УДК 004.77+004.9+34.342
DOI: 10.31733/2078-3566-2022-6-524-530

Людмила РИБАЛЬЧЕНКО©
кандидат економічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

КІБЕРЗЛОЧИННІСТЬ У ГЛОБАЛЬНОМУ ПРОСТОРІ

Щодня необхідність для забезпечення безпеки цифрової інфраструктури від кібератак зростає і є актуальним питанням сьогодення. Кіберзлочинність розвивається дуже швидко та має різноманітні прояви. Найпоширенішими є кібератаки, які спрямовані на несанкціонований доступ, блокування доступу до роботи з файлами, викрадення персональних даних, поширення вірусів в комп'ютерних системам та мережах, вимагання грошей та інше.

Український народ, який зробив свій *євроінтеграційний вибір,* і зараз продовжує відстоювати свої права за свободу та незалежність у цій війні. Україні у червні 2022 року було надано статус кандидата на вступ до Європейського Союзу і це прагнення українського народу підтримано на загальноєвропейському рівні. Україна повинна створити потужний та безпечний кіберпростір із врахуванням соціального, політичного та економічного розвитку для нейтралізації та мінімізації внутрішніх і зовнішніх загроз.

***Ключові слова*:** *кібербезпека, захист персональних даних, економічні злочини, несанкціонований доступ, конфіденційність інформації.*

Постановка проблеми. Швидкі зміни цифрового світу потребують ефективного захисту національної системи кіберзахисту, яка має гарантувати українцям безпечне функціонування усіх сфер життєдіяльності. Забезпечення кіберстійкості на усіх рівнях соціально-економічного розвитку, удосконалення законодавчого та нормативно правового забезпечення щодо захисту інформації, поліпшення діяльності щодо забезпечення кібербезпеки, виявлення можливих загроз та їх попередження, співпраця з іншими державами та міжнародними організаціями є важливою стратегією кібербезпеки України.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Питання забезпечення кібернетичної безпеки, в тому числі в контексті проблематики забезпечення інформаційної та національної безпеки досліджувались у працях О. Баранова, В. Бутузова, О. Довганя, Б. Кормича, Р. Лукянчука, А. Марущака, М. Ожевана, В. Пилипчука, М. Погорецького, Т. Качука, О. Тронько, І. Сопілки, В. Шеломенцева та інших науковців.

Метою статті є дослідження стану забезпечення кібербезпеки в Україні та визначення перспектив надійності, захисту та стратегій подальшого розвитку національної безпеки.

Виклад основного матеріалу. Відновлення світової економіки від спаду, який викликаний світовою пандемією COVID-19, що триває але йде дуже уповільнено. Після скорочення на 3,1 % у 2020 р. очікувалося, що глобальне економічне зростання досягне 5,9 % у 2021 році та сповільниться до 4,9 % у 2022 році. До 2024 року прогнозується, що розвиток світової економіки буде на 2,3 % менше, ніж був до пандемії. Ризики в економіці є значними. Рівень інфляції прискорюється, зростають ціни на товари та банківські відсоткові ставки у багатьох країнах, що формує зростання різноманітних ризиків в усіх галузях і сферах життєдіяльності. Відбувається напруження у підвищенні ризику боргу та підвищенні курсу долара США у світі.

Останніми роками відбувається усе більша необхідність робити в Інтернеті. Питання конфіденційності інформації, захисту персональних даних, надійності кіберпростору набуло актуальності та все більшого значення у житті кожного мешканця

ORCID iD: https://orcid.org/0000-0003-0413-8296
luda_r@ukr.net

планети. Країни в усьому світі нарощують свої можливості кібербезпеки.

До основних кіберзагроз належать порушення цілісності даних, несанкціонований доступ, конфіденційність інформації, втручання в корпоративну чи державну таємниці тощо. Такі загрози впливають на функціонування будь-якої інформаційної чи комунікаційної системи, сфери діяльності як на рівні підприємства чи установи, так і на державному та національному рівнях.

Тому для управління будь-якими кіберзагрозами необхідно створити потужний захист від можливих та потенційних загроз із залученням висококваліфікованого персоналу та з використанням сучасних програмних засобів.

