УДК 341
DOI https://doi.org/10.32844/2618-1258.2024.5.32

НАКОНЕЧНА І.В., БОНДАРЕНКО С.Ю.

ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ КІБЕРСУВЕРЕНІТЕТУ І ВИКЛИКИ МІЖНАРОДНОГО АДМІНІСТРАТИВНОГО ПРАВА

THEORETICAL AND LEGAL ANALYSIS OF CYBERSOVEREIGNTY AND CHALLENGES OF INTERNATIONAL ADMINISTRATIVE LAW

У статті розглядається нормативно-правовий зв'язок між кіберсуверенітетом і міжнародним адміністративним правом, зосереджуючись на регулятивних проблемах, пов'язаних з контрольованими державою кіберопераціями та захистом критичної інфраструктури. Використовуючи порівняльний аналіз Сполучених Штатів, Франції та Німеччини, досліджено правові складності, пов'язані з узгодженням національного кіберсуверенітету з міжнародно-правовими зобов'язаннями відповідно до адміністративного законодавства, які регулюють транснаціональну кібербезпеку. Концепція кіберсуверенітету, що ґрунтується на державоцентричній правовій доктрині, дозволяє державам затверджувати суверенну владу над відповідними кіберпросторами. Однак цей принцип дедалі більше суперечить глобалізованій природі кіберпростору, де кібероперації часто виходять за межі національних кордонів, ускладнюючи застосування традиційного адміністративного права. У цьому контексті дослідження ретельно вивчає адміністративні кодекси США (зокрема, Розділ 5 Кодексу Сполучених Штатів і Федеральний закон про модернізацію інформаційної безпеки), Франції (зокрема Закон № 2018-607 щодо безпеки справ і систем) d'information) та Німеччини (з акцентом на IT-Sicherheitsgesetz та Основному законі Федеративної Республіки Німеччини), щоб з'ясувати різні нормативні підходи до кібероперацій та безпеки критичної інфраструктури.

Отже, аналізуючи регуляторний режим США, який зосереджений на національну безпеку, а Франція орієнтована щодо гармонізації в рамках Директиви Європейського Союзу про мережеву та інформаційну безпеку (NIS). Німеччина виділяє дворівневий підхід щодо регулювання на федеральному та земельному рівнях.

Особливу увагу приділено фрагментацію адміністративної юриспруденції в управлінні кіберсуверенітетом. Проаналізовано, правові наслідки нормативних розбіжностей згідно міжнародного і адміністративного права, а також Будапештської конвенції про кіберзлочинність та резолюцій Генеральної Асамблеї ООН щодо кіберпростору. Визначено сутність міжнародного адміністративного право, що необхідно узгодити структуру щодо кіберрегулювання, значні правові дилеми виникають через різні тлумачення відповідальності держави, юрисдикційних обмежень та екстериторіального забезпечення дотримання кібернорм.

Стаття присвячена більш узгодженому підходу до кібероперацій у рамках міжнародного адміністративного права, який ефективно визначає інтереси національної безпеки з колективним імперативом захисту глобального кіберпростору. Автори пропонують визначити нормативно-правових актах транснаціональні реалії кібербезпеки для посилення державного суверенітету.

Ключові слова: *кіберсуверенітет, міжнародне і адміністративне право, кібероперації, критична інфраструктура, юрисдикційна фрагментація, транснаціональна кібербезпека.*

The article examines the regulatory relationship between cyber sovereignty and international administrative law, focusing on regulatory issues related to state-controlled

© НАКОНЕЧНА І.В. – доктор юридичних наук, доцент, професор кафедри загальноправових дисциплін (Національна академія Служби безпеки України) https://orcid.org/0000-0001-9405-4621

© БОНДАРЕНКО С.Ю. – фахівець кафедри технологій захисту кіберпростору центру кібербезпеки (Національна академія Служби безпеки України) https://orcid.org/0000-0001-8328-5117

cyber operations and the protection of critical infrastructure. Using a comparative analysis of the United States, France, and Germany, the legal complexities of reconciling national cyber sovereignty with international legal obligations under administrative law governing transnational cyber security are explored. The concept of cyber sovereignty, based on a state-centric legal doctrine, allows states to assert sovereign authority over their respective cyberspaces. However, this principle is increasingly at odds with the globalized nature of cyberspace, where cyber operations often transcend national borders, complicating the application of traditional administrative law. In this context, the study scrutinizes the administrative codes of the United States (in particular, Title 5 of the United States Code and the Federal Information Security Modernization Act), France (in particular, Law No. 2018-607 on the security of affairs and systems) d'information) and Germany (with an emphasis on IT-Sicherheitsgesetz and Basic Law of the Federal Republic of Germany) to clarify different regulatory approaches to cyber operations and critical infrastructure security.

So, analyzing the US regulatory regime, which is focused on national security, while France is oriented towards harmonization under the European Union's Network and Information Security (NIS) Directive. Germany has a two-tiered approach to regulation at the federal and state levels.

Special attention is paid to the fragmentation of administrative jurisprudence in the management of cyber sovereignty. The legal consequences of regulatory differences according to international and administrative law, as well as the Budapest Convention on Cybercrime and the resolutions of the UN General Assembly regarding cyberspace are analyzed.The essence of international administrative law has been determined, and it is necessary to harmonize the structure of cyber regulation, significant legal dilemmas arise due to different interpretations of state responsibility, jurisdictional limitations and extraterritorial enforcement of cyber norms.

The article is devoted to a more coherent approach to cyber operations within the framework of international administrative law, which effectively defines national security interests with the collective imperative to protect global cyberspace. The authors propose to define the transnational realities of cyber security in regulatory acts to strengthen state sovereignty.

