# *ТРАНСПОНУВАННЯ ДИРЕКТИВИ NIS2 У СЛОВАЧЧИНІ: ПОРІВНЯЛЬНО-ПРАВОВІ ОРІЄНТИРИ ДЛЯ РЕФОРМУВАННЯ ЗАКОНОДАВСТВА УКРАЇНИ*[I]*

УДК 341.217(4-6ЄС):004.056.5
DOI https://doi.org/10.32782/ehrlichsjournal-2026-18.03

**ОЛЕНА БІЛОСКУРСЬКА**
***кандидат юридичних наук, доцент, доцент кафедри публічного права***
**Чернівецького національного університету імені Юрія Федьковича, Україна**
*o.biloskurska@chnu.edu.ua*
*ORCID: 0000-0003-1005-2165*

**ІГОР КОВБАС**
***доктор юридичних наук, професор, завідувач кафедри публічного права***
**Чернівецького національного університету імені Юрія Федьковича, Україна**
*ig.kovbas@chnu.edu.ua*
*ORCID: 0000-0001-7039-1586*

**КАТЕРИНА СОЛОДАН**
***доктор філософії (з права), асистент кафедри публічного права***
**Чернівецького національного університету імені Юрія Федьковича, Україна**
*k.solodan@chnu.edu.ua*
*ORCID: 0000-0002-2872-5332*

*Анотація.* У статті здійснено порівняльно-правове дослідження транспонування Директиви (ЄС) 2022/2555 (NIS2) про заходи для високого спільного рівня кібербезпеки в Європейському Союзі у Словацькій Республіці та оцінено потенційний вплив словацької імплементаційної моделі на правопорядок України. Відправною точкою аналізу стало доктринальне розмежування категорій апроксимації, транспонування, імплементації, гармонізації та адаптації права, які донині нерідко вживаються у вітчизняному дискурсі як синонімічні. Обґрунтовано, що для держави – члена ЄС імперативним є транспонування нормативного акта, тоді як для України, яка перебуває у статусі кандидата й не має прямого юридичного обов'язку безпосереднього перенесення тексту Директиви, йдеться про режим випереджальної адаптації під впливом зовнішньої фінансово-правової зумовленості.

Проаналізовано передумови заміни Директиви (ЄС) 2016/1148 (NIS), зокрема фрагментацію національних режимів, надмірну дискрецію держав під час визначення операторів основних послуг та неповноту секторального охоплення.

Досліджено словацьку модель, оформлену Законом № 366/2024 Z. z. шляхом внесення змін до Закону № 69/2018 Z. z. про кібербезпеку. З'ясовано, що словацький законодавець відтворив логіку Директиви практично дослівно, доповнивши її національними розширеннями: покладенням обов'язків на третіх осіб, запровадженням сертифікації окремих ІСТ-продуктів та охопленням органів місцевого самоврядування. Зіставлення української та словацької юридичних конструкцій проведено за шістьма визначеними критеріями: способом визначення кола зобов'язаних суб'єктів, інституційною архітектурою нагляду, обсягом обов'язків з управління ризиками, режимом сповіщення, інститутом відповідальності та наглядово-санкційним інструментарієм. Сформульовано авторську типологію моделей транспонування європейських актів у державах Центрально-Східної Європи та окреслено межі й ризики запозичення словацького досвіду в умовах правового режиму воєнного стану.

[i] Публікація підготовлена в межах виконання науково-дослідної роботи «Транспозиція Директиви NIS2 у Словаччині та її вплив на правопорядок України: порівняльно-правове дослідження» (Державний реєстраційний номер 0126U004639; договір із МОН України № М/59-2026 від 31.08.2026) за фінансової підтримки Міністерства освіти і науки України в рамках міжнародного науково-технологічного співробітництва відповідно до Протоколу 7-го засідання Спільного українсько-словацького Комітету з питань науково-технічного і технологічного співробітництва від 08.04.2025 та Рішення про співфінансування словацько-українських спільних проєктів на 2026–2028 рр. від червня 2026 р.

