надходження зовнішньої енергії у вигляді позитивних факторів і деструктивних імпульсів, таких як кіберзагрози. Таке тлумачення системи кібербезпеки є надзвичайно важливим, оскільки: в замкнених системах з великою кількістю елементів виконується другий закон термодинаміки, сутністю якого є той факт, що ентропія S (міра хаоса) з часом зростає чи залишається сталою:

$$\Delta S \geq 0,$$

тобто хаос у замкненій системі не зменшується, а може лише зростати. Зауважимо, що всі штучно створені системи можна вважати відкритими, оскільки в них діють суб'єктивні закони, принципи та правила. Саме властивість відкритості, на нашу думку, дозволяє еволюціювати системі кібербезпеки, розгортати програму ієрархічного зростання, обмінюючись енергією, інформацією з іншими рівнями своєї еволюції та навколишнім середовищем.

Завдяки відкритості та обміну з навколишнім середовищем, постійне надходження зовнішньої енергії у вигляді кіберзагроз спочатку стимулюють її розвиток. Проте постійна стохастичність і мінливість призводить до появи флуктуацій і явищ біфуркацій. Так, зокрема, І.А. Пригожин вважає, що всі такі системи містять підсистеми, котрі постійно флуктуюються. Справді, постійний обмін інформацією призводить до появи, спочатку, незначних кіберзагроз. Проте, іноді, окрема флуктуація або їх комбінація можуть стати настільки сильними, що попередня організація системи не витримує і руйнується. Ми всі неодноразово були свідками руйнування ІТ-комплексів унаслідок потужних атак хакерів як на рівні окремого підприємства, так і державних установ. У цей переломний момент, який ще називають точкою біфуркації, принципово неможливо передбачити, в якому напрямі буде розвиватися система: чи стане її подальше існування хаотичнішим, чи перейде на новий, вищий рівень організації, який І.А. Пригожин назвав дисипативною структурою [3]. Усі ці явища можна спостерігати у функціонуванні системи кібербезпеки.

Наведені міркування безпосередньо стосуються стійкості системи. Будемо вважати, що стан, траєкторія чи програма системи — нестійка, якщо довільні як завгодно малі відхилен-

ня від них з часом збільшуються. Якщо це має місце лише для деяких типів відхилень, то можна говорити про часткову нестійкість. Саме точки біфуркаціїї системи пов'язані з її нестійкими станами.

Таким чином, систему кібербезпеки можна вважати відкритою, динамічною системою, в якій відчувається нестійкий рух, обмін інформацією та енергією з оточуючим навколишнім середовищем у вигляді як позитивних факторів — лояльних інформаційних потоків, так і збурюючих — деструктивних, які несуть небезпеку і загрози стійкості системи та приводять її до біфуркаційних станів.

Стосовно призначення системи кібербезпеки (рис. 2), то варто вказати, що вона здатна ефективно протидіяти негативним проявам і деструктивним чинникам, виконуючи інформаційну, аналітико-праностичну та превективну функції.

Структурними компонентами системи кібербезпеки є: об'єкт безпеки, суб'єкт безпеки, механізм реалізації кібербезпеки в самій системі. Всі компоненти системи кібербезпеки пов'язані між собою прямими та зворотними зв'язками, мають певні рівні ієрархії, які можна дослідити за допомогою багаторівневого підходу [4].

Реалізація механізму забезпечення та функціонування кібербезпеки. Для розуміння функціонування системи кібербезпеки подамо її в умовній системі координат (рис. 3). За вісь ОЄ розглянемо періоди функціонування системи залежно від виникнення потенційних загроз і впливу деструктивних факторів. За вісь Оŋ розглянемо рівень стійкості системи кібербезпеки зазначеним фактором.

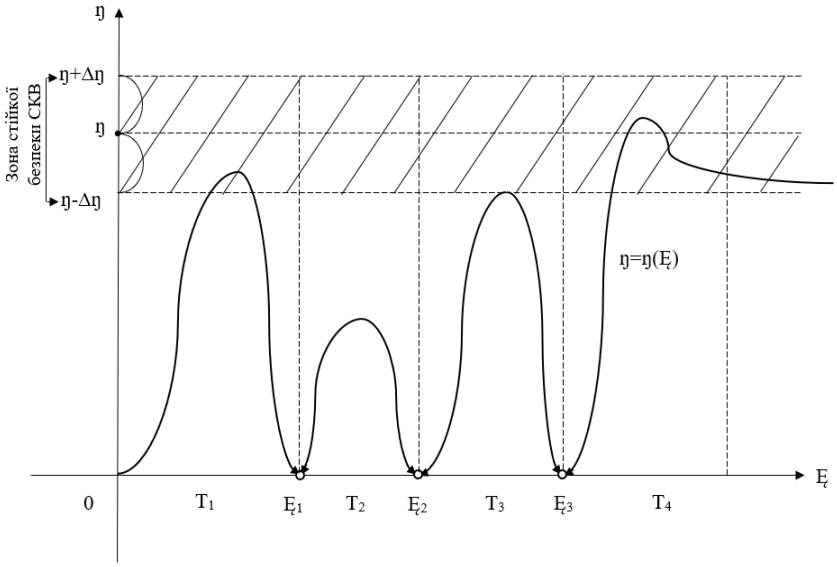
Період T_1 — характеризується надмірним функціонуванням системи кібербезпеки. Проте, внаслідок накопичення інформації та зростання хаосу виникають потенційні загрози, що призводить досить стійку систему в нерівноважений стан. У точці $Ę_1$ цього періоду система досягає біфуркаційного стану, в якому вона не лише довго перебуває і вимушена перейти в інший стан (період T_2).