Key words: *cyber sovereignty, international and administrative law, cyber operations, critical infrastructure, jurisdictional fragmentation, transnational cyber security.*

Постановка проблеми. Поширення кіберзагроз і все більша залежність від цифрової інфраструктури посилили важливість державного суверенітету в кіберпросторі, породивши доктрину кіберсуверенітету, за якою держави заявляють про контроль над своїми національними кібердоменами. Дана концепція, що розвивається, створює серйозні проблеми в рамках міжнародного адміністративного права, зокрема, оскільки держави беруть участь у контрольованих державою кібероперація, які часто перетинаються з проблемами глобальної кібербезпеки та захисту критичної інфраструктури. Внутрішній транснаціональний характер кібероперацій у поєднанні з глобальною взаємопов'язаністю критично важливих систем ускладнює традиційні парадигми адміністративного управління, створюючи правову трясовину на перетині суверенітету, юрисдикції та транснаціонального регулювання.

В основі цієї проблеми лежить протиріччя між національною нормативною базою, яка надає пріоритет державному контролю за кібердіяльністю, та міжнародно-правовими зобов'язаннями, спрямованими на встановлення єдиного глобального підходу до кібербезпеки. Зокрема, адміністративно-правова база в Сполучених Штатах, Франції та Німеччині пропонує різні підходи до регулювання контрольованих державою кібероперацій та захисту критичної інфраструктури, що відображає ширшу юриспруденційну фрагментацію у сфері кіберуправління.

Наприклад, у Сполучених Штатах відповідно до Розділу 5 Кодексу США та Федерального закону про модернізацію інформаційної безпеки (FISMA) використовується модель, орієнтована на національну безпеку, згідно з якою федеральний уряд здійснює широкий контроль над заходами кібербезпеки як для державних, так і для приватних організацій. у критичній інфраструктурі. Однак ця адміністративна структура викликає значні правові занепокоєння щодо екстериторіального впливу кібероперацій США, особливо тому, що вони стосуються транскордонних потоків даних і багатонаціональних корпоративних акторів. Крім того, регулятивний режим США часто

суперечить міжнародним договорам, таким як Будапештська конвенція про кіберзлочинність, де зберігаються питання перевищення юрисдикції та суперечливих регулятивних зобов'язань.

На противагу цьому, управління кібербезпекою у Франції тісніше узгоджується з наднаціональною нормативною архітектурою Європейського Союзу. Закон № 2018-607 про безпеку досліджень та систем інформації, який транспонує Директиву ЄС про безпеку мережі та інформації (NIS), накладає суворі адміністративні зобов'язання на операторів основних послуг і постачальників цифрових послуг. Незважаючи на те, що ця модель спрямована на гармонізацію правил кібербезпеки в ЄС, вона створює дворівневу нормативну структуру, яка, з одного боку, підтримує європейський принцип цифрового суверенітету, а з іншого – ускладнює його застосування до суб'єктів, які не входять до ЄС. у транскордонних кібероперація́х. Напруга між дотриманням Францією директив ЄС та її зобов'язаннями згідно з ширшими міжнародно-правовими рамками, такими як Резолюції Генеральної Асамблеї ООН щодо кібербезпеки, є прикладом юридичних проблем, які виникають при збалансуванні національних регулятивних імперативів із міжнародним адміністративним правом.

Німеччина, зі свого боку, діє згідно із Законом про безпеку ІТ (IT-Sicherheitsgesetz) та адміністративними положеннями, викладеними в Основному законі Федеративної Республіки Німеччина. Підхід Німеччини до регулювання кібербезпеки, незважаючи на те, що він надійний на національному рівні, відображає ширшу федералістську структуру німецького управління, створюючи додаткові складності у узгодженні регіональної політики кібербезпеки з федеральною системою. Ця децентралізована модель створює проблеми під час вирішення кібероперацій, які націлені або впливають на критичну інфраструктуру за межами кордонів Німеччини, особливо в світлі зобов'язань Німеччини в рамках міжнародних ініціатив із кібербезпеки та Загального регламенту захисту даних Європейського Союзу (GDPR), який накладає адміністративні вимоги на транскордонні дані. захисту.

Таким чином, фрагментація юрисдикції, очевидна в моделях кіберуправління США, Франції та Німеччини, підкреслює обмеження існуючого міжнародного адміністративного права в ефективному регулюванні контрольованих державою кібероперацій і безпеки критичної інфраструктури. Ці нормативні розбіжності призводять до невирішених правових питань щодо обсягу відповідальності держави, екстериторіального застосування адміністративних заходів та можливості виконання міжнародних норм перед обличчям вимог національного суверенітету. Оскільки кіберзагрози продовжують зростати, неадекватність поточної адміністративно-правової бази для вирішення глобального виміру кібербезпеки стає все більш очевидною.

Отже, аналізуючи правові дилеми, які виникають через суперечливі нормативні підходи до кіберсуверенітету, зосереджуючись на тому, як міжнародне адміністративне право може примирити конкуруючі інтереси державного контролю над кібероперація́ми з обов'язковим захистом критичної інфраструктури в глобально взаємопов'язаному кіберсередовищі. Спираючись на тематичні дослідження Сполучених Штатів, Франції та Німеччини, у цій статті розглядатимуться нормативні конфлікти між національними адміністративними кодексами та міжнародними рамками кібербезпеки з метою визначення шляхів до більш узгодженого та юридично обґрунтованого підходу до кіберуправління.

