УДК 338.242(477)
JEL O32
DOI: https://doi.org/10.26906/EiR.2022.1(84).2540

АНАЛІТИЧНИЙ ВИМІР КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ЗРОСТАННЯ ВИКЛИКІВ ТА ЗАГРОЗ

Онищенко Світлана Володимирівна*, доктор економічних наук, професор
Глушко Аліна Дмитрівна, кандидат економічних наук, доцент**
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

**ORCID 0000-0002-6173-4361*
***ORCID 0000-0002-4086-1513*

Стаття отримана редакцією 06.04.2022 р.
The article was received by editorial board on 06.04.2022

Постановка проблеми. Стрімкий розвиток процесів цифровізації став джерелом не лише нових можливостей, але й ризиків та загроз, в першу чергу інформаційній безпеці національній економіці. Поряд з традиційними загрозами, таким як промислове шпигунство, навмисне і ненавмисне розголошення конфіденційної інформації та комерційної таємниці працівниками, недобросовісні дії конкурентів, включаючи шкоду діловій репутації, втручання сторонніх осіб в інформаційні системи і мережі, порушення цілісності баз даних тощо, створюється ряд додаткових загроз інформаційним ресурсам і технологіям в економіці, методи діагностики і протидії яким поки що відпрацьовані не в повній мірі. В першу чергу, це загрози, які пов'язані з кібератаками, розкриттям персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерних програм тощо. За умов постійного зростання кіберризиків і кіберзагроз важливим є моніторинг рівня кібербезпеки України, висвітлення основних проблем розбудови національної системи кіберзахисту та визначення напрямів їх вирішення.

Огляд останніх досліджень та публікацій. Проблеми забезпечення безпеки національної економіки широко актуалізуються у працях вітчизняних науковців, зокрема О. Барановського, З. Варналія, О. Власюка, В. Гейця, Я. Жаліла, М. Єрмошенка, В. Шлемка, Н. Юрків та багатьох інших. Теоретичним та практичним аспектам забезпечення інформаційної безпеки присвячено праці таких науковців як: Н. Грабар, Б. Кормич, В. Петрик, Г. Яровенко та інших.

Питанням формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері присвятили свої праці такі науковці: Сопілко І.В., Куцаєв В.В., Живило Є.О., Мінін Д.С., Бурячок В.Л., Гнатюк С.О. та інші. Проте, незважаючи на значні наукові здобутки у зазначеній сфері, питання забезпечення кібербезпеки в Україні залишається актуальним.

Постановка завдання. Метою дослідження є дослідження кібербезпеки Україні в умовах зростання викликів та загроз в інформаційному просторі, визначення основних проблем національної системи кіберзахисту та визначення напрямів їх вирішення.

Основні результати дослідження. Розвиток ІТ-технологій поряд з безперечними перевагами стали причиною поглиблення ризиків та загроз в інформаційному середовищі, зокрема кіберпросторі. Так, якщо на початку 2020 року кількість кібератак у світі складала близько 5 тисяч за тиждень, то на початку 2021 року їхня кількість зросла до 200 тисяч [1]. При цьому 19% усіх кібератак у світі, зафіксованих у 2021 році, було скоєно проти України (на першому місці серед країн, проти яких спрямовані кібератаки – США) (рис. 1). Для порівняння, частка Бельгії, Німеччини та Японії не перевищує 3% [2]. Отже, Україна посідає друге місце у світових рейтингах за кількістю кібератак, які спрямовані, в першу чергу, на об'єкти критичної інфраструктури країни, тобто такі галузі як енергетична, фінансова, телекомунікаційна тощо, та державні електронні інформаційні ресурси, порушення функціонування яких є загрозою національним інтересам [3].

