ISSN 2308-0361



# СУЧАСНІ ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ

**Ольга Бакалінська,**
*доктор юридичних наук, професор,*
*старший науковий співробітник*
*відділу промислової власності*
*НДІ інтелектуальної власності НАПрН України*
*ORCID ID: 0000-0002-1092-0914*

Каталізатором змін у сфері кібербезпеки в нашій державі стала розв'язана російською федерацією гібридна війна із застосуванням як класичної, так і нелетальної зброї в кіберпросторі. Кібервійна в Україні виявила неефективність чинного міжнародно-правового механізму стримування. Найважливішим аспектом розвитку міжнародного гуманітарного права є формування сучасних принципів протидії недружнім діям агресорів у кіберпросторі.

Заохочення інноваційної діяльності та захист правовласників від кіберзагроз є основним напрямом державних (національних) стратегій інтелектуальної власності. Кібербезпека запобігає порушенню прав інтелектуальної власності. Саме ефективна державна позиція в цій сфері забезпечить швидке відновлення нашої держави після завершення війни.

*Ключові слова:* інформаційна безпека, кіберпростір, кібербезпека, інтелектуальна власність

Нові цифрові технології та глобальні інформаційні мережі, які здійснили справжню революцію у сфері накопичення та обміну інформацією, потребують фундаментальних змін у підходах та принципах захисту прав інтелектуальної власності, що створювалася в зовсім інших технологічних і світоглядних умовах. Глобальне середовище Інтернету та розвиток інформаційно-комунікаційних технологій потребують адекватного регулювання відносин із використанням інтелектуальної власності. Нові реалії сучасних ІТ-технологій та Інтернету, отримані знання у сфері біотехнологій та фармакології ставлять нові завдання, до виконання яких традиційний механізм захисту прав інтелектуальної власності не завжди пристосований.

Глобалізація та європеїзація українського законодавства, формування нової світоглядної моделі розвитку нашої держави, а також розвиток нових технологій та глобальних мереж зумовив зростання реального значення інтелектуальної власності та пришвидшення процесів її комерціалізації, підвищення значення комерційного аспекту використання та інвестиційної привабливості прав інтелектуальної власності, застосування виняткових прав інтелектуальної власності як інструменту конкурентної боротьби.

**Аналіз останніх досліджень і публікацій.** Дослідження цієї пробле-

ми можна розпочати з термінології, започаткованої в міжнародному стандарті ISO/IEC 27032:2012. Серед наукових здобутків варто виділити праці А. Алпеєва, О. Архіпова, Я. Чепуренко, В. Мохора, О. Бакалинського. О. Богданова, В. Грибуніна, О. Горбатько. Напрями розвитку кібербезпеки були описані В. Лєбєдєвим, Д. Огородніковим, М. Олейніком, Д. Прозоровим, А. Свищевим, Є. Брежнєвим, А. Коваленком, О. Ілляшенком. Аналізу оцінки ризиків кібербезпеки в банківській сфері присвячено роботу С. Євсеєва та інших. Наразі тема безпеки у кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

У 2021 році Європейська комісія оприлюднила своє бачення та цілі трансформації Європи до 2030 року, що надзвичайно важливо для досягнення переходу до кліматично нейтральної та стійкої економіки замкненого циклу. Амбіція ЄС полягає в тому, щоб бути незалежним у галузі цифрових технологій у відкритому і взаємопов'язаному світі та проводити цифрову політику, яка дає можливість людям та бізнесу здобути цифрове стійке майбутнє, орієнтоване на людину та процвітання. Це включає вирішення проблем вразливості та залежностей, а також пришвидшення інвестицій. ЄС також буде просувати свою цифрову програму на глобальній арені та сприятиме узгодженню або зближенню зі своїми нормами та стандартами. У Повідомленні [1] пропонується узгодити низку цифрових принципів, швидко розпочати важливі багатонаціональні проєкти та підготувати законодавчу пропозицію, що визначає надійну систему управління, для моніторингу прогресу — «Цифровий компас». За таких умов заохочення інноваційної діяльності та захист правовласників від кіберзагроз виходить на перший план у державних (національних) стратегіях захисту інтелектуальної власності. Інтелектуальна власність як особливо цінний нематеріальний актив (бази даних, комерційні секрети та ноу-хау, комп'ютерні програми тощо) є предметом нових загроз у кіберпросторі. Ефективна та дієва стратегія кібербезпеки і оборони запобігає порушенню прав інтелектуальної власності, а також забезпечує правовласникам конфіденційність баз даних, комерційної таємниці та ноу-хау. Захист інтелектуальної власності у кіберпросторі забезпечує необхідний рівень конкурентоспроможності для правовласників.

