

КІБЕРДИПЛОМАТІЯ ЯК ВАЖЛИВИЙ НАПРЯМОК МІЖНАРОДНО-ПРАВОВОГО СПІВРОБІТНИЦТВА В УМОВАХ РЕЖИМУ ВОЄННОГО СТАНУ

Поляков Олександр Миколайович,

orcid.org/0000-0002-8984-1476

начальник відділу

Українського науково-дослідного інституту спеціальної техніки

та судових експертиз

Служби безпеки України

У цій статті розглянуто засади міжнародного співробітництва у сфері забезпечення кібербезпеки. Акцентовано роль України як активного суб'єкта глобальної системи безпеки в умовах російської військової загрози. Деталізовано поняття та зміст кібердипломатії. Розкрито мету та завдання кібердипломатії як важливої складової частини зовнішньополітичної діяльності держави. Підкреслено, що основою кібердипломатії є формат побудови кібердіалогу. Визначено співвідношення категоріально-понятійного апарату між кібердипломатією та цифровою дипломатією. Акцентовано, що технології штучного інтелекту є ключовим елементом сучасної кібердипломатії, а її важливою складовою – кібернорми. Здійснено порівняння змісту понять «кібердипломатія» та «кібербезпека». Актуалізовано значення кібердипломатії у питаннях запобігання та протидії кіберінцидентам та під час проведення оцінки ландшафту кіберзагроз. Узагальнено напрями використання використання кібердипломатії у питаннях розробки основ національних політик кібербезпеки. Підсумовано, що кібердипломатія є важливим напрямком діяльності міжнародних організацій. Узагальнено, що практична складова частина кібердипломатії передбачає узгодження та досягнення зовнішньополітичних інтересів за участю кожної окремо узятій держави, формування єдиного та виваженого підходу у питаннях забезпечення міжнародної кібербезпеки. Деталізовано, що у рамках розбудови кібердипломатії міжнародна співпраця включає кооперацію між урядами держав, обмін інформацією про кіберзагрози, проведення спільного розслідування кіберзлочинів і кримінального переслідування кіберзлочинців. Розкрито інструментарій ЄС та його особливості у питаннях кібердипломатії. Визначено роль, значення та подальші напрями розбудови української кібердипломатії в умовах війни. Обґрунтовано подальші шляхи удосконалення кібердипломатії та удосконалення її нормативно-правового регулювання як важливої складової частини міжнародно-правової співпраці у сфері кібербезпеки.

Ключові слова: кібердипломатія, цифрова дипломатія, кібербезпека, кіберінциденти, кіберзагроза, кібератака, кіберпростір, кібердіалог, правовий режим воєнного стану, кібервійна, зовнішньополітичні інтереси, зловмисна кібердіяльність, Європейський Союз, США.

Polyakov Oleksandr. Cyber diplomacy as an important direction of international legal cooperation in the conditions of the regime of martial state

This article defines the principles of international cooperation in the field of cybersecurity. The role of Ukraine as an active subject of the global security system in the context of the Russian military threat is emphasized. The concept and content of cyber diplomacy are detailed. The goal and objectives of cyber diplomacy as an important component of the state's foreign policy are revealed. It is emphasized that the basis of cyber diplomacy is the format of building a cyberdialogue. The correlation of the categorical and conceptual apparatus between cyber diplomacy and digital diplomacy is determined. It is emphasized that artificial intelligence technologies are a key element of modern cyber diplomacy, and its important component is cyber norms. The content of "cyber diplomacy" and "cybersecurity" is compared. The importance of cyber diplomacy in preventing and countering cyber incidents and when assessing the cyber threat landscape is highlighted. The directions of using cyber diplomacy in the development of the foundations of national cybersecurity policies are summarized. It is concluded that cyber diplomacy is an important area of activity of international organizations. It is summarized that the practical component of cyber diplomacy involves the coordination and achievement of foreign policy

interests with the participation of each individual state, the formation of a unified and balanced approach to ensuring international cybersecurity. It is detailed that within the framework of the development of cyber diplomacy, international cooperation includes cooperation between governments of states, the exchange of information about cyber threats, the joint investigation of cybercrimes and the criminal prosecution of cyber criminals. The EU's tools and its features in cyber diplomacy are revealed. The role, significance and further directions of the development of Ukrainian cyber diplomacy in wartime are determined. Further ways to improve cyber diplomacy and improve its regulatory and legal regulation as an important component of international legal cooperation in the field of cybersecurity are substantiated.