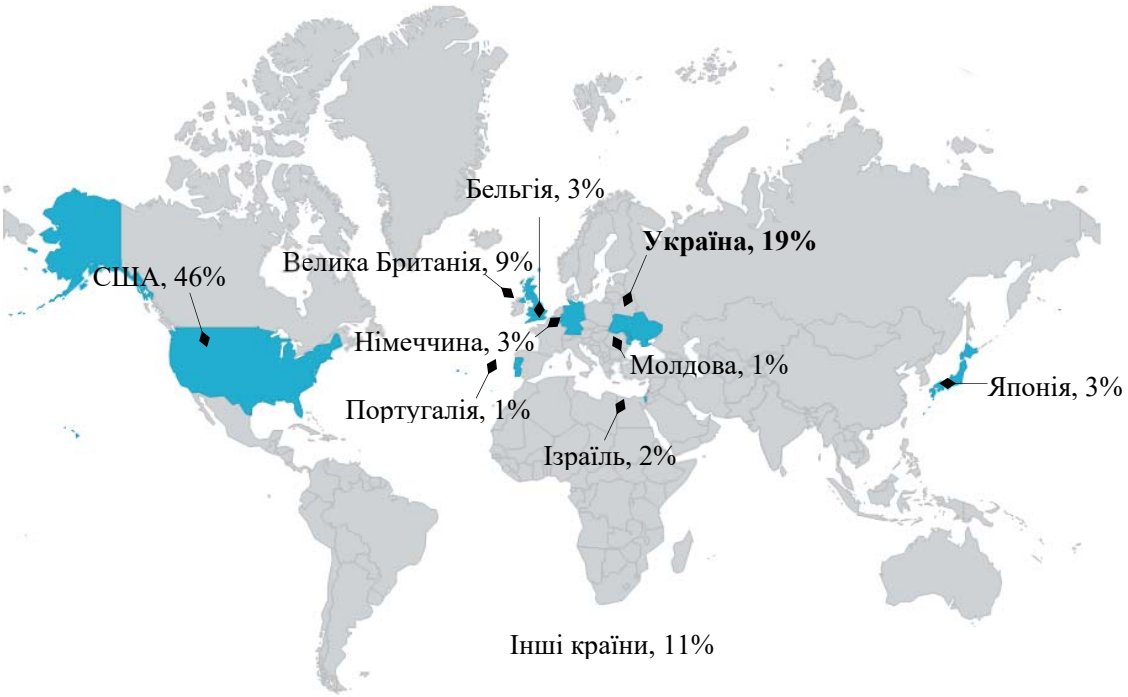

Рис. 1. Картосхема кібератак на країни світу за 2021 рік

Джерело: складено авторами за [2]

Згідно з даними компанії Microsoft найбільше кібератак протягом 2021 року було здійснено з території російської федерації – 58% усієї зафіксованої кількості. Друге місце серед країн, з територій яких здійснювались кібератаки, посіла Північна Корея (23%), а третє – Іран (11%) (рис. 2).

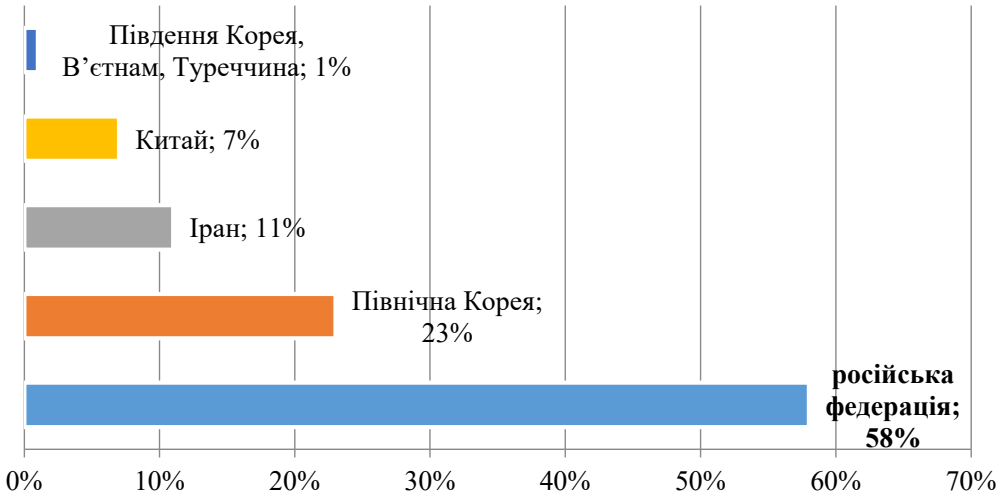

Рис. 2. Кібератаки за країнами походження за 2021 рік

Джерело: складено авторами за [2]

З початку 2022 року російська федерація розгортає кібервійну проти України – інтенсивність кібератак зросла: лише у січні було виявлено вже 6,8 млн підозрілих подій інформаційної безпеки, 25,5 тис. потенційних кіберінцидентів та зупинено 121 кібератаку. Для порівняння у квітні 2021 року фахівцями Служби безпеки України було виявлено 1,5 млн підозрілих подій та припинено 53 критичні кіберінциденти [4]. За січень-лютий 2022 року на об'єкти критичної інфраструктури та державні інформаційні ресурси України було здійснено 436 кібератак у порівнянні з 64 за такий же період 2021 року. Наймасштабніші з них представлено на рисунку 3.