Зауважимо, що на рис. 3 точку біфуркації $Ę_1$ ми показали як точку розриву досліджуваної функціональної залежності, вказуючи тим самим, що переходу до періоду T_2 може і не відбутися.

Підкреслюючи значимість точки, В.Г. Буданов зазначає, що лише в них можна несиловим, інформаційним способом, тобто як завгодно малою дією, вплинути на вибір поведінки системи, на її долю [5].

У період T_2 відбувається найбільший вплив на систему кібербезпеки зовнішніх дестабілізуючих факторів. Наростання хаосу призводить до руйнування системи та втрати як внутрішніх, так і

зовнішніх зв'язків між її компонентами та оточуючим середовищем. Суб'єкти безпеки у цей період оцінюють розміри заподіяної шкоди та підраховують суми завданих матеріальних, фінансових і соціальних збитків. На цьому етапі система кібербезпеки набуває нового біфуркаційного стану і відхилення її від зони стійкості є максимальним.



T_1 — період небезпеки та загроз у функціонуванні СКБ
T_2 — період витрат та завданих збитків у функціонуванні СКБ
T_3 — період стабілізації у функціонуванні СКБ
T_4 — період стійкої безпеки у функціонуванні СКБ

Рис. 3. Синергетична модель функціонування СКБ по періодах стійкості

Під час третього періоду відновлення всередині системи виникають осередки самоорганізації та дисипативні структури. Водночас вони зумовлюють побудову нових зв'язків між компонентами системи та зумовлюють її перехід до нового етапу розвитку. У цей період варто проаналізувати виявлені загрози, вивчити їх вплив на систему кібербезпеки загалом і всі її компоненти зокрема. Саме у цей період варто проводити стабілізаційні заходи, зокрема, на рівні держави, які б уможливили пом'якшення результатів впливу кіберзагроз. Сформулюємо отриманий результат у вигляді теореми:

Теорема. *У період T_4, унаслідок проведених стабілізаційних заходів система кібербезпеки входить у зону стійкої безпеки, в якій і залишається надалі:*

$$\lim_{E_i \to x} \eta(E_i) = \eta * \ .$$

У цей період стан кібербезпеки надає надійну захищеність життєво важливих інтересів держави: економічних, військових, екологічних і т.д., тобто усіх сфер життєдіяльності суспільства.

У цей період важливими є заходи на посилення аналітико-прогностичних досліджень, які б уможливили стабільний розвиток системи кібербезпеки.

Висновок. У роботі сучасними методами системного аналізу подана методологія кібербезпеки, як багатогранного утворення, невід'ємного складника національної безпеки. Ця складова частина характеризує стан захищеності національних інтересів від зовнішніх і внутрішніх загроз в інформаційній сфері. Водночас, аналіз подано із застосуванням логіко-структурних зв»язків, що поєднують інформаційно-психологічні та інформаційно-технологічні підсистеми кібербезпеки.

Бібліографічні посилання

1. Гаращенко Ю.В. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2019. Том 30 (69). С. 140 — 145.

2. Микитенко Т.В., Петровська І.О., Рогов П.Д. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в Укросучасних умовах. *Збірник наукових праць Центру воєнно — стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2014. №1. С. 24 –31.

3. Пригожин И. Порядок из хаоса. Новый диалог человека с природой. М.: Ком. Книга. 2008. 296 с.

4. Джалладова І., Батечко Н., Коломієць-Людвиг Є. Системний підхід до аналізу нормативно-правового забезпечення інформаційної безпеки. *Social Development & Security*. 2018. Vol. 7. №5. С. 3-20.

5. Буданов В.Г. Трансдисциплинарное образование, технологии и принципы синергетики. *Синергетическая парадигма: многообразие поисков и подходов: Сб. ст.* М. 2000. Прогресс-Традиции. С. 285-304.

Статтю подано до редакції 17.11.2021