Ефективність державного управління
Efficiency of public administration
ISSN 2070-4011 (print)
ISSN 2786-6580 (online)
https://doi.org/10.36930/508210
Article received 22.01.2025
Article accepted 26.06.2025
УДК 351.862.4:004.046.5+341.1/.8](4+100)
Correspondence author: V. O. Tkach Tkach.Vsevolod@nltu.lviv.ua

В. О. Ткач
Національний лісотехнічний університет України, м. Львів, Україна

МІЖНАРОДНЕ ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ГЛОБАЛЬНИЙ ТА ЄВРОПЕЙСЬКИЙ КОНТЕКСТ

У «цифрових реаліях» сьогодення кібербезпека стала ключовою сферою через зростання кіберзагроз та кількості кібератак, які становлять серйозну небезпеку для людей, бізнесу та цілих країн. Для подолання цих труднощів динамічного характеру було розроблено широкий спектр національних і міжнародних правил та норм у галузі кібербезпеки. У представленій дослідницькій роботі проведено ретельний аналіз цих правил та норм на основі конструктивістської парадигми дослідження та інструментарію контент-аналізу. Також розглянуто низку факторів, що ускладнюють законотворчість у галузі кібербезпеки та її регулювання на міжнародному рівні. Також проаналізовано перешкоди, що є спільними на законодавчому рівні ЄС та України. Показано, що впродовж перших двох десятиліть поточного тисячоліття кібербезпека стала повсюдним аспектом і дискурсом у міжнародних відносинах. Водночас з'ясовано, що, маючи ознаки зокрема й політичної проблеми, досі паттерни кібербезпеки та вектори її розвитку, навіть відповідно до нових загроз та ситуацій, що виникають, не призвели до формування чіткого ландшафту міжнародного регулювання. Виявлено просту причину, яка частково пояснює цю інерцію – вона полягає в тому, що обсяг, характер, значення та термінологія кібербезпеки є нечіткими. Окрім того, механізм забезпечення відповідальності не розроблений чітко та не збалансований. Ця стаття має на меті зробити внесок у тривалу наукову дискусію щодо визнання нового права кібербезпеки. Доведено, що хоча на національному рівні існує необхідність гнучкої та проактивної реакції від законодавців та регуляторних органів, нову парадигму глобального законодавчого простору кібербезпеки потрібно розглядати як нову багатосторонність, зокрема у площині колективного виміру притягнення держави до відповідальності за кіберзлочини.

Ключові слова: кібербезпека; кіберзагрози; узгодження правових стандартів; правова еволюція; концепт.

Вступ

Значення сфери кібербезпеки у контексті безпеки як окремих осіб, так і країн стало очевидним із розвитком технологій, що призвело до комп'ютеризації в усіх її формах та широкого доступу до Інтернету. Цей прямий доступ до інформації, що став можливим завдяки швидкому розвитку комп'ютерних систем, зараз є одним з основних факторів соціального та економічного зростання та часто визначає успіх чи невдачу будь-якої справи. Доступ до мережевих послуг вплинув на соціальні відносини та може бути інструментом для заохочення або контролю певних моделей поведінки, таких як політичні рішення. Дії, що здійснюють різні учасники у кіберпросторі, можуть безпосередньо призводити до певних економічних, соціальних чи політичних результатів. Це робить кіберпростір сферою, яка впливає на безпеку державного та приватного секторів, а також громадян і, як наслідок, країн загалом, як зазначає польський дослідник F.Radoniewicz [1].

У сучасну цифрову епоху технології радикально змінили те, як ми взаємодіємо, працюємо та живемо. Однак ця зміна не позбавлена своїх викликів, особливо коли йдеться про кібербезпеку та захист даних. Зростання кіберзлочинності зумовило нагальну потребу в міжнародних законах і нормативних актах, які ефективно б вирішували ці проблеми, створюючи узгоджену правову базу для подолання ризиків і захисту прав у кіберпросторі.

Транскордонний характер Інтернету створює фундаментальний виклик для традиційних правоохоронних органів та юрисдикції. Кіберзлочинці можуть діяти з будь-якої точки світу, користуючись відсутністю координації між юрисдикціями, щоб скоювати злочини, не боячись бути притягнутими до відповідальності. Ця реальність доводить нагальну потребу в посиленні міжнародної співпраці в галузі кібербезпеки.

У відповідь на таке зростання загрози різні міжнародні та регіональні органи працюють над встановленням спільних стандартів і принципів у сфері кібербезпеки та захисту даних. Однією з найважливіших віх у цьому розумінні є Конвенція Ради Європи про кіберзлочинність, також відома як Будапештська конвенція. Цей договір, ухвалений у 2001 р. та чинний з 2004 р., спрямований на гармонізацію національного законодавства та зміцнення міжнародної співпраці у боротьбі з кіберзлочинністю.

Окрім цього, Європейський Союз відіграв провідну роль у просуванні вищих стандартів захисту даних че-

Інформація про авторів:
Ткач Всеволод Олегович, здобувач програми доктора філософії кафедри публічного управління та адміністрування.
Email: Tkach.Vsevolod@nltu.lviv.ua; https://orcid.org/0009-0001-6582-0064
Цитування за ДСТУ: Ткач В. О. Міжнародне правове регулювання забезпечення кібербезпеки: глобальний та європейський контекст. *Ефективність державного управління* : зб. наук. пр. Вип. 1/2(82/83). Львів: НЛТУ України, 2025. С. 77–84.
Citation APA: Tkach, V. O. (2025). International legal regulation of cybersecurity: global and european context. *Efficiency of public administration, 1/2*(82/83), 77–84. https://doi.org/10.36930/508210

рез Загальний регламент про захист даних (GDPR). Ця нормативна база, що застосовується до всіх компаній, що обробляють персональні дані громадян ЄС, встановлює чіткі правила щодо згоди користувачів, безпеки даних та покарання за недотримання, незалежно від географічного розташування суб'єкта, що обробляє дані.

