Наталія ФІЛІПЕНКО,
доктор юридичних наук, професор,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: https://orcid.org/0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

Вячеслав ХАРЧЕНКО,
доктор технічних наук, професор, член-кореспондент НАН України, лауреат Державної премії України у галузі науки і техніки, завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій (503)
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: https://orcid.org/0000-0001-5352-077X
e-mail: v.kharchenko@csn.khai.edu

Сергій ЛУКАШЕВИЧ,
кандидат юридичних наук, доцент,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: https://orcid.org/0000-0001-8386-6237
e-mail: s.lukashevych@khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.03

ЕВОЛЮЦІЯ БЕЗПЕКОВОЇ ПОЛІТИКИ ЄВРОПЕЙСЬКОГО СОЮЗУ У КОНТЕКСТІ НОВИХ КІБЕРЗАГРОЗ: ВІД ДИРЕКТИВИ NIS1 ДО ДИРЕКТИВИ NIS2 (оглядова стаття)

Анотація. *У статті досліджено трансформацію нормативно-правового регулювання кібербезпеки в Європейському Союзі крізь призму еволюції від Директиви NIS1 (2016/1148/ЄС) до NIS2 (2022/2555/ЄС). Особливу увагу приділено аналізу ключових положень обох директив, їх порівнянню за критеріями охоплення, жорсткості вимог, механізмів контролю та санкцій. У контексті повномасштабної війни, розв'язаної російською федерацією, Україна стала мішенню багатьох хвиль кібератак, що актуалізувало питання кіберстійкості держави як складової національної безпеки. Розглянуто перспективи імплементації європейських стандартів кібербезпеки в українську правову систему, з урахуванням викликів війни, міжнародних зобов'язань та стратегічного курсу на євроінтеграцію, а також формування лідируючої позиції України в регіоні.*

Ключові слова: *безпекова політика, кібербезпека, Директива NIS1, Директива NIS2, Європейський Союз, Україна, критична інфраструктура, кіберстійкість, нормативне регулювання, цифрова безпека, євроінтеграція, гібридна війна.*

Вступ. Протягом останніх років Україна систематично зазнає масштабних та цілеспрямованих кібератак, які стали одним із ключових інструментів гібридної агресії проти держави. Ці атаки, що охоплюють як державні інформаційні ресурси, так і об'єкти критичної інфраструктури (енергетичні системи, транспорт, зв'язок, фінансовий сектор), завдали відчутної шкоди національній безпеці та стабільності управлінських процесів. Особливої гостроти проблема набула в умовах повномасштабної війни, розв'язаної російською федерацією, коли кіберпростір перетворився на повноцінний театр бойових дій.

За даними Державної служби спеціального зв'язку та захисту інформації України, протягом першого півріччя 2025 року було зафіксовано понад 1,5 млн унікальних підозрілих файлів, що містили шкідливий програмний код, зокрема такі сімейства як SmokeLoader, Agent Tesla, Snake Keylogger, Remcos та Formbook. CERT-UA, що функціонує в складі Держспецзв'язку, також повідомляє про зростання кількості цілеспрямованих атак на урядові установи та підприємства оборонно-промислового комплексу, з використанням фішингових кампаній, зокрема під виглядом «судових повісток» [1].

Ці події не лише порушили функціонування ключових секторів, але й висвітлили системну вразливість інформаційного середовища держави. Вони чітко продемонстрували, що навіть найвищий рівень технічної підготовки фахівців з кібербезпеки не здатен забезпечити належний рівень захисту без чітко сформованої, актуальної та дієвої нормативно-правової бази. Відсутність комплексного законодавчого регулювання, уніфікованих стандартів реагування та прозорих механізмів відповідальності значно ускладнює координацію дій між державними органами, приватним сектором та міжнародними партнерами. У цьому багатовимірному ландшафті особливе значення набувають кіберполігони [2, с. 58] – спеціалізовані платформи, що слугують не лише технічним середовищем для моделювання, тестування та тренування реагування на кіберінциденти, а й стратегічним інструментом формування національної кіберстійкості. Вони дозволяють відпрацьовувати сценарії атак різного рівня складності – від типових фішингових кампаній до складних багатовекторних загроз, що імітують дії державних або транснаціональних акторів. У таких умовах персонал має змогу діяти в реалістичному, контрольованому середовищі, що максимально наближене до реальних кризових ситуацій. Кіберполігони відіграють ключову роль у перевірці ефективності захисних механізмів, тестуванні нових технологій, оцінці процедур реагування та відновлення, а також у формуванні міжвідомчої координації між державними структурами, приватними компаніями, операторами критичної інфраструктури та науковими установами. Вони створюють умови для спільного навчання, обміну досвідом, розробки стандартів та протоколів, що можуть бути адаптовані до національного контексту.