Key words: *cyber diplomacy, digital diplomacy, cybersecurity, cyber incidents, cyber threat, cyberattack, cyberspace, cyber dialogue, martial law regime, cyberwar, foreign policy interests, malicious cyber activity, European Union, USA.*

Постановка проблеми. В умовах правового режиму воєнного стану питання посилення міжнародно-правової співпраці у сфері кібербезпеки набувають неабиякої актуальності. Підтримка України у кібернетичній сфері з боку наших партнерів та союзників, спільні та консолідовані зусилля є вагомим чинником виживання нашої держави в умовах потужної військової російської агресії, запорукою стабільності та гарантування сталої життєдіяльності як держави в цілому, її провідних інституцій, так і громадянського суспільства й приватного сектора економіки.

Україна була і залишається активним суб'єктом глобальної системи безпеки, пріоритетами для якої залишаються динамічний розвиток міжнародного партнерства й співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у цій сфері, що відповідає національним інтересам України, поглиблення співпраці з державами-членами ЄС та Північноатлантичного альянсу (НАТО) з метою підвищення національних спроможностей у сфері кібербезпеки, участь у заходах зі зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ та інших міжнародних структур. Україна реалізує стратегічні наративи та формує концептуальні засади за активної участі міжнародних партнерів щодо розвитку взаємної паритетної довіри та спільної відповіді на кібератаки, розробляє та реалізує сценарії подолання кризових ситуацій у сфері кібербезпеки: налагоджено обмін інформацією про кібератаки та кіберінциденти, проводяться регулярні кібернавчання та тренінги тощо. Попри війну, Україна забезпечує активну участь у конструктивному діалозі в рамках функціональної діяльності з ЄС та США, міжнародними організаціями

з метою спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Дієве міжнародне співробітництво у сфері забезпечення кібербезпеки та системної боротьби з кіберзагрозами триває на перманентній основі, набуває нових форматів, включаючи обмін досвідом та кращими практиками, проведення спільних навчань і тренувань, посилений захист державних інформаційних ресурсів, об'єктів критичної інфраструктури. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також із міжнародними організаціями, які проводять боротьбу із транснаціональною кіберзлочинністю. Окрім того, міжнародна взаємодія охоплює широке коло питань нормотворчого, методологічного, практичного, наукового і навчально-виховного спрямування.

У контексті зазначеного набувають актуальності питання кібердипломатії (cyber diplomacy) [1] та її розвитку як важливої складової частини міжнародно-правового співробітництва у сфері кібербезпеки, особливо в умовах війни. Загальновідомо, що кібердипломатія являє собою відносно новий термін, який включає спектр питань використання інформаційно-комунікаційних технологій для досягнення зовнішньополітичних цілей держави, окреслює наявні проблеми у сфері міжнародних відносин, які виникають у зв'язку із масштабуванням цифровізації. Визначення «кібердипломатія» використовується для опису застосування дипломатичних методів і переговорів у міжнародних відносинах, які стосуються питань, пов'язаних із забезпеченням безпеки у кіберпросторі.

Водночас кібердипломатія передбачає використання зовнішньополітичних зусиль і дипломатичних функцій для захисту національних інтересів у кіберпросторі, включає в себе питання забезпечення міжнародної та національної кібербезпеки, боротьби з транснаціональною кіберзлочинністю, заходи, які вживаються з метою зміцнення довіри, свободи та управління Інтернетом без прив'язки до державних кордонів. Кібердипломатія має вирішальне значення для боротьби з небезпеками у кіберпросторі, сприяє посиленню кібербезпеки та є чинником посилення захисту національних інтересів та зміцнення взаємної довіри між державами у цифровій сфері шляхом використання можливостей і зменшення загроз.

