СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Застосування інформаційних технологій у правоохоронній діяльності: матеріали круглого столу (м. Харків, 14 груд. 2023 р.). Харків: ХНУВС, 2023. С. 122–125.
2. Вікторчук М. В., Багатко А. С. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності // *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 3. № 86. С. 238–244.
3. Сучасні інформаційні технології в діяльності Національної поліції: матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 02 листоп. 2023 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2024. 184 с.
4. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект // *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 3. № 90. С. 184–190.
5. Базові аспекти цифровізації та їх правове забезпечення: монографія / за ред. К. В. Єфремової. Харків: НДІ ПЗІР, 2021. 180 с.

МАЦЮК МИКОЛА МИКОЛАЙОВИЧ
курсант 214 н. гр. факультету забезпечення державної безпеки Київський інститут Національної гвардії України

КОБА МАРІЯ МИКОЛАЇВНА
доктор філософії в галузі права, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності, Київський інститут Національної гвардії України

КІБЕРПРОСТІР У ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Проблема кібербезпеки набуває багатовимірного характеру та є критично важливою для забезпечення глобальної стабільності в умовах цифровізації суспільства. Зростання кількості та складності кібератак зумовлює необхідність посилення міжнародної співпраці та вироблення узгоджених правових підходів до протидії кіберзагрозам. Розвиток високотехнологічних форм кіберзлочинності та потреба у забезпеченні конфіденційності даних спонукають держави до формування нових правових механізмів регулювання кіберпростору [1].

Актуальність обраної нами проблематики посилюється безпрецедентним зростанням інформаційних загроз, що супроводжують сучасні збройні конфлікти. Гібридна війна, яку проводить рф проти України, характеризується поєднанням традиційних і нетрадиційних методів ведення війни, серед яких кібератаки та інформаційні операції займають ключове місце [2, с. 23]. Це формує нові виклики для міжнародного права та потребує переосмислення існуючих підходів до регулювання.

Проблематику міжнародно-правового регулювання кіберпростору та кіберконфліктів досліджують як вітчизняні науковці, зокрема Д. Дубов, О. Пазюк, О. Мережко, так і зарубіжні вчені, серед яких Michael N. Schmitt, Wolff Heintschel von Heinegg та Heather Harrison Dinniss.

Кібербезпека є однією з політичних сфер глобального управління даними. В умовах ескалації кіберзагроз, особливо у контексті збройних конфліктів, нагальною є потреба у створенні гармонізованої міжнародно-правової бази. Вирішення міжнародних проблем кібербезпеки та захисту даних потребує багатогранного підходу, що поєднує співпрацю між державами, зміцнення технічних і правових можливостей, а також формування глобальної культури кібербезпеки [1].

Правове регулювання кіберпростору ускладнюється його транскордонною природою, що створює труднощі для уніфікації нормативних підходів. У науковій літературі зазначається, що кіберпростір характеризується відсутністю чітких юрисдикційних меж, що суттєво ускладнює застосування традиційних норм міжнародного права [3]. У зв'язку з цим міжнародне право у сфері кібербезпеки залишається динамічним і таким, що перебуває на стадії формування.

Сучасні міжнародно-правові норми частково втрачають ефективність через швидкий розвиток технологій. Водночас складність атрибуції кібератак і низька прозорість кібероперацій ускладнюють досягнення міжнародного консенсусу щодо їх правової оцінки [4].

На нашу думку, сучасні кібератаки у межах гібридних конфліктів фактично трансформують класичне розуміння «застосування сили» у міжнародному праві, оскільки їхній вплив може бути співмірним із кінетичними засобами ураження, навіть за відсутності фізичного руйнування.

Специфічні характеристики кіберконфліктів включають їхню глобальність, швидкість поширення та складність ідентифікації суб'єкта атаки [4]. У цьому контексті важливими є напрацювання експертної групи Michael N. Schmitt, яка у межах Tallinn Manual 2.0 обґрунтувала застосовність норм міжнародного гуманітарного права до кібероперацій [3].

Поділяємо думку дослідників, що у гібридних конфліктах кібератаки визнаються одним із основних інструментів агресії. Вони не мають чіткої лінії фронту, а бойові дії часто здійснюються без формального оголошення війни. Інформаційні операції спрямовані на контроль інформаційного простору та підвищення ефективності військових дій [2, с. 23].

Системні кібератаки рф проти України, спрямовані на критичну інфраструктуру, актуалізують необхідність перегляду підходів до міжнародного регулювання кібербезпеки. Як зазначає Michael N. Schmitt, важливим питанням є визначення порогу застосування сили у кіберпросторі [3].

