Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2024. № 5.

DOI: http://doi.org/10.32702/2307-2105.2024.5.53

УДК 005.8:658.478

А. О. Рабчун,

к. т. н., докторант,

Міжнародний науково-технічний університет імені академіка Юрія Бугая

ORCID ID: https://orcid.org/0009-0002-1389-1263

ЕВОЛЮЦІЙНА МОДЕЛЬ ПОБУДОВИ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ ОРГАНІЗАЦІЙ ТА ПЕРЕХІД ДО АДАПТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ІНФОРМАЦІЙНИХ ГІБРИДНИХ ЗАГРОЗ

A. O. Rabchun,

PhD in Technical Sciences, Doctoral Student, International Scientific and Technical University named afterAcademician Yuri Bugai,

THE EVOLUTIONARY MODEL OF BUILDING INFORMATION SECURITY SYSTEMS OF FINANCIAL ORGANIZATIONS AND THE TRANSITION TO ADAPTIVE INFORMATION SECURITY MANAGEMENT IN THE CONDITIONS OF INFORMATION HYBRID THREATS

Стаття присвячена проблемі адаптивного управління інформаційною безпекою в умовах інформаційних гібридних загроз. У статті запропонована еволюційна модель побудови систем інформаційної безпеки фінансових організацій в залежності від фінансових можливостей, зовнішніх умов

функціонування та вимог щодо захисту корпоративної інформації. Пропонується підхід щодо створення адаптивного механізму управління інформаційною безпекою на основі гомеостазу системи, представлена концептуальна модель управління ефективністю функціонування адаптивної системи інформаційної безпеки в умовах динамічного інформаційного протистояння. Методи штучного інтелекту можуть відігравати ключову роль у побудові сучасних адаптивних систем інформаційної безпеки. Еволюційна модель для побудови систем інформаційної безпеки фінансових організацій включає кілька етапів: від початкового рівня з обмеженим бюджетом до рівня, де процеси інформаційної безпеки визначені на рівні всієї організації та побудови адаптивних систем інформаційної безпеки фінансових організацій з впровадженням в управління систем на основі технологій штучного інтелекту.

The article is devoted to the problem of adaptive management of information security in the context of information hybrid threats. At its core, the paper introduces an evolutionary model for constructing information security systems, which takes into account the nuanced interplay between financial capabilities, external factors, and the imperative to safeguard corporate information. This model represents a paradigm shift from static, one-size-fits-all security approaches to dynamic, context-aware systems capable of adapting to the ever-changing threat landscape A central tenet of the proposed framework is the concept of homeostasis, borrowed from biological systems, wherein the security ecosystem continuously adjusts its parameters to maintain equilibrium in the face of external disruptions. By leveraging real-time monitoring, sophisticated analytics, and adaptive response mechanisms, financial organizations can bolster their resilience against emerging threats while optimizing resource allocation. Artificial intelligence methods can play a key role in building modern adaptive information security systems. The evolutionary model for building information security systems of financial organizations includes several stages: from the initial level with a limited budget to the level where information security

processes are defined at the level of the entire organization and building adaptive information security systems of financial organizations with the introduction of systems based on artificial intelligence technologies into management. Critical to the efficacy of modern information security systems is the integration of artificial intelligence (AI) technologies. The integration of AI-driven technologies represents a pivotal step towards fortifying financial organizations against the evolving threat landscape. In conclusion, this paper offers a comprehensive roadmap for financial organizations seeking to navigate the complex terrain of information security in an age of hybrid threats. By embracing an evolutionary approach, leveraging adaptive mechanisms informed by homeostatic principles, and harnessing the power of AI technologies, organizations can forge resilient security ecosystems capable of withstanding the challenges posed by an increasingly volatile digital landscape.

Ключові слова: *адаптивна система, інформаційні гібридні загрози, адаптивне управління інформаційною безпекою, фінансові організації, оцінка ефективності, динамічне інформаційне протистояння.*

Keywords: *adaptive system, information hybrid threats, adaptive information security management, financial organizations, performance evaluation, dynamic information confrontation.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Актуальність впровадження ефективних систем інформаційної безпеки у діяльність фінансових організацій у наш час не викликає жодних сумнівів, перш за все це пов'язано зі збільшенням кількості гучних інцидентів (головним чином кібератак) у сфері інформаційної безпеки в сучасних умовах інформаційних гібридних загроз. В той же час враховуючи економічне становище та фінансові можливості кожної окремої фінансової організацій в області інвестування в інформаційну безпеку, нагально постає проблема вибору та побудови ефективної системи в умовах ресурсних обмежень. Як відомо, в загальному

випадку, під інформаційною безпекою фінансових організацій необхідно розуміти сукупність засобів, методів та процесів (процедур), які забезпечують захист інформаційних активів та, як наслідок, гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються та обробляються [1].