Стан дослідження. Міжнародно-правове співробітництво у сфері забезпечення кібербезпеки, його зміст, форми та особливості перебували у фокусі уваги таких вітчизняних науковців: Д. Дубова, А. Копиці, Р. Лук'янчука, М. Сливки, Т. Станіславського, М. Тетевіна, В. Шемчука, В. Фурашева та інших. У зарубіжній науковій літературі ці питання досліджували М. Абасі, Ф. Ланселот, А. Мухсін, П. Раданлієв. Проте кібердипломатію як важливу складову частину міжнародно-правового співробітництва у сфері забезпечення кібербезпеки в умовах війни жоден із вказаних науковців не розглядав, що посилює актуальність обраного тематичного наукового напрямку. За таких умов висвітлення кібердипломатії та шляхів її нормативного удосконалення як важливої складової частини міжнародно-правового співробітництва в умовах правового режиму воєнного стану є актуальним та своєчасним, та заслуговує на увагу.

Метою статті є визначення ролі та місця української кібердипломатії як важливої складової частини міжнародно-правового співробітництва в умовах війни, окреслення подальших шляхів її нормативно-правового забезпечення та удосконалення.

Виклад основного матеріалу дослідження. Міжнародне співробітництво має вирішальне значення для розробки політики, спрямованої на вирішення проблем, пов'язаних з управлінням Інтернетом, таких як системи доменних імен, розподіл Інтернет-протоколів і мережевий нейтралітет.

Уряди та дипломати використовують цифрові технології, соціальні медіа та онлайн-платформи для взаємодії з міжнародною аудиторією, обміну інформацією та здійснення дипломатичних контактів. Пряме спілкування стало можливим завдяки цифровій дипломатії, яка також заохочує до більшої відкритості в зовнішньополітичних відносинах. Використання соціальних медіа та онлайн-платформ для впливу на громадську думку та втручання у внутрішні справи будь-якої країни потрапляє під пильне дипломатичне спостереження.

Кібердипломатія зазвичай застосовується для подолання ускладнень та проблемних питань у сфері забезпечення кібербезпеки і спрямовується на забезпечення стабільності та безпечності у кіберпросторі. У сучасних реаліях не можна обійтися без використання важелів кібердипломатії у питаннях розробки національної політики кібербезпеки щодо держав-ворогів (РФ, КНДР, Білорусь, Іран), які можуть застосовувати алгоритми когнітивного ефекту, складні тактики соціальної інженерії, створювати стійкі кіберзагрози. Це вимагає від міжнародної спільноти покладання на кібердипломатію з метою пом'якшення загроз і викликів у кіберпросторі. Саме тому провідні держави світу активно співпрацюють для розробки кіберстандартів, які мають підтримувати безпечне та захищене онлайн-середовище.

Основою кібердипломатії є формат кібердіалогу, який проводиться за допомогою дипломатичних засобів та слугує майданчиком для спілкування між націями, обговорення вирішення конфліктів, завдяки чому світова спільнота намагається запобігти переростанню конфліктів у кіберпросторі у більшій геополітичній проблемі та навіть у кібервійну. Кібердипломатія має на меті вирішити проблему атрибуції шляхом створення організаційно-правових механізмів з метою притягнення до відповідальності винних у злочинній діяльності у кіберпросторі. Для ефективної боротьби з кіберзагрозами світова кібердипломатія сприяє консолідованій співпраці між урядами держав та приватним сектором. Водночас кібердипломатія спрямована на створення паритетного балансу між правами особи в кіберпросторі та національною безпекою [2, с. 245].

У сучасних умовах технології штучного інтелекту стають ключовим елементом кібердипломатії, впливаючи на різні аспекти – від виявлення кіберзагроз до ініціювання та проведення міжнародних переговорів. Здатність штучного інтелекту швидко аналізувати величезні масиви даних є важливою для виявлення потенційних кіберзагроз, що сприяє дипломатичним зусиллям у сфері забезпечення кібербезпеки. Починаючи з 2024 року особливу увагу з боку світової спільноти приділено злочинному використанню технологій штучного інтелекту, які постійно й активно застосовуються під час проведення масштабних кібератак хакерами та зловмисниками.