Вбачається, що Україна сьогодні виступає не лише об'єктом кіберзагроз, але й своєрідним «полігоном» для формування нових міжнародно-правових підходів до регулювання кібероперацій, що в перспективі може вплинути на еволюцію глобальної системи безпеки.

Особливої уваги заслуговує концепція «втрати функціональності», відповідно до якої виведення з ладу критичної інфраструктури через кібератаку може розглядатися як напад у розумінні міжнародного гуманітарного права навіть без фізичного знищення об'єктів [5].

Попри складність проблеми, вже існує низка міжнародних інструментів, що регулюють кіберпростір:

- Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.) – спрямована на гармонізацію національного законодавства та розвиток міжнародної співпраці [6].
- Загальний регламент ЄС про захист даних (GDPR) – встановлює високі стандарти захисту персональних даних [7].
- Резолюції Генеральної Асамблеї ООН, зокрема 70/237, які визначають принципи відповідальної поведінки держав у кіберпросторі [8].

Водночас існують значні прогалини у застосуванні цих норм. Ефективна протидія гібридним загрозам потребує не лише вдосконалення правової термінології, але й адаптації національної політики до сучасних викликів. Особливо важливою є гармонізація законодавства України з правом ЄС (GDPR, NIS2) та врахування практики міжнародних інституцій.

Таким чином, кібербезпека є комплексною міждисциплінарною проблемою, що має безпосередній вплив на міжнародний мир і безпеку. Гібридні війни інтегрують кіберпростір як ключовий елемент ведення бойових дій, що потребує гнучкої та адаптивної правової відповіді. Пріоритетним завданням є формування ефективної міжнародно-правової бази, що забезпечить належний рівень кібербезпеки та захисту даних. Це передбачає посилення співпраці між державами, бізнесом і громадянським суспільством.

Досвід України у протидії кібератакам у межах збройного конфлікту має важливе значення для розвитку міжнародного права, зокрема у контексті застосування концепції «втрати функціональності».

Подальший розвиток міжнародного права у сфері кіберпростору має бути спрямований на досягнення балансу між вимогами національної безпеки та захистом прав людини, з урахуванням сучасних умов воєнного стану та цифрових трансформацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карвацька С.Б., Маник А.З., Яремчук В.В. Кіберпростір: міжнародно-правове регулювання та практика застосування прецедентного права МС ООН. https://journal-app.uzhnu.edu.ua/article/view/328252.
2. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1–2. С. 20–26.
3. Schmitt M. N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/.
4. Грищенко С. М. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства. https://il.ippi.org.ua/article/view/340519.
5. М.О. Геревич, М.Т. Марушка Право людини на кібербезпеку: сутнісні характеристики та проблеми забезпечення» https://journal-app.uzhnu.edu.ua/article/view/345929.
6. Конвенція Ради Європи про кіберзлочинність : міжнародний договір від 23 листопада 2001 р. (Будапешт). Рада Європи, 2001. https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.
7. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних (General Data Protection Regulation). Офіційний журнал ЄС, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
8. Резолюція Генеральної Асамблеї ООН 70/237 «Досягнення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» від 23 грудня 2015 р. Організація Об'єднаних Націй, 2015. https://digitallibrary.un.org/record/1301308/files/A_72_327-EN.pd.

МОСКАЛЕНКО ТЕТЯНА ВОЛОДИМИРІВНА
курсант 234 навчальної групи, Національна академія Державної прикордонної служби України імені Богдана Хмельницького

БОРОВСЬКИЙ ВІТАЛІЙ СТЕПАНОВИЧ
викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького

АНАЛІЗ ТА УЗАГАЛЬНЕННЯ БОЙОВОГО ДОСВІДУ ПІДРОЗДІЛІВ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ У СУЧАСНІЙ ВІЙНІ

Повномасштабне вторгнення російської федерації на територію України 24 лютого 2022 року докорінно змінило умови виконання бойових завдань Державною прикордонною службою України (ДПСУ). Підрозділи відомства, що традиційно здійснювали охорону державного кордону в мирний час, були поставлені перед необхідністю вести активні бойові дії в умовах реального збройного конфлікту. Набутий у ході цих дій унікальний бойовий досвід потребує систематичного аналізу та узагальнення з метою підвищення боєздатності підрозділів ДПСУ.

Аналіз бойових дій підрозділів ДПСУ у 2022–2024 роках свідчить про те, що прикордонники зіткнулися з принципово новими для себе оперативно-тактичними задачами. Зокрема, було виявлено необхідність швидкої переорієнтації від завдань охорони кордону до безпосереднього