*Ключові слова:* Директива NIS2; транспонування; кібербезпека; Словацька Республіка; механізми наближення законодавства; гармонізація права; державні органи; європейські стандарти; цифровий простір; штучний інтелект.

# *TRANSPOSITION OF THE NIS2 DIRECTIVE IN SLOVAKIA: COMPARATIVE LEGAL BENCHMARKS FOR REFORMING UKRAINIAN LEGISLATION*[II]

UDC 341.217(4-6ЄС):004.056.5
DOI https://doi.org/10.32782/ehrlichsjournal-2026-18.03

**OLENA BILOSKURSKA**
***PhD in Law, Associate Professor, Associate Professor at the Department of Public Law***
**Yuriy Fedkovych Chernivtsi National University, Ukraine**
*o.biloskurska@chnu.edu.ua*
*ORCID: 0000-0003-1005-2165*

**IHOR KOVBAS**
***Doctor of Law, Professor, Head of the Department of Public Law***
**Yuriy Fedkovych Chernivtsi National University, Ukraine**
*ig.kovbas@chnu.edu.ua*
*ORCID: 0000-0001-7039-1586*

**KATERYNA SOLODAN**
***PhD in Law. Assistant Professor at the Department of Public Law***
**Yuriy Fedkovych Chernivtsi National University, Ukraine**
*k.solodan@chnu.edu.ua*
*ORCID: 0000-0002-2872-5332*

*Abstract.* The article provides a comparative legal analysis of the transposition of Directive (EU) 2022/2555 (NIS2), on measures for a high common level of cybersecurity across the European Union, in the Slovak Republic and assesses the potential impact of the Slovak transposition model on the Ukrainian legal order. The starting point of the analysis is the doctrinal distinction between the concepts of approximation, transposition, implementation, harmonisation and adaptation of law, which continue to be frequently used interchangeably in Ukrainian legal discourse. It is argued that, for an EU Member State, transposition of a legal act is mandatory, whereas Ukraine, which holds candidate status and is not under a direct legal obligation to transpose the text of the Directive, is pursuing a process of anticipatory legal adaptation driven by external financial and legal conditionality.

The article examines the reasons for replacing Directive (EU) 2016/1148 (NIS), including the fragmentation of national regulatory frameworks, excessive discretion afforded to Member States in identifying operators of essential services, and incomplete sectoral coverage.

The Slovak model, established by Act No. 366/2024 Coll., amending Act No. 69/2018 Coll. on Cybersecurity, is analysed. It is established that the Slovak legislature reproduced the logic of the Directive almost verbatim, while supplementing it with national extensions, including the imposition of obligations on third parties, the introduction of certification for certain ICT products, and the inclusion of local self-government bodies within its scope. The Ukrainian and Slovak legal frameworks are compared against six predefined criteria: the method

[ii] The publication was prepared within the framework of the research project «Transposition of the NIS2 Directive in Slovakia and Its Impact on the Legal Order of Ukraine: A Comparative Legal Study» (State Registration Number: 0126U004639; Agreement with the Ministry of Education and Science of Ukraine No. M/59-2026 dated 31 August 2026), with the financial support of the Ministry of Education and Science of Ukraine within the framework of international scientific and technological cooperation, pursuant to the Protocol of the 7th Meeting of the Joint Ukrainian-Slovak Committee on Scientific, Technical and Technological Cooperation dated 8 April 2025 and the Decision on Co-Financing of Slovak-Ukrainian Joint Projects for 2026–2028, dated June 2026.

for determining the entities subject to obligations, the institutional architecture of supervision, the scope of risk-management obligations, the incident-notification regime, the liability framework, and the supervisory and enforcement instruments. The article proposes an original typology of models for transposing European legal acts in Central and Eastern European countries and outlines the limits and risks of drawing on Slovak experience under Ukraine's martial law regime.