На світовому рівні Організація Об'єднаних Націй також визнала важливість вирішення проблем кібербезпеки та захисту даних. Так, резолюція Генеральної Асамблеї 70/237 визначає засадничі принципи, такі як повага до прав людини у кіберпросторі та міжнародне співробітництво для запобігання та пом'якшення наслідків кіберінцидентів. Однак, попри ці зусилля, залишаються значні прогалини у впровадженні та забезпеченні дотримання міжнародних стандартів кібербезпеки.

Масив головних системних перешкод ефективному здійсненню регулювання кіберпростору охоплює, зокрема, розбіжність інтересів між державами, а також відмінності в їхніх правових базах та технічних можливостях. Цей конфлікт інтересів ускладнює досягнення глобального консенсусу щодо правил та принципів, які повинні регулювати кіберпростір [2].

Окрім цього, стрімкий розвиток технологій (ШІ, Інтернет речей та ін.) створює додаткові виклики для розроблення відповідних законів та нормативних актів – критично необхідною стає гнучкість, достатня для того, щоб законодавчо-нормативна база могла адаптуватися до змін у цифровому ландшафті. Відповідно, потрібна гнучка та проактивна реакція від законодавців та регуляторних органів.

Специфіка змісту регулювання кібербезпеки в кожній країні також має велике значення. Уряд України прагнув побудувати найрозвиненішу в цифровому плані державу у Східній Європі. Ця мета завжди поєднувалася з посиленням можливостей та контролю в галузі кібербезпеки. Поряд з власними зусиллями, уряд активно залучає до зміцнення національних кіберсистем партнерів з державного та приватного секторів. Окрім цього, з 2020 р. через спеціальну програму USAID надавала підтримку в галузі кібербезпеки. Ця ініціатива допомогла Україні зміцнити свій кіберзахист та усунути слабкі місця. США збільшили свою гуманітарну допомогу Україні, яка охоплює кошти, спеціально виділені на кібербезпеку. Тим часом ЄС мобілізував команду експертів з кібербезпеки, які допомагають уряду України готуватися до потенційних кібератак.

Забезпечення кібербезпеки є необхідним компонентом національної безпеки в Україні. Виклики та кіберзагрози національному кіберпростору описано в розділі 3 Стратегії кібербезпеки України «Безпечний кіберпростір» та є запорукою успішного розвитку країни. До них, за статистичними даними [3], належать:

- широке застосування кіберзасобів у конкуренції у міжнародному масштабі;
- конкурентний характер розвитку інструментів кібербезпеки в ландшафті швидкого прогресивного розвитку цифрових технологій, зокрема хмарних та квантових обчислень, мереж 5G, великих даних, Інтернету речей (IoT), штучного інтелекту (ШІ) тощо;
- тенденції мілітаризації у кіберпросторі та розвиток кіберзброї, що дає можливості латентного здійснення кібератак для підтримки бойових дій та розвідувально-підривної діяльності у кіберпросторі;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії між громадянами та державою, які здійснюються безсистемно з точки зору заходів кібербезпеки та без належної оцінки ризиків.

Дослідження стосовно стану та перспектив ринку кібербезпеки в Україні аналізує фундаментальні тренди, сектори та інноваційні розробки в галузі на тлі повномасштабної кібервійни з боку Росії. Зокрема, автори дослідження наголошують, що повномасштабна війна призвела до суттєвого сплеску кібератак в Україні, водночас підвищивши попит на відповідні рішення та інноваційні технології. Ярослав Захаров [4] зазначає, що постійні кібератаки з боку російських хакерських угруповань (зокрема UAC-0010 та ін.) найчастіше здійснюються проти державних установ, ОПК, телекомунікаційної інфраструктури, установ фінансового сектору та енергетики. Захаров [4] наводить важливі статистичні дані: у 2023 р. було зафіксовано 2544 кіберінцидентів, тобто на 16% більше, ніж у 2022 році. Світовий ринок кібербезпеки, за прогнозами, досягне 186 млрд дол. США вже найближчим часом. Частка України наразі становить менше одного відсотка. Але Україна є трендсеттером ринку кібербезпеки, і перебуває попереду інших країн у кібер-експертизі завдяки роботі в R&D-сегменті, тобто саме в розробці інновацій. Так, хоча сьогодні на світовому ринку кібербезпеки домінантним є сегмент безпекових послуг з часткою 53% у 2024 р., на ринку України переважають кіберрішення з часткою 57% [4]. Лідерство України зумовлено, звісно, чинниками воєнного характеру – війна збільшила кількість та складність кібератак на Україну, що детермінувало швидке впровадження автоматизованих систем, в яких потрібне менше втручання з боку людини та пошук миттєвих і непередбачуваних рішень. При цьому основними драйверами ринку в Україні є цифровізація та збільшення ризику реальних втрат внаслідок кібератак. Також масив драйверів зростання ринку охоплює таке: (1) масштабне впровадження цифрових рішень у бізнесовому сегменті та державному секторі; (2) постійні російські атаки на критичну інфраструктуру, компанії та державні сервіси; (3) збільшення фінансових та репутаційних збитків від кібератак; (4) збільшення використання можливостей штучного інтелекту; (5) стимулювання ринку завдяки спеціальним таргетованим проєктам та програмам міжнародної технічної допомоги. Прогнозують зростання ринку кібербезпеки в Україні до 2029 р., зокрема в сегментах захисту мереж, хмарних сервісів та кінцевих точок. На рисунку показано прогнозну динаміку ринку.

Водночас, складається ситуація, коли практичний ландшафт зусиль з кібезбезпеки набагато випереджає еволюцію правового регулювання цієї сфери. Окрім цього, високий рівень технологічної залежності України від іноземних виробників продукції цифрових технологій та відсутність системи оцінювання ступеня відповідності такої продукції нормам безпеки підвищує ступінь вразливості інформаційної інфраструктури від незадекларованих функцій та звужує можливості протидії кіберзагрозам. Окрім того, існує недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільне впровадження положень європейського законодавства, недостатнє регулювання цифрової складової розслідування кримінальних правопорушень, а також низький

рівень юридичної відповідальності за порушення вимог законодавства у цій сфері. Також викликом є відсутність відповідних структурних підрозділів, необхідного штатного розпису та належного контролю за кіберзахистом у значній частині державних органів, а також недостатнє фінансування робіт з кіберзахисту за залишковим принципом. З початком повномасштабної війни у 2024 р. питання кібербезпеки стало одним із найважливіших компонентів національної системи безпеки. З огляду на це, розгляд ландшафту кібербезпеки як на рівні національної держави, так і на глобальному/регіональному рівнях є надзвичайно актуальним завданням.

