УДК 342.951:004.
DOI https://doi.org/10.32782/1813-338X-2025.1.35

Л. В. Сорока
доктор юридичних наук, професор, завідувачка відділу аспірантури і докторантури
Науково-дослідного інституту публічного права

О. О. Колесник
аспірант
Науково-дослідного інституту публічного права

МІЖНАРОДНО-ПРАВОВІ ПРИНЦИПИ РЕГУЛЮВАННЯ КІБЕРПРОСТОРУ: СУВЕРЕНІТЕТ, НЕВТРУЧАННЯ ТА DUE DILIGENCE

У статті здійснено теоретико-правовий аналіз принципів міжнародного права, що визначають поведінку держав у кіберпросторі, – суверенітету, невтручання та належної обачності (due diligence). Актуальність дослідження зумовлена трансформацією сучасного безпекового середовища, особливо в умовах триваючої збройної агресії проти України, що супроводжується масштабним використанням кіберзасобів і інформаційних операцій як інструментів гібридної війни. У цьому контексті зростає потреба в адаптації традиційних норм міжнародного права до цифрових реалій і забезпеченні їх ефективного застосування у сфері міжнародної кібербезпеки. Метою статті є розкриття змісту зазначених принципів, з'ясування їх сучасного тлумачення у міжнародній практиці та визначення їхньої ролі у формуванні міжнародно-правового режиму кіберзахисту. У роботі обґрунтовано, що суверенітет у кіберпросторі набуває функціонального змісту, поєднуючи право держави на контроль із позитивним обов'язком забезпечення безпеки власної кіберінфраструктури. Принцип невтручання тлумачиться крізь призму критерію примусу та застосовується лише до дій, спрямованих на обмеження суверенного вибору іншої держави. Принцип належної обачності розглядається як позитивний стандарт поведінки, що зобов'язує державу вживати належних заходів для запобігання використанню її території для шкідливих кібероперацій. Зроблено висновок, що міжнародне право повною мірою поширюється на кіберпростір і поступово формує узгоджену систему норм та практик відповідальної поведінки держав. Аргументовано доцільність кодифікаційного закріплення основних принципів у формі універсального договору, який би сприяв зміцненню міжнародної кіберстабільності та забезпеченню передбачуваного правопорядку у цифрову добу. Зроблено висновок, що міжнародне право формує нову якість правового режиму кіберпростору – таку, де суверенітет виступає не лише символом незалежності, а й індикатором відповідального управління, невтручання тлумачиться через призму недопустимості примусу, а належна обачність – як прояв солідарності та співпраці. Подальший розвиток цього напряму потребує кодифікаційного закріплення зазначених принципів у межах універсального міжнародного договору, який визначатиме стандарти відповідальної поведінки держав і механізми взаємодії у сфері кібербезпеки.

Ключові слова: *кібербезпека, інформаційна безпека, кіберзахист, національна безпека, правове регулювання, цифровий суверенітет.*

Актуальність теми. Сучасний етап розвитку міжнародних відносин характеризується стрімкою цифровізацією усіх сфер суспільного життя, що зумовило виникнення нової глобальної площини взаємодії – кіберпростору. У цьому середовищі дедалі частіше реалізуються процеси, здатні впливати на суверенітет держав, їхню політичну стабільність, обороноздатність та економічну безпеку. Ця обставина поставила перед міжнародним правом завдання осмислення його традиційних засад крізь призму нових технологічних реалій.

Попри визнання Організацією Об'єднаних Націй того, що міжнародне право повною мірою поширюється на кіберпростір, залишається відкритим питання визначення меж і змісту таких

базових принципів, як суверенітет, невтручання у внутрішні справи та належна обачність (*due diligence*). Адже саме вони формують нормативну основу взаємної відповідальності держав у цифровому вимірі. Однак відсутність чіткої кодифікації та усталеної практики застосування зазначених принципів призводить до неоднакового їх тлумачення у державній та доктринальній площинах, створюючи простір для правової невизначеності.

