МІЖРЕГІОНАЛЬНА АКАДЕМІЯ
УПРАВЛІННЯ ПЕРСОНАЛОМ

НАУКОВІ ПРАЦІ МІЖРЕГІОНАЛЬНОЇ АКАДЕМІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ

ЮРИДИЧНІ НАУКИ

SCIENTIFIC WORKS OF INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT

LEGAL SCIENCES

Випуск 3 (66), 2023

Видавничий дім
“Гельветика”
2023

УДК 34

Редакційна колегія

Кислий А. М., доктор юридичних наук, професор, заслужений юрист України, директор Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом **(головний редактор)**

Берзін П. С., доктор юридичних наук, доцент, професор кафедри кримінального права та кримінології Інституту права, Київський національний університет імені Тараса Шевченка

Богатирьов І. Г., доктор юридичних наук, професор, професор кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Вакулік О. О., кандидат юридичних наук, доцент, доцент кафедри криміналістики та судової медицини, Національна академія внутрішніх справ

Головко Л. О., кандидат юридичних наук, доцент, доцент кафедри міжнародного права та порівняльного правознавства, Національний університет біоресурсів і природокористування України

Гордієнко С. Г., доктор юридичних наук, доцент, професор кафедри національної безпеки Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Доценко О. С., доктор юридичних наук, професор, професор кафедри публічного управління та адміністрування, Національна академія внутрішніх справ

Заросило В. О., доктор юридичних наук, професор, завідувач кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Калиновський Б. В., доктор юридичних наук, професор, завідувач кафедри конституційного права та прав людини, Національна академія внутрішніх справ

Кисленко Д. П., кандидат юридичних наук, доктор педагогічних наук, доцент, професор кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Козаченко О. І., доктор юридичних наук, доцент, доцент кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна академія управління персоналом

Козін С. М., доктор юридичних наук, старший викладач кафедри теорії та історії держави і права, Національний університет біоресурсів і природокористування України

Колб О. Г., доктор юридичних наук, професор, заслужений юрист України, професор кафедри кримінології та кримінально-виконавчого права, Національний юридичний університет імені Ярослава Мудрого

Ладиченко В. В., доктор юридичних наук, професор, завідувач кафедри міжнародного права та порівняльного правознавства, Національний університет біоресурсів і природокористування України

Лисенко С. О., доктор юридичних наук, професор, професор кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Макєєва О. М., кандидат юридичних наук, доцент, доцент кафедри теорії та історії держави і права, Національний авіаційний університет

Мердова О. М., кандидат юридичних наук, доцент, завідувач кафедри адміністративно-правових дисциплін факультету № 2, Донецький державний університет внутрішніх справ

Муравйов К. В., доктор юридичних наук, доцент, завідувач кафедри адміністративного, фінансового та банківського права Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна академія управління персоналом

Омаров Азад Енвер огли, доктор наук з державного управління, доцент, професор кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом

Піддубний О. Ю., доктор юридичних наук, професор, завідувач кафедри цивільного та господарського права, Національний університет біоресурсів і природокористування України

Сервецький І. В., доктор юридичних наук, доцент, завідувач кафедри національної безпеки Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Стрельбицька Л. М., доктор юридичних наук, професор, професор кафедри цивільно-правових дисциплін, Національна академія Служби Безпеки України

Стрельбицький М. П., доктор юридичних наук, професор, головний науковий співробітник науково-організаційного центру, Національна академія Служби Безпеки України

Стрелюк Я. В., доктор юридичних наук, прокурор, Офіс Генерального прокурора України

Чуєнко В. І., кандидат юридичних наук, доцент кафедри цивільно-правових дисциплін та міжнародного права Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом

Шульга Є. В., доктор юридичних наук, доцент, професор кафедри міжнародного права та порівняльного правознавства, Національний університет біоресурсів і природокористування України

Яра О. С., доктор юридичних наук, професор, професор кафедри адміністративного та фінансового права, декан юридичного факультету, Національний університет біоресурсів і природокористування України

Łukasz Moniuszko, Doktor habilitowany, Profesor, Wyższa Szkoła Gospodarki w Bydgoszczy (Bydgoszcz, Rzeczpospolita Polska)

Agnieszka Szpak, dr hab., Professor, Department of International Security, Institute of Security Studies, Toruń, Poland

Dariusz Skalski, dr hab., Professor, Gdansk University of Physical Education and Sport, Gdańsk, Poland

Затверджено Вченою радою
Міжрегіональної Академії управління персоналом 18.10.2023 (протокол № 9)
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
серія КВ № 24777-14717Р,
видане Міністерством юстиції України 21.04.2021 р.

Відповідно до Наказу МОН України № 320 від 07 квітня 2022 року (додаток 2) журнал включено до Переліку наукових фахових видань України (категорія Б). Спеціальності: 081 – Право; 262 – Правоохоронна діяльність; 293 – Міжнародне право.

Видання індексується Google Scholar

DOI: 10.32689/2522-4603

Наукові праці МАУП. Юридичні науки. 2023. Вип. 3 (66). Київ : Міжрегіональна Академія управління персоналом, 2023. 48 с. Публікуються статті науковців, які досліджують актуальні проблеми розвитку права. Для науковців, викладачів, студентів та всіх, кого цікавить розвиток юридичної науки в Україні.

ISSN 2786-5134 (Print)
ISSN 2786-5142 (Online)

© Оформлення «Видавничий дім «Гельветика», 2023

ЗМІСТ

CONTENTS

УДК 343.102
DOI https://doi.org/10.32689/2522-4603.2023.3.1

Ігор ЛЕОНЕНКО
кандидат юридичних наук, доцент кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом, вул. Фроментівська, 2, м. Київ, Україна, 03039, leonenko_83@ukr.net
ORCID: 0000-0002-2963-5814

Ihor LEONENKO
Candidate of Legal Sciences, Associate Professor of the Department of Law Enforcement and Anti-Corruption Activities, Institute of Law named after Prince Volodymyr the Great, Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039, leonenko_83@ukr.net
ORCID: 0000-0002-2963-5814

ІНСТИТУТ ДЕТЕКТИВІВ У НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ: СУЧАСНИЙ СТАН, ПЕРЕВАГИ ТА ПЕРСПЕКТИВИ

INSTITUTE OF DETECTIVES IN THE NATIONAL POLICE OF UKRAINE: CURRENT STATE, ADVANTAGES AND PROSPECTS

Стаття присвячена проблематиці впровадження інституту поліцейських детективів у підрозділах Національної поліції України. Даний інститут передбачає створення єдиного підрозділу поліцейських детективів, який об'єднав би роботу слідчих органів та оперативних працівників. З моменту вторгнення Російської Федерації в Україну значно більшилося навантаження на поліцейські підрозділи, зокрема, в частині розслідування тяжких та особливо тяжких злочинів, що вимагає суттєвих змін та вдосконалення в оранізації досудового розслідування кримінальних правопорушень. Метою даної статті є аналіз чинного законодавства України, наукових досліджень та правозастосовної діяльності поліцейських з указаного напряму. Завданням статті є розробка та надання пропозицій і рекомендацій щодо законодавчого закріплення інституту поліцейських детективів у кримінальному процесуальному законодавстві України. У статі проведено аналіз сучасних поглядів вчених на вказану проблематику, розглянуто досвід зарубіжних країн, а також приділено увагу шляхам реформування Національної поліції й утворенню в її структурі інституту детективів. Запропоновано низку змін та доповнень в частині національного законодавства України, зокрема, до Кримінального процесуального кодексу України, Закону України «Про оперативно-розшукову діяльність» та Закону України «Про Національну поліцію». Наведені результати опитування майбутніх офіцерів та практичних працівників Національної поліції України щодо необхідності реформування кримінальної поліції та впровадженння інституту детективів. Так, зокрема, 62% респондентів висловилися за впровадження даного інституту у поліцейську діяльність. Наголошується, що створення інституту детективів в системі Національної поліції України, сприятиме зменшенню навантаження на органи досудового розслідування, більш якісному та швидкому розслідуванню кримінальних правопорушень, збереженню таємниці слідства, зменшенню рівня корупції та внутрішньої бюрократії в системі Національної поліції України. Зроблено висновоко, що остаточну крапку в даному питанні зміг би поставити відповідний законопроект, наслідком якого стала б переатестація слідчих та оперативних працівників Національної поліції України у детективи, підготовка сучасних кадрів у закладах освіти за напрямом (спеціальністю) «детективна діяльність», а також перехід до європейських стандартів та відмова від застарілої радянської системи.

Ключові слова: *поліцейський детектив, інститут детективів, досудове розслідування, кримінальне правопорушення, оперативний працівник, слідчий.*

The article devoted to the problems of introducing the institute of police detectives in units of the National Police of Ukraine. This institute provides for the creation of a single unit of police detectives, which would combine the work of investigative bodies and operatives. Since the invasion of the Russian Federation in Ukraine, the burden on police units has increased significantly, in particular, in terms of investigating serious and especially grave crimes, which requires significant changes and improvements in the organization of pre-trial investigation of criminal offenses. The article is aimed at analyzing the current legislation of Ukraine, scientific research and law enforcement activities of police officers in this area. The article is aimed at developing and providing proposals and recommendations for legislative consolidation of the institute of police detectives in the criminal procedural legislation of Ukraine. The article analyzes modern views of scientists on these issues, considers the experience of foreign countries, and also pays attention to ways of reforming the National Police and the formation of an institute of detectives in its structure. A number of amendments and additions to the national legislation of Ukraine have been proposed, in particular, to the Criminal Procedure Code of Ukraine, the Law of Ukraine "On Investigative Operations" and the Law of Ukraine "On the National Police". The results of a survey of future officers and practitioners of the National Police of Ukraine on the need to reform the criminal police and introduce the institute of detectives are presented.

© Леоненко І., 2023

Thus, in particular, 62% of respondents were in favor of introducing this institution into police activities. It is noted that the creation of the institute of detectives in the system of the National Police of Ukraine will help reduce the burden on pre-trial investigation bodies, better and faster investigation of criminal offenses, preserve the secrecy of the investigation, reduce the level of corruption and internal bureaucracy in the system of the National Police of Ukraine. It is concluded that the final point in this issue could be put by the relevant draft law, which would result in the re-certification of investigators and operatives of the National Police of Ukraine into detectives, training of modern personnel in educational institutions in the direction (specialty) of "detective activity", as well as the transition to European standards and the rejection of the outdated Soviet system.

Key words: *police detective, institute of detectives, pre-trial investigation, criminal offense, operative, investigator.*

Постановка проблеми. За останній рік, з моменту військового вторгнення держави-агресора Російської Федерації (далі – РФ) в Україну, діяльність правоохоронних органів здійснюється в умовах підвищеного навантаження, що пов'язано з виконанням як безпосередньо функцій з протидії злочинності так і з виконанням завдань з відсічі та стримування збройної агресії російської федерації. Так, станом на 01.01.2023 року, слідчими Національної поліції розпочато понад 56,1 тис. кримінальних проваджень за фактами вчинення на території країни злочинів військовослужбовцями збройних сил РФ та їх пособниками. З 24 лютого 2022 року розпочато досудове розслідування у майже 68 тис. кримінальних провадженнях щодо вчинення майнових злочинів в умовах воєнного стану, зокрема крадіжок (65,9 тис.), грабежів (1,8 тис.) та розбоїв (356) [1]. Цілком зрозуміло, що в сучасних надскладних умовах суттєвих змін та модернізації потребує, зокрема, система органів досудового розслідування в складі Національної поліції України (далі – НП України).

Стан дослідження проблеми. Дослідженням проблематики запровадження інституту поліцейських детективів в системі НП України займалися такі вітчизняні вчені, як С. А. Вишевський, О. М. Ємець, О. П. Заворіна, О. В. Злагода, С. М. Князєв, А. М. Кислий, В. А. Орлов, Р. В. Осуховський, С. І. Пічкуренко, І. В. Сервецький, С. В. Тихонов, В. В. Чернєй, С. С. Чернявський та ін. Однією з останніх досліджуваній тематиці була присвячена монографія авторського колективу у складі М. О. Семенишина, В. М. Бесчастного, С. С. Вітвіцького «Детективна діяльність в механізмі запобігання злочинності» [2]. Разом з тим слід зазначити, що не зважаючі на чисельні наукові дослідження та експерименти, в Україні досі відсутній законопроект, який передбачав би внесення відповідних змін і доповнень у кримільно процесуальне законодавство.

Мета і завдання дослідження. Метою даної статті є аналіз чинного законодавства України, наукових досліджень та правозастосовної діяльності поліцейських з указаного напряму. Завданням статті є розробка та надання пропозицій і рекомендацій щодо законодавчого закріплення інституту поліцейських детективів у кримінальному процесуальному законодавстві України.

Викладення основного матеріалу. Сьогодні в правоохоронних органах більшості країн ЄС та США функціонують детективні підрозділи, натомість таких посад, як *слідчий* та *оперуповноважений* не існує взагалі. Крім того, визначення посадових осіб, які займають розкриттям та розслідуванням злочинів вказаними термінами, не відповідає умовам сьогодення. Дана термінологія являється застарілою та запозиченою з радянських часів.

Безсумнівно, необхідно продовжувати реформування Національної поліції, а саме шляхом поєднання в одній посаді двох функцій: слідчої та оперативної і утворення інституту детективів в Національній поліції.

Серед країн пострадянського простору наша держава являється не єдиною, хто намагається створити інститут поліцейських детективів. Вперше досвід функціонування детективних підрозділів запровадила Грузія.

Так, наприклад, у Міністерстві внутрішніх справ Грузії взагалі відсутній інститут слідчого. Зокрема, ліквідовано посади оперативного працівника карного розшуку. Таким чином, сталося злиття оперативно-розшукової та слідчої діяльності, що свідчить про перейняття у ході реформ американського досвіду здійснення досудового розслідування [3, с. 12]. У Грузії, як і удержавах, де системно застосовуються досвід діяльності поліцейських органів США, поняття «детектив» означає назву посадової особи правоохоронних органів, яка на професійному рівні виконує функції по розслідуванню та розкриттю злочинів. Детектив, за родом діяльності, здійснює слідчі (процесуальні) та оперативні (оперативно-розшукові) функції [3, с. 13].

На думку О. П. Орлова, на сьогодні в підрозділах поліції склалась ситуація, коли співробітники підрозділів кримінальної поліції припинили будь-яку активну діяльність в очікуванні письмових доручень слідчого. А слідчі, через надмірне навантаження зареєстрованих кримінальних проваджень (200–300 на одного слідчого), фактично не в змозі аналізувати кожне

з них та визначати завдання оперативно-пошукового характеру. При чому слідчі в окремих випадках зловживають своїми повноваженнями і доручають виконання таких процесуальних дій, які вони в змозі виконати самостійно [4, с. 121]. Об'єднання в одному підрозділі співробітників органу досудового розслідування та кримінальної поліції на місцевому рівні (відділи, відділення поліції) надасть широкі повноваження місцевим поліцейським детективам щодо проведення досудового розслідування, негласних слідчих (розшукових) дій, оперативно-розшукової діяльності [5, с. 147].

Слід зазначити, що у чинному національному законодавстві відсутнє визначення поняття «детектив». Однак тлумачення даного терміну міститься у Великій українській юридичній енциклопедії, де вказано, що *детектив* – це службова особа відповідного органу досудового розслідування, уповноважена в межах своєї компетенції, визначеної кримінальним процесуальним законодавством, із застосуванням гласних і негласних методів здійснювати виявлення, попередження, розкриття та розслідування злочинів (проводити оперативно-розшукову діяльність і досудове розслідування) [6, с. 161].

Як справедливо зазначає О. П. Заворіна, детектив повинен об'єднувати функції поліцейського слідчого підрозділу та поліцейського кримінальної поліції. Об'єднання двох функцій у посаді детектива дозволить поліцейському максимально володіти всією інформацією про хід розслідування кримінальних проваджень, а також супроводжувати провадження від початку і до кінця [7, с. 78].

У 2018 р. в деяких підрозділах НП України почали проводитися чисельні експерименти щодо запровадження інституту детективної діяльності. Даний інститут передбачає створення єдиного підрозділу поліцейських детективів, який об'єднав би роботу слідчих органів та оперативних працівників. Відповідний досвід було запозичено у деяких держав-членів Європейського Союзу. Так, зокрема, наказом МВС України від 06.07.2017 р. № 570 «Про організацію діяльності органів досудового розслідування Національної поліції України» [8] у слідчих управліннях ГУНП в областях було створено відділи розслідування особливо тяжких злочинів (службу поліцейських детективів). Ініціаторами створення таких підрозділів була Консультативна місія Європейського Союзу в Україні (далі – КМЄС).

Так у восьми слідчих підрозділах в різних областях України розпочався експеримент під назвою «Поліцейський детектив», у якому об'єднали слідчих та оперативників в один структурний слідчий підрозділ. На зазначені підрозділи було покладено здійснення розслідувань за фактами скоєння найбільш складних, резонансних, тяжких та особливо тяжких кримінальних правопорушень, а також таких, що набули широкого суспільного резонансу. Головною концепцією експерименту щодо впровадження інституту детективів в Національній поліції України є: 1) усі поліцейські мають однакові повноваження щодо виявлення, розкриття та розслідування злочинів; 2) внутрішній поділ на оперативників та слідчих в межах одного підрозділу (посади оперативників та слідчих замінити посадами «детективів»); 3) краща координація розслідувань; 4) обмін інформацією по справах в провадженні; 5) відсутність внутрішньої бюрократії (єдина система підпорядкування); 6) збалансоване навантаження; 7) створення умов для більш успішного вирішення проблем та покращення якості розслідування [9].

Однак, не зважаючи на доцільність вищевказаного експерименту, у зв'язку з неврегульованістю в національному законодавстві питання про функціонування в поліції детективних підрозділів, виникали ситуації з недостатнім розумінням місця експериментальних підрозділів у структурі ГУНП в областях деякими керівниками прокуратури [10, с. 152].

З метою усунення відповідних непорузумінь та прогалин КМЄС запропонував ряд доречних пропозицій щодо впровадження інституту «детективів» та внесення певних змін до деяких законодавчих актів, зокрема: 1) у ч. 3 ст. 13 Закону України «Про Національну поліцію» виключити поняття «орган досудового розслідування»; 2) у ч. 2 ст. 38 Кримінального процесуального кодексу України (далі – КПК України) «слідчі підрозділи» замінити на «уповноважені підрозділи»; 3) у ст. 5 Закону України «Про оперативно-розшукову діяльність» слова «оперативні підрозділи» замінити словами «уповноважені підрозділи» [9].

З огляду на вищевикладене, пропонуємо наступну низку змін та доповнень в частині національного законодавства України, зокрема, до КПК України, Закону України «Про оперативно-розшукову діяльність» та Закону України «Про Національну поліцію»: 1) дати визначення самого поняття «детектив»; 2) запровадити положення, які б передбачали порядок створення та діяльності детективних підрозділів у складі НП України; 3) визначити процесуальний статус детективів, закріпивши тим самим їх функціональні права та обов'язки; 4) ліквідувати посади слідчих та оперативних працівників, запровадивши новий інститут – поліцейських детективів; 5) визначити підслідність

детективів Національного антикорупційного бюро України, Державного бюро розслідувать, Бюро економічної безпеки та Національної поліції України.

На користь відповідних змін свідчить нещодавне опитування майбутніх офіцерів та практичних працівників НП України щодо необхідності реформування кримінальної поліції та впровадженння інституту детективів. Так, зокрема, 62% респондентів висловилися за впровадження інституту детективів у поліцейську діяльність. Крім цього, 53% відсотки опитаних вважають, що впровадження інститут детективів сприятиме якіснішому розслідуванню кримінальних правопорушень, а 39% висловили думку, що даний інститут істотно зменшив би обсяг документообігу в оганах поліції [11].

Висновки. Таким чином, слід зазначити, що створення інституту детективів в системі НП України, на нашу думку, сприятиме: 1) зменшенню навантаження на органи досудового розслідування; 2) більш якісному та швидкому розслідуванню кримінальних правопорушень; 3) збереженню таємниці слідства; 4) зменшенню рівня корупції та внутрішньої бюрократії в системі НП України; 5) економії державних коштів.

Звісно, що процес трансформації органів досудового розслідування не буде швидким та одномоментним явищем, а потебуватиме поступових системних змін. Остаточну крапку в даному питанні зміг би поставити відповідний законопроект, наслідком якого стала б переатестація слідчих та оперативних працівників НП України у детективи, підготовка сучасних професійних кадрів у закладах освіти за напрямом (спеціальністю) «детективна діяльність», а також перехід до європейських стандартів та відмова від застарілої радянської системи.

Література:

1. Звіт Національної поліції України про результати роботи у 2022 році. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/%20НПУ%20за%202022%20рік_.pdf (дата звернення 03.06.2023).

2. Семенишин М. О., Бесчастний В. М., Вітвіцький С. С. Детективна діяльність в механізмі запобігання злочинності : колект монографія. Київ : ВД «Дакор», 2020. 160 с.

3. Чернєй В. В. Перспективи подальшого реформування органів досудового розслідування в системі Національної поліції України / Чернєй В. В. *Науковий вісник Національної академії внутрішніх справ.* 2016. № 3 (100). С. 5–18.

4. Орлов В. А. Проблемні аспекти діяльності кримінальної поліції по розкриттю злочинів. *Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції* : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичного семінару 23 березня 2018 року. Львів : ЛьвДУВС, 2018. С. 120–122.

5. Орлов В. А. Поліцейські детективи: проблеми теорії та практки. *Сучасні проблеми правового, економічного та соціального розвитку держави* : Міжнар. наук.-практ. конф. (м. Харків, 27 листоп. 2020 р.). Харків. С. 146–147.

6. Велика українська юридична енциклопедія : у 20 т. / редкол.: В. Т. Нор (голова) та ін. ; Нац. акад. правових наук України ; Ін-т держави і права ім. В. М. Корецького НАН України; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2020. Т. 19 : Кримінальний процес, судоустрій, прокуратура та адвокатура. 960 с.

7. Заворіна О. В., Пічкуренко С. І. Актуальні проблеми впровадження інституту детективів у Національній поліції України. *Шляхи реформування кримінальної поліції: вітчизняний та зарубіжний досвід* : матеріали Міжнар. наук.-практ. круглого столу (Київ, 18 лют. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 76–78.

8. Про організацію діяльності слідчих підрозділів Національної поліції України: Наказ МВС України від 06.07.2017 № 570. URL: https://zakon.rada.gov.ua/laws/show/z0918-17 (дата звернення 03.06.2023).

9. Презентація проекту об'єднання слідчих та оперативників (Харків, Україна 2016). Збінек Ванічек, провідний радник з питань кримінальних розслідувань КМЕС в Україні (email: zbynek.vanicek@euam-ukraine.eu).

10. Заворіна О. В. Діяльність підрозділів детективів у Національній поліції України: сучасний стан і перспективи. *Право і безпека*. 2021. № 2(81). С. 149–153.

11. Тіхонов С. В. Створення інституту детективів. Шляхи реформування кримінальної поліції. URL: https://www.naiau.kiev.ua/files/kafedru/ord/2022/present_inst_detektyviv.pdf (дата звернення 03.06.2023).

