УДК 342.951

КУЗНЄЦОВ О.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0001-9242-0835.

ЄВРОПЕЙСЬКИЙ ДОСВІД ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Анотація. *Здійснено огляд новел європейського законодавства у сфері забезпечення кібербезпеки. Узагальнено перспективи діджіталізації в ЄС. Розглянуто положення Стратегії кібербезпеки ЄС на 2021 – 2027 роки та Дорожньої карти "Цифровий компас". Визначено засади та пріоритети спільної європейської цифрової політики. Деталізовано стратегічні цілі та напрями успішної цифрової трансформації Європи до 2030 року. Розкрито організаційно-правовий механізм запровадження режиму кіберсанкцій в ЄС. Визначено шляхи співпраці між Україною та ЄС у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, кіберзагроза, діджиталізація, цифрові технології, режим кіберсанкцій, штучний інтелект.*

Summary. *The novelties of the European legislation in the sphere of cybersecurity are reviewed. Prospects for digitalization in the EU are summarized. The provisions of the EU Cyber Security Strategy for 2021 – 2027 and the Digital Compass Roadmap are considered. Basic principles and priorities of a common European digital policy are defined. The strategy targets and avenues for a successful digital transformation of Europe by 2030 are detailed. The organizational and legal mechanism for introducing the cyber sanctions regime in the EU has been revealed. The directions of the cooperation between Ukraine and EU in the sphere of cybersecurity are identified.*

Keywords: *cybersecurity, cyberattack, cyberthreat, digitalization, digital technologies, cyber sanctions regime, artificial intelligence.*

Аннотация. *Осуществлено рассмотрение новел европейского законодательства в сфере обеспечения кибербезопасности. Обобщены перспективы диджитализации в ЕС. Рассмотрены положения Стратегии кибербезопасности ЕС на 2021 – 2027 года и Дорожная карта "Цифровой компас". Определены основы и приоритеты совместной европейской цифровой политики. Детализированы стратегические цели и направления успешной цифровой трансформации Европы до 2030 года. Раскрыто организационно-правовой механизм внедрения режима киберсанкций в ЕС. Определены направления сотрудничества между Украиной и ЕС в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, киберугроза, диджитализация, цифровые технологии, режим киберсанкций, штучный интеллект.*

Постановка проблеми. Цифрові технології відкривають унікальні можливості для розвитку економіки та підвищення якості життя громадян. У сучасному світі більшість країн світу вимушені "на ходу" адаптувати своє законодавство та впроваджувати державне регулювання сфери інформаційних технологій, у тому числі й цифрових, враховуючи появу нових викликів щодо забезпечення захисту прав людини та безпеки держави. Сучасний світ постійно змінюється. Поширення популярності цифрової економіки як принципово нової моделі розвитку глобальної економічної системи постійно зростає, що провокує необхідність розробки дієвих механізмів забезпечення надійного та безпечного середовища її функціонування. Саме тому кібербезпека являє

собою стратегічну комплексну проблему яка, передусім, стосується економіки країни, особливо електронної промисловості, в тому числі питань розвитку інфраструктури електронних комунікацій, технологій кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, визначення заходів боротьби з кіберзлочинністю та кібертероризмом тощо.

Враховуючи сучасні тенденції розвитку пріоритетних засад спільної політики провідних країн ЄС за напрямом протидії загрозам у кіберпросторі, динаміку змін у внутрішній інформаційній політиці цих держав, спостерігається прагнення швидкого та адекватного реагування на нові виклики сучасності. Проте кібернетичні загрози формуються та розвиваються досить швидко, стають дедалі складнішими та більш адаптивними. Саме тому забезпечення кібернетичної безпеки та кіберстабільності відносяться до основних пріоритетів Єврокомісії у рамках реалізації програми цифрової трансформації ЄС. На цьому фоні важливим завданням залишається забезпечення стабільності комунікаційних мереж, заснованих на технологіях 5G, з якими ЄС пов'язує швидкий цифровий розвиток європейської економіки. Невипадково вказані пріоритети знайшли своє відображення у бюджеті ЄС на 2021 – 2027 роки.

