УДК 341.3
DOI 10.31558/2786-5835.2026.1.1.11

Пасешник Олександр Русланович,
аспірант кафедри міжнародного, цивільного та комерційного права
Державного торговельно-економічного університету
ORCID: https://orcid.org/0009-0005-6692-9925

ЗАСТОСУВАННЯ ПРИНЦИПУ ОБЕРЕЖНОСТІ ПІД ЧАС ПЛАНУВАННЯ КІБЕРАТАК

У статті досліджено елементи принципу обережності під час планування кібератак у контексті застосування міжнародного гуманітарного права до сучасних збройних конфліктів. Актуальність теми зумовлена тим, що кібератаки здатні впливати не лише на військові системи, а й на цивільну інфраструктуру, необхідну для забезпечення життєво важливих потреб населення. У кіберпросторі межа між військовими та цивільними об'єктами часто є технічно розмитою, оскільки одні й ті самі мережі, сервери, програмні платформи, системи обробки даних або канали зв'язку можуть одночасно використовуватися для військових і цивільних цілей.

Обґрунтовано, що принцип обережності, закріплений у статті 57 Додаткового протоколу I до Женевських конвенцій 1949 року та підтверджений звичаєвими нормами міжнародного гуманітарного права, у кіберпросторі не може тлумачитися лише як формальна вимога перевірити військовий характер цілі. Його зміст охоплює функціональну оцінку цифрової системи, аналіз її зв'язку з цивільними сервісами, перевірку контрольованості кіберзасобу, оцінку ризику самопоширення шкідливого коду, передбачення прямих і непрямих наслідків, а також вибір менш шкідливої альтернативи за наявності кількох можливих способів досягнення військової переваги.

Особливу увагу приділено проблемі втрати функціональності, статусу комп'ютерних даних і каскадних наслідків кібератак. Доведено, що для оцінки правомірності планування кібератаки значення має не лише можливість фізичного пошкодження об'єкта, а й ризик порушення функціонування систем, від яких залежить цивільне населення. Зроблено висновок, що принцип обережності у кіберпросторі треба розглядати не лише як обов'язок стриманості, а й як обов'язок належного попереднього пізнання цифрового середовища. Межі цього обов'язку визначаються критеріями практичної можливості та розумної передбачуваності, однак технічна складність кіберпростору не може виправдовувати поверхневе планування або ігнорування очевидних ризиків для цивільного населення.

Ключові слова: *міжнародне гуманітарне право, МКЧХ, запобіжні заходи, цивільне населення, цивільні об'єкти, збройний конфлікт, наслідки, кіберпростір.*

Постановка проблеми. Цифровізація воєнних дій істотно ускладнила застосування традиційних норм міжнародного гуманітарного права до сучасних збройних конфліктів. Кібератаки здатні впливати не лише на окремі військові системи, а й на цифрову інфраструктуру, від якої залежить функціонування цивільних сервісів, адміністративного управління, зв'язку, транспорту, енергетики, охорони здоров'я та інших життєво важливих сфер. Унаслідок цього розрізнення між військовими та цивільними об'єктами у кіберпросторі часто є неочевидним, а наслідки запланованого впливу можуть виходити за межі початково визначеної цілі.

Особливої ваги за таких умов набуває принцип обережності під час планування нападів. Принцип обережності (вжиття запобіжних заходів) призначений для захисту цивільного населення від наслідків воєнних дій. Його нормативна основа була сформована у межах класичного права ведення воєнних дій, однак у кіберпросторі цей принцип потребує змістовного уточнення. Проблема полягає в тому, що кібератака може спричинити шкоду не лише через фізичне пошкодження або знищення об'єкта, а й через втрату функціональності цифрової системи, блокування або спотворення даних, самостійне поширення шкідливого коду чи каскадне порушення роботи взаємозалежних цивільних сервісів. Саме тому формальна перевірка військового характеру цілі вже не є достатньою для належного дотримання принципу обережності.