References:

1. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2022 rotsi [The Report of the National Police of Ukraine on the results of work in 2022] (2022). Retrieved from https://media-www.npu.gov.ua/npu-pre-prod/sites/1/%20НПУ%20за%202022%20рік_.pdf (viewed 03.06.2023) [in Ukrainian].

2. Semenishyn, M, Beschastnyi, V., Vitvitskyi, S. (2020). Detektyvna diialnist v mekhanizmi zapobihannia zlochynnosti : kolekt monohrafiia [Detective activity in the mechanism of crime prevention: collection monograph]. Kyiv : Dakor Publishing House. 160 p. [in Ukrainian].

3. Cherney, V. (2016). Perspektyvy podalshoho reformuvannia orhaniv dosudovoho rozsliduvannia v systemi Natsionalnoi politsii Ukrainy [Prospects for further reform of pre-trial investigation bodies in the system of the National Police of Ukraine] / Cherney V. V. *Scientific Bulletin of the National Academy of Internal Affairs.* № 3(100). Pp. 5–18. [in Ukrainian].

4. Orlov, V. (2018). Problemni aspekty diialnosti kryminalnoi politsii po rozkryttiu zlochyniv [Problematic aspects of the activities of the criminal police to solve crimes]. Information and analytical support for the activities of criminal police units: a collection of scientific articles based on the reports of the All-Ukrainian scientific and practical seminar on March 23, 2018. Lviv. P. 120–122. [in Ukrainian].

5. Orlov, V. (2020). Politseiski detektyvy: problemy teorii ta praktky. *Suchasni problemy pravovoho, ekonomichnoho ta sotsialnoho rozvytku derzhavy* : Mizhnar. nauk.- prakt. Konf [Police detectives: problems of theory and practice. *Modern problems of legal, economic and social development of the state* : International. Sci.- Practical. conf.] (Kharkiv, November 27, 2020). Kharkiv. P. 146 – 147. [in Ukrainian].

6. Velyka ukrainska yurydychna entsyklopediia: u 20 t. [Great Ukrainian Law Encyclopedia (2020): in 20 vols.] / editorial board: Nor, V(chairman) and others; National. Acad. legal sciences of Ukraine ; Institute of State and Law. V. M. Koretsky NAS of Ukraine ; National. legal. Univ. them. Yaroslav the Wise. Kharkiv. Vol. 19: Criminal Procedure, Judiciary, Prosecution and Advocacy. 960 p. [in Ukrainian].

7. Zavorina, O, Pichkurenko, S. (2022). Aktualni problemy vprovadzhennia instytutu detektyviv u Natsionalnii politsii Ukrainy [Actual problems of implementation of the institute of detectives in the National Police of Ukraine]. *Ways of reforming the criminal police: domestic and foreign experience* : materials International. Sci.-Practical Round Table (Kyiv, Feb. 18, 2022). Kyiv: NAIU. P. 76 – 78. [in Ukrainian].

8. Pro orhanizatsiiu diialnosti slidchykh pidrozdiliv Natsionalnoi politsii Ukrainy: Nakaz MVS Ukrainy vid 06.07.2017 № 570 [On the organization of the activities of investigative units of the National Police of Ukraine (2017): Order of the Ministry of Internal Affairs of Ukraine dated 06.07.2017 No. 570]. Retrieved from https://zakon.rada.gov.ua/laws/show/z0918-17 (viewed 03.06.2023). [in Ukrainian].

9. Prezentatsiia proektu obiednannia slidchykh ta operatyvnykiv (Kharkiv, Ukraina 2016) [Presentation of the project of association of investigators and operatives (Kharkiv, Ukraine 2016)]. Zbinek Vaniček, EUAM Lead Criminal Investigation Adviser in Ukraine (email: zbynek.vanicek@euam-ukraine.eu).

10. Zavorina, O. (2021). Diialnist pidrozdiliv detektyviv u Natsionalnii politsii Ukrainy: suchasnyi stan i perspektyvy. *Pravo i bezpeka* [Activity of detective units in the National Police of Ukraine: current state and prospects. *Law and Security*]. 2021. № 2(81). P. 149–153. [in Ukrainian].

11. Tikhonov, S. (2017). Stvorennia instytutu detektyviv. Shliakhy reformuvannia kryminalnoi politsii [Creation of the Institute of Detectives. Ways to reform the criminal police]. Retrieved from https://www.naiau.kiev.ua/files/kafedru/ord/2022/present_inst_detektyviv.pdf (viewed 03.06.2023) [in Ukrainian].

УДК 343.132:343.985
DOI https://doi.org/10.32689/2522-4603.2023.3.2

Віталій ОСМОЛЯН
кандидат юридичних наук, декан гуманітарно-економічного факультету, доцент кафедри права та правоохоронної діяльності Хмельницького інституту, Міжрегіональна Академія управління персоналом, проспект Миру 101-А, м. Хмельницький, Україна, 29000, don.sahalin@meta.ua
ORCID: 0000-0002-9389-5581

Vitaliy OSMOLIAN
Candidate of Legal Sciences, Dean of the Faculty of Humanities and Economics, Associate Professor of the Department of Law and Law Enforcement of the Khmelnitsky Institute Interregional Academy of Personnel Management, 101-A, Myru Ave., Khmelnitsky, Ukraine, 29000, don.sahalin@meta.ua
ORCID: 0000-0002-9389-5581

ТАКТИКО-КРИМІНАЛІСТИЧНІ ПРИЙОМИ ДОПИТУ ЯК ПРАВОВА СКЛАДОВА ОТРИМАННЯ ДОСТОВІРНИХ ПОКАЗАНЬ УЧАСНИКІВ ПРОЦЕСУ

TACTICAL AND CRIMINALISTIC TECHNIQUES OF INTERROGATION AS A LEGAL COMPONENT OF RECEIVING RELIABLE TESTIMONY OF THE PARTICIPANTS IN THE PROCESS

У статті розкриваються тактико-криміналістичні прийоми допиту як невід'ємна правова складова в отриманні достовірних показань від учасників процесу під час здійснення досудового розслідування кримінального провадження. Надається на розгляд та обговорення загалу авторські рекомендації щодо прийомів та методів отримання доказової бази у кримінальному провадженні. Зокрема, розглядаються раніше напрацьовані та вже сформовані криміналістами-практиками тактико-криміналістичні прийоми допиту, опрацьовуються сучасні (інноваційні) процесуальні правила та тактичні прийоми допиту з урахуванням інформаційного розвитку сучасного суспільства. Автором статті наводяться та окреслюються правові грані щодо законності використання деяких криміналістично-процесуальних методик отримання та збирання доказової бази. Розкривається значення, надається оцінка цим новелам та новітнім підходам у реалізації завдань Кримінального та Кримінального процесуального кодексів України щодо захисту особи, суспільства та держави від кримінальних правопорушень, охороні прав, свобод та законних інтересів учасників кримінального провадження, а також у правовому забезпеченні охорони громадської безпеки та конституційного устрою України від кримінально-протиправних посягань, забезпечуючи таким чином мир і безпеку людства. Обґрунтовується необхідність подальших досліджень відповідної спрямованості, оскільки останні створюватимуть перспективи теоретичних та практичних напрацювань, а також сприятимуть розв'язанню проблемних питань у цьому напрямку процесуального права та криміналістики. Привернуто увагу на необхідність подальшої співпраці вчених і практиків у галузі матеріального та процесуального права, а саме: кримінального права, процесу та криміналістики.

Ключові слова: *докази, допит, кримінальний процес, криміналістика, кримінальне провадження, кримінальна справа, прийоми, сторони, тактика, учасник процесу.*

The article reveals the tactical and forensic techniques of interrogation as an integral legal component in obtaining reliable testimony from the participants in the process during the pre-trial investigation of criminal proceedings. The author's recommendations on techniques and methods of obtaining the evidence base in criminal proceedings are provided for review and discussion in general. In particular, tactical and forensic methods of interrogation previously developed and already formed by criminologists-practitioners are considered, modern (innovative) procedural rules and tactical methods of interrogation are developed taking into account the informational development of modern society. The author of the article states and outlines the legal aspects regarding the legality of using some forensic and procedural methods of obtaining and collecting the evidence base. The meaning is revealed and an assessment is made of these novels and the latest approaches in implementing the tasks of the Criminal and Criminal Procedure Codes of Ukraine regarding the protection of individuals, society and the state from criminal offenses, protection of the rights, freedoms and legitimate interests of participants in criminal proceedings, as well as in the legal provision of protection of public safety and of the constitutional system of Ukraine from criminal and illegal encroachments, thereby ensuring the peace and security of mankind. The need for further research in the appropriate direction is substantiated, as the latter will create prospects for theoretical and practical studies, as well as contribute to solving problematic issues in this area of procedural law and criminology. Attention was drawn to the need for further cooperation between scientists and practitioners in the field of material and procedural law, namely: criminal law, process and criminology.

Key words: *evidence, interrogation, criminal process, criminology, criminal proceedings, criminal case, techniques, parties, tactics, participant in the process.*

© Осмолян В., 2023

Постановка проблеми. Розвиток інноваційно-правової політики України набирає стрімких кроків, наближаючи мить вступу України до Європейського Союзу, як наслідок – все це вимагає від сучасного правознавця, вітчизняного законодавця приведення у відповідність власної правової системи до рівня європейських держав, зменшення рівня злочинності, вдосконалення та осучаснення норм існуючого законодавства держави, а отже, й до підвищення рівня правової освіти та свідомості у населення України, зокрема у працівників правоохоронних органів.

Неабияку роль у розбудові сучасної правової системи відіграють слідчі, детективи, експерти, криміналісти, працівники прокуратури та суду під час здійснення досудового та судового провадження у справах, а саме: при виконанні завдань кримінального провадження в частині захисту особи, суспільства та держави від кримінальних правопорушень, охороні прав, свобод та законних інтересів учасників кримінального провадження [1], а також при правовому забезпеченні охорони громадської безпеки та конституційного устрою України від кримінально-протиправних посягань [2], забезпечуючи таким чином мир і безпеку людства в рамках своєї діяльності. Зазначене не уявляється можливим без суворого дотримання норм Конституції України [3] та чинного законодавства України, моральних та етичних принципів Європейської спільноти [4, 5], глибокого знання та розуміння правоохоронцями власної участі у розбудові сучасної України. В цьому і полягає **актуальність** проблеми.

Аналіз останніх досліджень і публікацій. Проведений аналіз [1–10] показав, що вчені та практики неодноразово досліджували питання тактики отримання та збирання доказів у кримінальному процесі, а також методологію проведення допиту сторін кримінального провадження як у цілому, так її окремі аспекти зокрема. Проте розгляд тактико-криміналістичних (авторських) прийомів допиту як інноваційної правової складової у отриманні достовірних показань від учасників процесу вимагає свого детального дослідження та аналізу.

Мета статті. Метою статті є на підставі проведеного теоретичного аналізу та власного практичного досвіду розглянути тактико-криміналістичні прийоми допиту як правову складову отримання достовірних показань учасників процесу, розглянути сучасні процесуальні правила та тактичні прийоми допиту, навести авторські рекомендації щодо прийомів та методів отримання доказової бази у кримінальному провадженні, окреслити правові грані щодо законності їх використання, а також обґрунтувати необхідність подальшого дослідження відповідної спрямованості, адже останні створюватимуть перспективи теоретичних та практичних напрацювань та сприятимуть вдосконаленню вітчизняної методики отримання та збирання доказів у кримінальному провадженні, формуватимуть у працівників досудового розслідування вмотивовану та стійку правову позицію, як наслідок – покращуватимуть інноваційно-правову політику України взагалі.

Виклад основного матеріалу дослідження. Допит – це слідча дія, змістом якої є отримання та фіксація у встановленій кримінальним процесуальним законом формі показів, які містять фактичні дані, що мають значення для правильного вирішення кримінального провадження (кримінальної справи).

Як найпоширеніша слідча дія, яка проводиться у кожному кримінальному судочинстві, допит є ефективним засобом як для отримання нових, так і перевірки вже наявних у провадженні доказів.

Види допиту різняться залежно

– від процесуального становища осіб, що допитуються (допит свідка, потерпілого, підозрюваного, експерта);

– від віку допитуваних (допит дорослих та неповнолітніх, у тому числі й малолітніх);

– від складу учасників допиту (крім звичайних випадків можуть проводитися допити за участю прокурора, начальника слідчого відділу, захисника, експерта, спеціаліста, педагога, лікаря, батьків або законних представників неповнолітніх, а також одночасний допит);

– від змісту показів (правильні та помилкові покази, визнання та заперечення провини, наклеп та само обмовлення);

– від психологічної обстановки допиту (допит у конфліктній та безконфліктній обстановці);

– від того, чи допитувалася ця особа раніше, чи допитується вперше (первинний або повторний допит).

Порядок допиту регламентується Кримінальним процесуальним кодексом України (далі КПК України), який встановлює обов'язкові правила, що поширюються на всі без винятку випадки його проведення. Недотримання процесуальних правил допиту є суттєвим порушенням закону, спричиняє недійсність проведеної слідчої (судової) дії та недопустимість отриманих показів.

Разом з тим процесуальні правила носять загальний характер та не встановлюють прийомів та методів, за допомогою яких слідчий (детектив) у кожному окремому випадку отримує від допитуваних повні та достовірні показання. Цю роль виконують тактичні прийоми,

що виробляються слідчою практикою та криміналістикою.

Тактика допиту – це система заснованих на нормах кримінального процесу найбільш раціональних прийомів та методів, що забезпечують отримання об'єктивних, повних та достовірних показань [6].

Або ж, тактика допиту – це слідча (розшукова) дія, змістом якої є одержання показань від особи, яка володіє відомостями, що мають значення для розслідуваного кримінального правопорушення [7].

На відміну від процесуальних правил тактичні прийоми не передбачені кримінальним процесуальним Законом, їх застосування відбувається на розсуд слідчого (детектива) і визначається предметом допиту, процесуальним становищем допитуваного, його психічним та морально-вольовим виглядом та іншими обставинами, специфічними для кожного допиту.

Кваліфіковане застосування тактичних прийомів не можливо собі уявити без урахування та використання даних психології. З точки зору психології допит є спілкуванням слідчого з допитуваним із метою отримання від останнього інформації про кримінальне правопорушення, що розслідується [8]. Взаємодія при допиті має двосторонній характер, передбачає наявність контакту між особою, яка допитує, та допитуваним.

Встановленню правильних взаємин із допитуваним та отримання правдивих показань сприяє висока професійна культура розслідування. Етика допиту несумісна як із недобросовісністю, нервозністю, грубістю і зневагою до допитуваного, так й зі спробами будь-якими засобами завоювати його розташування. Слідчий (детектив) має бути витриманим, виявляти терпимість до допитуваного. Об'єктивність, принциповість, неупередженість слідчого (детектива) створюють сприятливі передумови для встановлення контакту.

Допит, як і будь-яке спілкування людей у процесі взаємодії, неможливий без взаємного психологічного впливу слідчого (детективу) та особи, яка допитується. Кримінальний процесуальний Закон забороняє слідчому (детективу) домагатися показань шляхом насильства, погроз та інших незаконних дій (ч. 2 ст. 11 та 18 КПК України) [1]. Під терміном «насильство» згідно із Законом розуміється не тільки фізичний, а й психічний примус. Що ж до загроз, їх застосування завжди пов'язано з незаконним впливом на психіку допитуваного. Нарешті, «інші незаконні заходи» також можуть бути обумовлені протиправними методами психологічного впливу, наприклад обманом.

Необхідною умовою отримання на допиті повних та достовірних показів є ретельна підготовка до проведення цієї слідчої дії. Незважаючи на те, що допити різних учасників процесу відрізняється як за процесуальним порядком, так й за тактичними прийомами, водночас, ми вважаємо, що вони мають деякі спільні риси.

Зокрема, загальним у підготовці до допиту є:

– вивчення матеріалів;

– визначення предмета допиту, тобто, кола тих обставин, які необхідно з'ясувати;

– вивчення психологічного портрету допитуваного та його взаємовідносин з іншими учасниками процесу, передусім з підозрюваними;

– забезпечення участі у допиті передбачених законом осіб.

Вихідним моментом підготовки до допиту є вивчення матеріалів провадження. Від цього слідчого (детектива) не звільняє навіть добра обізнаність у матеріалах справи, оскільки у даному разі йдеться про цільове та поглиблене вивчення слідчим (детективом) кримінального провадження у плані визначення тактики майбутнього допиту.

При вивченні матеріалів провадження вважаємо за доцільне робити з нього виписки із посиланням на відповідні аркуші, що суттєво полегшує складання плану та в подальшому стане у нагоді під час допиту.

Не уявляється проведення допиту без визначення переліку обставин, які необхідно з'ясувати та встановити. В іншому випадку допит буде мати загальний характер, а також може бути втрачено важливі для справи докази.

Предмет допиту визначається насамперед обізнаністю допитуваного про кримінальне правопорушення, що розслідується. Так, думку про поінформованість допитуваного про обставини справи та подію кримінального правопорушення слідчий (детектив) може та повинен скласти на підставі попереднього вивчення матеріалів провадження (справи).

Щоб знайти правильний індивідуальний підхід до особи, яка підлягає допиту, доцільно попередньо вивчити морально-психологічний портрет цієї особи ще на стадії підготовки слідчої (розшукової) дії. Не менш важливе значення має з'ясування взаємовідносин допитуваного з іншими учасниками кримінального провадження, його особистої зацікавленості у тому чи іншому результаті розслідування. Проте матеріали провадження (справи) не завжди нададуть достатні та вагомі відповіді на ці запитання. У таких випадках нами рекомендується вдаватися до «непроцесуальних» форм отримання інформації, а також використовувати з цією метою оперативні можливості поліції.

Ретельне ознайомлення з матеріалами кримінального провадження (справи) дозволяє скласти план допиту, у якому визначити обставини, які підлягають встановленню, зафіксувати питання, які слід поставити особі під час допиту, та визначити їх черговість.

Закінчується підготовка вжиттям у необхідних випадках заходів до виклику осіб, участь яких у допиті передбачена Законом (експерта, спеціаліста, перекладача, адвоката, педагога, батьків або законних представників неповнолітнього), а також викликом допитуваного.

Також, правоохоронцю необхідно чітко усвідомлювати, що значення показань підозрюваних залежить від того, наскільки результативно проведений їх допит: чим повніше та достовірніше отримані показання, тим успішніше їх можна використовувати для встановлення істини у справі. Однак отримати такі показання найчастіше вдається лише внаслідок значних зусиль, оскільки підозрювані зазвичай не схильні правдиво розповідати про скоєні ними кримінальні правопорушення. Слідчий (детектив) тим успішніше справляється зі складним завданням, що стоїть перед ним, чим повніше та майстерніше він використовує тактичні прийоми допиту. При цьому допит має здійснюватись у точній відповідності до порядку, встановленого Кримінальним процесуальним кодексом України.

Цей порядок зводиться переважно до наступного:

– слідчий зобов'язаний допитати підозрюваного негайно після його затримання чи взяття під варту, чи після оголошення йому підозри (ст.ст. 223, 224 КПК України). Закон не вказує певного терміну, протягом якого має бути проведений допит, у випадках, коли стосовно підозрюваного обрано запобіжний захід, не пов'язаний з позбавленням волі (наприклад, особисте зобов'язання чи особиста порука). Однак і в подібних випадках слідчий (детектив) не повинен відкладати допит підозрюваного на тривалий час, маючи на увазі, що з моменту обрання щодо нього будь-якого запобіжного заходу підозрюваний набуває права давати пояснення та заявляти клопотання (ст. 42 КПК України);

– підозрюваний допитується у місці проведення розслідування. Закон допускає також проведення допиту у місці знаходження особи, яка підлягає допиту, якщо це викликано тактичними міркуваннями (ст.ст. 218, 223 КПК України);

– так само, як і при допиті свідків та потерпілих, слідчий (детектив) зобов'язаний вжити заходів до того, щоб підозрювані, викликані по одному провадженні (справі), не мали можливості спілкуватися між собою;

– перед допитом підозрюваного йому має бути оголошено, у вчиненні якого кримінального правопорушення він підозрюється (ст. 42 КПК України);

– на нашу думку, доцільно розпочинати допит підозрюваного із з'ясування питання, чи визнає він себе винним у інкримінованому йому кримінальному правопорушенні. При цьому повинні бути отримані покази по кожному з пунктів оголошеної підозри, а у разі зміни тексту оголошеної підозри – знову у відношенні до усього об'єму оголошеної підозри;

– постановка питань підозрюваному допускається лише після того, як вислухано його вільне оповідання про події, які мали місце;

– у справах про кримінальні правопорушення вчинені неповнолітніми, а також осіб, які через фізичні або психічні недоліки самі не можуть здійснювати своє право на захист, до участі у провадженні (справі) допускається захисник. Відповідно у таких справах захисник має право бути присутнім при оголошенні підозри, допитах та ставити питання особі, яка допитується. Слідчий (детектив) може відвести питання захисника, але доцільно занести відведені питання до протоколу.

Більшість тактичних прийомів однаково прийнятні для допиту як підозрюваного, так і обвинувачуваного у суді [9]. Водночас тактика допиту останнього, на нашу думку, має низку особливостей, які пояснюються специфікою його процесуального становища. Відомо, що необхідність у допиті підозрюваного виникає у тих випадках, коли щодо такої особи зібрано дані, які дають підстави для затримання або обрання запобіжного заходу, але ще недостатні для оголошення кінцевої підозри, яка в подальшому ляже в основу звинувачення. Тому слідчий, приступаючи до допиту підозрюваного, в переважній більшості не має доказів, достатніх для викриття допитуваного. Доказів не лише замало, але останні ще й недостатньо перевірені, що, на нашу думку, зобов'язує слідчого (детектива) оперувати ними дуже обережно. Зрештою, у матеріалах справи явно недостатньо відомостей про особливості особистості підозрюваного, на підготовку до допиту якого (особливо якщо допитується затриманий) майже немає часу. Все це призводить до того, що у слідчого (детектива) до початку допиту ще не складається тверде переконання, з ким він має справу – з особою, яка справді вчинила кримінальне правопорушення, або з людиною, на яку впала безпідставна підозра

внаслідок несприятливого збігу обставин. Тому, ми вважаємо, щоб виключити самообмову, тактика допиту підозрюваного має бути обережнішою й ще більш вибірковою, ніж при допиті обвинуваченого в суді.

Очевидно, що тактичний план допиту підозрюваного залежить від того, чи допитується затриманий або особа, щодо якої обрано запобіжний захід, до оголошення йому підозри. Звичайно, в останньому випадку слідчому (детективу) легше намітити найбільш доцільну в тому чи іншому випадку тактику допиту, оскільки він, як правило, має більш широку інформацію та деякі відомості, що характеризують особливості особистості підозрюваного. Проте проведення допиту одразу ж після затримання теж має свої переваги, які пов'язані з тим, що допитуваний зазвичай не встигає вигадати та детально обґрунтувати неправдиву версію, швидше заплутується у власних протиріччях. Раптове затримання чинить на нього завжди сильне враження, вміле використання якого слідчим (детективом) нерідко полегшує подолання установки на брехню. Однак цей же фактор (затримання) може зламати волю особи, яка не винна у вчиненні кримінального правопорушення, та призвести до самообмови. Це завжди слід враховувати слідчому (детективу) при допиті підозрюваного, під час якого насамперед використовуються прийоми, найбільш доцільні за умов, коли доказів мало чи у їх сукупності є суттєві прогалини.