Аналіз останніх досліджень та публікацій. 1) Йорг Каммерхофер [Jörg Kammerhofer], відомий своєю роботою над принципами міжнародного адміністративного права та його застосуванням у різних контекстах, включаючи кібернетичне право; 2) Саманта Бессон [Samantha Besson], вчений-юрист, яка дослідила перетин міжнародного права та адміністративного права, зосереджуючись на регулятивній практиці та наслідках для суверенітету; 3) Даніель Айрланд-Пайпер [Danielle Ireland-Piper] займається дослідженнями міжнародного права, зокрема адміністративної та нормативної бази у відповідь на глобальні виклики, зокрема кібербезпеку; 4) Майкл Н. Шмітт [Michael N. Schmitt], експерт з міжнародного права кібероперацій, він зробив значний внесок у правові рамки поведінки держави в кіберпросторі; 5) Пол К. Шаш [Paul C. Szasz], зосереджений на правових наслідках міжнародних структур управління, зокрема в контексті адміністративного права та прав людини; 6) Антонія Хендлер Чейс [Antonia Handler Chayes], її дослідження включають роль міжнародного адміністративного права в управлінні транснаціональними питаннями, включаючи безпеку та захист інфраструктури; 7) Роберт Л. Гліксман [Robert L. Glicksman], вчений, чия робота включає перетин екологічного права, міжнародного адміністративного права та регулювання глобальних кіберзагроз; 8) Глен МакГі [Glen McGhee], науковець, чиї дослідження заглиблюються в наслідки державного суверенітету та адміністративного права в контексті кібероперацій та міжнародного управління.

Мета статті. Висвітлити правові дилеми в контексті міжнародного адміністративного права.

Виклад основного матеріалу. Еволюція цифрових технологій і зростання кібероперацій змінили традиційні межі суверенітету, породивши нові виклики в сфері міжнародного адміністративного права. Концепція кіберсуверенітету, яка підкреслює право держав здійснювати суверенний контроль над своїми національними кіберпросторами, представляє глибоку правову дилему в контексті контрольованих державою кібероперацій і регулювання критичної інфраструктури.

Кіберсуверенітет означає твердження державами своїх суверенних прав над кіберпростором у межах їх територіальних кордонів. Цей принцип, вкорінений у ширшій концепції державного суверенітету, закріпленій у статті 2(7) Статуту Організації Об'єднаних Націй, надає державам повноваження регулювати діяльність у кіберпросторі, включаючи управління критичною інфраструктурою, цифровими платформами та потоками даних [1]. Однак глобальний характер кіберпростору, який характеризується його зв'язністю без кордонів, ускладнює здійснення такого суверенітету, особливо коли кібероперації мають екстериторіальний вплив або залучають транснаціональних гравців.

У цьому контексті міжнародне адміністративне право стикається з унікальною дилемою: як узгодити суверенну прерогативу держав регулювати кібероперації в межах своїх власних кордонів із необхідністю глобальної нормативної бази, яка враховує транскордонний характер кіберзагроз. Ця напруга є особливо гострою, коли йдеться про регулювання критичної інфраструктури, визначеної як системи та активи, життєво важливі для національної безпеки, економіки, здоров'я населення чи безпеки держави, такі як електромережі, мережі зв'язку та фінансові системи. Захист критичної інфраструктури від кібератак є ключовою проблемою для національних урядів, але взаємозалежність цих систем через кордони вимагає співпраці та координації на міжнародному рівні.

Сполучені Штати, Франція та Німеччина мають різні правові рамки, що регулюють кібероперації та критичну інфраструктуру, що відображає їхні унікальні адміністративні традиції та підходи до державного суверенітету в кіберпросторі. Однак ці національні рамки також повинні діяти в рамках обмежень міжнародного права, що призводить до складних правових взаємодій і потенційних конфліктів.

У Сполучених Штатах на регулювання кібероперацій та критичної інфраструктури значною мірою впливають проблеми національної безпеки. Федеральний закон про модернізацію інформаційної безпеки (FISMA), кодифікований у розділі 44 Кодексу США [U.S. Code], встановлює основу для захисту федеральних інформаційних систем і зобов'язує федеральні агентства впроваджувати надійні заходи кібербезпеки [2; 3]. FISMA надає значні повноваження Департаменту внутрішньої безпеки (DHS) для нагляду за захистом критично важливої інфраструктури, включаючи повноваження видавати обов'язкові оперативні директиви для федеральних агентств і організацій приватного сектора.

Крім того, Закон про обмін інформацією про кібербезпеку (CISA) 2015 року полегшує обмін інформацією про кіберзагрози між федеральним урядом і суб'єктами приватного сектору з метою покращення загального стану кібербезпеки Сполучених Штатів [4]. Однак такий режим обміну інформацією викликає юридичні питання щодо захисту персональних даних і можливості надмірного втручання федерального уряду в діяльність приватних організацій, особливо тих, що працюють за кордоном.

Екстериторіальне застосування законів США про кібербезпеку є ще однією важливою проблемою, особливо в світлі Закону про роз'яснення законного використання даних за кордоном (CLOUD), який дозволяє правоохоронним органам США отримувати доступ до даних, що зберігаються за кордоном американськими компаніями [5]. Це екстериторіальне охоплення було оскаржено на міжнародних форумах, оскільки воно суперечить режимам захисту даних інших держав, зокрема в Європейському Союзі, що викликає занепокоєння щодо балансу між інтересами національної безпеки США та міжнародними нормами державного суверенітету.

Одним із центральних правових документів у цьому контексті є Федеральний закон про модернізацію інформаційної безпеки (FISMA), кодифікований у 44 U.S.C. § 3551 і далі. FISMA створює всеосяжну структуру для захисту федеральних інформаційних систем і критичної інфраструктури від кіберзагроз. Статут надає значні повноваження Міністерству внутрішньої безпеки (DHS) для нагляду та координації зусиль у сфері кібербезпеки між федеральними відомствами, наголошуючи на підході до безпеки критичної інфраструктури, що ґрунтується на оцінці ризиків. Відповідно до FISMA, DHS доручено видавати обов'язкові оперативні директиви (BOD), які є юридично обов'язковими наказами, спрямованими на пом'якшення ризиків кібербезпеки

у федеральних системах. Однак обсяг FISMA викликає питання щодо екстериторіального охоплення політики кібербезпеки США, особливо коли федеральні агентства беруть участь у кібероперaціях, які мають транскордонні наслідки.