У цьому зв'язку виникає потреба визначити, які саме дії повинна охоплювати належна підготовка кібератаки з погляду міжнародного гуманітарного права: перевірку функції цифрової цілі, аналіз її зв'язку з цивільною інфраструктурою, оцінку контрольованості обраного кіберзасобу, передбачення прямих і непрямих наслідків, вибір менш шкідливої альтернативи та перегляд рішення у разі появи нових даних. Водночас необхідно окреслити межі цього принципу, оскільки міжнародне гуманітарне право не вимагає абсолютного передбачення всіх можливих наслідків, але зобов'язує сторону конфлікту вживати всіх практично можливих заходів для мінімізації ризиків для цивільного населення і цивільних об'єктів. Саме цим зумовлюється наукова і практична актуальність дослідження застосування принципу обережності під час планування кібератак.

Аналіз останніх досліджень і публікацій. Дослідженням проблем застосування міжнародного гуманітарного права до кібератак під час збройних конфліктів, а також окремих аспектів вжиття запобіжних заходів, захисту цивільного населення та правової оцінки наслідків кібератак займалися Л. Гізель, Т. Роденгойзер, К. Дерманн, Е. Дж. Бріз, Г. Біджіо, О. Помсон, а також експерти Міжнародного Комітету Червоного Хреста. Водночас зміст принципу обережності саме на стадії планування кібератак залишається недостатньо конкретизованим, зокрема щодо перевірки цифрової цілі, контрольованості кіберзасобу, врахування функціональних і каскадних наслідків та меж розумної передбачуваності.

Постановка завдання. Метою статті є визначення змісту обережності під час планування кібератак у збройних конфліктах. Для досягнення цієї мети необхідно з'ясувати, які дії має охоплювати належне планування кібератаки та за якими критеріями треба оцінювати дотримання цього принципу у кіберпросторі.

Виклад основного матеріалу. Нормативною основою принципу обережності під час планування нападів є насамперед стаття 57 Додаткового протоколу I до Женевських конвенцій 1949 року, яка вимагає постійної турботи про щадіння цивільного населення, перевірки військового характеру цілі, вибору таких

засобів і методів нападу, що дають змогу уникнути або щонайменше мінімізувати випадкову шкоду, а також скасування чи зупинення нападу, якщо його неправомірність стає очевидною [1].

Зміст цієї норми не вичерпується забороною явно незаконних атак. Із коментаря МКЧХ до статті 57 випливає, що йдеться про активний обов'язок поведінки, який охоплює підготовку та здійснення нападу. Тому стадія планування має самостійне міжнародно-правове значення: сторона конфлікту повинна не лише утримуватися від ударів по цивільних цілях, а й завчасно організовувати підготовку так, щоб максимально зменшити ризик випадкової шкоди [2].

Нормативний зміст принципу обережності підтверджується також звичаєвим міжнародним гуманітарним правом, де передбачається обов'язок вживати всіх практично можливих запобіжних заходів під час нападу, перевіряти військовий характер цілі, обирати менш небезпечні засоби і методи ведення війни та оцінювати очікувані наслідки нападу для цивільного населення і цивільних об'єктів [3].

Застосовність міжнародного гуманітарного права до кібератак під час збройних конфліктів сьогодні загалом визнається у підходах МКЧХ. Водночас саме у кіберпросторі особливо гостро проявляється проблема взаємозалежності цивільних і військових мереж. Цифрова інфраструктура часто має цивільне або подвійне призначення, а тому планування кібератаки повинно враховувати не лише формальний військовий характер цілі, а й її зв'язок із цивільними сервісами та можливий гуманітарний ефект [4, с. 4].

Сучасний підхід МКЧХ до викликів збройних конфліктів додатково підкреслює, що кібератаки можуть завдавати шкоди не тільки через фізичне руйнування, а й через порушення життєво важливих послуг, виведення з ладу мереж або пошкодження даних. Для принципу обережності це означає необхідність оцінювати на етапі планування не лише ризик матеріального пошкодження, а й можливість порушення функціонування систем, від яких залежить цивільне населення [5, с. 1418].

Першим елементом принципу обережності є перевірка цілі. У кіберпросторі цей стандарт ускладнюється подвійним призначенням багатьох цифрових систем: один сервер, дата-центр, мережевий вузол чи програмна платформа можуть одночасно забезпечувати військові функції та цивільні послуги. Тому перевірка цілі не може обмежуватися встановленням її належності до певної установи чи мережі, а повинна охоплювати аналіз реальної функції цифрового об'єкта, його інтегрованості з іншими системами та потенційної залежності цивільної інфраструктури від його роботи [6, с. 34].

