https://doi.org/10.31891/2307-5740-2024-334-7
УДК 341.232

ДРИГА Дмитро
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/ 0000-0003-4426-7551
e-mail: dimadriga6@gmail.com

АНАЛІЗ ПРАВОВИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Стаття присвячена аналізу міжнародного досвіду у сфері забезпечення інформаційної безпеки, зокрема діяльності таких міжнародних організацій, як ООН, Рада Європи та Європейський Союз. Розглянуто законодавчі акти та резолюції, що регулюють питання інформаційної безпеки, кіберзлочинності та захисту прав людини в інформаційному просторі.

Основну увагу приділено розвитку правових механізмів та нормативно-правового регулювання в межах ЄС, включно з Директивою NIS та її оновленням NIS 2, які визначають стандарти кібербезпеки для країн-членів. Окремо висвітлено питання інтеграції міжнародних норм у національне законодавство окремих держав.

Окремо акцентовано на важливості Загальної декларації прав людини (1948) і Конвенції про захист прав людини та основоположних свобод (1950) для формування міжнародного правового регулювання інформаційної безпеки. Стаття охоплює аналіз міжнародних правових документів, спрямованих на боротьбу з кіберзлочинністю, включаючи Конвенцію Ради Європи про злочини у сфері комп'ютерної інформації та Директиву ЄС 2016/1148. Описані сучасні ініціативи та заходи ЄС у галузі кібербезпеки, зокрема запровадження Директиви NIS 2, яка встановлює суворі вимоги до забезпечення мережевої безпеки та взаємодії держав-членів.

Визначено, що основні принципи законодавчого регулювання суспільних відносин у сфері інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їх аналіз, є загальновизнаними та пріоритетними у розвитку інформаційного законодавства для України.

Ключові слова: інформація, інформаційна безпека, інформаційна інфраструктура, національна безпеки, інформаційні загрози, інформаційні системи, Інтернет, Європейський Союз (ЄС), Організація Об'єднаних Націй (ООН), Рада Європи.

DRYHA Dmytro
Open International University of Human Development "Ukraine"

ANALYSIS OF LEGAL MECHANISMS ENSURING INFORMATION SECURITY OF THE INFORMATION INFRASTRUCTURE OF THE EUROPEAN UNION

The article is devoted to the analysis of international experience in the field of ensuring information security, in particular the activities of such international organizations as the UN, the Council of Europe and the European Union. Legislative acts and resolutions regulating issues of information security, cybercrime and protection of human rights in the information space were considered.

The main focus is on the development of legal regulation within the EU, including the NIS Directive and its update NIS 2, which define cybersecurity standards for member states. The issue of integration of international norms into the national legislation of individual states is highlighted separately.

Special emphasis is placed on the importance of the Universal Declaration of Human Rights (1948) and the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) for the formation of international legal regulation of information security. The article covers the analysis of international legal documents aimed at combating cybercrime, including the Council of Europe Convention on Computer Information Crime and EU Directive 2016/1148. Modern initiatives and measures of the EU in the field of cyber security are described, in particular, the introduction of the NIS 2 Directive, which establishes strict requirements for ensuring network security and interaction of member states.

Global challenges related to information security are highlighted, including the growth of cybercrime - cybercriminals use increasingly sophisticated methods to attack government institutions, businesses, and critical infrastructure, which calls for increased international cooperation.

It was determined that the main principles of legislative regulation of social relations in the field of information security are formulated in the main international documents and, as their analysis shows, are generally recognized and prioritized in the development of information legislation for Ukraine.

Key words: information, information security, information infrastructure, national security, information threats, information systems, Internet, European Union (EU), United Nations (UN), Council of Europe.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інформаційна безпека є однією з ключових складових сучасного суспільства, особливо у контексті цифрової трансформації та зростаючої залежності від інформаційних технологій. Європейський Союз, як один із найбільших регіональних акторів на світовій арені, стикається з численними викликами в галузі захисту своєї інформаційної інфраструктури від кіберзагроз, кібертероризму та інших видів неправомірних дій. Сучасні загрози інформаційній безпеці вимагають не лише технічних рішень, але й ефективних правових механізмів регулювання, які здатні забезпечити стійкість і захищеність інформаційних систем.

Водночас, не всі аспекти правового регулювання цієї сфери достатньо розроблені, що ускладнює їхнє впровадження та адаптацію до стрімких технологічних змін. Відсутність єдиної стратегії та координації

зусиль на рівні держав-членів ЄС часто стає причиною розрізненості в підходах до забезпечення інформаційної безпеки, що створює вразливості для інформаційної інфраструктури всього регіону.

