УДК 34:342/35

ДОВГАНЬ О.Д., *доктор юридичних наук, професор,* радник при дирекції
ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-3453-4938.
ТКАЧУК Т.Ю., *доктор юридичних наук, професор,* в.о. керівника наукової
лабораторії інформаційної та кібернетичної безпеки
ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-4620-3300.

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ВИМІР

Анотація. *У статті досліджуються правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури, що є фундаментальним елементом національної безпеки у сучасному світі. Об'єкти критичної інфраструктури, такі як енергетичні системи, транспортні мережі, банківський сектор та державні установи, становлять особливу цінність і водночас є найбільш вразливими до кіберзагроз. З урахуванням постійного зростання кількості та складності кіберінцидентів, забезпечення правового регулювання цієї сфери є ключовим викликом для держав. Проаналізовано національне законодавство України, зокрема законодавчі акти, що регулюють кібербезпеку критичної інфраструктури, такі як Закон України "Про основні засади забезпечення кібербезпеки України" та суміжні нормативно-правові акти. Досліджено, наскільки ці документи відповідають сучасним викликам, включно з умовами воєнного стану, зростаючою цифровізацією та глобалізацією кіберзагроз. Особливу увагу приділено механізмам захисту інформації та міжвідомчій координації, а також їхній ефективності у практичній реалізації. Розглянуто міжнародний досвід у сфері кібербезпеки, зокрема підходи, впроваджені в Європейському Союзі, США та інших країнах. Здійснено аналіз ключових міжнародних стандартів і рекомендацій, таких як NIST, ISO/IEC 27001, Європейська Директива NIS2, що спрямовані на підвищення стійкості критичної інфраструктури до кіберзагроз. Показано, як міжнародне співробітництво та інтеграція у глобальні ініціативи, включаючи НАТО, ОБСЄ та ЄС, можуть сприяти вдосконаленню кібербезпеки на національному рівні. Результати роботи виявили низку проблем, що ускладнюють ефективне правове регулювання кібербезпеки в Україні: відсутність комплексного підходу до управління кіберризиками, слабка інтеграція міжнародних стандартів у національне законодавство, обмежені ресурси для реагування на кіберзагрози. У роботі запропоновано конкретні шляхи вдосконалення правового регулювання, серед яких гармонізація національного законодавства з міжнародними нормами, розробка чітких механізмів співпраці між державними органами, приватним сектором і міжнародними партнерами, а також посилення навчання фахівців у сфері кібербезпеки. Робота підкреслює важливість стратегічного планування у сфері кібербезпеки, формування довгострокової державної політики та активного залучення міжнародних організацій до розвитку цієї галузі.*

Ключові слова: *кібербезпека, критична інфраструктура, правове регулювання, національна безпека, кіберзагрози, Міжнародне гуманітарне право, Міжнародний кримінальний суд.*

Summary*. The article examines the legal aspects of ensuring cybersecurity of critical infrastructure, which is a fundamental element of national security in the modern world. Critical infrastructure, such as energy systems, transport networks, the banking sector and government institutions, are of particular value and at the same time are the most vulnerable to cyber threats. Given the constant increase in the number and complexity of cyber incidents, ensuring legal*

regulation of this area is a key challenge for states. The paper analyzes the national legislation of Ukraine, in particular the legislative acts regulating the cybersecurity of critical infrastructure, such as the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" and related regulatory legal acts. It examines the extent to which these documents meet modern challenges, including the conditions of martial law, increasing digitalization and globalization of cyber threats. Particular attention is paid to information protection mechanisms and interdepartmental coordination, as well as their effectiveness in practical implementation. The article also considers international experience in the field of cybersecurity, in particular the approaches implemented in the European Union, the USA and other countries. An analysis of key international standards and recommendations, such as NIST, ISO/IEC 27001, and the European NIS2 Directive, is carried out, which are aimed at increasing the resilience of critical infrastructure to cyber threats. It shows how international cooperation and integration into global initiatives, including NATO, OSCE and EU, can contribute to improving cybersecurity at the national level. The results of the study revealed a number of problems that complicate the effective legal regulation of cybersecurity in Ukraine: the lack of a comprehensive approach to cyber risk management, weak integration of international standards into national legislation, limited resources to respond to cyber threats. The paper proposes specific ways to improve legal regulation, including harmonizing national legislation with international norms, developing clear mechanisms for cooperation between government agencies, the private sector and international partners, as well as strengthening the training of cybersecurity specialists. The paper emphasizes the importance of strategic planning in the field of cybersecurity, the formation of long-term state policy and the active involvement of international organizations in the development of this industry. The article may be useful for academics, civil servants, private sector representatives and international experts dealing with cybersecurity, information security and legal regulation in the context of digitalization.