Для України, яка перебуває на цифровому фронті війни, створення національних кіберполігонів є не просто бажаним, а стратегічно необхідним кроком. Умови гібридної агресії з боку Російської Федерації, що включає масовані кібератаки на урядові системи, енергетичну інфраструктуру, медіа та фінансовий сектор, вимагають від держави не лише реактивної, а й проактивної позиції. Кіберполігони можуть стати основою для підготовки фахівців, тестування національних протоколів реагування, розробки сценаріїв кризового управління та формування спільного цифрового щита. Крім того, такі платформи відкривають можливості для інтеграції України в європейські та міжнародні тренувальні програми, зокрема в межах ENISA, NATO CCDCOE, EU-CyCLONe та інших ініціатив. Це дозволяє не лише підвищити рівень технічної компетентності, а й зміцнити довіру та оперативну сумісність між українськими структурами та партнерами з ЄС і НАТО. У ширшому контексті кіберполігони можуть стати інкубаторами інновацій, де тестуються нові підходи до захисту штучного інтелекту, інтернету речей, роботизованих і мобільних систем, хмарних сервісів, 5/6G-інфраструктури, а також моделюються ризики, пов'язані з транснаціональною кіберзлочинністю. Вони здатні об'єднати зусилля правників, технічних експертів, стратегів і етичних аналітиків у створенні цілісної системи цифрової безпеки, яка враховує не лише технічні, а й правові, організаційні та гуманітарні виміри.

У цьому контексті питання кіберстійкості набуває не лише технічного, а й стратегічного виміру. Йдеться про здатність держави не лише протистояти атакам, а й забезпечити безперервність функціонування критичних систем, зберігаючи довіру громадян і партнерів до цифрової інфраструктури. Саме тому формування сучасної, адаптивної та інтегрованої системи кібербезпеки – з урахуванням європейських стандартів, таких як Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року щодо заходів із забезпечення високого спільного рівня кібербезпеки на території Союзу (далі – NIS2) [3] – є не просто актуальним завданням, а питанням національного виживання в умовах гібридних війн XXI століття.

Літературні джерела. Кібербезпека – це багатовимірна сфера, яка охоплює технологічні, правові, організаційні та етичні аспекти. У контексті дослідження нормативно-правових засад кібербезпеки та її гармонізації з європейськими стандартами, варто зазначити, що окремі аспекти кримінологічного та кримінально-правового захисту інформаційного простору вже були предметом ґрунтовного аналізу вітчизняних науковців. Зокрема, вагомий внесок у розробку теоретичних і прикладних підходів до протидії кіберзлочинності зробили такі дослідники, як В. С. Венедіктов, В. В. Вертузаєв, М. В. Вєхов, В. В. Голіна, В. А. Журавель, М. В. Карчевський, М. М. Коваленко, В. К. Колпаков, О. В. Кохановська, О. М. Литвинов, С. Ю. Лукашевич, М. І. Панов, В. В. Пивоваров, Ф. П. Тарасенко, Л. К. Терещенко, Т. І. Тарахонич, Н. Є. Філіпенко, В. С. Харченко, В. М. Шевчук, В. Ю. Шепітько та інші. У їхніх працях розглядаються ключові проблеми – від концептуалізації інформаційної безпеки як об'єкта кримінально-правової охорони до класифікації кіберзлочинів і розробки моделей реагування на кіберзагрози в межах системи національної безпеки. Узагальнення наукових позицій свідчить про необхідність міждисциплінарного підходу до формування ефективної системи кіберзахисту, що поєднує кримінологічну аналітику, правові механізми та сучасні технологічні інструменти.

До кола авторитетних зарубіжних фахівців, чиї дослідження суттєво вплинули на розвиток

концепцій кібербезпеки та цифрової стійкості, належать такі науковці: Bruce Schneier, Eugene Spafford, Ross Anderson, Herbert Lin, Myriam Dunn Cavelty, Ronald Deibert, Thomas Rid, Richard Clarke, Laura DeNardis, Joseph Nye, Peter W. Singer, Dorothy Denning, Gary McGraw, Brian Krebs, Nils Melzer, Chris Inglis, Melissa Hathaway, David Sanger, James Lewis, Adam Segal. Їх праці належать до різних наукових шкіл та практичних напрямів –від технічної безпеки до стратегічного управління ризиками, кібердипломатії та цифрових прав. Їхні праці активно використовуються в академічних колах, урядових стратегіях і міжнародних ініціативах з кіберзахисту.

У світлі євроінтеграційного курсу України та з урахуванням приєднання до Конвенції ООН про боротьбу з кіберзлочинністю у 2025 році, особливої актуальності набуває завдання адаптації національного законодавства до положень Директиви NIS2. Такий вектор розвитку вимагає не лише оновлення правових норм, а й переосмислення ролі кримінального права у забезпеченні цифрової безпеки в умовах гібридних загроз та транснаціонального характеру сучасної кіберзлочинності.

Виклад основного матеріалу. Стрімкий розвиток індустрії високих технологій та їх широкомасштабне впровадження в ключові сфери суспільного життя – економіку, державне управління, освітню систему, охорону здоров'я, оборонний сектор – спричиняє глибоку трансформацію сучасного соціального простору. Ці процеси вже давно вийшли за межі суто технічного оновлення: вони набули системного, багатовимірного характеру, формуючи нову цифрову реальність, у якій змінюються не лише інструменти, а й самі принципи функціонування суспільства. Інформатизація та цифровізація дедалі більше впливають на структуру соціальних відносин, трансформують моделі комунікації, змінюють характер зайнятості, формати професійної діяльності, а також принципи публічного адміністрування. Відбувається поступове переосмислення ролі держави, бізнесу та громадян у цифровому середовищі, що вимагає нових підходів до регулювання, захисту прав, забезпечення кібербезпеки та формування цифрової компетентності населення. У цьому контексті цифрова трансформація постає не лише як технологічний процес, а як глибока соціальна, правова та культурна зміна, що визначає нові вектори розвитку державної політики, зокрема в сфері безпеки, освіти, економіки та правового регулювання. Вона вимагає системного осмислення та інтеграції до стратегічного планування на рівні національних і наднаціональних інституцій.