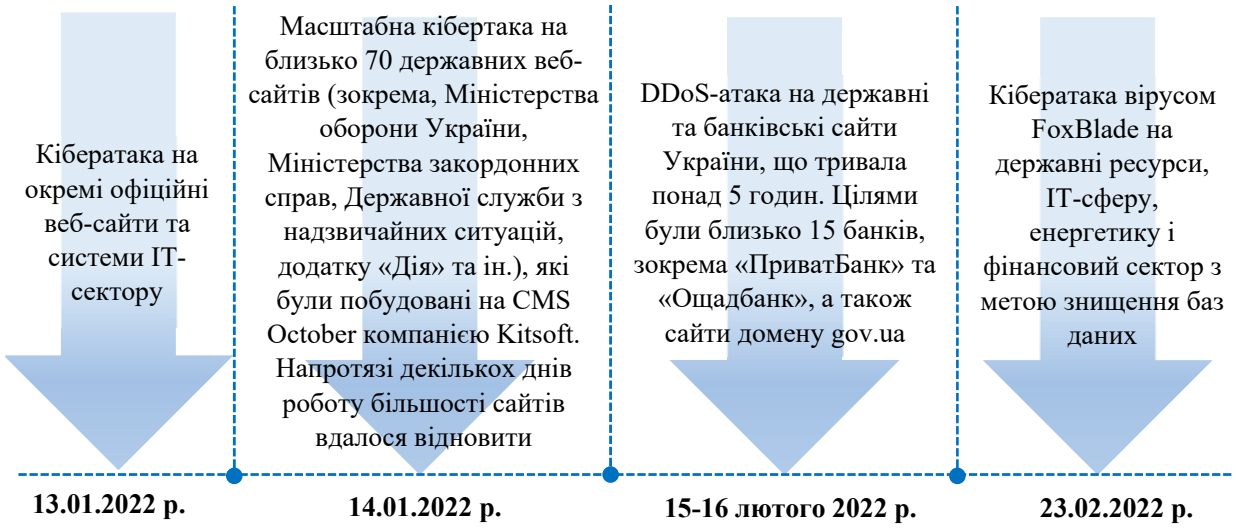

Рис. 3. Кібератаки на об'єкти критичної інфраструктури та державні інформаційні ресурси України у січні-лютому 2022 року

Джерело: складено авторами за [2; 5; 6; 7]

За даними Державної служби спеціального зв'язку та захисту інформації України [5] з початку військової агресії російської федерації була зареєстрована критична кількість DDoS-атак за одну добу – 271. У березні-травні 2022 року кібератаки на енергетичну сферу, логістичну інфраструктуру, сайти українських онлайн-медіа та офіційні державні ресурси продовжувалися.

Основними видами кібератак, які становлять найбільшу загрозу інформаційній безпеці національній економіці визначено програми-вимагачі, інсайдерські атаки, фішинг, цільові кібератаки та DDoS-атаки. Їх деструктивний вплив спричиняє, в першу чергу, значні фінансові втрати. Так, за даними американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) у 2020 р. втрати світової економіки у результаті кібератак склали понад 1 трлн дол США, що становило 1% світового ВВП. У порівнянні із 2018 р., даний показник зріс на понад 50%. У 2021 році збитки від кібератак зросли до 4,2–6 трлн. дол. США (рис. 4). Прогнозується, що у 2025 році обсяг фінансових втрат від кіберзлочинності сягне 10,5 трлн. дол. США.