Особливості тактики допиту обвинувачуваного в суді, на нашу думку, повинні визначатися тим, що надання ним показів є засобом реалізації його права на захист. Тому, не обмежуючись з'ясуванням питання, чи визнає він себе винним, від обвинуваченого необхідно отримати конкретне пояснення за кожною з обставин, що становлять зміст інкримінованого йому звинувачення у скоєнні кримінально протиправного діяння. Одержанню від обвинуваченого правдивих показань сприяє терпляче та детальне роз'яснення суті пред'явленого звинувачення в обвинувальному акті та процесуальних прав на захист, причому корисно роз'ясняти не лише зміст інкримінованих фактів, а й санкцію норми Кримінального кодексу України, за якою кваліфіковано діяння.

Застосування тих чи інших тактичних прийомів залежить передусім від того, у якій ситуації проводиться допит: безконфліктній чи конфліктній.

Безконфліктна ситуація виникає в основному у випадках, коли підозрюваний підтверджує правильність підозри, яка виникла відносно нього, а обвинувачений визнає себе винним. Конфліктна ситуація має місце при відмові від наданні показів та при повідомленні неправдивих показів (або таких, що відповідають дійсній обстановці, проте у даний момент розцінюються слідчим (детективом) та судом як помилкові).

Очевидно, що конфліктна та безконфліктна ситуації можуть чергуватись навіть під час одного допиту залежно від зайнятої особою-допитуваного позиції з того чи іншого питання. Так, підозрюваний може визнавати одні обставини та заперечувати інші, обвинувачений, визнаючи факти, що інкримінуються йому, може в суді не погоджуватися з їх правовою кваліфікацією тощо.

Крім того, основні правила допиту – вислуховування вільної розповіді з подальшою постановкою питань, що при необхідності супроводжується пред'явленням доказів, – зберігають своє значення для допиту в будь-якій ситуації.

При допиті за умов безконфліктної ситуації основне місце займають вислуховування вільної розповіді та постановка питань.

Методи впливу на допитуваного за умов конфліктної ситуації, викликаної наданням ним хибних показів, переважно діляться на прийоми емоційного впливу та прийоми, засновані на використанні доказів, причому останні прямо залежить від обсягу зібраних доказів. При цьому прийоми, які спонукають до дачі правдивих показань своєю логікою фактів та розраховані на емоційну дію, зазвичай тісно переплітаються між собою та рідко застосовують ізольовано один від одного.

За безконфліктної ситуації вислуховування вільної розповіді займає центральне місце в тактичному плані допиту.

При цьому необхідно дотримуватися наступних «правил» (надається авторське бачення сформованих «правил»):

– жодне з повідомлень підозрюваного не повинно бути залишено без перевірки, а для цього необхідно з'ясувати у нього все необхідне для встановлення доказів, які підтверджують чи спростовують отримані показання;

– щоб покази були надані підозрюваним у повній мірі його обізнаності про хід подій, слідчий (детектив) повинен вміло направити його розповідь, обравши при цьому хронологічну, логічну чи тактичну послідовність.

При хронологічній послідовності події з'ясовуються у тому порядку, як вони відбувалися. Логічна послідовність сприяє пожвавленню спогадів, тому що важливі для справи обставини з'ясовуються від причин до наслідків, які неминуче випливають з них. При так-

тичній послідовності спочатку з'ясовуються ті обставини, про які допитуваний розповідає найохочіше;

– якщо з'ясовується складна подія, тему вільної розповіді доцільно ділити на деякі епізоди. З'ясувавши все, що пов'язане з одним із епізодів чи фактів, слідчий (детектив) переходить до наступного. Такий прийом забезпечує повноту вільної розповіді, допомагаючи допитуваному переходити до викладу нових обставин лише після досконалого висвітлення попередніх епізодів чи фактів;

– якщо підозрюваний забув про факти, які цікавлять слідство, можна вдатися до прийомів, спрямованих на пожвавлення асоціативних зв'язків, які зазвичай рекомендуються для допиту свідків, зокрема вагомі результати досягаються допитом на місці, де відбувалися події, що цікавлять слідство.

При постановці питань слідчий (детектив) повинен стежити, щоб їх формулювання не містило інформації, що буде підказувати певну відповідь. Питання повинні перебувати між собою у логічній залежності щодо кожної з обставин, які з'ясовуються, та випливати одне з одного.

Вказане також формує і є основою попереджувальної роботи слідчого (детектива) у запобіганні кримінальним правопорушенням. Оскільки під час розслідування кримінальних проваджень, має свої особливості, які пов'язані, у першу чергу із поширеністю випадків застосування до винних осіб заходів виховного характеру натомість кримінального покарання та з формами й змістом самих заходів і проведених слідчих (розшукових) дій правоохоронцем [10].

Висновки. При проведенні вказаного наукового дослідження нами розглянуто тактико-криміналістичні прийоми допиту як правової складової отримання достовірних показань учасників процесу, досліджено сучасні процесуальні правила та тактичні прийоми допиту, вимоги законодавця України до вказаної слідчої (розшукової) дії, сформовано та надано на обговорення загалу (науковців, теоретиків та практиків кримінального процесу) власні авторські рекомендації щодо прийомів та методів отримання доказової бази у кримінальному провадженні, окреслено правові грані щодо законності їх використання.

Зважаючи на наявність недоліків у цій сфері кримінально-процесуальної та криміналістичної діяльності вважаємо за актуальні подальші дослідження відповідної спрямованості, адже останні створюватимуть перспективи теоретичних та практичних напрацювань та сприятимуть розв'язанню проблемних питань на цьому напрямку.

Література:

1. Кримінальний процесуальний кодекс України. *Відомості Верховної Ради України (ВВР).* 2013. № 9–10, № 11–12, № 13, ст. 88. (редакція станом на 24.08.2023). URL: http://zakon.rada.gov.ua (дата звернення: 23.10.2023).

2. Кримінальний кодекс України. *Відомості Верховної Ради України (ВВР).* 2001. № 25–26, ст. 131. (редакція станом на 05.10.2023). URL: http://zakon.rada.gov.ua (дата звернення: 23.10.2023).

3. Конституція України. *Відомості Верховної Ради України (ВВР).* 1996. № 30, ст. 141 (редакція станом на 01.01.2020). URL: http://zakon.rada.gov.ua (дата звернення: 23.10.2023).

4. Договір про заснування Європейської Спільноти (редакція станом на 01.01.2005). Конституційні акти Європейського Союзу. Частина I / Упорядник Г. Друзенко ; за загальною редакцією Т. Качки. К. : Видавництво "Юстініан", 2005 р. 512 с. URL: http://zakon.rada.gov.ua (дата звернення: 23.10.2023).

5. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: http://zakon.rada.gov.ua (дата звернення: 23.10.2023).

6. Копанчук В. О., Осмолян В. А., Кравчук О. В. «Рефлексія» як запорука результативності слідчо-криміналістичної тактики у реалізації завдань кримінального провадження / В. А. Осмолян. *Наше право* / *Our. Law*. 2023. № 1. С. 58–65.

7. Вакулик О. О. Тактика допиту. *Криміналістика* : мультимедійний навчальний підручник. Національна академія внутрішніх справ. Київ. URL: https://arm.naiau.kiev.ua. (дата звернення: 23.10.2023).

8. Осмолян В. А. Участь лікаря при допиті неповнолітньої особи як обов'язкова правова норма у законодавстві / В. А. Осмолян. *Медичні новини Грузії (Georgian Medical News).* Тбілісі – New York. № 4(313). Квітень 2021. ISSN 1512-0112. С. 186–192.

9. Осмолян В. А. Перспективи розвитку криміналістики в світлі нових кримінальних загроз, зокрема кіберзлочинності / В. А. Осмолян. *Науково-практичний журнал з проблем конституційного, цивільного, кримінального, екологічного та інших галузей права «Право. UA* / *Law.UA»*. 2020. № 2. С. 95–102.

10. Кравчук О. В., Осмолян В. А. Запобігання кримінальним правопорушенням неповнолітніх як невід'ємна складова попереджувальної роботи правоохоронця / В. А. Осмолян. *Актуальні проблеми юридичної науки. Політико-правові передумови європейської та євроатлантичної інтеграції України* : збірник тез міжнародної науково-практичної конференції «Двадцять другі осінні юридичні читання» (м. Хмельницький, 13 жовтня 2023 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2023. С. 249–250.

References:

1. Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine]. *Bulletin of the Verkhovna Rada of Ukraine (VVR),* 2013, No. 9–10, No. 11–12, No. 13, Article 88. (edited as of August 24, 2023). Retrieved from http://zakon.rada.gov.ua (date of application: 10/23/2023). [in Ukrainian].
2. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]. *Information of the Verkhovna Rada of Ukraine (VVR),* 2001, No. 25–26, Article 131. (edited as of 05.10.2023). Retrieved from http://zakon.rada.gov.ua (date of application: 10/23/2023). [in Ukrainian].
3. Konstytutsiia Ukrainy [Constitution of Ukraine]. Bulletin of the Verkhovna Rada of Ukraine (VVR), 1996, No. 30, Article 141) (edited as of January 1, 2020). Retrieved from http://zakon.rada.gov.ua (date of application: 10/23/2023). [in Ukrainian].
4. Dohovir pro zasnuvannia Yevropeiskoi Spilnoty (redaktsiia stanom na 01.01.2005) [Treaty on the establishment of the European Community (edition as of 01.01.2005)]. Constitutional acts of the European Union. Part I / Compiled by G. Druzenko, edited by T. Kachka. K. : "Justinian" Publishing House, 2005. 512 p. Retrieved from http://zakon.rada.gov.ua (date of application: 10/23/2023). [in Ukrainian].
5. Zahalna deklaratsiia prav liudyny [Universal Declaration of Human Rights]. Adopted and proclaimed by resolution 217 A (III) of the UN General Assembly of December 10, 1948. Retrieved from http://zakon.rada.gov.ua (date of application: 10/23/2023). [in Ukrainian].
6. Kopanchuk V. O., Osmolian V. A., Kravchuk O. V. «Refleksiia» yak zaporuka rezultatyvnosti slidchokryminalistychnoi taktyky u realizatsii zavdan kryminalnoho provadzhennia [«Reflection» as a key to the effectiveness of investigative and forensic tactics in the implementation of the tasks of criminal proceedings] / V. A. Osmolian. *Our.Law.* No. 1, 2023. P. 58–65. [in Ukrainian].
7. Vakulyk O.O. Taktyka dopytu. *Kryminalistyka* [Interrogation tactics. *Criminal studies*]. Multimedia textbook. National Academy of Internal Affairs. Kyiv. Retrieved from https://arm.naiau.kiev.ua. (date of application: 10/23/2023). [in Ukrainian].
8. V. A. Osmolian. Uchast likaria pry dopyti nepovnolitnoi osoby yak obov'iazkova pravova norma u zakonodavstvi [Participation of a doctor in the interrogation of a minor as a mandatory legal norm in the legislation] / V. A. Osmolian. *Georgian Medical News.* Tbilisi – New York. No. 4(313). April 2021. ISSN 1512–0112. P. 186–192. [in Ukrainian].
9. V. A. Osmolian. Perspektyvy rozvytku kryminalistyky v svitli novykh kryminalnykh zahroz, zokrema kiberzlochynnosti [Prospects for the development of criminology in the light of new criminal threats, including cybercrime] / V. A. Osmolian. *Scientific and practical journal on the problems of constitutional, civil, criminal, environmental and other fields of law "Law. UA / Law.UA"*. 2020. No. 2. P. 95–102. [in Ukrainian].
10. Kravchuk O. V., Osmolian V. A. Zapobihannia kryminalnym pravoporushenniam nepovnolitnikh yak nevid'iemna skladova poperedzhuvalnoi roboty pravookhorontsia [Prevention of criminal offenses by minors as an integral component of the law enforcement officer's preventive work] / V. A. Osmolian. *Current problems of legal science. Political and legal prerequisites of the European and Euro-Atlantic integration of Ukraine* : collection of theses of the international scientific and practical conference "twenty-second autumn legal readings" (Khmelnitsky, October 13, 2023). Khmelnitsky: Leonid Yuzkov Khmelnitsky University of Management and Law, 2023. P. 249–250. [in Ukrainian].

УДК 343.1
DOI https://doi.org/10.32689/2522-4603.2023.3.3

Іван СЕРВЕЦЬКИЙ
доктор юридичних наук, доцент, заступник завідувача кафедри правоохоронної на антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом,, вул. Фрометівська, 2, м. Київ, Україна, 03039, siv2055@gmail.com
ORCID: 0000-0002-5713-8911

Олег ДЕМ'ЯНЕНКО
аспірант кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом, вул. Фрометівська, 2, м. Київ, Україна, 03039
ORCID: 0009-0007-8318-5854

Ivan SERVETSKYI
Doctor of Law, Associate Professor, Deputy Head of the Law Enforcement and Anti-Corruption Department of the Educational and Scientific Institute of Law named after Prince Vladimir the Great, Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039, siv2055@gmail.com
ORCID: 0000-0002-5713-8911

Oleg DEMYANENKO
Postgraduate student of the Law Enforcement and Anti-Corruption Department of the Educational and Scientific Institute of Law named after Prince Vladimir the Great, Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039
ORCID: 0009-0007-8318-5854

ДЕЯКІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРШПИГУНСТВУ

SOME PROBLEMS OF COUNTERING CYBER ESPIONAGE

Стаття присвячена викриттю шпигунів «кібершпигунів», державних зрадників, виявленню колаборантів, встановленню осіб, які виправдовують, заперечують або визнають правомірною збройну агресію, глорифікації її учасників та притягненню до кримінальної відповідальності.

Статистичні дані свідчать про те, що за 2023 рік зареєстровано 57.093 злочинів проти національної безпеки, серед них – 37 за шпигунство, 712 державну зраду, 2.364 – колаборацію, 1007 за виправдовування військової агресію РФ проти України. З одного боку, це свідчить про успішну діяльність правоохоронних органів та спеціальних служб України, а з іншого це свідчить про те, що існує агентурна мережа, яка сприяє шпигунській діяльності, особливо у. кіберпросторі. України.

Тому, відносно таких осіб спецслужби здійснюють контррозвідувальні та оперативно-розшукові заходи, спрямовані, в першу чергу, на боротьбу з «кібершпигунством», негласно протидіє «кіберзлочинності», попереджає «кібератаки» щодо державних електронних інформаційних ресурсів, інформаційної інфраструктури; забезпечує реагування на всі інциденти у сфері державної безпеки.

На думку Манжая О. В. «…кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами».

Отже, спецслужби повинні забезпечити гласний і негласний захист громадян, здійснювати контррозвідувальні заходи у кіберпросторі застосовуючи форми і методи протидії кібершпигунству у кіберпросторі.

Саме визначення ролі та місця контррозвідувальної діяльності у кіберпросторі і є предметом нашого дослідження.

Діордіца І. В зазначає, що «…розвиток і вдосконалення заходів кримінально-правової охорони державної таємниці (секретної інформації) передбачає ґрунтовне дослідження та вдосконалення диспозиції відповідних норм Кримінального кодексу України, зокрема й шпигунства, та введення в нього такої нової правової категорії, як «кібершпигунство». При цьому, важливими аспектами є врахування сучасних суспільно-політичних змін у законодавчому регулюванні обігу секретної інформації, максимальна конкретизація та уніфікація понятійно-категорійного апарату, що застосовується в диспозиції норми, а також дотримання усталених принципів законодавчої техніки та використання наявної зарубіжної практики, норм і доктрин».

Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність». Якщо розглядати «кіберпростір» як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір

© Сервецький І., Дем'яненко О., 2023

(територія), який створений, працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки секретної інформації).

Проблемами дослідження "кібершпигунства", "кібернетична безпека", "кіберпростір", "кіберсфера", "кіберзлочинність", "кібервійна",. "кібероборона", займаються такі науковці як І.В. Арістова, І. В. Діордіца В.А., Ліпкана, О.В. Манжай, Д.С. Мінін, І.В. Сопілко, М.М. Чеховська, В.С. Цимбалюк, В.М. Шлапаченко .

Метою статті є здійснення етимологічного аналізу поняття «кібершпигунство».

На підставі цього запропоновані конкретні шляхи удосконалення протидії «кібершпигунству» з використанням сучасних форм і методів контррозвідувальної діяльності Службою безпеки України.

Ключові слова: *шпигунство, «кібершпигунство», «кібербезпека», «кіберпростір», контррозвідувальні заходи.*

The article is dedicated to exposing "cyberspies" spies, state traitors, identifying collaborators, establishing persons who justify, deny or recognize the legitimate armed aggression, glorify its participants and bring them to criminal responsibility.

Statistics show that in 2023, 57,093 crimes against national security were registered, including 37 for espionage, 712 for treason, 2,364 for collaboration, and 1,007 for justifying the military aggression of the Russian Federation against Ukraine. On the one hand, this indicates the successful activity of law enforcement agencies and special services of Ukraine, and on the other hand, it indicates that there is an agent network that facilitates espionage activities, especially in cyberspace of Ukraine.

Therefore, in relation to such persons, the special services carry out counter-intelligence and operative investigative measures aimed, first of all, at combating "cyber-espionage", covertly countering "cyber-crime", warning of "cyber-attacks" against state electronic information resources, information infrastructure; provides response to all incidents in the sphere of state security.

According to Manzhai O. V. "...cyberspace is an information environment (space) that arises (exists) with the help of technical (computer) systems during the interaction of people with each other, the interaction of technical (computer) systems and the management of these people technical (computer) systems".

Therefore, the special services must provide public and private protection of citizens, carry out counterintelligence measures in cyberspace using forms and methods of countering cyberespionage in cyberspace.

Defining the role and place of counterintelligence activities in cyberspace is the subject of our research.

Diorditsa I. V notes that "... the development and improvement of measures of criminal law protection of state secrets (secret information) involves a thorough study and improvement of the disposition of the relevant norms of the Criminal Code of Ukraine, in particular espionage, and the introduction of such a new legal category into it as " cyberespionage". At the same time, important aspects are the consideration of modern social and political changes in the legislative regulation of the circulation of secret information, the maximum specification and unification of the conceptual and categorical apparatus used in the disposition of the norm, as well as the observance of established principles of legislative technique and the use of existing foreign practice, norms and doctrines ".

The term "cyberspace" has become synonymous with the concept of "computer virtual reality." If we consider "cyberspace" as an abbreviation of the phrase "cybernetic space", then cyberspace is a space (territory) that is created and works on the basis of the principles and methods of cybernetics (the science of the general laws of receiving, storing, transmitting and processing secret information).

Research problems of "cyberespionage", "cybernetic security", "cyberspace", "cybersphere", "cybercrime", "cyberwar". "cyber defense", such scientists as I.V. Aristova, I.V. Diorditsa V.A., Lipkana, Manzhai O.V., D.S. Minin, I.V. Sopilko, M.M. Chekhovska, V.S. Tsymbalyuk, V.M. Shlapachenko.

The purpose of the article is to carry out an etymological analysis of the concept of "cyber espionage".

On the basis of this, specific ways of improving counteraction to "cyber espionage" using modern forms and methods of counterintelligence activities by the Security Service of Ukraine are proposed.

Key words: *espionage, "cyber espionage", "cyber security", "cyber space", counterintelligence measures.*

Постановка проблеми. Проведення розвідувальних операцій спецслужбами російської федерації проти України під час військових дій тісно пов'язані з використанням шпигунів та державних зрадників. За таких обставин головними завданнями правоохоронних органів та спеціальних служб є активна протидія військовій агресії російської федерації з викриття державних зрадників, шпигунів, виявлення колаборантів, встановлення осіб, які виправдовують, заперечують або визнають правомірною збройну агресію, глорифікація її учасників та притягнення до кримінальної відповідальності [1].

Станом на 1 січня 2024 року правоохоронними органами та спеціальними службами за 2023 рік зареєстровано 57.093 злочинів проти національної безпеки, серед них – 37 за шпигунство, 712 державну зраду, 2.364 – колаборацію, 1007 за виправдовування військової агресію РФ проти України [2].

Ці статистичні дані, з одного боку, свідчать про успішну діяльність правоохоронних органів та спеціальних служб України з викриття осіб, які вчиняють злочини проти основ національної безпеки, а з іншої, це свідчить про те, що серед громадян України створена агентурна мережа за допомогою якої спецслужби російської федерації намагаються підірвати основи нашої незалежності.

Для цього вони активно проводять шпигунські операції у кіберпросторі, застосовуючи при цьому новітні технології та найвищі досягнення людства у космічній галузях науки та техніки.

Тому, СБУ повинна здійснювати активні контррозвідувальні заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі [3].

Здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібершпигунством, негласно протидіє кіберзлочинності, розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформаційної інфраструктури; забезпечує реагування на всі інциденти у сфері державної безпеки [4].

Саме «кібершпигунство» передбачає використання в процесі шпигунської діяльності віртуального простору – кіберпростору.

На думку Манжай О.В. «…кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [5 , с. 216]. Тобто – це простір де громадяни України використовують комп'ютерні технології та для задоволення власних та державних потреб.

Відповідно спецслужби повинні забезпечити гласний і негласний захист громадян, здійснювати контррозвідувальні заходи у кіберпросторі застосовуючи форми і методи протидії кібершпигунству у кіберпросторі. Саме визначення ролі та місця контррозвідувальної діяльності у кіберпросторі і є предметом нашого дослідження.

Вперше термін «кіберпростір» було використано у вжиток письменником В. Гібсоном у 1982 р. у новелі «Спалення Хром» («Burning Chrome»). У 1984 р. це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). На думку В. Гібсона, кіберпростір (cyberspace) – це створена галюцинація, під дією якої щодня перебувають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів усього людства, потоки даних у просторі розуму; скупчення та сузір'я інформації [6, с. 32].

На думку І.В. Діордіца «…розвиток і вдосконалення заходів кримінально-правової охорони державної таємниці (секретної інформації) передбачає ґрунтовне дослідження та вдосконалення диспозиції відповідних норм Кримінального кодексу України, зокрема й шпигунства, та введення в нього такої нової правової категорії, як «кібершпигунство». При цьому важливими аспектами є такі: врахування сучасних суспільно-політичних змін у законодавчому регулюванні обігу секретної інформації, максимальна конкретизація та уніфікація понятійно-категорійного апарату, що застосовується в диспозиції норми, а також дотримання усталених принципів законодавчої техніки та використання наявної зарубіжної практики, норм і доктрин» [7].

Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність». Для того щоб з'ясувати значення слова «кіберпростір» у сучасному його контексті, необхідно дослідити його етимологію. Як бачимо, термін «кіберпростір» є сполученням двох слів – «кібер» та «простір». Слово «кібер» походить від грецького κυβερ та означає *над*. Згідно з одним із визначень великого тлумачного словника сучасної української мови [8, с. 1170] під простором розуміють вільний великий обшир; просторінь; територію.

Таким чином, якщо розглядати кіберпростір як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений, працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки секретної інформації) [8, с. 539].

Аналіз останніх досліджень та публікацій. Проблемами дослідження «кібершпигунства», «кібернетична безпека», «кіберпростір», «кіберсфера», «кіберзлочинність», «кібервійна», «кібероборона», займаються такі науковці як І.В. Аріστова [20–21], І.В. Діордіца, В.А., Ліпкана [1–5], О. В. Манжай, Д.С. Мінін [6], І.В. Сопілко [26], М.М. Чеховська [7], В.С. Цимбалюк [22–25], В.М. Шлапаченко [8].