Як слушно зазначають науковці [4], динамічний розвиток комп'ютерних технологій, зокрема впровадження штучного інтелекту, хмарних обчислень, великих даних і мережевих інфраструктур, стає потужним каталізатором цифрової трансформації сучасного суспільства. Ці інновації відкривають нові можливості для економічного зростання, оптимізації державного управління, модернізації освіти, медицини та оборонного сектору. Водночас, їх повсюдне поширення супроводжується виникненням складного комплексу ризиків, які охоплюють економічну, політичну, безпекову, соціальну та військову сфери. До економічних загроз належать кібершахрайство, цифрове рейдерство, порушення фінансової стабільності; до політичних – втручання у виборчі процеси, маніпуляція громадською думкою через цифрові платформи; до соціальних – посилення цифрової нерівності, технологічна залежність, втрата приватності; до безпекових – кібератаки на об'єкти критичної інфраструктури, інформаційні операції та гібридні загрози. У цьому контексті особливої актуальності набуває формування ефективної, цілісної системи правового регулювання цифрового середовища, яка здатна забезпечити баланс між інноваційним розвитком і безпекою. Така система має ґрунтуватися на глибокому кримінологічному аналізі нових форм злочинної поведінки у кіберпросторі, а також на своєчасному оновленні кримінально-правових інструментів, що дозволяють адекватно реагувати на цифрові загрози. Важливою складовою цього процесу є інтеграція міжнародних стандартів, зокрема положень Конвенції ООН про боротьбу з кіберзлочинністю та Директиви ЄС NIS2, яка встановлює нові вимоги до кіберстійкості критичної інфраструктури та цифрових послуг. Усе це вимагає міждисциплінарного підходу, що поєднує правову, технічну, соціальну та етичну експертизу, а також активної участі держави, бізнесу, наукової спільноти та громадянського суспільства у формуванні безпечного, стійкого й справедливого цифрового простору.

Європейський Союз, як складне наднаціональне об'єднання, послідовно розширює свої повноваження у сфері безпеки та оборони, трансформуючи їх із суто координаційних механізмів у системні інституційні інструменти. В умовах зростання геополітичної нестабільності, кіберзагроз та гібридних форм агресії, ЄС дедалі активніше формує власну стратегічну автономію у сфері безпекової політики, прагнучи не лише доповнювати національні оборонні системи держав-членів, а й виступати як самостійний суб'єкт глобального безпекового порядку. Цей процес включає розробку нормативних актів, створення спеціалізованих агентств, механізмів кризового реагування, кіберзахисту, а також поглиблення співпраці з НАТО, ООН та іншими міжнародними структурами. Зокрема, ухвалення таких документів, як Стратегічний компас ЄС, Директива NIS2, а також функціонування Європейської служби зовнішніх справ (EEAS) і Європейського оборонного агентства (EDA), свідчать про поступове становлення ЄС як повноцінного актора у сфері безпеки, здатного формувати політику превентивного захисту, реагування на кризові ситуації та забезпечення кіберстійкості в межах єдиного цифрового простору.

Як зазначено у звіті Служби досліджень Конгресу США, розвиток Спільної зовнішньої та безпекової політики ЄС упродовж двох десятиліть

дозволив цьому об'єднанню вийти за межі виключно економічного суб'єкта, доповнивши його ідентичність новим вагомим виміром – безпековим компонентом [5].

Захист критичної інфраструктури на загальноєвропейському рівні поступово трансформувався з технічного завдання окремих держав-членів у самостійний, стратегічно важливий напрям безпекової політики Європейського Союзу. Цей процес є невід'ємною складовою формування цілісної архітектури безпеки ЄС, яка охоплює не лише військову та зовнішньополітичну складову, а й внутрішню стійкість до багатовимірних загроз – від терористичних актів до природних катастроф і техногенних аварій.

Інституційне оформлення цього напряму відбувається на основі ключових програмних документів, зокрема Стокгольмської програми та Стратегії внутрішньої безпеки ЄС. У них визначено пріоритети запобігання тероризму, протидії радикалізації та вербуванню, а також забезпечення здатності Європи ефективно реагувати на кризові ситуації. Такий підхід вимагає переосмислення меж компетенції ЄС у сфері безпеки та визначення ступеня впливу наднаціональних рішень на національні політики держав-членів. Практичне усвідомлення важливості захисту критичної інфраструктури як елементу колективної безпеки ЄС виникло лише після низки резонансних подій, а саме терористичних атак у Мадриді в березні 2004 року. Ці події продемонстрували, що порушення функціонування ключових об'єктів – енергетичних систем, транспортних вузлів, телекомунікаційних мереж – може мати транскордонні наслідки, здатні паралізувати життєво важливі процеси в кількох державах одночасно. У відповідь на ці виклики Європейська Рада в червні 2004 року доручила Європейській Комісії розробити стратегічний документ, який би окреслив загальноєвропейський підхід до захисту критичної інфраструктури.

