УДК 004.056+346.12
DOI: https://doi.org/10.32782/2224-6282/190-20

Ніконенко У.М.
доктор економічних наук, професор,
Українська академія друкарства
ORCID: https://orcid.org/0000-0002-6015-6248

Халіна О.В.
кандидат економічних наук, доцент,
Українська академія друкарства
ORCID: https://orcid.org/0000-0002-4086-6314

Nikonenko Uliana, Khalina Olena
Ukrainian Academy of Printing

ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМ В УМОВАХ ВИКЛИКІВ СУЧАСНОСТІ

Комунікації в кіберпросторі із застосуванням цифрових технологій відображають світовий тренд і забезпечують ефективнішу реалізацію суспільних відносин загалом, й у сфері бізнесу зокрема. Забезпечення безпеки кіберпростору в умовах викликів сучасності, досить актуальне і водночас складне питання, вирішення якого потребує комплексного підходу. У статті окреслено конструкт організаційно-правового механізму, який регламентує організацію процесу забезпечення кібербезпеки соціально-економічних систем в правовому полі та виокремлено основні тези, які відображають суть функціонування цього механізму. Зазначено, що метою функціонування організаційно-правового механізму забезпечення кібербезпеки є організація процесу захисту кібепростору через використання нормативно-правової бази як регулюючого інструменту та ефективне управління ресурсами суб'єкта господарювання. Запропоновано покласти в основу формування дієвого організаційно-правового механізму ідею створення світової системи кібербезпеки як запоруки розвитку цивілізації в умовах новітніх технологій. Встановлено, що процес захисту кіберпростору здійснюється за допомогою людських та фінансових ресурсів. Запропоновано здійснювати міжнародну співпрацю в рамках кіберзахисту, яка передбачає ратифікацію міжнародних договорів в галузі кібербезпеки, імплементацію окремих (дієвих) міжнародних норм права в національне законодавство України.

Ключові слова: *кібербезпека, соціально-економічні системи, безпека кіберпростору, організаційно-правовий механізм кібербезпеки соціально-економічних систем, ідея світової системи кібербезпеки.*

ORGANIZATIONAL AND LEGAL MECHANISM FOR ENSURING CYBERSECURITY OF SOCIO-ECONOMIC SYSTEMS IN THE CONTEXT OF MODERN CHALLENGES

Communication in cyberspace with the use of digital technologies reflects a global trend and more effective implementation of social relations in general, and in the business sector in particular. The use of digital technologies in business significantly accelerates the exchange of various information, which increases the efficiency of business processes, in particular through the use of digital marketing, online platforms for negotiations, transactions, etc. At the same time the digital world has another side, which conceals a number of threats to businesses and their owners. Digitalization is the formation of a sustainable communication system using digital technologies and cyberspace. Therefore the integration of physical and virtual environments creates preconditions for the emergence of threats, which are mostly concentrated in cyberspace. Ensuring the security of cyberspace in the face of today's challenges is a highly relevant and at the same time complex issue that requires a comprehensive approach. The article outlines the construct of the organizational and legal mechanism which regulates the organization of the process of ensuring cybersecurity of socio-economic systems in the legal field and highlights the main theses which reflect the essence of its functioning. It has been noted that the purpose of the organizational and legal mechanism for ensuring cybersecurity is to organize the process of cyberspace protection through the use of the regulatory framework as a regulatory instrument and effective management of an economic entity's resources. It has been suggested to base the formation of an effective organizational and legal mechanism on the idea of creating a global cyber security system as a guarantee of civilization development in the conditions of the latest technologies. It has been established that process of protecting cyberspace is carried out with the help of human and financial resources. Training of cybersecurity specialists is an extremely important component of the process of ensuring cybersecurity of socio-economic systems, since a high level of cyber specialist qualification increases the ability of society to withstand cyber threats. At the same time, ensuring the process of cyber specialists training and forming the necessary material and technical base for cyberspace protection require sufficient financial resources. In this context, the issue of state funding for strategic cyberspace defense programs is important. It has been suggested to carry out international cooperation within the framework of cyber defense which involves ratification of international treaties in the field of cybersecurity, implementation of certain (effective) international legal norms into the national legislation of Ukraine.