Права інтелектуальної власності забезпечують інвесторам своєрідні гарантії інвестиційних ризиків і в багатьох джерелах розглядаються як певний товар чи навіть як своєрідна валюта [8]. Разом з цим, створена для прискорення інноваційного розвитку через захист інтересів правовласників та стимулювання процесу інновацій система захисту прав інтелектуальної власності має зворотний бік: стабільний економічний і технологічний розвиток супроводжується зниженням конкуренції, високими витратами з доступу до сучасних товарів та технологій, зростанням цін, тобто стає своєрідним фактором стримування НТП, що яскраво продемонструвала пандемія.

Вказані фактори стали передумовою виникнення дискусії щодо сучасного змісту та значення інтелектуальної власності в цифровому світі, оцінки і використання інтелектуальної власності як засобу національної та міжнародної конкуренції, швидкого вирішення складних технологічних проблем або нематеріального активу [2].

Глобалізація доступу до інформації, зокрема й комерційної, інформації про нові технології, інформації у формі баз даних та поява нових засобів її формування, поширення та використання актуалізували питання безпеки і легального використання масивів інформації. Інформаційна безпека виходить за межі потреб окремих власників і виступає вже як один із напрямів національної стратегії розвитку. У багатьох державах

протягом останніх десяти років створено сучасне ефективне законодавство, пов'язане із забезпеченням інформаційної безпеки в інформаційно-комунікаційних мережах, де застосовуються власні стратегії інформаційної безпеки.

З початку року Україна зазнала двох потужних кібератак: перша сталася в ніч із 13 на 14 січня і виявилася найпотужнішою за останні чотири роки, охопивши 70 урядових сайтів. Ця атака фактично була початком «гарячої фази» війни. З першого ж дня функціональні підрозділи основних суб'єктів забезпечення кібербезпеки перейшли на режим відбиття збройної агресії та почали діяти згідно з відповідними планами, розробленими в рамках підготовки до відбиття збройної агресії рф проти України. Атаку 15 лютого, яка порушила роботу двох найбільших державних банків («ПриватБанк» та «Ощадбанк»), фахівці вважають «найбільшою DDoS-атакою в історії України». За попередніми висновками слідства, обидва інциденти вчинені хакерами, підконтрольними рф [5].

Уперше поняття інформаційної безпеки було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» № 537-V від 9 січня 2007 року [11], у якому інформаційна безпека була визначена як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдавання шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Стратегія інформаційної безпеки (далі — Стратегія) від 28 грудня 2021 року [15] визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних.

Реалізація положень Стратегії здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки. Реалізація Стратегії розрахована на період до 2025 року.

Правовою основою Стратегії є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента № 392/2020 України від 14 вересня 2020 року, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Питання, пов'язані з кібербезпекою, визначаються Стратегією кібербезпеки України, затвердженою Указом Президента України № 447/2021 від 26 серпня 2021 року [12].

Відповідно до статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. У свою чергу Рада національної безпеки і оборони України формує робочий орган — Національний координаційний центр кібербезпеки, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпе-

чують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України [12].

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України. Одним зі шляхів забезпечення функціонування національної системи кібербезпеки є впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, упровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем. Місія організаійно-технічної моделі кіберзахисту — через розвиток зрілості (*maturity*) національної системи кібербезпеки забезпечити її стійкість (*resilience*) задля безпечного та сталого функціонування українських об'єктів критичної інфраструктури, систем надання електронних послуг, інформаційної інфраструктури, нейтралізації (зменшення наслідків) кібератак та кіберінцидентів [10]. Метою її впровадження є досягнення Україною високого рівня координації та реалізації ініціатив щодо побудови національної системи кібербезпеки, захисту національних інформаційних ресурсів, стабільного функціонування інформаційної інфраструктури державних установ, галузей економіки та бізнесу, отримання соціально-економічних зисків від надійного та безпечного функціонування кіберпростору, що відповідає міжнародним зобов'язанням України.