Кібердипломатія тісно пов'язана з кібербезпекою, але ці дві функції принципово відрізняються [3]. Кібербезпека запобігає несанкціонованому доступу, злому інформаційно-комунікаційних та комп'ютерних систем, сприяє запобіганню крадіжкам інформації та несанкціонованому доступу до баз даних тощо. З метою захисту даних і обмеження збоїв у кіберпросторі використовуються різні стратегії та технології кібербезпеки. Тоді як кібербезпека зосереджується на технічних і операційних аспектах захисту цифрових систем, кібердипломатія має справу з дипломатичними наслідками управління кіберзагрозами.

Ще одне поняття, яке тісно пов'язане із кібердипломатією, — це цифрова дипломатія [4], проте їхні функції є досить різними. Цифрова дипломатія, яка ще має назву «електронна дипломатія», або «дипломатія 2.0», використовує соціальні медіа урядів і дипломатів, онлайн-платформи та цифрові технології для взаємодії із міжнародною аудиторією, сприяння комунікації та здійснення дипломатичного контакту. Тобто цифрова дипломатія — це ширше поняття, яке включає технології, які використовуються для досягнення дипломатичних цілей, тоді як кібердипломатія зосереджена на питаннях вільного кіберпростору та забезпечення його безпеки.

Важливою складовою частиною поняття та змісту кібердипломатії є кібернорми. Кібернорми — це встановлені правила поведінки та керівні принципи, які спрямовують дії урядів держав світу у кіберпросторі. За таких умов кібердипломатія

має вирішальне значення для просування та узгодження цих стандартів між урядами цивілізованих держав світу [5, с. 43]. Національні уряди держав відіграють важливу та вирішальну роль у кібердипломатії, докладаючи зусиль для обговорення та визначення заходів у сфері боротьби з кіберзагрозами, домовляються про укладання та виконання відповідних договорів (угод, меморандумів), розробляють кібернорми та заохочують країни світу до відповідальної кіберповедінки. Держави як суб'єкти міжнародного права формують кіберплани та розробляють концепти політики кібербезпеки, обговорюють таку проблематику з іншими країнами або союзами держав. Зокрема, дипломатичні корпуси представляють свої уряди на міжнародних форумах та в Інтернет-розмовах, беруть участь в форумах та дискусіях, пов'язаних з кібернетичною безпекою, розвивають контакти з іншими країнами та відстоюють інтереси своєї країни.

Останнім часом спостерігається активна участь у кібердипломатії з боку ООН, США та ЄС. У 2022 році Державний департамент США оприлюднив новий звіт «Міжнародні норми поведінки держави в кіберпросторі» [6], Генеральна Асамблея ООН ухвалила резолюцію «Принципи відповідальної поведінки держав у кіберпросторі» [7], а у 2024 році в ЄС набула чинності нова Стратегія кібербезпеки [8]. З 2023 року ЄС та США відновили конструктивний діалог з кібербезпеки у рамках виконання спільного плану з метою зміцнення співпраці та реалізації дієвого механізму реагування на кіберзагрози та кіберінциденти в усьому світі, розвитку технічного співробітництва у питаннях кібербезпеки [9]. Також кібердипломатія є важливим напрямком діяльності міжнародних організацій, таких як Міжнародний союз електрозв'язку (МСЕ), Організація економічного співробітництва та розвитку (ОЕСР), Міжрегіональний науково-дослідний інститут ООН з питань злочинності та правосуддя (UNICRI), Управління ООН з наркотиків і злочинності (UNODC) тощо. Усі суб'єкти кібердипломатії сприяють переговорним процесам та ініціативам щодо розробки та запровадження кібернетичних норм. Як переконливо засвідчує передовий світовий досвід, кібердиплома-

тія була і залишається акселератором геополітичного прогресу, запорукою формування безпечного кіберпростору.