Проблема полягає в необхідності оцінки існуючих правових механізмів ЄС, виявлення їхніх недоліків і прогалин, а також розробки рекомендацій щодо вдосконалення законодавчої бази для гарантування більш ефективного захисту інформаційної інфраструктури на загальноєвропейському рівні.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У дослідженнях, що проводились провідними науковцями, розглядаюся питання присвячені аналізу правових механізмів у ЄС у сфері інформаційної безпеки та їх ключовим документам. Серед цих дослідників можна виділити праці: Лісовського П.М., Лісовської Ю.П., Ярового Т.С. Основну базу нашого дослідження становлять нормативні акти та міжнародні документи ЄС та ООН: Директиви, Конвенції, резолюції тощо.

Вчені, зокрема, звертають увагу на фрагментацію правових норм у державах-членах ЄС і складнощі в координації на рівні ЄС.

Таким чином, попередні дослідження закладають основу для подальшого аналізу правових механізмів інформаційної безпеки в ЄС, проте залишаються деякі нерозв'язані питання, що вимагають додаткового вивчення.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Досліджена тематика є досить актуальною, попри наявність низки міжнародних угод та ініціатив, залишається питання, як покращити міжнародну правову співпрацю у сфері забезпечення інформаційної безпеки, особливо в умовах глобальної взаємозалежності інформаційних систем.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета дослідження полягає у тому, щоб надати комплексний огляд і аналіз правових механізмів ЄС у сфері інформаційної безпеки, а також запропонувати шляхи їх удосконалення для підвищення ефективності захисту інформаційної інфраструктури.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Нині відбуваються активні процеси формування міжнародного досвіду у сфері забезпечення інформаційної безпеки, у рамках діяльності таких міжнародних організацій, як: ООН, Рада Європи, ЄС та інших.

Європейський Союз висловлює занепокоєння у зв'язку з інцидентами, що стосуються важливих безпекових питань, які відбуваються у світі та становлять серйозну загрозу для функціонування мережевих та інформаційних систем, перешкоджають економічній діяльності, а також спричиняють значні фінансові втрати [15].

Основні принципи законодавчого регулювання суспільних відносин у сфері інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їх аналіз, є загальновизнаними та пріоритетними у розвитку інформаційного законодавства для України [17].

Найважливішим кроком для розвитку законодавства як в інформаційній сфері в цілому, так і в галузі забезпечення інформаційної безпеки було прийняття та проголошення 10 грудня 1948 р. Генеральною асамблеєю ООН Загальної 9 декларації прав людини [14], у статтях 12, 19, 26 якої встановлено право кожної людини на свободу переконань, думки, совісті, релігії, право на освіту, а також право на вільне вираження цих переконань та право шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами, незалежно від державних кордонів.

Положення, що закріплюють інформаційні права та свободи, були розвинені в Конвенції Ради Європи про захист прав людини та основоположних свобод [16] 1950 року та Міжнародного пакту про громадянські та політичні права [18] 1966 року. У зазначених актах встановлено, що свобода отримання та розповсюдження інформації реалізується без будь-якого втручання з боку державних органів, незалежно від державних кордонів та поширюється на будь-яку інформацію (стаття 10 Конвенції, стаття 19 Міжнародного пакту). Таким чином, право на свободу інформації в тому вигляді, в якому воно закріплене в міжнародних документах з прав людини, не є новим суб'єктивним правом людини в галузі інформації, а проявом традиційних свобод думки та слова. Фактично вплив поглядів на свободі як втілення інформаційних прав громадян позначилося становленні принципу свободи інформації [18].

Питання інформаційної безпеки неодноразово обговорювалися на засіданнях Ради Європи. Зокрема, було прийнято перелік документів у цій галузі: Рекомендація Ради Європи № R (87), що регламентує забезпечення безпеки персональних даних; керівний документ - Рекомендація Ради Європи № R (89) про комп'ютерні злочини, що визначає перелік комп'ютерних злочинів і не тільки; у 1995 р. дві Рекомендації Ради Європи у сфері інформаційних технологій: Рекомендація Ради Європи № R (95) про захист

персональних даних у сфері телекомунікаційних послуг та Рекомендація Ради Європи № R (95) щодо кримінального процесу, пов'язаного з інформаційними технологіями.