Першим кроком стала ініціатива «Захист критичної інфраструктури в боротьбі з тероризмом», що заклала основу для створення Європейської програми захисту критичної інфраструктури (далі – EPCIP). Програма передбачала: ідентифікацію об'єктів критичної інфраструктури, що мають транскордонне значення; оцінку їхньої вразливості та взаємозалежності; розробку превентивних та реактивних заходів на основі комплексного підходу до аналізу загроз (all-hazard approach); інтеграцію безпекових заходів до систем планування діяльності правоохоронних органів та служб цивільного захисту; підвищення рівня обізнаності щодо терористичних ризиків серед ключових операторів інфраструктури тощо.

Подальший розвиток концептуальних засад EPCIP було здійснено через публікацію Зеленої книги Європейської Комісії у листопаді 2005 року, яка деталізувала цілі, принципи та механізми реалізації програми на рівні ЄС. Документ став основою для формування нормативної та інституційної бази, що дозволяє координувати зусилля держав-членів у сфері захисту критичних об'єктів, забезпечуючи єдність підходів та оперативну взаємодію в умовах криз. Захист критичної інфраструктури перетворився на системний елемент європейської безпекової політики, що поєднує правові, технічні та організаційні інструменти, спрямовані на зміцнення стійкості Європейського Союзу перед сучасними загрозами. У цьому контексті директиви на кшталт NIS2 відіграють ключову роль, забезпечуючи нормативне підґрунтя для кіберзахисту інфраструктурних систем у цифрову епоху.

Європейський Союз, реагуючи на сучасні виклики, особливо війну проти України, усвідомив необхідність формування узгодженого, системного підходу до забезпечення стійкості критичної інфраструктури, яка є основою стабільного функціонування спільного ринку, безперервного надання життєво важливих послуг та збереження соціальної згуртованості.

У грудні 2022 року Рада ЄС ухвалила «Рекомендації щодо скоординованого підходу до забезпечення стійкості критичної інфраструктури» [6], які стали важливим кроком у напрямі посилення колективної безпеки.

Ці рекомендації передбачають:

- поглиблення міждержавної координації між органами влади держав-членів, інституціями ЄС та операторами критичної інфраструктури з метою забезпечення оперативного реагування на загрози;

- розробку спільних механізмів оцінки ризиків, включно з транскордонними сценаріями, що враховують взаємозалежність інфраструктурних систем;

- створення єдиних стандартів стійкості, які мають бути інтегровані в національні стратегії безпеки та плани реагування;

- підвищення обізнаності та готовності операторів до дій у надзвичайних ситуаціях, зокрема через навчання, симуляції та обмін найкращими практиками;

- забезпечення безперервності надання послуг, що мають життєво важливе значення для населення, економіки та функціонування державних інституцій;

- інтеграцію кібербезпеки як ключового компонента стійкості, з урахуванням положень Директиви NIS2 та нової Директиви CER щодо фізичного захисту критичних об'єктів.

Державам-членам рекомендовано застосовувати методологію оцінювання ризиків критичної інфраструктури на основі підходу «all-hazard», що враховує вплив загроз будь-якого характеру, а також адаптувати до цього національні системи ризик-аналізу. Крім того, країни ЄС мають розпочати розроблення заходів з підвищення стійкості інфраструктур відповідно до положень оновленого законодавства, приділяючи особливу

увагу міждержавній співпраці, обміну інформацією з Єврокомісією, виявленню транскордонних загроз та посиленню підтримки операторів для забезпечення їх належного функціонування. Значну увагу рекомендовано зосередити на організації навчань і тренінгів з питань стійкості критичної інфраструктури із залученням експертного середовища, а також стимулювати участь фахівців у відповідних програмах підвищення кваліфікації [7].

У контексті зростаючих глобальних кіберзагроз Україна взяла на себе низку міжнародних зобов'язань, підписавши відповідні договори, що стосуються забезпечення безпеки в кіберпросторі. Ці зобов'язання стали основою для формування національної нормативно-правової бази у сфері кібербезпеки, яка має відповідати міжнародним стандартам, принципам правової узгодженості та вимогам цифрової стійкості. Підписання таких договорів передбачає не лише декларативне визнання стандартів, але й практичне їх імплементування в українське законодавство, що охоплює як технічні, так і організаційно-правові аспекти захисту державних інформаційних ресурсів. Хоча Україна не є членом Європейського Союзу і формально не ратифікувала Директиви NIS1 та NIS2, їх положення активно вивчаються та частково інтегруються в національні системи кіберзахисту.

Попри те, що Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року щодо заходів із забезпечення високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (далі – NIS1) [8] вже втратила чинність (підкреслено нами), все ж хочемо розпочати аналіз саме з її положень, тому що для розуміння стратегії безпеки Європейського Союзу саме вони стали визначальними. Цей документ було прийнято у липні 2016 року як дороговказ загальноєвропейським заходам щодо забезпечення високого спільного рівня безпеки мережевих та інформаційних систем.