Keywords: *cybersecurity, critical infrastructure, legal regulation, national security, cyber threats, International humanitarian law, ICC.*

Постановка проблеми. Критична інфраструктура (далі – КІ) є основою функціонування сучасного суспільства. Вона включає транспортні системи, енергетику, фінанси, зв'язок, охорону здоров'я та інші сфери, чия стабільна робота є ключовою для економічної та національної безпеки держави. Сучасні об'єкти критичної інфраструктури дедалі більше інтегруються у цифрове середовище, що підвищує їхню ефективність, але водночас робить вразливими до кіберзагроз.

Безпека життєво важливих системних мереж і ресурсів, від яких залежить функціонування економіки та суспільства, є ключовою складовою поняття кібербезпеки критичної інфраструктури. Захист таких інфраструктур від кібератак є не лише обов'язковою умовою їх стійкого функціонування, але й потребує впровадження високоякісних, системних політик і заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів.

Захист критичної інфраструктури (далі – ЗКІ) передбачає впровадження заходів та практик, спрямованих на забезпечення безперервної роботи цих систем та захист від потенційних загроз, таких як кібератаки, природні катастрофи та терористичні акти. Це включає використання систем управління та збору даних (SCADA) та промислових систем управління (ICS), які є ключовими для функціонування секторів, як-от енергетика, транспорт та сільське господарство. Однак захист критичної інфраструктури в умовах цифрової трансформації стає дедалі складнішим завданням. Глобалізація, розвиток технологій і зростання взаємозв'язків між системами породжують нові ризики. Кібератаки на критичну інфраструктуру можуть не лише завдати економічних збитків, але й спричинити соціальні потрясіння, а також загрожувати життю громадян. У зв'язку з цим захист таких об'єктів стає стратегічним пріоритетом для урядів, бізнесу та міжнародних організацій.

Метою статті є визначення правових аспектів забезпечення кібербезпеки об'єктів критичної інфраструктури, національних та міжнародних підходів до регулювання цієї сфери, виявлення проблем правового забезпечення кібербезпеки та запропонувати рекомендації щодо вдосконалення відповідного законодавства і практик в умовах сучасних цифрових викликів.

Для реалізації визначеної мети передбачається вирішення таких наукових завдань: здійснити теоретичний аналіз критичної інфраструктури як об'єкту кіберзагроз; виявити проблеми правового забезпечення кібербезпеки в Україні; оцінити роль міжнародного співробітництва у зміцненні кібербезпеки критичної інфраструктури України; розробити рекомендації щодо вдосконалення правового регулювання кібербезпеки критичної інфраструктури.

Виклад основного матеріалу. З точки зору кібербезпеки, критичну інфраструктуру можна назвати складною взаємопов'язаною екосистемою, яка включає активи, системи та мережі, що надає нам необхідні функції, необхідні для нашого способу життя, такі як транспортні та комунікаційні системи, лінії водопостачання та електропередачі тощо.