Здійснюючи обмін інформацією та співпрацюючи під час надзвичайних кіберситуацій, держави як повноправні суб'єкти міжнародного права повинні визнавати та поважати проблеми суверенітету та конфіденційності кожної країни окремо, що має відповідати практиці обміну інформацією відповідно до національного законодавства тієї чи іншої держави. За таких умов розробка міжнародних стандартів має вирішальне значення для забезпечення єдиного та узгодженого підходу до питань забезпечення кібербезпеки на рівні усіх держав. Міжнародна стандартизація забезпечує плідну співпрацю, обмін інформацією та взаємну підтримку під час кібернетичних криз, визначаючи єдині принципи, найкращі практики та відповідні правові рамки.

У рамках розбудови кібердипломатії міжнародна співпраця включає кооперацію між урядами держав, обмін інформацією про кіберзагрози, проведення спільного розслідування кіберзлочинів, подальшого кримінального переслідування кіберзлочинців та хакерів у всіх юрисдикціях. Практична складова частина кібердипломатії передбачає узгодження та досягнення зовнішньополітичних інтересів за участю кожної окремої держави, формування єдиного та виваженого підходу у питаннях забезпечення міжнародної кібербезпеки та її складників, системної боротьби з кіберзлочинністю, для чого розробляються відповідні механізми.

Так, наприклад, інструментарій ЄС з кібердипломатії – це спільна дипломатична відповідь на зловмисну кібердіяльність, яка сприяє пом'якшенню загроз кібербезпеці та побудові стабільних міжнародних відносин, що певним чином впливає на політичну поведінку потенційних держав-агресорів. Дипломатична реакція ЄС на зловмисну кібердіяльність пропорційна масштабу, тривалості, інтенсивності, складності кожної протиправної кіберактивності. 14 березня 2017 році Європейська служба зовнішніх справ та Європейська комісія представили документ, у якому встановлено дипломатичні обмежувальні заходи в рамках реалізації

спільної зовнішньої та безпекової політики [10]. У контексті викладеного заслуговує на увагу думка Р. Черниша про те, що на теренах ЄС зміст поняття «кібернетична дипломатія» передбачає інструментарій для запобігання кібернетичним нападам та реагування на такі атаки, якщо вони скоєні проти ЄС, у таких сферах, як стійкість мереж постачання, критично важлива інфраструктура та послуги, демократичні процедури та діяльність державних інституцій, економічна безпека тощо [11, с. 119].

В умовах, коли російські хакери постійно шукають нових підходів для проникнення в інформаційні системи, намагаються отримати доступ до державних інформаційних ресурсів, для України питання розбудови кібердипломатії є важливими та такими, що потребують свого логічного розвитку. У положеннях Стратегії зовнішньополітичної діяльності України [12] задекларовано, що оптимальним форматом кібердипломатії було визначено саме кібердіалог між Україною та ЄС і США, міжнародними організаціями з метою побудови паритетної співпраці, надання нашій державі підтримки та сприяння, обміну досвідом, спільного проведення оцінки ландшафту кіберзагроз в умовах військової російської загрози. 18 квітня 2023 року було оприлюднено План дій з реалізації Стратегії зовнішньополітичної діяльності України [13], у якому чітко простежується причинно-наслідковий зв'язок між зовнішньою політикою України та питаннями забезпечення кібербезпеки, підтверджується необхідність проведення кібердіалогу із партнерами, зокрема ЄС та США. У липні 2023 року на засіданні Національного координаційного центру кібербезпеки при РНБО України [14] було ухвалено рішення щодо необхідності розробки плану заходів у сфері кібердипломатії за участю Міністерства закордонних справ України.