Keywords: *cybersecurity, cyberspace security, organizational and legal mechanism of cybersecurity, the idea of a global cybersecurity system.*

JEL classification: *L63, L86, K42*

Постановка проблеми. Сучасний світ функціонує в умовах постійних викликів, які, тією чи іншою мірою, породжують ряд загроз для безпеки соціально-економічних систем всіх рівнів. Одним із таких викликів є безпека кіберпростору, який використовується як майданчик для комунікацій, зокрема в рамках здійснення бізнес-процесів. Питання забезпечення безпеки кіберпростору одне з ключових в системі національної і міжнародної соціально-економічної безпеки. Відтак дослідження організаційно-правових аспектів забезпечення кібербезпеки вбачається нами досить актуальним.

Аналіз останніх досліджень і публікацій. Дослідженням питання кібербезпеки, зокрема її організаційно-правового аспекту займалися такі науковці як: О. Бакалінська, О. Бакалинський. О. Берназюк, В. Биков, О. Буров, С. Вдовенко, Ю. Даник, В. Докіль, Н. Дементієвська, В. Дудикевич, Є. Живило, Ю. Кіндзерський, І. Коропатнік, Г. Микитин, А. Ребець, О. Поляков, П. Воробієнко, Д. Хом'яков, В. Чернега, О. Чорноног та інші.

Аналіз наукових досліджень дав змогу визначити основні аспекти забезпечення кібербезпеки соціально-економічних систем. Так, у своїх працях Ю. Кіндзерський окреслює взаємозв'язок між кібербезпекою та рівнем розвитку цифрової економіки в контексті формування рекомендацій щодо політики цифровізації. Автор наголошує на необхідності впровадження дієвих систем кібербезпеки державного і корпоративного управління, а також на важливості наукових досліджень з розробки засобів кіберзахисту [5, с. 23].

Науковці В. Дудикевич, Г. Микитин та А. Ребець досліджували роль і значення фізичного аспекту кібербезпеки. Вони пропонують комплексно підходити до безпеки кіберфізичної системи, використовуючи модель «загрози-профілі-інструментарій», що забезпечує захищеність процесу відбору даних, їх збереження та передавання [4, с. 85].

Правовий аспект процесу забезпечення кібербезпеки та кібероборони розглядали в своїх роботах такі науковці як: С. Вдовенко, Є. Живило, О. Чорноног, В. Докіль, О. Бакалінська, О. Бакалинський.

Зокрема, в наукових доробках О. Бакалінської та О. Бакалинського зазначається, що найперспективнішими напрямами розвитку національної системи кіберзахисту є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; забезпечення процесу підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності та культури комунікацій в кіберпросторі; розвиток міжнародного співробітництва у сфері кібербезпеки [1, с. 106].

Аналізуючи особливості функціонування системи кібероборони в нормативно-правовому контексті, автори С. Вдовенко, Є. Живило, О. Чорноног та В. Докіль окреслюють еволюцію нормативно-правових актів України стосовно підходів щодо дій в кіберпросторі і доходять висновків, що сучасна нормативно-правова база забезпечення кібербезпеки перебуває в стадії формування та становлення. Окрім цього, автори вказують на низку протиріч, а саме:

– дефініційно-термінологічні розбіжності нормативно-правової бази сфери кібербезпеки та кібероборони;

– нормативно-правові розбіжності нормативно-правової бази України сфер кібербезпеки та кібероборони;

– законодавчі, нормативно-правові, дефініційно-термінологічні розбіжності між нормативно-правовою базою сфери кібербезпеки і кібероборони України та міжнародного співтовариства.

Автори наголошують на потребі в розробці та ухваленні нових Законів України у сфері кібербезпеки та кібероборони, що забезпечить ефективніше функціонування нормативно-правового поля кібербезпеки, кібероборони та кіберзахисту у всіх сферах національної безпеки України [2, с. 65].