У цій ситуації науково-практична проблема полягає у необхідності глибокого аналізу природи та змісту міжнародно-правових принципів регулювання кіберпростору, з'ясування їхньої ролі в забезпеченні стабільності міжнародного правопорядку й формуванні системи колективної кібербезпеки. Вирішення цього завдання має не лише теоретичне, а й прикладне значення для подальшого удосконалення міжнародно-правового механізму запобігання, розслідування та нейтралізації кіберзагроз.

Аналіз останніх досліджень і публікацій. Проблематика міжнародно-правового регулювання діяльності держав у кіберпросторі займає сьогодні провідне місце у сучасній системі досліджень міжнародного публічного права. Вона охоплює питання визначення правового статусу кіберпростору, дії базових принципів міжнародного права у цифровому середовищі, меж державного суверенітету, а також проблеми міжнародної відповідальності за кіберінциденти.

У вітчизняній науковій думці вагомий внесок у дослідження цих питань зробили М. В. Камчатний, який одним із перших окреслив нормативно-правові засади міжнародного співробітництва у сфері кібербезпеки та наголосив на необхідності імплементації міжнародних стандартів у національне законодавство України [1]. Значну увагу до теоретико-правової природи кібербезпеки як складової системи інформаційного права приділяє В. С. Павленко, який підкреслює взаємозалежність між правовим режимом інформаційних ресурсів і забезпеченням кіберзахисту держави [2]. І. М. Сопілко у своїй праці проводить ґрунтовне порівняльно-правове дослідження понять «інформаційна безпека» та «кібербезпека», підкреслюючи потребу в гармонізації їх змісту у національній і міжнародній правовій термінології [3].

У світовій доктрині міжнародного публічного права питання кібербезпеки розглядаються крізь призму фундаментальних принципів міжнародного правопорядку. Серед зарубіжних авторів особливе місце належить Р. Бучану, який розмежовує категорії «застосування сили» та «втручання» у контексті кібероперацій і підкреслює необхідність формування чітких юридичних критеріїв для визначення правомірності таких дій [6]. М. Роскіні, спираючись на концепцію обмеженого застосування сили у кіберпросторі, доводить, що норми *jus ad bellum* і *jus in bello* можуть бути застосовані до кібероперацій з урахуванням їх фактичних наслідків [15].

Особливу роль у кодифікації міжнародно-правових підходів до діяльності держав у кіберпросторі відіграла колективна праця під редакцією М. Шмітта *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [16], у якій було систематизовано міжнародні принципи, що застосовуються до кібероперацій у мирний і воєнний час. Ці положення стали основою для подальших напрацювань ООНівських експертних груп – GGE (2015, 2021) та OEWG (2021–2025), котрі офіційно підтвердили, що міжнародне право, включно з принципами Статуту ООН, поширюється на діяльність у кіберпросторі [19; 20; 22].

Важливий внесок у розроблення концепції державної поведінки у цифровому середовищі зробили П. Рогуський, який у своїй праці *Application of International Law to Cyber Operations* [14] здійснив порівняльний аналіз офіційних позицій провідних держав щодо застосування міжнародного права до кібероперацій, та К. Mačák, котрий розглядає еволюцію нормотворчого процесу у сфері кіберправа – від «м'якого» до «жорсткого» права (*soft law → hard law*) [12].

Дослідження К. Баларабе [4] розширює поняття суверенітету, вводячи категорію «цифрових кордонів» як прояву державного контролю в інформаційній сфері. Д. Брудерс і Ф. Крістіано [5] аналізують феномен кібернорм у системі ООН, доводячи, що процес їх формування є компромісом між стратегічною невизначеністю та прагненням до універсальних «правил гри» у кіберпросторі. У цьому контексті праці М. Фіннемор та Д. Холліса [8], О. Гетевей і Р. Крутоф [9], а також Дж. Ная [13] висвітлюють політико-правові аспекти міжнародної взаємодії в цифровому середовищі, зокрема проблему легітимності звинувачень у кібератаках і створення багаторівневої системи глобального управління кіберпростором (*regime complex*).