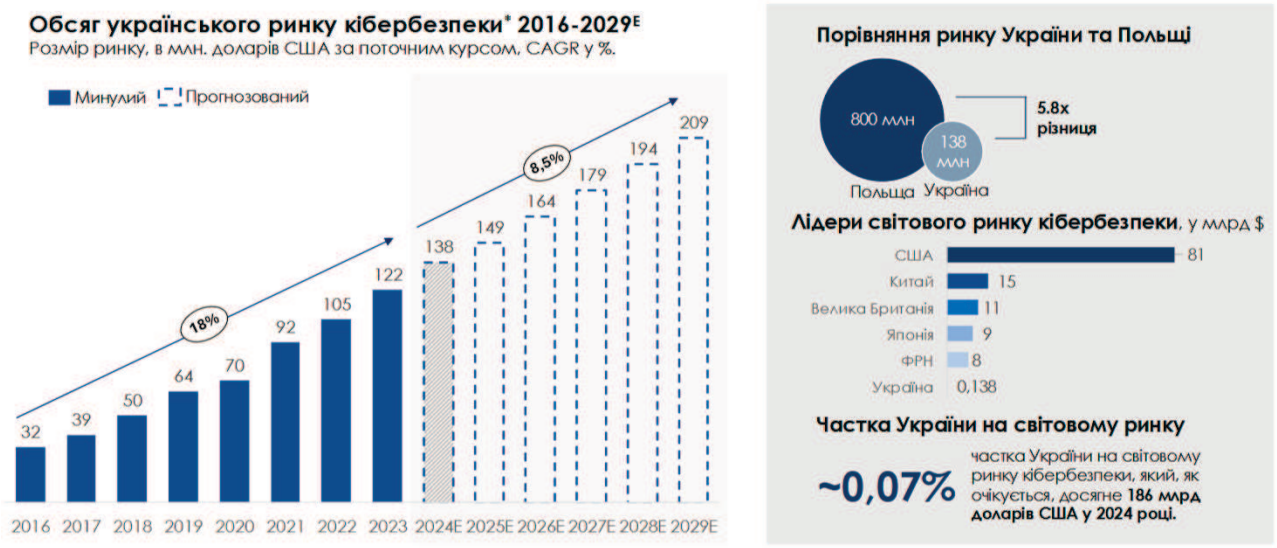

Рисунок. Прогнозна динаміка ринку кібербезпеки в Україні [5]

Методи дослідження

Було ініційовано багато політичних ініціатив щодо різних (під)сфер кібербезпеки, зокрема в контексті ООН та ЄС. Обидві організації прагнуть відіграти провідну роль у підвищенні стійкості кібербезпеки. Оскільки обидві організації мають доволі унікальні, різні законотворчі процеси, і перша є унікальною глобальною організацією, тоді як друга є унікальним типом регіональної організації, у цій статті, зокрема, буде порівняно нормативні ініціативи щодо кібербезпеки *sensu stricto*, які здійснили ці дві організації. Загальна мета полягає в тому, щоб обговорити, як і якою мірою заповнюються прогалини у глобальному управлінні кібербезпекою, шляхом аналізу найважливіших останніх подій у законодавстві кібербезпеки в ООН та ЄС. По-перше, на більш абстрактному рівні ми обговоримо, чи може міжнародне право адекватно регулювати питання кібербезпеки: які перешкоди виникають у регулюванні в кіберсфері.

Дослідження виконано в рамках конструктивістської наукової парадигми. Інструментарій містить контент-аналіз, компаративний аналіз, класифікацію та узагальнення. Формування вибірки даних проведено на основі пошуку в бібліометричних базах даних Google Scholar, JSTOR, ScienceDirect та Wiley.

Аналіз літературних джерел

Оскільки держави приділяють дедалі більше уваги управлінню кіберпростором (технічна архітектура, яка дає змогу функціонувати глобальному Інтернету) та управлінню в кіберпросторі (як держави, промисловість та користувачі можуть використовувати цю технологію), роль міжнародного права в кіберконтексті набуває дедалі більшої ваги. Ми погоджуємось з думкою N. Mishra [6], який стверджує, що складне узгодження між кібербезпекою та міжнародною правотворчістю можна пояснити низкою факторів: швидкою та високотехнологічною кіберреволюцією; суверенітетом, територіальністю, фрагментацією юрисдикції та правового припису-вання; роллю уряду проти приватного сектору. З огляду на ці численні виклики, потрібно наголосити, що досі не існує глобальної конвенції в галузі кібербезпеки *sensu stricto*.

Подальші обговорення, зокрема представлені в публікації Coates та ін. [7], зосередилися на розвитку застосування принципу невтручання в кіберпросторі. Цей дискурс, на нашу думку, справді є дуже важливим. Західні країни, зокрема, стали активними прихильниками поширення цього принципу на цифрову сферу, маючи законні побоювання, що спонукають до цього зрушення. Цю зміну розглядають як можливість як для західних, так і для незахідних країн взяти участь у реалістичних дискусіях щодо своїх проблем та потенційних сфер досягнення згоди. Це може сприяти підвищенню ефективності принципу, який, як справедливо зазначає N. Mishra, історично був одним з найбільш порушуваних [6]. Останнім часом, значну увагу в дискусіях щодо невтручання в кіберпростір зосереджено на питанні примусу, що розглядає, зокрема, F.Delarue [8]. Деякі держави намагаються розширити принцип невтручання та його тлумачення. Однак висловлюється занепокоєння, що таке розширення може призвести до надмірного тлумачення цього принципу та охопити дії, які можуть насправді не порушувати його. Зміщення фокусу зі свободи вирішувати на свободу контролю може призвести до надмірно розширювального тлумачення. Це зміщення може замінити принцип суверенітету принципом невтручання, що викликає занепокоєння щодо стабільності кіберпростору. Експерти наголошують на необхідності активнішої ролі незахідних країн у тлумаченні та застосуванні принципу невтручання у кіберпростір [9]. Заохочення їхньої активної участі у формуванні тлумачення та застосування цього принципу, враховуючи такі країни, як Китай, вважається вирішальним [10]. На нашу думку, інклюзія незахідного бачення

та регіональних інтересів відповідних держав є дійсно важливим моментом.