*Key words:* NIS2 Directive; transposition; cybersecurity; Slovak Republic; mechanisms for the approximation of legislation; harmonisation of law; public authorities; European standards; digital space; artificial intelligence.

---

**Постановка проблеми.** Упродовж останнього десятиліття кіберзахист об'єктів критичної інфраструктури сформувався як предмет самостійного правового регулювання, у межах якого держава визначає коло зобов'язаних осіб, зміст їхніх обов'язків та наслідки невиконання. Директива (ЄС) 2022/2555 від 14 грудня 2022 р. закріпила відповідний підхід на загальноєвропейському рівні, скасувавши Директиву (ЄС) 2016/1148 та встановивши для держав-членів граничний строк транспонування її норм до 17 жовтня 2024 р. [1]. Отримавши статус держави-кандидата, Україна постала перед необхідністю узгодження національної архітектури кіберзахисту з правовою рамкою Європейського Союзу. Складність цього завдання зумовлена тим, що вітчизняне законодавство формувалося в умовах збройної агресії російської федерації проти України й спрямоване першочергово на забезпечення потреб оборони, а не на забезпечення правового комплаєнсу. У цьому контексті виникає практична проблема щодо визначення правових конструкцій європейського акта, які є придатними для рецепції у національну систему, та тих, що потребують істотної адаптації. Відповідь на це питання неможливо отримати безпосередньо з тексту Директиви, оскільки вона залишає державам-членам свободу вибору форми та засобів досягнення мети, а отже, реальний зміст регулювання розкривається лише на рівні національних імплементаційних актів. Відповідно, постає потреба в аналізі досвіду держав, чиї вихідні умови є зіставними з українськими. Дефінітивним прикладом такої держави є Словацька Республіка, для якої характерні подібний масштаб економіки, наявність спільного кордону, подібність успадкованих енергетичних і транспортних мереж, постсоціалістична інституційна спадщина, а також успішно пройдений шлях від набуття статусу кандидата до повноправного членства в ЄС. Водночас словацька модель імплементації, попри її високу релевантність, практично не потрапляла в поле зору української юридичної науки, а наявні узагальнення європейського досвіду переважно обмежуються аналізом тексту самої Директиви без дослідження правозастосовної практики на рівні національних актів держав-членів.

Понятійні засади гармонізації вітчизняного законодавства з правом Європейського Союзу розробив О. В. Тарасов, довівши, що розмежування категорій «адаптація», «імплементація» та «гармонізація» є фундаментальним для розрізнення добровільного наближення норм і зобов'язального транспонування [2].

Теоретико-правові та прикладно-орієнтовані аспекти Директиви NIS2 висвітлено у працях вітчизняних дослідників. В. Ю. Зубок, А. В. Давидюк і Т. М. Клименко деталізували нову категоризацію об'єктів і секторів [3], О. П. Федієнко узагальнив європейську модель кіберстійкості [4], а низка науковців констатувала низький рівень гармонізації у сфері сертифікації, кадровий дефіцит і міжвідомчу неузгодженість [5].

У зарубіжному доктринальному дискурсі зміну регуляторної парадигми розкрито T. Sievers [6], тоді як D. Markopoulou, V. Papakonstantinou і P. De Hert обґрунтували вичерпаність попередньої дискреційної моделі [7]. На дефіцит правової визначеності щодо порога значущості інцидентів указує S. Schmitz-Berndt [8], а F. Casarosa та G. Comandé довели ризик національної фрагментації через розбіжності у транспонуванні норм державами-членами [9]. Політико-правовий вимір Директиви як інструменту цифрового суверенітету ЄС опрацювали M. Kianpour, P. A. Earls Davis, I. M. Windekilde [10]. Прикладну словацьку модель кіберстійкості сформулювали J. Ristvej, M. Tonhauser, D. Chovanec, J. Kubáš, B. Kollár і Z. Zamiar [11]. Питання формування права на кібербезпеку – P. Chiara [12], а нові механізми сертифікації та міждержавної солідарності – M. Rampášek et al. [13], A. Khurshid et al. [14] та S. Villani [15].

