УДК 519.8:004.056
JEL: C53; D89; G29; L86
DOI: https://doi.org/10.32983/2222-4459-2023-11-180-187

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ ОРГАНІЗАЦІЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

©2023 КАРПЕНКО О. О., РАБЧУН А. О.

УДК 519.8:004.056
JEL: C53; D89; G29; L86

Карпенко О. О., Рабчун А. О. Математичне моделювання управління ресурсами захисту в системах інформаційної безпеки фінансових організацій в умовах гібридних загроз

Стаття присвячена математичному моделюванню при проєктуванні адаптивних систем у галузі інформаційної безпеки фінансових організацій. Досліджуються ключові виклики, що виникають у зв'язку з гібридними загрозами, в умовах становлення інформаційної економіки, стрімкого розвитку електронних платежів у фінансовій сфері та постійних інформаційних кібератак в умовах російсько-української війни. У статті наведено математичну модель, розроблену на основі моделі Гросса для оцінки рівня інформаційної безпеки фінансових організацій за різних умов функціонування. Спеціальну увагу приділено ролі моделі в оптимізації розподілу ресурсів захисту для забезпечення надійності інформаційної безпеки в умовах реального часу. Запропонований підхід дозволить досягнути раціонального розподілу ресурсів захисту при побудові адаптивних систем інформаційної безпеки, що збільшить ефективність захисту від гібридних загроз. Стаття пропонує конкретну модель для оцінки інформаційної безпеки фінансових організацій, включно з важливим аспектом вибору критеріїв та встановлення пріоритетів. Відзначається, що ефективний розподіл ресурсів захисту є ключовим пріоритетом управління інформаційною безпекою; підкреслено його важливість для забезпечення захисту від гібридних загроз у сучасних реаліях інформаційного економічного середовища.

Ключові слова: *гібридні загрози, розподіл ресурсів захисту, модель Гросса, інформаційна безпека, адаптивна система, фінансові організації, оцінка рівня інформаційної безпеки.*
Рис.: *3.* ***Формул:*** *3.* ***Бібл.:*** *16.*

Карпенко Оксана Олександрівна *– доктор економічних наук, професор, професор кафедри менеджменту, маркетингу та публічного адміністрування, Міжнародний науково-технічний університет імені академіка Юрія Бугая (пров. Магнітогорський, 3, Київ, 02660, Україна)*
E-mail: *o.karpenko@istu.edu.ua*
ORCID: *https://orcid.org/0000-0003-2943-1982*
Researcher ID: *https://www.webofscience.com/wos/author/record/F-2435-2017*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=56509240700*

Рабчун Андрій Олександрович *– кандидат технічних наук, докторант, Міжнародний науково-технічний університет імені академіка Юрія Бугая (пров. Магнітогорський, 3, Київ, 02660, Україна)*
E-mail: *rabchunandrew@gmail.com*
ORCID: *https://orcid.org/0009-0002-1389-1263*

UDC 519.8:004.056
JEL: C53; D89; G29; L86

Karpenko O. O., Rabchun A. O. Mathematical Modeling of Protection Resource Management in Information Security Systems of Financial Organizations in the Context of Hybrid Threats

The article is devoted to mathematical modeling in the design of adaptive systems in the field of information security of financial organizations. The key challenges arising in connection with hybrid threats, in the context of the formation of the information economy, the rapid development of electronic payments in the financial sector, and constant information cyberattacks in the context of the russian-Ukrainian war are studied. The article presents a mathematical model developed on the basis of the Gross model for assessing the level of information security of financial organizations under different conditions of functioning. Particular attention is paid to the role of the model in optimizing the allocation of protection resources to ensure the reliability of information security in real time. The proposed approach will allow to achieve a rational allocation of protection resources in the construction of adaptive information security systems, which will increase the effectiveness of protection against hybrid threats. The article proposes a specific model for assessing the information security of financial institutions, including an important aspect of choosing criteria and setting priorities. It is noted that the effective allocation of protection resources is a key priority of information security management; its importance for ensuring protection against hybrid threats in the modern realities of the information and economic environment is emphasized.

Keywords: *hybrid threats, allocation of protection resources, Gross model, information security, adaptive system, financial institutions, assessment of the level of information security.*
Fig.: *3.* ***Formulae:*** *3.* ***Bibl.:*** *16.*

Karpenko Oksana O. *– D. Sc. (Economics), Professor, Professor of the Department of Management, Marketing and Public Administration, Academician Yuriy Bugay International Scientific and Technical University (3 Mahnitohorskyi Ln , Kyiv, 02660, Ukraine)*
E-mail: *o.karpenko@istu.edu.ua*
ORCID: *https://orcid.org/0000-0003-2943-1982*
Researcher ID: *https://www.webofscience.com/wos/author/record/F-2435-2017*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=56509240700*

Rabchun Andrii O. *– PhD (Engineering), Candidate on Doctor Degree, Academician Yuriy Bugay International Scientific and Technical University (3 Mahnitohorskyi Ln , Kyiv, 02660, Ukraine)*
E-mail: *rabchunandrew@gmail.com*
ORCID: *https://orcid.org/0009-0002-1389-1263*

Україна вступила в період глибоких економічних перетворень, пов'язаних з рухом до повноцінного членства в ЄС. Здійснюється курс на органічне включення економіки країни до системи європейського та світового господарства. Крім того, суттєвих змін зазнає діяльність підприємств і фінансових організацій в умовах стрімкого розвитку інформаційної економіки. Також в умовах російсько-української війни вітчизняні підприємства та фінансові організації щоденно стикаються з проблемами забезпечення безпеки й ефективності функціонування на тлі різноманітних гібридних загроз – техногенного, природного та військового характеру, що створює нове економічне середовище – середовище підвищеного ризику. Все це обумовлює значну увагу до забезпечення інформаційної безпеки як фінансової системи України загалом, так і окремих фінансових організацій.