Виклики, пов'язані із ЗКІ, включають:

• *складні кібератаки:* зловмисники націлюються на мережі КІ, включаючи урядових та сторонніх постачальників, використовуючи передові кібератаки, які можуть порушити основні послуги, викрасти конфіденційну інформацію та підготувати ґрунт для майбутніх атак;

• *широкий спектр цілей:* кібератаки на КІ можуть впливати на різні сектори, від енергетичних систем та ядерних ресурсів до водопостачання, авіації та сільського господарства;

• *еволюція загроз:* кіберзагрози постійно розвиваються, стають більш складними та швидко поширюються, що ускладнює організаціям підтримання належного рівня безпеки;

• *ручні процеси:* традиційно моніторинг кіберзагроз та оцінка заходів безпеки здійснювалися вручну, що часто призводило до обмеженої видимості та затримок у реагуванні на нові загрози;

• *потреба в ефективному зборі розвідданих:* для ефективної протидії цим загрозам урядам та агентствам необхідні ефективні методи збору та аналізу розвідданих про кіберзагрози. Ця інформація є критично важливою для розробки ефективних стратегій та політик безпеки;

• *обмежена видимість:* багато організацій, відповідальних за захист національної безпеки, стикаються з обмеженою видимістю кібербезпеки КІ, що ускладнює прийняття обґрунтованих рішень.

Кіберзахист об'єктів критичної інфраструктури України наразі стикається з серйозними викликами, які обумовлені як внутрішніми факторами, так і зовнішніми загрозами, головною з яких є військова агресія рф. Актуальність цієї проблематики зростає у зв'язку з наростаючою інтенсивністю та складністю кібератак на державні та приватні об'єкти, які є життєво важливими функціями суспільства [1].

На сьогодні можемо констатувати такі основні виклики у сфері кіберзахисту національної критичної інфраструктури:

1. Цілеспрямовані атаки на критичну інфраструктуру. Російські кібератаки, спрямовані на енергетичний сектор, водопостачання, транспорт та фінансові установи, мають на меті дестабілізацію економіки України та створення соціальної напруги. Такі атаки часто є частиною гібридної війни і мають координацію з військовими операціями. Одним із прикладів є використання шкідливого програмного забезпечення, такого як

“Industroyer” та “NotPetya”, яке завдало значної шкоди енергетичній та фінансовій системам України в попередні роки.

2. Використання передових кіберзагроз. Російські хакерські угруповання, зокрема APT28 (Fancy Bear) та Sandworm, використовують сучасні технології, такі як автоматизовані ботнети, інструменти соціальної інженерії, а також складні багаторівневі методи проникнення в мережу. Це вимагає від захисників постійного вдосконалення засобів виявлення та запобігання.

3. Нестача кваліфікованих фахівців. Захист об’єктів критичної інфраструктури потребує високого рівня компетенції спеціалістів, здатних оперативно реагувати на загрози. Однак в Україні є нестача кадрів із достатнім досвідом у сфері кібербезпеки, що ускладнює ефективну протидію новітнім загрозам.

4. Низький рівень захищеності об’єктів. Багато об’єктів критичної інфраструктури мають застарілу технічну базу, яка не відповідає сучасним вимогам кібербезпеки. Відсутність достатнього фінансування для модернізації та впровадження ефективних заходів захисту робить ці об’єкти вразливими до зовнішніх атак.

5. Розвідувальні операції та шпигунство. Росія активно використовує кіберпростір для збору розвідувальної інформації, що включає компрометацію інформаційних систем державних установ та стратегічно важливих об’єктів. Такі дії становлять загрозу національній безпеці, отримані дані можуть бути використані для наступних атак.

Захист критичної інфраструктури у цифрову епоху став одним із найбільш актуальних викликів для державної безпеки. Події, що сталися і продовжують відбуватися в Україні, яскраво демонструють, як кібератаки можуть перетворитися на інструмент геополітичного впливу та військових дій. Одними з перших прикладів таких атак були інциденти, які стосувалися енергомережі України у 2015 та 2016 роках. Ці події стали поворотним моментом у розумінні кіберзагроз, відкривши нову сторінку в історії глобальної кібербезпеки.