В європейській практиці посилання на відповідальність держави, чітко виражені в державній практиці, розуміння її форм та очікуваних наслідків недостатньо добре задокументовані. Розуміння посилання на відповідальність держави передбачає вивчення засобів правового захисту, заходів, які має вжити держава, що вчинила порушення, очікуваних гарантій неповторення та виду запитуваного відшкодування [11]. Однак, хоча практика порушення питання про відповідальність держави обмежена, публічне приписування є поширеним явищем. Учені, зокрема E. Fahey [12], також зазначили, що визначення того, коли кібероперація є міжнародно визнаним протиправним діянням, можливе лише з посиланням на первинні правила, з чим ми погоджуємось. Вторинні правила застосовують під час визначення ступеня незаконності та характеру кібероперацій, особливо коли йдеться про кілька операцій. Визначення характеру операції, формулювання позову та визначення обсягу позову є критично важливими аспектами.

Результати дослідження

Окрім деяких винятків (найпомітнішими серед них є Будапештська конвенція про кіберзлочинність та Конвенція Африканського Союзу про кібербезпеку та захист персональних даних), міжнародне право не має спеціалізованих правил регуляторної діяльності у кіберпросторі. Понад це, ця технологія є водночас новою та динамічною. Отже, впродовж кількох років залишалися відкритими питання про те, чи взагалі застосовується чинне міжнародне право до кіберпростору. Сьогодні більшість держав та кілька міжнародних організацій, враховуючи Перший комітет Генеральної Асамблеї ООН з роззброєння та міжнародної безпеки, G20, Європейський Союз, АСЕАН та ОАД, підтвердили, що чинне міжнародне право застосовується до використання ІКТ-державами. Отже, нинішній дискурс зосереджений не на тому, чи є міжнародне право застосовним, а на тому, як відбувається це застосування [13]. Ця думка D. Hollis є слушною.

На відміну від багатьох інших міжнародних питань, управління кіберпростором виникло не в державах, а в академічних установах та приватних суб'єктах, які й створили Інтернет (хоча й за державного фінансування). З комерціалізацією Інтернету з'явилися ІКТ-компанії; сьогодні їхні платформи слугують середовищем для переважної більшості кіберповедінки, включаючи державні та спонсоровані державою кібероперації. За цим слідував інтерес держав до кіберпростору, зокрема як зони геополітичного суперництва. Отже, управління кіберпростором включає ключових зацікавлених сторін, до яких належать, але аж ніяк не обмежуються, держави.

Однак міжнародне право – це, передусім, правовий порядок для держав (та утворюваних ними інституцій, таких як міжнародні організації). Отже, міжнародне право не має монополії на регулювання кіберпростору. З огляду на представників промисловості та громадянського суспільства, інші регуляторні режими (наприклад, саморегулювання галузі) пропонують альтернативні засоби. Наприклад, багатостороннє управління стало основним шляхом управління архітектурою Інтернету. Водночас недержавні суб'єкти висловили зацікавленість у питаннях того, як міжнародне право застосовується до управління в кіберпросторі. Наприклад, Міжнародний комітет Червоного Хреста та Незалежні групи експертів, які є авторами двох Талліннських посібників (з планами розробки третього), дослідили, як чинні норми та принципи міжнародного права враховуються в кіберконтексті. Президент компанії Microsoft навіть закликав держави укласти нову «Цифрову Женевську конвенцію» для регулювання поведінки держав у кіберпросторі.

Група урядових експертів ООН (ГУЕ) з питань кібербезпеки, з моменту свого створення у 2004 р., відіграла ключову роль у встановленні міжнародних норм відповідальної поведінки держав у кіберпросторі. Скликана Генеральною Асамблеєю ООН на тлі зростаючої стурбованості щодо неправомірного використання інформаційно-комунікаційних технологій (ІКТ) та потенційних кіберконфліктів, ГУЕ досліджує загрози міжнародній безпеці та рекомендує керівні норми. Ключовою віхою стала третя доповідь 2013 р., в якій було визнано, що чинне міжнародне право, включаючи Статут ООН, застосовується до поведінки держав у кіберпросторі, підтверджуючи, що такі принципи, як суверенітет, невтручання та заборона застосування сили, є актуальними в цій сфері [14].

Звіти ГУЕ ООН щодо врегулювання конфлікту за 2013 та 2015 рр. є найважливішими та найвпливовішими. У своїй консенсусній доповіді від 24 червня 2013 р. ГУЕ ООН встановила, що міжнародне право, і зокрема Статут ООН, застосовується в кіберпросторі так само, як й у фізичному просторі. Це включає правила щодо державного суверенітету та принципи, що випливають з поняття суверенітету. Наприклад, держава має юрисдикцію над інфраструктурою ІКТ на своїй території, і держава несе відповідальність за міжнародні незаконні кібератаки, які можуть бути їй приписані. У своїй консенсусній доповіді за 2015 р. ГУЕ ООН висунула такі принципи Статуту ООН та міжнародного права, що застосовуються в кіберпросторі до поведінки держав: суверенітет, суверенна рівність, мирне врегулювання конфліктів, заборона застосування або погрози насильством проти територіальної цілісності або політичної незалежності держави, повага до прав людини та основоположних свобод, а також принцип невтручання у внутрішні справи інших держав. Таке перенесення у кіберпростір основних принципів міжнародного права, які майже всі становлять обов'язкове звичаєве міжнародне право та/або були підтверджені Міжнародним Судом ООН, є предметом досить широкого консенсусу. Кілька держав, включаючи деякі «кібернаддержави», відтоді підтвердили застосовність міжнародного права в кіберпросторі у своїх коментарях до звітів ГУЕ ООН та у своїх національних стратегіях кібербезпеки. На той момент звіти ГУЕ ООН за 2013 та 2015 рр. можна було розглядати як свідчення зростаючого консенсусу з цього питання та як свідчення розвитку певного *opinio juris*, що є одним із елементів, необхідних для остаточного формування звичаєвого міжнародного права.