Серед усього переліку гібридних загроз, за кваліфікацією Європейського центру передового досвіду з протидії гібридним загрозам (також відомого як *Hybrid Centre of Excellence*, або *Hybrid CoE* – міжнародна мережева організація в Гельсінкі, яка також служить платформою між ЄС і НАТО), інформаційні гібридні загрози (різноманітні кібератаки) є одними з ключових і найнебезпечніших для ефективній діяльності фінансових організацій країн ЄС і НАТО [8].

Інформаційні ресурси, які використовуються у фінансовій сфері, мають критичне значення для забезпечення нормального функціонування бізнесу та збереження конкурентоспроможності.

Необхідність ефективного захисту інформації фінансових організацій обумовлена потенційними загрозами, що включають кібератаки, крадіжки конфіденційних даних, а також маніпулювання інформацією з метою нанесення репутаційних збитків. Загрози цього роду можуть призвести до серйозних фінансових втрат, втрати довіри клієнтів, порушення законодавства щодо захисту конфіденційної інформації.

Інформаційна безпека є невід'ємною складовою економічної безпеки. Захист від інформаційних загроз передбачає створення сучасних адаптивних систем захисту, здатних вчасно реагувати на потенційні ризики. Ефективна система захисту дозволить уникнути негативних економічних наслідків та зберегти стійкість і надійність фінансових організацій.

Проблеми впливу різноманітних інформаційних гібридних загроз на ефективність функціонування фінансових організацій досліджували закордонні та вітчизняні вчені, а саме: Libicki M. C., Ablon L., Webb T. [1], Rosenzweig P. [2], Radin A. [3], Blank S., Perkovich G., Levite A. E. [4], Nye S. J. [5], Hingant J., Zambrano M., Pérez F. J., Pérez I., Esteve M. [6], Iancu N., Fortuna A., Barna C., Teodor M. [7], Лапко О. О., Конарівська О. Б. [14], Веселова Л. Ю. [15], Саркісян Л. Г., Самсонова Л. В. [16]. Автори досліджують виклики та стратегії захисту від різноманітних кіберзагроз. Дослідження спрямоване на вивчення конфліктів у кіберпросторі та їхній вплив на глобальне середовище. Вивчається природа та наслідки гібридної інформаційної війни, зокрема в Балтійському регіоні. Автори пропонують аналогії для легшого розуміння кіберконфліктів. Розглядаються виклики кіберінформаційної війни та стратегії для захисту фінансових організацій країн ЄС і блоку НАТО [8]. Досліджуються уроки, вивчені під час протидії інформаційним гібридним загрозам з фокусом на досвіді України. Аналізується явище інформаційних гібридних загроз, з розкриттям їхніх складнощів та характеристик.

Метою даного дослідження є аналіз застосування моделі Гросса в галузі інформаційної безпеки фінансових організацій. У статті розглядаються ключові виклики, пов'язані з інформаційними гібридними загрозами, що спричинені сучасним економічним, геополітичним і військовим середовищем. Пропонується розроблена модель для оцінки рівня інформаційної безпеки, яка враховує вибір критеріїв, параметрів розрахунку та функціональних залежностей. Основна ідея моделі полягає в досягненні ефективного розподілу ресурсів для захисту від інформаційних гібридних загроз, зокрема в умовах реального часу. Стаття також пропонує конкретну модель для оцінки адаптивної системи інформаційної безпеки фінансових організацій, враховуючи важливий аспект вибору критеріїв та встановлення пріоритетів. Зазначається, що ефективний розподіл ресурсів захисту відіграє ключову роль управління інформаційною безпекою для захисту від інформаційних гібридних загроз.

У даній статті пропонується розроблена спеціально для фінансових організацій модель оцінки рівня інформаційної безпеки залежно від можливих етапів інформаційного протистояння. Побудова цієї моделі потребує системного підходу, що включає такі ключові кроки:

1. *Вибір оптимальних критеріїв*. Перший крок включає визначення та вибір найбільш прийнятних критеріїв для оцінки ефективності адаптивних систем інформаційної безпеки фінансових організацій. Ці критерії формують основу для подальшої моделі.
2. *Визначення параметрів розрахунку та функціональних залежностей*. Цей етап передбачає визначення конкретних параметрів і встановлення функціональних зв'язків, які будуть інтегровані в математичну модель. Ці параметри можуть охоплювати різні аспекти інформаційної безпеки, фінансової ефективності та розподілу ресурсів адаптивних систем.
3. *Установлення пріоритетів*. Важливою частиною процесу розробки моделі є призначення пріоритетів для цих параметрів. Цей крок вимагає ретельного розгляду унікальних вимог і проблем фінансової організації. Слід брати до уваги такі фактори, як потенційна

втрата даних, витрати, пов'язані із захистом від інформаційних гібридних загроз, і окупність інвестицій для витрат на безпеку. Ці пріоритети керуватимуть моделлю під час оцінки найбільш критичних аспектів інформаційної безпеки для фінансової організації.