Другим елементом є оцінка засобу і методу нападу. У сфері кібератак це передбачає аналіз не лише очікуваної військової користі, а й технічних власти-

востей обраного інструменту: здатності до самопоширення, можливості локалізувати його дію, ризику переходу через суміжні мережі, ймовірності хибного спрацювання та наявності механізмів зупинки або деактивації. Якщо засіб не дає змоги утримати вплив у межах визначеної цілі, виникає серйозний сумнів у його правомірності [1].

Третім елементом є оцінка передбачуваних наслідків. Для міжнародного гуманітарного права недостатньо встановити, що кібератака спрямована проти військової цілі. Необхідно також оцінити прямі й непрямі наслідки, які можна розумно очікувати від її реалізації. У цифровому середовищі вплив на один вузол системи може спричинити порушення роботи пов'язаних цивільних сервісів, зокрема енергопостачання, медицини, водопостачання, транспорту чи зв'язку. Тому планування кібератаки повинно враховувати системну взаємозалежність інфраструктури, у межах якої застосовується відповідний засіб [3].

Важливе значення має зв'язок принципу обережності з використанням розвідувальної інформації. Сторона конфлікту повинна діяти не на основі формального припущення про військовий характер об'єкта, а з урахуванням доступного знання про ціль, середовище атаки та можливі наслідки. Для кібератак це означає потребу в попередньому аналізі мережевих залежностей, технічних вразливостей, функціональних зв'язків між системами та можливих вторинних наслідків [7, с. 312].

Звідси випливає, що у кіберпросторі принцип обережності є не лише обов'язком стриманості, а й обов'язком належного попереднього пізнання цифрового середовища. Одним із ключових проявів такого підходу є необхідність врахування втрати функціональності цифрових систем.

У сучасній доктрині обговорюється, чи повинні правила про напад і запобіжні заходи охоплювати лише фізичне пошкодження об'єкта, чи також ситуації, коли система внаслідок кібератак втрачає здатність виконувати свою функцію. Розширений підхід видається переконливим, оскільки припинення роботи лікарняних, енергетичних, водопостачальних, логістичних чи комунікаційних систем може становити реальну шкоду для цивільного населення навіть без фізичного руйнування відповідного обладнання [8, с. 242].

Водночас питання втрати функціональності не є остаточно вирішеним, оскільки в доктрині зберігається і більш стриманий підхід, який пов'язує поняття нападу переважно з пораненням осіб або фізичним пошкодженням чи знищенням об'єктів. Проте для принципу обережності важливо, що істотне порушення функціонування цивільно значущих систем має враховуватися на етапі планування незалежно від остаточного вирішення цієї доктринальної дискусії.

З цією проблемою пов'язане питання статусу даних. Кібератаки можуть бути спрямовані не на фізичну інфраструктуру, а на дані, без яких робота цивіль-

них систем фактично неможлива. У доктрині міжнародного гуманітарного права питання про те, чи треба вважати дані об'єктом у правовому сенсі, залишається спірним і має істотне значення для оцінки законності операцій у кіберпросторі [9, с. 350]. Для принципу обережності ключовим є практичний наслідок цієї проблеми: якщо втручання в дані може порушити роботу життєво важливих сервісів, такий ризик має враховуватися під час планування кібератаки.

Ще одним елементом принципу обережності є вибір менш шкідливої альтернативи. Якщо існує кілька способів досягнення порівнянної військової переваги, перевага має надаватися тому, який створює менший ризик для цивільного населення і цивільних об'єктів. У кібератаках це стосується не лише вибору цілі, а й часу операції, способу доступу до системи, виду шкідливого інструменту, інтенсивності впливу, тривалості втручання, масштабу використаної вразливості та можливості припинення операції після досягнення необхідного ефекту [1]. Якщо один спосіб дає змогу досягти воєнної мети з локалізованим ефектом, а інший створює підвищений ризик самопоширення або каскадного збою, перевага повинна надаватися першому.

Окремого аналізу потребує проблема каскадних наслідків кібератак. У кіберпросторі побічна шкода не завжди обмежується безпосереднім впливом на обрану систему, оскільки такий вплив може розгортатися через залежні сервіси та спільну цифрову інфраструктуру. Вимкнення одного цифрового сегмента може спочатку здаватися локальним, але згодом спричинити порушення ширшої мережі цивільних сервісів. Тому під час планування кібератаки необхідно оцінювати не лише прямий вплив, а й архітектуру ширшого цифрового середовища. Там, де системна взаємозалежність є відомою або очевидною, її ігнорування становитиме правову ваду планування [6, с. 34].