Створення більшістю розвинених держав світу власних стратегій кібербезпеки тісно пов'язане з національними стратегіями розвитку інформаційної безпеки та інтелектуальної власності. Оскільки кібербезпека — це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз у кіберпросторі — мережі Інтернет, без якої на сьогодні важко уявити розвиток новітніх технологій, належний і ефективний обмін інформацією та інтелектуальною власністю. У США ще у 2013 році було прийнято стратегічний план стимулювання та захисту інтелектуальної власності у XXI ст., що визначає орієнтири у боротьбі уряду з контрафактною продукцією та інтелектуальним піратством, припиненням порушень прав інтелектуальної власності в Інтернеті та передбачає підвищення відкритості правозастосовної практики і міжнародних переговорів у сфері доступності виключних прав, а також покращення взаємодії державних органів та всіх зацікавлених сторін у сфері інтелектуальної власності та закріплює в якості основної правозастосовної доктрини — доктрину сумлінного використання (*fair use*); передбачає підвищення ефективності взаємодії федеральних органів штатів та місцевих органів (зокрема шляхом застосування нових технологій захисту інтелектуальної власності при прикордонному та транскордонному контролі); посилення захисту від загроз порушення прав інтелектуальної власності на іноземних інтернет-сайтах та захисту доменних імен першого рівня у поєднанні з підтримкою національних підприємств на зовнішніх ринках; передбачає систематизацію чинного законодавства у сфері інтелектуальної власності. У матеріалах до стратегічного плану наголошується, що інформаційна безпека є необхідною умовою інновацій. Інноваційний процес, за допомогою якого нові ідеї генеруються та успішно впроваджуються на ринку, як передбачає національна стратегія, є основною рушійною силою економічного зростан-

ня та національної конкурентоспроможності США [8, 64].

Ефективність захисту прав інтелектуальної власності у цифровому просторі Інтернету визначається можливістю протистояти таким порушенням та загрозам їх настання. Загрози порушення прав інтелектуальної власності в кіберпросторі (кіберзагрози) пов'язані з певними ризиками і можуть впливати саме на існування об'єкта виключних прав інтелектуальної власності. Зокрема в результаті кібератак можуть бути втрачені бази даних, що містять певну інформацію, яка є важливою для розвитку окремого суб'єкта господарювання та держави загалом, або можуть бути розголошені відомості, що містять комерційну таємницю. Отож ефективна система захисту прав інтелектуальної власності є частиною кібербезпеки та національної безпеки, оскільки саме наукова творчість є основою інновацій, які дають змогу державам перемагати в конкурентній боротьбі та закладають підвалини економічного і соціального прориву.

За останнє десятиліття кіберпростір став п'ятою окремою специфічною та важливою сферою ведення збройної боротьби, поряд із чотирма традиційними — «Земля», «Море», «Повітря» та «Космос». Нині вже буденним сприймається застосування державами кібервійськ та кіберзброї, здійснення кібероборони, кібероперацій та кібератак.

Військово-політичне керівництво провідних держав світу визнає протиборство в кіберпросторі як одну з вирішальних умов реалізації національних інтересів і вигідного врегулювання кризових ситуацій. З урахуванням вирішення цього завдання розвиваються національні та міждержавні органи управління, сили та засоби кібервоєн, реалізуються нові підходи до побудови системи протиборства в кіберпросторі на всіх рівнях.

Таким чином, кіберпростір стає місцем ведення військових дій. Війни в цьому просторі є новим різновидом протиборства, яке в перспективі може мати вирішальний вплив на всю систему світового правопорядку, оскільки розвиток технологій постійно пришвидшується, а глобальні мережі дають змогу використовувати розвинений арсенал засобів для проведення кібератак, від яких складно захиститися. Залежність безпеки та економіки держави від стану важливих об'єктів і системи інфраструктури (об'єктів критичної інфраструктури: енергозабезпечення, водопостачання, баз даних, телекомунікації, зв'язку та транспорту) обумовлює визнання кібербезпеки провідним елементом державної безпеки.