Прагнення політичного керівництва держав світу зміцнювати та посилювати систему забезпечення кібербезпеки нерозривно пов'язано із реагуванням на реальні та потенційні загрози, що передбачає вдосконалення законодавства, визначення стратегічних засад подальшого розвитку у базових програмних документах та їх реалізації. Враховуючи прагнення України інтегруватися у європейський інформаційний простір, актуальним та своєчасним є огляд новел сучасного законодавства ЄС, зокрема оновленої Стратегії кібербезпеки, яка визначає поступальні та дієві кроки спільної європейської інформаційної політики з метою посилення спроможності держав-членів ЄС у сфері забезпечення кібербезпеки, захисту надбань цифрової економіки.

Результати аналізу наукових публікацій. Правове забезпечення кібербезпеки України та висвітлення шляхів його удосконалення були предметом досліджень А. Баранова, М. Василенка, В. Гавловського, М. Гуцалюка, О. Довганя, Д. Дубова, А. Марущака, М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева та інших вітчизняних науковців. Більш детально аналізу європейських законодавчих ініціатив у сфері забезпечення кібербезпеки приділяли свою увагу такі фахівці як: О. Балуєва, Є. Боєр, С. Вдовенко, І. Забара, Т. Сліпченко, Р. Лук'янчук тощо. Водночас, слід констатувати, що дослідження процесів забезпечення кібербезпеки як важливої складової фарватеру цифрової економіки та її складових в контексті розбудови засад сучасної європейської інформаційної політики детально не розглядалося, що посилює актуальність обраної теми наукового дослідження. Масштабні збитки цифрової економіки провокують потребу пошуку шляхів мінімізації збитків, у тому числі й шляхом посилення кібербезпеки.

Метою статті є висвітлення й узагальнення кращих практик європейського досвіду щодо побудови та удосконалення системної протидії кіберзагрозам в сучасних умовах, проведення огляду новел європейського законодавства у сфері забезпечення кібербезпеки, зокрема Стратегії ЄС у вказаній сфері та висвітлення базових напрямків дорожньої карти "Цифровий компас", оприлюдненої Єврокомісією 9 березня 2021 року.

Виклад основного матеріалу. Останнім часом зусилля європейської спільноти спрямовані на узгодження та розвиток безпекової політики у кіберпросторі. Результатом цих узгоджених дій стала підготовка та оприлюднення 16 грудня 2020 року оновленої Стратегії кібербезпеки ЄС [1], ключовими завданнями якої є підвищення стійкості життєво необхідних структур та системна протидія масштабним зовнішнім кібератакам.

Пріоритетом визначено посилення колективної безпеки у кіберпросторі, забезпечення рівної можливості для усіх громадян у ЄС та представників бізнесу щодо використання надійних цифрових послуг та інструментів у повсякденному житті. Усі електронні мережі, банки, транспорт, лікарні, державні органи мають бути гарантовано захищеними від кібернетичних загроз та будь-яких ризиків у цій площині. У зв'язку з цим Єврокомісія запропонувала створити мережу Центрів оперативної безпеки по усій території ЄС, які будуть діяти на основі впровадження технологій штучного інтелекту та нададуть змогу створити реальний "щит кібернетичної безпеки" для зони ЄС. Згідно із цим задумом, система має розпізнавати кібернетичні атаки на ранніх стадіях та пропонувати алгоритми дій, спрямованих на їх упередження, викриття та ліквідацію.

На виконання цих стратегічних планів важлива роль відводиться інституційному удосконаленню складових кібербезпеки та її безперебійному забезпеченню. Зокрема, очікується створення нової структури ЄС – "Об'єднаний кібернетичний відділ", який у рамках своїх повноважень, має здійснювати координацію та консолідацію спільних дій та проведення операцій з метою виявлення та нівелювання хакерських атак, надання належної відсічі їм. Це також дозволить активізувати співпрацю між відповідальними структурами держав-членів ЄС, які є уповноваженими щодо виявлення кібератак та оперативного реагування на них. Кіберпідрозділ має посилити співробітництво у цій сфері між євроінституціями та державами-членами, включаючи цивільні структури та правоохоронні органи, дипломатичні установи та спеціалізовані підрозділи кібернетичного захисту.