Вітчизняний інституційно-безпековий контекст досліджувався через порівняльний аналіз підходів ЄС і НАТО [14], оцінку кіберзахисту критичної інфраструктури [17], поліцентричність системи органів [18] та воєнну трансформацію профілю кіберзагроз в енергетиці [19].

Утім, за наявності вагомого теоретичного доробку поза увагою дослідників залишається низка суттєвих аспектів.

Вітчизняна правнича наука досліджує європейський акт переважно в його первинному, наднаціональному вимірі, зіставляючи національні норми безпосередньо з текстом Директиви. Подібний підхід залишає поза увагою суттєвий аспект: Директива не володіє прямою дією, а набуває практичного змісту виключно через національні імплементаційні акти, змістовні рішення яких можуть суттєво різнитися між державами-членами. Словацька модель, оформлена законодавчими новелами до чинного Закону про кібербезпеку, досі не ставала предметом окремого теоретичного аналізу у вітчизняній доктрині. Саме вона демонструє приклад розв'язання практичних питань категоризації суб'єктів, їх реєстрації, диференціації наглядових режимів та формування санкційної шкали державою із зіставним інституційним спадком.

Наявні наукові праці або констатують загальну потребу в гармонізації законодавства, або пропонують відповідні «дорожні карти», проте не порушують зворотного питання: які саме конструкції європейського акта є непридатними для держави, що веде оборонну війну, частина об'єктів критичної інфраструктури якої перебуває під тимчасовою окупацією. Досі відсутня й типологія моделей транспонування, яка б дала змогу розглянути український досвід у порівняльно-правовому контексті держав Центрально-Східної Європи.

**Метою статті** є виявлення особливостей словацької моделі транспонування Директиви NIS2, зіставлення її з чинним правовим регулюванням України та визначення правових меж і можливостей використання словацького досвіду в процесі адаптації українського законодавства.

У цьому контексті доцільним убачається розмежування понятійного апарату гармонізації права України з правом Європейського Союзу. Апроксимація означає прийняття, зміну чи скасування правових норм задля встановлення механізмів наближення законодавства України до актів іншої держави або міжнародного об'єднання без вимоги щодо досягнення повної тотожності. Транспонування є вужчою та суворішою категорією, яка позначає перенесення положень Директиви задля досягнення ідентичності юридичного результату, і застосовується виключно у відносинах між державою-членом та Європейським Союзом. Імплементація охоплює правотворчу і правозастосовну діяльність із реалізації узятих зобов'язань, гармонізація – усунення суперечностей і досягнення системної сумісності правопорядків, а адаптація постає як найширший процес приведення національного масиву законодавства у відповідність до acquis [2]. З огляду на це, можна зробити висновок, що Словацька Республіка зобов'язана досягти визначеного результату під загрозою застосування процедури порушення, тоді як Україна діє у режимі добровільного випереджального наближення. Відповідно, механічне перенесення словацьких нормативних рішень без урахування цієї відмінності у правових статусах є методологічно хибним.

Слід зауважити, що Директива (ЄС) 2016/1148 (NIS) передбачала інформування лише про суттєві інциденти, що звужувало можливості їх своєчасного виявлення. Натомість NIS2 розширила обсяг інформації, яку необхідно оприлюднювати, посиливши відповідні зобов'язання суб'єктів, але не сформувала єдиних і послідовних рекомендацій щодо їх виконання, унаслідок чого виникли додаткові труднощі зумовлені відсутністю однозначного тлумачення понять, пов'язаних із хмарними сервісами та певною правовою невизначеністю щодо обсягу обов'язків із розкриття інформації та вимог до третіх сторін. У такій ситуації компетентні державні органи вимушені самостійно узгоджувати інструменти оцінювання, які суттєво різняться за рівнем якості та періодичністю застосування. Утворений певний вакуум нормативної визначеності створює перешкоди під час координації дій держав-членів і суб'єктів під час кризових ситуацій та виступає предметом критики з боку представників індустрії, зокрема компанії Microsoft [20].