Таким чином, розроблена модель повинна дозволяти розв'язувати основні задачі у сфері захисту інформації, які стоять перед менеджментом (управлінням) фінансової організації:

1) вибір оптимальної кількості ресурсів із зосередженням на мінімізації очікуваних витрат, пов'язаних із захистом від інформаційних гібридних загроз. Ці витрати охоплюють як ті, що пов'язані із заходами захисту інформації, так і потенційні фінансові втрати в результаті порушень безпеки. Цей процес прийняття рішень враховує відповідні вагові коефіцієнти для забезпечення комплексної оцінки;
2) поліпшення розподілу ресурсів безпеки для протидії інформаційним гібридним загрозам, які передбачають різний рівень важливості інформації, демонструють чіткі рівні вразливості та поширюються на різні захисні рівні;
3) встановлення найбільш ефективного розподілу спільних ресурсів у контексті багатогранного інформаційного конфлікту. У цьому складному середовищі кожна сторона одночасно захищає свою власну інформацію, одночасно активно намагаючись отримати дані противника. Крім того, частина цих ресурсів може бути призначена для розвідувальної діяльності;
4) оцінка стану інформаційної безпеки фінансових організацій, враховуючи потенційні дії конкурентів: Початковий крок передбачає комплексну оцінку стану інформаційної безпеки фінансових організацій. Ця оцінка бере до уваги потенційні стратегії та дії, які можуть застосувати конкуренти для порушення або компрометації цілісності даних фінансових організацій;
5) динамічне керування ІТ-ресурсами захисту, узгоджене з інформаційною безпекою фінансових організацій, коригуючи їх у режимі реального часу відповідно до умов інформаційної безпеки фінансових організацій, що розвиваються. Цей динамічний підхід гарантує, що фінансові організації можуть швидко реагувати на нові загрози, пристосовуватися до мінливих обставин і зміцнювати свій захист за потреби. Це дозволяє фінансовим організаціям залишатися проактивними в підтримці надійної позиції інформаційної безпеки.

Забезпечення ефективного розподілу ресурсів адаптивних систем для захисту від інформаційних гібридних загроз є головною відповідальністю у сфері управління інформаційною безпекою. Витоки цієї проблеми можна простежити до необхідності розробки стратегій розподілу ресурсів у контексті військового планування.

Отже, це привело до того, що відомо як проблема Гросса [9]. У задачі Гросса ми знаходимо дві протиборчі сторони, що володіють ресурсами, позначеними як X та Y. Результат їх протистояння визначається цільовою функцією, яка демонструє лінійну залежність від диспропорції в розподілених ресурсах [10]. Ця складність перетворює виклик на задачу лінійного програмування. По суті, проблема Гросса охоплює основну концепцію оптимізації розподілу ресурсів для посиленого захисту від загроз:

$$I(x,y) = \sum_{k-1}^{l} (x_k, y_k) = \sum_{k=1}^{l} g_k \max(x_k - y_k, 0), \quad (1)$$

де k – номер об'єкта, x_k та y_k – ресурси нападу та захисту на k-му об'єкті, g_k – ваговий коефіцієнт.

Якщо ми розглядаємо це питання в економічному контексті, його можна порівняти з конкурентною грою за участю двох гравців, які змагаються за домінування на ринку [10–13]. Проте коли ми переходимо до сфери інформаційної безпеки, проблема оптимізації розподілу ресурсів набуває чітких характеристик, які суттєво впливають на різні аспекти проблеми. До цих особливостей належать постановка проблеми, структура конфронтаційної динаміки, формулювання цільової функції та інтерпретація результатів. Серед цих факторів першорядне значення набуває побудова цільової функції.

У царині економіки цей виклик являє собою змагання «голова до голови», у якій беруть участь два гравці, що ведуть запеклу боротьбу за частку прибуткових ринків збуту. Але коли ми переходимо до динамічної сфери інформаційної безпеки, ця проблема зазнає трансформації, перетворюючись на багатогранну. Вона набуває чітких характеристик, які глибоко впливають на формулювання проблеми, динаміку, що формує взаємодію між залученими сторонами, структуру цільової функції та навіть те, як ми інтерпретуємо результати.

Серед цих різних аспектів створення цільової функції постає як центральна та критична точка фокусу. Вона відіграє ключову роль у розкритті складності цього виклику та в розробці ефективних рішень.

Тепер варто глибше розглянути можливість використання функції Гросса. Ця конкретна функція може мати потенціал для надання цінної інформації та вказівок у пошуках оптимізації розподілу ресурсів адаптивної системи захисту в цьому складному та багатогранному економічному середовищі. Її застосування може пролити світло на те, як орієнтуватися в складнощах управління інформаційною безпекою фінансових організацій, і, проаналізувавши цю можливість, ми можемо вивчити потенційні переваги та

обмеження функції Гросса у вирішенні унікальних проблем проєктування адаптивних систем захисту. Функція Гросса $I(x, y) = g \cdot (x - y)$, яка в нашому випадку буде виражати обсяг втрат інформації, а g – її кількість у фінансовій організації. Залежність $I(x, y)$ має кусково-лінійний характер. Відповідно до моделі Гросса при $x - y \le 0$ $I(x, y) = 0$. Виходячи зі специфіки нашої задачі при $x - y \ge 1$ $I(x, y) = g$, оскільки вилучена інформація не може бути більшою за її обсяг на об'єкті. Центральна дільниця залежності $I(x)$ має кутовий коефіцієнт $tg\,\alpha$, який залежить від g (*рис. 1*). Використовуючи наведені умови $I(x_0, y) = 0$ і $I(x_г, y) = g$, знаходимо значення граничних точок: $x_0 = y$ (значення задається захистом і на лініях рис. 1 виступає як параметр) і $x_г = x_0 + g\,ctg\,\alpha$.