Питання оновлення змісту класичних принципів міжнародного права у цифрову добу отри-

мало відображення у працях Н. Цагуріаса [17] та М. Фаррелла [18], які доводять, що принципи суверенітету, невтручання та належної обачності мають функціональний характер і потребують адаптації до особливостей мережевого середовища. Ці дослідження узгоджуються з концепціями Х. Коха [11] та Р. Гурвіца [10], котрі розглядають кіберпростір як сферу, де відбувається поступове поєднання норм міжнародного права і стандартів поведінки, вироблених міжнародними організаціями та багатосторонніми форумами.

Попри значну кількість наукових напрацювань, варто констатувати, що питання юридичної природи та співвідношення принципів суверенітету, невтручання і належної обачності (*due diligence*) у контексті міжнародного кіберправа залишаються недостатньо розробленими. Немає єдності у визначенні меж державної відповідальності за кіберінциденти, а також у кваліфікації актів, що не досягають порогу застосування сили, але створюють суттєві політичні чи економічні наслідки. Подальше теоретико-правове осмислення цих принципів є необхідною передумовою формування узгодженого міжнародно-правового режиму кіберпростору, що відповідає викликам колективної безпеки цифрової епохи.

Метою статті є теоретико-правовий аналіз змісту та сучасного тлумачення принципів суверенітету, невтручання і належної обачності (*due diligence*) у контексті їх застосування в кіберпросторі. Дослідження спрямоване на з'ясування їх еволюції під впливом цифровізації міжнародних відносин, визначення особливостей нормативного закріплення в актах ООН і доктрині міжнародного права, а також окреслення їхньої ролі у формуванні міжнародно-правового режиму відповідальної поведінки держав у сфері кібербезпеки.

Виклад основного матеріалу

1. Міжнародно-правовий статус кіберпростору

Кіберпростір не створює *sui generis* правопорядку, а функціонує в межах загальної системи міжнародного права. Цей підхід є спільним як для міжурядових процесів, так і для сучасної доктрини. У Звіті Групи урядових експертів ООН 2015 року наголошено, що «міжнародне право, зокрема принципи Статуту ООН, повною мірою застосовуються до діяльності держав у сфері інформаційно-комунікаційних технологій» [19]. У звіті Відкритої робочої групи (OEWG) 2021 року ця позиція отримала подальший розвиток: підкреслено необхідність забезпечення відповідальної поведінки держав, запобігання інцидентам у кіберпросторі та поглиблення співпраці задля зміцнення довіри [20]. Як слушно зазначає Г. Кох, кіберпростір не є «правовим вакуумом» – держави зобов'язані дотримуватися своїх договірних і звичаєвих обов'язків незалежно від форми та засобів їхньої реалізації [11].

Відсутність універсального міжнародного договору у сфері кібербезпеки компенсується еволюцією звичаєвих норм і розвитком механізмів *soft law*. Важливим орієнтиром у цьому процесі є *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, у якому систематизовано застосування норм *jus ad bellum* і *jus in bello* до кібероперацій та визначено критерії правомірності дій держав у мирний і воєнний час [16]. Водночас праці М. Роскіні, О. Гетевей та Р. Крутоф доводять, що встановлення порогів «втручання» й «застосування сили» в кіберпросторі сприяє формуванню узгоджених звичаєвих стандартів державної поведінки [15; 9].

Суттєве значення для розвитку міжнародно-правового регулювання мають офіційні позиції держав, узагальнені у порівняльному дослідженні П. Рогуського *Application of International Law to Cyber Operations* [14]. Аналіз цих документів свідчить, що національні підходи концентруються навколо чотирьох ключових принципів: суверенітету, невтручання, належної обачності (*due diligence*) та державної відповідальності. Саме їх взаємозв'язок і послідовне практичне застосування забезпечують стабільність правового режиму кіберпростору.