Словаччина транспонувала Директиву NIS2 не через ухвалення окремого спеціального закону, а через внесення змін до чинного Закону № 69/2018 Z. z. про кібербезпеку [21]. Імплементаційним актом став Закон № 366/2024 Z. z., схвалений Національною радою 28 листопада 2024 р., оприлюднений у Збірнику законів 19 грудня 2024 р. та чинний із 01 січня 2025 р. [22]. Компетентним органом і єдиним національним контактним пунктом залишилося Національне бюро безпеки, тоді як практичне реагування на інциденти забезпечує Національний центр реагування.

Словацька юридична конструкція відтворює логіку Директиви майже дослівно: суб'єкти самостійно оцінюють свою відповідність критеріям належності до регульованих секторів, реєструються

у компетентному органі протягом 60 днів, а національна термінологія розрізняє операторів базової послуги та операторів критичної базової послуги, що функціонально відповідає європейському поділу на важливі та ключові суб'єкти. Механізми самоідентифікації через електронні інструменти, ведення реєстру операторів і багатоетапний режим сповіщення транспоновано без істотних відхилень.

Разом із тим в окремих аспектах словацька модель виявилася радше розширювальною, ніж мінімалістичною. Закон визнає самостійно зобов'язаними суб'єктами третіх осіб, які мають суттєвий вплив на стан кібербезпеки та уклали договір з оператором критичної базової послуги, запроваджує обов'язкову сертифікацію окремих продуктів інформаційно-комунікаційних технологій і деталізовані технічні вимоги до інформаційних та операційних систем, а також, скориставшись дискреційними опціями Директиви, поширює дію нормативних вимог на органи місцевого самоврядування, вилучаючи при цьому сфери національної безпеки й оборони. Орієнтація на інститут сертифікації у цьому контексті є не випадковою: розвиток стандартизації та підтвердження відповідності дедалі виразніше перебирає на себе функцію регулятивного впливу, яку раніше виконувало пряме нормотворення, зокрема стосовно продуктів із компонентом штучного інтелекту [13; 14].

Згідно з пояснювальною запискою до імплементаційного акта, законодавець розраховував, що новела охопить щонайменше 3 403 організації та врегулює понад 80 послуг у 16 галузях, хоча подальші неофіційні оцінки компетентного органу зросли приблизно до 14 тис суб'єктів. Шкала фінансових санкцій сягає 500 тис євро за окремі види порушень, а перехідні положення дають змогу операторам до 31 грудня 2026 р. застосовувати заходи кіберзахисту за попередньою редакцією закону. Показово, що Європейська Комісія 07 травня 2025 р. надіслала обґрунтовані висновки 19 державам-членам за неповне транспонування норм Директиви, і Словаччини серед них немає [23], що підтверджує нормативне завершення процесу на початку 2025 р. Отже, досвід Словаччини є прикладом дещо запізнілого, але практично дослівного і подекуди суворішого за європейські мінімальні стандарти транспонування. Утім, розбіжності між національними актами держав-членів залишаються настільки відчутними, що ставлять під сумнів досяжність повної гармонізації у цій сфері [9].