У зв'язку з цим, фінансові організації потребують більш надійного захисту, включаючи міцніші системи кібербезпеки, посилення моніторингу та аналізу, а також постійні оновлення та навчання персоналу з питань кібербезпеки.

Одним з чинників, що на теперішній час, сприяє забезпеченню ефективності інформаційної безпеки є застосування технологій штучного інтелекту. Адже штучний інтелект та його впровадження є одним з трендових напрямів, яким охоплені сьогодні всі розвинуті країни світу. Особливого значення та актуальності набуває використання штучного інтелекту в системі забезпечення інформаційної безпеки фінансових організацій в контексті динамічного інформаційного протиборства. Прийняття рішень за допомогою технологій штучного інтелекту допомагає знаходити загрози, попереджувати ризики та виконувати відповідні дії. Більш того, методи штучного інтелекту та машинного навчання можуть відігравати вирішальну роль у побудові сучасних адаптивних систем інформаційної безпеки, що в свою чергу обумовлює підвищену увагу та актуальність дослідження проблеми адаптивного управління ресурсами захисту в умовах інформаційних гібридних загроз.

Аналіз останніх досліджень і публікацій. Дослідженню питань щодо впровадження технологій штучного інтелекту та проблем систем інформаційної безпеки присвячені ряд робот як вітчизняних, так і закордонних науковців, зокрема, Libicki, M. C., Ablon, L., & Webb, T. [2], Rosenzweig, P. [3], Radin, A. [4], Blank, S., Perkovich, G., & Levite, A. E. [5], Nye S. J. [6], Hingant, J., Zambrano, M., Pérez, F. J., Pérez, I., & Esteve, M. [7], Iancu, N., Fortuna, A., Barna, C., & Teodor, M. [8], Лапко, О.О., Конарівська, О.Б. [9], Веселова Л.Ю. [10],

Саркісян Л. Г., Самсонова Л. В. [11]. Автори досліджують виклики та стратегії захисту від різноманітних інформаційних гібридних загроз. Розглядаються виклики кіберінформаційної війни та стратегії для захисту фінансових організацій країн ЄС і блоку НАТО [12]. Досліджуються уроки, вивчені під час протидії інформаційним гібридним загрозам з фокусом на досвіді України. Проте, враховуючи думки зазначених авторів, доводиться констатувати, що в умовах динамічного інформаційного протистояння, постійного впливу зовнішніх та внутрішніх чинників необхідно приділити більше уваги дослідженню проблем застосування штучного інтелекту в побудові адаптивних систем інформаційної безпеки, як альтернативі в протидії застосуванню штучного інтелекту при продукуванні інформаційних гібридних загроз.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування переходу до адаптивного управління інформаційною безпекою фінансових організацій на сучасному етапі розвитку цифрової економіки з використанням технології штучного інтелекту.

Виклад основного матеріалу дослідження. Для вирішення зазначеної проблеми спочатку проведемо аналіз трансформаційних змін СІБ, на кожному етапі розвитку (життєвого циклу) фінансової організації. Пропонується прив’язати еволюційні етапи побудови СІБ, котрі використовуються для забезпечення інформаційної безпеки фінансових організацій, до методології визначення необхідного та достатнього рівня інформаційної безпеки в залежності від фінансових можливостей, зовнішніх умов функціонування та вимог щодо захисту корпоративної інформації. Як основу для цього використаємо модель в Capability Maturity Model Integrated (CMMI) (Інтеграційна Модель Зрілості Спроможностей) [13].