У грудні 2015 року Україна вперше зазнала масштабного знеструмлення, спричиненого кібератакою, внаслідок якої сотні тисяч громадян залишилися без електропостачання. Наступного року сталася друга атака, коли п’ята частина Києва опинилася в темряві. Ця атака була здійснена з використанням спеціалізованого шкідливого програмного забезпечення, розробленого для автономного порушення роботи енергетичної інфраструктури. Обидва інциденти продемонстрували ескалацію ризиків, пов’язаних із кіберзагрозами.

Через шість років, у 2022 році, під час широкомасштабного російського вторгнення в Україну, було зафіксовано спробу об’єднання кінетичних і кібератак для паралізації української енергомережі. Ці атаки не лише завдали значних збитків, але й засвідчили зростаючу складність методів, що використовуються в кібервійнах.

Злочинні кампанії, організовані російськими спецслужбами, набули багатовекторного характеру, включаючи шпигунство, дезорганізацію та маніпулятивну соціальну інженерію. Метою таких дій є послаблення захисту України, компрометація конфіденційних даних і проникнення в безпечні канали зв’язку.

Групи передової постійної загрози (APT), зокрема Gamaredon, значно посилили свої атаки після початку повномасштабного вторгнення. Наприклад, група UAC-0184 намагалася використати програми обміну повідомленнями, такі як Signal, для зараження пристроїв українських військових шкідливим програмним забезпеченням, маскуючи файли під відео бойових дій або матеріали для вербування [2].

У грудні 2023 року одна з найбільших кібератак, організована угрупованням “Солнцепьок”, порушила роботу системи повітряної тривоги, що ускладнило

оповіщення про авіаудари. Ця атака на "Київстар" стала важливим сигналом для міжнародної спільноти щодо зростаючих загроз кібербезпеці [3].

Попри те, що Римський статут не містить прямих згадок про кіберзлочини, існує зростаючий консенсус щодо їх розгляду як можливих військових злочинів. За словами прокурора Міжнародного кримінального суду (далі – МКС) Каріма Хана, подібні дії потенційно можуть відповідати ознакам злочинів проти людства або військових злочинів, особливо якщо вони спрямовані на цивільну інфраструктуру.

Дослідники з Центру прав людини Каліфорнійського університету вже подали до МКС низку документів, в яких йдеться про випадки російських кібератак, які вразили енергетичні системи, фінансові установи та інші об'єкти цивільного значення. Серед цих інцидентів особливе місце посідає атака NotPetya у 2017 році, яка завдала світовій економіці збитків на понад 10 мільярдів доларів.

Інциденти, пов'язані з атакою на супутникові модеми Viasat у перші дні вторгнення, демонструють ширший масштаб кібервійни, що охоплює не лише Україну, але й низку європейських країн. Такі дії вказують на системний характер російських кіберкампаній, які створюють значні ризики для міжнародної стабільності.

Досвід України в протидії кіберзагрозам підкреслює необхідність міжнародного співробітництва у сфері кібербезпеки, вдосконалення технологій захисту та посилення правового регулювання. Прогрес у розслідуванні кібератак як міжнародних злочинів може стати важливим прецедентом для глобального правопорядку. Водночас, продовження агресивної кібердіяльності з боку рф вимагає постійного вдосконалення стратегій захисту та посилення міжнародної координації в умовах гібридних загроз.

Під час російсько-української війни було зафіксовано численні кібератаки на українську критичну інфраструктуру, зокрема на енергетичну мережу, банки та системи зв'язку. Деякі з цих атак були настільки масштабними, що можуть вважатися військовими злочинами. Наприклад, атака NotPetya у 2017 році завдала глобальних збитків на суму понад 10 мільярдів доларів, вразивши понад 60 країн.

Крім того, атака на супутникові модеми Viasat, що була здійснена в день повномасштабного вторгнення росії в Україну, вплинула на кілька європейських країн, створюючи прецедент для міждержавних кіберконфліктів.