В своїй роботі С. Федосюк та С. Магдисюк досліджували зарубіжний досвід забезпечення кібербезпеки на прикладі США та Китаю. Автори акцентують увагу на протистоянні США та Китаю і розглядають кібербезпеку – як сферу конкуренції між цими країнами. Визнаючи першість за Сполученими Штатами Америки, як найбільш кібеспроможною країною світу, автори водночас вказують на суттєві досягнення Китаю в сфері розробки засобів кіберзахисту та кібератак. Посилена конкуренція у сфері кібербезпеки між двома країнами, що є лідерами у цій галузі, досить суттєво здатна вплинути на безпеку світового кіберпростору.

Досліджуючи основні аспекти міжнародної співпраці у сфері забезпечення кібербезпеки, О. Поляков наголошує на актуалізації проблеми забезпечення кібербезпеки на міжнародному рівні і вказує на підвищення рівня загроз світовому кіберпростору через конфронтацію і протиборство між групами держав (США, РФ, КНР), які прагнуть довести своє домінування у кіберпросторі. В цьому контексті автор зазначає, що актуальним напрямом для України залишається продовження партнерської співпраці з НАТО у кіберсфері. Водночас головним зовнішньополітичним фарватером України у сфері кібербезпеки є: поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками НАТО; розвиток спроможності національної системи кібербезпеки та захисту національних інтересів у кіберпросторі [7, с. 134].

Таким чином, наукові розвідки питання кібербезпеки в різних її аспектах, визначили інформаційне підґрунтя застосування комплексного підходу до формування організаційно-правового механізму забезпечення кібербезпеки соціально-економічних систем в умовах викликів сучасності.

Відзначаючи всебічність і ґрунтовність проведених наукових досліджень основних аспектів кібербезпеки, зважаючи на актуальність досліджуваного питання та усвідомлення потреби пошуку нових підходів до формування дієвого механізму безпеки кіберпростору, нами вбачається доцільним продовжити наукові напрацювання в галузі кібербезпеки соціально-економічних систем, зокрема в частині її організаційно-правового регулювання.

Мета статті полягає у створенні теоретичного підґрунтя для формування ефективного організаційно-правового механізму забезпечення безпеки кіберпростору соціально-економічних систем в умовах викликів сучасності.

Виклад основних результатів дослідження. Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та дер-

жави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [8, с. 2].

Комплексний підхід до формування будь-якої системи чи механізму передбачає врахування всіх аспектів досліджуваної теми в контексті їхньої взаємодії один з одним та із зовнішнім середовищем.

Основними аспектами організаційно-правового механізму забезпечення кібербезпеки є:

– нормативно-правова база, що регламентує процес захисту кіберпростору від загроз та визначає основні норми і правила комунікацій в кіберпросторі;

– організація процесу забезпечення кібербезпеки силами та засобами суб'єктів безпеки на різних рівнях функціонування соціально-економічних систем та комунікативних цифрових платформ.

– ресурсне забезпечення функціонування організаційно-правового механізму кібербезпеки, яке включає фінансовий ресурс, як засіб оплати за товари, роботи, послуги та людський ресурс – як джерело інтелектуальної, управлінської та інженерної діяльності для реалізації процесу забезпечення кібербезпеки необхідними пристроями, додатками, програмними продуктами тощо.

Нормативно-правовий захист – це вид захисту, що ґрунтується на низці державних законів, указів, постанов, розпоряджень та відповідних міжнародних документів [3, с. 25].

Конструкт організаційно-правового механізму базується на організації процесу забезпечення кібербезпеки в правовому полі. Функціонування даного конструкту забезпечується, з одного боку, державним регулюванням через сукупність нормативно-правових актів, з іншого – суб'єктами кібербезпеки через ефективне управління ресурсами (кадровими, фінансовими) (рис. 1).

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначаються Законом України «Про основні засади забезпечення кібербезпеки України» [8].