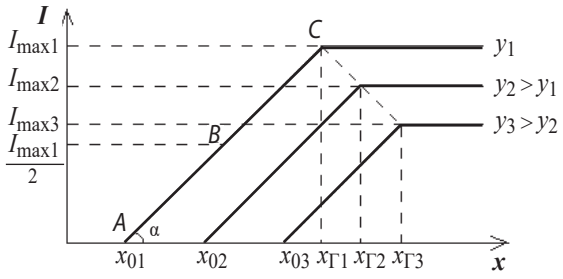

Рис. 1. Хід функції Гросса за різних значеннях *y*

Приймаючи кусково-лінійний характер залежності $I(x)$, зазначимо, що параметри α, x_0, $x_г$ вибрані евристично та свого обґрунтування не мають. Зокрема, при визначенні положення граничної точки $x_г$ не враховано протидію служби безпеки фінансової організації спробам вилучення інформації. Насправді при їх зростанні, що в нашій моделі виражається збільшенням ресурсів нападу x, зростає й імовірність p того, що ці спроби будуть зафіксовані та блоковані. Отже, I_{max} буде залежати від величини p, яка, своєю чергою, залежить від x та y і зростає зі зростанням кожної з цих величин: $I_{max3} < I_{max2} < I_{max1} = g$. Зменшення I_{max} при зростанні y виражає той факт, що ефективність вкладених нападом ресурсів при збільшенні ресурсів захисту зменшується. Щодо постановки задачі та одержаних рекомендацій, то у військовому плануванні вони мають ряд відмінностей, які зрештою приводять до деяких висновків, неприйнятних у нашому випадку. Зазначимо основні відмінності.

1. У військовому плануванні цільова функція відрізняється від нашої тим, що вона є дискретною. Це означає, що вона конкретно визначає кількість одиниць, які змогли прорвати оборону або які були знищені під час нападу чи оборони.
2. Оскільки головною метою нападу є прорив оборони, виникає висновок, який відомий у військовій теорії: слід направляти основні сили на найслабшу дільницю. У нашому ж випадку обмежені ресурси захисту від гібридних загроз спрямовані на об'єкти, що містять мінімум інформації. Концентрація зусиль нападу в цьому напрямку не приведе до досягнення бажаного результату.
3. У задачах військового планування об'єкти протистояння (літаки, зенітні установки тощо) однакові ($g_k = 1$), з чого випливає логічний висновок – оптимальною стратегією захисту в умовах невизначеності є рівномірний розподіл ресурсів між об'єктами [10–13]; у нашому ж випадку різні об'єкти мають різні обсяги інформації, тому в цільовій функції необхідно враховувати ваговий коефіцієнт g_k, який суттєво впливає на розподіл ресурсів адаптивної системи захисту.

З урахуванням наведених міркувань цільова функція нашої задачі згідно з моделлю Гросса приймає вигляд:

$$I_{ij}(x, y) = \sum_{k=1}^{l} g_k p_{ijk} (x_{ik} - y_{jk}),$$

де i та j – номери варіантів розподілу ресурсів нападу та захисту;

p_{ijk} – імовірність ij-го розподілу ресурсів на об'єкті під номером k,

$$x_{ik} - y_{jk} = \begin{cases} 0, \text{ при } x_{ik} - y_{jk} \le 0 \\ x_{ik} - x_{jk}, \text{при } 0 \le x_{ik} - y_{jk} \le 1 \\ 1, \text{ при } x_{ik} - y_{jk} \ge 1. \end{cases}$$

Схему протистояння графічно зображено на *рис. 2.*

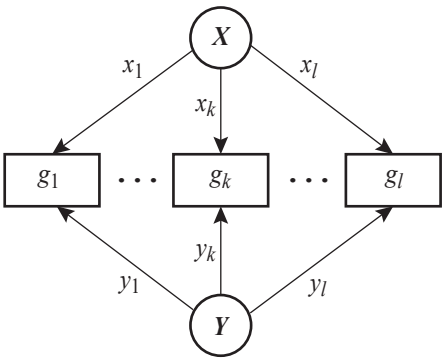

Рис. 2. Схема адаптивної системи захисту фінансових організацій від гібридних загроз

Розглянемо тепер аспекти обчислень у цій задачі. Рішення поставленої задачі ускладнюється значною кількістю змінних, які впливають на остаточний результат. Ці змінні можна розподілити на дві групи.

I. Змінні параметри, які визначаються стороною захисту (керовані змінні):

1) Y – ресурси захисту;

2) використання ресурсів на об'єктах захисту y_k (у фінансових підрозділах);

3) $k = \overline{1, l}$ – номер об'єкта захисту, $\sum_{k=1}^{l} y_k = Y$;

4) значення вагових коефіцієнтів g_k, які характеризують обсяг і важливість інформації на кожному об'єкті;

5) граничний рівень ризику $r = \sum_{k=1}^{l} r_k$ втрати інформації, який визначає максимально допустиме значення I.