Кібербезпека, тобто безпека у сфері глобального Інтернету та інших цифрових інформаційно-комунікаційних мережах, тісно пов'язана з вирішенням завдань національної безпеки, зокрема в затвердженій у 2015 році Воєнній доктрині України йшлося лише про необхідність «… забезпечення кіберзахисту об'єктів критичної інфраструктури» та «поглиблення кооперації та співробітництва з НАТО і ЄС у сфері … боротьби з кіберзлочинністю» [14]. Нова Стратегія воєнної безпеки «Всебічна безпека — всеохоплююча оборона» [13] 2021 року визначає, що на глобальному рівні основними аспектами воєнної безпеки є руйнування створеної після Другої світової війни системи міжнародної безпеки, підвищення рівня невизначеності та непередбачуваності безпекового середовища, яке характеризується, зокрема, конкуренцією держав у сфері космічних, квантових, інформаційних, кібер-, гіперзвукових, біологічних, нано- та інших технологій, розробленням на їх основі систем озброєнь з використанням нових фізичних принципів, робототехніки та новітніх матеріалів, мілітаризацією навколоземного космічного простору, а також поширенням міжнародного тероризму та злочинності, загрозою розповсюдження зброї масового ураження [13].

Гібридна війна росії проти України, що з 2014 року активно супроводжується кібернападами на сайти урядових установ та навіть на об'єкти забезпечення

життєдіяльності населення (атаки на «Прикарпаттяобленерго»), — не перша апробація гібридної агресії [9].

В українській Стратегії зазначається, що «враховано положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО». Однак документ не містить переліку чи окремого додатка про те, які саме положення враховані, за винятком одного з пунктів Плану реалізації, що передбачає імплементацію Директиви Європейського парламенту і Ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елементу євроінтеграції України.

Головними загрозами в нашій стратегії визначено гібридну агресію рф, кіберзлочинність, організовані та спонсоровані урядами інших держав кібератаки, кібертероризм та іншу підтримку терористичної діяльності. Водночас у стратегії йдеться про те, що повільна імплементація положень європейського законодавства є одним із чинників, що формує вищезазначені загрози. У рамках гарантування безпеки цифрового простору Україна повинна спрямувати свої зусилля на розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог з урахуванням європейських та міжнародних стандартів.

Україна вже має певний досвід протистояння гібридним загрозам. Саме в нашій країні рф випробовує нові методи і засоби ведення гібридної війни. Проте відсутність достатніх ресурсів та засобів для самостійного відбиття агресії росії посилює важливість не тільки політичного сприяння на міжнародній арені з боку ЄС і НАТО, а й практичної допомоги у розвитку здатності України протистояти сучасним загрозам. У цьому контексті кібербезпека опинилась у центрі взаємодії Україна — НАТО — ЄС. Вона увійшла до переліку семи ключових напрямів безпекової співпраці НАТО — ЄС, визначених у Спільній декларації про співробітництво НАТО і ЄС, стала пріоритетом для обох організацій у наданні ними допомоги з посилення українських можливостей гарантувати власну безпеку.

З метою забезпечення завдань державної безпеки і оборони держава гарантує створення і запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони. Окрім того, у рішенні Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» визначено, що кібероборона є складовою частиною плану оборони України. Сучасна доктрина кібероборони України заснована на взаємодії з державами членами ЄС та НАТО, проведенні щонайменше двічі на рік спільних тематичних навчань з відповідними підрозділами держав-членів НАТО задля досягнення оперативної сумісності, а також передбачає створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних сил України, налагодивши на постійній основі співпрацю з європейською військовою CERT-мережею.

Кіберзагрози в сучасному суспільстві набувають значного масштабу. Відтепер успішна атака хакерів може знеструмити цілу область або країну. Кіберзагрози являють собою наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів, кожен з яких є самостійною системою і разом з тим містить у собі окремі об'єкти інтелектуальної власності. За таких умов захисту підлягає як система накопичення інформації, так і сама інформаційна система. Уразливими для реалізації кіберзагроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору.

Таким чином, об'єкти, завдавання шкоди яким можливе шляхом деструктивного кібервпливу (кібератаки), тобто спрямованих (навмисних) дій у кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

У 2020–2021 роках Україна зрівнялася із США за кількістю кібератак, спрямованих на установи держави. Статистика Microsoft, зібрана за 2020–2021 роки, вказує на те, що фронт кібервійни проходить через українську територію. Половина атак хакерів була спрямована проти Сполучених Штатів — 46 %, а кожне п'яте втручання «чорних хакерів» припало на Україну — 19 %, де, наприклад, тільки від російської хакерської групи Nobelium постраждало близько 1200 структур. Велика Британія відстає зі значним відривом — 9 %. Решта атак припала на Бельгію, Японію, Німеччину (3 %) та інші країни [3].