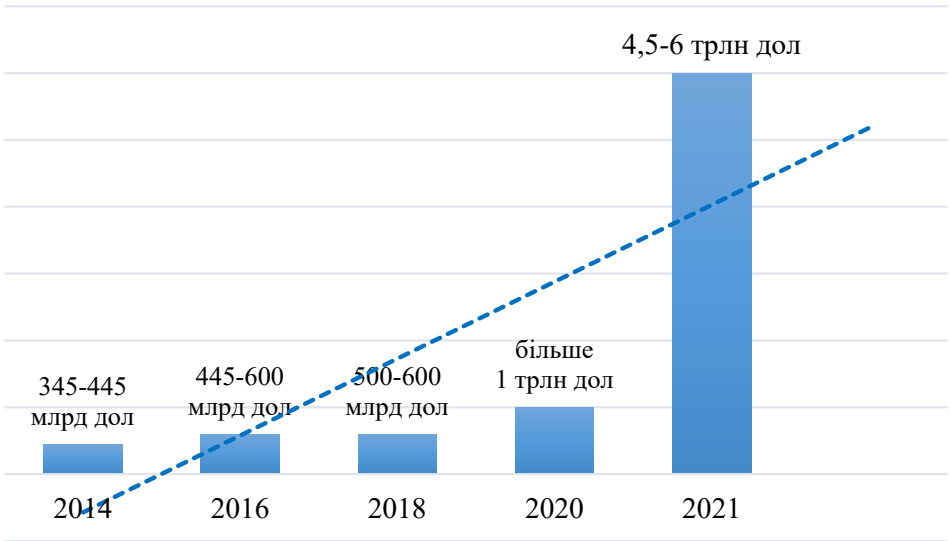

Рис. 4. Світові фінансові втрати від кібератак у 2014–2021 роках

Джерело: складено авторами за [8]

Слід відмітити, що у 2021 році зафіксовано найвищу середню вартість витоку даних за останні 17 років – 4,24 млн дол. Аналогічний показник за 2020 рік становив 3,86 млн дол. [9]. Найбільш

поширеною причиною витоку даних були фішинг-атаки. Крім прямих фінансових збитків кібератаки спричиняють втрати робочого часу, а також іміджеві втрати компаній [10]. Є й інші приховані втрати від кіберзлочинності – зокрема, зниження рівня задоволеності працівників роботою.

Враховуючи зростання негативних фінансових наслідків від реалізації кіберзагроз, необхідність підвищення рівня інформаційної безпеки в умовах розвитку цифрової інфраструктури є безумовною.

На сьогоднішній день розроблено ряд глобальних індексів, які дозволяють визначити можливості країни у сфері кіберзахисту, оцінити її кіберпотужність, зокрема спроможність регуляторних заходів та засобів для досягнення стратегічних цілей кібербезпеки. Слід відмітити високий потенціал України в цьому напрямі. Це підтверджується позиціями у світових рейтингах.

Згідно з Національним індексом кіберезпеки (NCSI), який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна на кінець 2021 року році піднялася на 24 місце серед 160 країн та поліпшила свою позицію на 4 пункти у порівнянні з 2019 роком. За можливостями кіберзахисту національного інформаційного простору Україна наближується до Швейцарії (23 місце) та Великобританії (22 місце). Водночас згідно з Глобальним індексом кібербезпеки (GCI) Україна посідає 78 місце. У порівнянні з попереднім роком відбулося зниження на 24 позиції. За Національним індексом кіберпотужності (NCPI), який дозволяє вимірювати ефективність державної стратегії, реагування на правопорушення та боротьби з ними, можливості оборони, розподіл ресурсів, участь приватного сектору, рівень ефективності робочої сили та інновацій у сфері кібербезпеки, у 2020 році Україна посіла лише 26 місце із 30 країн світу та 10 місце серед європейських країн. Водночас, слід відмітити, що до рейтингу потрапили ті країни, які мали найбільш розвинуті сили кібербезпеки, що підтверджує наявність в України потенційних можливостей нарощення кіберпотужностей та підвищення рівня інформаційної безпеки.

Графічна інтерпретація позицій України у світових рейтингах з кібербезпеки представлені на рисунку 5.

Рис. 5. Позиції України у міжнародних рейтингах з кібербезпеки

Джерело: складено авторами за [11; 12; 13]

Потенціал України у сфері кібербезпеки відмічається не лише світовими рейтингами, але й міжнародними організаціями. Зокрема, на початку квітня 2022 року Україна прийнята до складу Об'єднаного центру передових технологій з кібероборони НАТО як учасник-контрибутора.