Важливе місце в положеннях Стратегії посідає міжнародний напрямок діяльності, зокрема, це активізація взаємодії з міжнародними організаціями щодо розробки загальних методологічних підходів до кіберзахисту, зміцнення партнерства з державами світу в контексті розвитку глобального, відкритого, стабільного кібернетичного простору на основі засад верховенства права, дотримання та виконання фундаментальних свобод та демократичних цінностей. Запропоновано реформування у сфері забезпечення кібербезпеки мереж та інформаційних систем, що дозволить підвищити кібернетичну стійкість критичної інфраструктури ЄС, включаючи заклади охорони здоров'я, залізниці, центри зберігання даних, дослідницьких та виробничих установ, які можуть бути уразливими до швидких кібернетичних атак.

У рамках розбудови міжнародного вектору, Євросоюз тісно співпрацюватиме зі структурами ООН та іноземними партнерами, має використовувати "інститут санкцій" з метою захисту прав людини й громадянина, фундаментальних свобод в інформаційному просторі, розвивати міжнародні норми та стандарти безпеки у цій площині. Єврокомісія планує проведення поетапних переговорів з усіма зацікавленими суб'єктами у цьому контексті. Таким чином, започаткована активізація міжнародного співробітництва за ініціативи ЄС є ключовим моментом щодо ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози. Очікується, що міжнародне співробітництво також здійснюється з метою зміцнення взаємної довіри у сфері кібербезпеки, у першу чергу, між ЄС та ООН, іншими міжнародними організаціями та альянсами держав, надасть можливість вироблення спільних підходів у протидії кіберзлочинності, консолідації зусиль у розслідуванні та запобіганні транснаціональним кіберзлочинам. При цьому в основі реалізації європейської інтеграції та її просування знаходиться культура політичного компромісу.

З метою реалізації цього програмного документу Єврокомісія має намір залучити 4,5 млрд. євро-інвестицій з метою підвищення кібербезпеки на теренах ЄС протягом

2021 – 2027 років, завдяки спільним зусиллям євро-інституцій, країн-членів та промисловості. Очікується, що перспективні інвестиції у кібербезпеку сприятимуть покращенню та оздоровленню у майбутньому онлайн-простору та мінімізуватимуть ймовірні ризики для об'єктів критичної інфраструктури. У положеннях Стратегії окрема увага присвячена створенню в ЄС мережі оперативних центрів кібербезпеки з можливістю залучення та впровадження в практичну площину штучного інтелекту задля виявлення кібернападів та протидії їм.

Підготовка цього фундаментального документа на стратегічному рівні стала певною реакцією європейського співтовариства на збільшення кількості кібератак, які виникають на перманентній основі, підвищення уразливості та збитковості цифрової економіки ЄС. Також підставами для розробки цієї Стратегії стали такі виклики як: підвищення ризиків для критичної інфраструктури, перехід 40 % працівників в ЄС на віддалений формат роботи під час пандемії коронавірусу в 2020 році, масштабні щорічні збитки світової економіки від кіберзлочинності у розмірі 5,5 трильйонів EUR, офіційно зафіксованих 450 кібератак на європейські об'єкти критичної інфраструктури у 2019 році, недоукомплектовано 291 тис. посад фахівців у сфері інформаційної безпеки в ЄС. Також можна сюди добавити потужну хакерську кібератаку 9 грудня 2020 року на Європейське агентство з лікарських засобів, яке здійснює сертифікацію вакцин від коронавірусу. Хакери, які атакували Європейське агентство з лікарських засобів, отримали доступ до документів щодо вакцини Pfizer/BioNTech [2]. Одночасно з Стратегією кібербезпеки ЄС була схвалена Директива щодо забезпечення стабільності критично важливих об'єктів [3].