II. Некеровані параметри, які визначаються стороною нападу (некеровані змінні):

1) X – ресурс нападу;

2) розподіл ресурсів нападу x_k по об'єктах, $\sum_{k=1}^{l} x_k = X$;

3) імовірності нападу на кожний з об'єктів.

Задача вирішується як оптимум цільової функції за одним із визначених критеріїв. При постановці завдання існують два підходи:

1) однокритеріальний, де оптимізується одна з характерних величин, таких як кількість вилученої інформації $I(x, y)$, ресурс захисту Y чи рівень ризику $r(Y)$;
2) багатокритеріальний, де пошук оптимуму відбувається одночасно за декількома критеріями та встановлюється ієрархія або додаткові обмеження на кожен з них.

Залежно від інформованості про дії суперника розглядаються дві ситуації: «за умов ризику», коли ймовірність подій може бути визначена, і «за умов невизначеності», коли це неможливо через відсутність достатньої інформації. Розгляд розпочинається з пошуку оптимальних рішень за умов невизначеності.

Недоліком функції Гросса (1) як цільової функції нашої задачі, як уже зазначалось, є її кусково-лінійний характер, який, очевидно, не може повністю відповідати реальній ситуації. Крім того, викликає сумнів хід кривої Гросса на початковому етапі, де кількість вилученої інформації $I_k(x_k, y_k)$ в межах $0 < x_k < y_k$ дорівнює нулю, а в незахищеному об'єкті ($y_k = 0$) залежить від x_k і вилучається повністю лише при $x_k = 1$. Вид аналітичної залежності та форма кривої між точками $I = 0$ та $I = 1$ не можуть бути встановлені точно через відсутність статистичних даних. Наше завдання – апроксимувати її на основі аналізу можливих ситуацій. Ці ситуації включають у себе:

а) вид об'єктів захисту інформації (приміщення, електронна інформаційна система, телекомунікації);

б) форму збереження та передачі інформації (електронна, паперова, суб'єктивна), а також деякі кількісні параметри, які впливають на положення кривої, зокрема значення x у точці, з якої починається вилучення інформації, у точці, яка відповідає, скажімо, значенню $I = 0{,}5$, і в точці, в якій інформація вилучається повністю (на лінії Гросса це, відповідно, точки A, B і C).

Наступним кроком є встановлення виду нелінійності між граничними точками, яка характеризує зв'язок кількості вилученої інформації зі співвідношенням ресурсів нападу та захисту. Передусім це стосується напрямку опуклості. Ставлячи за мету наближення до лінії Гросса, очевидно, що слід направити опуклість на початковій стадії $\left(\frac{x}{y} < 0{,}5\right)$ донизу, а на кінцевій $\left(\frac{x}{y} > 1{,}5\right)$ – догори. Після цього, використовуючи стандартні методи апроксимації, можемо сформувати цільову функцію.

Наведемо вид можливих цільових функцій, які задовольняють поставленим вимогам. Переходячи для спрощення запису від нормованого значення $\frac{x}{y}$ до x, представимо цільову функцію у вигляді:

$$I(x) = \frac{ax^n}{bx^n + c}. \qquad \textbf{(2)}$$

Поряд зі степеневою шукану функцію можна представити у вигляді показникової функції:

$$I(x) = 1 - ke^{-mx}. \qquad \textbf{(3)}$$

Константи a, b, c, k, m, n визначають положення і нахил кривих (2), (3) для різних об'єктів захисту та залежать від специфіки об'єкта. Ці значення можуть бути визначені зі статистичних даних (шляхом «прив'язки» до характерних точок), а за їх відсутності – в результаті експертної оцінки.

З *рис. 3,* де зображені залежності (2), (3) за різних значень констант, видно, що можна одержати функцію, яка досить тісно наближається до функції Гросса (крива 4).

Знайшовши вид цільової функції та використовуючи теоретико-ігровий підхід, будуємо платіжну матрицю для функції $I(x, y)$, в якій рядки відповідають варіантам $\{x_{ik}\}$ розподілу ресурсів нападу, а стовпчики – імовірним варіантам $\{y_{jk}\}$ розподілу ресурсів захисту. Шукана стратегія цієї матричної гри являє собою оптимальний розподіл ресурсів на захист від гібридних загроз, який знаходять по одному з відомих критеріїв [13]. У [10] розглянуто варіант цієї гри з використанням функції Гросса, в якому ресурси захисту розподілено між об'єктами, ресурс нападу концентрується на одному з них (невідомо якому), а мірилом оптимальності служить критерій Севіджа,

