УДК 004.94
DOI: 10.31733/2078-3566-2024-1-36-44

Олена ПАРШИНА©
доктор економічних наук, професор
(Університет митної справи та фінансів, м. Дніпро, Україна)

Юрій ПАРШИН©
доктор економічних наук, професор
(Інженерний навчально-науковий інститут ім. Ю. М. Потебні Запорізького національного університету, м. Запоріжжя, Україна)

КІБЕРБЕЗПЕКА В СУЧАСНИХ УМОВАХ ЗРОСТАННЯ ЗАГРОЗ НАЦІОНАЛЬНІЙ ТА СВІТОВІЙ БЕЗПЕЦІ

Зважаючи на умови наявної тенденції зростання загроз національній та світовій безпеці, акцентовано на доцільності глобального погляду на забезпечення кібербезпеки і безпеки критично важливих об'єктів та інфраструктур. Здійснено аналіз проблеми побудови сучасної моделі кібербезпеки, що повинна відображати основні процеси, котрі відбуваються в кібернетичному просторі, з метою оптимізації процесів захисту інформації. Для аналізу кількісної оцінки кібернетичної безпеки використано глобальний індекс кібербезпеки Global Cybersecurity Index. Порівняльну оцінку рівня кібербезпеки України здійснено на регіональному рівні з огляду на складові критерії. Аналіз динаміки обсягів витрат на технології кібербезпеки у світі дозволив встановити основні тенденції та прогнози глобальних витрат на захист від кіберзлочинності. Визначено ключові тренди розвитку галузі кібербезпеки із зазначенням набуття сектором кібербезпеки стратегічного пріоритету.

Ключові слова: *кібербезпека, загрози, національна безпека, захист інформації.*

Постановка проблеми. В умовах загострення глобальних конфліктів у сучасному світи спостерігається стійка тенденція зростання загроз національній та світовій безпеці. Після терактів 11 вересня 2001 р. було визначено доцільність глобального погляду на забезпечення безпеки критично важливих об'єктів та інфраструктур. На світовому рівні окреслені питання були поєднані в єдину систему боротьби з тероризмом й міграційною кризою після терористичних атак 13–14 листопада 2015 р. у Парижі. Інтегрований підхід до проблеми безпеки дозволив розпочати формування такої системи на міжнародному рівні під час економічного саміту G20 15 листопада 2015 р. в Анкарі.

Проведені дослідження сучасних процесів світової глобалізації [10] засвідчують формування багатополярної моделі світу, у межах якої з'являються нові центри сили з різними політичними та економічними інтересами. Внаслідок динамічного розвитку цих процесів посилюється нестабільність на міжнародному рівні та виникають збройні конфлікти.

За останні роки спостерігається динамічне зростання кібератак на державні органи, оборонно-промисловий комплекс, об'єкти критичної інфраструктури, ІТ-мережі та засоби масової інформації, що, безумовно, негативно впливає на рівень національної безпеки нашої держави. Проведений моніторинг реалізації Стратегії національної безпеки дозволяє відзначити значне зростання інтенсивності кібернетичних атак, що спрямовані на інформаційно-телекомунікаційну інфраструктуру в Україні. Зокрема,

© О. Паршина, 2024
ORCID iD: https://orcid.org/0000-0002-7836-0140
parschina@ukr.net

© Ю Паршин, 2024
ORCID iD: https://orcid.org/0000-0002-8650-5303
parshin22@ukr.net

відповідно до проведених розслідувань зазначено [26], що було здійснено не менше 5 тис. кібератак проти органів державної влади та критично важливої інфраструктури нашої країни. 14 січня 2022 р. майже 70 українських урядових сайтів, зокрема Міністерства закордонних справ України, Кабінету Міністрів України та РНБО України, були тимчасово зіпсовані російськими хакерами [7].

Слід зазначити, що, незважаючи на складну політичну та економічну ситуацію, Україна змогла здобути перевагу у протистоянні значній кількості кібератак та інформаційній агресії. Зокрема, за період із січня до червня 2023 р. було відбито 762 кібератаки на об'єкти критичної інфраструктури та сфери бізнесу нашої країни [7].

З огляду на наявні тенденції зростання кібератак зазначимо, що проблема забезпечення інформаційної безпеки, кібербезпеки та захисту інформаційних ресурсів визначається як пріоритетна у сфері державної політики національної безпеки України.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Вирішення проблеми забезпечення кібербезпеки та інформаційної безпеки сучасні вчені та практики пов'язують із розкриттям природи явища, що полягає у порушенні властивостей інформації, та розробкою практичних методів, моделей та систем захисту інформації.