Тобто, удосконалення процесів з метою забезпечення кібербезпеки в ЄС передбачає адаптацію до нових викликів та кіберзагроз, які досить швидко поширюються та розвиваються, вбачається комплексним процесом, який вимагає посилення спроможності сектору безпеки і оборони, співпраці усіх зацікавлених суб'єктів, держав та інституцій ЄС, приватного сектору, правоохоронних органів з використанням дипломатії та міжнародного співробітництва з метою забезпечення гарантованого захисту громадян та усієї інфраструктури. Результатом практичного впровадження європейської політики у сфері забезпечення кібербезпеки має стати створення автономного щита кібернетичного захисту на теренах ЄС. Оновлена Стратегія кібербезпеки ЄС передбачає також розширення сфери дій правил, що вже працюють у Союзі. Раніше вони стосувалися об'єктів охорони здоров'я, банківської справи, питного водопостачання та енергетичної інфраструктури. Тепер до такого переліку внесене також держуправління, об'єкти харчової промисловості та фармацевтичне виробництво. Протягом 18 місяців з дати набуття чинності Стратегією кібербезпеки ЄС, усі країни-члени мають привести свої нормативно-правові акти у відповідність до положень цього програмного документа.

Слід зазначити, що попередня редакція Стратегії кібербезпеки ЄС була ухвалена ще в лютому 2013 року та передбачала кроки, націлені на нарощування потужності задля попередження кіберзагроз, включаючи кіберзлочинність та кібертероризм, при цьому боротьба з високотехнологічними злочинами була визначена як один із основних пріоритетів у діяльності Європейського поліцейського управління (European Police Office – Europol) [4].

Також слід акцентувати увагу, що в Євросоюзі запроваджено практичний механізм застосування санкцій за кібератаки, який передбачає запровадження обмежень та негативних наслідків для осіб, які підозрюються у їх скоєнні. Цей режим було розроблено на виконання рішення Євросоюзу від 12 червня 2017 року про створення механізму реагування на недружні дії у кібернетичному просторі, так званого

“Інструментарію кібернетичної дипломатії”. Так, у Європейському Союзі запроваджено санкції проти осіб, відповідальних за кібернапад на німецький Бундестаг у 2015 році. Таким чином, у ЄС вже існує певний досвід застосування режиму “кіберсанкцій”, який фактично було накладено на 8 фізичних та 4 юридичних осіб з РФ, КНР та Північної Кореї у 2020 році.

Режим кіберсанкцій являє собою дію правових рамок адресних обмежувальних заходів проти особи або установ, які залучалися до скоєння кібернетичних атак, що завдали значної шкоди та представляють зовнішню загрозу для ЄС або його країн-членів. Стратегією регламентовано, що ЄС може також застосовувати санкції у відповідь на кібернетичні атаки проти третіх країн або міжнародних організацій, якщо рішення про застосування таких обмежувальних заходів вважатиметься доцільним в рамках Спільної політики ЄС з безпеки й оборони. Кінцевою метою запровадження цих заходів є стримування та реагування на кібернетичні атаки, при цьому санкції можуть включати заборону на подорожі до держав ЄС, заморожування фінансових активів осіб та установ. Навіть особи й установи, які перебуватимуть у “санкційному списку” не матимуть доступу до жодних фондів від ЄС. Таким чином, “режим кіберсанкцій” створює для ЄС правову основу щодо можливостей застосування обмежувальних заходів проти фізичних осіб або установ, що залучаються до кібернетичних атак на Євросоюз або його держави-члени.

Окрім вищезгаданих санкцій, пропонується зміцнювати потенціал протидії зловмисній поведінці третіх країн у кіберпросторі. Передбачається створення робочої групи кіберрозвідки у складі Центру розвідки ЄС. На виконання положень Стратегії кібербезпеки, у майбутньому планується побудова та кооперація всередині ЄС щодо розвитку концептів кібероборони, створення спільних структур енергетичної та військової кібербезпеки у рамках постійної структурованої співпраці (PESCO).

Цифрові технології зіграли вирішальну роль у підтриманні економічного та соціального життя під час кризи, пов’язаної з короновірусом, та залишаються ключовим фактором в успішному переході до постпандемічної економіки у майбутньому. Тобто масштабна цифрова трансформація залишається пріоритетом створення умов для глобального впливу ЄС на світову геополітику та економіку.

9 березня 2021 року Колегія Єврокомісії схвалила дорожню карту “Цифровий компас” [5] – декларативний документ, який визначає перспективи та завдання у сфері розвитку глобальної цифрової трансформації до 2030 року. Як йдеться в документі, “Цифровий компас” відображає перспективи технологічного розвитку ЄС до 2030 року у чотирьох напрямах – цифрова освіта, цифрова інфраструктура, цифровий розвиток бізнесу, цифровий розвиток державного сектору.