Відмічена позитивна динаміка пов'язана, в тому числі, з удосконаленням вітчизняного законодавства у сфері інформаційної та кібербезпеки. На сьогоднішній день нормативно-правова база регулювання та забезпечення безпеки в інформаційному просторі, в тому числі кіберпросторі, включає: Конституцію України, Закон України «Про національну безпеку України», Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про Основні засади розвитку інформаційного

суспільства в Україні на 2007–2015 роки», Стратегію національної безпеки, Стратегію інформаційної безпеки, Стратегію кібербезпеки України, Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки, Концепцію розвитку цифрових компетентностей, Міжнародні стандарти серії ISO/IEC 27000, нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України стосовно створення і функціонування КСЗІ, інші нормативно-правові акти, що регулюють відносини у сфері інформаційної безпеки.

Також відмічається посилення співпраці з міжнародними організаціями у сфері кібербезпеки. У вересні 2021 року Державною службою спеціального зв'язку та захисту інформації України укладено угоду з Агентством з кібербезпеки та безпеки інфраструктури США, яка передбачає: координацію дій щодо захисту об'єктів критичної інформаційної інфраструктури та вдосконалення системи реагування на кіберінциденти; обмін досвідом у рамках системи управління ризиками (Risk Management), що дозволить забезпечити національну стійкість України до кіберзагроз; використання досвіду США щодо організації взаємодії державних органів та бізнесу у сфері кібербезпеки; реалізацію міжнародних проєктів технічної допомоги щодо побудови мережі галузевих і регіональних операційних центрів безпеки (Security Operation Centre) та команд реагування (CSIRT), які передбачені Стратегією кібербезпеки України.

Приєднання України до складу Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), яке відбулося у квітні 2022 року, забезпечує можливість обміну досвідом у виявленні та протидії сучасним кіберзагрозам, відпрацювання навичок спільного реагування на кібератаки та проведення операцій оборони і стримування у кіберпросторі.

Розвиток міжнародної співпраці в напрямку посилення кіберстійкості України є пріоритетним завданням з метою попередження глобальних інформаційних загроз, забезпечення високого рівня якості розслідування кіберзлочинів, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки.

Водночас існують напрями у сфері кібербезпеки, які негативно впливають на позиції України у зазначених рейтингах та потребують вдосконалення. Зокрема, низький рівень внеску на сьогоднішній день у глобальну кібербезпеку, недостатній рівень захисту цифрових послуг, недостатньо розвинений напрям військових кібероперацій.

Слід відмітити, що з початку 2022 року ведеться активна діяльність по всім відміченим проблемним аспектам: Україна стала активним учасником міжнародного співробітництва у сфері кібербезпеки; йде процес формування кібервійська [14], яке відповідає за інформаційну безпеку, захист критичної інфраструктури та розвідку.

Враховуючи досягнення України в кіберпросторі, правомірно визначити її рівноправним учасником на міжнародній арені у сфері кібербезпеки. Перспективними завданнями мають стати подальше удосконалення систем інформаційного захисту об'єктів критичної інфраструктури на основі передових світових практик, а також узгодженість дій з міжнародними організаціями щодо протидії загрозам, пов'язаним з розвитком цифрової економіки та інформаційного суспільства. Побудова ефективної системи кібербезпеки в аспекті комплексної протидії кіберзагрозам сприятиме формуванню превентивного механізму протидії загрозам та їх стримуванні, випереджальному реагуванню на динамічні зміни, що відбуваються у кіберпросторі.

Висновки. На основі проведеного дослідження правомірно зробити наступні висновки:

1. В умовах стрімкої трансформації цифрового середовища спостерігається зростання ризиків та загроз інформаційній безпеці України, в тому числі кібербезпеці. Збільшення кількості кібератак на об'єкти критичної інфраструктури та державні інформаційні ресурси, у зв'язку з розгорнутою російською федерацією кібервійною, підтверджує актуальність проблеми підвищення кіберстійкості національного інформаційного простору.

2. Враховуючи зростання негативних фінансових наслідків від реалізації кіберзагроз, доведено необхідність впровадження комплексних та скоординованих заходів на національному та міжнародному рівнях для запобігання реалізації кіберінцидентів з боку органів влади, бізнесу та суспільства.