Мета статті (постановка завдань) – здійснити етимологічний аналіз понять «кібершпигунство». його основні складові, які становлять основу категорійного ряду дослідження, а саме: «кібернетична безпека», «кіберпростір», інформаційний, загроза, кібернетичний і безпека, яке здійснюється з використанням обходу (злому) систем комп'ютерної безпеки, із застосуванням програмного забезпечення, включно з шпигунськими програмами, а потім шляхом їх поєднання визначити його небезпеку під час воєнних дій.

Основні завдання дослідження направлені на з'ясування науково-теоретичних проблем, а саме:

1) дослідити поняття «кібершпигунства», а також точки зору вчених щодо його суспільної небезпеки в сучасних умовах військової агресії проти України.

2) визначити кіберпростір, в якому здійснюються шпигунська діяльність та проаналізувати юрисдикційну складову «кібершпигунства» та підставі кримінальної юрисдикції.

3) надати авторські пропозиції у підвищенні ефективної діяльності СБУ у здійсненні контрозвідувальних заходів з протидії «кібершпигунству».

Виклад основного матеріалу дослідження. Сьогодні в Україні особливої гостроти набуває проблема протидія «кібершпигунству» як необхідної складової забезпечення національної безпеки, територіальної цілісності та існування незалежності держави.

За останні десятиліття інформаційні технології міцно увійшли у повсякденне життя кожної людини. При цьому слід зазначити, що активний розвиток інформаційних технологій пов'язаний не з розробкою новітніх технологій, зі створенням найбільш удосконаленого, універсального програмного забезпечення. Ці технології успішно використовують шпигуни у своїй протиправній шпигунській діяльності [9].

Досліджуючи поняття та зміст кібершпигунства, перш за все зазначу, що до цієї категорії входять два окремі поняття: шпіон «шпигун», шпіонаж, шпіонство, шпіонити; – р. болг. шпибн, бр. шпіен, п. (рідк.) szpion, ч. (розм.) spion, слц. spion, вл. spion, м. иіпион, схв. шпщун, слн. spijon; – запозичення з німецької мови; н. Spion п «шпіон, шпигун за посередництвом французької «і та іспанської (фр. espion. icп. spionе «тс.») запозичене з італійської; іт. spionе «шпигун» утворене від spїaге «шпіонити, вистежу вати, підстерігати», джерелом якого є германські мови (пор. пгер. speph-де «уважно, гостро дивитися» і генетично, пов'язані з ним двн. spehoп, spiohопте.«стежити, вистежувати [10, с. 404] та терміни – «кібер» («кібернетичне») [11, с. 168], утворюючи сучасне слово «кібершпигунство»

Отже, для здійснення ґрунтовного дослідження вищезазначеної категорії, проаналізуємо окремо. В словнику української мови *«шпигунство»* – це злочинна діяльність, яка полягає в таємному збиранні відомостей або викраданні матеріалів, вистежування, розшук матеріалів, що становлять державну таємницю з метою передачі їх іншій державі [8, с. 1404]. Відповідно «кібернетичний» стосується кібернетики; який створено, працює на основі принципів, методів кібернетики [11, с. 168].

«Кібершпигунство», або комп'ютерний шпіонаж (вживається також термін «*кіберрозвідка*») – термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюване з використанням обходу (злому) систем комп'ютерної безпеки, зі застосуванням шкідливого програмного забезпечення, включно з «троянськими конями» і шпигунськими програмами. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами.

Отже, під кібершпигунством Діордіца І.В. слід розуміти злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, інформації, якщо ці дії вчинені іноземцем або особою без громадянства із використанням кібернетичного простору [13].

У Кримінальному кодексі України «шпигунство» визначено як – передача або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства (ст. 114 КК України) [1]. *Безпосереднім об'єктом шпигунства* (кібершпигунства – *Д. І.*) є к*ібернетична загроза* зовнішній безпеці України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека.

Кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [4].

Предметом цього злочину є відомості, що містять державну таємницю, вичерпний перелік яких міститься в Законі України «Про державну таємницю» від 21 січня 1994 р. Згідно з цим Законом *державна таємниця* (також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України, та які визнані в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [13].

Ці відомості мають гриф секретності і входять до компетенції у сфері забезпечення охорони державної таємниці є Служба безпеки України [3].

Для того, щоб з'ясувати питання компетенції в кіберпросторі, перш за все, необхідно визначити зміст поняття «юрисдикція». Юрисдикція (лат. jurisdictio – судочинство, від jus (juris) – право і dicere – говорити, проголошувати) – це повноваження давати правову оцінку фактам, розв'язувати правові питання [14, с. 1644]. У юридичній енциклопедії

зазначено, що юрисдикція (в тому значенні, що нас цікавить) поділяється на *юрисдикцію держави* та *юридикцію міжнародну*.

Юрисдикція держави поділяється на *територіальну* та *особисту* (національну). Юрисдикція територіальна зумовлюється суверенністю влади держави в межах її території, де вона має абсолютну юрисдикцію, за винятком випадків, коли відповідними міжнародними угодами не передбачається інше. Особиста (національна) юрисдикція держави поширюється на своїх громадян, які перебува- ють за межами її території (наприклад, у відкритому морі, океані, в космічному просторі). В окремих випадках, передбачених національним законодавством, юрисдикція держави поширюється на громадян цієї держави, які перебувають на території іншої держави, однак здійснюватися така юрисдикція може лише на території своєї держави, якщо інше не передбачено міжнародними угодами. Юрисдикція міжнародна – це підсудність певної категорії справ міжнародним органам. Даний вид юрисдикції, на відміну від юрисдикції держави, є певним обмеженням державного суверенітету. Цей фактор зумовлює те, що для визнання юрисдикції будь-якого міжнародного органу необхідна явно виражена згода відповідної держави [14, с. 490]. Одним з основних завдань для визначення юрисдикції у сфері кіберпростору є встановлення факту поширення внутрішньодержавних правових норм на відносини в цьому середовищі.

У ст. 2 Конституції України [15] вказується, що суверенітет України поширюється на всю її територію. Згідно зі ст. 8 Конституції України вона має найвищу юридичну силу. Таким чином, законодавчо стверджується влада України над своєю територією.

На цей момент під територією держави розуміють не лише певну ділянку землі область (сухопутна територія), але й води (внутрішні та територіальні води), повітряний простір, розташований над сушею і водами (тропосфера, стратосфера, іоносфера, а також значна частина простору). Надра, що знаходяться під сухопутною і водною територією, є приналежністю даної держави до технічно доступної глибини [16, с. 509]. Свого часу Г. Кельзен указував на те, що територія – не річ, зокрема, не земля або її частина. Це образний вираз, що позначає певне якісне право, територіальну сферу, національного юридичного порядку [17, с. 226]. Виходячи з наведених тверджень та самого визначення терміна «кіберпростір», його можна умовно розглядати як специфічний вид території, що не має геологічної основи, з усіма відповідними правовими наслідками.

Отже, на думку Монжая О.В. кіберпростір у широкому сенсі можна співвіднести з поняттям «територія», тож необхідно з'ясувати її вид: міжнародна, державна або зі змішаним статусом. Крім того необхідно проаналізувати правові концепції, що можуть застосовуватися до кіберпростору. Слід зазначити, що досить часто кіберпростір асоціюють зі поняттям «Інтернет». Однак це велике узагальнення, яке не враховує окремі випадки [5, с. 226].

Так, Манжая О.В. кіберпростір характеризує за трьома основними ознаками

– це інформаційний простір;

– комунікативним середовищем;

– він утворюється за допомогою технічних систем [5, с. 216].

У першому та другому випадках на кіберпростір безумовно має поширюватися відповідна територіальна юрисдикція. Щодо третього випадку, то багато юристів схиляється до думки про необхідність оголошення кіберпростору, який має транскордонні масштаби (Інтернет), міжнародною територією на кшталт Антарктиди або космічного простору.

Найбільш обґрунтовану позицію щодо цього питання було викладено в роботі Д. Менте «Юрисдикція в кіберпросторі: теорія міжнародних просторів» [18] у якій він зазначає, що суттєвий поштовх у розвитку інформаційних технологій дала популяризація та активне використання у різних процесах глобальної інформаційно-телекомунікаційної мережі Інтернет. У ній Д. Менте пропонує вважати Інтернет територією, на яку не поширюється суверенітет окремої держави. Як аналогію автор наводить відносини в Антарктиді, космосі та нейтральних водах. У той же час у деяких державах спостерігалися спроби встановити власну компетенцію над частиною Інтернету або поширити особисту юрисдикцію на окремі сфери діяльності в цьому середовищі**.**

Отже Манжай В.О. пропонує три шляхи вирішення питання щодо правового режиму Інтернету і відповідно визначення компетенції держави в цій сфері:

1) Інтернет є міжнародним простором, і його правовий режим має визначатися нормами міжнародного права;

2) Інтернет є територією зі змішаним правовим режимом на кшталт континентального шельфу прибережних держав;

3) в окремих випадках інтернет можна віднести до державної території [5].

Становлення інформаційних технологій в Україні та удосконалення комп'ютерної техніки, використання телекомунікаційних мереж майже в усіх сферах життєдіяльності людини полегшило можливість передання інформації

в системі Інтернет створили низку проблем. У період глобалізації швидкий розвиток інформаційних технологій та комп'ютерних систем супроводжується зловживаннями цими технологіями, що призводить до вчинення злочинів з використанням комп'ютерної техніки створюючи при цьому сприятливі умови для реалізації нових схем і методів злочинної діяльності. Рівень можливостей, які отримують зловмисники, тенденція до збільшення кількості вчинення злочинів у сфері комп'ютерних інформаційних технологій, становлять загрозу не лише демократичним перетворенням і розвитку інформаційного суспільства в Україні, а й безпосередньо національній безпеці.

На думку Н.А. Чеснокова «… Інтернет охоплює всі країни світу, оскільки із застосуванням нових технологій (використання мобільних супутникових пристроїв зв'язку) можливе підключення до мережі Інтернет із будь-якої точки земної кулі. Якщо вести розмову про розгорнуту інфраструктуру, то в такому контексті Інтернет охоплює сьогодні понад 150 країн світу» [19]. пов'язаних зі створенням безпечних умов використання віртуального простору. Так, відповідно до офіційної статистики Офісу Генерального прокурора України за 2023 рік, проти «кіберзлочинів» зареєстровано – 3415, а саме: «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», ст. 361 КК України – 1 403, «створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-1 КК України – 280, «несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 361-2 КК України – 60, «несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 362 КК України – 1 664, «порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 363 КК України – 3, «перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку», ст. 363-1 КК України – 5 [2].

Наведені статистичні дані кіберзлочинності свідчить, що удосконалилися й інструменти для шпигунства з використанням як спеціалізованих пристроїв, так і з використанням програмного забезпечення. На відміну від класичних методів розвідки та шпигунства нові технології внесли до них суттєві коригування. Нині часом неможливо встановити, хто саме розробив те чи інше програмне забезпечення для проведення розвідувальних чи шпигунських дій у сфері високих технологій. Розробниками такого спеціалізованого програмного забезпечення є як приватні особи, так і організації різної організаційно-правової форми з різними джерелами фінансування (у тому числі за державні кошти). Як заявила директор з розвідки компанії з кібербезпеки бізнесу Red Canary, старший науковий співробітник програми Cyber Statecraft Initiative Атлантичної ради Кеті Нікелс «кібершпигунство» – це те, що є ніби очікуваним від російських розвідувальних служб, фінансованих державою-супротивником. Вони прагнуть отримати інформацію про уряд або пов'язані з урядом об'єкти. Це потребує зовсім іншої політичної відповіді, ніж та, коли йдеться про російських кіберзлочинців, які стоять за більшістю атак вимагачів». За її словами, шпигунство здійснюють державні структури російської федерації, повністю підконтрольні уряду, тоді як оператори програм-викупів «можливо, не контролюються безпосередньо російським урядом» [20]. Крім того, урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA на виконання Закону України "Про основні засади забезпечення кібербезпеки України" [4], з'ясовано, що однією з найбільших «кіберзагроз» є UAC-0010 (Armageddon), діяльність якої здійснюється колишніми "офіцерами" ГУ СБУ в АР Крим, які у 2014 році зрадили військовій присязі і почали прислужувати ФСБ російської федерації [21]. Основним завданням цього угрупування є «кібершпигунство» у відносно сил безпеки та оборони України. При цьому, відомо, щонайменше, про один випадок здійснення деструктивної діяльності на об'єкті інформаційної інфраструктури. За наявною інформацією кількість одночасно інфікованих комп'ютерів, переважно функціонуючих в межах інформаційно-комунікаційних систем державних органів, може сягати кількох тисяч [22].

У 2022 році команда CERT-UA загалом обробила 2194 випадки ворожих атак, з яких

1148 інцидентів мали критичний або високий рівень небезпеки. Найбільш атакованим сектором з боку ворожого кібершпигунства та агресивних операцій, за даними Держспецзв'язку, залишається цивільна інфраструктура України, зокрема державні установи та об'єкти критичної інфраструктури (енергетичні та логістичні компанії, комерційні організації, Міністерство енергетики, Міністерство фінансів, Міністерство закордонних справ тощо). Мішенню також є оборонні організації – Міністерство оборони, Державна прикордонна служба тощо. Особливу небезпеку становлять повільні та "тихі" атаки, спрямовані на шпигунство. Зокрема, такі атаки здійснює угрупування InvisiMole (Служба зовнішньої розвідки російської федерації). Їхньою основною мішенню є високопосадовці, дипломати та інші фахівці, які мають доступ до найбільш чутливої інформації. Оскільки такі "тихі" атаки складніше виявити, вони можуть мати більш критичні наслідки [22]. Як зазначає А.Ю. Нашинець-Наумова, іноді особи, які розробили шкідливе програмне забезпечення або спеціальне обладнання, не є тими хто його використовує у своїй шпигунській діяльності, що часто призводить до неможливості встановити особу, яка здійснює злочину діяльність з метою її притягнення до відповідальності [23]. Крім того, Сполучені Штати та країни всього світу покладають на Китайську Народну Республіку відповідальність за підривну і дестабілізуючу поведінку в кіберпросторі, яка становить серйозну загрозу їх економічній і національній безпеці. У заяві пресслужби Білого дому, зокрема, наголошується, що Міністерство державної безпеки (МДБ) КНР сприяло створенню системи злочинних хакерів-контрактників, які здійснюють спонсоровані державою кіберзлочини. Офіційно підтверджено, що хакери МДБ Китаю використовували вразливість Microsoft Exchange Server для масштабної операції з кібершпигування, внаслідок якої були зламані тисячі комп'ютерів і мереж, ідеться в повідомленні. Як свідчить обвинувальний висновок щодо трьох співробітників МДБ і одного з їхніх хакерів-контрактників, Сполучені Штати накладатимуть санкції на кіберзлочинців КНР за їхню безвідповідальну поведінку в кіберпросторі. Державний департамент США закликав усі держави, які прагнуть стабільності в кіберпросторі, приєднатися до цих зусиль [24].

Аналіз міжнародного досвіду з протидії кіберзлочинності та кібершахрайству виокремлює Конвенцію про кіберзлочинність (ратифікована Україною 1 липня 2004 р.) Вона представляється первинною міжнародною угодою у сфері протидії правопорушенням, вчиненим посередництвом комп'ютера. В рамках одинадцятого і дванадцятого Конгресів організації щодо запобігання злочинності та кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися проблеми інтернаціонального партнерства у війні з кіберзлочинністю. Члени Конгресів обговорювали заходи щодо інтенсифікації інтернаціонального партнерства і поліпшення державного законодавства у галузі боротьби з відмиванням коштів, торгівлі наркотиками, тероризмом та кіберзлочинністю. Тобто, ООН встановила комп'ютерні правопорушення в єдиний цикл з тероризмом, що вказує на спеціальний інтерес до даного питання зі сторони світової спільноти [25].

Висновок. Сьогодні в Україні особливої гостроти набуває проблема протидії «кібершпигунству» як необхідної складової забезпечення національної безпеки, територіальної цілісності та існування незалежності держави.

Отже, «кібершпигунство» або комп'ютерний шпіонаж – термін, який позначає несанкціоноване проникнення в інформаційні системи з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням (злому), вербування громадян України, що використовують кіберпростір та працюють з інформацією обмеженого користування, із застосуванням шпигунського програмного забезпечення.

Доведено, що сприятливим середовищем для шпигунської діяльності є кіберпростір, а це підтверджує наше дослідження, що «кібершпигунство» може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами ("кротами"), а також хакерами.

На думку вчених у цій сфері «кібершпигунством визначає» є злочином, який здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їх представникам, якщо ці дії вчинені іноземцем або особою без громадянства і з використанням методів кібернетики, що підпадає під ознаки стаття 114 Кримінального кодексу України, а громадяни України які їм сприяють у кіберпросторі несуть кримінальну відповідальність за ст.ст. 114 ч. 2, 111 ч. 2, 436 ч. 2, як такі, що вчинені при обтяжуючих обставинах.

Таким чином, це дозволить активно протидіяти «кібершпигунству», що дало б можливість успішно попереджати та викривати та притягувати їх до кримінальної відповідальності.

Література:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України (ВВР).* 2001. № 25–26, ст. 131.

2. Про роботу органів прокуратури · Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Про осіб, які вчинили кримінальні правопорушення. Статистика – Офіс Генерального прокурора. 2023. new.gp.gov.ua › posts › statistika

3. Закон України Про Службу безпеки України. Відомості Верховної Ради України від 7 липня 1992, № 27, Ст.382. Закон України «Про контррозвідувальну діяльність». *Відомості Верховної Ради України*, від 3 квітня 2003, № 12, Ст. 89.

4. Закон України "Про основні засади забезпечення кібербезпеки України" Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. URL: https://cert.gov.ua/article/5160737

5. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай. *Право і Безпека*. 2009. № 4. С. 215–219. URL: http://nbuv.gov.ua/UJRN/Pib_2009_4_50

6. Gibson W. Neuromancer / W. Gibson. London : HarperCollins, 1994. 271 p.

7. Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємство, господарство і право. Адміністративний процес.* 2017. № 4. С. 76–84.

8. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Г. Бусел]. К. ; Ірпінь : ВТФ «Перун», 2003. 1440 с.

9. Шлапаченко В. М. Шпигунство як діяльність зі здобування інформації. *Інформаційна безпека людини, суспільства, держави*. Київ, 2015. № 1(17). С. 99–109.

10. Етимологічний словник Української мови. Вид. «Наукова думка». 2012. Т. 7. С. 404.

11 Словник іншомовних слів. 23000 слів та термінологічних словосполучень / уклад. Л. О. Пустовіт та ін. К. : Довіра, 2000, 338 с.

12. Про державну таємницю : Закон України від 21 січня 1994 року № 3855-XII зі змінами. URL: http://zakon4.rada.gov.ua/laws/show/3855- 12/print1360009387090304

13. Діордіца І. В. Поняття та зміст кібершпигунства / І. В. Діордіца. URL: https://goal-int.org/ponya

14. Юридична енциклопедія : в 6 т. Т. 6 Т–Я / [редкол. Ю. С. Шемшученко (голова редкол.) та ін.]. К. : Укр. енцикл., 2004. 768 с.

15. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. С. 141.

16. Большая советская энциклопедия : в 30 т. Т. 25. Струнино – Тихорецк / [гл. ред. А. М. Прохоров]. Изд. 3-е. М. : Советская энциклопедия, 1976. 600 с.

17. Kelsen H. Principles of International Law / Hans Kelsen. New York : Rinehart & Company Inc., 1952. 461 p.

18. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces / D. Menthe. *Mich. Telecomm.* Tech. L. Rev. URL: http://www.mttlr.org/volfour/menthe.html

19. Чесноков Н.А. Правові основи інформаційної безпеки у сучасних умовах. *Правова ініціатива.* 2013. № 4.

20. Директор з розвідки компанії з кібербезпеки бізнесу Red Canary, старший науковий співробітник програми Cyber Statecraft Initiative Атлантичної ради Кеті Нікелс… «кібершпигунство – це те, що є ніби очікуваним від російських розвідувальних служб».

21. Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. URL: https://cert.gov.ua/article/5160737 ; URL: https://www.ukrinform.ua/rubric-world/3285329-kiberataki-rf-peresliduut-dvi-rizni-cili-spigunstvo-ta-vimaganna-grosej-ekspert.html

22. Кібервійна проти України: Держспецзв'язку дослідила мотивацію, методи та інструменти російських хакерів. URL: https://ms.detector.media/withoutsection/post/31351/2023-03-08-kiberviyna-proty-ukrainy-derzhspetszvyazku-doslidyla-motyvatsiyu-metody-ta-instrumenty-rosiyskykh-khakeriv/

23.Нашинець-Наумова А. Ю. Кібершпіонаж – загроза сучасному інформаційному суспільству. *Кібербезпека в Україні: правові та організаційні питання* : матеріали міжнар. наук.-практ. конф., (Одеса, 22 листоп. 2019 р.). Одеса : ОУВС, 2019. С. 11–13.

24. Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. URL: https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

25. Міжнародний досвід протидії кіберзлочинності та кібершахрайству URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/%D0%9A%

References:

1. Kryminalnyi kodeks Ukrainy vid 05.04.2001 № 2341-III [Criminal Code of Ukraine dated April 5, 2001 No. 2341-III. *Bulletin of the Verkhovna Rada of Ukraine (VVR)*], 2001, No. 25–26, Article 131. [in Ukrainian].

2. Pro robotu orhaniv prokuratury · Pro zareiestrovani kryminalni pravoporushennia ta rezultaty yikh dosudovoho rozsliduvannia · Pro osib, yaki vchynyly kryminalni pravoporushennia [About the work of prosecutor's offices. About registered criminal offenses and the results of their pre-trial investigation. About persons who have committed criminal offenses]. Statistics – Office of the Prosecutor General. (2023). new.gp.gov.ua › posts › statistics [in Ukrainian].

3. Zakon Ukrainy Pro Sluzhbu bezpeky Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy vid 7 lypnia 1992, № 27, St.382. Zakon Ukrainy «Pro kontrrozviduvalnu diialnist» [Law of Ukraine On the Security Service

of Ukraine. Information of the Verkhovna Rada of Ukraine of July 7, 1992, No. 27, Article 382. The Law of Ukraine "On counter-intelligence activities"]. *Bulletin of the Verkhovna Rada of Ukraine*, dated April 3, 2003, No. 12, Art. 89. [in Ukrainian].

4. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" Zvedena informatsiia shchodo diialnosti uhrupuvannia UAC-0010 stanom na lypen 2023 roku [Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" Summarized information on the activities of the UAC-0010 group as of July 2023]. Retrieved from https://cert.gov.ua/article/5160737 [in Ukrainian].

5. Manzhai O.V. Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [Use of cyberspace in operational and investigative activities] / O. V. Manzhai. *Law and Security*. 2009. No. 4. P. 215–219. Retrieved from http://nbuv.gov.ua/UJRN/Pib_2009_4_50 [in Ukrainian].