Сучасні вчені акцентують наважливості побудови сучасної моделі кібербезпеки, що повинна відображати основні процеси, котрі відбуваються в кібернетичному просторі, з метою оптимізації процесів захисту інформації. Зокрема, С. Головань, О. Голубенко, А. Карпов, І. Опірський, О. Петров, М. Попова, В. Хорошко, Ю. Яремчук пропонують представити такі процеси у загальному вигляді як процеси розподілу і використання ресурсів, що виділяються на захист інформації [4; 8; 11].

Сучасними вченими розроблено численну кількість моделей та з метою упорядкування їхньої розмаїтості запропоновано використання різних критеріїв. Зокрема, моделі класифікують за способами реалізації, за характером процесів у системі, за характером підходу до моделювання об'єкта, за призначенням об'єктів дослідження, за характеристиками досліджуваного об'єкта тощо. З метою проведення системної класифікації моделей І. Опірським було запропоновано спрощену класифікацію моделей захисту інформації [8].

При розробці моделей інформаційної безпеки вчені використовують різні наукові підходи. Зокрема, Д. Дячков розглядає формування структурної моделі інформаційної безпеки на підґрунті використання положень комплексного підходу [5]. О. Балалаєва та А. Кочукова пропонують функціональну модель комплексної системи захисту інформації [2]. Деякі вчені пропонують представити комплексну систему захисту інформації у вигляді орієнтованого графа, де вершинам відповідають компоненти об'єкта критичної інфраструктури, а ребрам – інформаційні потоки між цими об'єктами [11].

З метою проведення ґрунтовних досліджень процесів захисту інформації та отримання необхідного рівня деталізації й розробки заходів із забезпечення інформаційної безпеки вчені приділяють особливу увагу питанням моделювання. Зокрема, для моделювання комплексної системи захисту інформації з точки зору поточного опису процесів С. Черемних, І. Семенов та В. Ручкін пропонують використовувати методологію IDEF – технологію опису бізнес-процесів у цілому як множини взаємозалежних дій або функцій [14]. З огляду на практичний досвід у цій галузі вважаємо за доцільне використовувати аналітичні технології та платформи для проведення моделювання складних інформаційних процесів [10; 9; 19].

В умовах ведення проти України гібридної війни спостерігається тенденція зростання загроз та кібератак із пошкодженням об'єктів критичної інфраструктури. Стратегією національної безпеки України визначено перелік загроз безпеці критичної інфраструктури, котрі насамперед полягають у значній зношеності основних фондів об'єктів інфраструктури України [13]. Крім того, було зроблено акцент на недостатньому рівні захищеності критичної інфраструктури від терористичних посягань і диверсій, а також на неефективному управлінні безпекою критичної інфраструктури та систем життєзабезпечення.

Тому проблема забезпечення кібернетичного захисту в умовах стійкого зростання загроз національній та світовій безпеці потребує проведення подальших досліджень.

Мета статті полягає в дослідженні сучасного стану забезпечення кібербезпеки в

умовах загострення нестабільності на міжнародному рівні та зростання загроз національній і світовій безпеці.

Виклад основного матеріалу. Забезпечення кібербезпеки та захисту інформації має здійснюватися у напрямі вирішення трьох взаємопов'язаних завдань: конфіденційності, цілісності та доступності [1; 6; 12]. Зокрема, з огляду на три основні складові інформаційну безпеку визначено у міжнародному стандарті як «збереження конфіденційності, цілісності та доступності інформації».

Вважається, що проблема комп'ютерного захисту бере свій початок у 1970-ті рр. [25]. Історія кібербезпеки починається з 1972 р., коли стартував дослідницький проєкт ARPANET (мережа агентства перспективних дослідних проєктів), що був по суті попередником Інтернету [3]. У мережі ARPANET вперше з'явилися протоколи для віддалених комп'ютерних мереж. Отже, інформаційна безпека спрямована на захист даних незалежно від місця знаходження інформації або засобу її використання, а кібербезпека має забезпечувати захисні механізми саме в кібернетичному просторі. Таким чином, під кібербезпекою будемо розуміти процес захисту інформації в кіберпросторі, тобто у віртуальній реальності, що існує як «всередині» комп'ютерів, так і «всередині» комп'ютерних мереж.