У сучасному світі кібератаки стали невід'ємною частиною воєнних дій, створюючи нові виклики для міжнародного права та безпеки. Події останніх років, зокрема широкомасштабне російське вторгнення в Україну, висвітлили критичну важливість вирішення правових питань, пов'язаних із кіберопераціями. Як і традиційні засоби ведення війни, кібероперації у воєнний час мають підпадати під дію норм Міжнародного гуманітарного права (далі – МГП). Водночас, технологічний розвиток ускладнює їх регулювання, зокрема через відсутність чіткої правової бази.

Швидкий розвиток цифрових технологій суттєво змінив обличчя сучасного світу. Кіберпростір став невід'ємною частиною нашого життя, однак водночас він став ареною для нових видів злочинної діяльності. Кібератаки на критичну інфраструктуру, викрадення персональних даних, маніпуляції інформацією – це лише деякі з викликів, з якими стикається сучасне суспільство. У відповідь на ці виклики МКС зіштовхується з необхідністю адаптації своєї діяльності до нових реалій.

Існує загальна згода, що МГП, як і будь-яке інше міжнародне право, застосовується до всіх форм воєнних дій, включаючи кібероперації. Це підтвердив Міжнародний суд ООН ще у 1996 році, зазначивши, що МГП стосується будь-яких видів зброї, незалежно від їхньої природи. У контексті кібероперацій це означає, що:

- заборонено націлювання на цивільні об'єкти та невибіркові атаки;

• медичні служби та персонал мають отримувати захист навіть у разі використання новітніх засобів ведення війни.

Міжнародний Комітет Червоного Хреста (далі – МКЧХ), як головний гарант дотримання МГП, наголошує, що кібероперації під час збройних конфліктів мають підлягати тим самим обмеженням, що й традиційні засоби війни. Якщо ефекти кібероперацій можна прирівняти до наслідків кінетичних атак, наприклад, бомбардувань, вони також можуть кваліфікуватися як дії, що розпочинають міжнародний збройний конфлікт. Проте, на сьогодні існує ряд правових викликів кібероперацій у контексті їх криміналізації, зокрема:

1. Відсутність прямої регуляції у міжнародному праві. Римський статут [4] не містить прямих згадок про кіберзлочини, оскільки він був створений до появи концепції кібервійни. Проте багато положень міжнародного права є технологічно нейтральними. Вони можуть застосовуватись до кібероперацій, якщо останні мають порівняний вплив із кінетичними атаками, такими як руйнування об'єктів критичної інфраструктури або цивільних мереж.

Катрін Німан-Меткалф, професор права Талліннського технологічного університету, вказує, що хоча адаптація чинного законодавства до кіберзлочинів може бути складною, вона є доцільнішою за створення нових законів, особливо враховуючи сучасний геополітичний контекст [5].

2. Проблеми атрибуції. Однією з найбільших складностей у розслідуванні кіберзлочинів є встановлення відповідальних осіб. Анонімність і глобальна природа кіберпростору дозволяють агресорам заперечувати свою причетність, що ускладнює судові процеси. Наприклад, держави можуть стверджувати, що кібератаки здійснювалися приватними особами, а не їхніми урядовими структурами.

3. Визначення тяжкості наслідків. Для того щоб кібератака підпадала під юрисдикцію МКС, вона повинна мати значний вплив, наприклад, завдавати шкоди цивільній інфраструктурі, позбавляти людей доступу до базових ресурсів або створювати загрозу життю. Оцінка таких наслідків може бути складною через їхній неочевидний характер, хоча довготривалий вплив таких дій може бути катастрофічним.

4. Участь цивільних у кібервійні. Зростаюча кількість цивільних хакерів, які беруть участь у збройних конфліктах, створює додаткові виклики для МГП. МКЧХ вважає це "тривожною тенденцією", оскільки цивільні особи не мають статусу комбатантів і в разі захоплення не підпадають під захист норм міжнародного права.

Щоб мінімізувати ризики, МКЧХ розробив вісім правил поведінки для цивільних хакерів, зокрема заборону націлюватися на цивільні об'єкти та зобов'язання дотримуватися принципу пропорційності. Однак навіть при виконанні цих правил межа між комбатантами і цивільними залишається розмитою, що ставить під загрозу як безпеку хакерів, так і цивільного населення загалом.