Директива NIS1 стала першим нормативним актом ЄС, що системно врегулював питання кібербезпеки, заклавши інституційні та правові основи для побудови спільної архітектури кіберстійкості. Директива мала на меті забезпечити високий спільний рівень безпеки мережевих та інформаційних систем у межах Союзу, особливо в критичних секторах, таких як енергетика, транспорт, охорона здоров'я, водопостачання та цифрова інфраструктура. Одним із ключових нововведень NIS1 стало впровадження класифікації суб'єктів на операторів основних послуг (OES) та постачальників цифрових сервісів (DSP), що дозволило чітко окреслити коло відповідальних за забезпечення кібербезпеки. Директива зобов'язувала держави-члени розробити національні стратегії кібербезпеки, створити компетентні органи та команди реагування на комп'ютерні інциденти (CSIRT), а також запровадити обов'язок повідомлення про серйозні кіберінциденти. Вона також започаткувала механізми міждержавної координації через створення Групи співпраці та мережі CSIRTs, що сприяло обміну інформацією, кращими практиками та спільному реагуванню на загрози. Хоча NIS1 виявила низку недоліків – зокрема нечіткі критерії класифікації, нерівномірну імплементацію в державах-членах та обмеженість санкційних механізмів – її значення як першого кроку до уніфікованої європейської кіберполітики є беззаперечним. Саме на її основі було сформовано підґрунтя для подальшого вдосконалення нормативної бази, що втілилося у прийнятті NIS2 – більш жорсткої, деталізованої та адаптованої до сучасних викликів директиви, яка продовжує логіку NIS1, але з урахуванням нових реалій цифрової безпеки.

Для України, яка прагне інтегруватися до цифрового простору ЄС, аналіз NIS1 має не лише історичне, а й практичне значення. Він дозволяє зрозуміти логіку побудови нормативної системи кібербезпеки, визначити ключові інституційні компоненти та адаптувати національне законодавство до європейських стандартів.

Як вже зазначалося нами, NIS 2 – це скорочена назва Директиви Європейського Союзу 2022/2555, яка є оновленою версією першої редакції NIS, ухваленої у 2016 році. Абревіатура NIS розшифровується як Network and Information Security – «Мережева та інформаційна безпека» [3]. Документ спрямований на підвищення рівня кіберзахисту в організаціях, що належать до критичної інфраструктури.

NIS2 суттєво розширює сферу дії попередньої директиви, охоплюючи не лише традиційні сектори (енергетика, транспорт, охорона здоров'я), а й нові галузі – публічне управління, космічну індустрію, управління відходами, харчову промисловість, виробництво медичного обладнання та ІКТ-послуги. Директива встановлює обов'язкові вимоги до управління ризиками, включаючи впровадження політик безперервності бізнесу, багатофакторної автентифікації, захисту ланцюгів постачання, навчання персоналу та криптографічного захисту.

Ця Директива не є універсальною – її дія залежить від галузі, в якій функціонує компанія, та її масштабів. До категорії Essential (високої значущості) належать організації, що працюють у таких секторах, як енергетика, транспорт, банківська справа, водопостачання та водовідведення, цифрова інфраструктура, управління ІКТ-послугами (B2B), фінансові ринки, охорона здоров'я, державне управління та космічна галузь. Для кожного сектора передбачено окремі критерії, що визначають, чи підпадає організація під дію NIS 2. Важливим чинником є розмір компанії: великі підприємства (понад 250 працівників або річний дохід понад 50 млн євро) зазвичай класифікуються як Essential, а середні (50–249 працівників або понад 10 млн євро доходу) – як Important. Визначення розміру базується на Рекомендації Європейської комісії 2003/361/ЕС. Загалом, NIS 2 охоплює лише середні та великі компанії у зазначених секторах. Винятком є оператори електронного зв'язку, постачальники TSP та DNS-

послуг, а також реєстратори доменних імен – для них директива діє в повному обсязі, незалежно від розміру чи інших обставин. Якщо компанія працює в кількох секторах, застосовуються вимоги найсуворішого з них.

На рівні держав-членів директива зобов'язує уряди розробити оновлені національні стратегії кібербезпеки, створити або модернізувати компетентні органи (зокрема CSIRT – команди реагування на комп'ютерні інциденти), забезпечити ефективну координацію між державними структурами, приватним сектором і міжнародними партнерами. Важливим елементом є створення Європейської мережі кризового реагування (EU-CyCLONe), яка має забезпечити оперативну взаємодію між країнами у випадку масштабних кіберінцидентів. Така інституційна архітектура сприяє формуванню єдиного кібербезпекового простору в межах ЄС, заснованого на принципах довіри, обміну інформацією та спільної відповідальності.

Директива NIS2 приділяє особливої уваги не лише формуванню нормативних вимог до кіберстійкості, а й створенню дієвих механізмів нагляду, контролю та санкцій, які мають забезпечити реальну відповідальність суб'єктів за недотримання встановлених стандартів. На відміну від NIS1, де контрольні функції були сформульовані досить загально, NIS2 встановлює чіткі зобов'язання для держав-членів щодо організації ефективного моніторингу виконання директиви. Це включає регулярне проведення аудитів, перевірок на місцях, інспекцій, а також розслідувань інцидентів, що можуть свідчити про порушення вимог безпеки. Компетентні національні органи отримують розширені повноваження для збору інформації, доступу до внутрішніх документів організацій, оцінки технічних і організаційних заходів, а також накладення санкцій. У разі виявлення порушень передбачено значні адміністративні штрафи – до 10 мільйонів євро або 2% річного глобального обороту компанії (для essential entities), що є суттєвим інструментом впливу на великі транснаціональні структури. Для important entities передбачено штрафи до 7 мільйонів євро або 1,4% обороту.