У багатьох документах ЄС голосно заявляв про своє бажання відігравати провідну роль у кібербезпеці [15]. Директива NIS є першим в історії ЄС горизонтальним та юридично обов'язковим інструментом з кібербезпеки *sensu stricto*. Вона спрямована на захист критичної інфраструктури (постачальників основних послуг та постачальників цифрових послуг) від кіберінцидентів, які

мають «значний руйнівний вплив». Головною метою Директиви NIS є гарантування високого загального рівня безпеки мереж та ІТ. Однією з головних причин її ухвалення було те, що деякі держави-члени ЄС не мали законодавства про кібербезпеку, і навіть коли воно було, між державами-членами існували значні розбіжності. Директива NIS накладає на держави-члени різні зобов'язання, включаючи забезпечення мінімального національного потенціалу шляхом призначення компетентних органів NIS, створення кризових команд та через національні стратегії та плани співпраці щодо NIS. По-друге, варто вказати на Закон ЄС про кібербезпеку, викладений у Регламенті (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 р. про ENISA (Агентство ЄС з кібербезпеки) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій.

Однак Група експертів ООН з питань кібербезпеки зіткнулася з труднощами, переходячи від питання «чи» до питання «як» [16]. На цей момент ООН стикається з реальною загрозою того, що поділ на два процеси – з нинішньою ГУЕ та Робочою групою відкритих ресурсів (OEWG) – зробить загальну згоду менш імовірною та ще більше віддалиться від міжнародної *opinio juris*. Регулювання кібербезпеки загальмувалося радше через політику, ніж через право на рівні ООН, тоді як поточний геополітичний імпульс у ЄС щодо регулювання є високим. У будь-якому разі, пропаганда виключно регулювання кібербезпеки *sensu stricto* на рівні ООН або ЄС є хибною дихотомією. Швидше, доцільно шукати синергії та співпраці.

Український дослідник В. Ткач [17], розглядаючи глобальне управління у сфері безпеки в контексті сучасних викликів України, також відзначає кібербезпеку як основний фактор національної та міжнародної безпеки XIX століття. Дослідник аргументує, що великий масив ініціатив у сфері правового забезпечення кібербезпеки охоплює тільки невелику частину міжнародної правової системи, зокрема, стосовно захисту критичної інфраструктури, захисту приватних даних у мережі, ведення війни із застосуванням кібертехнологій. Він слушно зазначає, що «кібербезпека не може бути спрямована на захист від максимальної кількості загроз, тим більше що їхня кількість стрімко зростає і вони постійно модифікуються. Потрібно забезпечити наявність середовища, максимально сприятливого для роботи користувачів та всіх систем у кіберпросторі» [17, с. 87]. З цим важко не погодитись. Такі висновки зумовлюють необхідність, зокрема, розгляду питання правового регулювання забезпечення кібербезпеки України в розрізі геополітичних аспектів та інтересів країни, що підтверджує і дослідження Carrapico та Farrand [18].

Серед пріоритетів у сфері забезпечення кібербезпеки України потрібно зазначити такі: забезпечення кіберпростору для захисту державного суверенітету та розвитку суспільства; захист прав, свобод та законних інтересів громадян України в кіберпросторі; європейська та євроатлантична інтеграція у площині кібербезпеки. Утворення нової якості національної системи кібербезпеки вимагає чіткого та зрозумілого визначення стратегічних цілей, досягнення яких має відбутись упродовж періоду реалізації цієї стратегії. Для формування потенціалу стримування (С) необхідно досягти таких цілей стратегічного характеру:

Ціль С.1. Ефективний кіберзахист – Україна створює та забезпечує розвиток (включаючи кадровий та технічний) підрозділів, що мають повноваження вести збройний конфлікт у кіберпросторі, формує відповідну правову, організаційну та технологічну модель їх функціонування та застосування; забезпечує ефективну взаємодію між ключовими суб'єктами національної системи кібербезпеки та сил оборони під час заходів кіберзахисту, належну підготовку та фінансове забезпечення таких структур; систематичну кіберпідготовку; оцінювання можливостей та ефективності підрозділів; розробку відповідних показників ефективності.

Ціль С.2. Забезпечення потрібного рівня протидії розвідувальній та підривній діяльності у кіберпросторі та кібертероризму – безперервне впровадження контррозвідувальних заходів для виявлення, запобігання та припинення розвідувальної та підривної діяльності іноземних держав, кібершпигунства та кібертероризму, усунення умов, що сприяють їм, та причин їх виникнення.

Ціль С.3. Ефективна протидія кіберзлочинності – Україна забезпечує правоохоронним органам та спеціальним державним органам з правоохоронними функціями можливості мінімізувати загрози кіберзлочинності, зміцнює їхні технологічні та людські ресурси для здійснення превентивних заходів та розслідування кіберзлочинів.

Ціль С.4. Вироблення асиметричних інструментів стримування – Україна створює умови, необхідні у площині стримування агресивних дій у кіберпросторі проти неї шляхом використання економічних, розвідувальних та дипломатичних заходів, а також використання потенціалу акторів приватного сектору.