Звернемо увагу на те, що на сучасному етапі розвитку кіберзлочинність є ключовою загрозою світовій економіці. Про важливість питань, пов'язаних із кіберзахистом, свідчить те, що вони постійно виходять на порядок денний на міжнародних зустрічах «Великої двадцятки» та на майданчику ООН. Міністри телекомунікацій та інформаційних технологій різних країн також обговорюють питання цього напряму, оскільки вони безпосередньо торкаються елементів управління критичною інфраструктурою Інтернету.

З метою кількісної оцінки кібернетичної безпеки використовуються загальновизнані рейтинги, зокрема: Global Cybersecurity Index (GCI) – глобальний індекс кібербезпеки [20], National Cyber Security Index (NCSI) – національний індекс кібербезпеки [16], National Cyber Power Index (NCPI) – національний індекс кіберпотужності [23] та Cyber Readiness Index (CRI) – національний індекс кіберготовності [15].

Експерти Міжнародної спілки електрозв'язку ООН (International Telecommunication Union) щороку складають рейтинг країн за рівнем кібербезпеки. Перша редакція глобального індексу кібербезпеки (GCI) була опублікована у 2015 р. з метою вимірювання прихильності 193 держав-членів Міжнародної спілки електрозв'язку (МСЕ) до кібербезпеки задля визначення галузі для покращення та спонукання країн до відповідних дій шляхом підвищення обізнаності про стан кібербезпеки в усьому світі.

Національний індекс кібербезпеки (NCSI) – це глобальний індекс, що дозволяє в режимі реального часу здійснювати вимірювання готовності країн щодо запобігання кіберзагрозам та управління кіберінцидентами. Цей індекс, на відміну від попередньо розглянутого, сфокусований на окремих аспектах кібербезпеки, котрі запроваджуються урядами країн на національних рівнях за такими чотирма напрямами – сфера чинного законодавства, сфера сформованих інституцій, сфера співпраці та сфера результатів.

Використання національного індексу кіберпотужності (NCPI) дозволяє вимірювати державні стратегії, можливості для оборонних і руйнівних операцій, розподіл ресурсів та можливості приватного сектора в країні [27]. Рейтинг National Cyber Power Index 2022 був складений для 30 держав, за результатами якого Україна посідає 26 місце за загальними оцінками: з найвищими –захисту, нападу і можливостей спостереження і нижчими – щодо норм, інтелекту, комерції, контролю інформації [21].

За результатами рейтингу з використанням глобального індексу кібербезпеки (GCI) Global Cybersecurity Index 2020 [17] перше місце посіли Сполучені Штати Америки з індексом 100 балів. Друге місце поділяють Великобританія та Саудівська Аравія з індексом 99,54. На третьому місці – Естонія з індексом 99,48. Україна займає 78 місце з показником 65,93 бали зі 194 учасників оцінювання. Індекси окремих країн надано у табл. 1 [17].

Таблиця 1

Рейтинг країн за рівнем кібербезпеки

Країни	Індекс	Ранг
США	100	1
Великобританія	99,54	2
Саудівська Аравія	99,54	2
Естонія	99,48	3
Південна Корея	98,52	4
Сінгапур	98,52	4
Іспанія	98,52	4
Росія	98,06	5
ОАЕ	98,06	5
Малайзія	98,06	5
…	…	
Болгарія	67,38	77
Україна	65,93	78
Пакистан	64,88	79
…	…	
Ємен	0	182

Глобальний індекс кібербезпеки (GCI) [17; 20] дозволяє здійснити комплексну оцінку кібербезпеки всіх країн світу за п'ятьма складовими критеріями:

– юридичним (Legal Measures) – наявність правових систем і структур, що займаються питаннями кібербезпеки та кіберзлочинів;

– технічним (Technical Measures) – технічні можливості у сфері кібербезпеки;

– організаційної підготовленості (Organizational Measures) – існування інститутів координації політики та стратегій розвитку кібербезпеки на державному рівні;

– розвитку освітнього та дослідницького потенціалу країни (Capacity Development) – наявність науково-дослідних, освітніх та підготовчих програм, а також сертифікованих фахівців та держустанов, що сприяють нарощуванню потенціалу у сфері інформаційної безпеки;

– готовності до співпраці (Cooperative Measures) – наявність партнерства, механізмів співробітництва та систем обміну інформацією з іншими країнами.

У регіональному рейтингу (серед країн Європи) з використанням глобального індексу кібербезпеки Україна посіла 39 місце (з-поміж 42 країн Європи) [17]. На рис. 1 представимо у графічному вигляді оцінку рівня кібербезпеки з урахуванням п'яти критеріїв для України та порівняємо зі складовими індексу кібербезпеки сусідніх країн, зокрема Молдови, Польщі, Румунії та Чехії.