Українська модель побудована на відмінній правовій логіці. Зокрема, Закон України «Про основні засади забезпечення кібербезпеки України» визначає національну систему кібербезпеки, проводить розмежування між кіберзахистом об'єктів критичної інформаційної інфраструктури й загальним захистом державних інформаційних ресурсів та закріплює принцип мінімально необхідного регулювання [24]. Інституційна архітектура є багатосуб'єктною: формування політики та координацію забезпечує Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України [25], технічний кіберзахист державних ресурсів і діяльність урядової команди реагування – Державна служба спеціального зв'язку та захисту інформації, а протидію кіберзлочинності й контррозвідувальний захист – Служба безпеки України. Поліцентричність цієї конструкції неодноразово фіксувалася у доктрині як її структурна ознака [18], а неповнота та фрагментарність контрольно-наглядових механізмів – як її слабке місце [17]. Закон України «Про критичну інфраструктуру» доповнює цю архітектуру реєстровим підходом, за яким оператори розробляють паспорти безпеки та плани стійкості, однак сам Закон відсилає урегулювання питань кіберзахисту до спеціального законодавства [26]. Також варто зауважити, що в законодавстві України механізми цивільно-правової відповідальності топ-менеджменту за незадовільний стан кіберзахисту є недостатньо сформованими, а санкції співмірної фінансової ваги за порушення вимог регуляторного комплаєнсу нині відсутні.

Пропонуємо здійснити порівняльно-правовий аналіз транспонування директиви NIS2 у Словаччині та її наближення в Україні за окремими критеріями. Так, за способом визначення кола зобов'язаних суб'єктів Словаччина застосовує автоматичний секторальний підхід із процедурою самоідентифікації, тоді як Україна зберігає реєстрово-категоризаційний підхід, за яким суб'єкт підпадає під регуляторний контроль виключно через внесення до відповідного переліку, а не через факт перевищення критеріїв розміру чи фінансових показників у визначеному секторі. За інституційною архітектурою словацька система має єдиний регуляторний центр тяжіння – Національне бюро безпеки, тоді як українська ж система функціонує в умовах розподілу повноважень між кількома суб'єктами, що періодично спричиняє міжвідомчу неузгодженість [5]. За обсягом обов'язків з управління ризиками словацьке законодавство дослівно відтворює європейський перелік і додатково запроваджує обов'язкову сертифікацію, тоді як українські нормативно-правові вимоги залишаються менш деталізованими та фрагментарними.

За режимом сповіщення Словаччина запровадила імперативну багатоетапну модель інформування, тоді як Україна лише перебуває на етапі нормативного формування чітких строкових зобов'язань. За інститутом відповідальності словацька модель запровадила персональну відповідальність керівного складу та штрафні санкції, прив'язані до річного обороту суб'єкта, тоді як в Україні відповідний режим відповідальності залишається переважно адміністративним із низьким рівнем стримувального ефекту. За наглядовими інструментами словацька конструкція чітко диференціює проактивний та реактивний контроль, тоді як українська політика у цій сфері фрагментарна. Відсутність поділу суб'єктів на дві категорії з різними наглядовими режимами й досі становить одну з найпомітніших системно-структурних розбіжностей між порівнюваними правопорядками [3].

Реагуючи на окреслені нормативні прогалини та зовнішню зумовленість, Верховна Рада України 27 березня 2025 р. ухвалила Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [27]. Даний нормативно-правовий акт створює єдину національну систему реагування на кібератаки, запроваджує посади керівників із кіберзахисту в органах державної влади та на об'єктах критичної інформаційної інфраструктури та формує мережу національних, секторальних і регіональних команд реагування. Таким чином, вітчизняне регулювання наблизилося до європейської правової рамки, проте воно охопило переважно державний сектор і не відтворило принципу секторального автоматизму в повному обсязі. Якщо припустити, що подальші законодавчі кроки відбуватимуться у логіці фрагментарних змін, розрив між реєстровим та автоматичним способами визначення зобов'язаних суб'єктів зберігатиметься, а разом із ним триватиме й дискреція, від якої європейський законодавець свідомо відмовився.