Крім фінансових санкцій, директива передбачає можливість тимчасового призупинення діяльності організацій, які систематично порушують вимоги, або навіть усунення керівництва, якщо буде доведено їхню бездіяльність чи недбалість у питаннях кібербезпеки. Такий підхід формує нову культуру відповідальності, де кібербезпека розглядається не як технічна опція, а як стратегічний обов'язок, що має бути інтегрований у корпоративне управління [3]. Важливо, що NIS2 також зобов'язує держави-члени забезпечити прозорість процедур контролю, доступність інформації про порушення та санкції, а також можливість апеляційного оскарження рішень наглядових органів. Це сприяє формуванню довіри до регуляторної системи та стимулює суб'єктів до проактивного дотримання вимог, впровадження внутрішніх механізмів самоконтролю та постійного вдосконалення політик безпеки.

У нормативному вимірі Директива NIS2 демонструє високий рівень гармонізації з провідними міжнародними стандартами у сфері кібербезпеки, що забезпечує її інтеграцію у глобальну систему цифрового захисту. Зокрема, положення директиви узгоджуються з вимогами ISO/IEC 27001, який встановлює рамки для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS), а також з ISO/IEC 27002, що містить практичні рекомендації щодо реалізації заходів безпеки, включаючи контроль доступу, криптографію, захист фізичних активів та управління інцидентами. Крім того, NIS2 враховує принципи NIST Cybersecurity Framework, розробленого Національним інститутом стандартів і технологій США, який пропонує модель управління ризиками, побудовану навколо п'яти ключових функцій: ідентифікація, захист, виявлення, реагування та відновлення. Така структура дозволяє суб'єктам критичної інфраструктури системно оцінювати свої вразливості, формувати політики реагування та забезпечувати безперервність бізнесу.

У контексті реалізації Директиви NIS2 важливу роль відіграють рекомендації та аналітичні напрацювання Європейського агентства з кібербезпеки (ENISA), яке функціонує як головний центр експертизи, методологічної підтримки та координації в межах Європейського Союзу. ENISA не лише забезпечує технічне консультування для держав-членів, а й формує стратегічні орієнтири для імплементації директиви на національному рівні. Зокрема, агентство розробляє технічні керівництва, моделі оцінки ризиків, стандарти сертифікації, індикатори кіберстійкості, а також аналітичні звіти, що дозволяють адаптувати положення NIS2 до конкретних галузевих і регіональних контекстів.

Одним із фундаментальних нововведень NIS2 є згадана вище класифікація організацій на дві категорії залежно від кількості персоналу. Важливим для такої класифікації є також сфери, де вони функціонують і вплив на економіку і безпеку: «Суттєві» (essential entities) – великі структури, що здійснюють діяльність у критичних секторах (енергетика, транспорт, охорона здоров'я, цифрова інфраструктура тощо); «Важливі» (important entities) – середні організації, які також мають значний вплив на економіку та суспільну стабільність. Для обох категорій встановлено обов'язкові вимоги, що мають бути інтегровані в операційну діяльність організацій. Зокрема: впровадження систем управління ризиками, що охоплюють ідентифікацію загроз, оцінку вразливостей, планування реагування та відновлення; захист ланцюгів постачання, включаючи перевірку кіберстійкості партнерів і підрядників; призначення відповідального за кібербезпеку на рівні керівництва, що забезпечує стратегічну інтеграцію безпекових політик; оперативне повідомлення про кіберінциденти –

попереднє повідомлення протягом 24 годин, детальний звіт упродовж 72 годин, фінальний – не пізніше ніж через місяць; проведення внутрішніх аудитів, що дозволяють виявляти недоліки та вдосконалювати політики безпеки; навчання персоналу, спрямоване на підвищення обізнаності, формування навичок реагування та запобігання інцидентам тощо. Ці заходи не лише формалізують обов'язки організацій, а й сприяють становленню проактивної культури безпеки, де кіберзахист розглядається як невід'ємна частина стратегічного управління, а не як реакція на інциденти. Відповідно, NIS2 стимулює перехід від фрагментарного реагування до системного управління ризиками, інтегрованого в усі бізнес-процеси – від закупівель і логістики до комунікацій і управління персоналом.

Директива NIS2 відіграє ключову роль у формуванні нормативної узгодженості між європейськими та глобальними підходами до кібербезпеки, забезпечуючи можливість інтеграції найкращих міжнародних практик у національні системи держав-членів. Її положення гармонізовані з такими авторитетними стандартами, як ISO/IEC 27001 (система управління інформаційною безпекою), ISO/IEC 27002 (практичні заходи безпеки), NIST Cybersecurity Framework (модель управління ризиками, розроблена у США), а також рекомендаціями Європейського агентства з кібербезпеки (ENISA). Така нормативна сумісність сприяє не лише підвищенню кіберстійкості окремих країн, а й створенню єдиного цифрового простору, де безпека розглядається як колективна відповідальність, а стандарти – як взаємно визнані та технічно сумісні. Особливої уваги NIS2 надає викликам, що виникають у зв'язку з впровадженням новітніх технологій, які водночас є джерелами ризику та інструментами захисту. Зокрема, директива враховує специфіку таких технологій, як штучний інтелект (AI), інтернет речей (IoT), хмарні обчислення та мережі п'ятого покоління (5G). Вона стимулює держави-члени до розробки спеціалізованих політик, які не лише враховують потенційні вразливості, пов'язані з цими технологіями, а й використовують їх для підвищення ефективності кіберзахисту – наприклад, через автоматизоване виявлення загроз, прогнозування інцидентів, адаптивне управління ризиками та захист ланцюгів постачання. Тобто, NIS2 формує нормативну рамку, здатну реагувати на динаміку технологічного прогресу, забезпечуючи гнучкість, адаптивність і стратегічну стійкість. Вона не лише регламентує мінімальні вимоги до безпеки, а й створює умови для інноваційного розвитку цифрової екосистеми, де технології працюють на захист, а не на загрозу [3].