6. Gibson W. Neuromancer / W. Gibson. London : HarperCollins, 1994. 271 p.

7. Diorditsa I. V. Poniattia i zmist kiberzahroz na suchasnomu etapi [The concept and content of cyber threats at the modern stage]. *Enterprise, economy and law. Administrative process.* 2017. No. 4. P. 76–84. [in Ukrainian].

8. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy [A large explanatory dictionary of the modern Ukrainian language] / [comp. and heads ed.V.G. Bussel]. K. ; Irpin : VTF "Perun", 2003. 1440 p. [in Ukrainian].

9. Shlapachenko V. M. Shpyhunstvo yak diialnist zi zdobuvannia informatsii. [Espionage as an information gathering activity]. *Information security of a person, society, state*. Kyiv, 2015. No. 1(17). P. 99–109. [in Ukrainian].

10. Etymolohichnyi slovnyk Ukrainskoi movy [Etymological dictionary of the Ukrainian language]. Kind. Scientific thought. 2012, vol. 7. P. 404. [in Ukrainian].

11 Slovnyk inshomovnykh sliv [Dictionary of foreign words]. 23,000 words and terminological phrases / Compilation. L. O. Pustovit et al. K. : Dovira. 2000. 338 p. [in Ukrainian].

12. Pro derzhavnu taiemnytsiu : Zakon Ukrainy vid 21 sichnia 1994 roku № 3855-XII zi zminamy [On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII as amended] Retrieved from http://zakon4.rada.gov.ua/laws/show/3855-12/print1360009387090304 [in Ukrainian].

13. Diorditsa I. V. Poniattia ta zmist kibershpyhunstva [Concept and content of cyber espionage] / I. V. Diorditsa Retrieved from https://goal-int.org/ponya [in Ukrainian].

14. Yurydychna entsyklopediia [Legal encyclopedia]: in 6 vols. T. 6 T–Я / [ed. Yu. S. Shemshuchenko (head of editorial) and others]. K. : Ukr. encyclopedia, 2004. 768 p. [in Ukrainian].

15. Konstytutsiia Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy* [Constitution of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*]. (1996). No. 30. Art. 141. [in Ukrainian].

16. Bolshaya sovetskaya encyclopedia: in 30 vols. Vol. 25. Strunino – Tikhoretsk / [ch. ed. A. M. Prokhorov]. Ed. 3rd M. : Soviet encyclopedia, 1976. 600 p.

17. Kelsen H. Principles of International Law / Hans Kelsen. New York : Rinehart & Company Inc., 1952. 461 p.

18. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces / D. Menthe // Mich. Telecomm. Tech. L. Rev. Retrieved from http://www.mttlr.org/volfour/menthe.html

19. Chesnokov N.A. Legal foundations of information security in modern conditions. *Law initiative.* 2013. No. 4.

20. Dyrektor z rozvidky kompanii z kiberbezpeky biznesu Red Canary, starshyi naukovyi spivrobitnyk prohramy Cyber Statecraft Initiative Atlantychnoi rady Keti Nikels [Director of Intelligence at business cybersecurity firm Red Canary, senior fellow at the Atlantic Council's Cyber Statecraft Initiative, Kathy Nickels]... “cyber espionage is what is expected of Russian intelligence

21. Zvedena informatsiia shchodo diialnosti uhrupuvannia UAC-0010 stanom na lypen 2023 roku [Summary information on the activities of the UAC-0010 group as of July 2023]. Retrieved from https://cert.gov.ua/article/5160737. Retrieved from https://www.ukrinform.ua/rubric-world/3285329-kiberataki-rf-peresliduut-dvi-rizni-cili-spigunstvo-ta-vimaganna-grosej-ekspert.html [in Ukrainian].

22. Kiberviina proty Ukrainy: Derzhspetszviazku doslidyla motyvatsiiu, metody ta instrumenty rosiiskykh khakeriv [Cyber war against Ukraine: The State Intelligence Service investigated the motivation, methods and tools of Russian hackers]. Retrieved from https://ms.detector.media/withoutsection/post/31351/2023-03-08-kiberviyna-proty-ukrainy-derzhspetszvyazku-doslidyla-motyvatsiyu-metody-ta-instrumenty-rosiyskykh-khakeriv/ [in Ukrainian].

23. Nashinets-Naumova A. Yu. Kibershpionazh – zahroza suchasnomu informatsiinomu suspilstvu [Cyberespionage is a threat to the modern information society]. Cybersecurity in Ukraine: legal and organizational issues: materials of the International science and practice conference, (Odesa, November 22, 2019). Odesa : OUVS, 2019. P. 11–13. [in Ukrainian].

24. Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. Retrieved from https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

25. Mizhnarodnyi dosvid protydii kiberzlochynnosti ta kibershakhraistvu [International experience of combating cybercrime and cyberfraud] Retrieved from https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Free encyclopedia // Retrieved from https://uk.wikipedia.org/wiki/%D0%9A% [in Ukrainian].

УДК 342.6(045)
DOI https://doi.org/10.32689/2522-4603.2023.3.4

Марія АЛЕКСАНДРОВА
аспірантка Міжрегіональної Академії управління персоналом,
вул. Фрометівська, 2, м. Київ, Україна, 03039
ORCID: 0000-0003-3631-125X

Mariia ALEKSANDROVA
Postgraduate Student of the Interregional Academy of Personnel Management,
2 Frometivska str., Kyiv, Ukraine, 03039
ORCID: 0000-0003-3631-125X

ФОРМУВАННЯ ЦИФРОВОГО МАЙБУТНЬОГО ЄВРОПИ: АНАЛІЗ СТРАТЕГІЧНИХ ТА НОРМАТИВНИХ ДОКУМЕНТІВ, ДОСВІД ДЛЯ УКРАЇНИ

SHAPING EUROPE'S DIGITAL FUTURE: ANALYSIS OF STRATEGIC AND REGULATORY DOCUMENTS, EXPERIENCE FOR UKRAINE

Стаття присвячена аналізу стратегічних, програмних та законодавчих документів щодо розвитку цифрового майбутнього Європи, зокрема програма "Цифрове десятиліття ЄС", Європейська декларація "Про цифрові права та принципи", Закон "Про цифрові послуги", Закон "Про штучний інтелект", Закон "Про свободу медіа" тощо. А також проаналізовано можливості адаптації європейських норм та принципів в законодавство України.

Визначено, що цифрова трансформація держав – це головний пріоритет як країн Європейського Союзу, які всі свої ресурси зосереджують на розвиток цифрової трансформації, так і України, яка не є винятком, оскільки задекларувала курс на розвиток цифрової державу. Проаналізовано ініціативу «Цифрове десятиліття ЄС», яка визначає напрями розвитку цифрової трансформації ЄС до 2030 року, серед яких виділено таких чотири цілі цифрового десятиліття – підключення, цифрові навички, цифровий бізнес і цифрові державні послуги. Та аргументовано доречність впровадження визначених даною ініціативою напрямів цифрової трансформації для України в частині розвитку електронного урядування.

Проаналізовано результати Звіту щодо впровадження програми "Цифрове десятиліття" та з'ясовано, що успіх цифрової трансформації ЄС вимагатиме суттєве прискорення та поглиблення ЄС і дій державчленів щодо здійснення реформ, покращення бізнес середовища, забезпечення мотивації та збільшення інвестиції в цифрові технології, навчання цифровим навичкам та розбудовую інфраструктури.

Варто зауважити, що ЄС важливу роль зосереджує на міжнародному партнерстві в напрямку розвитку цифрової трансформації. Програма Digital Decade 2030 окреслює важливість міжнародного співробітництва для просування цінностей ЄС з партнерами-однодумцями, зокрема ЄС також активізував підтримку цифрової трансформації України, ввівши країну в зону безкоштовного роумінгу ЄС.

З'ясовані проблемні питання, пов'язані із цифровоою трансформацію. І одна із них – це те, що цифровий світ має базуватися на європейських цінностях, суть яких полягає в тому, що кожна людина має бути забезпечена можливістю користуватися цифровими технологіями, а для цього необхідно забезпечити достатній рівень володіння цифровими навичками. Зазначено, що в Україні в цьому напрямку варто було б розробити комплексну національну стратегію в області цифрових навичок і компетенцій.

Ключові слова: *цифрові права, цифрові принципи, цифрове майбутнє, правове забезпечення, електронне урядування, цифрова трансформація, цифрові технології, цифровізація, інформаційна безпека, цифрове суспільство, захист інформації, кібербезпека, електронна взаємодія, цифрові навчики.*

The article is devoted to the analysis of strategic, programmatic and legislative documents regarding the development of Europe's digital future, in particular the "EU Digital Decade" program, the European Declaration "On Digital Rights and Principles", the Law "On Digital Services", the Law "On Artificial Intelligence", the Law "On media freedom" etc. The possibility of adapting European norms and principles into the legislation of Ukraine was also analyzed.

It was determined that the digital transformation of states is the main priority of both the countries of the European Union, which focus all their resources on the development of digital transformation, and Ukraine, which is no exception, as it has declared a course for the development of a digital state. The "Digital Decade of the EU" initiative, which defines the directions of development of the digital transformation of the EU until 2030, is analyzed, among which four goals of the digital decade are highlighted – connectivity, digital skills, digital business and digital public services. The appropriateness of the implementation of the directions of digital transformation determined by this initiative for Ukraine in terms of the development of e-governance is argued.

© Александрова М., 2023

The results of the Report on the implementation of the "Digital Decade" program were analyzed and it was found that the success of the digital transformation of the EU will require a significant acceleration and deepening of the actions of the EU and the member states regarding the implementation of reforms, improvement of the business environment, ensuring motivation and increasing investment in digital technologies, training in digital skills and build infrastructure.

It is worth noting that the EU focuses an important role on international partnership in the direction of the development of digital transformation. The Digital Decade 2030 program outlines the importance of international cooperation for the promotion of EU values with like-minded partners, in particular, the EU has also stepped up support for Ukraine's digital transformation by introducing the country into the EU's free roaming zone.

Clarified problematic issues related to digital transformation. And one of them is that the digital world should be based on European values, the essence of which is that every person should be provided with the opportunity to use digital technologies, and for this it is necessary to ensure a sufficient level of possession of digital skills. It is noted that Ukraine should develop a comprehensive national strategy in the field of digital skills and competencies in this direction.

Key words: *digital rights, digital principles, digital future, legal support, e-government, digital transformation, digital technologies, digitalization, information security, digital society, information protection, cyber security, electronic interaction, digital learners.*

Постановка проблеми. Формування цифрового майбутнього – одна із основних цілей країн Європи загалом та України зокрема. Над розвитком цифрового суспільства працюють держави-члени ЄС та їх уряди, бо цифрове суспільство і цифрові технології забезпечують нові способи навчання, роботи, досліджень, реалізації амбіцій тощо. В той же час цифрова трансформація створює нові права та свободи громадян та стирає кордони між країни в частині отримання тих чи інших цифрових послуг. Однак в той же час існує багато проблем пов'язаних із цифровою трансформацією, зокрема щодо доступу до цифрових технологій та можливості користуватися ними. В рамках європейської декларації «Цифові права та принципи» виділено такі основні напрями: поставити людей та їхні права в центр цифрової трансформації; підтримка солідарності та інклюзії; забезпечення свободи вибору онлайн; сприяння участі в цифровому публічному просторі; підвищення безпеки, безпеки та розширення можливостей осіб; сприяння стійкості цифрового майбутнього.

Наукові публікації та дослідження з теми. Питання цифрової трансформації України та країн Європи досліджується відчизняними та закордонними науковцями та практиками. Зокрема серед українських науковців слід відзначити наукові роботи у цій сфері О. Бикова, І. Жаровської, О. Баранова, Н. Бортник, М. Міхровської, І. Личенко, В. Чорноніської, І. Бородін, О. Капля та інших. Також зазначені питаннями висвітлені в працях представників іноземної доктрини, зокрема: RepucciS.,SlipowitzA, GarikipatiS.,Kambhampat iU,ZamaniY.S.,.M.Nakib та інші. Однак проблематика залишається актуальною тому потребує подальшого комплексного дослідження.

Мета статті – дослідження питання щодо цифрового майбутнього країн Європи через аналіз *стратегічних, програмних та законодавчих документів* та їх імплементація в розвиток цифрової трансформації України.

Виклад основного матеріалу. Цифрова трансформація держав та їх урядів залишається головним пріоритетом для країн Європейського Союзу, саме тому в рамках стратегічних документів таких як ініціатива «Цифрове десятиліття ЄС» та європейська декларація "Цифрові права та принципи" визначені цілі, які власне визначають напрям розвитку цифрової трансформації ЄС до 2030 року та визначено цінності ЄС, які необхідно поважати в цифровому світі та які в той же час імпонують Україні. І саме досягнення цих цілей має на меті забезпечити розвиток суверенного, стійкого та конкурентоспроможного цифрового потенціалу ЄС. ЄС у досягненні цифрових цілей і завдань Європи до 2030 року, зосереджуючись на чотирьох основних стовпах: цифрові навички, цифрова інфраструктура, цифровізація бізнесу, включаючи використання штучного інтелекту (AI), і цифровізація державних послуг. В той же час особливу увагу ЄС зосереджує на забезпеченні цифрових прав та принципів. Це свідчить про те, що країни ЄС мають на меті забезпечити розвиток цифрової трансформації таким чином, щоб забезпечити в першу чергу права людей, що свідчить про людиноцентризький підхід. Такий підхід притаманний і Україні. Оскільки впровадження різноманітних цифрових інструментів та забезпечення доступу до отримання різноманітних публічних послуг за тими чи іншими життєвими ситуаціями свідчить про орієнтацію в першу чергу на потреби людей.

Політична програма «Цифрове десятиліття ЄС до 2030 року» зосереджується на таких основних напрямках діяльності країн та урядів держав-членів ЄС: безпечна цифрова інфраструктура, цифровізація бізнесу, цифровізація державних послуг, цифрові навички, цінності та принципи онлайн-суспільства,

міжнародне партнерство тощо. Зосередимося детальніше на кожному [3].

Цифрова інфраструктура – безпечне підключення. Відповідно до поточної цілі ЄС в рамках ініціативи «Цифрове десятиліття ЄС» до 2030 року, гігабітне покриття має бути доступним для всіх, а продуктивні мережі 5G мають бути в усіх населених пунктах. Наразі оптоволоконні мережі, які мають вирішальне значення для забезпечення гігабітного з'єднання, охоплюють лише 56% домогосподарств, у той час як покриття 5G становить 81% населення, зменшившись до 51% у сільській місцевості. Однак розгортання автономних мереж 5G відстає, і якість 5G все ще не відповідає очікуванням кінцевих користувачів і потребам галузі. 55% сільських домогосподарств все ще не обслуговуються жодною сучасною мережею, а 9% ще не охоплені жодною фіксованою мережею взагалі. Щоб забезпечити повне гігабітне покриття в ЄС, а також покриття 5G у всіх населених пунктах, потрібні додаткові інвестиції в розмірі щонайменше 200 мільярдів євро. Держави-члени повинні визначити свої прогалини в підключенні та вивчити фінансування, щоб доповнити приватні інвестиції в райони, які є комерційно нежиттєздатними, включаючи сільські та віддалені райони, користуючись перевагами проінвестиційної нормативної бази ЄС. В Україні схожа ситуація із покриттям, однак варто врахувати ще наслідки широкомасштабної війни, яку розпочала росія. Україна теж має на меті забезпечити покриттям всі регіони для створення сприятливих умов для цифрової трансформації та доступу всіх, без винятку громадян до переваг цифровізації.

Цифровізація бізнесу – це одна із основних напрямів розвитку цифрової трансформації в рамках згаданої вище ініціативи. Реалізація напрямку щодо цифрового бізнесу можлива через досягнення таких трьох цілей: 75% підприємств ЄС мають використовувати у своїй діяльності послуги хмарних обчислень, великі дані та/або штучний інтелект (AI); більше 90% малих і середніх підприємств (МСП) повинні досягти принаймні базового рівня цифрової інтенсивності; подвоїти кількість «єдинорогів» (компаній з оцінкою понад 1 мільярд євро). Однак для досягнення відповідних цілей в напрямку цифрового бізнесу теж необхідні інвестиції. Щоб покращити впровадження технологій, держави-члени повинні підвищувати обізнаність про переваги цифровізації бізнесу , а також просувати та підтримувати Європейські центри цифрових інновацій. За останнє десятиліття кількість єдинорогів у ЄС значно зросла. Продовження цієї тенденції дозволило б ЄС досягти своєї мети до 2030 року, але це не є підставою для самовдоволення на нестабільних ринках. Крім того, відмінності з іншими розвиненими економіками залишаються: на початку 2023 року в ЄС було 249 єдинорогів, у порівнянні з 1444 у США та 330 у Китаї [4].

Цифровізація державних послуг. Цілі «Цифрового десятиліття» передбачають 100% онлайн-доступність ключових державних послуг. В тому числі забезпечити електронну ідентифікацію для 100% громадян. Багато держав-членів мають хороші можливості для досягнення повної цифровізації державних послуг і медичних записів , а також розгортання eID для своїх громадян. Однак необхідні значні інвестиції для покращення транскордонної доступності та ефективності державних послуг. Що стосується European Digital Identity Wallet, то його повне розгортання триває: очікується, що воно буде завершено до 2030 року та доповнено цифровим євро, запропонованим у червні 2023 року. Україна має такі ж амбіції в частині цифровізації всіх державних послуг.

Цифрові навички. ЄС прагне розвинути базові цифрові навички щонайменше у 80% осіб у віці 16–74 років і охопити 20 мільйонів фахівців з ІКТ до 2030 року.

Саме для досягнення цієї мети державамчленам необхідно віддавати пріоритет інвестиціям у високоякісну освіту та опанування цифрових навичок. Україна уже сьогодні активно працює над цим напрямком. Держава створює великий спектр курсів та тренінгів для всіх охочих громадян щодо опанування цифрових навичок, в той же час діє мережа навчань для державних службовців, які власне і повинні забезпечувати впровадження цифрової трансформації у всі без винятку сфери суспільного життя.

Цінності та принципи онлайн-суспільства. ЄС є провідником у створенні безпечної та орієнтованої на людину цифрової трансформації, як це закріплено в Європейській декларації про цифрові права та принципи. ЄС запровадив відповідні політичні та законодавчі заходи, такі як Закон про цифрові послуги, Закон про штучний інтелект, Європейський закон про свободу медіа та Комунікації у віртуальних світах. Саме ця законодавча база повинна забезпечити права громадян в рамках цифрової трансформації держав-членів ЄС [6].

Стійкий цифровий перехід – ще один напрям розвитку цифрової трансфрмації країчленів ЄС. Сьогодні ЄС всі свої зусилля спрямовує на те, щоб зробити цифровий перехід

«екологічнішим». Впроваджуючи такі ініціативи як ініціатива «Право на ремонт», критерії екологічного дизайну для мобільних телефонів і планшетів і план дій ЄС щодо цифровізації енергетичних систем, які мають на меті зменшити вплив цифрових технологій на навколишнє середовище. Подальші інвестиції через національні плани відновлення та стійкості країн-членів ЄС, або спільні інвестиції також мають вирішальне значення для сприяння повному переходу до цифрових рішень, а також покращені механізми моніторингу для вимірювання екологічного сліду електронних комунікаційних послуг.

Варто зауважити, що ЄС важливу роль зосереджує на міжнародному партнерстві в напрямку розвитку цифрової трансформації. Програма Digital Decade 2030 окреслює важливість міжнародного співробітництва для просування цінностей ЄС з партнерами-однодумцями. І як показує результ впровадження зазначеної ініціативи прогресу в досягненні цієї мети було досягнуто завдяки цифровому партнерству з Японією, Республікою Корея та Сінгапуром, а також Торгово-технологічним радам із Сполученими Штатами та Індією. ЄС також активізував підтримку цифрової трансформації України, ввівши країну в зону безкоштовного роумінгу ЄС. Це надзвичайно важливе рішення для України та українців, які перебувають за її межами, щоб не втрачати зв'язок з рідними, особливо в умовах повномасштабної війни.

Забезпечення цифрових права та принципів – основна мета цифрового десятиліття Європи та України. 15 грудня 2022 року президент Європейської комісії Урсула фон дер Ляєн підписала Європейську декларацію про цифрові права та принципи (далі – Декларація) разом із президентом Європейського парламенту Робертою Мецолою та прем'єр-міністром Чехії Петром Фіалою під час головування в Раді [2]. Декларація, висунута Комісією в січні 2022 року, представляє зобов'язання ЄС щодо безпечної та стійкої цифрової трансформації, яка ставить людей у центр, відповідно до основних цінностей ЄС і основних прав людей [5].

Цифрова трансформація впливає на кожен аспект життя людей. Він пропонує можливості для підвищення особистого добробуту, стабільності та зростання, але також може підвищувати ризики, на які потрібна реакція державної політики. За допомогою Декларації про цифрові права та принципи ЄС хоче захистити європейські цінності шляхом:

– поставлення людей у центр цифрової трансформації;

– підтримка солідарності та інклюзії через підключення, цифрову освіту, навчання та навички, чесні та справедливі умови праці та доступ до цифрових державних послуг;

– підкреслюючи важливість свободи вибору та справедливого цифрового середовища;

– сприяння участі в цифровому публічному просторі;

– підвищення безпеки, захисту та розширення можливостей у цифровому середовищі, зокрема для молоді;

– сприяння стійкості.

Конкретно ці права та принципи означають: доступне та високошвидкісне цифрове підключення скрізь і для всіх, добре обладнані класи та вчителі з цифровими навичками, безперебійний доступ до державних послуг онлайн, безпечне цифрове середовище для дітей, відключення після робочого дня, отримання легкого – розуміти інформацію про вплив наших цифрових продуктів на навколишнє середовище, контролювати те, як використовуються особисті дані та з ким вони передаються. Розглянемо кожен із них [7].

Люди в центрі – чи не найважливіший принцип цифрової трансформації, оскільки свідчить про те, що саме на людину спрямовані ключові зміни в державах, що мають на меті забезпечити їм комфортне життя та реалізацію основоположних прав та інтересів. Цифрові технології мають захищати права людей, підтримувати демократію та гарантувати, що всі цифрові гравці діють відповідально та безпечно, що в жодному разі не порушить права людей. ЄС просуває ці цінності по всьому світу.

Свобода вибору – чи не найпоширеніше цифрове право, що має на меті забезпечити людям можливість отримувати користь від справедливого онлайн-середовища, бути захищеними від незаконного та шкідливого вмісту та мати повноваження під час взаємодії з новими технологіями, що розвиваються, як-от штучний інтелект. Саме онлайн середовище забезпечує плюралізм можливостей щодо користування тими чи іншими цифровими інструментами.

Безпека та захист. Зазначене право гарантує людям безпечне цифрове середовище. Усі користувачі, починаючи від дітей і закінчуючи людьми у віці повинні бути забезпеченні інформаційною безпекою та захистом інформації.

Солідарність та інклюзивність. Забезпечення даного принципу має на меті об'єднувати, а не роз'єднувати людей через використання цифрових технологій. Адже кожен повинен мати доступ до Інтернету, володіти цифровими навичками, а в разі їх відсутності мати змогу їх опанувати через відповідне доступне навчання, доступ до всіх

цифрових державних послуг і справедливих умов праці.

Право участі – громадяни мають можливість брати участь у демократичному процесі на всіх рівнях і контролювати в тому числі власні персональні дані, та будь яку інформацію, яка їх стосується.