3. На основі дослідження позицій України в міжнародних рейтингах з кібербезпеки та встановлення індикаторів, які лежать в основі глобальних індексів NCSI, GCI та NCPI, обґрунтовано сильні та слабкі сторони кіберспроможності країни. Перспективними завданнями визначено удосконалення систем інформаційного захисту об'єктів критичної інфраструктури на основі передових світових практик, а також узгодженість дій з міжнародними організаціями щодо протидії загрозам, пов'язаним з розвитком цифрової економіки та інформаційного суспільства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Financial Stability Board. Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective. *Interim report.* July 13, 2021.
2. Microsoft Special Report: Ukraine. *An overview of Russia's cyberattack activity in Ukraine.* April 27, 2022.
3. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management (IJM).* 2020. Volume 11, Issue 12. P. 1709–1726. DOI: 10.34218/IJM.11.12.2020.157
4. Служба безпеки України. Захист інформаційного та кіберпростору. *Звіт SIEM.* URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення: 05.04.2022).
5. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення: 05.04.2022).
6. Офіційний сайт Служби безпеки України. URL: https://ssu.gov.ua/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv (дата звернення: 05.04.2022).
7. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (дата звернення: 05.04.2022).
8. CIS Controls Implementation Guide for SMEs. URL: CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org) (дата звернення: 05.04.2022).
9. ESET. Підсумки року: яким був 2021 рік для кібербезпеки. URL: https://eset.ua/ua/news/view/933/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti (дата звернення: 05.04.2022).
10. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. Increasing Information Protection in the Information Security Management System of the Enterprise. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) *Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering.* Springer, Cham. Volume 181, 725–738 (2020). DOI: https://doi.org/10.1007/978-3-030-85043-2_67
11. Офіційний сайт NCSI Project Team. URL: https://ncsi.ega.ee/country/ua/ (дата звернення: 06.04.2022).
12. Комітет з питань цифрової трансформації. Кращі практики управління кібербезпекою. *Оглядовий звіт.* URL: https://www1.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf (дата звернення: 06.04.2022).
13. Новий глобальний індекс кібербезпеки – Національний індекс кіберпотужності. URL: https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-naczionalnyj-indeks-kiberpotuzhnosti/#_ftn1 (дата звернення: 06.04.2022).
14. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» від 26 серпня 2021 року № 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (дата звернення: 06.04.2022).

REFERENCES:

1. Financial Stability Board. Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective. *Interim report.* July 13, 2021.
2. Microsoft Special Report: Ukraine. *An overview of Russia's cyberattack activity in Ukraine.* April 27, 2022.
3. Onyshchenko, S., Yanko, A., Hlushko, A. and Sivitska, S. (2020), "Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization", *International Journal of Management (IJM)*. Volume 11, Issue 12. P. 1709–1726. DOI: 10.34218/IJM.11.12.2020.157
4. Security Service of Ukraine. Protection of information and cyberspace. *SIEM report*, available at: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (Accessed 05 April 2022).
5. The official website of the State Service for Special Communications and Information Protection of Ukraine, available at: https://cip.gov.ua/ua (Accessed 05 April 2022).
6. Official website of the Security Service of Ukraine, available at: https://ssu.gov.ua/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv (Accessed 05 April 2022).
7. The official website of the Cyber Police Department of the National Police of Ukraine, available at: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (Accessed 05 April 2022).
8. CIS Controls Implementation Guide for SMEs, available at: CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org) (Accessed 05 April 2022).
9. ESET. Year in Review: What 2021 Was Like for Cyber Security, available at: https://eset.ua/ua/news/view/933/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti (Accessed 05 April 2022).
10. Onyshchenko, S., Yanko, A., Hlushko, A. and Sivitska, S. (2020), Increasing Information Protection in the Information Security Management System of the Enterprise. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) *Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering.* Springer, Cham., vol. 181, pp. 725–738. DOI: https://doi.org/10.1007/978-3-030-85043-2_67
11. Official website NCSI Project Team. available at: https://ncsi.ega.ee/country/ua/ (Accessed 06 April 2022).
12. Committee on Digital Transformation. Cyber security management best practices. *Review report,* available at: https://www1.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf (Accessed 06 April 2022).

13. The new global cyber security index is the National Cyber Power Index, available at: https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-naczionalnyj-indeks-kiberpotuzhnosti/#_ftn1 (Accessed 06 April 2022).

14. Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On urgent measures for the cyber defense of the state" dated August 26, 2021 № 446/2021, available at: https://zakon.rada.gov.ua/laws/show/446/2021#Text (Accessed 06 April 2022).