В загальному вигляді дана еволюційна модель в застосуванні щодо побудови СІБ фінансових організацій включає п’ять етапів:

1 рівень — Початковий (характерний для новостворених з обмеженим бюджетом фінансових організацій). В розрізі інформаційної безпеки фінансової організації цей рівень характеризує початок створення інфраструктури

забезпечення інформаційної безпеки. Процеси захисту не регламентовані, не контролюються, не уніфіковані (в одній СІБ може використовуватися ПЗ захисту інформації різних вендорів), а якість захисту залежить суто від індивідуальних якостей відповідальних осіб. На такому рівні захист інформації, як правило обмежується елементарними засобами: антивірусне ПЗ та міжмережеві екрани (FireWall), у рідких випадках впроваджується система єдиної аутентифікації.

2 рівень — На цьому етапі процеси захисту інформації у фінансових організаціях визначені на рівні проектів побудови СІБ. Зазвичай такі СІБ впроваджуються у відповідь на певні події (інциденти) ІБ характерні для умов функціонування фінансових організацій. СІБ, котрі використовуються фінансовими організаціями, на другому рівні розвитку, є програмні комплекси виявлення та запобігання атакам. Впровадження цих комплексів є індивідуальним для кожної фінансової організації і враховує її специфіку. На відміну від антивірусів та брандмауерів, системи виявлення та попередження атак мають іншу ідеологію і створювалися саме для корпоративного застосування. Тобто, IDS/IPS мають функції централізованого управління, моніторингу і оновлення — ті функції, які так важливі при функціонуванні сучасних фінансових організаціях.

Крім виявлення атак актуальним є їх запобігання, тобто створення умов, що перешкоджають реалізації несанкціонованого доступу. Однією з технологій, що використовують такий підхід, є пошук вразливостей (аналіз захищеності), який полягає в ідентифікації різних «дірок» на вузлах корпоративної інформаційної мережі і своєчасному їх усуненні до того, як ними зможуть скористатися зловмисники.

Цей же етап характеризується застосуванням систем контролю вмісту, які дозволяють аналізувати весь мережевий трафік, що циркулює в мережі. Такі засоби, DLP системи, котрі представлені в Україні і західними і вітчизняними виробниками, дуже затребувані, особливо в організаціях, що обробляють конфіденційну інформацію.

3 рівень — Процеси інформаційної безпеки визначені на рівні фінансової організації в цілому. Заходи по забезпеченню визначеного рівня інформаційної безпеки покладаються на спеціальний підрозділ з інформаційної безпеки.

Разом з тим у міру зростання фінансової організації, збільшується число її клієнтів та співробітників і, як наслідок, зростає корпоративна мережа - зростає число корпоративних вузлів і ресурсів, точок виходу в Internet, філій і т.п. Все це накладає особливий відбиток на забезпечення інформаційної безпеки. Головним болем стає завдання забезпечення доступу сотень тисяч користувачів з різних сегментів мережі до сотням ресурсів. Напевно, тому третім етапом еволюції інфраструктури інформаційної безпеки фінансових організацій є впровадження системи єдиної аутентифікації, яка може бути реалізована по-різному, наприклад, на базі інфраструктури відкритих ключів (PKI).

Використання технології єдиної аутентифікації дозволяє користувачеві проходити процес перевірки і підтвердження свої ідентичності тільки один раз для отримання доступу до різних ресурсів чи сервісів. Крім того, така технологія:

- спрощує контроль доступу співробітників до ресурсів компанії, в т.ч. і до конфіденційної інформації;
- оптимізує певні процеси в роботі співробітників відділу захисту інформації;
- полегшує процедуру доступу користувачів до десятків різних вузлів, як у корпоративній мережі і за її межами.

Знаходження на даному етапі говорить про зрілість компанії та її розумінні ролі інформаційних технологій у своєму бізнесі. Однак, дійшовши до третього етапу, фінансові організації стикаються з проблемою. Це лавина повідомлень від різнорідних засобів захисту, встановлених в самих критичних місцях мережі. І проблема ще в тому, що засоби захисту поставляються різними виробниками. Наприклад, міжмережевий екран від компанії Cisco Systems, система виявлення атак - від Internet Security Systems, VPN - від CheckPoint Software, і т.п. Навіть використовуючи все від одного виробника, ви не

застраховані від того, що вони не будуть узгоджено працювати разом. Візьмемо для прикладу рішення компанії Symantec, яка на сьогоднішній день пропонує практично весь спектр програмних засобів захисту інформації (від антивірусних систем до міжмережевих екранів). Однак, у кожного з продукту, що випускається під маркою Symantec (а їх для корпоративного ринку налічується більше 20) своя власна консоль управління.