Поряд з ним, нормативно-правову базу складають такі законодавчі акти України як: Закон України «Про національну безпеку України», Закон України «Про Державну службу спеціального зв'язку та захисту інформації України, Закон України «Про критичну інфраструктуру». Окрім цього, сферу кібербезбеки регулює ціла низка Указів Президента України, Постанов Кабінету Міністрів України та інших нормативних актів.

Незважаючи на те, що в Україні процес розвитку нормативно-правової бази для регулювання процесів і відносин у кіберпросторі лише зароджується [11, с. 235], кількість законодавчих та концептуальних документів є достатньою, щоб охопити ефективні правові механізми регулювання відносин у віртуальному інформаційному середовищі, зокрема, що стосується кібербезпеки. Однак, наявна нормативно-правова база, не забезпечує необхідний рівень безпеки кіберпростору, як на рівні держави, так і на рівні особистості, що створює передумови для пошуку ефективних підходів до формування організаційно-правового механізму в галузі кібербезпеки.

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– Збройні Сили України, інші військові формування, утворені відповідно до закону;

– Національний банк України;

– підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

– суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяль-

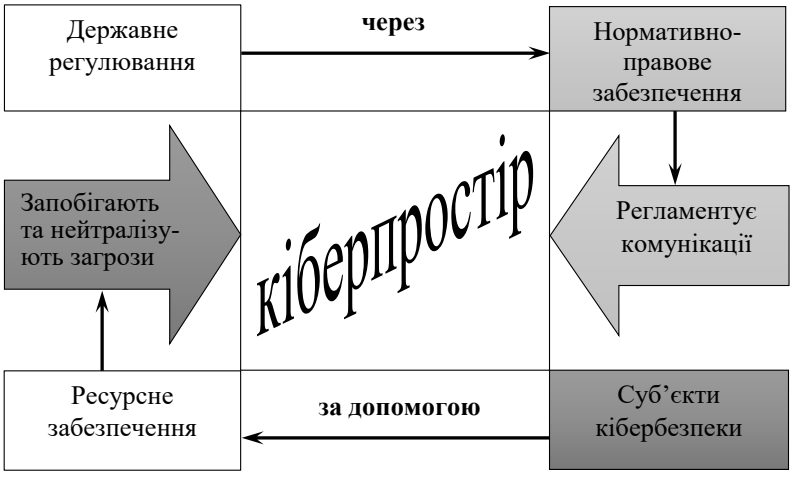

Рис. 1. Конструкт організаційно-правового механізму

Джерело: авторська розробка

ність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Важливим аспектом в конструкті кібербезпеки є ресурсне забезпечення, оскільки саме воно дає можливість здійснювати будь-яку діяльність, пов'язану із захистом кіберпостору.

Головним ресурсом в процесі забезпечення безпеки кіберпростору є фахівці з кібербезпеки. Завдяки інтелектуальним та творчим здібностям розробника програмного забезпечення створюється продукт, здатний виконувати функцію захисту інформації та даних. Фахівці з кібербезпеки працюють над створенням і функціонуванням надійної, захищеної від дій зловмисників структури обміну даними та усуненням вразливих місць в мережі.

Необхідним ресурсом в процесі забезпечення кібербезпеки є фінанси, які не лише супроводжують весь процес захисту кіберпростору у формі плати за роботи, товари, послуги, а й забезпечують економічні гарантії всім учасникам процесу.

Державні інституції, які є суб'єктами забезпечення кібербезпеки, в межах своїх повноважень, повинні здійснювати постійний супровід процесу забезпечення кібербезпеки на всіх рівнях соціально-економічних систем, в тому числі із застосуванням права держави на примус у випадках, коли це необхідно.

Забезпечення кібербезпеки на міжнародному рівні є транснаціональним завданням, яка не може бути виконане однією державою чи групою держав. Це завдання усіх цивілізованих країн, спільні зусилля яких матимуть інтегральний ефект і сприятимуть підвищенню рівня міжнародної безпеки в кіберпросторі як окремо взятої держави, так і всього світового співтовариства загалом [3, с. 283].