Інструменти, які використовують для здійснення серйозних міжнародних злочинів, постійно еволюціонують – від звичайної зброї, такої як куля до цифрових технологій, включно із соціальними мережами, Інтернетом та штучним інтелектом. У зв'язку з тим, що держава й інші суб'єкти дедалі частіше застосовують кіберпростір як інструмент управління і ведення війни, зловживання цим середовищем може сприяти або навіть прямо призводити до військових злочинів, злочинів проти людяності, геноциду чи актів агресії.

Міжнародне право, що регулює збройні конфлікти, забороняє напади на цивільні об'єкти відповідно до Женевських конвенцій. Проте наразі немає чітко визначених правових норм щодо того, що саме є кібервійськовим злочином. У 2017 році було

створено *"Талліннський посібник із застосування міжнародного права до кібервійни та кібероперацій"* [6], але навіть цей документ досі залишає відкритими деякі важливі питання.

Міжнародна спільнота дедалі більше схиляється до консенсусу, що кіберпростір не є сферою, вільною від правового регулювання, а підлягає чіткому формуванню норм міжнародного права. Офіс прокурора МКС вважає це важливим [7].

Кібероперації часто є елементом стратегії гібридної війни, яка діє на межі між станами війни та миру, законними й незаконними діями. Подібні дії часто прикриваються діяльністю проксі-акторів, що ускладнює їх ідентифікацію та притягнення до відповідальності. У такому контексті МКС за допомогою своєї юрисдикції може відігравати ключову роль у формуванні колективної міжнародної відповіді, що охоплює різні держави, корпорації та інституції.

Як центральний елемент системи міжнародного правосуддя, МКС може сприяти зміцненню правової відповідальності й зменшенню неоднозначності у розробці гібридних стратегій через чітке визначення правових меж та інсталяції істини. Співпраця з технологічними компаніями, зокрема корпорацією Microsoft, відкриває нові можливості для забезпечення правосуддя через інноваційні підходи, такі як використання штучного інтелекту та геопросторових даних.

Оскільки частота та інтенсивність кібератак зростають, виникає гостра необхідність удосконалювати інформаційну інфраструктуру та технічні можливості МКС. За активної підтримки держав, громадськості та технологічних компаній, МКС активно розширює співпрацю, спрямовану на модернізацію механізмів розслідування та захисту. Партнерства з такими гігантами, як Microsoft і Planet Labs, свідчать про важливість інновацій у контексті розслідування міжнародних злочинів.

Одним із ключових завдань є адаптація міжнародного кримінального права до реалій сучасних конфліктів, які дедалі частіше переносяться в кіберпростір. Аналіз злочинів, пов'язаних із кіберопераціями, вимагає комплексного підходу, який поєднує не лише традиційні юридичні аспекти, але й глибоке розуміння технічних особливостей таких дій. Використання штучного інтелекту, аналіз великих даних та дослідження кібернетичних атак на критичну інфраструктуру стають невід'ємною частиною сучасних розслідувань.

Співпраця МКС із державами-членами, міжнародними організаціями, приватним сектором та експертними спільнотами має вирішальне значення. Така співпраця не лише координує зусилля, але й сприяє розробці новітніх підходів до розслідування та притягнення до відповідальності за кіберзлочини. Водночас МКС залишається відданим захисту основоположних прав людини та принципу верховенства права.

Ліндсі Фріман із Центру прав людини Каліфорнійського університету Берклі зазначає, що унікальний характер кіберзасобів може навіть полегшити доведення намірів злочинців у порівнянні з традиційними військовими засобами. Водночас для успішного судового переслідування необхідна висока технічна компетентність і міжнародна співпраця. Карім Хан, прокурор МКС, наголошує, що суд працює над модернізацією своєї технічної бази для ефективного розслідування кіберзлочинів. Однак для забезпечення успіху необхідно не лише підвищити експертність судових органів, але й розширити міжнародну взаємодію для збору доказів та їхнього аналізу [8].