Правову основу забезпечення кібербезпеки в Україні закладено в Конституції України, законах України про основи національної безпеки, принципах внутрішньої та зовнішньої політики, електронних комунікаціях, а також про захист державних інформаційних ресурсів та інформації, вимога щодо захисту яких встановлена законом. Цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти КМУ, а також інші нормативно-правові акти, затверджені на виконання законів України. Базовими законами у цій галузі є Закон України «Про інформацію», Закон України «Про державну таємницю» та Закон України «Про основні засади забезпечення кібербезпеки України». Цей Закон визначає як правові, так і організаційні основи забезпечення захисту життєво важливих інтересів особи та громадянина, суспільства та держави, національних інтересів України у кіберпросторі, а також основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, фізичних осіб та громадян у цій сфері та основні принципи координації їхньої діяльності щодо забезпечення кібербезпеки. Цей Закон визначає об'єкти кібербезпеки та кіберзахисту, суб'єктів кібербезпеки, описує принципи, які покладено в основу кібербезпеки об'єктів критичної інфраструктури, принципи кібербезпеки, національну систему кібербезпеки та завдання урядової команди з реагування на комп'ютерні надзвичайні події України CERT-UA. Також закладено основи державно-приватного співробітництва у сфері кібербезпеки та надання допомоги суб'єктам, що забез-

печують кібербезпеку в Україні. Закон передбачає відповідальність за порушення законодавства у сфері кібербезпеки, враховує питання фінансового забезпечення заходів кібербезпеки, міжнародного співробітництва у сфері кібербезпеки та контролю за законністю заходів щодо забезпечення кібербезпеки в Україні.

Обговорення отриманих результатів

Питання щодо застосування міжнародного права до кіберпростору, можна поділити на п'ять окремих категорій: (1) «мовчання»; (2) екзистенційні розбіжності; (3) проблеми тлумачення; (4) атрибуція та (5) підзвітність.

Щодо «мовчання», варто зазначити, що без спеціально розроблених договорів з кіберпитань застосування міжнародного права залежить від визначення норм звичаєвого міжнародного права, тобто державної практики, визнаної як закон. Упродовж багатьох років визначення того, що держави робили в кіберпросторі, не кажучи вже про те, що, на їхню думку, має сказати про це міжнародне право, ускладнювалося так званим «мовчанням» держав. Однак упродовж останнього десятиліття кілька держав почали висловлюватися. Починаючи з 2012 р., Сполучені Штати почали висловлювати свою точку зору в серії промов та заяв. У 2018 р. Генеральний прокурор Сполученого Королівства зробив важливу заяву про погляди Сполученого Королівства стосовно цих питань. Наступними роками інші (переважно європейські) держави почали пропонувати свої власні детальні перспективи, включаючи Австралію, Естонію, Фінляндію, Францію, Німеччину та Нідерланди. Поточні зусилля в ООН та в регіональних контекстах, таких як ОАД, зараз спрямовані на розширення переліку держав, які мають думки щодо міжнародного права у кіберпросторі. Однак наразі переважна більшість держав зберігають мовчання [19].

Серед тих держав, які зайняли позиції щодо застосування міжнародного права до кіберпростору, існує низка «екзистенційних» розбіжностей – конкурентних тверджень про те, що певна міжнародно-правова норма чи режим повністю включені або виключені з кіберпростору. Наприклад, у контексті ООН кілька держав оскаржили доступність міжнародного гуманітарного права, право на самооборону, обов'язок належної обачності та право вживати контрзаходів щодо онлайн-активності. Існування (або відсутність) однієї або кількох із цих правових рамок у кіберпросторі має значні наслідки для застосування міжнародного права, впливаючи на те, як держави проводять свої кібероперації у збройних конфліктах, на їхню здатність реагувати на зловмисну кіберактивність, що здійснюється іншими державами, та на те, які дії вони повинні вжити для захисту прав третіх держав від шкоди, що виникає на їхніх власних територіях [20].

Щодо питань тлумачення, навіть коли держави визнають, що певна міжнародно-правова норма чи режим застосовується в кіберпросторі, суттєві питання тлумачення часто залишаються відкритими для обговорення. Міжнародно-правові режими, такі як невтручання, суверенітет та права людини, стикаються з великою неоднозначністю у своєму застосуванні до кіберпростору. Наприклад, обов'язок невтручання захищає міжнародні та зовнішні справи держави від «примусового» втручання з боку інших держав. Однак немає консенсусу щодо того, які «справи» захищає цей обов'язок, не кажучи вже про те, що відрізняє примусову від непримусової кібердіяльності. Так само суверенітет, безсумнівно, є однією з основних архітектурних особливостей міжнародного правового порядку. Однак держави, вочевидь, розходяться в думках щодо того, чи є суверенітет лише основоположним принципом, на якому ґрунтуються інші міжнародно-правові норми (такі як невтручання), чи це незалежне правило, яке може бути безпосередньо порушене певними кібероперaціями іноземних держав [21].

Міжнародне право забезпечує регулювання лише діяльності певних суб'єктів міжнародного права (наприклад, держави). Воно зазвичай не призначене для керування поведінкою ІКТ-компаній або окремих осіб (які зазвичай підпорядковуються одному або кільком внутрішнім правопорядкам). Тому для застосування міжнародного права в кіберпросторі необхідно знати особу відповідального за відповідну діяльність: чи це держава або суб'єкт, що спонсорується державою, на якого поширюється міжнародне право, чи це особа(и), яка(і) здійснює(ють) поведінку поза межами сфери дії міжнародного права [22]. Однак така ідентифікація є складною в кіберпросторі, враховуючи відомі проблеми технічної атрибуції – визначення джерел зловмисної кіберповедінки часто є складним і трудомістким. Понад це, коли держави використовують посередників, атрибуція ще більше ускладнюється необхідністю пред'явлення доказів державного «контролю» над посередником (міжнародне право ще не повністю вирішило, який рівень контролю потрібен або які докази необхідно пред'явити для його демонстрації).

Хоча кількість фіксованих державних та спонсорованих державою кібероперацій може зростати, практичне застосування механізмів відповідальності виявилось складним. Держави, які звинувачують інші держави у зловмисній кіберповедінці, рідко посилаються на міжнародне право. Відсутність міжнародно-правової риторики може означати, що така поведінка може бути законною, навіть якщо вона небажана. Також і викриття, що існувало, могло не вплинути на поведінку обвинуваченого (хоча таке викриття може допомогти прояснити існування та значення міжнародного права у кіберпросторі). Деякі держави працюють над створенням коаліцій, які можуть співпрацювати для покращення механізму відповідальності шляхом колективних звинувачень або навіть санкцій. Однак досі такі зусилля не зосереджувалися на використанні критеріїв міжнародного права для оцінки зловмисної кіберповедінки, а також інструментів (наприклад, контрзаходів) для боротьби з порушеннями кібербезпеки.