Як справедливо зауважує К. Mačák, сучасний етап розвитку міжнародного кіберправа характеризується переходом від «кібернорм» до «кіберправил» – тобто від політичних декларацій до формування звичаєвих норм, що спираються на усталену практику держав та *opinio juris* [12]. Цей процес відбувається в межах багаторівневої системи, яку Дж. Най визначає як «режимний комплекс»: у ній одночасно діють договірні, звичаєві та рекомендаційні механізми, які взаємодоповнюють один одного [13]. У цьому контексті особливе значення набувають механізми міжнародної легітимації – так звані інструменти «публічного осуду» (*naming and shaming*), що, за М. Фіннемор і Д. Холлісом, відіграють роль регуляторів поведінки держав поза межами формального примусу [8].

Таким чином, міжнародно-правовий статус кіберпростору формується як багаторівнева і гнучка система регулювання, у якій норми *hard law* (Статут ООН, звичаєві принципи, положення про відповідальність держав – ARSIWA) поєднуються з *soft law* інструментами (резолюції, рекомендації та керівні принципи процесів GGE та OEWG) [21; 19; 20; 22]. Така модель відображає сучасну тенденцію до гармонізації жорстких і м'яких форм права, що забезпечує адаптивність міжнародного правопорядку до технологічних змін. У межах цієї системи принципи суверенітету, невтручання та належної обачності постають не ізольованими категоріями, а взаємопов'язаними засадами відповідальної поведінки держав у цифровому середовищі.

2. Принцип суверенітету у кіберпросторі

У сучасних міжнародно-правових реаліях проблема суверенітету у кіберпросторі набуває принципового значення, оскільки саме вона визначає межі допустимої поведінки держав у цифровому середовищі. Традиційно суверенітет розглядався як невід'ємна ознака державності, що охоплює територіальну цілісність, політичну незалежність і верховенство влади в межах своєї юрисдикції. Однак цифрова трансформація глобального простору зумовила необхідність переосмислення цього поняття у контексті нових технологічних викликів.

Як слушно зауважує Н. Цагуріас, у кіберпросторі суверенітет постає не лише як право контролю над національними інформаційними ресурсами, а й як обов'язок держави забезпечувати належне функціонування й захист своєї цифрової інфраструктури, запобігаючи використанню власної території для завдання шкоди іншим суб'єктам [17]. Таким чином, суверенітет у кіберсфері набуває не лише декларативного, а й функціонального змісту, поєднуючи владну компетенцію з юридичною відповідальністю.

Офіційні позиції держав у цій сфері демонструють різні підходи до розуміння меж суверенітету. Франція у своєму документі *International Law Applied to Operations in Cyberspace* (2019) чітко визначила, що будь-яке несанкціоноване проникнення в інформаційні системи, розташовані на її території, розцінюється як порушення державного суверенітету, незалежно від наслідків таких дій [14]. Велика Британія, навпаки, у заяві Генерального прокурора 2022 року (*International Law in Future Frontiers*) зазначила, що суверенітет не є самостійною нормою, порушення якої автоматично тягне міжнародно-правову відповідальність, а виступає загальним принципом, що набуває юридичного значення лише у поєднанні з конкретними протиправними діями, наприклад із втручанням у внутрішні справи чи застосуванням сили [14].

У науковій літературі також спостерігається плюралізм підходів. Так, М. Шмітт, редактор *Tallinn Manual 2.0*, вказує, що суверенітет не слід абсолютизувати: він має тлумачитися як принцип, який конкретизується через інші норми міжнародного права – невтручання, заборону застосування сили, належну обачність та відповідальність держав [16]. Подібної думки дотримується і М. Роскіні, який вважає, що правомірність кібероперації залежить не від самого факту проникнення у системи іншої держави, а від наявності реального впливу на здійснення її суверенних функцій, заподіяння шкоди або примусу [15].