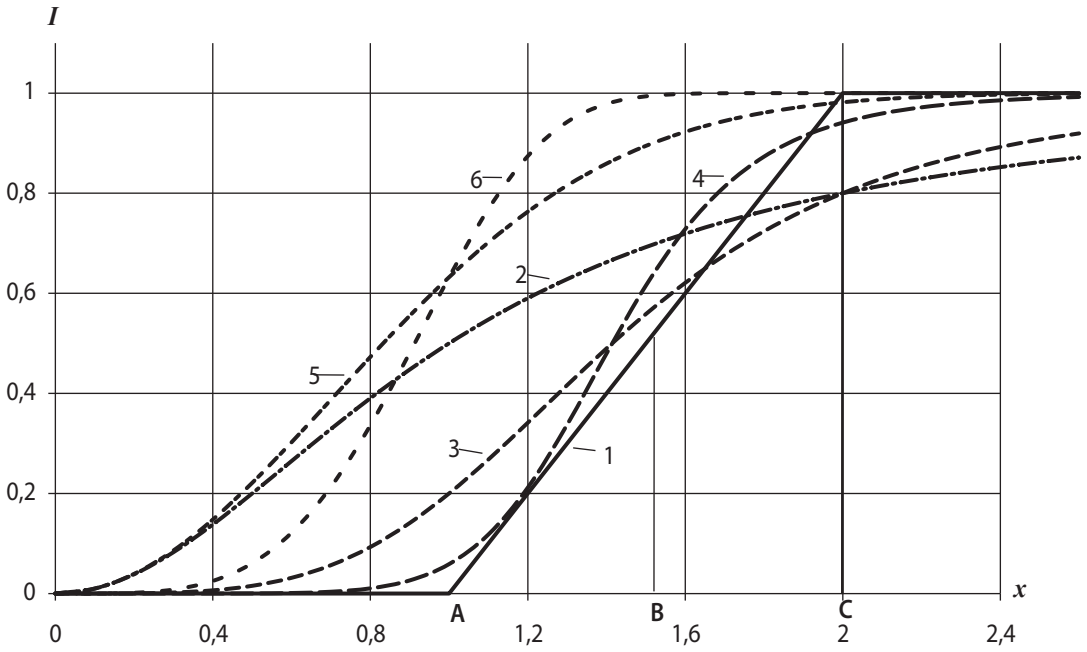

Рис. 3. Види цільових функцій

1 – функція Гросса; $2-I=\frac{x^2}{x^2+a^2}$, $a=1$; $3-I=\frac{x^4}{x^4+a^4}$, $a=2$; $4-I=\frac{x^8}{x^8+a^8}$, $a=4$;

$5-I=1-e^{-x^2}$; $6-I=1-e^{-x4}$.

тобто пошук $\min\limits_{j}\max\limits_{i} I_{ij}(x,y)$, де $I_{ij}(x,y)$ – інформація, вилучена при *i*-му варіанті розподілу ресурсів нападу та *j*-му варіанті розподілу ресурсів захисту, *i* = *k*.

У [10] наведено вираз для оптимального рішення антагоністичної гри за моделлю Гросса та приклад застосування цього виразу для випадку $Z=\frac{X}{Y}=1.$

З [10] випливає, що всі ресурси захисту слід направляти на більш важливі об'єкти, а менш важливі залишати без захисту. По відношенню до сил нападу вважається доцільним направляти всі сили на один об'єкт, який обирається з певним розподілом імовірностей. Цей висновок можна вважати очевидним при обмеженому ресурсі нападу $(Z\approx 1)$, коли розпорошення коштів по різних об'єктах відповідно до (1) дає близький до нульового результат. При *Z* >> 1 (наприклад, при *Z* = 3) таке рішення в нашій задачі не можна вважати оптимальним, оскільки воно може призвести до нераціональних витрат, адже кількість раціонально витрачених нападом коштів на кожному з об'єктів (на відміну від військового планування) обмежена величиною $x_{jk}-y_{ik}=1$ для всіх значень i,j,k.

Таким чином, висновок про максимальну концентрацію ресурсів на одному, найбільш слабкому напрямку, відомий як один з основних принципів військово-стратегічного планування, в нашому випадку втрачає свою універсальність і є додатковим свідченням необхідності коригування моделі Гросса.

При достатньому ресурсі нападу (*Z* >> 1) частину коштів, очевидно, можна спрямувати на розвідку. Оптимальна величина відношення $\frac{X^{(1)}}{X^{(2)}}$, де $X^{(1)}$ та $X^{(2)}$ – кошти, виділені на розвідку, та, відповідно, здобуття інформації, залежить від величини $\underline{Z}$. Також розглядалося питання про ефективність розвідки в задачі Гросса для окремих випадків, і було дано математичне обґрунтування задачі. Проведення розвідки можна розглядати як перший крок у застосуванні динамічного програмування для пошуку оптимального рішення нашої задачі.

Наступний крок у вирішенні поставленої задачі полягає у введенні перешкод, які є захистом від гібридних загроз. Ці перешкоди можуть розташовуватись послідовно – тоді ми маємо багаторубіжну (в термінології військового планування) систему захисту, і паралельно – із адресною системою захисту, де кожна перешкода захищає певну ділянку об'єкта. Подальше ускладнення задачі може йти в напрямку врахування можливого протистояння системі захисту двох супротивників, які діють незалежно.

ВИСНОВКИ

Таким чином, запропонована модель, на відміну від відомих аналогів, дає можливість визначи-

ти більш широкий спектр показників інформаційної безпеки, зокрема знайти не тільки оптимальний розмір ресурсів захисту інформації, а й їх розподіл між об'єктами захисту, котрі відрізняються кількістю інформації, уразливістю та ймовірністю нападу.