Для формування ефективного організаційно-правового механізму забезпечення кібербезпеки соціально-економічних систем, нами виокремлено основні (ключові) тези, які відображатимуть суть його функціонування.

Перша теза. Метою функціонування організаційно-правового механізму забезпечення кібербезпеки є організація процесу захисту кібепростору через використання нормативно-правової бази як регулюючого інструменту та ефективне управління ресурсами суб'єкта господарювання.

Друга теза. В основі формування дієвого організаційно-правового механізму має лежати ідея створення світової системи кібербезпеки як запоруки розвитку цивілізації в умовах новітніх технологій, яка відображатиме еволюцію свідомості людей, котрі прагнуть жити в цивілізованому світі, де найвищою цінністю є людина, і будь-яка діяльність спрямована лише на захист її інтересів загалом.

Третя теза. Процес захисту кіберпростору здійснюється за допомогою людських та фінансових ресурсів.

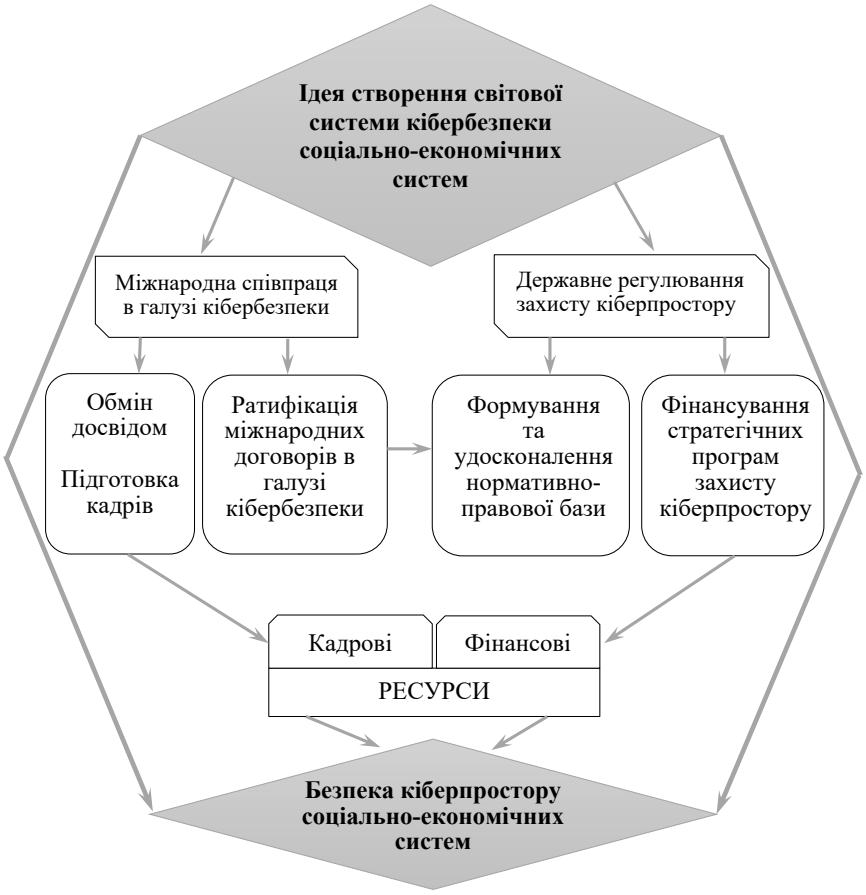

Рис. 2. Організаційно-правовий механізм забезпечення кібербезпеки соціально-економічних систем

Джерело: авторська розробка

Підготовка фахівців з кібербезпеки – вкрай важлива складова процесу забезпечення кібербезпеки соціально-економічних систем, оскільки високий рівень кваліфікації кіберфахівців підвищує здатність суспільства протистояти кіберзагрозам. Водночас забезпечення процесу підготовки кіберфахівців та формування необхідної матеріально-технічної бази захисту кіберпростору потребує достатнього обсягу фінансових ресурсів. В цьому контексті важливим є питання державного фінансування стратегічних програм захисту кіберпростору.