Нормативні підстави міжнародно-правових зобов'язань України закладені у змісті Угоди про асоціацію, глава якої про інформаційне суспільство передбачає поступове наближення законодавства у сфері електронних комунікацій та цифрових послуг [28], а також у переговорній рамці щодо вступу до ЄС, у межах якої напрям кібербезпеки віднесено до розділу, за яким Україна вже пройшла процедуру офіційного скринінгу [29]. Додатковим джерелом зумовленості стала програма фінансової підтримки Європейського Союзу, у якій реформа кіберзахисту та наближення до європейських стандартів закладені як імперативна умова отримання допомоги, що надає процесу адаптації не лише декларативного, а й фінансово-зобов'язального характеру. Саме ця зовнішня зумовленість пояснює оперативне ухвалення профільного Закону навесні 2025 р. та підтверджує тезу про формування у праві Європейського Союзу самостійного виміру цифрового суверенітету, дія якого поширюється й на держави-кандидати [10; 12].

Повномасштабне вторгнення російської федерації докорінно змінило логіку нормативного регулювання, перевівши кіберзахист із площини регуляторного комплаєнсу у площину забезпечення національної безпеки та виживання держави. Окремим проблемним аспектом залишається недостатня узгодженість механізмів повідомлення про кіберінциденти, обміну інформацією та формування міжсуб'єктної довіри. Директива NIS2 запроваджує поетапну процедуру інформування про значні інциденти, що передбачає, зокрема, подання первинного сповіщення протягом 24 годин. Зважив ши на високу інтенсивність кібератак в Україні, особливої актуальності набуває забезпечення оперативного виявлення та класифікації інцидентів, своєчасного повідомлення про них і налагодження міжвідомчого обміну технічними індикаторами компрометації. Спостерігається стрімке зростання кількості кіберінцидентів, що вказує на необхідність деталізованого нормативного врегулювання процедур інформаційного обміну, зокрема за участю приватного сектору, із дотриманням гарантій конфіденційності. Велике значення у цьому контексті мають розвиток інституційної довіри до цифрових послуг та належне забезпечення їхньої кіберстійкості за допомогою організаційно-правових інструментів, що є передумовою ефективного реагування на кіберзагрози [30].

Масштабна атака на найбільшого мобільного оператора у грудні 2023 р., яка спричинила збій у наданні послуг зв'язку для мільйонів абонентів, а також кібератака на державні реєстри у грудні 2024 р. підтверджують критичність цієї проблеми. Дослідження стійкості об'єктів енергетичної інфраструктури в умовах воєнного стану засвідчують, що профіль загроз і вимоги до реагування суттєво відрізняються від умов мирного часу [19]. Такі обставини доводять, що європейська модель із її

обов'язковим сповіщенням, управлінням ризиками та безпекою ланцюгів постачання є для України не абстрактною формальністю, а безпековою потребою.

Водночас сумісність такої моделі з режимом воєнного стану залишається проблемною: частина критичної інфраструктури перебуває під військовим управлінням, частина об'єктів – на тимчасово окупованих територіях, а окремі процедури Директиви, зокрема публічність реєстрів та участь приватних суб'єктів у наглядових процедурах, складно узгодити з вимогами охорони державної та воєнної таємниці. Досвід держав-членів і структур НАТО щодо розподілу повноважень між безпековими та цивільними органами дає лише часткову відповідь, оскільки жодна із цих держав не функціонувала в умовах повномасштабної оборонної війни [16].

Звідси випливає ключовий ризик, який доцільно кваліфікувати як «формальну рецепцію»: існує ймовірність ситуації, коли закон буде ухвалено, проте кадрового, технічного та координаційного ресурсу для його належного виконання бракуватиме. Модель кіберстійкості, побудована безпосередньо на основі словацьких нормативно-правових актів, розрахована на середовище зі сформованою усталеною наглядовою практикою та передбачуваним бюджетним фінансуванням [11], тоді як український правопорядок характеризується дефіцитом профільних фахівців і міжвідомчою конкуренцією. Часткову компенсацію у цій ситуації може забезпечити залучення України до європейських механізмів солідарності, які передбачають спільне реагування на масштабні інциденти та використання резерву кіберспроможностей [15]. Утім, участь держави, яка не є членом Європейського Союзу, у таких механізмах потребує окремого міжнародно-правового оформлення та не заміщує розвитку внутрішньої інституційної спроможності. Попри це, поєднання накопиченого Україною унікального практичного досвіду протидії комплексним кібератакам із європейськими нормативними стандартами створює передумови для посилення її ролі у забезпеченні загальноєвропейської безпеки [5].