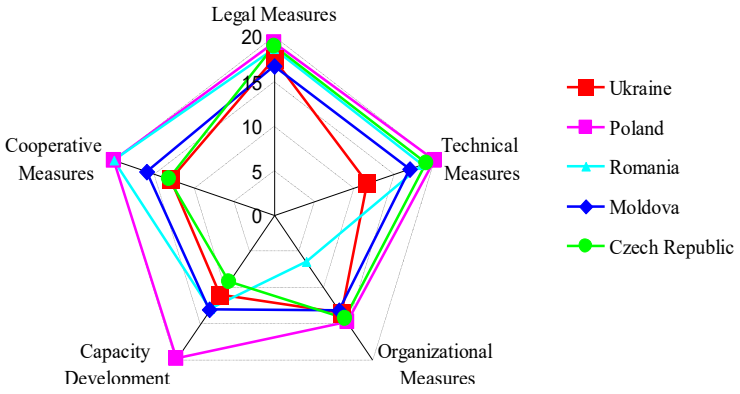

Рис. 1. Графічна інтерпретація оцінки кібербезпеки з урахуванням п'яти складових критеріїв глобального індексу

Аналіз за кількісними показниками з використанням складових критеріїв глобального індексу кібербезпеки дозволяє зазначити, що за критерієм організаційної підготовленості (Organizational Measures) показник України (13,6) перевищує аналогічний показник Румунії (6,42). Позитивну ситуацію можна спостерігати й за показником розвитку освітнього та дослідницького потенціалу країни (Capacity Development) – показник України (10,94) перевищує аналогічний показник Чехії (9,14). За всіма іншими показниками спостерігається відставання від аналогічних показників сусідніх країн.

Забезпечення високого рівня кібернетичного захисту потребує відповідних фінансових ресурсів та впровадження інвестиційних проєктів. У світовому масштабі спостерігається постійне збільшення обсягів витрат на технології кібербезпеки. Динаміку витрат за аналітичними даними компанії Canalys [19] надано на рис. 2. Представлені сумарні значення витрат сформовані з урахуванням показників із шести ключових сегментів ринку IT-технологій, як-от: засоби забезпечення безпеки кінцевих елементів (точок); інструменти мережного захисту; програмне забезпечення для пошуку та аналізу вразливостей; веббезпека та захист електронної пошти; безпека даних та системи керування доступом до ідентифікаційних даних.

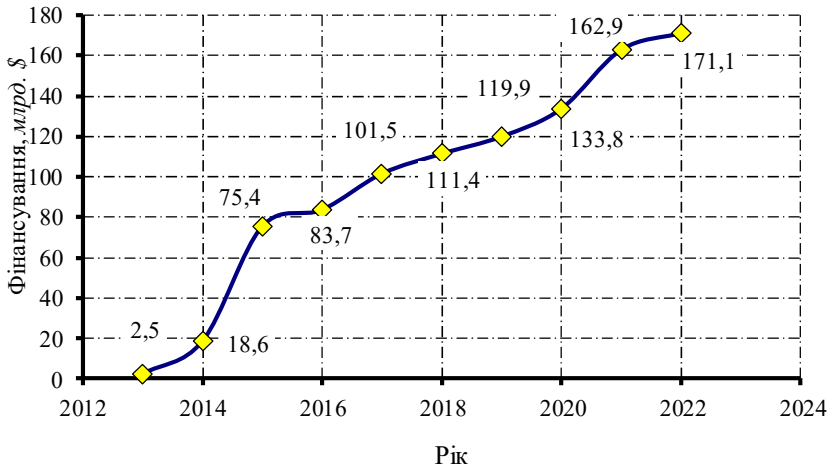

Рис. 2. Динаміка обсягів витрат на технології кібербезпеки у світі

Аналітики компанії Kaspersky провели дослідження за тематичним напрямом «Інформаційна безпека бізнесу» з метою з'ясування витрат компаній на кіберзахист із формуванням прогнозів цих витрат на майбутнє. Розглядаючи різні регіони, зазначимо, що витрати на кіберзахист теж є різними. Наприклад, у США та Канаді у невеликих організаціях у 2022 р. витрати становили у середньому 350 тис. дол. при загальному бюджеті на розвиток IT 750 тис. дол., у великих компаніях – 3,750 млн дол. при загальному бюджеті 17,25 млн дол. Щорічні збільшення витрат на кіберзахист плануються у середньому на 13–14%.