Питаннями національного рівня є визначення кіберзагроз, заходів та можливостей кібербезпеки, розробка основних показників кібербезпеки, їх дослідження за певними ознаками та створення відповідних груп показників кібербезпеки для аналізу та розробки заходів щодо їх уникнення. Метою проведення такого дослідження є сприяння глобальній культурі кібербезпеки та поліпшення сфери захисту в усьому світі.

За даними компанії Microsoft, більше половини хакерських атак у 2020–2021 роках було здійснено росією. Україна на другому місці серед тих, проти кого вони були спрямовані. Саме з березня 2021 року росія почала проводити підготовку до вторгнення в Україну. Масштабні російські кібероперації здійснювалися із метою руйнування інформаційного кіберпростору України [11]. Серед основних кіберзагроз – мережеві атаки, мережеве сканування, спроби WEB-атак, фішинг, шкідливе програмне забезпечення, кількість випадків яких становить понад мільйон випадків.

Протягом ІІ півріччя 2020 року та у І півріччі 2021 року найбільше хакерських атак було зафіксовано з росії – 58 %. На другому місці опинилася Північна Корея (23 %), а третьому – Іран (11 %). Також 8 % атак зафіксували з Китаю.

Менше 1 % атак системи безпеки Microsoft зафіксували з Південної Кореї, В'єтнаму і Туреччини.

Діяльність найбільш активних хакерських груп росії, що становило 59 %, була спрямована на атаки в галузях державного управління, дипломатії, оборони, ядерної політики, неурядових організацій, ІТ-сфери, телекомунікацій, аналітичних центрів, науки, журналістики, економіки та аерокосмічної сфери.

Активна діяльність хакерської групи Північної Кореї, яка становила 21 %, здійснювала напади на аналітичні центри, дипломатію, науку, оборону та аерокосмічну сфери. Діяльність 11 % хакерських груп Ірану здійснювала напади на дипломатію, оборону, науку та аналітичні центри, а також державного управління, оборону та ІТ-сфери. Діяльність 5 % хакерських груп Китаю здійснювала напади на структури державного управління, дипломатію та економіку.

Найбільш уразливими до хакерських атак були сфери: державного управління (48 %), неурядові організації та аналітичні центри (31 %), освіта (3 %), міжнародні міжурядові організації (3 %), ІТ-сфера (2 %), медіа (1 %), охорона здоров'я (1 %), енергетика (1 %) та інше (1 %).

З 01.07.2020 по 30.06.2021 рр. 46 % хакерських атак були спрямовані проти США, 19 % – проти України, 9 % – проти Великої Британії, по 3 % – проти Німеччини, Бельгії та Японії, по 2 % – проти Ізраїлю та Молдови, по 1 % – проти Португалії та Саудівської Аравії, решту 11 % становили інші країни світу.

Через те, що хакерські атаки відбуваються в режимі реального часу, відповідно їх треба і виявити та знешкодити у режимі реального часу [3]. Більшість шахрайських атак відбувається у Сполучених Штатах Америки та Китаї. Фейкові акаунти, частка яких становлять більше 21 %, спрямовані на фінансові послуги, які створені у США та 17 % - в Китаї [1]. Цікаво, що злочинні групи залучають різних постачальників хмарних послуг залежно від атаки. Шахраї залучаються до соціальних платформ і використовують їх у своїх злочинних намірах.

Досліджуючи Глобальний індекс кібербезпеки ITU [2], необхідно сказати, що у 2020 році рейтинг очолили США з оцінкою показника 100 балів, відповідно займаючи 1-у сходинку рейтингу (рис. 1). На другому місці Об'єднане Королівство та Саудівська Аравія (99,54 бала) і третє місце посідає Естонія (99,48 бала). До першої десятки належать: республіка Корея, Сінгапур та Іспанія (98,52 бала, 4 місце), рф, Об'єднані Арабські Емірати та Малайзія (98,06 бала, 5-е місце), Литва (97,93 бала, 6-е місце), Японія (97,82 бала, 7-е місце), Канада (97,67 бала, 8-е місце), Франція (97,6 бала, 9-е місце) та Індія (97,5 бала, 10-е місце). Україна посідала 78-е місце (65,93 бала).