Надалі варто зазначити, що існують два домінантних питання щодо застосування міжнародного права до кіберпростору: (а) яку форму має мати будь-яке вирішення основних проблем та (б) на яких форумах це має відбуватися?

Притягнення держави до відповідальності охоплює [23]:

- формулювання претензій державою-мішенню, що вимагає надання суттєвої інформації з кібербезпеки для підтвердження цих претензій;
- визначення засобів правового захисту, таких як заходи, які має вжити держава-порушник, очікування гарантій неповторення та форми відшкодування;
- та повідомлення про претензію державі-порушнику.

Претензія стосовно відповідальності держави може бути реалізована дипломатичними або судовими засобами. Однак виникають проблеми щодо взаємовідносин між державними та недержавними суб'єктами, дипломатичного захисту, збитків приватних компаній та страхових претензій. Колективний вимір притягнення держави до відповідальності вимагає врахування сценаріїв багатоопераційної діяльності, потенційної участі кількох держав та відшкодування. Держави, які не є об'єктами кібератак, також можуть висувати претензії на підтримку інших держав, потенційно захищаючи колективні інтереси.

Навіть попри те, що у міжнародному праві немає спеціально спроєктованих правил, різні держави та зацікавлені сторони стверджують, що чинного міжнародного права достатньо для регулювання поведінки держав: для цих суб'єктів майбутнє має вирішити, як впровадити та покращити підзвітність згідно з чинним законодавством. Натомість інші держави та зацікавлені сторони припускають, що в чинному законодавстві існують прогалини або паттерни неефективності, що вимагає формулювання нових правил – через новий договір або еволюцію звичаєвого міжнародного права.

Тобто, навіть коли держави долають своє початково стримане ставлення щодо застосування міжнародного права стосовно поведінки різних суб'єктів у кіберпросторі, наслідки виникнення нових «голосів» у різних формах та на різних форумах заслуговують на посилену увагу. Держави та інші зацікавлені сторони повинні ретельно відстежувати різні питання та поведінку залучених гравців, з огляду на загальну картину, вбачаючи, чи може міжнародне право мати більше можливостей, ніж просто застосовування в кіберконтекстах. Справжнє питання залишається відкритим: чи може воно застосовуватись у такий спосіб, щоб ефективно регулювати поведінку держав та інших суб'єктів, що викликають міжнародне занепокоєння.

Висновки

У полі сформульованої мети зазначимо, що, зрештою, вирішення міжнародних проблем кібербезпеки та захисту даних вимагає багатогранного підходу, який поєднує співпрацю між державами, зміцнення технічних та правових можливостей, а також сприяння глобальній культурі кібербезпеки. Хоча прогрес у цьому напрямі є обнадійливим, ще багато роботи попереду для забезпечення безпечного кіберпростору для всіх. Постійна співпраця між урядами, бізнесом та громадянським суспільством матиме вирішальне значення для вирішення цього спільного виклику та захисту прав у цифровому світі.

Виконуючи поставлене завдання розгляду ландшафту кібербезпеки як на рівні національної держави, так і на глобальному/регіональному рівнях, зазначимо, що встановлення відповідальності держав у кіберпросторі розглядають як життєво важливий аспект майбутнього розвитку кіберсфери. Хоча деякі держави публічно поклали на себе відповідальність за певні кібероперації, вони ще не застосували міжнародне право для встановлення відповідальності ймовірних правопорушників. Наступний крок, ймовірно, включатиме притягнення винної держави до відповідальності перед міжнародним трибуналом або арбітражним розглядом. Окрім того, контрзаходи, ймовірно, відіграватимуть вирішальну роль, даючи державам змогу реагувати на порушення міжнародного права та обґрунтовувати свою відповідь. У цьому контексті виникають нові дебати щодо використання контрзаходів у кіберпросторі.

References

1. Radoniewicz, F. (2021). International regulations on cybersecurity. In: K. Chałubińska-Jentkiewicz, F. Radoniewicz, & T. Zieliński (eds.). Cybersecurity in Poland, 53–71. https://doi.org/10.1007/978-3-030-78551-2_5
2. Bradford, A. (2023). Digital Empires. Oxford: Oxford University Press.
3. Davydiuk, A., & Potii, O. (2024). National Cybersecurity Governance: Ukraine. NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf
4. IT Ukraine (2025) Український ринок кібербезпеки зріс у чотири рази за вісім років. URL: https://itukraine.org.ua/ukrayinskij-rinok-kiberbezpeki-zris-u-chotiri-razi-za-visim-rokiv/
5. Zakharov, Y. (2025). В Україні ринок кібербезпеки зросте на 50% до 2029 року. Головне зі звіту IT Ukraine Association. URL: https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/
6. Mishra, N. (2024). International Trade Law and Global Data Governance: Aligning Perspectives and Practices. Oxford: Hart Publishing.
7. Coates, C., Shahidulah, Sh., & McGee, Z. (Eds.). (2022). Advancements in Global Cyber Security Laws and Regulations. Business Science Reference.
8. Delarue, F. (2020). Cyber Operations and International Law. Cambridge: Cambridge University Press.
9. Joshi, A. (2024). Study of Cybersecurity Laws and Regulations. *Indian Journal of Law, 2*(3), 7–14. https://doi.org/10.36676/ijl.v2.i3.27
10. Zhao, F., Shi, Y., & Yao, K. (2021). Challenges and Countermeasures of China's Cyberspace Governance in the New Era. SHS Web of Conferences, 96, 01005.
11. Chiara, P. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review, 53*, 105961. https://doi.org/10.1016/j.clsr.2024.105961
12. Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration, 46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240
13. Hollis, D. (2021). A Brief Primer on International Law and Cyberspace. Carnegie Endowment. URL: https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en
14. Serrano, A. (2024). Global Cybersecurity and International Law. Routledge.
15. Kohler, C. (2020). The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization. International Cybersecurity Law Review, 1(1), 7–12. https://doi.org/10.1365/s43439-020-00008-1
16. Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyy009
17. Ткач, В. О. (2024). Глобальне управління у сфері кібербезпеки в контексті сучасних викликів та загроз Україні. *Ефективність державного управління, 1*(78/79), 84–89. https://doi.org/10.36930/507813
18. Carrapico, H., & Farrand, B. (2024). Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics. *JCMS: Journal of Common Market Studies, 62*, 147–158. https://doi.org/10.1111/jcms.13654
19. Obendiek, A. S., & Seidl, T. (2023). The (False) Promise of Solutionism: Ideational Business Power and the Construction of Epistemic Authority in Digital Security Governance. *Journal of European Public Policy, 30*, 1305–1329. https://doi.org/10.1080/13501763.2023.2172060
20. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-Directive Stacks up Against Its Predecessor. *Computer Law and*