Особливий інтерес становить концепція К. Баларабе, який у контексті глобалізації цифрових потоків обґрунтовує необхідність «обмежувального» підходу до розуміння суверенітету: держава не може претендувати на абсолютний контроль над усім інформаційним простором, адже природа Інтернету є транскордонною. На його думку, правова оцінка кібероперації має базуватися на принципі пропорційності та зважуванні інтересів – наявності реальної шкоди чи втручання у владні функції [4].

Аналіз офіційних позицій держав і доктринальних джерел дозволяє виокремити три основні підходи до тлумачення суверенітету в кіберпросторі:

– *абсолютний* – будь-яке несанкціоноване втручання в інформаційні системи на території держави є порушенням її суверенітету (характерний для позиції Франції, частково Ірану).

– *функціональний* – суверенітет виступає рамковим принципом, який сам по собі не створює окремої підстави для міжнародно-правової відповідальності (США, Велика Британія, підтримується більшістю експертів *Tallinn Manual*) [16].

– *обмежувальний* (*пропорційний)* – допускає, що певні транскордонні кібероперації не є порушенням суверенітету, якщо вони не мають примусового характеру та не завдають шкоди основним державним функціям (Нідерланди, Італія, концептуально – Баларабе) [4; 14].

Отже, у сучасній міжнародно-правовій доктрині відбувається поступовий перехід від класичного територіального до функціонально-від-

повідального розуміння суверенітету. Його зміст визначається не стільки просторовими межами, скільки спроможністю держави забезпечувати контроль і безпеку в цифровому середовищі, не завдаючи шкоди іншим суб'єктам міжнародного права. Такий підхід узгоджується з тенденцією до поєднання принципів суверенітету, невтручання та належної обачності як взаємопов'язаних елементів єдиного міжнародно-правового режиму кіберпростору [17; 14; 16; 15; 4].

Принцип невтручання у внутрішні справи. У класичній доктрині принцип невтручання випливає із суверенітету й охоплює заборону примусових дій держави в сферах, що належать до *domaine réservé* іншої держави (зокрема визначення політичного курсу, виборчі процеси, формування уряду). Міжнародний Суд ООН у справі *Nicaragua v. United States of America* (1986) визначив, що втручання є протиправним лише тоді, коли воно має примусовий характер і спрямоване на обмеження суверенного вибору держави у сферах її внутрішньої компетенції (політичної, економічної чи соціальної). Цей підхід став класичною основою для подальших доктринальних розробок у сфері міжнародного кіберправа, що узагальнено у працях Р. Бучана, М. Роскіні та у *Tallinn Manual 2.0* [6; 15; 16].

Пороговий критерій – примус. Р. Бучан пропонує застосовувати «нікарагуанський» тест безпосередньо до кібероперацій: втручання має місце тоді, коли кіберзасоби спонукають або змушують іншу державу змінити поведінку у її суверенній сфері (напр., вплив на оборонні рішення, вибори, внутрішнє адміністрування) [6]. Аналогічний підхід відображено у *Tallinn Manual 2.0*: незаконним втручанням визнаються операції, які, не досягаючи порогу «застосування сили», коерсивно порушують здійснення державних функцій у *domaine réservé*; натомість дії, що не мають примусового характеру, залишаються поза сферою заборони невтручання (хоч можуть порушувати інші норми) [16]. На необхідності оцінювати інтенсивність і наслідки впливу наголошує і М. Роскіні, підкреслюючи, що не кожен дистанційний технічний ефект автоматично дорівнює правопорушенню: вирішальними є спрямованість на суверенні прерогативи та реальний вплив на їх здійснення [15].