Таким чином, для того щоб уникнути цієї проблеми, необхідна ефективна система управління та моніторингу інформаційної безпеки корпоративної мережі фінансової організації це - **4 Рівень**. Тобто найбільший ефект досягається тоді, коли всі використовувані захисні засоби об'єднані в єдину керовану систему, яка:

- уніфікує управління різнорідними програмними засобами захисту інформації в єдиних термінах політики безпеки;
- зменшує часові та фінансові витрати на вивчення фахівцями з інформаційної безпеки різних консолей управління;
- дозволяє ефективно оновлювати всі керовані засоби захисту;
- групує всі ресурси що захищаються за різними ознаками з метою фокусування уваги на необхідних в даний моментах вузлах;
- дозволяє фільтрувати події з метою усунення «шумових» даних і зниження навантаження на адміністратора безпеки;
- дозволяє корелювати данні від різнорідних засобів захисту з метою зниження числа помилкових спрацьовувань і оповіщення про події що дійсно відбуваються в межах порушення політики безпеки.

Вершиною еволюції, її завершальним **п'ятим етапом**, є перехід до побудови адаптивних СІБ фінансових організацій з впровадженням в управління системою елементів на основі технологій штучного інтелекту.

В даній статті розглянемо та запропонуємо один з підходів щодо побудови таких систем.

Як відомо, в загальному вигляді успішна адаптація можлива при умові своєчасного отримання інформації про зміни в зовнішньому середовищі, а

також при наявності можливостей для оперативної трансформації у відповідності до ситуації.

В 2014 році віце-президент Gartner Нил Макдональд в загальному вигляді представив ідею адаптивної архітектури інформаційної безпеки (Adaptive Security Architecture, ASA), в основі якої лежить концепція оперативної «акліматизації» до нових видів інформаційних атак за допомогою циклічного повтору чотирьох етапів– Prevent, Detect, Respond та Predict(3).

1. **Prevent** (Превентивний) – блокування та придушення дій, які однозначно трактуються як зловмисні;
2. **Detect** (Виявлення) – виявляються підозрілі дії та події, та здійснюється їх контейнерізація;
3. **Respond** (Реагування) – реакція на інцидент, що відбувся, ретроспективний аналіз, розслідування та «рефлексія»;
4. **Predict** (Прогнозування) – виявлення закономірностей і кореляцій, виявлення причинно-наслідкових зв’язків і функціональних залежностей для прогнозування і передбачування атак на основі збору та аналізу різнорідних даних, як безпосередньо пов'язаних з інформаційною безпекою, а також «охоплення» інших сфер, наприклад, політики, економіки, соціально-демографічних та технологічних аспектів тощо.

Вважається що етап **Prevent** також повинен бути пов'язаний з накопиченням досвіду, контекстно-орієнтованим підходом та формуванням історичних індикаторів (baselining): система захисту вивчає та розуміє з часом, як «виглядає» еталонна модель поведінки в межах заданої інфраструктури та розпізнає будь-яке відхилення від очікуваних дій як аномалію - тобто повинна мати адаптаційний механізм управління.

Розглянемо підхід щодо створення такого механізму на основі гомеостазу системи.

Процес формування такої адаптивної поведінки системи рівнозначно дослідженню управління ефективністю її цільового застосування за різних умов, тобто під управлінням ефективністю будемо розуміти процеси впливу на

підсистеми та окремі компоненти СІБ, які переводять систему з одного стану в інший, сприяють виконанню її основної цільової функції в умовах динамічного інформаційного протистояння.

Відомо, що управління такого плану тісно пов’язане з поняттям гомеостазу, який може підтримуватись в системі як за рахунок внутрішніх ресурсів, так і за рахунок зовнішнього по відношенню до системи середовища [14-16]. Гомеостаз, або здатність системи зберігати сталість внутрішнього середовища, можна розглядати також як прагнення системи інформаційної безпеки підтримувати заданий рівень безпеки, повертатися в рівноважний стан із зовнішнім середовищем після відображення руйнівного впливу.