Іншим ключовим нормативним актом є Закон про обмін інформацією про кібербезпеку (CISA) 2015 року, який полегшує обмін індикаторами кіберзагроз і захисними заходами між федеральним урядом і організаціями приватного сектору. Кодифіковано в 6 U.S.C. § 1501 і далі, CISA заохочує добровільний обмін інформацією, одночасно забезпечуючи захист від відповідальності для приватних організацій, які діляться даними про кіберзагрози з урядом. Цей статут підкреслює важливість державно-приватного партнерства в забезпеченні критичної інфраструктури, але він також викликає юридичні занепокоєння щодо захисту персональних даних і потенційного конфлікту між внутрішніми заходами безпеки та міжнародними законами про конфіденційність, такими як Загальний регламент ЄС про захист даних (GDPR).

Закон про роз'яснення законного використання даних за кордоном (Clarifying Lawful Overseas Use of Data, CLOUD), кодифікований у 18 U.S.C. § 2713 ще більше ускладнює правовий ландшафт, дозволяючи правоохоронним органам США вимагати розкриття даних, які зберігаються американськими компаніями за кордоном. Екстериторіальне застосування Закону CLOUD спричинило судові суперечки в міжнародних судах, оскільки це потенційно суперечить суверенітету іноземних держав та їхнім законам про захист даних. Цей статут підкреслює суперечність між заявами США про кіберсуверенітет і міжнародним принципом невтручання, закріпленим у статті 2(4) Статуту Організації Об'єднаних Націй, яка забороняє державам втручатися у внутрішні справи інших держав.

Одним із найбільш спірних питань у регулюванні контрольованих державою кібероперацій є екстериторіальне застосування кіберзаконів США. Як зазначалося раніше, Закон CLOUD дозволяє правоохоронним органам США отримувати доступ до даних, що зберігаються за кордоном, що створює правові конфлікти із законами про захист даних інших штатів. Подібним чином, Закон про міжнародні надзвичайні економічні повноваження (International Emergency Economic Powers Act, IEEPA), кодифікований у 50 U.S.C. § 1701 і наступні надають президенту широкі повноваження регулювати міжнародну торгівлю у відповідь на незвичайні або надзвичайні загрози, включаючи кіберзагрози. Згідно з IEEPA, президент може накладати санкції на іноземні організації, які займаються кібердіяльністю, яка вважається шкідливою для національної безпеки США або критичної інфраструктури.

Екстериторіальне застосування кіберзаконів США оскаржувалося на різних міжнародних юридичних форумах, зокрема, згідно з принципом ввічливості, який вимагає від держав поважати суверенітет інших держав у забезпеченні виконання їхніх внутрішніх законів. Твердження США про екстериторіальну юрисдикцію в кіберсфері також було піддано критиці через потенційне порушення принципу Лотоса, сформульованого в рішенні Постійної палати міжнародного правосуддя [Cour permanente de justice internationale] у справі Лотус (Франція проти Туреччини, 1927), згідно з яким держави не можуть здійснювати їхню юрисдикцію за межі їхніх кордонів, якщо це прямо не дозволено міжнародним правом [6].

Підхід Франції до кібербезпеки сформований її членством у Європейському Союзі та її прагненням узгодити національне законодавство з директивами ЄС. Закон № 2018-607 про безпеку досліджень і систем інформації, який транспонує Директиву про мережеву та інформаційну безпеку (NIS) у законодавство Франції, накладає суворі зобов'язання на операторів основних послуг (OES) і постачальників цифрових послуг [7]. (DSP) для впровадження надійних заходів кібербезпеки. Французька адміністративна структура кібербезпеки контролюється Агентством національної безпеки систем інформації (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI), яке відповідає за координацію захисту критичної інфраструктури та реагування на кіберінциденти.

Директива NIS, яка застосовується у Франції, створює дворівневу нормативну структуру, яка вимагає відповідності як на національному рівні, так і на рівні ЄС, що відображає наднаціональний характер правової системи Європейського Союзу. Однак цей дворівневий підхід також створює юридичні складності, особливо у випадках, коли французькі організації діють у кількох юрисдикціях ЄС або беруть участь у кібероперaціях, які мають екстериторіальний вплив. Крім того, зобов'язання Франції відповідно до Загального регламенту захисту даних (GDPR) додають ще один рівень адміністративної складності, оскільки GDPR встановлює суворі вимоги до обробки та передачі персональних даних, що може суперечити потребам національних служб безпеки, залучених до кібероперaцій [8].

Франція вже давно є прихильником кіберсуверенітету як основного аспекту своєї стратегії національної безпеки. Це відображено в її Кодексі оборони [Code de la Défence], зокрема в статті L2321-1, яка окреслює повноваження держави над критичною інфраструктурою, включаючи мережі, життєво важливі для національної безпеки [9]. Крім того, Закон про цифрову республіку (Loi pour une République numérique), прийнятий у 2016 році, посилює регуляторний вплив держави в кіберпросторі шляхом посилення суверенітету даних і кібербезпеки [10].

Вирішальним компонентом режиму кібербезпеки Франції є Національне агентство з безпеки систем інформації (ANSSI), створене згідно з Указом № 2009-834, яке є головним регулюючим органом, що наглядає за державними операціями з кібербезпеки та захистом критичної інфраструктури [11]. ANSSI відіграє ключову роль у координації національної кіберзахисту, встановленні обов'язкових стандартів кібербезпеки та нагляді за контрольованими державою кіберопераціями.