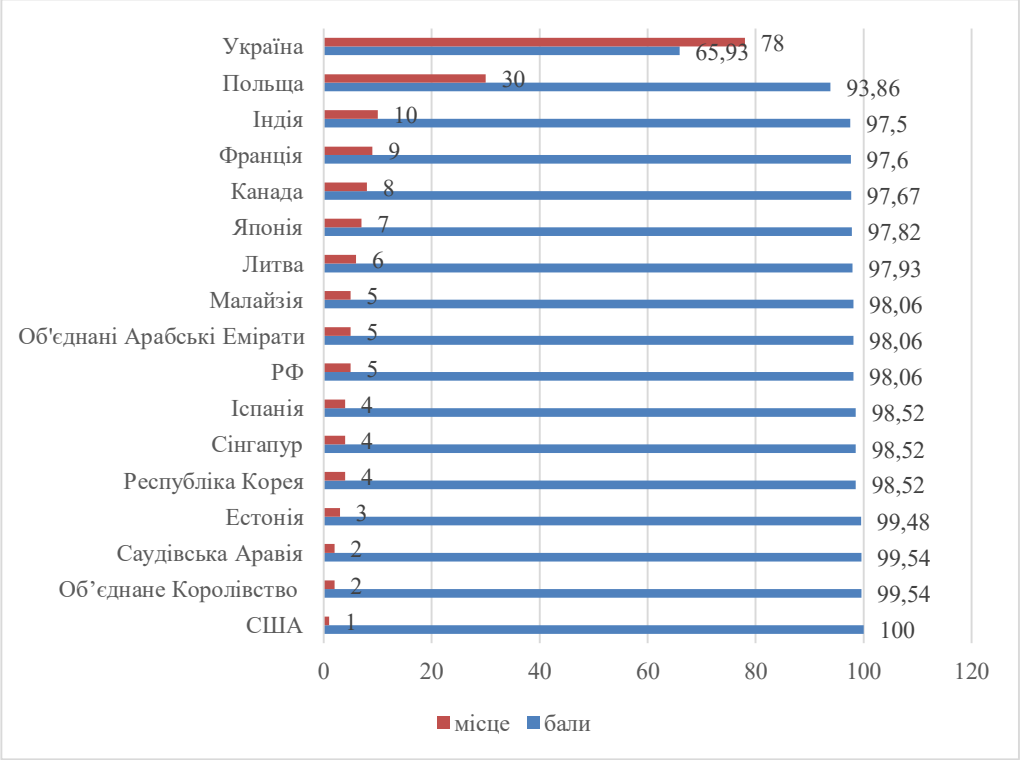

Рис. 1. Глобальний індекс кібербезпеки у 2020 році
Джерело: побудовано автором за даними [2]

У Південній Кореї наявна кількість хакерів становить приблизно 700. Бюджет її становить 400 млн дол. на рік. Характерним для цих кібервійськ є оборонна функція.

З 2020 року Литва стала на чолі формування сил швидкого реагування на кібератаки у всьому Євросоюзі. Державні органи Литви, Естонії, Польщі, Нідерландів, Румунії та Хорватії підписали меморандум про співпрацю. Для протидії усім можливим інцидентам та кібератакам створена Міжнародна організація, що складається з військових та цивільних осіб, які розслідують небезпечні кіберінциденти. У такий спосіб Литва створила підгрунтя для міжнародного співробітництва та протистояння можливим кіберзагрозам, обміну знаннями та проведення навчань щодо протидії кібернебезпеці.

Бюджет підрозділу кібероборони Німеччини становить 250 млн дол. на рік. Кібероборона є стратегічним напрямом щодо надійного забезпечення безпеки інформаційних систем збройних сил Німеччини та захисту від злому цифрових технологій.

Тож поточний стан усіх подій, які відбуваються у кіберпросторі України, показують, що стратегічним та найважливішим завданням щодо забезпечення безпеки держави є створення потужної національної кібергвардії, яка призначена для надійного та безпечного кіберпростору України.

Серед країн Європи найвищій [12] рівень кібербезпеки в Об'єднаному Королівстві 99,54 бала, далі йдуть Естонія (99,48 бала), Іспанія (98,52 бала), Литва (97,93 бала), Франція (97,6 бала). Польща посідає на 18 місці (93,86 бала), а Україна на 39 (65,93 бала) (рис. 2).

