**Нечай А., здобувач**
**Науковий керівник: Сапарова А. О.,**
**к.ю.н, доцент, доцент кафедри правового забезпечення безпеки бізнесу**
**Державний торговельно-економічний університет**

## ПРОБЛЕМИ МІЖНАРОДНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ ДЕРЖАВ У СФЕРІ ІНТЕРНЕТУ

Кіберпростір являє собою глобальне цифрове середовище, яке формує новий вимір взаємодії між державними та недержавними суб'єктами. Зростання кількості та масштабності кібероперацій підвищує важливість питання про дотримання норм міжнародного правопорядку. Згідно з базовими доктринальними підходами та офіційними позиціями провідних міжнародних інституцій, чинні норми міжнародного права, включно зі Статутом ООН, застосовуються до кіберпростору в повному обсязі [1, с. 1195]. Втім, серйозною проблемою залишається відсутність спеціалізованого міжнародного договору, який би комплексно регулював сферу інформаційних технологій. Як наслідок, державна практика та доктрина вимушені пристосовувати загальні принципи міжнародного права до умов цифрового середовища, що призводить до численних правових суперечностей. Відповідно до статті 1 Проєкту статей Комісії міжнародного права ООН про відповідальність держав за міжнародно-протиправні діяння 2001 року кожне міжнародно-протиправне діяння держави тягне за собою її міжнародну відповідальність. При цьому для виникнення такої відповідальності необхідно встановити, що відповідна поведінка може бути приписана державі та становить порушення її міжнародного зобов'язання.

Діяльність у кіберпросторі ґрунтується на ключових принципах міжнародного права. Один із них – принцип суверенної рівності та територіального суверенітету, згідно з яким держави мають суверенне право контролю над власною критичною кіберінфраструктурою. Неузгоджене проникнення агентів іншої держави або підконтрольних їм хакерів у комп'ютерні мережі може розглядатися як порушення її суверенітету [1, с. 1197]. Принцип невтручання у внутрішні справи підкреслює, що маніпуляція інформаційним середовищем, як-от кібершпигунство або вплив через соціальні мережі, є загрозою для демократичних інститутів. Проте, кваліфікація цих дій як втручання часто викликає суперечки. Також існує заборона на застосування сили, згідно з пунктом 2(4) Статуту ООН, яка ще не визнає інформаційні атаки окремим видом агресії на універсальному рівні, що ускладнює їх юридичну оцінку як акти збройної агресії. Щодо критеріїв збройного нападу та права на самооборону (стаття 51 Статуту ООН), в міжнародному праві тривають обговорення щодо порогу, коли кібероперація може бути визнана «збройним нападом». Концепція масштабу та наслідків враховує такі фактори, як масова загибель або поранення людей, велика фізична руйнація або параліч критичних об'єктів інфраструктури [1]. Якщо кібероперація досягає цих показників, постраждала держава може мати право на самооборону. Однак, оцінка таких критеріїв є вкрай складною через невловимість кіберпростору. Основною перешкодою у притягненні держав до міжнародно-правової відповідальності є проблема атрибуції, тобто технічне і юридичне встановлення відповідальності конкретної держави за кібератаки [2]. Держави часто використовують «кібернайманців», проксі-групи та хакерські угруповання, що ускладнює встановлення контролю держави над такими суб'єктами відповідно до високих юридичних стандартів, зокрема принципу ефективного контролю, якого дотримується Міжнародний Суд ООН. Додатковою складністю є те, що шкідливе програмне забезпечення може бути приховане через маршрутизацію через сервера нейтральних третіх держав, що маскує справжнє джерело атаки. У розслідуваннях міждержавних кіберінцидентів спостерігається брак уніфікованого набору правил щодо надання доказів у міжнародному праві. У міжнародному судочинстві тягар доказування переважно лежить на позивачі, який повинен довести факт протиправної поведінки з боку іншої держави. Заяви про самозахист у

відповідь на кібероперації повинні бути підтримані чіткими та переконливими доказами [1]. При розгляді справ Міжнародний Суд ООН надає найбільшу доказову вагу офіційним документам держав і уповноважених міжнародних організацій, таких як звіти органів ООН або офіційні заяви урядів.

Отже, головними проблемами міжнародно-правової відповідальності держав у кіберпросторі залишаються складність юридичної кваліфікації кібероперацій, встановлення їх належності конкретній державі та формування достатньої доказової бази. Незважаючи на те, що загальні норми міжнародного права застосовуються до кіберпростору, специфічний характер кібероперацій ускладнює практичну реалізацію механізмів міжнародно-правової відповідальності.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Карвацька С. Б., Маник А. З., Яремчук В. В. Кіберпростір: міжнародно-правове регулювання та практика застосування прецедентного права МС ООН. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 2. С. 1194–1199. DOI https://doi.org/10.24144/2788-6018.2025.02.180

2. Whyte Christopher and Brian Mazanec. Understanding Cyber Warfare: Politics, Policy and Strategy. London; New York, NY: Routledge Taylor & Francis Group. 2019.

**Новіцька С.В., здобувач**
**Науковий керівник: Павліченко Ірина Миколаївна,**
**старший викладач кафедри права, публічного управління та адміністрування**
**Державний університет «Житомирська політехніка»**

## ПРАВОВИЙ ЗАКОН У СУЧАСНІЙ УКРАЇНІ: СПІВВІДНОШЕННЯ ФОРМИ ТА ЗМІСТУ В КОНТЕКСТІ ВЕРХОВЕНСТВА ПРАВА

Проблема співвідношення права і закону є однією з важливих у сучасній теорії держави і права, оскільки вона пов’язана з визначенням меж державної влади, особливостями правового регулювання та забезпеченням прав людини. Закон займає центральне місце серед нормативно-правових актів, проте його прийняття компетентним органом із дотриманням установленої процедури не завжди дає змогу зробити висновок про належну якість його змісту. У зв’язку з цим важливого значення набуває розмежування закону як нормативно-правового акта, що має встановлену юридичну форму, та правового закону, зміст якого повинен відповідати основоположним принципам права. Метою дослідження є визначення співвідношення формальної законності та змістовної правомірності закону, а також з’ясування критеріїв його відповідності вимогам верховенства права.

У формально-юридичному розумінні закон є нормативно-правовим актом, який приймається Верховною Радою України в межах її конституційних повноважень і відповідно до встановленої процедури. Основні вимоги щодо прийняття законів визначені Конституцією України та конкретизовані в Регламенті Верховної Ради України [1; 2]. Дотримання компетенції суб’єкта правотворчості, установленого порядку прийняття акта та вимог щодо набрання ним чинності забезпечує належне юридичне оформлення законодавчих приписів. Водночас дотримання зазначених вимог не означає, що зміст закону в усіх випадках відповідає принципам справедливості, рівності та поваги до прав людини. Тому під час аналізу закону необхідно враховувати не лише порядок його прийняття, а й особливості правового регулювання, яке він установлює.

Як зазначає О. О. Томкіна, принцип верховенства права у сфері законодавчої діяльності передбачає необхідність прийняття законів, зміст і цілі яких пов’язані із забезпеченням прав людини, а форма та процедура відповідають установленим правовим вимогам [3, с. 112–119]. Такий підхід дає змогу розглядати правовий закон як теоретичну модель визначення якості