В загальному випадку для складних технічних систем трактування гомеостазу може ототожнюватись з концепцією цільового функціонування в складних динамічних середовищах. Ступінь гомеостазу ефективності цільового застосування таких систем вимірюється їх спроможністю зберігати свої специфічні функціональні, структурні і організаційні особливості всупереч зовнішнім та внутрішнім дестабілізуючим факторам. Причому, чим більше число характеристик системи залишається постійними чи в межах допустимості, та чім ширший можливий для функціонування системи діапазон впливу зовнішніх та внутрішніх дестабілізуючих факторів, тим вище ступінь гомеостазу заданої системи.

Під гомеостазом в нашому випадку будемо розуміти можливість адаптивних СІБ змінювати значення своїх параметрів при зміні параметрів зовнішнього та внутрішнього середовища з метою підтримки максимально можливого в конкретних умовах обстановки рівня ефективності цільового застосування як компонентів (в основному програмних засобів захисту інформації) так і всієї системи в цілому [17-19]. Концептуальна модель управління ефективністю цільового застосування адаптивної СІБ в умовах динамічного інформаційного протистояння показана на рис. 1.

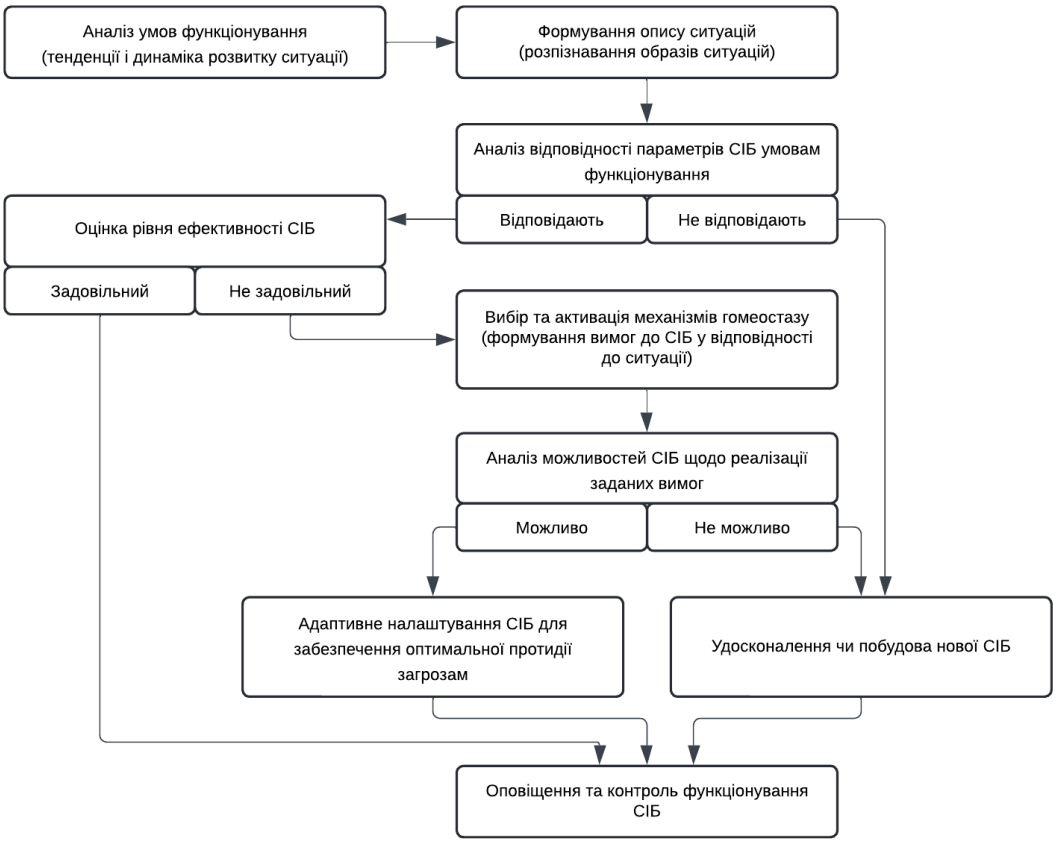

Рис. 1. Концептуальна модель управління ефективністю функціонування адаптивною СІБ в умовах динамічного інформаційного протистояння

З [14] слідує що, для оцінки гомеостатичних властивостей СІБ необхідно виділити керуючий (компонент ініціювання процесу гомеостазу), механізми гомеостазу та їх ресурси, а також характер, принципи та алгоритми їх впливу на змінні параметри компонентів СІБ. В якості керуючого компонента на рівні функціонування СІБ можуть виступати як фахівці з інформаційної безпеки (при ручному управлінні) так і логіко-динамічні комунікатори (на основі технологій штучного інтелекту при автоматичному управлінні) здатні фіксувати чи прогнозувати зміни рівня ефективності цільового застосування СІБ чи її окремих компонентів. В якості ресурсів гомеостатичних механізмів СІБ виступають як правило програмні ресурси для захисту від різноманітних типів та видів інформаційних гібридних загроз.