Однак утвердження французького кіберсуверенітету створює значні проблеми, особливо у зв'язку з екстериторіальним застосуванням французьких законів у кіберпросторі. Згідно з міжнародним правом, державам, як правило, заборонено здійснювати екстериторіальну юрисдикцію, якщо це прямо не дозволено міжнародними договорами чи звичаєвим правом. Принцип Лотоса, встановлений Постійною палатою міжнародного правосуддя (PCIJ) у справі С. С. Лотус (Франція проти Туреччини, 1927 р.), передбачає, що держави можуть здійснювати свою юрисдикцію лише тоді, коли міжнародним правом немає прямої заборони. Тим не менш, збільшення частоти транскордонних кібероперацій викликає питання про обмеження цього принципу в епоху цифрових технологій.

Крім того, Загальний регламент захисту даних (GDPR), прийнятий Європейським Союзом, накладає суворі вимоги до обробки персональних даних у межах ЄС, що викликає занепокоєння щодо перетину французького кіберсуверенітету з міжнародними потоками даних. Стаття 3 GDPR прямо розширює територіальну сферу дії на будь-яку юридичну особу, яка обробляє персональні дані громадян ЄС, незалежно від того, де розташована юридична особа. Це положення має значні наслідки для контрольованих державою кібероперацій, пов'язаних зі збором і обробкою даних, особливо в контекстах, де такі операції перетинаються з іноземними юрисдикціями.

Контрольовані державою кібероперації у Франції регулюються складним набором національних і міжнародних правових інструментів. Loi de programmation militaire (Закон про військове програмування), зокрема його положення відповідно до статті L2321-2 Кодексу оборони, уповноважує уряд Франції проводити кібероперації для захисту інтересів національної безпеки, включаючи запобігання кібератакам на критичну інфраструктуру.

Однак проведення контрольованих державою кібероперацій створює значні правові дилеми з точки зору міжнародного права. Статут ООН, зокрема стаття 2(4), забороняє застосування сили або втручання у внутрішні справи суверенних держав. Цей принцип тлумачиться в контексті кібероперацій Талліннським керівництвом 2.0 з міжнародного права, застосовного до кібероперацій, яке передбачає, що кібероперації, які призводять до значної шкоди критичній інфраструктурі або посягають на суверенітет іншої держави, можуть потенційно порушити принцип невтручання.

Крім того, участь Франції в Агентстві Європейського Союзу з кібербезпеки (ENISA) і Спільному центрі передового досвіду кіберзахисту НАТО (CCDCOE) підкреслює її відданість міжнародній співпраці в галузі кібербезпеки. Однак відсутність чітких міжнародно-правових норм, які регулюють контрольовані державою кібероперації, продовжує створювати проблеми для Франції, особливо в світлі її екстериторіальних зобов'язань і необхідності збалансувати національний суверенітет і міжнародне співробітництво.

4. Захист критичної інфраструктури у Франції: правові та міжнародні міркування

Захист критичної інфраструктури є ключовим компонентом політики кіберсуверенітету Франції. Прийнятий у 2018 році Закон про безпеку досліджень і систем інформації (Закон NIS) транспонує Директиву ЄС щодо безпеки мережевих та інформаційних систем (Директива NIS) у законодавство Франції. Закон про NIS накладає суворі зобов'язання на операторів основних послуг і постачальників цифрових послуг щодо забезпечення безпеки своїх мереж і систем, а також повідомляти ANSSI про значні інциденти кібербезпеки.

Рамки захисту критичної інфраструктури Франції також формуються міжнародними договорами та зобов'язаннями. Будапештська конвенція про кіберзлочини, яку підписала Франція, забезпечує правову основу для міжнародного співробітництва в розслідуванні та судовому переслідуванні кіберзлочинів, включаючи атаки на критичну інфраструктуру. Однак Будапештська

конвенція в першу чергу стосується кіберзлочинності, а не контрольованих державою кібероперацій, створюючи прогалину в міжнародно-правовій базі для регулювання діяльності держави в кіберпросторі.

Крім того, Резолюція Генеральної Асамблеї ООН 70/237 про захист критичної інфраструктури [UN General Assembly Resolution 70/237] підкреслює важливість міжнародного співробітництва у захисті критичної інфраструктури від кібератак [12]. Ця резолюція узгоджується із зобов'язаннями Франції згідно зі статтею 1 Міжнародного пакту про громадянські та політичні права (МПГПП), яка гарантує право людей вільно розпоряджатися своїми природними багатствами та ресурсами, включаючи цифрові ресурси, життєво важливі для критичної інфраструктури [13]. Таким чином, внутрішня законодавча база Франції має узгоджуватися з її міжнародними зобов'язаннями щодо захисту критичної інфраструктури від кібератак, одночасно гарантуючи, що її кіберсуверенітет не порушує права інших держав згідно з міжнародним правом.

Нормативно-правова база як федералістський підхід Німеччини щодо кібербезпеки регулюється Законом про безпеку ІТ (IT-Sicherheitsgesetz), який накладає суворі вимоги до операторів критичної інфраструктури щодо впровадження заходів кібербезпеки та звітування про кіберінциденти до Bundesamt für Sicherheit in der Informationstechnik (BSI), федерального органу з кібербезпеки Німеччини. Агентство [14]. Основний закон Федеративної Республіки Німеччина також відіграє вирішальну роль у формуванні правового ландшафту кібербезпеки, оскільки він встановлює конституційну основу для захисту прав особи та розподілу повноважень між федеральним урядом і землями.

Федералістична система Німеччини створює унікальні проблеми в регулюванні кібероперацій, оскільки землі мають значні повноваження щодо певних аспектів кібербезпеки, зокрема щодо місцевої критичної інфраструктури. Ця децентралізована модель ускладнює зусилля з розробки єдиної національної стратегії кібербезпеки, оскільки різні регіони можуть прийняти різні підходи до регулювання кібероперацій і захисту критичної інфраструктури.