Глобальний індекс кібербезпеки розраховано за багатьма показниками, які поділено на п'ять основні напрями. За результатами кожного з цих напрямів, які вимірювались у двадцятибальній шкалі, в Україні вони становили: правові заходи (17.46), технічні заходи (11.6), організаційні (13.06) та заходи співпраці між державами (12,87), а також заходи, що сприяють підвищенню потенціалу розвитку (10,94).

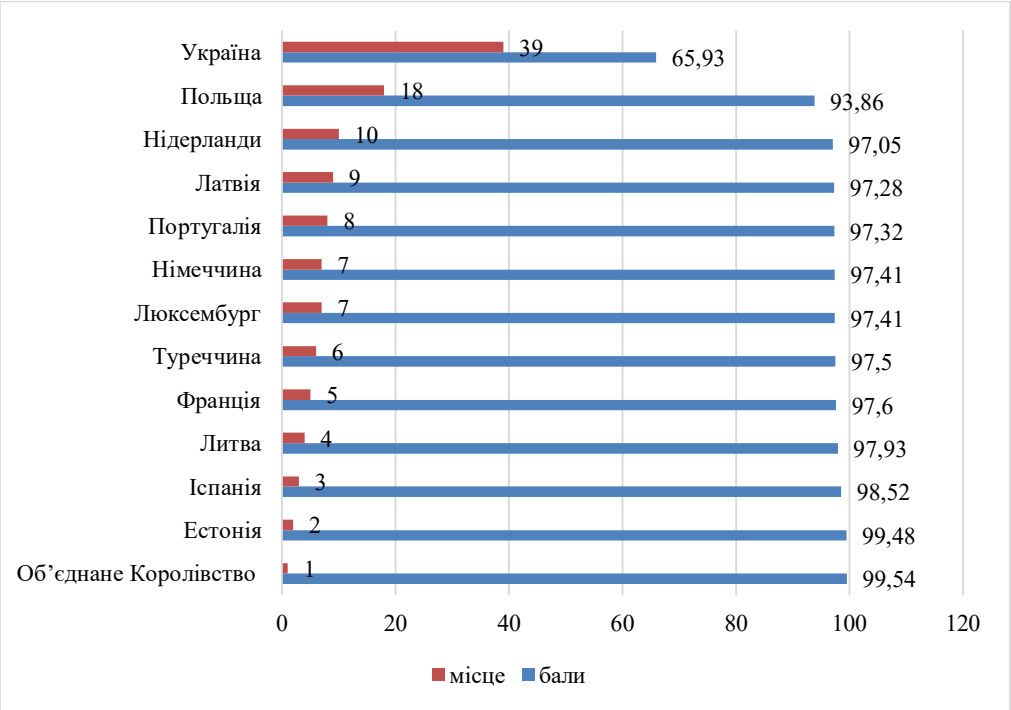

Рис. 2. Глобальний індекс кібербезпеки серед країн Європи
Джерело: побудовано автором за даними [2]

З яких видно, що найбільше в Україні було розвинено правове поле серед усіх заходів кібербезпеки і найменше потенціал розвитку.

Правові заходи засновано на законодавчій базі, яка спрямована на розробку законів та нормативних документів, що регулюють кібербезпеку в країні і містить основні механізми, розслідування злочинів та порушення законів.

До технічних заходів належать установи та структури, що займаються виявленням та розслідуванням кіберзлочинів. Такі структури розробляють відповідні критерії безпеки та схеми для програмного забезпечення, і впроваджують їх в урядові та національні структури для попередження можливих наслідків атак чи інцидентів.

До організаційних заходів належать стратегічні цілі та плани щодо забезпечення захисту від можливих кіберзагроз. Впровадження відповідної моделі управління та наглядового органу в різних галузях економіки держави для ефективної роботи розвитку кібербезпеки.

Заходи з підвищення потенціалу базуються на програмах досліджень, освіти та навчання, підвищенні кваліфікації персоналу з підготовки напряму кібербезпеки, які направлено на розвиток самого персоналу того чи іншого підприємства чи установи, а також впровадження новітніх технологій в різних галузях для боротьби із кібершахраями.

Заходи співпраці базуються на партнерських стосунках між державами у напрямі боротьби із зловмисниками та створенню програм щодо попередження та виявлення кіберінцидентів, а також створення надійних заходів та взаємозв'язків для кібербезпеки і зменшення кіберризиків.