Кожен з цих ресурсів характеризується наступними параметрами:

- ступінь впливу ресурсу на досягнення цілі гомеостазу;
- ступінь доступності ресурсу в конкретних умовах обстановки цільового застосування СІБ;
- діапазоном змін визначаючим потенціал використання ресурсу в процесі гомеостаза ефективності СІБ;
- керованістю тобто можливістю цілеспрямованого змінювання в заданих межах;
- компліментарністю тобто зв'язаністю з іншими видами ресурсів гомеостазу;

Багаторубіжна ієрархічна структура сучасних СІБ обумовлює багаторівневий характер відповідних керуючих впливів, як на компоненти (ресурси) в самій СІБ так і на її структуру в цілому для підтримки гомеостазу при функціонуванні за різних умов інформаційних гібридних загроз, що в свою чергу потребує для реалізації автоматичного адаптивного управління, перш за все розробки математичних моделей процесів функціонування адаптивних СІБ фінансових організацій в умовах динамічного інформаційного протистояння для машинного навчання керуючих елементів на основі штучного інтелекту.

Висновки та перспективи подальших розвідок у даному напрямі. Побудова адаптивних СІБ фінансових організацій з використанням технологій штучного інтелекту потребує систематичного аналізу рівня ефективності їх цільового застосування з метою підтримки максимально можливого в конкретних умовах обстановки рівня ефективності застосування як компонентів (в основному програмних засобів захисту інформації) так і всієї системи в цілому. Запропонована модель, на основі гомеостазу системи, дає можливість для управління ефективністю цільового застосування адаптивної СІБ в умовах динамічного інформаційного протистояння, що в свою чергу дасть змогу виробити практичні рекомендації при розробці **адаптивних систем інформаційної безпеки фінансових організацій України в умовах сучасного розвитку інформаційної економіки.**

Література

1. Ліпкан, В., Максименко, Ю., Желіховський, В. (2006), Інформаційна безпека України в умовах євроінтеграції: навчальний посібник, Київ: *КНТ*, 280 с.

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

3. Rosenzweig, P. (2013), *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, Library of Congress Cataloging-in-Publication Data, Washington, US.

4. Radin, A. (2017), *Hybrid Warfare in the Baltic*, National Security Research Division. RAND Corporation, Santa Monica, US.

5. Blank, S., Perkovich, G. and Levite, A. (2017), *Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press, Washington, US.

6. Nye, J. (2019), *Protecting Democracy in an Era of Cyber Information War*. Belfer Center for Science and International Affairs, Cambridge, US.

7. Hingant, J., Zambrano, M., Pérez, F., Pérez, I. and Esteve, M. (2018), "A Hybrid Intelligence System for Critical Infrastructures Protection", *HYBINT*, vol. 2018, pp. 1-13.

8. Iancu, N., Fortuna, A., Barna, C. and Teodor, M. (2016), "Countering Hybrid Threats: Lessons Learned from Ukraine", *IOS Press*, Amsterdam, NL.

9. Лапко, О., Конарівська, О. (2015), Моделювання тенденцій розвитку небанківських фінансових установ в Україні. *Бізнес Інформ, 2*, С. 103-107.

10. Веселова, Л. (2019), Особливості державної політики України у сфері забезпечення кібернетичної безпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2*, С. 23-27.

11. Саркісян, Л., Самсонова, Л. (2020), Гібридні загрози в торговельно-економічних відносинах. Актуальні проблеми розвитку економіки регіону.16.2, С. 62-76.

12. Hybrid CoE. Гібридні загрози як поняття. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (дата звернення: 07.05.2024).

13. Godfrey, S. (2008), *What is CMMI*, NASA, Washington, US.

14. Somayaji, A. and Forrest, S. (2000), "Automated Response Using System-Call Delays", *Proceedings of the 9th USENIX Security Symposium*, USENIX Association, Denver, pp. 185–198.