Ідея забезпечення міжнародної інформаційної безпеки вперше отримала практичну реалізацію в Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» від 4 грудня 1998 р. Цей документ започаткував спільне обговорення питань створення абсолютно нового міжнародно-правового режиму, структурним елементом якого в перспективі стали інформація, інформаційна технологія і методи її використання [11].

Резолюція Генеральної Асамблеї ООН A/RES/54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 1 грудня 1999 р. вперше вказала на загрози міжнародній безпеці інформаційного простору стосовно не лише до цивільної, а також до військової сфери [12].

Розробка проєкту конвенції про злочини у сфері комп'ютерної інформації тривала з 1996 р. до 2001 р., в якому і була прийнята. У рамках виконання цієї Конвенції Європейським комітетом з проблем злочинів створено структуру, функціями якої є запобігання та боротьба з кіберзлочинами. Інформаційні технології, проникаючи у всі сфери суспільства, створюють точки напруженості та вразливості, що використовуються для кіберзлочинів. У лютому 1997 р. Комітетом міністрів Ради Європи засновано Комітет експертів зі злочинів у кіберпросторі. У 2000 р. на 50 пленарну сесію Комітету було представлено переглянутий варіант Конвенції, в якій регламентувалися обов'язкові міжнародно-правові норми у сфері інформаційної безпеки.

Таким чином, можна відзначити, що Рада Європи здійснювала розробку та систематизацію правового регулювання з 1987 р. У 2001 р. Рада Європи схвалила Конвенцію про злочинність у сфері комп'ютерної інформації, до якої приєдналося понад 30 держав (що стосується росії, то вона не є учасницею зазначеної Конвенції). У ній передбачено наступний правовий механізм міжнародного співробітництва та дотримання принципів міжнародного права з метою протидії кіберзлочинності: заборона протиправного використання інформаційних технологій та комп'ютерних засобів, поширення шкідливого інформаційного змісту; взаємодія правоохоронних органів у сфері здійснення процесуальних дій; обов'язок надання допомоги у сфері судових розглядів та розслідування комп'ютерних злочинів; заборона на здійснення соціально небезпечних діянь, таких як порушення доступності та цілісності комп'ютерної інформації та систем; порушення авторських та суміжних прав [3].

Конвенція містить пропозиції до держав-учасниць щодо включення норм матеріального кримінального права до національного законодавства, що передбачають кримінальну відповідальність за низку дій, що носили злочинний характер.

Конвенція про злочини у сфері комп'ютерної інформації пропонувала об'єднати зусилля міжнародного співтовариства у боротьбі з кіберзлочинами, що мають транскордонний характер та уніфікувати законодавство у цій сфері. Як передбачалося, це має спростити боротьбу з комп'ютерними злочинами та полегшити взаємодію органів державної влади для притягнення винних осіб до відповідальності.

У Директиві ЄС 2016/1148 зазначається, що наявних можливостей недостатньо для забезпечення високого рівня безпеки мережевих та інформаційних систем у Союзі. Держави-члени мають дуже різні технологічні рівні, що призводить до роздроблених підходів у рамках Союзу, до нерівного рівня захисту споживачів та підприємств та підриває загальний рівень безпеки мережевих та інформаційних систем. Крім того, відсутність загальних вимог до операторів основних послуг та постачальників цифрових послуг унеможливлює створення глобального та ефективного механізму міжнародного співробітництва в даній сфері.

2016 рік став важливим періодом у боротьбі з кіберзлочинністю. По-перше, було підписано Спільну декларацію між ЄС та НАТО, яка заклала основи їхньої співпраці. По-друге, Європейським парламентом та Радою Європи було прийнято Директиву з безпеки мережі та інформаційних систем (The Security of Network and Information Systems – NIS, далі - Директива NIS). У ній передбачено зобов'язання держав-учасниць ЄС розробити та прийняти національні стратегії безпеки мережевих та інформаційних систем для безперебійного функціонування внутрішнього ринку [4].

Як вказується в цій Директиві мережеві та інформаційні системи, а у першу чергу інтернет, відіграють важливу роль у сприянні транскордонному переміщенню товарів, послуг та людей, внаслідок чого суттєві порушення цих систем, чи це навмисні чи ненавмисні і незалежно від того, де вони відбуваються, можуть торкнутися окремих держав-членів та ЄС у цілому.

Положення Директиви NIS не застосовуються до підприємств, що надають мережі загального користування або загальнодоступні послуги електронного зв'язку, визначені Директивою 2002/21/ ЄС Європейського Парламенту та Ради Європи і підпадають під її регулювання, на них поширюються вимоги безпеки та цілісності, викладені в Директиві 2002/21 / ЄС. Положення Директиви NIS також не повинні застосовуватися до постачальників послуг довіри, відносини з якими регулюються Регламентом (ЄС) № 910/2014 Європейського Парламенту та Ради Європи [5].