За таких умов саме кібердипломатія є вагомим інструментом розвитку зовнішньополітичної діяльності провідних держав світу, а з огляду на геополітичний контекст розвиток української кібердипломатії вимагає систематичних та стратегічних зусиль не лише задля посилення діалогу у сфері цифровізації, а й розбудови безпекового партнерства на європейському та міжнародному рівнях. Оскільки державну політику

у сфері кібердипломатії в Україні формує та реалізує Міністерство закордонних справ, то необхідне проведення чіткого розподілу обов'язків між державними органами у цій площині, прискорення та схвалення на державному рівні стратегії кібердипломатії з метою просування геополітичних інтересів України у світі, визначення завдання, географічних та тематичних пріоритетів зовнішньої політики, деталізації шляхів побудови ефективного та взаємовигідного партнерства у рамках співпраці з ЄС та НАТО на підставі кращих практик міжнародного та вітчизняного досвіду.

Висновки. У світових масштабах кібердипломатія асоціюється з використанням дипломатичних ресурсів з метою захисту національних інтересів у кіберпросторі, комплексного обговорення на міжнародному та міждержавному рівнях проблемних питань у цій сфері. Кібердипломатія була і залишається акселератором міжнародного геополітичного прогресу, важливим інструментом забезпечення безпечного кіберпростору. Для України

кібердипломатія залишається важливим напрямком міжнародно-правового співробітництва, який потребує динамічного розвитку та відповідного законодавчого забезпечення. Саме кібердипломатія має бути адекватно інтегрована в діяльність дипломатичних представництв України за кордоном як окремий стратегічний напрям. З огляду на викладене у рамках розбудови організаційно-правових засад вітчизняної кібердипломатії та уніфікації категоріально-понятійного визначення у чинному законодавстві потребує прискорення схвалення законопроект «Про внесення змін до Закону України «Про дипломатичну службу» щодо вдосконалення проходження дипломатичної служби» від 22.12.2023 року № 10370 [15]. Водночас вважаємо за доцільне прискорення схвалення на державному рівні стратегії кібердипломатії, яка має визначити пріоритети подальшої співпраці між державами, засади обміну кращими практиками міжнародного та національного досвіду у сфері кібербезпеки.

ЛІТЕРАТУРА:

1. Cyberdiplomacy. URL: <https://cyberdiplomacy.disarmamenteducation.org/home>.
2. Lancelot J.F. Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*. 2020. Vol. 4. P. 240–254.
3. Cyber diplomacy and cybersecurity: guardians of the digital realm. URL: <https://www.ie.edu/uncover-ie/cyber-diplomacy-and-cybersecurity-guardians-of-the-digital-realm>.
4. Digital diplomacy: Where tech meets international relations. URL: <https://www.ie.edu/uncover-ie/digital-diplomacy-where-tech-meets-international-relations>.
5. Radanliev P. Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*. 2024. Vol. 1. P. 1–51.
6. US Department of State. Bureau of cyberspace and digital policy – United States Department of State. URL: <https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy>.
7. United Nations. The UN norms of responsible state behaviour in cyberspace. URL: <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>.
8. Regulation 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302841.
9. EU-US Joint Statement on CyberSafe Products Action Plan. URL: <https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan>.
10. The Cyber Diplomacy Toolbox. URL: <https://www.cyber-diplomacy-toolbox.com>.
11. Черниш Р.Ф. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального судочинства*. 2021. № 3–4. С. 112–121.
12. Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року «Про Стратегію зовнішньополітичної діяльності України»: Указ Президента України від 26 серпня 2021 року № 448/2021. URL: <https://www.president.gov.ua/documents/4482021-40017>.

13. Про затвердження плану дій з реалізації Стратегії зовнішньополітичної діяльності України : Розпорядження Кабінету Міністрів України від 18 квітня 2023 року № 327. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-dii-z-realizatsii-stratehii-zovnishnopolitychnoi-diialnosti-ukrainy-327r-180423>.

14. На засіданні НКЦК обговорено питання щодо розбудови кібердипломатії та стану виконання Стратегії кібербезпеки України. URL: <https://www.rnbo.gov.ua/ua/Diialnist/6522.html>.

15. Про внесення змін до Закону України «Про дипломатичну службу» щодо вдосконалення проходження дипломатичної служби : Проект Закону України від 22 грудня 2023 року № 10370. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/43445>.