Водночас міжнародне гуманітарне право не вимагає абсолютного передбачення всіх можливих наслідків. Застосування принципу обережності визначається критеріями практичної можливості та розумної передбачуваності. Тому правова оцінка має зосереджуватися не на тому, чи були передбачені всі можливі наслідки, а на тому, чи було використано доступне знання, здійснено реалістичний аналіз і враховано очевидні ризики. Якщо непрямий наслідок був віддаленим, малоймовірним і технічно непередбачуваним навіть за належної підготовки, його неврахування не обов'язково свідчить про порушення. Однак якщо ризик випливав із відомих властивостей інструменту, очевидної взаємозалежності мережі, наявної розвідувальної інформації або характеру самої цілі, посилання на складність кіберсередовища не може виправдати поверхневе планування.

Принцип обережності не зводиться до одноразового попереднього рішення. Якщо під час підготовки або безпосередньо перед реалізацією кібератак з'являються нові дані про тісніший зв'язок цілі з цивільними сервісами чи про ризик

ширшого поширення шкідливого інструменту, початковий план має бути переглянутий. За потреби це може означати зміну параметрів, відкладення або скасування операції [1].

Оцінка обраного засобу повинна охоплювати і його власну надійність. У цифровому середовищі контроль над інструментом не є даністю, тому під час планування має враховуватись, чи не може дія шкідливого коду бути змінена, поширена або відхилена від початкового алгоритму так, що створить додатковий ризик для цивільних систем.

Порушення принципу обережності під час планування кібератак має самостійне міжнародно-правове значення. Якщо сторона конфлікту не перевіряє ціль, ігнорує відомі мережеві залежності, використовує очевидно неконтрольований інструмент або не переглядає рішення після появи нових даних про цивільні ризики, таке неналежне планування може становити порушення відповідних звичаєвих норм міжнародного гуманітарного права [3].

Водночас не кожна помилка прогнозу автоматично свідчить про порушення міжнародного гуманітарного права. Оцінка має враховувати обсяг доступної інформації, часові межі, технічну складність системи, характер інструменту, ймовірність непрямих наслідків, наявність менш небезпечних альтернатив і сумлінність процесу планування. Такий підхід дає змогу зберегти баланс між гуманітарною спрямованістю права та реалістичністю його застосування у цифровому середовищі.

У цьому контексті важливо підкреслити, що принцип обережності є не лише технічним, а й юридичним стандартом. Він не вичерпується кібербезпековою перевіркою або розвідувальним аналізом, а потребує правової оцінки очікуваного впливу: чи є ціль військовою, чи не буде побічна шкода надмірною, чи не створює засіб ризику невибіркової дії та чи є він достатньо контрольованим.

Висновки. Принцип обережності під час планування кібератак має комплексний міжнародно-правовий зміст і охоплює перевірку цифрової цілі, оцінку засобу і методу нападу, аналіз прямих, непрямих і каскадних наслідків, врахування втрати функціональності, вибір менш небезпечної альтернативи та перегляд рішення у світлі нової інформації. У кіберпросторі цей принцип не може зводитися до формальної ідентифікації військової цілі, оскільки цифрові системи часто мають подвійне призначення і можуть бути пов’язані з цивільно значущими сервісами. Саме тому належне планування кібератаки повинно поєднувати технічний аналіз цифрового середовища з його правовою оцінкою, зокрема щодо військового характеру цілі, контрольованості обраного засобу, ризику невибіркової дії та можливості надмірної побічної шкоди.

Застосування принципу обережності визначається критеріями практичної можливості та розумної передбачуваності. Міжнародне гуманітарне право не

вимагає абсолютного знання про всі можливі наслідки кібератаки, але зобов'язує сторону конфлікту належно використовувати доступну інформацію, не ігнорувати очевидні ризики та здійснювати сумлінну передопераційну оцінку. Перспективи подальших досліджень пов'язані з уточненням правового значення втрати функціональності, статусу даних у міжнародному гуманітарному праві та критеріїв оцінки належного планування кібератак.