Відповідно до ст. 346 Договору про функціонування Європейського Союзу жодна держава-член не зобов'язана надавати інформацію, розкриття якої, на думку держави, суперечить основним інтересам її

безпеки. У ньому також зазначено, що при визначенні відповідності вимог щодо безпеки мережевих та інформаційних систем та повідомлення про інциденти, що містяться у галузевих правових актах ЄС вимогам, що міститься в Директиві 95/46 / ЄС , слід враховувати ті положення, які відповідають правовим актам ЄС [2].

Крім того, у галузі правового регулювання безпеки мережевих інформаційних систем ЄС діє ст. 13 Рамкової директиви (2009/140 / ЕС), запроваджена у 2009 р. для забезпечення безпеки та цілісності мережі та доступності послуг електронних комунікацій [6].

Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148 (NIS 2) [13].

За допомогою NIS 2 (Network and Information Security – мережна та інформаційна безпека) ЄС запровадив суворі правила кібербезпеки для своїх країн-членів. NIS 2 є наступником Директиви NIS, яка набула чинності у 2016 році. Тому реалізація цілісної стратегії безпеки вже не тільки необхідна для захисту від кібератак, а й потрібна за законом. Держави-члени повинні вжити необхідних заходів для дотримання Директиви NIS 2 до 17 жовтня 2024 року та вживати цих заходів з 18 жовтня 2024 року.

NIS 2 - це покращена версія Директиви NIS 2016 року, яка вже була покликана забезпечити високий рівень безпеки мережевих та інформаційних систем у Союзі, але мала низку недоліків.

Директива NIS 2 – це директива ЄС, яка набула чинності 16 січня 2023 року та спрямована на підвищення кібербезпеки та стійкості критично важливих інфраструктур та постачальників цифрових послуг. Директива зобов'язує відповідні компанії та організації дотримуватися ефективного управління ризиками та повідомляти про серйозні або значні кіберінциденти компетентним національним органам, які потім можуть вжити необхідних заходів. Щоб звести до мінімуму потенційні збитки для користувачів, довкілля та громадського порядку, необхідно на ранніх стадіях виявляти прогалини в системі безпеки та вживати превентивних заходів щодо їх усунення. Для того, щоб усі учасники процесу дотримувалися однаково високих стандартів, компанії також несуть відповідальність за безпеку всього ланцюжка поставок і передають вимоги своїм діловим партнерам та постачальникам. Інші заходи включають, зокрема:

— застосування належних та пропорційних заходів безпеки, що відповідають сучасним стандартам та передовому досвіду, для забезпечення конфіденційності, цілісності, доступності та справжності своїх даних та послуг;

— створення та оновлення плану забезпечення безперервності бізнесу, що дає змогу відновити нормальні умови роботи після кіберінциденту;

— для запобігання несанкціонованого доступу вводиться багатофакторна автентифікація при доступі до своїх мереж та інформаційних систем [1].

Агентство ЄС з кібербезпеки (ENISA) відіграватиме ключову роль у моніторингу та підтримці застосування цих правових актів.

В галузі безпеки мобільних систем Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (англ. European Union Agency for Network and Information Security, ENISA) – провідна організація ЄС, відповідальна за проведення кібернавчань, визначила мінімальні вимоги до забезпечення кібербезпеки [10].

Заходи, що забезпечують безпеку з'єднання через встановлені точки відкритого доступу, визначені Рекомендацією № R (99) 14 про універсальні суспільні послуги щодо нових комунікативних і інформаційних послуг. В галузі електронних ідентифікаційних та довірчих послуг для здійснення електронних транзакцій на внутрішньому ринку (elDAS), був розроблений Регламент (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та замінив Директиву 1999/93/ЄС. У жовтні 2017 р. Європейська рада запропонувала Комісії ООН розробити пропозиції щодо забезпечення кібербезпеки [9].

У 2018 р. ЄС розробив загальну систему сертифікації інформаційних систем, яка забезпечує кібербезпеку та адекватний рівень надання продуктів та послуг інформаційно-комунікаційних технологій (далі-ІКТ). У тому ж році Європейська комісія запропонувала ухвалити закон про кібербезпеку , в якому передбачається вісім варіантів політики, що охоплюють ENISA про сертифікацію кібербезпеки інформаційно-комунікаційних технологій.