Security Review, 52, 105890. https://doi.org/10.1016/j.clsr.2023.105890
21. Wouters, J., & Verhelst, A. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. International Organisations Research Journal. https://doi.org/10.17323/1996-7845-2020-02-07
22. Syrovatchenko, M. (2024). Legal aspects of cybersecurity in Ukraine: current challenges and the role of national legislation. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 11*(1(41)), 314–320. https://doi.org/10.23939/law2024.41.314
23. Futter, A. (2018). Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy, 3*(2), 201–216. https://doi.org/10.1080/23738871.2018.1514417

V. O. Tkach
Ukrainian National Forestry University, Lviv, Ukraine

INTERNATIONAL LEGAL REGULATION OF CYBERSECURITY: GLOBAL AND EUROPEAN CONTEXT

Introduction. In the current digital era, technology has fundamentally altered how we communicate, work, and live. But there are drawbacks to this shift, particularly in terms of data security and protection. Due to the surge in cybercrime, there is an immediate need for international rules and regulations that successfully handle these issues and establish a logical legal framework for managing risks and defending rights online. Numerous regional and international organizations are attempting to provide uniform guidelines and standards in the areas of data security and protection in response to this escalating threat.

States' conflicting interests, as well as variations in their legal systems and technological capacities, are among the many significant systemic barriers to successful cyberspace governance. It is challenging to reach an international agreement on the norms and values that ought to guide cyberspace because of these conflicts of interest.

Furthermore, the swift advancement of technology (such as artificial intelligence and the Internet of Things) poses new difficulties for the creation of pertinent rules and regulations. Additionally crucial are the particulars of each nation's cybersecurity regulations. There is now a situation where the actual state of cybersecurity efforts is far ahead of how laws and regulations are developing in this field. Given this, it is imperative that the cybersecurity environment be taken into account at the national and international levels.

Materials and methods. The research was conducted within the framework of the constructivist scientific paradigm. The tools included content analysis, comparative analysis, classification and generalization. The data sample was formed based on a search in the bibliometric databases Google Scholar, JSTOR, ScienceDirect and Wiley.

Analysis of literature sources. The quick and high-tech nature of the cyber revolution, territoriality, sovereignty, fragmentation of jurisdiction and legal attribution, and the engagement of the public and private sectors are some of the variables that contribute to the challenging alignment between cybersecurity and international lawmaking. The evolution of the application of the principle of non-interference in cyberspace was the subject of additional discussions. This discussion is crucial. Western nations in particular have taken a proactive stance in favor of applying this idea to the digital realm. The topic of coercion has received a lot of attention lately in conversations about non-interference in cyberspace. Experts stress that non-Western nations should play a more active role in interpreting and implementing the principle of non-interference in cyberspace.

Results. Today, the majority of States and a number of international organizations, including as the G20, the European Union, ASEAN, the OAS, and the UN General Assembly First Committee on Disarmament and International Security, have confirmed that current international law governs how States use ICTs. As a result, the current discussion is on the application of international law rather than its applicability. Nonetheless, states (and the entities they establish, such international organizations) are the primary beneficiaries of international law. Therefore, the regulation of cyberspace is not exclusively the domain of international law. Other regulatory frameworks, such as industry self-regulation, provide different options for business and civil society. For instance, multilateral governance is now the primary method used to control the Internet's infrastructure. Non-state actors have also shown interest in the application of international law to internet governance. Only a small portion of the international legal system is covered by the wide range of initiatives in the field of legal support for cybersecurity, particularly when it comes to the protection of critical infrastructure, the protection of private data on the network, and the use of cyber technologies in warfare.

Discussion. Issues concerning the application of international law to cyberspace can be divided into five distinct categories: (1) "silence"; (2) existential disagreements; (3) problems of interpretation; (4) attribution; and (5) accountability. There are several "existential" disputes among the governments that have adopted stances regarding the application of international law to cyberspace, which are conflicting assertions that a specific international legal standard or regime is completely included or excluded from cyberspace. The availability of international humanitarian law, the right to self-defense, the obligation of due diligence, and the right to take countermeasures against online behavior, for instance, have all been contested by a number of governments in the UN framework.

The presence (or lack) of one or more of these legal frameworks in cyberspace has a big impact on how international law is applied. It affects how states respond to malicious cyber activity by other states, how they conduct cyber operations during armed conflicts, and what steps they should take to protect third states' rights from harm that occurs on their own soil.

Only the actions of specific subjects of international law such as states are governed by it. It is typically not meant to regulate the behavior of ICT businesses or persons, who are typically governed by one or more domestic legal orders. Therefore, it is essential to determine whether the relevant action is being carried out by a state or a state-sponsored body that is subject to international law in order to apply international law in cyberspace. Regarding the application of international law to cyberspace, there are two main questions: (a) how should the underlying issues be resolved, and (b) where should this be done?

Conclusion. A multidimensional strategy that incorporates state collaboration, bolstering technical and legal capabilities, and fostering a global cybersecurity culture is needed to address global cybersecurity and data protection issues. Although there has been positive progress in this area, much more needs to be done to guarantee that everyone can use the internet safely. Addressing this common issue and defending rights in the digital sphere will need ongoing collaboration between governments, corporations, and civil society. Additionally, countermeasures are probably going to be essential in allowing states to react to transgressions of international law and provide justification for their actions. New discussions about the employment of countermeasures in cyberspace are emerging in this setting.

Keywords: cybersecurity, cyber threats, harmonization of legal standards, legal evolution, concept.