Інформаційні операції та межа допустимого. Найбільш дискусійним залишається питання кваліфікації інформаційних кампаній. У науковій літературі відрізняють: (а) переконання/пропаганду як форму політичного висловлювання держави у зовнішніх зносинах; (б) координований примусовий вплив (напр., злам і маніпуляція виборчою інфраструктурою, примусове перешкоджання функціям органів влади). Лише другий різновид зазвичай підпадає під заборону невтручання [16; 15; 6]. Водночас сучасна практика підкреслює роль «репутаційних» механізмів реагування на операції, що не досягають порога правопорушення: інструменти публічного осуду та приписування (*naming and shaming*, дипломатичні демарші) виконують регулятивну функцію поза сферою примусу, сприяючи формуванню стандартів відповідальної поведінки держав [8].

У застосуванні до кіберпростору принцип невтручання зберігає ядро норми – вимогу примусу та орієнтацію на суверенні сфери іншої держави. Кваліфікація конкретної операції залежить від: (1) спрямованості на *domaine réservé*; (2) наявності коерсивного елементу; (3) інтенсивності/наслідків для здійснення державних функцій. Такий підхід узгоджується з провідною доктриною і квазікодифікаційними орієнтирами *Tallinn Manual 2.0*, забезпечуючи послідовність між класичною практикою МС ООН і сучасною природою кібероперацій [16; 6; 15; 8].

Принцип належної обачності (due diligence). Походження принципу *due diligence* сягає загального міжнародного права та практики міжнародних судових органів. У справах Trail Smelter (1941) та Corfu Channel (1949) сформульовано ключову ідею: держава не повинна допускати, щоб її територія використовувалася для завдання шкоди іншій державі, а за наявності відомостей про загрозу – вживати належних і можливих заходів для її запобігання. У площині відповідальності держав ця логіка співвідноситься з рамкою ARSIWA: стандарт належної обачності впливає на оцінку наявності обов'язку діяти та протиправності бездіяльності (ст. 2 – елементи міжнародно-протиправного діяння; загальні положення про атрибуцію та наслідки) [21].

У кіберконтексті *due diligence* означає, що держава повинна докладати належних зусиль, аби її територія, інфраструктура або підконтрольні суб'єкти не використовувалися для вчинення шкідливих кібероперацій проти інших. Цей підхід відображено в процесах ООН: GGE (2015) визнав застосовність принципів Статуту ООН і підтримав норми відповідальної поведінки, пов'язані з недопущенням зловмисної діяльності з території держави [19]; OEWG (2021) зафіксував орієнтир на превенцію,

співпрацю та взаємодопомогу у реагуванні на інциденти, включно з обміном інформацією та зміцненням потенціалів [20]. Хоч ідеться про *soft law*, їхня конвергенція зі сталою практикою держав поступово посилює звичаєвий характер відповідного стандарту.

Показовою є позиція Нідерландів (2019): держава зобов'язана вживати належних заходів для запобігання, припинення та розслідування шкідливої кібердіяльності, що походить з її території або від суб'єктів під її юрисдикцією, навіть якщо така діяльність не досягає порогу застосування сили [14]. Італія (2021) дотримується спорідненого підходу, розглядаючи *due diligence* не лише як самообмеження суверенітету, а й як позитивний обов'язок міжнародної співпраці з метою підтримання кіберстабільності (координація компетентних органів, своєчасний обмін даними, спільна протидія загрозам) [19].

Отже, *due diligence* у кіберпросторі – це позитивний стандарт поведінки: держава повинна діяти завчасно і розумно, виходячи з наявної інформації та своїх реальних можливостей, аби запобігати використанню її території/інфраструктури для шкідливих кібероперацій, співпрацювати у локалізації інцидентів і відновлювати безпеку. Такий підхід органічно поєднує суверенітет із взаємною відповідальністю держав у цифровому середовищі [19; 20; 14; 21].

Висновки. Підсумовуючи проведене дослідження, слід наголосити, що принципи суверенітету, невтручання та належної обачності становлять засадничу основу міжнародно-правового регулювання кіберпростору. Їхній зміст відображає еволюцію класичних норм міжнародного публічного права у новому технологічному вимірі, де право покликане не лише фіксувати кордони державної влади, а й визначати межі відповідальної поведінки держав у глобальному цифровому середовищі.