Залучення кваліфікованих експертів для побудови цільової функції та використання потужного інструментарію дослідження операцій дасть змогу виробити практичні рекомендації при розробці адаптивних систем інформаційної безпеки фінансових організацій України в умовах сучасного розвитку інформаційної економіки. ■

БІБЛІОГРАФІЯ

1. Libicki M. C., Ablon L., Webb T. The Defender's Dilemma: Charting a Course Toward Cybersecurity. National Security Research Division. Santa Monica, CA : RAND Corporation, 2015. 134 p.
2. Rosenzweig P. Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World. Praeger, 2013. 291 p.
3. Radin A. Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica, CA : RAND Corporation, 2017. 58 p.
4. Understanding Cyber Conflict: 14 Analogies / Perkovich G., Levite A. E. (Eds.). Georgetown University Press, 2017. 304 p.
5. Nye S. J. Protecting Democracy in an Era of Cyber Information War / Belfer Center for Science and International Affairs, 2019. 32 p. URL: https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf
6. Hingant J., Zambrano, M., Pérez, F. J. et al. HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection. *Security and Communication Networks*. 2018. Iss. 3. P. 1–13. DOI: https://doi.org/10.1155/2018/5625860
7. Countering Hybrid Threats: Lessons Learned from Ukraine / Iancu N., Fortuna A., Barna C., Teodor M. (Eds.). IOS Press, 2016. 286 p.
8. Hybrid threats as a concept / Hybrid CoE. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
9. Gross O., Wagner R. A Continuous Colonel Blotto Game. Santa Monica, CA : RAND Corporation, 1950. 15 p. URL: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM408.pdf
10. Левченко Є. Г., Рабчун А. О. Модель Гросса в протистоянні двох сторін у сфері захисту інформації. *Сучасна спеціальна техніка*. 2009. № 3. С. 75–81.
11. Левченко Є. Г., Рабчун А. О. Оптимізаційні задачі менеджменту інформаційної безпеки. *Сучасний захист інформації*. 2010. № 1. С. 16–23. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/783/727
12. Левченко Є. Г., Демчишин М. В., Рабчун А. О. Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології*. 2011. № 4. С. 88–96. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50130/07-Levchenko.pdf?sequence=1
13. Рабчун А. О. Оптимізація сумарних втрат в сфері захисту інформації. *Безпека інформації*. 2012. № 1. С. 32–36.
14. Лапко О. О., Конарівська О. Б. Моделювання тенденцій розвитку небанківських фінансових установ в Україні. *Бізнес Інформ*. 2015. № 2. С. 103–107. URL: https://www.business-inform.net/export_pdf/business-inform-2015-2_0-pages-103_107.pdf
15. Веселова Л. Ю. Особливості державної політики України у сфері забезпечення кібернетичної безпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2019. № 2. С. 23–27. DOI: https://doi.org/10.32999/ksu2307-8049/2019-2-4
16. Саркісян Л. Г., Самсонова Л. В. Гібридні загрози в торговельно-економічних відносинах. *Актуальні проблеми розвитку економіки регіону*. 2020. Вип. 16. Т. 2. С. 62–76. DOI: https://doi.org/10.15330/apred.2.16.62-76

REFERENCES

Countering Hybrid Threats: Lessons Learned from Ukraine. IOS Press, 2016.

Gross, O., and Wagner, R. "A Continuous Colonel Blotto Game". Santa Monica, CA : *RAND Corporation*, 1950. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM408.pdf

"Hybrid threats as a concept". *Hybrid CoE*. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hingant, J. et al. "HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection". Security and Communication Networks, no. 3 (2018): 1-13. DOI: https://doi.org/10.1155/2018/5625860

Lapko, O. O., and Konarivska, O. B. "Modeliuvannia tendentsii rozvytku nebankivskykh finansovykh ustanov v Ukraini" [Modeling of Development Trends in the Non-Bank Financial Institutions in Ukraine]. *Biznes Inform*, no. 2 (2015): 103-107. https://www.business-inform.net/export_pdf/business-inform-2015-2_0-pages-103_107.pdf

Levchenko, Ye. H., and Rabchun, A. O. "Model Hrossa v protystoianni dvokh storin u sferi zakhystu informatsii" [Gross's Model in the Confrontation of two Parties in the Field of Information Protection]. *Suchasna spetsialna tekhnika*, no. 3 (2009): 75-81.

Levchenko, Ye. H., and Rabchun, A. O. "Optymizatsiini zadachi menedzhmentu informatsiinoi bezpeky" [Optimization Tasks of Information Security Management]. *Suchasnyi zakhyst informatsii*, no. 1 (2010): 16-23. https://journals.dut.edu.ua/index.php/dataprotect/article/view/783/727

Levchenko, Ye. H., Demchyshyn, M. V., and Rabchun, A. O. "Matematychni modeli ekonomichnoho menedzhmentu informatsiinoi bezpeky" [Mathematical Models of Economic Management of Information Security]. *Systemni doslidzhennia ta informatsiini tekhnolohii*, no. 4 (2011): 88-96. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50130/07-Levchenko.pdf?sequence=1

Libicki, M. C., Ablon, L., and Webb, T. The Defender's Dilemma: Charting a Course Toward Cybersecurity. *National Security Research Division*. Santa Monica, CA: RAND Corporation, 2015.

Nye, S. J. "Protecting Democracy in an Era of Cyber Information War". *Belfer Center for Science and International Affairs*, 2019. https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf

Rabchun, A. O. "Optymizatsiia sumarnykh vtrat v sferi zakhystu informatsii" [Optimization of Total Losses in the Field of Information Protection]. *Bezpeka informatsii*, no. 1 (2012): 32-36.

Radin, A. *Hybrid Warfare in the Baltics: Threats and Potential Responses*. Santa Monica, CA: RAND Corporation, 2017.

Rosenzweig, P. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Praeger, 2013.