У регіоні МЕТА (Близький Схід, Африка та Туреччина) у невеликих організаціях у 2022 р. бюджет на IT-розвиток склав 375 тис. дол., а на кіберзахист – 150 тис. дол., у великих компаніях, відповідно, бюджет – 18,5 млн дол., кіберзахист – 7,5 млн дол. Щодо планування витрат на наступні періоди: малі та середні підприємства планують їх збільшення на рівні 15 %, а великі компанії – 18 %.

Аналітики інвестиційного проєкту First Trust NASDAQ Cybersecurity ETF (NASDAQ: CIBR) прогнозують, що до 2025 р. глобальні витрати від кіберзлочинності досягнуть 10,5 трлн дол. США [7].

За результатами прогнозування провідного експерта з технологічних ринків у межах проведеного дослідження Juniper Research було виявлено, що до 2028 р. витрати на кібербезпеку промислових кінцевих точок досягнуть 7,8 млрд дол. США [7]. До

основних причин такого збільшення слід віднести такі, як: підвищення складності ІТ-інфраструктури компанії, необхідність розширення компетенцій фахівців із кібербезпеки та поява нових загроз і ризиків у зв'язку з геополітичними факторами.

З-поміж основних проблем кібербезпеки для бізнесу доцільно зазначити такі: захист даних; витрати на забезпечення безпеки (з технологічної точки зору) середовищ; проблеми, що виникають у зв'язку із запровадженням хмарної інфраструктури.

Фахівці багатьох провідних компаній у галузі кіберзахисту дійшли висновку: для того, щоб ризики кібератак і витоків даних були максимально низькими, а ефективність вкладених у кібербезпеку інвестицій – максимально високими, необхідно використовувати надійний захист для кінцевих пристроїв із можливостями детектування загроз і своєчасного реагування на них. З огляду на дослідження у сфері безпеки, що було проведено фахівцями компанії Hikvision, доцільно виокремити такі ключові тренди [16]:

– динамічний розвиток штучного інтелекту з поступовим поєднанням Інтернету речей та штучного інтелекту;

– розвиток хмарних технологій та послуг, заміна традиційних сховищ даних конвергентними системами;

– розвиток та поширення біометричних технологій контролю доступу;

– запровадження в системах безпеки моделей типу Zero Trust (моделі нульової довіри: мінімум довіри, максимум перевірок).

Також можна очікувати зростання попиту на деталізацію зображення у складних умовах роботи систем безпеки, а також на пристрої безпеки, що оснащені сонячними батареями, тощо.

Таким чином, за результатами проведеного дослідження слід констатувати наявність значного попиту на ефективні рішення з кібербезпеки. Саме тому компанії, що працюють у секторі кіберзахисту, мають реальні можливості для отримання вигоди за результатами впровадження інвестиційних проектів. Зокрема, ґрунтуючись на прогнозах щодо зростання до 2028 р. ринку хмарних технологій та безпеки Інтернету речей (IoT) до 23 %, а також середньорічного зростання ринку штучного інтелекту до 22 %, що в ціновому еквіваленті оцінюється приблизно на рівні 63 млрд дол. США [7], слід звернути увагу на використання реальних можливостей у цьому напрямі для приватних інвесторів.

Серед провідних постачальників інструментів кібербезпеки з їхнєю долею витрат на ринку можна виокремити такі компанії (табл. 2).

Таблиця 2

Провідні постачальники інструментів кібербезпеки на світовому ринку

№	Доля на ринку, %	Назва компанії	Посилання
1.	7,9	Palo Alto Networks	https://www.paloaltonetworks.com/
2.	6,8	Fortinet	https://www.fortinet.com/
3.	6,1	Cisco	https://www.cisco.com/
4.	3,8	Check Point	https://www.checkpoint.com/
5.	3,2	CrowdStrike	https://www.crowdstrike.com/
6.	3,1	IBM	https://www.ibm.com/us-en
7.	3,0	Okta	https://www.okta.com/uk/
8.	2,9	Microsoft	https://www.microsoft.com/uk-ua
9.	2,9	Trellix	https://www.trellix.com/en-us
10.	2,6	Symantec	https://www.broadcom.com/products/cybersecurity/endpoint
11.	2,4	Splunk	https://www.splunk.com/
12.	2,3	Trend Micro	https://www.trendmicro.com/
13.	52,9	Інші	

Водночас в інформаційно-аналітичному дайджесті зазначено, що актуальною темою протягом 2024 р. залишається дефіцит фахівців із навичками, необхідними для захисту організацій від кібератак [7]. Про збільшення дефіциту кадрів у сфері кібербезпеки в усіх регіонах світу засвідчують результати дослідження Cybersecurity Workforce Study. Зростає попит на розробку та впровадження нових технологій, таких як: виявлення загроз на основі штучного інтелекту та реагування на них, захисту даних,

Інтернету речей (IoT), а також технологій, методів та програмного забезпечення з використанням штучного інтелекту.