На міжнародному рівні Німеччина пов'язана своїми зобов'язаннями згідно з Будапештською конвенцією про кіберзлочинність, яка встановлює основу для міжнародного співробітництва в розслідуванні та судовому переслідуванні кіберзлочинів [15]. Проте положення Будапештської конвенції про транскордонний доступ до даних і співпрацю правоохоронних органів критикували за те, що вони не повністю вирішують проблеми, пов'язані з контрольованими державою кіберопераціями та захистом критичної інфраструктури.

У Німеччині концепція кіберсуверенітету тісно пов'язана з національною безпекою та захистом критичної інфраструктури. Правова база Німеччини для кібербезпеки в основному визначається Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), широко відомим як Закон про безпеку ІТ. Цей закон, кодифікований у Законі про телекомунікації (TKG) і Законі про телемедіа (TMG), надає федеральному уряду повноваження регулювати стандарти кібербезпеки для постачальників критичної інфраструктури. Закон про ІТ-безпеку накладає суворі вимоги на операторів критичної інфраструктури, включаючи обов'язкове звітування про інциденти кібербезпеки до Федерального відомства з інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik, BSI).

Однією з ключових проблем, пов'язаних із Законом про безпеку ІТ, є сфера його екстериторіального застосування. Оскільки критична інфраструктура Німеччини все більше залежить від глобальних ланцюгів постачання та міжнародних потоків даних, твердження про кіберсуверенітет Німеччини ризикує конфліктувати з суверенітетом інших держав, особливо коли кібероперації Німеччини чи регуляторні заходи впливають на іноземну критичну інфраструктуру. Федеральний конституційний суд розглядав питання екстериторіальної юрисдикції у справах кібербезпеки в кількох постановах, наголошуючи на необхідності тесту на пропорційність відповідно до конституційного права Німеччини. Ці рішення підкреслюють суперечність між інтересами національної безпеки Німеччини та її зобов'язаннями згідно з міжнародним правом, зокрема принципом невтручання.

Окрім національних законів, правовий підхід Німеччини до кіберсуверенітету формується її зобов'язаннями згідно із законодавством Європейського Союзу. Загальний регламент ЄС із захисту даних (GDPR), який застосовується до обробки персональних даних у всьому ЄС, накладає суворі обмеження на екстериторіальну передачу даних, що викликає сумніви щодо сумісності кіберсуверенітету Німеччини з міжнародними законами про захист даних. Відповідно до статті 3 GDPR, будь-яка організація, яка обробляє дані громадян ЄС, підлягає регулюванню, незалежно від того, де відбувається обробка. Це має значні наслідки для контрольованих державою

кібероперацій, які передбачають збір або обробку персональних даних, особливо в транскордонному контексті.

Правова база Німеччини для контрольованих державою кібероперацій є складним поєднанням національних законів, міжнародних правових принципів і директив Європейського Союзу. Одним із ключових законів, що регулюють кібероперації в Німеччині, є Gesetz über das Bundesamt für den Verfassungsschutz (BfV-Gesetz), який регулює повноваження Федерального відомства з охорони конституції (BfV) [16]. Відповідно до цього закону BfV має право брати участь у кіберопераціях з метою захисту від загроз конституційному порядку, включаючи шпигунство, диверсії та тероризм.

У контексті кібероперацій Німеччини принцип відповідальності держави є особливо актуальним. Відповідно до статті 16 проекту статей про відповідальність держав за міжнародно-протиправні дії (ARSIWA), держава може нести відповідальність за допомогу іншій державі у здійсненні міжнародно-протиправних дій, включаючи кібероперації, які порушують суверенітет третіх держав. Таким чином, законодавча база Німеччини повинна гарантувати, що контрольовані державою кібероперації відповідають міжнародному праву, особливо коли такі операції мають екстериторіальний вплив.

Будапештська конвенція про кіберзлочинність, учасницею якої є Німеччина, забезпечує основу для міжнародного співробітництва в розслідуванні та судовому переслідуванні кіберзлочинів, включаючи кібероперації, контрольовані державою. Проте в Будапештській конвенції прямо не йдеться про відповідальність держави за кібероперації, що проводяться державними суб'єктами, що залишає значну прогалину в міжнародно-правовій базі для регулювання контрольованої державою кібердіяльності. Участь Німеччини в Агентстві Європейського Союзу з кібербезпеки (ENISA) і Спільному центрі передового досвіду кіберзахисту НАТО (CCDCOE) відображає її прихильність до міжнародного співробітництва в галузі кібербезпеки, але відсутність чітких міжнародних правил, що регулюють контрольовані державою кібероперації, продовжує становити законність [17].

Захист критичної інфраструктури є центральною проблемою політики кібербезпеки Німеччини, особливо в світлі зростаючої загрози кібератак на основні служби, такі як енергетика, транспорт і зв'язок. Критична інфраструктурна інформація (KRITIS-Verordnung), видана відповідно до Закону про безпеку ІТ, визначає сектори критичної інфраструктури та накладає обов'язкові вимоги до кібербезпеки для операторів основних послуг [18]. Регламент вимагає від операторів критичної інфраструктури впроваджувати найсучасніші заходи безпеки та повідомляти BSI про значні кіберінциденти.

Внутрішня правова база Німеччини щодо захисту критичної інфраструктури доповнюється її зобов'язаннями згідно з міжнародним правом, зокрема в контексті Європейського Союзу. Директива ЄС щодо безпеки мережевих та інформаційних систем (Директива NIS), яка була перенесена в законодавство Німеччини через IT-Sicherheitsgesetz 2.0, встановлює правову основу для забезпечення безпеки основних послуг і критичної інфраструктури в ЄС. Директива NIS вимагає від держав-членів призначати національні органи, відповідальні за кібербезпеку, і вживати заходів для підвищення стійкості критичної інфраструктури до кіберзагроз.