Аналізуючи показники оцінювання ризику, які пов'язані з кіберпростором, то в багатьох країнах їх немає (рис. 3), тобто немає з чим визначати рівень кіберзагроз. Наприклад, як в деяких країнах (37) Африки чи Америки (27).

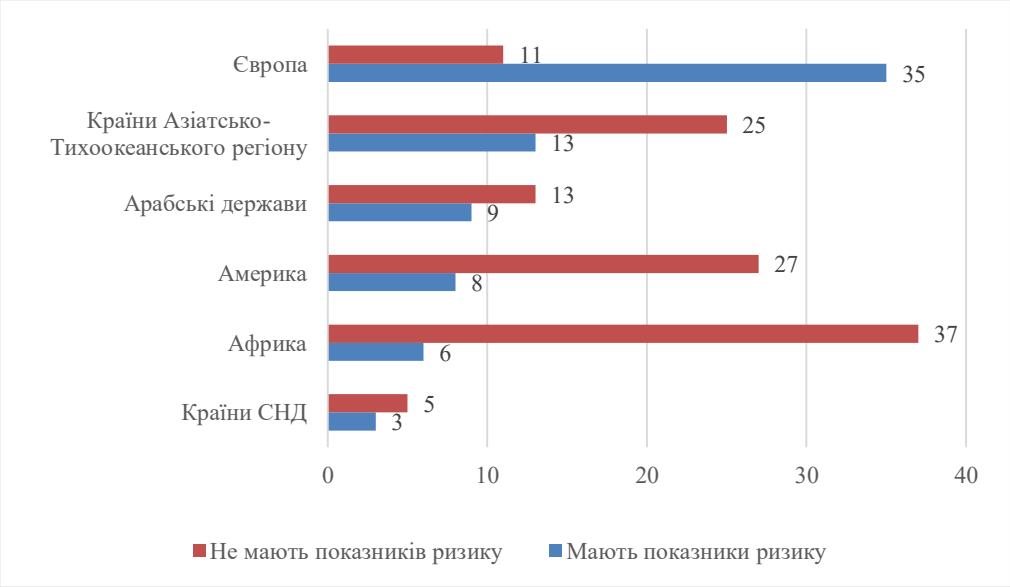

Рис. 3. Показники оцінювання ризику в країнах світу
Джерело: побудовано автором за даними [2]

Сприяння кібербезпеці повинно мати системний характер та супроводжуватися напрямами щодо зростання рівня кібербезпеки, із залученням високого професійного рівня IT-спеціалістів та сучасних інформаційних технологій, покращення механізмів для заохочення впровадження кібербезпеки для розвитку кібербезпеки в приватних підприємствах та на державному рівні.

Країни, які беруть участь у багатосторонніх угодах з кібербезпеки з підписанням чи їх ратифікацією та створили угоди щодо обміну інформацією та розвитку потенціалу у напрямі боротьби з кіберзлочинами – табл. 1.

Таблиця 1

Участь країн у багатосторонніх угодах з кібербезпеки

Країни	*Підписано угоду*	*Не мають підписаної угоди*	*На стадії підписання*
Європа	41	4	1
Країни Азіатсько-Тихоокеанського регіону	26	12	
Країни Африки	19	24	1
Арабські країни	12	10	
Постраднянські країни	7	2	
Америка	7	28	

Із 194 країн світу, 57,73 % країн мають багатосторонню угоду з країнами щодо співпраці з кібербезпеки, 41,24 % країн не мають підписаної багатосторонньої угоди і лише 1 % країн перебувають на стадії її підписання (табл. 1).

Від початку повномасштабного вторгнення рф в Україну, а саме з 24 лютого 2022 року, було виявлено приблизно 500 фактів шахрайств, що вчинено з використанням високих інформаційних технологій, в яких підозрюють 171 особу, відкрито 422 кримінальних правопорушення. Інтернет-шахраїв виявили українські кіберполіцейські.

Збитки, які причинили кібершахраї, становлять більше 46,5 млн грн. Шахраї адаптуються до потреб громадян, створюють нові схеми для своїх зловмисних дій, відкривають рахунки для фейкових зборів на потреб військових та багато іншого.