Аналіз законодавства у сфері кібербезпеки, а також організаційних заходів, спрямованих на розбудову ефективних систем кіберзахисту провідних країн світу, свідчить, що ключові світові гравці вдосконалюють власні можливості з кіберзахисту відповідно до трансформації сучасних кіберзагроз. Останнім часом фіксується суттєва зміна форм, суб'єктів і наслідків реалізації основних загроз кібербезпеці держав. Так, кібератаки стають усе більш комплексними та складними, їх наслідки становлять загрозу ключовим національним інтересам, а їхніми організаторами або замовниками все частіше виявляються спецслужби іноземних держав чи терористичні організації [6].

За даними американської транснаціональної компанії Cisco, що спеціалізується у галузі високих технологій та телекомунікацій, майже кожна четверта організація, яка зазнала кібератаки, втрачає бізнес-можливості, а близько 30 % підприємств втратили прибуток. В Україні зазначена проблема підсилюється станом гібридної війни проти нашої країни. Ключовим гібридним інструментом агресор використовує саме інформаційні технології та системи комунікацій у кіберпросторі. За даними Держспецзв'язку України щодо захисту державних інформаційних ресурсів, лише за останніх 9 місяців зареєстровано понад 60 млн підозрілих подій та понад 3 млн атак різних видів, які система захищеного доступу державних органів до мережі Інтернет заблокувала. Щотижня фіксується від 600 тис. до 900 тис. підозрілих подій, а система захищеного доступу державних органів до мережі Інтернет блокує понад 0,5 млн різних видів атак [4, 18].

Більшість дослідників дійшли висновку, що джерелами кіберзагроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо [7].

Основними видами кіберзагроз (загроз у сфері кібербезпеки) є кіберзлочинність; кібертероризм та кібершпигунство; кібервійна. Деякі дослідники вказують на те, що самостійним видом кіберзагроз є гібридна війна.

Злочини з використанням сучасних інформаційних технологій стають усе звичнішою практикою в житті укра-

їнських громадян. До того ж новітні технології застосовуються для скоєння не лише традиційних видів злочинів, а й нових, характерних передусім для розвинутого інформаційного суспільства. Найбільше увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів. Усе ще актуальною залишаються проблеми боротьби з дитячою порнографією та порушеннями авторських і суміжних прав.

**Висновки.** Дослідивши проблеми і тенденції подальшого розвитку правового регулювання кібербезпеки в нашій державі, можемо вказати таке.

Удосконаленню підлягають норми національного законодавства у сфері кібербезпеки, формулювання яких допускають неоднозначне тлумачення чи містять умисні прогалини законодавства та не забезпечують принципи правової визначеності, що унеможливлює реалізацію завдань і функцій кібербезпеки і кібероборони, або є підставою конфлікту повноважень різних уповноважених органів, порушують принципи розумної достатності правового регулювання. З цією метою варто використати досвід США, НАТО і Швейцарії.

Підлягають розробленню нормативно-правові акти, спрямовані на створення і забезпечення функціонування кібервійськ, які повинні стати взаємосумісними з аналогічними структурами Збройних сил країн НАТО.

Україні варто використати досвід та практики ЄС і НАТО для створення широкої національної схеми сертифікації з кібербезпеки, розроблення планів для відповіді на широкомасштабні інциденти і кризи (від Національного плану реагування на надзвичайні (кризові) ситуації в кіберпросторі до планів реагування на конкретних об'єктах критичної інформструктури), поглиблювати державно-приватне партнерство і посилювати дослідження в цій сфері; ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе нашій країні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері; нарощувати оборонний технічний потенціал України у сфері кібербезпеки. Військова агресія рф проти України призвела до формування нових відносин у сфері кіберзахисту та кібероборони. Усі вони повинні бути систематизовані та уніфіковані, на їх основі має бути сформований пакет відповідних змін і доповнень до законодавчих актів з цих питань. Залишаються неімплементованими норми кількох директив ЄС у сфері кібербезпеки та міжнародних стандартів у цій сфері.