Перший напрямок стосується цифрової освіти населення та підготовки досвідчених фахівців у сфері цифрових технологій. Це означає, що до 2030 року, 80 % усього населення ЄС повинні мати базові цифрові навички. При цьому в ЄС мають бути працевлаштовані не менше 20 мільйонів фахівців у цифровій сфері, серед яких має суттєво зрости доля зайнятості жінок.

Другий – передбачає розвиток безпечної, ефективної та захищеної цифрової інфраструктури. До 2030 року всі домогосподарства мають бути забезпечені комунікаціями гігабітного рівня, а всі населені регіони мають отримати покриття мережею 5G. На той час на Європу має припадати не менше 20 % світового обсягу виробництва напівпровідників, виробництво передових та стійких напівпровідників у Європі має становити 20 % світового виробництва. Передбачається створення не менше 10 тис. ефективних та екологічних передавальних вузлів. У Європі має з’явитися

перший квантовий комп'ютер до 2025 року. До 2030 року очікується створення конкурентних європейських підприємств з повними циклами роботи щодо постачання напівпровідників – від проектування компонентів до готових продуктів. Центром суцільної цифровізації стануть промислові підприємства з виробництва процесорів формату 5G. Також планується значно знизити залежність від поставок цифрових продуктів з Південно-Східної Азії та Китаю.

Третій – стосується цифрового розвитку для бізнесу. До 2030 року три з чотирьох компаній мають використовувати "хмарні" комп'ютерні послуги, бази "великих даних" та засоби штучного інтелекту. Очікується, що не менше 90 % малих та середніх промислових підприємств мають досягти принаймні базового рівня інтенсивності у застосуванні комп'ютерних технологій.

Четвертий – цифровий розвиток державного сектору передбачає, що до 2030 року всі ключові громадські та соціальні послуги мають бути доступними у форматі онлайн. Громадяни ЄС зможуть повноцінно використовувати засоби цифрової ідентифікації, мати безобмежений доступ до власних електронних даних.

Усі перераховані напрямки програми "Цифровий компас" ЄС будуть включені в Політичну програму, яка має пройти розгляд і затвердження на рівні Європейського Парламенту та Ради ЄС, після чого стане частиною скоординованих дій з цифрового розвитку у всіх державах-членах. Такі зусилля, на переконання Єврокомісії, мають допомогти ЄС у подоланні глобальних викликів, розвинути співпрацю з міжнародними партнерами та організаціями, які мають схожі цілі, розвинути стійке та ефективне цифрове партнерство. У цьому контексті ЄС вже запропонував створити нову Раду ЄС-США з питань торгівлі і технологій. ЄС має намір підтримувати інших міжнародних партнерів, зокрема, шляхом створення Фонду цифрових комунікацій [6].

Таким чином, "Цифровий компас" ЄС являє собою звіт правил амбіційного та динамічного розвитку цифрової сфери та суцільної діджиталізації на поточні 10 років, а його практичне впровадження надасть змогу піднятися Євросоюзу у рейтингу світового технологічного розвитку на лідерські позиції, налагодити масштабне промислове виробництво напівпровідників та встановити контроль над 20 % світових поставок мікросхем та процесорів у цьому сегменті.

В Україні все ще діє стратегія кібербезпеки, схвалена у 2016 році [7].

З цього приводу у [8, С. 135] слушно зазначається: "…*стан реалізації Стратегії кібербезпеки України є незадовільним, що негативно впливає на всю сферу кібербезпеки та кіберзахисту України та є свідченням формального підходу з боку відповідальних державних органів до стратегічного планування, формування та реалізації державної політики, а також здійснення стратегічного контролю у цій сфері. Фактично цей документ розроблявся на 5 років*".

Висновки.

Забезпечення цифрового суверенітету та цифрового благополуччя бізнесу та населення політичним керівництвом ЄС визначається пріоритетами у роботі.