22 серпня 2022 року Мінцифри, Держспецзв'язку та Канцелярія прем'єр-

міністра Польщі підписали меморандум про взаєморозуміння у сфері кіберзахисту. Такий меморандум забезпечить посилення спільної боротьби із злочинами у кіберпросторі та зробить обмін досвідом та інформацією про кіберінциденти швидшим і ефективнішим.

Оскільки зараз триває війна в Україні, зростає необхідність у забезпеченні безпеки проти загроз у кіберпросторі. Досліджуючи перспективи кібербезпеки в Україні, необхідно сказати, що пріоритетним є ухвалення стратегічних рішень щодо стійкості та управління ризиками підприємства, які займаються безпекою. Більшість керівників підприємств бачать кіберстійкість пріоритетом бізнесу в їх організації. Перехід від кібербезпеки до кіберстійкості є важливим кроком до більш надійного та стабільного майбутнього.

На державному рівні повинно бути розроблене та удосконалене чинне законодавство в напрямі правового захисту від кіберзагроз. Необхідно створити підрозділи, організації у напрямі захисту від небезпек, створити співпрацю з подібними підрозділами інших країн світу.

Висновки. Отже, щорічний розвиток цифрових технологій стає привабливим для економічної злочинності, постають найважливішими питання надійності та забезпечення безпеки у глобальному кіберпросторі.

Вирішення організаційних, технічних та юридичних питань стає дедалі найважливішим та актуальнішим. Ці питання є стратегічними не лише для країн, в яких рівень кібербезпеки є найбільшим чи високим, а й країн, що розвиваються, та більше за все стосується країн, які відчувають саме зараз найбільші кібератаки на просторі свої країни, до яких саме належить Україна.

Необхідно використовувати свої конкурентні переваги для зростання кіберзахисту в усіх сферах життєдіяльності. Проведення моніторингу стратегій кібербезпеки, залучення міжнародного практичного досвіду з питань кібербезпеки, проведення наукових досліджень та розвиток національних груп реагування на комп'ютерні інциденти, проведення тренінгів з розвитку потенціалу з питань кібербезпеки для ІТ-фахівців допоможе зменшити рівень кіберзагроз та підвищити рівень кібербезпеки в країні.

Список використаних джерел

1. Voo Julia, Hemani Irfan. National Cyber Power Index 2020. Methodology and Analytical Considerations. *China Cyber Policy Initiative. Report*, September 2020. P. 84.

2. Global Cybersecurity Index 2020 / International Telecommunication Union. Development Sector. 2020. P. 172.

3. Гребенюк А. М., Рибальченко Л. В., Прокопов С. О. Моніторинг кіберінциндентів хмарних сервісів та захист цифрових каналів зв'язку. *The First Special Humanitarian Issue of Ukrainian Scientists. European Scientific e-Journal*, 3. Ostrava : Tuculart Edition, 2022. (18). 40–53.

4. The Global Risks Report 2022, 17th Edition. World Economic Forum.

5. Гребенюк А. М. Основи управління інформаційною безпекою : навч. посібник. Дніпро : ДДУВС, 2020. 144 с. URL: https://er.dduvs.in.ua/handle/123456789/5717.

6. Global Cybersecurity Outlook 2022. INSIGHT REPORT JANUARY 2022. (2022, January 30). *The World Economic Forum*. Retrieved March 15, 2022 from https://weforum.org.

7. Rybalchenko L., Ryzhkov E., Ohrimenco S. Modeling economic component of national security. *Philosophy, Economics and Law Review*, 2021. 1(1). P. 25–36.

8. Rybalchenko L., Ryzhkov E., Ohrimenco S. Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review*, 2021. 1(2). P. 67–80.

9. Rubalchenko L., Ryzhkov E. Ensuring enterprise economic security. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Special Issue № 1, 2019. P. 268-271.

10. Rubalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. Special Issue, 2019. № 1. P. 264-267.

11. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Microsoft's Digital Security Unit. April 27, 2022. URL: https://www.radiosvoboda.org/a/news-microsoft-rosia-kiberataky/31824183.html.

12. Rybalchenko L., Ryzhkov E., Ciobanu G.. Global consequences of the loss of business in countries around the world caused by fraud. *Philosophy, Economics and Law Review*, 2022. No 1(2). P. 93–102.