Оскільки Україна перебуває фактично у стані кібервійни з рф, варто ставити на порядок денний усього світового співтовариства питання перегляду норм і правил міжнародного гуманітарного права (МГП), яким регулюються такі відносини. Це стосується права держави захищати себе; права на дії у відповідь навіть тоді, коли це може завдати шкоди об'єктам критичної інфраструктури, посягання на які заборонені чинними конвенційними домовленостями. Аналогічна проблема виникає при здійсненні заходів кібероборони та захисту спеціально створеними військовими формуваннями держави, розмежування статусу кіберзлочинця та військовослужбовця, що виконує свої функції захисту держави в кіберпросторі, оскільки дії та наслідки дій цих осіб можуть бути аналогічними, проте спрямування та мета — різними.

Використання державами світу інформаційних технологій цілком підпадає під дію всіх чинних норм міжнародного права, включаючи МГП. Таким чином, щоб цивільні особи та цивільна інфраструктура користувалися тим же рівнем захисту, що й у минулому, і щоб на всі види кіберозброєнь поширювалися ті ж обмеження, що й на традиційні засоби ведення війни,

необхідно відповідні зміни, доповнення та поправки до МГП узгодити з міжнародною спільнотою. Окрім цього, має бути вирішене й питання про права держави на належний захист у разі агресії в кіберпросторі та гарантії прав військових, що здійснюють оборону і захист інтересів своєї держави.

**Список використаних джерел / List of references**


1. *Communication from the Commission to the European Parlament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade//COM/2021/118 final// URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX: 52021DC0118.*
2. *Matthew Littleton. The TRIPS Agreement and Transfer of Climate-Change-Related Technologies to Developing Countries. United Nations Department of Economic and Social Aff airs. Working Paper No. 71. ST/ESA/2008/DWP/71. С. 1–2.*
3. *Бутченко М. Кибервойна с Россией: как организованы хакерские атаки и как защищаются украинские спецслужбы. URL: https://itc.ua/articles/gotovnost-k-kibervojne-rossijskie-hakery-uzhe-vosem-let-atakuyut-ukrainu-kak-organizovany-ataki-i-naskolko-uspeshno-spravlyayutsya-nashi-speczsluzhby.*
4. *Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: дис. … докт. юрид. наук: 12.00.07. Одеський державний університет внутрішніх справ. Одеса, 2021. С. 18.*
5. *Держспецзв'язку: з початку 2022 року в Україні зафіксували 436 кіберінцидентів — це у сім разів більше, ніж за аналогічний період торік (18.02.2022). URL: https://itc.ua/news/derzhspeczzvyazku-z-pochatku-2022-roku-v-ukrayini-zafiksuvali-436-kiberinczidentiv-cze-u-sim-raziv-bilshe-nizh-za-analogichnij-period-torik.*
6. *Діордіца І. В. Класифікація кіберзагроз в нормативно-правових актах України. URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini.*
7. *Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі. URL: https://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi.*
8. *Карцхия А. А. Кибербезопасность и интелектуальная собственность. Вопросы кибербезопасности. № 1(2). 2014. С. 61–66.*
9. *Нова стратегія кібербезпеки: як Україна захищатиметься в кіберпросторі? Аналітичний центр ADASTRA. URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori.*
10. *Положення про організаційно-технічну модель кіберзахисту. Затверджено постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426.*
11. *Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537-V. Відомості Верховної Ради України (ВВР). 2007. № 12. Ст. 102.*
12. *Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7.*
13. *Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661.*
14. *Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : Указ Президента України № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/n0016525-15#Text.*