15. Karen R. and Merrill W. (2017), "Risk homeostasis in information security: challenges in confirming existence and verifying impact", *NSPW '17: 2017 New Security Paradigms Workshop*, Association for Computing Machinery, New York, pp. 57-70.

16. Schrom, E. et al. (2023), "Challenges in cybersecurity: Lessons from biological defense systems", *Mathematical Biosciences*, vol. 362, pp. 47-73.

17. Левченко, Є., Рабчун, А. (2010), Оптимізаційні задачі менеджменту інформаційної безпеки. *Сучасний захист інформації, 1*, С. 16-23.

18. Рабчун, А. (2012), Оптимізація сумарних втрат в сфері захисту інформації. *Безпека інформації, 1(17)*, С. 32-36.

19. Левченко, Є., Демчишин, М., Рабчун, А. (2011), Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології, 4*, С. 88-96.

References

1. Lipkan, V., Maksymenko, Yu. and Zhelikhovskyi, V. (2006), *Informatsijna bezpeka Ukrainy v umovakh ievrointehratsii* [Information security of Ukraine in the conditions of European integration: Science textbook], KNT, Kyiv, Ukraine.

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

3. Rosenzweig, P. (2013), *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, Library of Congress Cataloging-in-Publication Data, Washington, US.

4. Radin, A. (2017), *Hybrid Warfare in the Baltic*, National Security Research Division. RAND Corporation, Santa Monica, US.

5. Blank, S., Perkovich, G. and Levite, A. (2017), *Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press, Washington, US.

6. Nye, J. (2019), *Protecting Democracy in an Era of Cyber Information War*. Belfer Center for Science and International Affairs, Cambridge, US.

7. Hingant, J., Zambrano, M., Pérez, F., Pérez, I. and Esteve, M. (2018), "A Hybrid Intelligence System for Critical Infrastructures Protection", HYBINT, vol. 2018, pp. 1-13.

8. Iancu, N., Fortuna, A., Barna, C. and Teodor, M. (2016), "Countering Hybrid Threats: Lessons Learned from Ukraine", IOS Press, Amsterdam, NL.

9. Lapko, O. and Konarivska, O. (2015), "Modeling trends in the development of non-bank financial institutions in Ukraine", *Biznes Inform*, vol. 2, pp. 103-107.

10. Veselova, L. (2019), "Peculiarities of the state policy of Ukraine in the sphere of ensuring cyber security in the conditions of hybrid warfare", *Naukovyi visnyk Khersonskoho derzhavnoho universytetu*. *Seriia «Yurydychni nauky»*, vol. 2, pp. 23-27.

11. Sarkisian, L. and Samsonova, L. (2020), "Hybrid threats in trade and economic relations", *Aktualni problemy rozvytku ekonomiky rehionu*, vol. 16.2, pp. 62-76.

12. Hybrid CoE (2023), "Hybrid threats as a concept", available at: *https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/* (Accessed 07 May 2024).

13. Godfrey, S. (2008), *What is CMMI*, NASA, Washington, US.

14. Somayaji, A. and Forrest, S. (2000), "Automated Response Using System-Call Delays", *Proceedings of the 9th USENIX Security Symposium*, USENIX Association, Denver, pp. 185–198.

15. Karen R. and Merrill W. (2017), “Risk homeostasis in information security: challenges in confirming existence and verifying impact”, *NSPW '17: 2017 New Security Paradigms Workshop*, Association for Computing Machinery, New York, pp. 57-70.

16. Schrom, E. (2023), “Challenges in cybersecurity: Lessons from biological defense systems”, *Mathematical Biosciences*, vol. 362, pp. 47-73.

17. Levchenko, Ye. and Rabchun, A. (2010), “Optimization tasks of information security management”, *Suchasnyi zakhyst informatsii*, vol. 1, pp. 16-23.

18. Rabchun, A. (2012), “Optimization of total losses in the field of information protection”, *Bezpeka informatsii,* vol. 1(17), pp. 32-36.

19. Levchenko Ye., Demchyshyn, M. and Rabchun, A. (2011), “Mathematical models of economic management of information security”, *Systemni doslidzhennia ta informatsiini tekhnolohii*, vol. 4, pp. 88-96.

Стаття надійшла до редакції 07.05.2024 р.