Принцип стійкості – цифрові пристрої повинні підтримувати сталість і екологічний перехід . Люди повинні знати про вплив своїх пристроїв на навколишнє середовище та енергоспоживання [7].

Цифрові права та принципи, викладені в Декларації, доповнюватимуть існуючі права, такі як ті, що вкорінені в Хартії основних прав ЄС, а також законодавство про захист даних і конфіденційність. Вони забезпечать довідкову базу для громадян щодо їхніх цифрових прав, а також вказівки для держав-членів ЄС і для компаній щодо роботи з новими технологіями. Вони покликані допомогти кожному в ЄС отримати максимум від цифрової трансформації.

Першу оцінку впровадження цифрових принципів надано у звіті «Про стан цифрового десятиліття» за 2023 рік (далі- Звіт). У першому звіті про стан цифрового десятиліття підводиться підсумок прогресу ЄС на шляху до успішної цифрової трансформації, як зазначено в політичній програмі цифрового десятиліття до 2030 року. У цьому звіті підкреслюється необхідність прискорення та поглиблення колективних зусиль, у тому числі шляхом політичних заходів та інвестицій у цифрові технології, навички та інфраструктуру.

На цій основі звіт містить конкретні рекомендації державам-членам перед ухваленням їхніх національних стратегічних дорожніх карт і щодо їх майбутніх коригувань. Цей Звіт також включає моніторинг Європейської декларації про цифрові права та принципи цифрового десятиліття, яка перетворює бачення ЄС цифрової трансформації на принципи та зобов'язання. Успіх Цифрового десятиліття буде критично важливим для ЄС в частині майбутнього розвитку та процвітання. Досягнення порядку денного цифрового десятиліття ЄС може розблокувати понад 2,8 трильйона євро в економічній вартості, що еквівалентно 21% поточної економіки ЄС [8].

Ситуація, представлена в цьому Звіті, демонструє, що успіх цифрової трансформації ЄС вимагатиме суттєве прискорення та поглиблення ЄС і дій держав-членів щодо здійснення реформ, покращення бізнес середовища, забезпечення мотивації та збільшення інвестиції в цифрові технології, навчання цифровим навичкам та розбудовую інфраструктури. Результати дослідження також свідчать про важливість більшої скоординованості дії щодо цифрової трансформації ЄС.

Висновки. Формування цифрового майбутнього Європи загалом та України зокрема нерозривно пов'язано із цифрової трансформацією усіх без винятку сфер суспільного життя. Напрямки розвитку цифрових трансформаційних процесів закріплені в стратегічних, програмних та законодавчих документах краї ЄС. А моніторингові дослідження щодо їх впровадження та реалізацію дають змогу відслідкувати стан речей та зрозуміти яким чином розвивати ту чи іншу сферу цифрової трансформації. Впровадження європейських принципів та цілей розвитку цифрової трансформації сприятиме розвитку й адміністративно правого забезпечення системи електронного урядування в Україні. Серед яких варто видалити такі ключові рекомендації. По-перше, створювати цифрові продукти таким чином, щоб громадяни могли легко й швидко ними скористатися, тобто людина повинна бути в центрі цифрової трансформації, а задоволення її прав та свобод – основна ціль трансформації. По-друге, систематизувати електронні послуги за життєвими ситуаціями, що зробить їх простішими і доступнішими в пошуку та використанні, а також забезпечити навчання цифрових навичок для всіх охочих громадян. По-третє, оптимізувати взаємодію між суб'єктами держава –громадянин, держава – бізнес, щоб забезпечити більш послідовний і менш затратний по часу і ресурсах процес.

Література:

1. DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

2. Millard, J., Impact of digital transformation on public governance, Manzoni, M. and Schade, S. editor(s), Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/204686, https://publications.jrc.ec.europa.eu/repository/handle/JRC133975

3. 2030 Digital Compass: the European way for the Digital Decade. 2021. URL: https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf.

4. Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. 2021.

5. Digital Economy and Society Index (DESI) 2020 (2021). URL: Thematic chapters. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086

6. EUROPE 2020. A European strategy for smart, sustainable and inclusive growth. 2010. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

7. The Digital Decade policy programme 2030, file:///Users/captainroshchuk/Downloads/Digital_Decade_factsheet_update_January_2023_sQJEKpJFAruAY4d2AcLTsMmKBLY_79267.pdf

8. United Nations, General Assembly, "Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation", report of the Secretary-General (A/74/81), 29 May 2020. URL: https://www.un.org/en/content/digital-cooperation-roadmap/

References:

1. DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

2. Millard, J., Impact of digital transformation on public governance, Manzoni, M. and Schade, S. editor(s), Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/204686, https://publications.jrc.ec.europa.eu/repository/handle/JRC133975

3. 2030 Digital Compass: the European way for the Digital Decade (2021). Retrieved from https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf.

4. Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030 (2021).

5. Digital Economy and Society Index (DESI) 2020 (2021). Retrieved from Thematic chapters. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086

6. EUROPE 2020. A European strategy for smart, sustainable and inclusive growth (2010). Retrieved from https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%2 0007%20-%20Europe%202020%20-%20EN%20version.pdf

7. The Digital Decade policy programme 2030, file:///Users/captainroshchuk/Downloads/Digital_Decade_factsheet_update_January_2023_sQJEKpJFAruAY4d2AcLTsMmKBLY_79267.pdf

8. United Nations, General Assembly, "Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation", report of the Secretary-General (A/74/81), 29 May 2020. Retrieved from https://www.un.org/en/content/digital-cooperation-roadmap/

УДК 346.2:339.128
DOI https://doi.org/10.32689/2522-4603.2023.3.5

Святослав ХІМІЧ
аспірант Навчально-наукового Інституту управління, економіки та бізнесу,
Міжрегіональної Академії управління персоналом, вул. Фроментівська, 2, м. Київ, Україна, 03039
ORCID: 0009-0000-8811-8801

Sviatoslav KHIMICH
Postgraduate Student of the Educational and Scientific Institute of Management, Economics and Business
of the Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039
ORCID: 0009-0000-8811-8801

ІНСТИТУЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПІДПРИЄМСТВ

INSTITUTIONAL AND LEGAL MECHANISM OF THE STATE REGULATION OF THE DIGITAL TRANSFORMATION OF ENTERPRISES

У статті розглянуто інституційно-правовий механізм який є критичним чинником розвитку цифрової економіки в будь-якій країні. Визначено, що в сучасній Україні даний механізм включає в себе створення правових норм, законів, стратегій та програм, спрямованих на підтримку та регулювання цифрового розвитку.

Мета роботи. *Метою статті є аналіз інституційно-правового механізму державного регулювання цифрової трансформації підприємств в Україні; розгляд ресурсного забезпечення цифрової трансформації, зокрема у контексті концепцій "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості" та "Відкрите виробництво"; розглянути інфраструктуру інституційно-правового забезпечення цифрової трансформації в частині складових, які сприяють створенню ефективної та динамічної цифрової екосистеми; дослідити кон'юнктуру інституційно-правового забезпечення промислової трансформації та формування єдиного цифрового простору із ЄС для успішного інтегрування України в європейські економічні та технологічні процеси.*

Наукова новизна. *Доведено, що все більше фахівців досліджують тему державного регулювання цифрової трансформації підприємств в Україні. Зазначено, що залучення відповідального робочого органу для координації цифровізації економіки та розбудови інститутів розвитку цифрової економіки стає доцільним для ефективної інтеграції та розвитку цифрових технологій. Це дозволяє створити сприятливі умови для інновацій та забезпечити необхідну підтримку для стартапів та інноваційних підприємств.*

Методи та методологія. *У ході дослідження були використані такі методи, як аналіз та синтез, методи історичного та логічного моделювання. Також були застосовані теоретичні підходи, зокрема метод формалізації, метод «від абстрактного до конкретного», а також метод економічної інтерпретації.*

Результати. *У запропонованій статті особливу увагу приділено аналізу аспектів практичного застосування інституційно-правового механізму державного регулювання цифрової трансформації підприємств в Україні.*

Висновки. *Інституційно-правовий механізм виявляється ключовим чинником у сприянні розвитку цифрової економіки. Розробка та прийняття важливих законодавчих актів, таких як Закон "Про цифрову економіку", а також стратегічних програм цифровізації, мають визначальне значення у вирішенні даного завдання. Ресурсне забезпечення включає в себе фінансові, інтелектуально-кадрові та технічно-технологічні ресурси, які необхідні для успішної реалізації проектів з цифровізації. Належне ресурсне забезпечення є важливою передумовою для досягнення успіху у даному напрямі.*

Ключові слова: *цифровізація, цифрова трансформація, інституційно-правовий механізм, розробка законодавчих актів, ресурси.*

The article examines the institutional and legal mechanism, which is a critical factor in the development of the digital economy in any country. It was determined that in modern Ukraine this mechanism includes the creation of legal norms, laws, strategies and programs aimed at supporting and regulating digital development.

Purpose. *The purpose of the article is to analyze the institutional and legal mechanism of state regulation of digital transformation of enterprises in Ukraine; consideration of resource provision of digital transformation, in particular in the context of the concepts "Industry 4.0", "Digital production", "Internet in industry" and "Open production"; consider the infrastructure of institutional and legal support for digital transformation in terms of components that contribute to the creation of an effective and dynamic digital ecosystem; to investigate the conjuncture of institutional and legal support for industrial transformation and the formation of a single digital space with the EU for the successful integration of Ukraine into European economic and technological processes.*

© Хіміч С., 2023

Scientific novelty. *It has been proven that more and more experts are researching the topic of state regulation of digital transformation of enterprises in Ukraine. It is noted that the involvement of a responsible working body for the coordination of the digitization of the economy and the development of institutions for the development of the digital economy becomes expedient for the effective integration and development of digital technologies. This allows creating favorable conditions for innovation and providing the necessary support for startups and innovative enterprises.*

Methods and methodology. *In the course of the research, such methods as analysis and synthesis, methods of historical and logical modeling were used. Theoretical approaches were also applied, in particular the method of formalization, the method "from abstract to concrete", as well as the method of economic interpretation.*

Results. *In the proposed article, special attention is paid to the analysis of aspects of the practical application of the institutional and legal mechanism of state regulation of the digital transformation of enterprises in Ukraine.*

Conclusions. *The institutional and legal mechanism is a key factor in promoting the development of the digital economy. The development and adoption of important legislative acts, such as the Law "On Digital Economy", as well as strategic digitalization programs, are of decisive importance in solving this task. Resource support includes financial, intellectual and human resources, and technical and technological resources, which are necessary for the successful implementation of digitization projects. Adequate resource provision is an important prerequisite for achieving success in this direction.*

Key words: *digitalization, digital transformation, institutional and legal mechanism, development of legislative acts, resources.*

Постановка проблеми. Розвиток сектора цифрової економіки в сучасному світі неможливий без врахування важливих чинників, які впливають на його стан і динаміку. Серед них особливу увагу слід звернути на формування сприятливого бізнес-середовища для впровадження цифровізації. Це означає створення умов для ефективного взаємодії між державними органами, бізнесом та науково-дослідними установами.

Також важливим чинником є ресурсне забезпечення процесів цифровізації. Наявність кваліфікованого інтелектуального та кадрового потенціалу, а також дослідницько-інноваційних ресурсів, є запорукою успішної інтеграції цифрових технологій у всі сфери економіки.

Окрім цього, важливим є розвиток інфраструктури, необхідної для цифровізації. Створення інноваційних центрів, підтримка науково-дослідних організацій та ІТ-компаній сприяє впровадженню сучасних технологій у виробництво та обслуговування. Не менш важливим є вплив кон'юнктурних факторів на розвиток сектора цифрової економіки. Активний попит на ІТ-розробки та високотехнологічні продукти, конкурентоспроможні ціни на впровадження цифрових процесів і висока відкритість ринку сприяють зростанню цього сектору.

Загалом, створення умов для розвитку цифрової економіки вимагає комплексного підходу з боку держави в частині прийняття на законодавчому рівні відповідних законопроектів, які будуть враховувати взаємозв'язки між різними галузями економіки. Тільки таким чином можна досягти сталого й ефективного росту сектора цифрової економіки в країні.

Аналіз останніх досліджень та публікацій. Особливу увагу слід приділити вченим, які внесли значний внесок у дослідження цифрової економіки. Зокрема, варто відзначити праці Апалькової В. [1], Коляденка С. [2], Чмерука Г. [3], та Веретюка С. [4]. Попередні дослідження у правовій сфері зазвичай фокусувались на конкретних сферах використання цифрових платформ, не надаючи аналізу явищу як об'єкту правового аналізу.

Наприклад, попередні наукові праці досліджували аспекти трудових відносин, що виникають у зв'язку з використанням цифрових платформ [5]. Також проводився аналіз міжнародних тенденцій у нормативному регулюванні цифрової економіки [6] та інших важливих аспектів. Зрозуміло, що цифрові платформи мають бути розглянуті як самостійне правове явище, і їх вплив на різні сфери суспільства та економіки потребує додаткового вивчення та аналізу.

Мета роботи. Метою статті є аналіз інституційно-правового механізму державного регулювання цифрової трансформації підприємств в Україні; розгляд ресурсного забезпечення цифрової трансформації, зокрема у контексті концепцій "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості" та "Відкрите виробництво"; розглянути інфраструктуру інституційно-правового забезпечення цифрової трансформації в частині складових, які сприяють створенню ефективної та динамічної цифрової екосистеми; дослідити кон’юнктуру інституційно-правового забезпечення промислової трансформації та формування єдиного цифрового простору із ЄС для успішного інтегрування України в європейські економічні та технологічні процеси.

Виклад основного матеріалу. Цифрова трансформація підприємств стала однією з ключових тем у сучасному бізнес-дискурсі, і її дослідження привертає увагу вчених як в Україні, так і за кордоном. Основні дослідження в цій області розкривають декілька важливих аспектів:

1. Стратегічний підхід до цифрової трансформації: вчені досліджують стратегічні

аспекти впровадження цифрових технологій в підприємствах. Вони аналізують, які чинники впливають на вибір технологій, прийняття рішень щодо цифрової трансформації та її вплив на стратегічний розвиток компаній.

2. Технологічні інновації та інфраструктура: вчені вивчають технологічні аспекти цифрової трансформації, такі як використання штучного інтелекту, блокчейну, Інтернету речей та інших сучасних технологій. Оцінюється вплив цих інновацій на ефективність підприємств.

3. Організаційні зміни та культура підприємства: вчені аналізують вплив цифрової трансформації на організаційну культуру підприємства. Важливо вивчити, як ця трансформація впливає на структуру, комунікацію та робочі процеси.

4. Ефективність та конкурентоспроможність: оцінка впливу цифрової трансформації на фінансові показники підприємств є одним із ключових аспектів досліджень. Вчені вивчають, як цифрові ініціативи впливають на прибутковість, ринкову частку та інші показники ефективності.

5. Проблеми та виклики цифрової трансформації: вчені аналізують труднощі та виклики, які виникають під час впровадження цифрових технологій, такі як кадрові аспекти, проблеми кібербезпеки та інші ризики.

Українські вчені, крім вивчення загальних аспектів цифрової трансформації, акцентують увагу на специфічних особливостях українського бізнес-середовища, локальних ринкових умов та геополітичних аспектах цифрової трансформації.

Зарубіжні дослідження в свою чергу часто надають порівняльний аналіз цифрової трансформації в різних країнах, досліджують глобальні тенденції та вплив міжнародних технологічних компаній. Усі ці аспекти важливі для розуміння суті та потенціалу цифрової трансформації підприємств, а також для розробки ефективних стратегій впровадження цифрових технологій у бізнес-процеси.

Інституційно-правовий механізм є критичним чинником розвитку цифрової економіки в будь-якій країні. Він включає в себе створення правових норм, законів, стратегій та програм, спрямованих на підтримку та регулювання цифрового розвитку.

1. Законодавча база:

Закон "Про цифрову економіку" визначає основні принципи та правила функціонування цифрового сектору. Він має регулювати правові відносини в галузі електронних послуг, кібербезпеки, захисту персональних даних та інші аспекти цифрової економіки.

2. Стратегії та програми цифрового розвитку:

Стратегія цифрового розвитку національної економіки встановлює загальні цілі та завдання в цифровій сфері на деякий термін (наприклад, на 5–10 років). Вона визначає пріоритети, рекомендації та рекомендації щодо розвитку цифрової інфраструктури, технологій та галузей.

Цільові програми цифровізації сфер та галузей економіки спрямовані на реалізацію конкретних завдань та проектів в окремих галузях економіки (наприклад, освіта, охорона здоров'я, транспорт і т.д.). Вони можуть передбачати фінансову підтримку, створення інноваційних центрів, підтримку досліджень та інші заходи.

3. Органи та інституції управління цифровою економікою:

Створення спеціалізованих урядових агентств, департаментів чи комісій, які відповідають за регулювання та розвиток цифрового сектору. Ці органи мають надавати консультації, підтримку та регулювати правові відносини у сфері цифрової економіки.

4. Забезпечення кібербезпеки та захисту даних:

Важливим аспектом є прийняття та впровадження нормативно-правових актів, що забезпечують кібербезпеку та захист персональних даних. Це включає в себе стандарти, протоколи та політики зберігання та обробки даних.

5. Міжнародне співробітництво:

Укладення міжнародних договорів та участь у міжнародних проектах у галузі цифрової економіки може сприяти обміну досвідом та технологіями, а також відкривати нові можливості для компаній на міжнародному ринку.

6. Нормативна база для стартапів та інновацій:

Створення сприятливого правового середовища для розвитку інновацій та стартапів може прискорити розвиток цифрового сектору.

Узагальнюючи, ефективний інституційно-правовий механізм є критичним чинником для успішного розвитку цифрової економіки. Він надає стійку правову базу для інновацій та новаторського росту, сприяє захисту прав та інтересів учасників цифрового ринку та сприяє створенню конкурентоспроможного та інноваційного бізнес-середовища.

Ресурсне забезпечення інституційно-правового забезпечення цифрової трансформації, зокрема у контексті концепцій "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості" та "Відкрите виробництво", включає в себе низку ключових аспектів:

1. Інтелектуально-кадровий потенціал: наявність висококваліфікованих спеціалістів, які володіють необхідними навичками у сфері цифрових технологій. Це може включати програми навчання та підвищення кваліфікації, академічні та промислові партнерства.

2. Дослідницько-інноваційний потенціал: наявність наукових установ, дослідницьких лабораторій та інноваційних центрів, які здійснюють дослідження та розробки у сфері цифрових технологій.

3. Фінансово-інвестиційне забезпечення: наявність інвестиційних ресурсів, які спрямовані на розвиток цифрових технологій та інфраструктури, підтримку інноваційних стартапів та проектів.

4. Техніко-технологічне забезпечення: доступ до сучасних технологічних рішень, обладнання та програмних продуктів, які необхідні для впровадження концепцій "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості" та "Відкрите виробництво".

Інституційно-правове забезпечення включає в себе ряд правових актів та політик, що регулюють та сприяють впровадженню цифрових концепцій:

– Прийняття концепцій: ухвалення офіційних концепцій, таких як "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості" та "Відкрите виробництво", які визначають основні стратегічні напрямки розвитку цифрової економіки.

– Зміни в законодавстві щодо криптовалют: удосконалення законодавства для визнання та регулювання криптовалют та блокчейн-технологій. Це може включати в себе регулювання обміну криптовалют, встановлення правил для проведення Initial Coin Offerings (ICO) та інші нормативні акти.

– Закони про кібербезпеку та захист персональних даних: прийняття та впровадження законів, які забезпечують кібербезпеку та захист персональних даних у цифровому середовищі.

– Створення правових рамок для електронного урядування та електронних послуг: розробка та ухвалення нормативних актів, які регулюють надання електронних громадянських та адміністративних послуг, впровадження електронних систем урядування.

– Регулювання в сфері інтелектуальної власності: удосконалення правових аспектів охорони та використання інтелектуальної власності у цифровому середовищі.

Загальна мета інституційно-правового забезпечення є створення стійкого та прозорого правового середовища, яке сприяє розвитку та впровадженню цифрових технологій, а також захисту прав та інтересів учасників цифрового ринку.

Інфраструктура інституційно-правового забезпечення цифрової трансформації включає в себе ряд ключових складових, які сприяють створенню ефективної та динамічної цифрової екосистеми:

– Створення органу для координації дій із цифровізації економіки: створення спеціалізованого органу або агентства, що відповідає за координацію та контроль реалізації цифрових стратегій та програм. Цей орган може включати представників уряду, громадськості та приватного сектору.

– Розбудова інститутів розвитку цифрової економіки: створення та підтримка спеціалізованих інститутів, які сприяють розвитку та впровадженню цифрових технологій. Ці інституції можуть надавати фінансову, консультативну та технічну підтримку для цифрових проектів.

– Формування науково-дослідних організацій та інноваційних центрів: підтримка та розвиток наукових установ та дослідницьких лабораторій, які спеціалізуються у цифрових технологіях. Створення інноваційних центрів сприяє об'єднанню вчених, бізнесу та уряду для спільної реалізації цифрових проектів.

– Розвиток інфраструктури та технологічних кластерів: створення спеціалізованих технологічних кластерів та інфраструктури для розробки та тестування цифрових рішень. Це може включати в себе створення спільних лабораторій, інноваційних просторів та інших спеціалізованих об'єктів.

– Організація конференцій, семінарів та інших заходів: сприяння обміну знань, досвіду та кращих практик у сфері цифрової трансформації через проведення спеціалізованих заходів та подій.

– Створення інноваційно-технологічних партнерств: розвиток партнерських відносин між громадським сектором, приватним бізнесом та вищими навчальними закладами для спільного розв'язання завдань та реалізації проєктів у сфері цифрової трансформації.

– Формування інфраструктури для тестування та впровадження цифрових рішень: створення лабораторій та тестових майданчиків для впровадження та тестування цифрових технологій та продуктів.

Загальна мета інфраструктури інституційно-правового забезпечення цифрової трансформації полягає в створенні сприятливого та ефективного середовища для розвитку та впровадження цифрових технологій, а також у забезпеченні координації та підтримці різних учасників цифрового екосистеми.

Кон'юнктура інституційно-правового забезпечення промислової трансформації та формування єдиного цифрового простору із ЄС є критичним для успішного інтегрування України в європейські економічні та технологічні процеси:

– Розробка концепції промислової трансформації: укладення фундаментального правового документу, який визначає стратегічні напрямки та завдання промислової трансформації. Ця концепція повинна враховувати специфічність української економіки та потенціал для інтеграції в європейський цифровий простір.

– Формування єдиного цифрового простору із ЄС: утворення правового механізму, який дозволяє Україні і Європейському Союзу інтегрувати свої цифрові ринки. Це включає в себе стандартизацію, гармонізацію законодавства, а також забезпечення взаємного визнання та використання цифрових технологій.

– Забезпечення права інтелектуальної власності: удосконалення законодавства та практики щодо захисту прав інтелектуальної власності. Це включає в себе патентування винаходів, реєстрацію товарних знаків, авторські права та інші аспекти.

– Визначення стандартів інформаційної безпеки: розробка та прийняття стандартів та нормативів щодо кібербезпеки та захисту інформації в цифровому середовищі.

– Формування публічно-приватного партнерства: створення правового механізму для співпраці між урядом та приватним сектором у сфері цифрової трансформації. Це може включати в себе механізми фінансової підтримки, спільних проектів та обмін досвідом.