Сучасний розвиток міжнародного кіберправа переконливо засвідчує, що принципи Статуту ООН повною мірою поширюються на сферу інформаційно-комунікаційних технологій. Цю позицію підтверджують як рішення ООНівських структур (GGE, OEWG), так і національні доктрини провідних держав, що конкретизують правові наслідки порушення суверенітету, втручання та невиконання обов'язку належної обачності. Від декларативних формул міжнародне співтовариство переходить до практичного застосування принципів міжнародного права, що є свідченням поступової інституціоналізації кіберпростору як сфери відповідальності держав.

Особливої ваги у цьому процесі набуває принцип належної обачності (*due diligence*), який втілює позитивний обов'язок держави діяти активно – запобігати, припиняти та розслідувати шкідливу кібердіяльність, що походить із її території або здійснюється суб'єктами під її юрисдикцією. Його зміст свідчить про переосмислення традиційного суверенітету у бік функціонального підходу, де державна влада невіддільна від міжнародної відповідальності.

Узагальнюючи, можна стверджувати, що міжнародне право формує нову якість правового режиму кіберпростору – таку, де суверенітет виступає не лише символом незалежності, а й індикатором відповідального управління, невтручання тлумачиться через призму недопустимості примусу, а належна обачність – як прояв солідарності та співпраці. Подальший розвиток цього напряму потребує кодифікаційного закріплення зазначених принципів у межах універсального міжнародного договору, який визначатиме стандарти відповідальної поведінки держав і механізми взаємодії у сфері кібербезпеки.

Список використаної літератури:

1. Камчатний М. В. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві. *Актуальні проблеми сучасного міжнародного права* : зб. наук. ст. 2015. Ч. 1. С. 320–323.
2. Павленко В. С. Сутність кібербезпеки у теорії інформаційного права *Право та державне управління*. 2021. № 2(47). С. 43–49.
3. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. 2021. № 2(59). С. 110–115.
4. Balarabe K. Digital Borders and Beyond: Establishing Normative Grounds for Cybersecurity and Sovereignty in International Law. *Computer Law & Security Review.* 2025. Vol. 55. Art. 106180. URL: https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537
5. Broeders D., Cristiano F. Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road. Milano : ISPI, 2020. 20 p.
6. Buchan R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions. *Journal of Conflict & Security Law*. 2012. Vol. 17, No. 2. P. 211–227.
7. DeNardis L. Protocol Politics: The Globalization of Internet Governance. Cambridge, MA : MIT Press, 2009. 272 p. URL: https://direct.mit.edu/books/monograph/3160/Protocol-PoliticsThe-Globalization-of-Internet