Висновки. З огляду на аналіз положень Директив NIS1 і NIS2, а також сучасні виклики цифрової безпеки, Україна має унікальну можливість не лише адаптувати своє законодавство до стандартів Європейського Союзу, а й закласти фундамент для побудови стійкої, інституційно зрілої та технологічно адаптивної системи кібербезпеки. Попри втрату чинності NIS1, її концептуальні положення залишаються важливими для розуміння логіки еволюції європейської безпекової політики. Саме вона започаткувала ключові механізми: класифікацію операторів основних послуг і цифрових сервісів, створення національних стратегій кібербезпеки, формування CSIRT-команд та обов'язок повідомлення про інциденти. NIS2, у свою чергу, суттєво розширює ці підходи, вводячи нову класифікацію суб'єктів на «суттєві» та «важливі», встановлюючи жорсткіші вимоги до управління ризиками, захисту ланцюгів постачання, навчання персоналу, внутрішніх аудитів і оперативного реагування на інциденти.

Особливу увагу NIS2 приділяє механізмам нагляду, контролю та санкцій, зобов'язуючи держави-члени забезпечити ефективний моніторинг дотримання вимог через аудити, перевірки та розслідування. У разі порушень передбачено значні штрафи – до 10 мільйонів євро або 2% річного обороту компанії, а також можливість тимчасового призупинення діяльності або усунення керівництва. Такий підхід формує нову культуру відповідальності, де кібербезпека інтегрується в корпоративне управління як стратегічний обов'язок і, навіть, інноваційний чинник.

У нормативному сенсі NIS2 гармонізована з провідними міжнародними стандартами – ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework – та рекомендаціями ENISA, що забезпечує узгодженість між європейськими та глобальними підходами. Це дозволяє державам-членам, зокрема Україні, адаптувати найкращі практики до власних нормативних систем, підвищуючи кіберстійкість і сприяючи формуванню єдиного цифрового простору, де безпека є спільною відповідальністю.

Важливо, що NIS2 також враховує виклики, пов'язані з новими технологіями – штучним інтелектом, інтернетом речей, хмарними обчисленнями та 5G – і стимулює держави до розроблення спеціалізованих політик, які розглядають ці технології не лише як джерела ризику, а й як інструменти підвищення кіберстійкості.

У цьому контексті Україна має реалізувати низку стратегічних кроків: гармонізувати законодавство з положеннями NIS2; створити реєстр критичних суб'єктів; запровадити ефективну систему нагляду, санкцій і внутрішнього аудиту; розробити політики щодо новітніх технологій; забезпечити навчання персоналу та формування культури кібербезпеки; а також інтегруватися в європейські платформи обміну інформацією та реагування. Слід також розвивати методологічні і технологічні напрями, які детально не окреслено в NIS2: аналізувати вплив і протистояти загрозам на всіх безпекових рівнях і периметрах: рівнях інформаційних (інформаційна і кібербезпека) та операційних технологій (функційна безпечність); фізичному,

інформаційному та сигнальному периметрах. Це дозволяє не тільки створювати інтегровані системи управління безпекою індустріальних підприємств і об'єктів критичної інфраструктури [9], але й опрацьовувати додаткові канали кіберзлочинності та нейтралізувати відповідні загрози. Крім того, треба враховувати потужний і динамічний чинник впливу штучного інтелекту на кібербезпеку і безпеку в цілому: йдеться про його системний аналіз, який базується на тріаді «AI як актив (AI as a protected asset), що захищається, - AI як засіб підсилення захисту інформаційного (кібер) активу (AI powered protection) – AI як засіб для підсилення атаки (AI powered attack)» [10]. Окремої уваги потребують мобільні інтелектуальні гетерогенні системи як фактор безпеки критичних інфраструктур.

Ці заходи набувають особливої актуальності в умовах повномасштабної війни, яку веде Російська Федерація проти України, що супроводжується масованими кібератаками, інформаційними операціями та спробами дестабілізації критичної інфраструктури. У цьому багатовимірному ландшафті особливе значення набувають кіберполігони – спеціалізовані платформи для моделювання, тестування та тренування реагування на кіберінциденти. Вони дозволяють відпрацьовувати сценарії атак, перевіряти ефективність захисних механізмів, навчати персонал у реалістичних умовах та формувати міжвідомчу координацію. Для України, яка перебуває на цифровому фронті війни, створення національних кіберполігонів є критично важливим кроком: це не лише інструмент підготовки, а й простір для інновацій, обміну досвідом та інтеграції в європейські та міжнародні тренувальні програми.