– Забезпечення конфіденційності та захисту персональних даних: розробка та впровадження нормативних актів, які гарантують захист приватності та персональних даних громадян.

– Підтримка стартапів та інноваційних підприємств: розробка правових механізмів, які сприяють розвитку та функціонуванню інноваційного сектору, включаючи податкові пільги, фінансову підтримку та інші заходи.

Аналіз та впровадження цих елементів в інституційно-правове забезпечення сприятиме ефективному інтегруванню України в європейську цифрову екосистему, сприяючи розвитку промисловості та цифрової економіки країни.

Узагальнюючи, можна зазначити, що ефективне державне регулювання сектора цифрової економіки базується на використанні інструментів інституційно-правового механізму. Розробка та прийняття таких ключових законодавчих актів, як Закон "Про цифрову економіку", Стратегія цифрового розвитку національної економіки та концепції економічного розвитку "Індустрія 4.0.", "Цифрове виробництво", "Інтернет у промисловості", "Відкрите виробництво", є важливим етапом у цьому процесі.

Залучення відповідального робочого органу для координації цифровізації економіки та розбудова інститутів розвитку цифрової економіки стає доцільним для ефективної інтеграції та розвитку цифрових технологій. Це дозволяє створити сприятливі умови для інновацій та забезпечити необхідну підтримку для стартапів та інноваційних підприємств.

Значущим етапом у цифровій трансформації є також розробка концепції промислової трансформації та формування єдиного цифрового простору з країнами ЄС. Це відкриває нові можливості для співпраці, обміну технологічними рішеннями та розвитку міжнародних проектів у сфері цифрової економіки.

Враховуючи внутрішні та зовнішні кон'юнктурні фактори, державне регулювання повинно бути гнучким та адаптивним. Це дозволить країні виходити на нові рівні цифрового розвитку та ефективно конкурувати на світовому ринку.

Для ефективної реалізації економічного механізму важливо використовувати широкий спектр фінансово-мотиваційних інструментів. Ці заходи мають спрямовуватися як на пряме бюджетне фінансування цифровізації соціальної сфери та впровадження цифрових технологій в державному управлінні, так і на стимулювання впровадження цифровізації у сфері бізнесу.

Податкова, митна, інвестиційна та інноваційна політика має бути адаптована до вимог цифрової економіки. Надання пільгового кредитування та зменшення мит на обладнання і технології стануть потужним стимулом для компаній, щоб впроваджувати цифрові рішення у свою діяльність.

Створення пільгових режимів оподаткування та сприяння розвитку цифрової інфраструктури є ключовими елементами, що сприятимуть розбудові цифрового сектору. Також важливим є запровадження концесійних та сервісних моделей фінансування та управління інвестиційними проектами. Це створить додаткові можливості для залучення приватного сектору до цифрових ініціатив та забезпечить ефективну реалізацію проектів.

Загалом, використання цих фінансово-мотиваційних інструментів сприятиме активізації цифрової трансформації у всіх сферах економіки, сприяючи зростанню конкурентоспроможності та інноваційного потенціалу країни.

Організаційний механізм є ключовим компонентом успішної цифрової трансформації економіки країни. Його інструменти визначають способи та методи, за допомогою яких здійснюється впровадження цифрових технологій та процесів.

Організація та планування процесів цифровізації. Це включає в себе створення спеціалізованих організацій, комітетів чи робочих груп, що відповідають за розробку та впровадження стратегій цифровізації. Планування включає у себе визначення пріоритетних напрямків та завдань, а також розподіл ресурсів.

Розбудова необхідної інфраструктури. Це включає в себе розвиток телекомунікаційних мереж, центрів обробки даних, хмарних платформ та іншої технічної інфраструктури, необхідної для ефективного функціонування цифрового сектору.

Перехід на електронний документообіг і оцифрування технічної документації. Цей інструмент дозволяє забезпечити ефективний обмін даними та документами у електронному форматі, що раціоналізує бізнес-процеси та полегшує прийняття рішень.

Визнання та застосування міжнародних стандартів "Індустрії 4.0". Цей елемент дозволяє уніфікувати підходи до впровадження цифрових технологій, що сприяє взаєморозумінню та спільному розвитку з іншими країнами.

Стандартизація та сертифікація технологій. Ці процеси гарантують високу якість та сумісність цифрових рішень, що є важливим для підтримки безпеки в екосистемі цифрової економіки.

Ліцензування технологій та послуг. Цей механізм дозволяє контролювати та регулювати використання деяких технологій, особливо в сферах, які мають важливе стратегічне значення для країни.

Організаційний механізм є основним фундаментом для ефективної реалізації цифрової трансформації. Його правильне використання сприяє створенню сприятливого середовища для розвитку цифрової економіки та забезпечує стійкий та інноваційний розвиток країни.

Висновки. Інституційно-правовий механізм виявляється ключовим чинником у сприянні розвитку цифрової економіки. Розробка та прийняття важливих законодавчих актів, таких як Закон "Про цифрову економіку", а також стратегічних програм цифровізації, мають визначальне значення у вирішенні даного завдання. Ресурсне забезпечення включає в себе фінансові, інтелектуально-кадрові та технічно-технологічні ресурси, що необхідні для успішної реалізації проектів з цифровізації. Його належне забезпечення є важливою передумовою для досягнення успіху у даному напрямі.

Інфраструктура, яка включає телекомунікаційні мережі та центри обробки даних, є обов'язковим компонентом для ефективного функціонування цифрового сектору. Кон’юнктура також має важливе значення. Вплив ринкових факторів, таких як попит на ІТ-розробки та рівень конкуренції, може визначати темпи та напрями розвитку цифрової економіки. У цілому, успішна цифрова трансформація економіки країни потребує комплексного підходу та урахування всіх чинників та механізмів. Інституційно-правовий механізм, ресурсне забезпечення, інфраструктура та кон’юнктура є важливими компонентами цього процесу, кожен з яких вносить власний вагомий внесок у досягнення успіху.

Література:

1. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету. Серія : Менеджмент інновацій.* 2015. Вип. 4. С. 9–18.

2. Коляденко С. Цифрова економіка: передумови та етапи становлення в Україні і у світі. *Економіка. Фінанси. Менеджмент*. 2016. № 6. С. 106–107. URL: www.irbis-nbuv.gov.ua

3. Чмерук Г. Г. Деякі аспекти цифрової трансформації підприємств. *Економіка та управління підприємствами*. 2018. Вип. № 34. С. 97–101.

4. Веретюк С. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. *Фінансовий простір*. 2017. № 3(27).

5. Going Digital: Making the Transformation Work for Growth and Well-being, URL: http://www.oecd.org./going-digital/project

6. Australian Government. Digital Sourcing Policies. URL: https://www.dta.gov.au/help-and-advice/ict-procurement/digital-sourcing-frame-work-ict-procurement/ digital-sourcing-policies

7. Ковтонюк К. В. Цифровізація світової економіки як фактор економічного зростання. *Науковий вісник Херсонського державного університету*. 2017. Вип. 27. Частина 1. С. 29–33.

8. British Computer Society. The Digital Economy. URL: https://policy.bcs.org/position_statements/digital-econonomy

9. Чмерук Г.Г. Цифрова трансформація як нова форма трансформації фінансових відносин суб’єктів господарювання. *Вісник ОНУ імені І. І. Мечникова.* 2019. Т. 24. Вип 4(77).

10. Ковальчук К. Ф., Бандоріна Л. М. , Удачина К. О. Цифрова економіка – економіка XXI століття. *Цифрова економіка* : зб. матеріалів Національної наук.-метод. конф., 4–5 жовтня 2018 р., м. Київ : КНЕУ. 2018. С. 185–188.

References:

1. Apalkova V. V. (2015). Kontseptsiia rozvytku tsyfrovoi ekonomiky v Yevrosoiuzi ta perspektyvy Ukrainy [The concept of digital economy development in the European Union and prospects of Ukraine]. *Visnyk Dnipropetrovskoho universytetu – Bulletin of Dnipropetrovsk University*. *Series : Innovation Management*, 4, 9–18 [in Ukrainian].

2. Kolyadenko S. (2016). Tsyfrova ekonomika: peredumovy ta etapy stanovlennia v Ukraini i u sviti. Ekonomika [Digital economy: prerequisites and stages of formation in Ukraine and in the world]. *Finansy. Menedzhment. – Economy. Finances. Management,* 6, 106–107. Retrieved from www.irbis-nbuv.gov.ua [in Ukrainian].

3. Chmeruk G. G., Kralich V. R., Burlakova I. A. (2018). Deiaki aspekty tsyfrovoi transformatsii pidpryiemstv. [Some aspects of digital transformation of enterprises]. *Ekonomika ta upravlinnia pidpryiemstvamy. – Economics and Management of Enterprises*, 34, 97–101 [in Ukrainian].

4. Veretyuk C., Pilinsky V. (2017). Vyznachennia priorytetnykh napriamkiv rozvytku tsyfrovoi ekonomiky v Ukraini. [Determining the priority areas of digital economy in Ukraine]. *Finansovyi prostir. – Financial space*, № 3(27) [in Ukrainian].

5. Going Digital: Making the Transformation Work for Growth and Well-being, Retrieved from: http://www.oecd.org./going-digital/project [in Ukrainian].

6. Australian Government (2019). Digital Sourcing Policies. Retrieved from: https://www.dta.gov.au/help-and-advice/ict-procurement/digital-sourcing-frame-work-ict-procurement/digital-sourcing-policies

7. Kovtoniuk K. V. (2019). Tsyfrovizatsiia svitovoi ekonomiky yak faktor ekonomichnoho zrostannia [Digitization of the world economy as a factor of economic growth]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. – Scientific Bulletin of Kherson State University*. V. 27. 1. 29–33. [in Ukrainian].

8. British Computer Society (2013). The Digital Economy. Retrieved from: https://policy.bcs.org/position_statements/digital-econonomy

9. Chmeruk G.G., Storozhenko O.O. (2019). Tsyfrova transformatsiia yak nova forma transformatsii finansovykh vidnosyn subiektiv hospodariuvannia. [Digital transformation as a new form of transformation of financial relations of business entities]. *Visnyk ONU imeni I. I. Mechnykova. – Bulletin of ONU named after I. I. Mechnikova,* 24, 4(77) [in Ukrainian].

10. Koval'chuk, K. F., Bandorina, L. M. & Udachyna, K. O. (2018). Tsyfrova ekonomika – ekonomika KhKhI stolittia. [Digital economy – economy of the 21st century]. *Tsyfrova ekonomika* : zb. materialiv Natsionalnoi nauk.-metod. konf., 4–5 zhovtnia 2018 r., m. Kyiv. KNEU. – *Digital economy :* materials national sciences. Kiev : KNEU, 185–188 [in Ukrainian].

УДК 343.1
DOI https://doi.org/10.32689/2522-4603.2023.3.6

Андрій ГРЕКУ
аспірант Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, 03039, filippboitsov@protonmail.com
ORCID: 0009-0006-5645-7618

Andrii HREKU
Postgraduate Student at the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine, 03039, filippboitsov@protonmail.com
ORCID: 0009-0006-5645-7618

ЗАСАДИ СПРАВЕДЛИВОСТІ У СУДОЧИНСТВІ

PRINCIPLES OF JUSTICE IN JUDICIARY

Кожна країна повинна гарантувати, на законодавчому рівні, основні засади справедливого судочинства. Адже людські права та свободи не повинні порушуватись. Вони потребують особливого захисту та гарантій. Хто, як не держава забезпечує кожному законність рішень судових органів та відповідність їх національним та міжнародним нормам. Судочинство повинно проходити враховуючи правила моралі у суспільстві.

Через збройну агресію росії та вторгнення її на територію України, часто зустрічаємо порушення загальних засад справедливості. Ця нагальна проблема потребує дослідження та розв'язання. Воєнний стан не повинен впливати на судовий процес. Законодавство має працювати таким чином, щоб не порушувати людські права та врегулювати роботу судів, не зважаючи на зовнішні фактори та ризики.

Актуальним виступає вивчення вітчизняної теоретико-правової та міжнародної наукової літератури, для аналізу та дослідження фундаменту здійснення правосуддя в нашій державі.

***Мета.** Метою статті є теоретичний аналіз джерельної бази та виокремлення основних засад справедливості у судочинстві.*

***Матеріали і методи.** Матеріалами вивчення є: законодавча міжнародна та національна нормотворча база та наукові здобутки вчених та їх дослідження. При проведенні наукового аналізу застосовано загальнонаукові та спеціальні методи. Особливе місце відводиться юридичному методу. Застосовано метод аналізу, при вивченні наукової літератури. Також зустрічається порівняння, структурно-функціональний метод та прогнозування.*

***Результати.** У результаті теоретичного та правового аналізу проаналізовані нормативно правові джерела та праці вчених, структуровано науковий матеріал, запропоновано авторські пропозиції, щодо класифікації основних засад справедливого судочинства і рекомендації про вивчення позитивного міжнародного досвіду та застосування його в Україні.*

***Перспективи.** Правовий та теоретичний аналіз та дослідження наукового та правового джерельного фундаменту, з питань захисту основних засад справедливого судочинства, надає змогу, з'ясувати основні проблеми сьогодення та дослідити їх в майбутньому на глобальному рівні та застосувати авторські пропозиції в практичній діяльності.*

***Ключові слова:** справедливе судочинство, джерельна база, основні засади, судові рішення, теоретико-правове дослідження, норми закону, норми моралі.*

Each country must guarantee, at the legislative level, the basic principles of a fair trial. After all, human rights and freedoms should not be violated. They need special protection and guarantees. Who, if not the state, ensures everyone the legality of the decisions of judicial bodies and their compliance with national and international norms. Judicial proceedings must take into account the rules of morality in society.

Because of Russia's armed aggression and its invasion of the territory of Ukraine, we often encounter violations of the general principles of justice. This urgent problem needs to be investigated and solved. Martial law should not affect the judicial process. Legislation should work in a way that does not violate human rights and regulate the work of courts, regardless of external factors and risks.

The study of domestic theoretical-legal and international scientific literature is relevant for the analysis and research of the foundation of the administration of justice in our country.

***Purpose.** The purpose of the article is the theoretical analysis of the source base and the identification of the main principles of justice in judicial proceedings.*

***Materials and methods.** The study materials are: legislative, international and national normative base and scientific achievements of scientists and their research. General scientific and special methods were used during the scientific analysis. A special place is given to the legal method. The method of analysis is applied when studying scientific literature. Comparison, structural-functional method and forecasting are also found.*

***Results.** As a result of the theoretical and legal analysis, the normative legal sources and works of scientists were analyzed, the scientific material was structured, the author's proposals were proposed, regarding the classification*

© Греку А., 2023

of the main principles of a fair trial and recommendations on the study of positive international experience and its application in Ukraine.

***Discussion**. Legal and theoretical analysis and research of the scientific and legal source foundation, on issues of protection of the basic principles of fair justice, makes it possible to find out the main problems of the present and to investigate them in the future at the global level and to apply the author's proposals in practical activities.*

***Key words:** fair justice, source base, basic principles, court decisions, theoretical and legal research, norms of the law, norms of morality.*

Постановка проблеми. Засади справедливості у судочинстві є гарантією демократичності судового процесу та розвиненої правової держави. На сьогодні, через воєнне вторгнення росії на територію України, основні загальні принципи міжнародного та національного законодавства можуть порушуватись.

У нормотворчій діяльності є значні прогалини, адже на практиці через відсутність електроенергії, зв'язку особи не можуть бути присутніми на судових засіданнях навіть в онлайн режимі. Звичайно, з розвитком інтернет-технологій, можна звертатися до суду з проханням підключення відеозв'язку, але дуже часто працівники суду не ідуть на зустріч, через особисте небажання, або відсутність технічних засобів. У такому випадку порушуються основні засади справедливості судового процесу, що є величезною проблемою сьогодення.

Це звичайно суперечить міжнародному законодавству, адже кожна людина має право на доступ до судового засідання. Вважаємо, що необхідно проаналізувати зарубіжний досвід та підлаштувати законодавство України під воєнний час. Було б доречно залучати міжнародну спільноту для обміну досвідом.

Аналіз останніх досліджень і публікацій. Науковою та правовою джерельною базою є законодавство та теоретичний матеріал, таких вчених як, В. Котюк [4], О. Кучинська [5], Г. Мамка [6], N. Bondar [12], Л. Сердюк [7], D. Chyzhov [13], S.Zhdanenko [14], O. Skrypniuk [15].

Проаналізовані основні міжнародні та національні акти, а саме: ЗДПЛ [2], Європейської конвенції 1950 року [11], Конституція України [3], Закон України № 2469-VIII [9], Закон України № 2206-VIII [9], Конвенція 1989 року [10].

При написанні статті використано юридичні методи, метод аналізу, системний метод, статистичний метод, структурно-функціональний метод, історичний метод, метод порівняння тощо.

Формулювання цілей статті (постановка завдання). Метою статті є вивчення і дослідження джерельної бази та виокремлення основних засад справедливості у судочинстві. Основним завданням є теоретико-правовий аналіз зарубіжної та вітчизняної наукової літератури та внесення авторських пропозицій, щодо власної загальної класифікації та програми щодо дотримання засад справедливого судочинства в умовах воєнного стану.

Виклад основного матеріалу. Судовий процес в Україні повинен здійснюватись на засадах справедливості, враховуючи вітчизняні та зарубіжні норми. В умовах воєнного стану судочинство в Україні має проходити в безпечних умовах. Закон № 2469-VIII від 31 березня 2023 року нормативно закріпив основні положення безпеки в країні [9]. ЗДПЛ [2] та Європейська конвенція 1950 року [11], на міжнародному рівні закріплюють гарантії захисту людських прав та гарантують кожному захист основних свобод.

Через воєнні дії дуже часто порушуються основні засади справедливості судочинства, що є нагальною ключовою проблемою сьогодення. Доступ до судового засідання кожного учасника гарантується і на міжнародному і на національному рівні, а саме Конституцією України, вважаємо що на державному рівні повинні бути закріплені додаткові гарантії справедливого судочинства.

Неможливо не погодитись з Чижов Д., який зазначає що кожна країна повинна гарантувати безпеку своєму населенню. Погоджуємось з його думкою, що нормотворчість має працювати таким чином на загальному рівні, щоб не порушувати людські свободи та права [13, с. 101].

С. Жданенко та О. Дзьобан також досліджують безпеку суспільства [14, с. 15]. Дійсно судочинство повинно проходити у безпечних умовах, це сприятиме здоровому підходу щодо моральності прийняття рішень. Тому держава повинна забезпечувати безпеку судового процесу, врахувавши на законодавчому рівні всі ризики.

В. О. Котюк вказує, що термін справедливість пов'язаний саме з правом та є фундаментом демократичності та свободи. Справедливість характеризується загальністю та державним і громадським характером. Мораль характеризується суспільними уявленнями про справедливість, добро та зло [4, с. 20; 5, с. 2]. Судді, при винесені рішень, та законотворці, під час створення нормативно-правових актів, обов'язково повинні враховувати норми справедливості.

Слушно підкреслити, що Г. М. Мамка, проводячи дослідження категорії справедливості у судочинстві з кримінальних справ, наголо-

шує, що важливими є саме загальні засади. Він досліджував нормативно-правові акти зарубіжних країн і судову практику з захисту людських прав Європейського суду. Справедливість, на думку науковця, є загальним принципом і може регулювати будь-яку галузь вітчизняного права, у тому числі і кримінального [6, с. 123].

Г. М. Мамка пропонує закріпити принцип справедливості у кримінальному законодавстві окремо [6, с. 123]. Вважаємо, що дана пропозиція є актуальною та важливою і потребує подальшого аналізу та вивчення в майбутньому. На нашу думку, поняття справедливості є загальною, широкою категорією. Зазначена засада повинна закріплюватись, як окремо, так і в кожній галузі національного права.

О. А. Кучинська також пропонує розширення КПК статтею, яка розкривала б основні засади справедливості судочинства у кримінальних справах. Рішення суду повинні відповідати Конституції та не порушувати права людини на міжнародному рівні. Способи впливу на порушників повинні відповідати ступеням небезпечності та бути законними [5, с. 10].

Закон № 1402-VIII від 02.06.2016 гарантує кожному справедливий суд. При його написанні враховувались міжнародні стандарти [10]. Цей нормативно-правовий акт є гарантом справедливого судочинства в Україні. Тому його важливість є значною та він виступає як фундамент регулювання нормотворчої діяльності у цій галузі.

На нормативному рівні закріплено, що правосуддя відбувається на засадах справедливості та верховенства права. На законодавчому рівні забезпечується кожному право на справедливість судового процесу та повагу до його учасників. Відповідно до законодавства кожен має право на доступність судочинства [3]. Іноземцям, юридичним особам, як і громадянам України, а також особам без громадянства, гарантується право захисту своїх прав [10]. Це, також, важливе положення, яке не може бути без уваги.

Н. Оніщенко стверджує, що свобода пов'язується з загальним принципом справедливості [8, с. 56–58]. Погоджуємося з його думкою, адже права та свободи гарантуються на міжнародному рівні.

Слушно підкреслити, що N.A. Bondar у своїх наукових працях, відмічає, що у вітчизняному законодавстві фундаментом захисту людських свобод та прав є справедливий судовий розгляд [12, с. 27]. Основна, загальна засада справедливого судочинства, доречно, виокремлена вченим.

Сьогодні, через воєнні дії на практиці, на жаль, порушуються загальні засади справедливого судочинства. Наприклад, доступ до судового засідання кожного учасника гарантується, як міжнародними, так і державними нормативно-правовими актами. На національному рівні основним є саме Конституція України.

Вважаємо що на державному рівні повинні бути закріплені додаткові гарантії доступності та роз'яснення працівникам суду щодо необхідності проведення онлайн засідань та забезпечення установ суду всім необхідним технологічно. Обмін зарубіжного досвіду дасть змогу обрати перспективний шлях розвитку судової системи нашої держави.

Вважаємо, що для запобігання порушенням людських прав у судовому процесі, а саме його справедливості, необхідно зафіксувати алгоритм послідовної процедури, під час воєнних дій, взявши до уваги проблемні аспекти, ризики зовнішнього та внутрішнього характеру. Актуальним та важливим буде, на державному рівні, залучення працівників суду з інших держав, для обміну інформацією.

Вчений Сердюк Л. стверджує, що в сучасному вітчизняному законодавстві важливо конкретно виділити випадки обмеження людських свобод та прав [5, с. 271]. Вважаємо, що нормотворча діяльність повинна будуватися таким чином, щоб уникнути таких ситуацій.

На нашу думку, актуальною буде авторська програма, щодо дотримання засад справедливого судочинства в умовах воєнного стану, адже сьогодні, під час здійснення судочинства, зустрічається безліч проблем. Виокремлена мета цієї програми та шляхи застосування зазначених положень в практичній діяльності (табл. 1).

Авторська розробка, у вигляді програми потребує подальшого аналізу, вивчення та доповнення в майбутньому і є актуальною та важливою сьогодні. Адже, через воєнне вторгнення росії на територію України, суспільство має безліч проблем, які необхідно вирішувати ефективно.