Особливу увагу необхідно приділити розробці інноваційних механізмів збору доказів у кіберпросторі. Інструменти на основі штучного інтелекту, геопросторового аналізу та алгоритмів для виявлення і запобігання злочинам можуть стати потужними засобами для забезпечення справедливості. МКС вже використовує подібні інструменти,

що демонструють їх ефективність у встановлених фактах і притягненнях до відповідальності порушника. Так, у травні 2023 року прокурор МКС Карім Хан оголошує про запуск розширеної платформи для надання доказів OTPLink, яка забезпечить чітку єдину точку доступу, замінивши різні системи та процеси, які раніше використовувалися для отримання інформації, включаючи подання відповідно до статті 15 Римського статуту [9].

Незважаючи на існуючі виклики, перспективи розвитку міжнародного кримінального правосуддя у сфері кібербезпеки є позитивними. Подальша інтеграція технологій у роботу МКС, розширення міжнародного співробітництва та розробка нових юридичних інструментів дозволять суду ефективніше боротися з кіберзлочинами та забезпечувати справедливість у цифрову епоху.

Міжнародний кримінальний суд відіграє важливу роль у боротьбі з кіберзлочинами. Завдяки своїй діяльності МКС сприяє зміцненню міжнародної безпеки та захисту прав людини в кіберпросторі. Однак для досягнення більших успіхів необхідно посилити міжнародне співробітництво, розробити нові юридичні інструменти та забезпечити ефективне використання технологій у правосудді.

Прокурори МКС розпочали розслідування масштабних російських кібератак на цивільну інфраструктуру України, кваліфікуючи їх як можливі військові злочини. Це перший відомий прецедент, коли міжнародна юстиція звернула свою увагу на кіберзлочини в контексті збройного конфлікту [10].

Отже, підсумовуючи зазначене вище, виокремимо ряд характерних тенденцій забезпечення ***кібербезпеки національних об'єктів критичної інфраструктури*** та розвитку міжнародного гуманітарного права:

• *націлювання на критичну інфраструктуру.* За даними слідства, російські хакерські угруповання здійснювали цілеспрямовані атаки на енергетичну систему, системи водопостачання та зв'язку України. Мета таких атак полягала в дестабілізації ситуації в країні, ускладненні гуманітарної допомоги та підриві морального духу населення. Зокрема, зловмисники намагалися вивести з ладу мобільні мережі, які використовувалися для оповіщення про повітряні тривоги.

• *потенційні наслідки для міжнародного права.* Розслідування МКС має потенціал створити новий прецедент у міжнародному гуманітарному праві. Якщо суд визнає, що кібератаки на критичну інфраструктуру з метою завдати шкоди цивільному населенню є воєнним злочином, це може призвести до розробки нових норм міжнародного права, які будуть регулювати проведення військових дій у кіберпросторі.

• *співпраця з Україною та міжнародними партнерами.* Українська сторона активно співпрацює з МКС, надаючи слідчим необхідні докази. Зокрема, Служба безпеки України передала інформацію про кібератаки на телекомунікаційну мережу "Київстар". Експерти вважають, що цей інцидент може бути кваліфікований як воєнний злочин відповідно до Талліннського посібника.

• *важливість розслідування.* Розслідування МКС є важливим кроком у напрямку встановлення відповідальності за кіберзлочини, вчинені в ході збройних конфліктів. Це також сприятиме підвищенню рівня обізнаності про загрози, які несуть у собі кібератаки, та стимулюватиме розробку ефективних засобів захисту від них.

Розслідування російських кібератак на Україну є знаковим моментом у розвитку міжнародного права. Воно демонструє, що кіберзлочини більше не можуть залишатися поза увагою міжнародної спільноти. За результатами цього розслідування можуть бути сформовані нові міжнародні стандарти, які допоможуть боротися з кібервійною та захищати цивільне населення від її наслідків.