УДК 338.242(477)
JEL O32

Онищенко Світлана Володимирівна, доктор економічних наук, професор. **Глушко Аліна Дмитрівна,** кандидат економічних наук, доцент, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз.**

У статті актуалізована проблема забезпечення кібербезпеки України в умовах зростання викликів та загроз в інформаційному просторі. Розглянуто питання формування додаткових загроз інформаційним ресурсам і технологіям в умовах стрімкої трансформації цифрового середовища (загрози, які пов'язані з кібератаками, розкриттям персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерних програм тощо), методи діагностики і протидії яким поки що відпрацьовані не в повній мірі. Підкреслено, що саме інформація (дезінформація) в кіберпросторі стала найважливішим ресурсом та основною миттєвою, рушійною силою. Проаналізовано динаміку кібератак та рівень фінансових втрат світової економіки від реалізації кіберзагроз. Доведено, що кібератаки на об'єкти критичної інфраструктури України та державні інформаційні ресурси є загрозою національним інтересам. Проведено статистичний аналіз зростання їх інтенсивності на початку 2022 року як складової частини реалізації військової агресії російської федерації проти України. На основі аналізу позицій України в глобальних рейтингах визначено можливості країни у сфері кіберзахисту, оцінено її кіберпотужність, тобто спроможність регуляторних заходів та засобів для досягнення стратегічних цілей кібербезпеки. Доведено наявність високого потенціалу України у сфері кібербезпеки. Водночас визначено проблемні аспекти в напрямку забезпечення кіберзахисту національного інформаційного простору. Зокрема, відмічено низький рівень внеску на сьогоднішній день у глобальну кібербезпеку, недостатній рівень захисту цифрових послуг, недостатньо розвинений напрям військових кібероперацій. Обґрунтовано перспективні завдання в аспекті забезпечення кібербезпеки України в умовах зростання викликів та загроз, серед яких правомірно відмітити подальше удосконалення систем інформаційного захисту об'єктів критичної інфраструктури на основі передових світових практик, а також узгодженість дій з міжнародними організаціями щодо протидії загрозам, пов'язаним з розвитком цифрової економіки та інформаційного суспільства.

Ключові слова: кібербезпека, інформаційна безпека, виклики та загрози, кіберстійкість, кіберзахист, інформаційне середовище.

UDC 338.242(477)
JEL O32

Svitlana Onyshchenko, Doctor of Economics, Professor. **Alina Hlushko,** PhD in Economics, Associate Professor, National University "Yuri Kondratyuk Poltava Polytechnic". **Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats.**

The article updates the problem of ensuring cyber security of Ukraine in the conditions of growing challenges and threats in the information space. The question of the formation of additional threats to information resources and technologies in the conditions of rapid transformation of the digital environment is considered (threats associated with cyber attacks, disclosure of personal data, the influence of spyware and viruses, phishing, threats related to updating computer programs, etc.), methods of diagnosis and countermeasures which have not yet been fully developed. It is emphasized that it is information (disinformation) in cyberspace that has become the most important resource and the main immediate driving force. The dynamics of cyber attacks and the level of financial losses of the world economy from the implementation of cyber threats are analyzed. It has been proven that cyber attacks on critical infrastructure of Ukraine and state information resources are a threat to national interests. A statistical analysis of the increase in their intensity at the beginning of 2022 as a component of the implementation of the russian federation's military aggression against Ukraine was carried out. Based on the analysis of Ukraine's position in the global rankings, the country's capabilities in the field of cyber protection were determined, and its cyber power was assessed, i.e., the ability of regulatory measures and means to achieve the strategic goals of cyber security. It has been proven that Ukraine has a high potential in the field of cyber security. At the same time, problematic aspects in

the direction of ensuring cyber protection of the national information space are identified. In particular, the low level of contribution to global cyber security, the insufficient level of protection of digital services, and the insufficiently developed direction of military cyber operations were noted. Prospective tasks in the aspect of ensuring Ukraine's cyber security in the face of growing challenges and threats are substantiated, among which it is rightful to note the further improvement of information protection systems of critical infrastructure objects based on world best practices, as well as the coordination of actions with international organizations in countering threats related to development of the digital economy and information society.

Key words: cybersecurity, information security, challenges and threats, cyber resilience, cybersecurity, information environment.