Четверта теза. Міжнародна співпраця в рамках кіберзахисту передбачає ратифікацію міжнародних договорів в галузі кібербезпеки, імплементацію окремих (дієвих) міжнародних норм права в національне законодавство України. Водночас міжнародна співпраця в галузі кібербезпеки має передбачати залучення до співпраці кіберфахівців різних країн, з метою обміну досвідом та підготовки кадрів.

Беручи за основу викладені вище ключові тези нами, з урахуванням комплексного підходу, розроблено організаційно-правовий механізм забезпечення кібербезпеки соціально-економічних систем (рис. 2).

Таким чином, при формуванні організаційно-правового механізму забезпечення кібербезпеки соціально-економічних систем, було акцентовано увагу на важливості ідеї світової кібербезпеки, яка відображає новий рівень розвитку суспільства, головною цінністю якого є людина, а вся діяльність спрямована на її благо.

Висновки. Підбиваючи підсумки дослідження, варто наголосити на важливості основних (ключових) тез. Зародження ідеї безпеки світового кіберпростору є природньою потребою цивілізованого світу, однак практичне її втілення потребує цілої низки складних механізмів на рівні всіх держав світу, що робить цей процес важкопрогнозованим з точки зору його результативності. Водночас потреба у світовій кібербезпеці на всіх рівнях світової соціально-економічної системи, створює передумови до пошуку дієвих прикладних механізмів її реалізації. Одним з таких механізмів є організаційно-правовий механізм забезпечення кібербезпеки як координуючий інструмент діяльності всіх суб'єктів у кіберпросторі.

Розробка нових підходів до забезпечення кібербезпеки повинна здійснюватися на рівні держави і втілюватися на всіх рівнях соціально-економічного середовища суспільства. Нові підходи повинні ґрунтуватися не лише на збільшенні кількості нових нормативно-правових актів, а і на їх ефективності, що забезпечуватиметься чітким й однозначним його трактуванням. Це, передусім, передбачає залучення до розробки проєктів нормативно-правових актів, що регулюють діяльність у кіберпросторі як юристів, так і фахівців з інформаційних технологій та зв'язку. В такому контексті важливим завданням є підготовка фахівців з кібербезпеки як головної рушійної сили у формуванні нової парадигми функціонування світового кіберпростору, яка б відображала ідею світової кібербезпеки як запоруки розвитку цивілізації в умовах викликів сучасності.

Список використаних джерел:

1. Бакалінська О, Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство, право*. 2019. № 9. С. 100–108.

2. Вдовенко С.Г., Живило Є.О., Черноног О.О., Докіль В.М. Аналіз особливостей функціонування системи кібероборони. Нормативно-правові аспекти. *Збірник наукових праць Військового інституту КНУ імені Тараса Шевченка*. 2022. № 74. С. 52–72.

3. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони : підруч. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.

4. Дудикевич В.Б, Микитин Г.В., Ребець А.І. Комплексна система безпеки кіберфізичної системи, IPHONE-WI-FI, Bluettooth-додавачі. *Системи обробки інформації.* 2017. № 2(148). С. 84–87.

5. Кіндзерський Ю.В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник.* 2020. № 3. С. 18–25.

6. Павленко С.В. Сутність кібербезпеки у теорії інформаційного права. *Право та державне управління.* 2021. № 2. С. 28–33.

7. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2(37). С. 129–138.

8. Про основні засади забезпечення кібербезпеки України : Закон України від 17 бер. 2022 р. № 2470-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 22.02.2024).

9. Trzonkowski K., Khalina O., Kolisnichenko P., Rozumovych N., Zhyhulin, O. Information systems for financial and economic security in the face of cyberthreats: study of characteristics in the context of modern administrative and legal mechanism. *Amazonia Investiga*. 2023. № 12(69). P. 315–324.

10. Халіна О.В., Сидоренко Я.А. Механізм забезпечення кібербезпеки бізнесу в умовах викликів сучасності. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали IX Всеукр. наук.-практ. конф., 23–25 листоп. 2023 р. Львів : Укр. акад. друкарства, 2023. С. 127–128.