Висновки. За результатами проведених досліджень слід констатувати наявність зростання кіберзагроз з негативними наслідками впливу на рівень національної та світової безпеки. Зважаючи на прогресивні тенденції розвитку інформаційної галузі та технологій штучного інтелекту, слід очікувати у 2024 р. набуття сектором кібербезпеки стратегічного пріоритету. У зв'язку з цим питання забезпечення персональних даних, безпечного використання хмарних технологій, забезпечення функціонування об'єктів критичної інфраструктури набувають особливого значення та потребують проведення фундаментальних і прикладних досліджень.

Список використаних джерел

1. Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. Нормативно-правовий довідник з охорони інформації в Україні. Київ : ДУІКТ, 2010. 155 с.
2. Балалаєва О. Ю., Кочукова А. В. Моделювання і реінжиніринг процесів системи захисту інформації на основі теорії графів і методології IDEF. *Наука та виробництво*. 2020. Вип. 22. С. 9–14.
3. Гладун А. Я. Арпанет. *Велика українська енциклопедія*. URL : https://vue.gov.ua/АРПАНЕТ.
4. Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М., Яремчук Ю. Є. Політика інформаційної безпеки. Луганськ : Вид-во СНІ ім. В. Даля. 2009. 300 с.
5. Дячков Д. В. Формування моделі інформаційної безпеки. *Причорноморські економічні студії.* 2017. С. 263–267.
6. Захист бази даних від несанкціонованого доступу. *IITD.* URL : https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/.
7. Кібербезпека в інформаційному суспільстві : інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В.І.Вернадського. Київ, 2023. № 10. 320 с.
8. Опірський І. Р. Классифікація моделей захисту інформації в інформаційних мережах держави. *Науковий вісник НЛТУ України*. 2015. Вип. 25(10). С. 329–335.
9. Паршина О. А., Паршин Ю. І., Воскобойник В. О. Концептуальні аспекти забезпечення конкурентоспроможності комплексних систем захисту інформації // Проблеми правового, фінансового та економічного забезпечення розвитку національної економіки (галузевий та територіальний аспекти) : монографія / за ред. Л. М. Савчук, Л. М. Бандоріної. Дніпро : Пороги, 2021. 468 с. С. 194–206.
10. Паршина О. А., Паршина М. Ю., Чумак Т. В. Фактори економічного розвитку країн в умовах загострення глобальних проблем світової безпеки. *Приазовський економічний вісник*. 2021. Вип. 2(25). С. 3–7. URL : http://pev.kpu.zp.ua/journals/2021/2_25_ukr/3.pdf.
11. Попова М. С., Карпов А. П. Застосування теорії графів для виявлення потенційних загроз безпеці інформації. *Проблеми сучасної науки та освіти*. 2016. № 35(77). С. 1–3.
12. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.
13. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 р. № 287/2015. URL : http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7.
14. Черемних С.В., Семенов И.О., Ручкзін В.С. Структурний аналіз систем. IDEF-технології. К.: Статистика України, 2018. 243 с.
15. Cyber Readiness Index Country Profiles. *Potomac Institute for Policy Studies.* URL : https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.
16. Cybersecurity center. *Hikvision.* URL : https://www.hikvision.com/en/support/cybersecurity/.
17. Global Cybersecurity Index 2020. 172 p. URL : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
18. National Strategy to Increase Foreign Direct Investment in Ukraine. 96 p. URL : https://ukraineinvest.gov.ua/wp-content/uploads/2021/08/FDI-Strategy-Section-2-Digital-Infrastructure-ENG.pdf.
19. Parshyna O., Parshyn Yu. Analytical platform to provide competitiveness of ore-mining machinery manufacturing. *Mining of Mineral Deposits*. 2020. Vol. 14. Issue 3. P. 61–70. URL : http://mining.in.ua/articles/volume14_3/08.pdf.
20. Polotai O., Lagun A., Kukharska N., Samotyy V. Trend extrapolation method for qualitative prognosis of the global cybersecurity index in Ukraine. ISTCMTM. 2020. Vol. 81(4). P. 30–34. URL : https://science.lpnu.ua/istcmtm/all-volumes-and-issues/volume-81-no4-2020/trend-extrapolation-method-qualitative-prognosis.
21. The history of cybersecurity. *Avast.* URL : https://blog.avast.com/history-of-

cybersecurity-avast.