Можна констатувати, що ЄС нарощує свій потенціал у сфері тотальної діджіталізації, максимально намагаючись впроваджувати цифрові технології у всі сфери життєдіяльності європейського суспільства. Основним базовим документом в ЄС, який регулюватиме сферу кіберзахисту, є оновлена Стратегія кібербезпеки на 2021 – 2027 роки. ЄС концептуально має намір та вживає заходів з метою оперативного реагування на виклики та загрози сучасності в інформаційній сфері, впроваджує у реалії життя на загальнонаціональному рівні концепти "ризик-менеджменту" в умовах пандемії, визначаючи при цьому цифрові права та свободи громадян, їх захист найвищою цінністю.

Аналіз положень Стратегії передбачає використання регуляторних та інвестиційних механізмів, політичних ініціатив за такими напрямами: забезпечення стабільності, технологічного суверенітету та лідерства; здатність попереджувати, стримувати та адекватно реагувати на кібератаки; розвиток міжнародного співробітництва з метою формування глобального та відкритого кіберпростору. Актуальним та важливим напрямом щодо створення надійного європейського "Кіберщита" є утворення об'єднаної спільноти (Joint Cyber Unit) з метою оперативного обміну інформацією про загрози та надання допомоги в реагуванні на них, підтримка життєдіяльності середніх та малих підприємств, перезавантаження та удосконалення "CERT-EU", запровадження дієвих заходів з метою забезпечення безпеки мереж 5G, законодавче врегулювання Інтернету речей (Internet of Secure Things).

Інноваційний підхід закладено у положеннях цієї Стратегії щодо запровадження механізму "кіберсанкцій". ЄС може застосовувати їх проти зовнішніх суб'єктів за дотримання певних умов: по-перше, має бути встановлено, що такі недружні дії зроблені з-поза кордонів ЄС; по-друге, здійснені атаки проводилися персонами та установами, які утворені або діють за межами ЄС, або здійснюються за підтримки організацій або персон, які знаходяться за межами ЄС. Санкції можуть бути спричинені навмисними кібернетичними атаками, які можуть потенційно завдати значної шкоди Євросоюзу або його державам-членам. Компетенція щодо ухвалення та продовження рішень про запровадження "режиму кіберсанкцій" належить виключно Раді ЄС. Для України є цікавим досвід ЄС у сфері запровадження "режиму кіберсанкцій", який можливо імплементувати у вітчизняне законодавство з урахуванням національних особливостей.

Як вважаємо, з набуттям чинності новою Стратегією національної безпеки України 2020 р. вітчизняна стратегія кібербезпеки має бути переглянута з урахуванням нових гібридних загроз та викликів у цій сфері, повинна деталізувати пріоритети національних інтересів у сфері кібербезпеки, а також основні підходи та напрями до формування питань кіберзахисту.

Враховуючі політичні реалії та сучасні спрямування, Україна має активізувати співробітництво у сфері забезпечення кібербезпеки за такими напрямами: створення механізму оперативної координації та взаємодії, обміну інформацією про кіберзагрози й кіберінциденти між компетентними органами України та ЄС; вдосконалення міжнародного співробітництва у сфері кібербезпеки; імплементація міжнародно-правових та європейських норм у національне законодавство України, особливо щодо запровадження режиму кіберсанкцій.

Використана література

1. New EU Cybersecuritu Strategy. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (дата звернення: 20.02.2021).

2. Кібератака на агентство ЄС: хакери викрали дані щодо вакцини Pfizer/BioNTech. URL: https://www.eurointegration.com.ua/news/2020/12/10/7117477 (дата звернення: 20.02.2021).

3. Directive Of The European Parliament And Of The Council on the resilience of critical entities. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (дата звернення: 20.02.2021).

4. Яцишин М.Ю. Роль міжнародних організацій у протидії кіберзлочинності. *Українське право*. URL: https://ukrainepravo.com/international_law/public_international_law/rolmizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti (дата звернення: 20.02.2021).

5. Europe's Digital Decade: Digitally empowered Europe by 2030. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983 (дата звернення: 20.02.2021).

6. Єврокомісія визначила стратегічні цілі цифрового розвитку ЄС до 2030 року. URL: https://www.ukrinform.ua/rubric-world/3205020-evrokomisia-viznacila-strategicni-cili-cifrovogo-rozvitku-es-do-2030-roku.html (дата звернення: 20.02.2021).

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 20.02.2021).

8. Ткачук Н.В. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право.* № 1(28)/2019. С. 129-134.

9. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.02.2021).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~