Стратегічне геополітичне положення України – на східних теренах Європи, які межують з Азією Європи та Азії – робить її не лише об'єктом, а й потенційним щитом цифрової безпеки для всього європейського регіону. Водночас, транскордонний характер сучасних загроз, зокрема транснаціональної кіберзлочинності, вимагає від України активної участі в міжнародних механізмах протидії: від обміну оперативною інформацією до спільних розслідувань і правового співробітництва. Таким чином, імплементація положень NIS2 для України – це не лише крок до євроінтеграції, а й стратегічна відповідь на виклики війни, геополітичної нестабільності та глобальної цифрової конкуренції. Це шанс побудувати сучасну, стійку, захищену кіберекосистему, здатну не лише протистояти загрозам, жорстко і проактивно відповідати на них, але й формувати нові стандарти безпеки та резильєнтності в регіоні, ставати об'єктивним методологічним і технологічним лідером за цим напрямом.

Бібліографічні посилання

1. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua?form=MG0AV3&form=MG0AV3 (дата звернення: 28.09.2025).

2. Oleksii Lytvynov, Nataliia Filipenko, Hanna Spitsyna, Aleksandar Ivanović (2024) Cyberpolygon - the practice of protecting critical infrastructure facilities and aerospace industry enterprises from cyberterrorist attacks - the experience of Ukraine and the world (review article). Архів кримінології та судових наук : наук. журн. Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2024. №. 2 (10) 2024. 244 с. С. 50-60.

3. Директива Європейського Парламенту І Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). Офіційний портал Верховної ради України. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 11.10.2025).

4. Filipenko, N., Pavlykivskyi, V., Lukashevych, S., Trofymenko, V., Teteriatnyk, H. (2025). Categorical and Conceptual Framework and Legal Regulation Protection and Resilience of Critical Infrastructure. In: Lytvynov, O., Pavlikov, V., Krytskyi, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2024. ICTM 2024. Lecture Notes in Networks and Systems, vol 1474. Springer, Cham. https://doi.org/10.1007/978-3-031-94852-7_9

5. The European Union: Foreign and SecurityPolicy. Congressional Research Service. URL: https://www.fas.org/sgp/crs/row/R41959.pdf (дата звернення: 16.10.2025).

6. Council Recommendationof 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure 2023/C 20/01. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content /EN/TXT/ ?uri =CELEX :32023H0120(01) (дата звернення: 13.10.2025).

7. Горбачова В. Правове забезпечення захисту та стійкості критичної інфраструктури в Європейському союзі. Пропілеї права та безпеки, 2025. №6-7. С. 41-43. DOI: https://doi.org/ 10.32620/pls.2025.67.08.

8. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. Офіційний портал Верховної ради України. URL: https://zakon.rada.gov.ua/ laws/show/984_013-16#Text. Втратила чинність! (дата звернення: 11.10.2025).

9. Kharchenko, V., Paturej, A. Potii, O. (Editors). Manual on Cybersecurity, Reliability and Resilience Assurance in the Critical Industries. International Centre for Chemical Safety and Security, Warsaw, 2024. – 228 p.

10. Veprytska, O., Kharchenko, V., Illiashenko, O. Cybersecurity and Artificial Intelligence: Triad-Based Analysis and Attacks Review. Cybernetics and Information Technologies, 2025. Volume 25. № 3. P. 156-185. DOI: 10.2478/cait-2025-0028

Filipenko N., Kharchenko V., Lukashevych S.

The Evolution of the European Union's Security Policy: From the NIS1 Directive to the NIS2 Directive (Review Article)

Abstract. This article explores the evolution of cybersecurity regulation within the European Union, focusing on the transition from Directive NIS1 (2016/1148/EU) to its enhanced successor, NIS2 (2022/2555/EU). The study provides a comparative analysis of both directives, examining their scope, regulatory stringency, enforcement mechanisms, and sanctioning frameworks. Particular attention is paid to the implications of these legislative shifts for Ukraine, which has become a persistent target of large-scale cyberattacks in recent years–especially in the context of the full-scale war launched by the Russian Federation. These attacks have exposed critical vulnerabilities in Ukraine's digital infrastructure and underscored the strategic importance of national cyber resilience as a pillar of state security.

The authors argue that technical expertise alone is insufficient to counter modern cyber threats without a robust legal foundation. In this regard, harmonizing Ukrainian cybersecurity legislation with the provisions of NIS2 is presented not only as a necessary step toward EU accession, but also as a means of strengthening the protection of critical infrastructure and aligning with European standards of digital governance. The article outlines the practical and institutional challenges of implementing NIS2-compliant frameworks in Ukraine, including the need for coordinated oversight, transparent reporting, and accountability across both public and private sectors.

Furthermore, the study highlights the broader geopolitical and normative significance of adopting EU cybersecurity standards in Ukraine's legal system. It emphasizes the role of NIS2 in fostering cross-border cooperation, enhancing supply chain security, and establishing a unified response to cyber crises through mechanisms such as EU-CyCLONe. By situating Ukraine's cybersecurity reform within the trajectory of European integration, the article contributes to the discourse on digital sovereignty, resilience, and legal modernization in times of hybrid warfare.

Keywords: security policy, cybersecurity, Directive NIS1, Directive NIS2, European Union, Ukraine, critical infrastructure, cyber resilience, legal regulation, digital security, EU integration, hybrid warfare.

Зразок для цитування:

Філіпенко Н., Харченко В., Лукашевич С. Еволюція безпекової політики Європейського союзу і контексті нових кіберзагроз: від директиви nis1 до директиви nis2 (оглядова стаття). Пропілеї права та безпеки, 2025. № 8. С. 34-42. DOI: https://doi.org/10.32620/pls.2025.8.03.