22. Ukraine Identifies Russian FSB Officers Hacking As Gamaredon Group. *The Hacker News.* URL : https://thehackernews.com/2021/11/ukraine-identifies-russian-fsb-officers.html.

23. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Cambridge : Harvard Kennedy School, 2022. 66 p. URL : https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

Надійшла до редакції 22.01.2024
Прийнято до опублікування 06.02.2024

References

1. Artemov, V. Iu., Lienkov, O. S., Pashkov, A. S., Stadnik, O. M., Khoroshko, V. O. (2010) Normatyvno-pravovyi dovidnyk z okhorony informatsii v Ukraini [Regulatory and legal guide on information protection in Ukraine]. Kyiv : DUIKT. 155 p. [in Ukr.].

2. Balalaieva, O. Iu., Kochukova, A. V. (2020) Modeliuvannia i reinzhynirynh protsesiv systemy zakhystu informatsii na osnovi teorii hrafiv i metodolohii IDEF [Modelling and reengineering of information protection system processes based on graph theory and IDEF methodology]. *Nauka ta vyrobnytstvo*. № 22, pp. 9–14. [in Ukr.].

3. Hladun, A. Ia. Arpanet [Arpanet]. *Velyka ukrainska entsyklopediia.* URL : https://vue.gov.ua/АРПАНЕТ. [in Ukr.].

4. Holubenko, O. L., Khoroshko, V. O., Petrov, O. S., Holovan, S. M., Yaremchuk, Yu. Ie. (2009) Polityka informatsiinoi bezpeky [Information security policy]. Luhansk : Vyd-vo SNI im. V.Dalia. 300 p. [in Ukr.].

5. Diachkov, D. V. (2017) Formuvannia modeli informatsiinoi bezpeky [Formation of information security model]. *Prychornomorski ekonomichni studii,* pp. 263–267. URL : https://dspace.pdau.edu.ua/items/950422ff-df3f-4754-9efe-fac01de7a98b. [in Ukr.].

6. Zakhyst bazy danykh vid nesanktsionovanoho dostupu [Protection of the database against unauthorized access]. *IITD.* URL : https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/ [in Ukr.].

7. Kiberbezpeka v informatsiinomu suspilstvi [Cyber security in the information society] : informatsiino-analitychnyi daidzhest / vidp. red. O. Dovhan ; uporiad. O. Dovhan, L. Lytvynova, S. Dorohykh. Derzhavna naukova ustanova «Instytut informatsii, bezpeky i prava NAPrN Ukrainy» ; Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho. Kyiv, 2023. № 10. 320 p. [in Ukr.].

8. Opirskyi, I. R. (2015) Klassyfikatsiia modelei zakhystu informatsii v informatsiinykh merezhakh derzhavy [Classification of information protection models in state information networks]. *Naukovyi visnyk NLTU Ukrainy*. № 25(10), pp. 329–335 [in Ukr.].

9. Parshyna, O. A., Parshyn, Yu. I., Voskoboinyk, V. O. (2021) Kontseptualni aspekty zabezpechennia konkurentospromozhnosti kompleksnykh system zakhystu informatsii [Conceptual aspects of ensuring the competitiveness of complex information protection systems] // Problemy pravovoho, finansovoho ta ekonomichnoho zabezpechennia rozvytku natsionalnoi ekonomiky (haluzevyi ta terytorialnyi aspekty) : monohrafiia / za red. L. M. Savchuk, L. M. Bandorinoi. Dnipro : Porohy. 468 p., pp. 194–206. [in Ukr.].

10. Parshyna, O. A., Parshyna, M. Iu., Chumak, T. V. (2021) Faktory ekonomichnoho rozvytku krain v umovakh zahostrennia hlobalnykh problem svitovoi bezpeky [Factors of economic development of countries in the conditions of aggravation of global problems of world security]. *Pryazovskyi ekonomichnyi visnyk*. Vyp. 2(25), pp. 3–7. URL : http://pev.kpu.zp.ua/journals/2021/2_25_ukr/3.pdf. [in Ukr.].