Окрім законодавства ЄС, Німеччина пов'язана міжнародними договорами, які регулюють захист критичної інфраструктури від кіберзагроз. Будапештська конвенція про кіберзлочинність забезпечує правову основу для міжнародного співробітництва у боротьбі з кіберзлочинністю, включаючи атаки на критичну інфраструктуру. Крім того, Резолюція Генеральної Асамблеї ООН 70/237 про захист критичної інфраструктури підкреслює важливість міжнародного співробітництва для забезпечення безпеки критичної інфраструктури від кібератак. Хоча ці міжнародні документи забезпечують основу для співпраці, вони не повністю вирішують правові складнощі, пов'язані з контрольованими державою кіберопераціями, спрямованими на іноземну критичну інфраструктуру.

Однак контрольовані державою кібероперації, які проводить Німеччина, викликають значні правові дилеми з точки зору міжнародного права, зокрема принципів відповідальності держави та належної обачності. Талліннський посібник 2.0 [Tallinn Manual 2.0] щодо міжнародного права, застосовного до кібероперацій, хоча і не є юридично обов'язковим, надає авторитетні вказівки щодо того, як міжнародно-правові принципи, такі як суверенітет, невтручання та відповідальність держави, застосовуються до кібероперацій [19]. Згідно з Талліннським посібником, держави мають юридичне зобов'язання проявляти належну обачність, щоб запобігти використанню їх території для запуску кібероперацій, які завдають шкоди іншим державам. Цей принцип

відображено в статті 2(4) Статуту Організації Об'єднаних Націй, яка забороняє застосування сили або інших форм втручання у внутрішні справи суверенних держав.

Транснаціональний характер кіберзагроз та критичної інфраструктури зумовлює необхідність міжнародної співпраці в регулюванні контрольованих державою кібероперацій. Проте затвердження кіберсуверенітету такими державами, як Німеччина, може створювати юридичні перешкоди для такої співпраці, особливо коли національне законодавство суперечить міжнародним правовим зобов'язанням. Агентство Європейського Союзу з кібербезпеки (ENISA) і Спільний центр передового досвіду кіберзахисту НАТО (CCDCOE) є ключовими установами, через які Німеччина співпрацює з іншими державами в розробці політики кібербезпеки та захисту критичної інфраструктури. Однак відсутність обов'язкових міжнародних правил, що регулюють контрольовані державою кібероперації, продовжує створювати проблеми для міжнародного співробітництва.

Правовий принцип належної обачності відіграє вирішальну роль у регулюванні контрольованих державою кібероперацій. Згідно з міжнародним правом, держави мають юридичне зобов'язання запобігати використанню своєї території для здійснення кібероперацій, які завдають шкоди іншим державам. Цей принцип, кодифікований у Талліннському посібнику 2.0, вимагає від держав вживати всіх розумних заходів для запобігання кіберопераціям, які порушують суверенітет інших держав. У контексті кібероперацій Німеччини принцип належної обачності є особливо актуальним, оскільки контрольовані державою кібероперації часто мають екстериторіальні наслідки, які можуть порушувати суверенітет інших держав.

Висновки. Регулювання контрольованих державою кібероперацій створює значні правові дилеми в контексті міжнародного адміністративного права. Однією з ключових проблем є екстериторіальний вплив кібероперацій, оскільки держави часто беруть участь у кібердіяльності, яка навмисно чи ненавмисно впливає на критичну інфраструктуру інших держав. Це викликає питання про відповідальність держав за міжнародним правом, особливо в світлі принципів, закріплених у проекті статей про відповідальність держав за міжнародно-протиправні дії, які встановлюють, що держави можуть бути притягнуті до відповідальності за дії, які порушують суверенітет інших держав.

Регулювання контрольованих державою кібероперацій та захист критичної інфраструктури є серйозними проблемами для міжнародного адміністративного права. Різні правові рамки Сполучених Штатів, Франції та Німеччини відображають ширшу напругу між здійсненням національного суверенітету в кіберпросторі та необхідністю скоординованої міжнародної відповіді на кіберзагрози. Оскільки кібероперації продовжують ускладнюватися та масштабуватися, існує гостра потреба у розробці більш узгодженої та гармонізованої глобальної правової бази, яка могла б узгодити конкуруючі інтереси державного суверенітету, національної безпеки та міжнародного співробітництва у захисті критичної інфраструктури.

Така структура повинна вирішувати правові дилеми, викликані екстериторіальним впливом кібероперацій, фрагментацією адміністративних правил і відповідальністю держав згідно з міжнародним правом за кібердіяльність, яка виходить за межі національних кордонів. Регулювання контрольованих державою кібероперацій та захист критичної інфраструктури є серйозною юридичною дилемою для Сполучених Штатів, особливо в контексті міжнародного адміністративного права. Законодавча база США, сформована національним законодавством, таким як FISMA, CISA та CLOUD Act, відображає сильний акцент на національній безпеці та кіберсуверенітеті. Однак екстериторіальна дія кіберзаконів США та проведення кібероперацій, які впливають на іноземну критичну інфраструктуру, викликають глибокі питання щодо відповідальності держави, належної обачності та сумісності законів США з міжнародними правовими зобов'язаннями. Оскільки кіберзагрози продовжують розвиватися, існує нагальна потреба в розробці більш узгодженої та міжнародно прийнятої правової бази, яка б регулювала контрольовані державою кібероперації та захист критичної інфраструктури. Така структура повинна врівноважувати вимоги національного суверенітету з реаліями глобальної взаємопов'язаності, гарантуючи, що держави можуть захищати свій кіберпростір, не порушуючи прав інших.