Sarkisian, L. H., and Samsonova, L. V. "Hibrydni zahrozy v torhovelno-ekonomichnykh vidnosynakh" [Hybryd Threats in Trade and Economic Relations]. *Aktualni problemy rozvytku ekonomiky rehionu*, vol. 2, no. 16 (2020): 62-76.
DOI: https://doi.org/10.15330/apred.2.16.62-76

Understanding Cyber Conflict: 14 Analogies. Georgetown University Press, 2017.

Veselova, L. Yu. "Osoblyvosti derzhavnoi polityky Ukrainy u sferi zabezpechennia kibernetychnoi bezpeky v umovakh hibrydnoi viiny" [Peculiarities of the State Policy of Ukraine in the Field of Providing Cyber Security in Conditions of Hybrid War]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia «Yurydychni nauky»*, no. 2 (2019): 23-27.
DOI: https://doi.org/10.32999/ksu2307-8049/2019-2-4

УДК 33.303.519.85
JEL: C1; C49; R12
DOI: https://doi.org/10.32983/2222-4459-2023-11-187-194

МОДЕЛЮВАННЯ РІВНЯ СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ РЕГІОНІВ НА ОСНОВІ PROXY-ЗМІННИХ

©2023 **ГУР'ЯНОВА Л. С., КАГАНОВСЬКИЙ О. С., СЕРГІЄНКО О. А., МИРОНЕНКО А. Ю.**

УДК 33.303.519.85
JEL: C1; C49; R12

Гур'янова Л. С., Кагановський О. С., Сергієнко О. А., Мироненко А. Ю. Моделювання рівня соціально-економічного розвитку регіонів на основі proxy-змінних

У статті запропоновано моделі оцінки рівня соціально-економічного розвитку та економічної безпеки регіонів, які на основі синтезу техніки proxy-змінних і кластерного аналізу дозволяють оцінити зміну міжрегіональної диференціації, просторові економічні трансформації, виявити «опорні» регіони, оцінити рівень економічної безпеки регіонів за умов обмежених даних. Обґрунтовано систему proxy-змінних соціально-економічного розвитку регіонів; розроблено класифікації регіонів за рівнем соціально-економічного розвитку на основі методів ієрархічного агломеративного та ітеративного кластерного аналізу; проведено динамічний аналіз структури кластерів; проаналізовано зміни характеристик розподілу proxy-змінних; здійснено оцінку міжрегіональної диференціації та асиметрії розвитку. Результати кластерного аналізу на основі proxy-змінних дозволили зробити висновок, що останні роки привели до суттєвих трансформацій економічного простору в регіональному аспекті. У кластері «опорних» регіонів спостерігається посилення позицій Дніпропетровської та Львівської областей, конвергенція із регіонами із середнім рівнем розвитку – Київської, Харківської та Одеської областей. Найбільш кризова ситуація характерна для Луганської, Донецької та Херсонської областей. Донецька область перейшла із кластера регіонів із середнім рівнем розвитку до кластера регіонів із кризовим розвитком. Релокація підприємств і згладжування асиметрії за змінною «Приріст юридичних осіб» на даний момент меншою мірою зачіпає індикатори бюджетної безпеки регіонів. Харківська область, незважаючи на погіршення соціально-економічної ситуації, зберігає своє становище у кластері «опорних» регіонів. Отримані результати можуть бути використані в системі антисипативного управління регіональним розвитком для адаптації регіональних стратегій до нових реалій.
Ключові слова: *регіон, соціально-економічний розвиток регіону, економічна безпека, математичне моделювання, кластеризація, proxy-змінні.*
Рис.: *8.* ***Бібл.:*** *8.*

Гур'янова Лідія Семенівна *– доктор економічних наук, професор, завідувачка кафедри економічної кібернетики і системного аналізу, Харківський національний економічний університет імені Семена Кузнеця (просп. Науки, 9а, Харків, 61166, Україна); професор кафедри економічної кібернетики та прикладної економіки Харківського національного університету ім. В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*
E-mail: *guryanovalidiya@gmail.com*
ORCID: *https://orcid.org/0000-0002-2009-1451*
Researcher ID: *https://www.webofscience.com/wos/author/record/L-3402-2017*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=36068855600*

Кагановський Олександр Семенович *– доктор філософії (економіка), аспірант кафедри менеджменту та бізнесу, Харківський національний економічний університет імені Семена Кузнеця (просп. Науки, 9а, Харків, 61166, Україна)*
E-mail: *kag.ole.68@gmail.com*
ORCID: *https://orcid.org/0009-0008-1965-625X*

Сергієнко Олена Андріанівна *– доктор економічних наук, професор, професор кафедри підприємництва, торгівлі і логістики, Національний технічний університет «Харківський політехнічний інститут» (вул. Кирпичова, 2, Харків, 61002, Україна)*
E-mail: *Elena.Sergienko@khpi.edu.ua*
ORCID: *https://orcid.org/0000-0002-9796-9218*
Researcher ID: *https://www.webofscience.com/wos/author/record/O-3966-2015*
Scopus Author ID*: https://www.scopus.com/authid/detail.uri?authorId=57219245125*

Мироненко Артем Юрійович *– магістр, кафедра економічної кібернетики і системного аналізу, Харківський національний економічний університет імені Семена Кузнеця (просп. Науки, 9а, Харків, 61166, Україна)*
E-mail: *artem135135@gmail.com*