Для забезпечення інформаційної безпеки створюється європейська платформа сертифікації в галузі кібербезпеки продуктів та послуг у сфері ІКТ , яка визначає схеми сертифікації в цій галузі, що дозволяє цим продуктам та послугам бути визнаними у всіх державах-членах.

Крім того, ЄС створює єдину інформаційну інфраструктуру, яка забезпечить взаємодію таких інформаційних систем: в'їзду/виїзду (EES); візової інформаційної системи (VIS); Євродак - Шенгенської інформаційної системи (SIS) та Європейської системи збирання інформації про кримінальні злочини для громадян третіх країн (ECRIS - TCN), таким чином, щоб вони та їх дані доповнювали одна одну.

Для створення єдиної інформаційної інфраструктури як компоненти функціональної сумісності розробляються європейський пошуковий портал (ESP), спільно використовувана служба біометричного зіставлення (BMS), загальне резидентне сховище (CIR) та детектор множинного ідентифікатора (MID).

Упродовж чотирьох років країни-члени ЄС розробляють національне законодавство щодо регулювання інформаційної інфраструктури. Так, ФРН підтримує зусилля щодо узгодження методів застосування міжнародного законодавства при національному регулюванні використання ІКТ, у тому числі у разі розробки норм технічного регулювання, що застосовуються в добровільному порядку, правил (принципів) відповідальної поведінки держави, які спрямовані на створення відкритої, безпечної, стабільної , доступною та мирною ІКТ. Особливе значення у цьому контексті має робота груп урядових експертів з питань розвитку галузі створення та використання інформації та телекомунікацій.

Доречі ФРН брала активну участь у визначенні та здійсненні заходів зміцнення довіри, спрямованих на забезпечення безпеки в галузі державного використання ІКТ. Серед останніх національних заходів регулювання слід назвати прийняття у 2015 р. Закону « Про техніку безпеки» , переглянутого у листопаді 2016 р., Стратегії кібербезпеки та прийняття Урядом ФРН рішення про створення інституту міжнародної кібербезпеки з метою систематизації зусиль у цій галузі. Зусилля ФРН щодо інформації та телекомунікацій у контексті інформаційної безпеки є частиною інтенсивної роботи зі сприяння безпеці ІКТ .

Греція ратифікувала Конвенцію про злочини у сфері комп'ютерної інформації та Додатковий протокол до неї, що стосується криміналізації дій, пов'язаних з поширенням расової ворожнечі та інформації, що носить ксенофобський характер, вчинених за допомогою комп'ютерних систем [7].

Однак інтеграція Директиви ЄС з безпеки мережевих та інформаційних систем до національного законодавства Греції здійснювалася і до ратифікації зазначеної Конвенції. Згідно з інформацією, наданою Міністерством оборони Греції, на національному рівні були зроблені зусилля щодо зміцнення інформаційної безпеки та сприяння міжнародному співробітництву. Зокрема, розроблено Національну стратегію в галузі кібербезпеки Греції, у якій передбачені дії щодо підтримки мінімальних вимог кібербезпеки, яка є частиною планів національної оборони. Створено Центр операцій із кібербезпеки, функціями якого передбачено розробку мережевих систем національної військової оборони країни.

Таким чином можна відзначити, що в країнах ЄС розроблено та постійно вдосконалюються процедури реагування на безпекові інциденти (надзвичайні ситуації). Створюються групи швидкого реагування, які включаютьсяв роботу у найкоротші терміни, для усунення наслідків кібератак, здійснених у військових чи громадських мережах. Процедури відновлення при комп'ютерних збоях або кібератаках інтегровані у комп'ютерну інформаційну безпеку та політичні документи [8].

Взаємодія між інформаційними системами країнами-членами ЄС дозволяє узгоджувати вимоги до їх якості та забезпечення ефективного використання даних Європолу та баз даних Інтерполу шляхом полегшення доступу до них відповідних структур.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Формування правової основи єдиного інформаційного простору України тісно пов'язане з міжнародним та зарубіжним досвідом і має здійснюватися на основі принципу системності та збалансованості правових норм з урахуванням загальновизнаних принципів та норм міжнародного права. Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їх аналіз, є загальновизнаними та пріоритетними у розвитку інформаційного законодавства та для України.