Правові дилеми, викликані затвердженням Німеччиною кіберсуверенітету в регулюванні контрольованих державою кібероперацій і захисту критичної інфраструктури, підкреслюють потребу в більш узгодженій і міжнародно прийнятій правовій базі, що регулює кіберпростір. Транснаціональний характер кіберзагроз у поєднанні зі складністю міжнародного права вимагає тонкого балансу між імперативами національної безпеки та необхідністю міжнародної співпраці. Хоча внутрішня законодавча база Німеччини забезпечує міцну основу для регулювання кібербезпеки,

відсутність чітких міжнародних правил, що регулюють контрольовані державою кібероперації та захист критичної інфраструктури, продовжує створювати серйозні проблеми для міжнародного адміністративного права.

Законодавча база Франції також має відповідати принципу належної обачності, сформульованому в статті 1 Проекту статей про відповідальність держав за міжнародно-протиправні дії (ARSIWA). Цей принцип зобов'язує держави гарантувати, що їхня територія не використовується для проведення кібероперацій, які завдають значної шкоди іншим державам. Це зобов'язання є особливо актуальним у контексті контрольованих державою кібероперацій, які включають транскордонну діяльність або впливають на критичну інфраструктуру інших держав. Таким чином, правовий режим Франції повинен включити міжнародні зобов'язання щодо належної обачності у свою національну нормативну базу для забезпечення дотримання міжнародного права.

Затвердження Францією свого кіберсуверенітету в регулюванні контрольованих державою кібероперацій і захисту критичної інфраструктури створює складну правову дилему. У той час як французьке законодавство забезпечує міцну основу для регулювання кібердіяльності в межах її кордонів, транснаціональний характер кіберпростору та відсутність чітких міжнародних правових норм, що регулюють контрольовані державою кібероперації, створюють значні проблеми. Законодавча база Франції повинна збалансувати необхідність захисту національної безпеки та критичної інфраструктури з її зобов'язаннями згідно з міжнародним правом, зокрема принципами державного суверенітету, невтручання та належної обачності. Крім того, участь Франції в таких міжнародних установах, як ENISA та CCDCOE, підкреслює важливість міжнародного співробітництва у вирішенні правових проблем, пов'язаних з контрольованими державою кіберопераціями. Зрештою, регулювання контрольованих державою кібероперацій та захисту критичної інфраструктури у Франції підкреслює ширшу потребу в узгодженій міжнародно-правовій базі, що регулює кіберпростір. Оскільки держави продовжують стверджувати кіберсуверенітет, правові дилеми, пов'язані з контрольованими державою кіберопераціями, залишатимуться центральною проблемою в міжнародному адміністративному праві.

Список використаних джерел:

1. Учасники проектів Вікімедіа. Статут Організації Об'єднаних Націй – Вікіджерела. Вікіджерела – вільна бібліотека. URL: https://uk.wikisource.org/wiki/Статут_Організації_Об'єднаних_Націй (дата звернення: 11.10.2024).

2. Federal Information Security Modernization Act (FISMA). Information Security & Privacy Group. Homepage – URL: https://security.cms.gov/learn/federal-information-security-modernization-act-fisma (дата звернення: 21.10.2024).

3. OLRC Home. The Office of the Law Revision Counsel. URL: https://uscode.house.gov/ (дата звернення: 21.10.2024).

4. An official website of the U.S. Department of Homeland Security. *CISA*. URL: https://www.cisa.gov/ (дата звернення: 21.10.2024).

5. The CLOUD Act. Eurojust. URL: https://www.eurojust.europa.eu/publication/cloud-act#:~:text=The%20Clarifying%20Lawful%20Overseas%20Use,the%20context%20of%20criminal%20investigations. (дата звернення: 21.10.2024).

6. The Case of the S.S. Lotus, France v. Turkey, Judgment, 7 September 1927, Permanent Court of International Justice (PCIJ). *WorldCourts: International Case Law Database (Judgments, AdvisoryOpinions, Views & Decisions)*. URL: https://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (дата звернення: 21.10.2024).

7. Implementing regulation – 2018/607. EUR-Lex – Access to European Union law. URL: https://eur-lex.europa.eu/eli/reg_impl/2018/607/oj (дата звернення: 21.10.2024).

8. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент; Європейський Союз від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/go/984_008-16 (дата звернення: 21.10.2024)

9. Defense Code, 2004 (as amended on 2010), Code de la Défence. *International Humanitarian Law Databases*. URL: https://ihl-databases.icrc.org/en/national-practice/defense-code-2004-amended-2010 (дата звернення: 21.10.2024).

10. LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique – Dossiers législatifs – Légifrance. Légifrance. URL: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/ (дата звернення: 21.10.2024).

11. Regulation – 834/2009 – EN – EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009R0834 (дата звернення: 21.10.2024).

12. Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)] 70/237. Developments in the field of information and telecommunications in the context of international security. Official Document System – UN. URL: https://documents.un.org/doc/undoc/gen/n15/457/57/pdf/n1545757.pdf (дата звернення: 21.10.2024).

13. Міжнародний пакт про громадянські і політичні права : Пакт; ООН від 16.12.1966 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_043 (дата звернення: 21.10.2024)

14. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). *Bundesamt für Sicherheit in der Informationstechnik*. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (дата звернення: 21.10.2024).

15. Convention on cybercrime | EUR-Lex. EUR-Lex – Access to European Union law. URL: https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html (дата звернення: 21.10.2024).

16. BVerfSchG – nichtamtliches Inhaltsverzeichnis. *Gesetze im Internet*. URL: https://www.gesetze-im-internet.de/bverfschg/ (дата звернення: 21.10.2024).

17. CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/ (дата звернення: 21.10.2024).

18. BSI-KritisV – Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz. Gesetze im Internet. URL: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (дата звернення: 21.10.2024).

19. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/news/2017/tallinn-manual-2-0-on-the-international-law-applicable-to-cyber-operations-to-be-launched/ (дата звернення: 21.10.2024).