Надійшла до редакції 12.12.2022

References

1. Voob Julia, Hemani Irfan (2020) National Cyber Power Index 2020. Methodology and Analytical Considerations. *China Cyber Policy Initiative*. Report, September, p. 84.
2. Global Cybersecurity Index 2020 / International Telecommunication Union. Development Sector. 2020, p. 172.
3. Hrebeniuk, A. M., Rybalchenko, L. V., Prokopov, S. O. (2022) Monitorynh kiberintsyndentiv khmarnykh servisiv ta zakhyst tsyfrovykh kanaliv zviazku [Monitoring of cyber incidents of cloud services and protection of digital communication channels]. *The First Special Humanitarian Issue of Ukrainian Scientists. European Scientific e-Journal*, 3. Ostrava : Tuculart Edition,. (18), pp. 40–53. [in Ukr.].
4. The Global Risks Report 2022, 17th Edition. World Economic Forum.
5. Hrebeniuk, A. M. (2020) Osnovy upravlinnia informatsiinoiu bezpekoiu [Fundamentals of information security management] : navch. posib. Dnipro : DDUVS, 144 p. URL : https://er.dduvs.in.ua/handle/123456789/5717. [in Ukr.].
6. Global Cybersecurity Outlook 2022. INSIGHT REPORT JANUARY 2022. (2022, January 30). *The World Economic Forum*. Retrieved March 15, 2022 from https://weforum.org
7. Rybalchenko, L., Ryzhkov, E., Ohrimenco, S. (2021) Modeling economic component of national security. *Philosophy, Economics and Law Review*, No 1(1), pp. 25–36.
8. Rybalchenko, L., Ryzhkov, E., Ohrimenco, S. (2021) Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review*, No 1(2), pp. 67–80.
9. Rubalchenko, L., Ryzhkov, E. (2019) Ensuring enterprise economic security. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. Special Issue № 1, pp. 268-271.
10. Rubalchenko, L., Kosychenko, O. (2019) Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. Special Issue № 1, pp. 264-267.
11. Special Report: Ukraine. An overview of Russias cyberattack activity in Ukraine. Microsofts Digital Security Unit. April 27, 2022. URL : https://www.radiosvoboda.org/a/news-microsoft-rosia-kiberataky/31824183.html.
12. Rybalchenko, L., Ryzhkov, E., Ciobanu G. (2022) Global consequences of the loss of business in countries around the world caused by fraud. *Philosophy, Economics and Law Review*, No 1(2), pp. 93–102.

ABSTRACT

Liudmyla Rybalchenko. Cybercrime in the global space. The necessity of ensuring the security of digital infrastructure from cyber attacks grows every day and becomes the topical issue of nowadays. Cyber crime develops very quickly and has various different types and forms. Among the most widespread cyber attacks are those which aimed to steal or gain unauthorized access, block the access to the work files, stealing of the personal data, spreading viruses in computer systems and networks, extorting money and so on.

Cybercrime tends to grow not only every year, but also every day. Therefore, it is important to ensure the security of digital infrastructure. Cyber security has an important priority for the national security system of Ukraine. Providing reliable protection of the national cyber security system and resistance to any cyber threats must be ensured on a permanent basis and with the use of accumulated practical experience of other leading developed countries in this important matter.

The rapid development of information technology has become a significant postulate for the creation of new ways of cyber security, which is caused by the situation of a new technological level. The distribution of spheres of influence in cyberspace is constantly increasing. The ability of the state to protect its national interests is a priority component of each country's cyber security. Establishment of the “cyberforces” in the state will significantly contribute to effective protection of information infrastructure from possible cyber attacks, reliable protection against intrusion into the national information space, as well as the control of enemy’ information systems and their destruction.

Cyberterrorism and cyber-sabotage have become even more pronounced during the Russian invasion of Ukraine. The hybrid war against Ukraine with the use of cyber warfare, information technologies and mechanisms caused real threats not only to Ukrainian but to international cyber security as well. Cyber intelligence activities in cyberspace are part of the hybrid warfare against Ukraine.

The Ukrainian people, who made their European integration choice and now continue to defend their rights for freedom and independence in this war. In June 2022, Ukraine was granted the status of a candidate for joining the European Union, and this aspiration of the Ukrainian people was supported at the pan-European level.

Keywords: *cyber security, protection of personal data, economic crimes, unauthorized access, confidentiality of information.*