На основі вивчення міжнародних правових актів, що стосуються протидії новим викликам та загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, очевидним є висновок про необхідність подальшої імплементації положень міжнародних правових актів та гармонізації законодавства держав. Лише використання скоординованих та взаємодоповнюючих заходів на двосторонньому, регіональному та міжнародному рівнях дозволить адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері. При цьому серед можливих напрямів співробітництва передбачається сприяння розробці міжнародної правової бази співробітництва та вироблення єдиного понятійного апарату у сфері забезпечення інформаційної безпеки.

Література

1. European Commission. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
2. Council framework decision 2005/222/JHA on attacks against information systems. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur - lex.europa.eu/legal - content/EN/TXT/?toc=0J:L:2016:194:T0C&uri=uriserv:0J.L_.2016.194.01.0001.01.ENG.
5. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common

regulatory framework for electronic communications networks and services (Framework Directive) OJ. L. 108. 24.4.2002. p. 33.

6. Directive 2009/140/EC of the European parliament and of the Council of 25 November 2009. URL: https://eur - lex.europa.eu/legal - content/EN/TXT/PDF/?uri=CELEX:32009L0140.
7. Greek National Cyber Security Strategy. URL: https://www.enisa.europa.eu/topics/national - cyber - security - strategies/ncss - map/strategies/national - cyber - security - strategy – greece.
8. Network and information security: proposal for a european policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
9. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ. L .257. 28.8.2014.P.73.
10. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.
11. Rezoljucija A/RES/53/70 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti». URL: https://undocs.org/ru/A/RES/53/70.
12. Rezoljucija A/RES/54/49 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti». URL: https://undocs.org/ru/A/RES/54/49.
13. The NIS 2 Directive. URL: https://www.nis-2-directive.com.
14. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. Неофіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
15. Загородня А. С., Кулик А. В. Фасилітація цифрової дипломатії у контексті політики та міжнародної інформаційної безпеки. Modern scientific journal (Сучасний науковий журнал). 2024. No1(3). С. 78-84. DOI: https://doi.org/10.36994/2786-9008-2024-3-10
16. Конвенція про захист прав людини і основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
17. Лісовський П.М., Лісовська Ю.П. Захист інформації: міжнародні відносини та політичний консалтинг: навч. посібник. К.: Видавництво Ліра-К, 2022. 312 с.
18. Міжнародний пакт про громадянські і політичні права. Ратифіковано Указом Президії Верховної Ради Української РСР N 2148-VIII (2148-08) від 19.10.73 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.

References

1. European Commission. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
2. Council framework decision 2005/222/JHA on attacks against information systems. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur - lex.europa.eu/legal - content/EN/TXT/?toc=0J:L:2016:194:T0C&uri=uriserv:0J.L_.2016.194.01.0001.01.ENG.
5. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ. L. 108. 24.4.2002. p. 33.
6. Directive 2009/140/EC of the European parliament and of the Council of 25 November 2009. URL: https://eur - lex.europa.eu/legal - content/EN/TXT/PDF/?uri=CELEX:32009L0140.
7. Greek National Cyber Security Strategy. URL: https://www.enisa.europa.eu/topics/national - cyber - security - strategies/ncss - map/strategies/national - cyber - security - strategy – greece.
8. Network and information security: proposal for a european policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
9. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ. L .257. 28.8.2014.P.73.
10. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.
11. Rezoljucija A/RES/53/70 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti». URL: https://undocs.org/ru/A/RES/53/70.
12. Rezoljucija A/RES/54/49 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti». URL: https://undocs.org/ru/A/RES/54/49.
13. The NIS 2 Directive. URL: https://www.nis-2-directive.com.
14. Universal Declaration of Human Rights. Adopted and proclaimed by resolution 217 A (III) of the UN General Assembly of December 10, 1948. Unofficial translation. URL: https://zakon.rada.gov.ua/laws/show/995 [in Ukrainian].
15. Zahorodnya , A. S., Kulyk, A. V. (2024). Facilitation of digital diplomacy in the context of politics and international information security. Modern scientific journal. No. 1(3). P. 78-84. DOI: https://doi.org/10.36994/2786-9008-2024-3-10 [in Ukrainian].
16. Convention on the Protection of Human Rights and Fundamental Freedoms. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].
17. Lisovskii, P.M., Lisovska, Yu.P. (2022). Information protection: international relations and political consulting: education. manual. K.: Lira-K Publishing House, 312 p. [in Ukrainian].
18. International Covenant on Civil and Political Rights. Ratified by Decree of the Presidium of the Verkhovna Rada of the Ukrainian SSR N 2148-VIII (2148-08) dated 19.10.73. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text [in Ukrainian].