Список використаних джерел

1. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 57. URL: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-57 (дата звернення: 10.10.2025).
2. Commentary of 1987 to Article 57 of Protocol Additional I of 1977. *International Committee of the Red Cross.* URL: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-57/commentary/1987 (дата звернення: 15.10.2025).
3. Customary International Humanitarian Law. Rules 15–19. *International Committee of the Red Cross.* URL: https://ihl-databases.icrc.org/en/customary-ihl/v1 (дата звернення: 25.10.2025).
4. International Humanitarian Law and Cyber Operations during Armed Conflicts. *International Committee of the Red Cross.* 2019. URL: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (дата звернення: 5.11.2025).
5. International humanitarian law and the challenges of contemporary armed conflicts. *International Review of the Red Cross.* 2024. Vol. 106, № 927. P. 1357–1450. DOI: 10.1017/S181638312400064X. URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2025-03/reports-and-documents-ihl-and-the-challenges-of-contemporary-armed-conflicts-927.pdf (дата звернення: 1.12.2025).
6. Gisel L., Rodenhäuser T., Dörmann K. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross.* 2020. Vol. 102. P. 1–48. DOI: 10.1017/S1816383120000387. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2020-ICRC-IHL-and-Protection-of-Civilians-against-Effects-of-Cyber-Operations-during-Armed-Conflict.pdf (дата звернення: 15.11.2025).
7. Breeze E. J. Duty to act on knowledge: precautions, intelligence and the law of armed conflict. *Journal of Conflict and Security Law.* 2024. Vol. 29, iss. 3. P. 311–329. DOI: 10.1093/jcsl/krae015. URL: https://academic.oup.com/jcsl/article/29/3/311/7915959 (дата звернення: 1.12.2025).
8. Biggio G. Regulating non-kinetic effects of cyber operations: the Loss of Functionality approach and the military necessity-humanity balance under International Humanitarian Law. *Journal of Conflict and Security Law.* 2025. Vol. 30, iss. 2. P. 241–263. DOI: 10.1093/jcsl/kraf008. URL: https://academic.oup.com/jcsl/article/30/2/241/8108791 (дата звернення: 21.01.2026).
9. Pomson O. Objects? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law.* 2023. Vol. 28, iss. 2. P. 349–387. DOI: 10.1093/jcsl/krad002. URL: https://academic.oup.com/jcsl/article/28/2/349/7010697 (дата звернення: 2.02.2026).

Oleksandr Paseshnyk. The Application of the Principle of Precaution in the Planning of Cyberattacks

The article examines the elements of the principle of precaution in the planning of cyberattacks in the context of the application of international humanitarian law to contemporary armed conflicts. The relevance of the topic is determined by the fact that cyberattacks may affect not only military systems but also civilian infrastructure necessary for ensuring the vital needs of the

population. In cyberspace, the distinction between military and civilian objects is often technically blurred, since the same networks, servers, software platforms, data-processing systems or communication channels may simultaneously be used for military and civilian purposes.

It is substantiated that the principle of precaution, enshrined in Article 57 of Additional Protocol I to the Geneva Conventions of 1949 and confirmed by customary rules of international humanitarian law, cannot be interpreted in cyberspace merely as a formal requirement to verify the military character of a target. Its content includes functional assessment of a digital system, analysis of its connection with civilian services, verification of the controllability of the cyber means, assessment of the risk of self-propagation of malicious code, anticipation of direct and indirect consequences, and selection of a less harmful alternative where several possible ways of achieving a military advantage are available.

Particular attention is paid to the loss of functionality, the status of computer data and the cascading effects of cyberattacks. It is demonstrated that, for assessing the lawfulness of planning a cyberattack, not only the possibility of physical damage to an object is relevant, but also the risk of disrupting the functioning of systems on which the civilian population depends. The article concludes that the principle of precaution in cyberspace should be understood not only as an obligation of restraint, but also as an obligation of proper prior knowledge of the digital environment. The limits of this obligation are determined by the criteria of practical feasibility and reasonable foreseeability; however, the technical complexity of cyberspace cannot justify superficial planning or the disregard of obvious risks to the civilian population.

Keywords: *international humanitarian law, ICRC, precautionary measures, civilian population, civilian objects, armed conflict, consequences, cyberspace.*

Дата першого надходження статті до видання: 11.04.2026 р.
Дата прийняття статті до друку після рецензування: 19.04.2026 р.