Висновки.

Стратегія захисту національної критичної інфраструктури повинна включати:

- впровадження багаторівневого захисту: використання комплексних рішень, що поєднують різні технології та методи захисту, дозволяє ефективніше виявляти та реагувати на загрози;
- постійний моніторинг та аналіз: безперервний моніторинг мережевої активності та аналіз поведінки систем дозволяють виявляти аномалії та потенційні загрози на ранніх стадіях;
- оновлення та патчинг систем: регулярне оновлення програмного забезпечення та операційних систем є критично важливим для закриття відомих вразливостей;
- навчання та підвищення обізнаності персоналу: проведення тренінгів та освітніх програм для співробітників допомагає зменшити ризик успішних соціально-інженерних атак;
- розробка та тестування планів реагування на інциденти: наявність чітких планів дій у разі кіберінцидентів та регулярне їх тестування забезпечують швидке та ефективне реагування на загрози;
- співпраця між державним та приватним секторами: обмін інформацією про загрози та найкращі практики між різними організаціями сприяє підвищенню загального рівня кібербезпеки.

Захист критичної інфраструктури від кіберзагроз вимагає комплексного підходу, що поєднує технологічні рішення, організаційні заходи та людський фактор. Враховуючи постійний розвиток загроз, організації повинні бути готовими адаптувати свої стратегії та інструменти для забезпечення безперервності та надійності основних послуг. У цьому контексті, на основі аналізу розробленого Національним центром кібербезпеки (NCSC) Великобританії посібника для організацій, включаючи операторів критичної інфраструктури "Cyber Assessment Framework", рекомендуємо розробити та впровадити національний Посібник із покращення кібербезпеки підприємств, установ та організацій критичної інфраструктури.

Кібероперації у збройних конфліктах відкривають нову еру у веденні війни, яка потребує переосмислення існуючих правових норм. Хоча МГП залишається актуальним для регулювання кібероперацій, його адаптація до реалій цифрового світу є необхідною. Розробка технічної експертизи, міжнародна співпраця та інтеграція кіберзасобів у правові системи стають ключовими кроками на шляху до ефективного регулювання кібервійни. Український досвід у протидії кіберзагрозам слугує важливим уроком для міжнародної спільноти, демонструючи необхідність системного підходу до вирішення цієї проблеми.

Використана література

1. World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023. Forescout Research/Vedere Labs. Jan 29, 2024. URL: https://securitytoday.com/Articles/2024/01/29/World-Critical-Infrastructure-Suffered-13-Cyber-Attacks-Every-Second-in-2023.aspx

2. Бондар Г. Російські APT-групи продовжують атакувати Україну. – (УНІАН, 31.01.23). URL: https://www.unian.ua/techno/communications/rosiyski-apt-grupi-prodovzhuyut-atakuvati-ukrajinu-12128238.html

3. Хто стоїть за атакою на "Київстар" і коли відновлять зв'язок. – (BBC, 13.12.23). URL: https://www.bbc.com/ukrainian/articles/c51z82rdppxo

4. Rome Statute of the International Criminal Court. ICC. URL: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf

5. Karim A.A. Technology Will Not Exceed Our Humanity. Digital Front Lines. URL: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity

6. The Tallin Manual on International Law applicable to Cyber Warfare Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. URL: http://csef.ru/media/articles/3990/3990.pdf

7. ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink. Statement: 24 May 2023. URL: https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink

8. Anthony Deutsch, Stephanie van den Berg, James Pearson Exclusive: ICC probes cyber attacks in Ukraine as possible war crimes, sources say. *REUTERS*: 14 June 2024. URL: https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14

9. International Criminal Court. URL: https://otplink.icc-cpi.int

10. Матеріали справи за фактом кібератаки на "Київстар" спрямують на розгляд МКС. – (Укрінформ, 04.04.24). URL: https://www.ukrinform.ua/rubric-ato/3848169-illa-vituk-naca lnik-departamentu-kiberbezpeki-sbu.html

~~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~