11. Хом'яков Д.О., Коропатнік І.М. Система здійснення нормативно-правового регулювання кібербезпеки у США. *Юридичний науковий електронний журнал*. 2020. № 4. С. 234–237 URL: http://www.lsej.org.ua/4_2020/58.pdf (дата звернення: 10.02.2024).

References:

1. Bakalinska O, Bakalynskyi O. (2019) Pravove zabezpechennia kiberbezpeky v Ukraini [Legal support for cybersecurity in Ukraine]. *Pidpryiemnytstvo, hospodarstvo, pravo – Entrepreneurship, business, law,* vol. 9, pp. 100–108.

2. Vdovenko S. H., Zhyvylo Ye. O., Chernonoh O. O., Dokil V. M. (2022) Analiz osoblyvostei funktsionuvannia systemy kiberoborony. Normatyvno-pravovi aspekty [Analysis of the functioning of the cyber defense system. Regulatory and legal aspects] *Zbirnyk naukovykh prats Viiskovoho instytutu KNU imeni Tarasa Shevchenka – Collection of scientific papers of the Military Institute of Taras Shevchenko National University of Kyiv,* no. 74, pp. 52–72.

3. Danyk Yu. H., Vorobiienko P. P., Cherneha V. M. (2019) Osnovy kiberbezpeky ta kiberoborony [Fundamentals of cybersecurity and cyber defense]. Odesa: ONAZ im. O. S. Popova. (in Ukrainian)

4. Dudykevych V. B, Mykytyn H. V., Rebets A. I. (2017) Kompleksna systema bezpeky kiberfizychnoi systemy, IPHONE-WI-FI, Bluettooth-dodavachi [Integrated security system of cyber-physical system, IPHONE-WI-FI, Bluettooth devices]. *Systemy obrobky informatsii – Information processing systems,* vol. 2, no. 148, pp. 84–87.

5. Kindzerskyi Yu. V. (2020) Kiberbezpeka ta stanovlennia tsyfrovoi ekonomiky: problemy vzaiemozviazku [Cybersecurity and the emergence of the digital economy : problems of interconnection]. *Ekonomichnyi visnyk – Economic Bulletin,* vol. 3, pp. 18–25.

6. Pavlenko S. V. (2021) Sutnist kiberbezpeky u teorii informatsiinoho prava [The essence of cybersecurity in the theory of information law]. *Pravo ta derzhavne upravlinnia – Law and public administration,* no. 2, pp. 28–33.

7. Poliakov O. M. (2021) Aktyvizatsiia mizhnarodnoi spivpratsi u sferi zabezpechennia kiberbezpeky : shliakhy udoskonalennia v realiiakh sohodennia [Intensification of international cooperation in the field of cybersecurity : ways to improve in today's realities]. *Informatsiia i pravo – Information and law,* vol. 2, no. 37, pp. 129–138.

8. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» from 17 August 2022. № 2470-IX.

9. Trzonkowski K., Khalina O., Kolisnichenko P., Rozumovych N., Zhyhulin, O. (2023) Information systems for financial and economic security in the face of cyberthreats : study of characteristics in the context of modern administrative and legal mechanism. *Amazonia Investiga,* vol. 12, no. 69, pp. 315–324.

10. Khalina O. V., Sydorenko Ya. A. (November 23–25, 2023) Mekhanizm zabezpechennia kiberbezpeky biznesu v umovakh vyklykiv suchasnosti [A mechanism for ensuring business cybersecurity in the face of modern challenges]. *Proceedings of the Materialy IX Vseukrain. nauk.-prakt. konf.*, pp. 127–128.

11. Khomiakov D. O., Koropatnik I. M. (2020) Systema zdiisnennia normatyvno-pravovoho kiberbezpeky u SShA [The system of regulatory cybersecurity in the USA]. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal scientific electronic journal,* no. 4, pp. 234–237. Available at: http://www.lsej.org.ua/4_2020/58.pdf