8. Finnemore M.; Hollis D. B. Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law*. 2020. Vol. 31, No. 3. P. 969–1003. URL: https://doi.org/10.1093/ejil/chaa052.
9. Hathaway O. A., Crootof R., Levitz P., Proctor H., Nowlan A. E., Perdue W., Spiegel J. The Law of Cyber-Attack. California Law Review. 2012. Vol. 100, No. 4. P. 817–885.
10. Hurwitz R. The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests*. 2014. Vol. 36, No. 5. P. 322–331. https://doi.org/10.1080/10803920.2014.972048.
11. Koh H. H. International Law in Cyberspace. *Harvard International Law Journal (Online Symposium).* 2012. Vol. 54. P. 1–12. URL: https://harvardilj.org/2012/12/online-54-koh/
12. Mačák K. From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers. *Leiden Journal of International Law*. 2017. Vol. 30, No. 4. P. 877–899. URL: https://doi.org/10.1017/S0922156517000417.
13. Nye J. S. Jr. The Regime Complex for Managing Global Cyber Activities. Waterloo, ON : CIGI; London : Chatham House, 2014. 28 p. URL: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/
14. Roguski P. Application of International Law to Cyber Operations: A Comparative Analysis of States' Views. The Hague : The Hague Program for Cyber Norms, 2020. 28 p. URL: https://www.thehagueprogram.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views
15. Roscini M. Cyber Operations and the Use of Force in International Law. Oxford : Oxford University Press, 2014. 328 p.
16. Schmitt M. N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. 598 p.
17. Tsagourias N. The Legal Status of Cyberspace: Sovereignty Redux? *Research Handbook on International Law and Cyberspace* 2nd ed. Cheltenham : Edward Elgar Publishing, 2021. P. 1–25. URL: https://doi.org/10.4337/9781789904253.00010
18. Tsagourias N.; Farrell M. Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*. 2020. Vol. 31, No. 3. P. 941–970. URL: https://doi.org/10.1093/ejil/chaa057.
19. United Nations Group of Governmental Experts. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York : United Nations, A/70/174. 2015. 17 p.
20. United Nations Open-ended Working Group (OEWG) on Security of and in the Use of ICTs (2019–2021). Final report. New York : United Nations, 18.03.2021. A/75/816. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/067/22/PDF/N2106722.pdf
21. United Nations. Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). New York : United Nations, 2001. 86 p. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.
22. United Nations. Open-ended Working Group on Security of and in the Use of ICTs 2021–2025: Annual progress report 2024. New York : United Nations, 22.07.2024. A/79/214. – URL: https://documents.un.org

Soroka L. V., Kolesnyk O. O. International legal principles of cyberspace regulation: sovereignty, non-intervention and due diligence

The article presents a comprehensive theoretical and legal analysis of the core principles of international law that regulate state conduct in cyberspace – sovereignty, non-intervention, and due diligence. The study emphasizes the growing relevance of these principles in the context of rapid digitalization, the increasing role of cyber operations in international relations, and the need to adapt traditional legal frameworks to the challenges of the information age. The research objective is to clarify the contemporary understanding of these principles, identify their doctrinal and practical interpretation, and determine their role in shaping the international legal regime of cybersecurity and cyber defense. The article demonstrates that sovereignty in cyberspace has acquired a functional dimension that combines the right of states to control digital infrastructure with their responsibility to ensure its integrity and security. It argues that the principle of non-intervention applies to cyber operations through the criterion of coercion – only actions that compel another state to alter its sovereign decisions may be considered unlawful interventions. The analysis further reveals that the principle of due diligence is evolving into a positive obligation of states to prevent their territory or infrastructure from being used for harmful cyber activities and to cooperate in mitigating and investigating such incidents. Drawing upon UN documents (GGE 2015, 2021; OEWG 2021), national positions (France, the Netherlands, Italy, the United Kingdom), and leading academic works (Tallinn Manual 2.0; Schmitt, Roscini, Tsagourias, Buchan, Roguski), the study concludes that international law fully applies to cyberspace and that its implementation is gradually moving from declarative

recognition to operational practice. It highlights the growing convergence of hard law norms, customary principles, and soft law mechanisms, which collectively form a coherent framework for responsible state behavior in the digital environment. It is substantiated that the development of a universal international treaty on responsible state conduct in cyberspace would enhance normative clarity, strengthen international cooperation, and ensure predictability of the global legal order in the digital era. The article concludes that the integration of classical international legal principles with new regulatory standards reflects the transformation of international law into a dynamic system capable of maintaining stability, accountability, and trust in cyberspace as a new domain of international security. It is concluded that international law is forming a new quality of the legal regime of cyberspace – one where sovereignty is not only a symbol of independence, but also an indicator of responsible governance, non-interference is interpreted through the prism of the inadmissibility of coercion, and due diligence is interpreted as a manifestation of solidarity and cooperation. Further development of this direction requires codification of these principles within the framework of a universal international treaty, which will determine the standards of responsible behavior of states and mechanisms of interaction in the field of cybersecurity.

Key words: *national security, international law, cyberspace, sovereignty, non-intervention, due diligence, state responsibility, cyber governance, cyber defense, digital sovereignty.*