Провівши аналіз та узагальнивши джерельну базу доречно в майбутньому далі досліджувати проблемні аспекти. Слушно зазначити, що гарантії справедливого судочинства повинні надаватись на державному рівні. Це відкриває можливість розв'язати ключові проблеми сучасності як в Україні, так і в інших державах, тому важливим є обмін досвіду між країнами.

Висновки і перспективи подальших досліджень. У результаті теоретичного та правового аналізу наукової літератури та законодавства, проаналізовані нормативно правові джерела та праці вчених, узагальнено науковий

Таблиця 1

Програма дотримання засад справедливого судочинства в умовах воєнного стану

№ пп	Мета програми	Застосування на практиці
1	Теоретичне вивчення засад справедливості та виокремлення основних складових: доступності, демократизму, моральності, законності, дослідження зарубіжної практики.	Запропоновано пов'язати справедливість судочинства з моральністю та в науковій літературі виокремити загальні складові.
2	Спеціальна процедура, впровадження засад справедливого судочинства на практиці	Анкетування учасників судового процесу для проведення статистики щодо порушення людських прав.
3	Узагальнення спеціальних правил для ведення справедливого судочинства.	Роз'яснення учасникам судового процесу їхніх прав та свобод. Підвищення кваліфікації працівників суду щодо справедливого судочинства.
4	Вирішення проблеми справедливого судочинства у воєнний час	Удосконалення законотворчості, поліпшення обізнаності суспільства.

** Джерело: авторська розробка на основі теоретичного аналізу наукових джерел*

матеріал, запропоновано авторські пропозиції, щодо класифікації основних засад справедливого судочинства, а саме: доступності, демократизму, моральності, законності, та наведена авторська програма, щодо дотримання засад справедливого судочинства в умовах воєнного стану.

Вказано на необхідності аналізу зарубіжного досвіду та підлаштування законодавства України під воєнний час. Було б доречно залучати міжнародну спільноту для обміну досвідом. Рекомендовано детальне вивчення позитивного міжнародного досвіду та застосування його в Україні.

Правовий та теоретичний аналіз та дослідження наукового та правового джерельного фундаменту, з питань захисту основних засад справедливого судочинства, надає змогу з'ясувати основні проблеми сьогодення та дослідити їх в майбутньому на глобальному рівні та продовжити удосконалювати авторську програму для застосування на практиці.

Література:

1. Бисага Ю. М., Палінчак М. М., Бєлов Д. М., Данканич М. М. Основні права людини [Електронний ресурс]. Ужгород: Ліра, 2003. 66 с. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/5101/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%20%D0%BF%D1%80%D0%B0%D0%B2%D0%B0.pdf

2. Загальна декларація прав людини 10 грудня 1948 року [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

3. Конституція України від 26 червня 1996 року. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

4. Котюк В. О. Основи держава і права : навч. посіб.. 3-є вид., доп. і перероб. К. : Атіка, 2001. 432с.

5. Кучинська О. А. Зміст принципу справедливості у кримінальному судочинстві України [Електронний ресурс]. *Часопис Національного університету «Острозька академія». Серія «Право»,* 2011. № 1(3). URL: https://lj.oa.edu.ua/articles/2011/n1/11koaksu.pdf

6. Мамка Г. М. Справедливість як категорія та засада кримінального провадження [Електронний ресурс]. *Науковий вісник Ужгородського Національного університету. Серія : Право*. Ужгород : «Гельветика», 2018. Т. 2. Вип. 48. С. 120–123. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34432/1/%D0%A1%D0%9F%D0%A0%D0%90%D0%92%D0%95%D0%94%D0%9B%D0%98%D0%92%D0%86%D0%A1%D0%A2%D0%AC%20%D0%AF%D0%9A%20%D0%9A%D0%90%D0%A2%D0%95%D0%93%D0%9E%D0%A0%D0%86%D0%AF%20%D0%A2%D0%90%20%D0%97%D0%90%D0%A1%D0%90%D0%94%D0%98.pdf

7. Сердюк Л. Законодавчо визначені підстави правомірного обмеження конституційних прав і свобод людини в умовах воєнного стану [Електронний ресурс]. *Науковий вісник Дніпропетровського державного університету внутрішніх справ,* 2022. № 2. С. 269–272. URL: 10.31733/2078-3566-2022-6-269-272

8. Оніщенко Н. М. Правова система і держава в Україні. К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2002. 132 с.

9. Про національну безпеку України. Закон України № 2469-VIII від 31.03.2023. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

10. Про судоустрій і статус суддів № 1402-VIII від 02.06.2016 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text

11. Про права людини (Конвенція). 1950. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

12. Bondar N. A., Mishchenko's M. S. Freedom as a legal value: nature and features. *Analytical and Comparative Jurisprudence*, 2023. 26–30. DOI: 10.24144/2788-6018.2023.05.3

13. Chyzhov D. Organizational and legal support of human rights and freedoms in the national security of Ukraine. *Entrepreneurship, Economy and Law*, 2021. 7, 98–103. URL: http://pgp-journal.kiev.ua/archive/2021/7/16.pdf

14. Dzioban, O. P., Zhdanenko, S. B. Prava liudyny i natsionalna bezpeka: filosofsko-pravovi aspekty vzaiemozviazku. *Human rights and national security: philosophical and legal aspects of the relationship,* 2020. 9–22.

15. Skrypniuk O., Tokarchuk L. Protection of children's rights and interests under war conditions in the east of Ukraine and in the annexed Crimea Republic: new challenges for Ukraine. July 2020. ScienceRise Juridical Science.

References:

1. Bysaga Y. M., Palinchak M. M., Belov D. M., Dankanych M. M. Fundamental human rights. (2003). Uzhgorod: Lira, 66. Retrieved from https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/5101/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%20%D0%BF%D1%80%D0%B0%D0%B2%D0%B0.pdf (access date: 23.02.2024).

2. Universal Declaration of Human Rights (1948). Retrieved from https://zakon.rada.gov.ua/laws/show/995_015 (date of application: 25.02.24).

3. Constitution of Ukraine of June 26, 1996. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (access date: 24.02.2024).

4. Kotyuk V. O. (2001). Fundamentals of the state and law: education. manual. 3rd ed., add. and processing. K. : Atika. 432.

5. Kuchynska O. A. (2011). Content of the principle of justice in the criminal justice system of Ukraine. *Journal of the National University "Ostrozka Academy". "Law" series*, 1(3). Retrieved from https://lj.oa.edu.ua/articles/2011/n1/11koaksu.pdf (date of application: 25.02.24).

6. Mamka G. M. (2018). Justice as a category and basis of criminal proceedings. *Scientific Bulletin of the Uzhgorod National University: series: Law*, 2.48. 120–123. Retrieved from https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34432/1/%D0%A1%D0%9F%D0%A0%D0%90%D0%92%D0%95%D0%94%D0%9B%D0%98%D0%92%D0%86%D0%A1%D0%A2%D0%AC%20%D0%AF%D0%9A%20%D0%9A%D0%90%D0%A2%D0%95%D0%93%D0%9E%D0%A0%D0%86%D0%AF%20%D0%A2%D0%90%20%D0%97%D0%90%D0%A1%D0%90%D0%94%D0%98.pdf (access date: 22.02.2024).

7. Serdyuk L. (2022). Legislatedly defined grounds for lawful restriction of constitutional rights and freedoms of a person in the conditions of martial law. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs, Special Issue* No. 2, 269–272. DOI: 10.31733/2078-3566-2022-6-269-272 (access date: 22.02.2024).

8. Onishchenko N. M. (2002). Legal system and state in Ukraine. *Institute of State and Law named after V. M. Koretsky National Academy of Sciences of Ukraine*, 132.

9. On the national security of Ukraine. Law of Ukraine No. 2469-VIII dated March 31, 2023. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text (access date: 23.02.2024).

10. Pro Laws in Supplementary Status. (Law of Ukraine). No 1402-VIII dated 02.06.2016. Retrieved from https://zakon.rada.gov.ua/laws/show/1402-19#Text (access date: 23.02.2024).

11. European Convention on the Protection of Rights and Fundamental Freedoms (1950). Retrieved from https://zakon. rada.gov.ua/laws/show/995_004 (date of application: 18.01.24).

12. Bondar N. A., Mishchenko's M.S. (2023). Freedom as a legal value: nature and features. *Analytical and Comparative Jurisprudence,* 26–30. DOI: 10.24144/2788-6018.2023.05.3 (date of access: 22.02.2024).

13. Chyzhov D. (2021). Organizational and legal support of human rights and freedoms in the national security of Ukraine. *Entrepreneurship, Economy and Law,* 7, 98–103. Retrieved from http://pgp-journal.kiev.ua/archive/2021/7/16.pdf (access date: 23.02.2024).

14. Dzioban, O. P., Zhdanenko, S. B. (2020). Prava liudyny i natsionalna bezpeka: filosofsko-pravovi aspekty vzaiemozviazku. *Human rights and national security: philosophical and legal aspects of the relationship,* 9–22.

15. Skrypniuk O., Tokarchuk L. Protection of children's rights and interests under war conditions in the east of Ukraine and in the annexed Crimea Republic: new challenges for Ukraine. July 2020. ScienceRise Juridical Science.

УДК 343.1:004
DOI https://doi.org/10.32689/2522-4603.2023.3.7

Володимир ПОЛІЩУК
аспірант Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, 03039, Polishchuk.Volodymyr.20@proton.me
ORCID: 0009-0002-2642-9326

Volodymyr POLISHCHUK
Postgraduate Student at the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine, 03039, Polishchuk.Volodymyr.20@proton.me
ORCID: 0009-0002-2642-9326

КІБЕРЗЛОЧИНИ ТА КІБЕРБЕЗПЕКА: БОРОТЬБА З КОМП'ЮТЕРНИМИ ЗЛОЧИНАМИ І КІБЕРАТАКАМИ

CYBERCRIMES AND CYBER SECURITY: COMBATING COMPUTER CRIMES AND CYBERATTACKS

Анотація. *Дана робота досліджує різні типи кіберзлочинів та їхні особливості, а також методи та інструменти, які використовуються кіберзлочинцями, а також заходи, які можна вжити для захисту від кіберзлочинів; роль правоохоронних органів та міжнародної співпраці у боротьбі з кіберзлочинністю. Автор розглядає актуальні тенденції та прогнози розвитку кіберзлочинності в Україні та міжнародний досвід боротьби із кіберзлочинами.*

У роботі зроблена спроба ознайомитися з розвитком нових форм вчинення кіберзлочинів у контексті історичного розвитку.

Кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці. Кіберзлочинці часто ховаються за анонімністю, що ускладнює їх ідентифікацію та притягнення до відповідальності. Законодавство у сфері кіберзлочинності постійно еволюціонує, адже не завжди встигає за темпами розвитку нових технологій. Важливо зазначити, що кіберзлочинність є серйозною загрозою для суспільства, тому необхідні спільні зусилля держави, приватного сектору та громадян для її подолання.

Боротьба з кіберзлочинністю та забезпечення кібербезпеки – одна із найактуальніших проблем сьогодення. Це питання, яке потребує комплексного підходу, що містить як правові, так і технічні аспекти.

Очікуваними результатами роботи є:

– Визначення та систематизація основних понять кіберзлочинності та кібербезпеки.

– Розробка типології кіберзлочинів.

– Узагальнення та аналіз методів та інструментів кіберзахисту.

– Визначення шляхів удосконалення діяльності правоохоронних органів у сфері боротьби з кіберзлочинністю.

– Обґрунтування рекомендацій щодо розвитку кібербезпеки.

– Результати дослідження можуть бути використані для розробки та вдосконалення політики кібербезпеки на державному та приватному рівні.

Розслідування кібератак як воєнних злочинів може допомогти притягнути винних до відповідальності, а також запобігти подібним злочинам у майбутньому.

Ключові слова: *кіберзлочинність, кібербезпека, комп'ютерні злочини, кібератаки, шахрайство, крадіжка особистих даних, шпигунство, критична інфраструктура, захист інформації, правоохоронні органи, міжнародна співпраця.*

Abstract. *This paper examines the different types of cybercrimes and their characteristics, as well as the methods and tools used by cybercriminals, as well as measures that can be taken to protect against cybercrimes; the role of law enforcement agencies and international cooperation in the fight against cybercrime. The author examines current trends and forecasts of the development of cybercrime in Ukraine and international experience in combating cybercrime.*

The work attempts to familiarize with the development of new forms of committing cybercrimes in the context of historical development.

Cybercrimes are often difficult to investigate due to a lack of skilled personnel, necessary tools and international cooperation. Cybercriminals often hide behind anonymity, making it difficult to identify and prosecute them. Legislation in the field of cybercrime is constantly evolving, because it does not always keep up with the pace of development of new technologies. It is important to note that cybercrime is a serious threat to society, therefore joint efforts of the state, private sector and citizens are necessary to overcome it.

Fighting cybercrime and ensuring cyber security is one of the most urgent problems today. This is an issue that requires a comprehensive approach that includes both legal and technical aspects.

© Поліщук В., 2023

The expected results of the work are:
– Definition and systematization of the main concepts of cybercrime and cyber security.
– Development of a typology of cybercrimes.
– Generalization and analysis of cyber protection methods and tools.
– Determination of ways to improve the activities of law enforcement agencies in the field of combating cybercrime.
– Justification of recommendations for the development of cyber security.
– Research results can be used to develop and improve cyber security policy at the state and private level.
Investigating cyber-attacks as war crimes can help bring perpetrators to justice and prevent similar crimes in the future.
Key words: *cyber-crime, cyber security, computer crimes, cyber-attacks, fraud, identity theft, espionage, critical infrastructure, information protection, law enforcement, international cooperation.*

Постановка проблеми. У сучасному світі, де все більше аспектів життя переходить в онлайн, кіберзлочинність та кібербезпека стають актуальними питаннями.

Згідно з даними ФБР, у 2022 році зареєстровано 800 944 скарги на кіберзлочинність. Це означає, щонайменше 422 мільйони людей постраждали від цього негативного явища. У 2023 році зламано майже 33 мільярди облікових записів [1], вартість яких оцінено у 8 трильйонів доларів. Кіберзлочинність – індустрія злочинців, яка коштує трильйони доларів, і 43% атак спрямовані на малий і середній бізнес. Протягом останніх двадцяти років, у період з 2001 по 2021 роки кіберзлочинність забрала щонайменше 6,5 мільйонів жертв. За цей самий період сума збитків склала майже 26 мільярдів доларів.

На думку експертів видання Cybercrime Magazine у наступні п’ять років витрати від кіберзлочинності зростуть на 15% і до 2025 року досягнуть 10,5 трлн. Програми-вимагачі щороку коштують своїм жертвам близько 265 мільярдів доларів США [4]. 80% зареєстрованих кіберзлочинів зазвичай пов’язані з фішинговими атаками в технологічному секторі. Це значна проблема, яка потребує негайного вирішення спільними зусиллями, оскільки кіберзлочини, такі як шахрайство, крадіжка особистих даних, шпигунство та атаки на критичну інфраструктуру, можуть мати значні наслідки як для окремих осіб, так і для цілих організацій та держав.

Мета роботи – дослідження проблем кіберзлочинності та кібербезпеки, а також аналіз шляхів боротьби з комп'ютерними злочинами й кібератаками.

Для досягнення мети роботи передбачається вирішити наступні завдання:

– проаналізувати типи та особливості кіберзлочинів;

– розглянути методи та інструменти кіберзахисту;

– визначити актуальні проблеми та перспективи розвитку кібербезпеки.

Кіберзлочинність постійно змінюється, постійно виникають нові типи злочинів та використовуються нові технології. Загалом цей процес можна поділити на кілька етапів розвитку. На початку шістдесятих з'являються перші комп'ютерні мережі, що дає поштовх до розвитку кіберзлочинності. Саме тоді почалися і перші випадки крадіжки даних та комп'ютерних програм. У вісімдесятих набули поширення персональні комп'ютери та Інтернет. І у цей період з'являються перші кіберзлочинні групи, які використовують кібершантажу та викрадення даних. У 1990-ті відбулося стрімке зростання кіберзлочинності, перші масштабні кібератаки. З'являються нові типи кіберзлочинів [2]. На початку 2020 спостерігається різке зростання кількості кібератак на державні органи та приватні компанії. Кібербезпека стає одним з пріоритетів національної безпеки. Кіберзлочинність стає все більш витонченою та складною. Зростає кількості кібератак на штучний інтелект та інші нові технології.

Перше покоління кіберзлочинів включає атаки, спрямовані на комп’ютери, комп’ютерні мережі та дані.

Друге покоління пов'язане з розвитком IT-мереж і атаками хакерів на їх цілісність і доступність.

Третє покоління пов'язане з помітним процесом автоматизації кіберзлочинності, що є, в тому числі результатом використання спеціального програмного забезпечення[3].

Нове покоління кіберзлочинів не вчиняється особисто та безпосередньо злочинцями, а є результатом автоматизованих атак з використанням програмного забезпечення, створеного для цієї мети.

Разом з тим, намагаючись постійно розв'язувати проблеми кібератак, фахівці розробили сучасні методи кіберзахисту, до яких відносять:

1. Запобігання кібератакам шляхом впровадження відповідних заходів безпеки.

2. Своєчасне виявлення кібератак для мінімізації їхніх наслідків.

3. Заходи для нейтралізації кібератак та відновлення роботи систем.

Серед інструментів кіберзахисту найчастіше використовують антивірусне програмне забезпечення, яке захищає комп'ютерні системи від

вірусів, шпигунських програм та інших шкідливих програм [5]. Брандмауер – теж один з інструментів захисту, який блокує несанкціонований доступ до комп'ютерних систем.

Системи запобігання вторгненням блокують підозрілу активність у комп'ютерних мережах [5]. Метод шифрування захищає дані від несанкціонованого доступу через використання спеціальних шифрів та обмежує доступ до комп'ютерних систем та даних. Не варто забувати й про підвищення обізнаності користувачів щодо ризиків кіберзлочинності, які спрямовані на захист себе від них [5]. Враховуючи загрози сьогодення важливо використовувати комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти. Зважаючи на ряд актуальних проблем кібербезпеки можемо виділити наступне:

Кіберзлочинці постійно вдосконалюють свої методи, що робить кібератаки все більш складними для виявлення та нейтралізації [6].

Існує гостра нестача фахівців з кібербезпеки, що ускладнює захист організацій від кібератак.

Різні організації та країни мають різні підходи до кібербезпеки, що ускладнює міжнародну співпрацю [7].

Зростання залежності від Інтернету робить суспільство більш вразливим до кібератак.

Кіберзлочинність постійно еволюціонує, з'являються нові типи кіберзлочинів, що потребує постійного вдосконалення методів боротьби з ними [8].

Штучний інтелект може допомогти у виявленні та нейтралізації кібератак. Зростання обізнаності про кібербезпеку допоможе людям краще захищати себе від кіберзлочинності. Рухаючись у напрямі міжнародної співпраці кожна країна може допомогти собі у боротьбі з транснаціональною кіберзлочинністю. Вдосконалення законодавства сприятиме забезпеченню ефективного розслідування та переслідування злочинців [9].

Висновки. Кібератаки стають все більш витонченими та складними, що робить кібербезпеку критично важливою. Ефективна боротьба з кіберзлочинністю потребує співпраці між державами, приватним сектором та громадянами. Необхідно постійно вдосконалювати методи кібербезпеки, використовуючи нові технології та підвищуючи обізнаність. Важливо розробити міжнародні стандарти та законодавство для боротьби з транснаціональною кіберзлочинністю. Майбутнє кібербезпеки залежить від здатності різних зацікавлених сторін працювати разом для захисту інформаційних систем та даних.

Література:

1. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал.* 2012. № 12. С. 409–414.

2. Музика В. В. Атрибуція кібератак проти об’єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення : дис. … д-ра філософії : 081 / Нац. ун-т. «Одеська юридична академія». Одеса, 2021. 219 с.

3. Фещуков Г. В. Застосування МГП по відношенню до кібероперацій, що проводяться під час збройних конфліктів. *Юридичний науковий електронний журнал*. 2023. № 9. С. 437–439.

4. Geers K. Strategic cyber security : Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.

5. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris : веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/ (дата звернення: 25.02.2024).

6. The Prosecutor’s New Policy on ‘Cyber Operations’ before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law: веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (дата звернення: 25.02.2024).

7. Information for victims. International Criminal Court : веб-сайт. URL: https://www.icc-cpi.int/victims/ukraine (дата звернення: 25.02.2024).

8. Римський статут Міжнародного кримінального суду. *Міністерство юстиції України* : веб-сайт. URL: https://minjust.gov.ua/m/ mijnarodniy-kriminalniy-sud (дата звернення: 25.02.2024).

9. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. – Cambridge University Press (дата звернення: 25.02.2024).

References:

1. Yurtayeva, K. V. (2012). Kryminal′na vidpovidal′nist′ za kiberzlochyny, vchyneni pid chas zbroynoho konfliktu: mizhnarodni tendentsiyi ta ukrayins′ki realiyi [Criminal liability for cybercrimes committed during armed conflict: international trends and Ukrainian realities]. *Yurydychnyy naukovyy elektronnyy zhurnal – Legal scientific electronic journal,* 12, 409–414.

2. Music, V. V. (202). Atrybutsiya kiberatak proty ob″yektiv krytychnoyi infrastruktury: vyznachennya osnovnykh problem ta shlyakhiv yikh vyrishennya : dys. … d-ra filosofiyi : 081 [Attribution of cyber attacks against critical infrastructure objects: definition of the main problems and ways to solve them: diss. ... doctor of philosophy: 081]. *Nats. un-t. «Odes'ka yurydychna akademiya». Odesa – Nat. Univ. "Odesa Law Academy". Odesa*, 219.

3. Feshchukov, G. V. (2023). Zastosuvannya MHP po vidnoshennyu do kiberoperatsiy, shcho provodyat′sya pid chas zbroynykh konfliktiv [Application of IHL in relation to cyber operations conducted during armed conflicts]. *Yurydychnyy naukovyy elektronnyy zhurnal – Legal scientific electronic journal*, 9, 437–439.

4. Geers, K. (2011). Strategic cyber security: Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 169.

5. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris : Website. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/ (access date: 02/25/2024).

6. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law: website. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (date application: 25.02.2024).

7. Information for victims. International Criminal Court : website. URL: https://www.icc-cpi.int/victims/ukraine (access date: 25.02.2024).

8. Ryms′kyy statut Mizhnarodnoho kryminal′noho sudu [Rome Statute of the International Criminal Court]. *Ministerstvo yustytsiyi Ukrayiny: veb-sayt – Ministry of Justice of Ukraine: website.* URL: https://minjust.gov.ua/m/ mijnarodniy-kriminalniy-sud (date of application: 02/25/2024).

9. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. Cambridge University Press (access date: 25.02.2024).

Наукове видання

НАУКОВІ ПРАЦІ МІЖРЕГІОНАЛЬНОЇ АКАДЕМІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ

ЮРИДИЧНІ НАУКИ

Випуск 3 (66), 2023

Засновано 2001 року
Видання виходить 6 разів на рік

Коректор *В. І. Вишнякова*
Комп'ютерне верстання *А. О. Марєєва*

Підписано до друку 18.10.2023 р. Замовлення № 0124/096.
Формат 60×84/8. Гарнітура Times New Roman.
Папір офсет. Цифровий друк. Ум. друк. арк. 5,58.
Наклад 100 прим.

Надруковано: Видавничий дім "Гельветика"
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022 р.