11. Popova, M. S., Karpov, A. P. (2016) Zastosuvannia teorii hrafiv dlia vyiavlennia potentsiinykh zahroz bezpetsi informatsii [Application of graph theory in identifying potential information security threats]. *Problemy suchasnoi nauky ta osvity*. № 35(77), pp. 1–3. [in Ukr.].

12. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the main principles of ensuring cyber security of Ukraine] : Zakon Ukrainy vid 5 zhovtnia 2017 r. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukr.].

13. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine «On the National Security Strategy of Ukraine»] : Ukaz Prezydenta Ukrainy vid 26 travnia 2015 r. № 287/2015. URL : http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7. [in Ukr.].

14. Cheremnykh, S. V., Semenov, Y. O., Ruchkyn, B. C. (2018) Strukturnyi analiz system IDEF-tekhnolohii [Structural analysis of systems. IDEF technologies]. Kyiv : Statystyka Ukrainy. 243 p. [in Ukr.].

15. Cyber Readiness Index Country Profiles. *Potomac Institute for Policy Studies.* URL : https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

16. Cybersecurity center. *Hikvision.* URL : https://www.hikvision.com/en/support/cybersecurity/.

17. Global Cybersecurity Index 2020. 172 p. URL : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

18. National Strategy to Increase Foreign Direct Investment in Ukraine. 96 p. URL : https://ukraineinvest.gov.ua/wp-content/uploads/2021/08/FDI-Strategy-Section-2-Digital-Infrastructure-ENG.pdf

19. Parshyna O., Parshyn Yu. Analytical platform to provide competitiveness of ore-mining machinery manufacturing. *Mining of Mineral Deposits*. 2020. Vol. 14. Issue 3. P. 61–70. URL : http://mining.in.ua/articles/volume14_3/08.pdf.

20. Polotai O., Lagun A., Kukharska N., Samotyy V. Trend extrapolation method for qualitative prognosis of the global cybersecurity index in Ukraine. ISTCMTM. 2020. Vol. 81(4). P. 30–34. URL : https://science.lpnu.ua/istcmtm/all-volumes-and-issues/volume-81-no4-2020/trend-extrapolation-method-qualitative-prognosis.

21. The history of cybersecurity. *Avast.* URL : https://blog.avast.com/history-of-cybersecurity-avast.

22. Ukraine Identifies Russian FSB Officers Hacking As Gamaredon Group. *The Hacker News.* URL : https://thehackernews.com/2021/11/ukraine-identifies-russian-fsb-officers.html.

23. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Cambridge : Harvard Kennedy School, 2022. 66 p. URL : https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

ABSTRACT

Olena Parshyna, Yuriy Parshyn. Cyber security in the current conditions of growing threats to national and global security. Taking into account the conditions of the existing trend of growing threats to national and global security, emphasis is placed on the expediency of a global approach to ensuring cyber security and the security of critically important objects and infrastructures. An analysis of the problem of building a modern cyber security model, which should reflect the main processes taking place in the cyberspace, with the aim of optimizing information protection processes, was carried out.

The Global Cybersecurity Index was used to analyze the quantitative assessment of cyber security. A comparative assessment of the level of cyber security of Ukraine was carried out at the regional level, taking into account the constituent criteria. Analysis of the dynamics of spending on cyber security technologies in the world made it possible to establish the main trends and forecasts of global spending on protection against cybercrime. The key trends in the development of the cyber security industry have been identified, indicating that the cyber security sector has become a strategic priority.

Keywords: *cyber security, threats, national security, information protection.*

УДК 343.32(477)
DOI: 10.31733/2078-3566-2024-1-44-51

Роман КАТОРКІН©
доктор філософії (право)
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

ДЕТЕРМІНАНТИ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ

Здійснено аналіз детермінантів такого виду кримінальних правопорушень проти основ національної безпеки України, як колабораційна діяльність.

Зазначено, що широкомасштабна війна, що її російська федерація розв'язала проти України у лютому 2022 р., стала потужним чинником поширення цілого комплексу актів деліктної поведінки, зокрема колабораційної діяльності.

Акцентовано, що основними детермінантами колабораційної діяльності є: російська пропаганда, котру проводить держава-терорист у межах інформаційної війни проти України; соціально-економічні чинники, викликані війною; недоліки у сфері національно-патріотичного виховання; прогалини у чинному законі про кримінальну відповідальність тощо.

Ключові слова: *детермінанти кримінальних правопорушень, злочин, кримінальне правопорушення, колабораційна діяльність, чинники злочинності.*

ORCID iD: https://orcid.org/0000-0002-0115-8198
katorkinroman@gmail.com