15. *Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.*

1. *Communication from the Commission to the European Parlament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade//COM/2021/118 final// URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX: 52021DC0118.*
2. *Matthew Littleton. The TRIPS Agreement and Transfer of Climate-Change-Related Technologies to Developing Countries. United Nations Department of Economic and Social Aff airs. Working Paper No. 71. ST/ESA/2008/DWP/71. S. 1–2.*
3. *Butchenko M. Kybervoina s Rossyei: kak orhanyzovanы khakerskye ataky y kak zashchyshchaiutsia ukraynskye spetssluzhbы. URL: https://itc.ua/articles/gotovnost-k-kibervojne-rossijskie-hakery-uzhe-vosem-let-atakuyut-ukrainu-kak-organizovany-ataki-i-naskolko-uspeshno-spravlyayutsya-nashi-speczsluzhby.*
4. *Veselova L. Yu. Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoi viiny: dys. … dokt. yuryd. nauk: 12.00.07. Odeskyi derzhavnyi universytet vnutrishnikh sprav. Odesa, 2021. S. 18.*
5. *Derzhspetszviazku: z pochatku 2022 roku v Ukraini zafiksuvaly 436 kiberintsydentiv — tse u sim raziv bilshe, nizh za analohichnyi period torik (18.02.2022). URL: https://itc.ua/news/derzhspeczzvyazku-z-pochatku-2022-roku-v-ukrayini-zafiksuvali-436-kiberinczidentiv-cze-u-sim-raziv-bilshe-nizh-za-analogichnij-period-torik.*
6. *Diorditsa I. V. Klasyfikatsiia kiberzahroz v normatyvno-pravovykh aktakh Ukrainy. URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini.*
7. *Diorditsa I. V. Poniattia i zmist kiberzahroz na suchasnomu etapi. URL: https://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi.*
8. *Kartskhyia A. A. Kyberbezopasnost y yntelektualnaia sobstvennost. Voprosы kyberbezopasnosty. № 1(2). 2014. S. 61–66.*
9. *Nova stratehiia kiberbezpeky: yak Ukraina zakhyshchatymetsia v kiberprostori? Analitychnyi tsentr ADASTRA. URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori.*
10. *Polozhennia pro orhanizatsiino-tekhnichnu model kiberzakhystu. Zatverdzheno postanovoiu Kabinetu Ministriv Ukrainy vid 29 hrudnia 2021 r. № 1426.*
11. *Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky : Zakon Ukrainy vid 09.01.2007 r. № 537-V. Vidomosti Verkhovnoi Rady Ukrainy (VVR). 2007. № 12. St. 102.*
12. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» : Ukaz Prezydenta Ukrainy № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7.*
13. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku «Pro Stratehiiu voiennoi bezpeky Ukrainy» : Ukaz Prezydenta Ukrainy № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661.*
14. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 2 veresnia 2015 roku «Pro novu redaktsiiu Voiennoi doktryny Ukrainy» : Ukaz Prezydenta Ukrainy № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/n0016525-15#Text.*
15. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky» : Ukaz Prezydenta Ukrainy № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.*

Надійшла до редакції 14.09.2022 року

**Bakalinska O. Current legal trends of cyber security and intellectual property.** The catalyst for changes in the sphere of cyber-security in our country has been the hybrid war unleashed by the Russian Federation with the use of both classic and non-lethal weapons, through cyberspace and across cyberspace included. Challenges and threats to the national security of Ukraine in the cyberspace led to the creation of the Cybersecurity Strategy of Ukraine.

The cyberwar in Ukraine showed the ineffectiveness of the current international legal deterrence mechanism. The most important aspect of the development of international humanitarian law is the formation of modern principles of counteraction to unfriendly actions of aggressors in cyberspace. Encouraging innovative activity and protecting rights holders from cyber threats is the main direction of state (national) intellectual property strategies, as a significant foundation for the rapid development of industrial potential. Cybersecurity prevents the infringement of intellectual property rights and also ensures the privacy of databases, trade secrets and know-how to rights holders. It is the effective state position in this area that will ensure the rapid recovery of our state after the end of the war.

Legislative regulation of cyber protection in Ukraine corresponds to international standards and modern cybersecurity strategies of the EU and NATO. In our opinion, the most promising directions of development of the national cyber defence system are: improvement of the legal basis of cyber defence for critical infrastructure facilities; implementation of the system of independent information security; development of international cooperation in the field of cybersecurity; increase in digital literacy of citizens and culture of safe behaviour in the cyberspace.

The cyberwar in Ukraine has shown the ineffectiveness of the current international legal deterrence mechanism. The most important aspect of the development of international humanitarian law is the formation of modern principles of counteraction in cyberspace and the protection of the interests of small countries from unfriendly actions.

*Keywords:* informational security, cyberspace, cybersecurity, intellectual property