Отже, узагальнюючи вищевикладене, зазначимо, що процес гармонізації права у сфері кібербезпеки для Словацької Республіки є транспонуванням у вузькому юридичному сенсі, тоді як для України він має характер випереджальної адаптації. Указана відмінність статусів зумовлює необхідність вибіркової рецепції словацького досвіду з його обов'язковою верифікацією на сумісність із режимом воєнного стану.

Релевантними для запозичення у вітчизняний правопорядок є такі елементи словацької моделі, як секторальний автоматизм визначення суб'єктів та інститут їх самоідентифікації, диференціація суб'єктів на дві категорії із застосуванням пропорційних режимів нагляду, імперативна багатоетапна модель сповіщення про кіберінциденти, персональна юридична відповідальність керівного складу.

Формування джерельної бази дослідження ускладнюється відсутністю сталого масиву правозастосовної практики внаслідок дії перехідних положень словацького імплементаційного акта до 31 грудня 2026 р. Оновлення системи законодавства України за відсутності належного інституційного й кадрового забезпечення та подолання міжвідомчої неузгодженості створюють ризик «формальної рецепції». Перспективним напрямом подальших досліджень є моніторинг наглядової практики Словаччини після завершення перехідного періоду та її зіставлення з першими результатами застосування оновленого законодавства України.

## ВИКОРИСТАНІ МАТЕРІАЛИ

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

2. Тарасов О. В. Адаптація, імплементація чи гармонізація права ЄС? *Європейська інтеграція в контексті сучасної геополітики*. Харків : Право, 2016. С. 30–39. URL: https://dspace.nlu.edu.ua/bitstreams/65ab0a50-5c9a-4349-8c7a-a01edaa8e9cf/download

3. Zubok V., Davydiuk A., Klymenko T. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555. *Електронне моделювання*. 2023. Т. 45, № 5. P. 54–66. DOI: https://doi.org/10.15407/emodel.45.05.054

4. Федієнко О. П. Європейський досвід законодавчого забезпечення посилення кіберстійкості. *Інформація і право*. 2024. № 2 (49). С. 178–189. URL: https://il.ippi.org.ua/article/download/306208/345660

5. Крайнюк О., Євсеєв С., Діденко Н., Піксасов М. Трансформація нормативно-правового поля кібербезпеки України: аналіз відповідності вимогам директиви NIS2 та Закону про кібербезпеку. *Територія безпеки*. 2025. Т. 1, № 3. С. 40–48. DOI: https://doi.org/10.20998/3083-6298.2025.03.05

6. Sievers T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021. Vol. 2, Iss. 2. P. 223–231. DOI: https://doi.org/10.1365/s43439-021-00033-8

7. Markopoulou D., Papakonstantinou V., De Hert P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*. 2019. Vol. 35, Iss. 6. Art. 105336. DOI: https://doi.org/10.1016/j.clsr.2019.06.007

8. Schmitz-Berndt S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*. 2023. Vol. 9, Iss. 1. Art. tyad009. DOI: https://doi.org/10.1093/cybsec/tyad009

9. Casarosa F., Comandé G. Implementing the NIS 2 Directive: towards harmonisation or further fragmentation? *CEUR Workshop Proceedings*. 2026. Vol. 4198. Paper 19. URL: https://ceur-ws.org/Vol-4198/paper19.pdf

10. Kianpour M., Earls Davis P. A., Windekilde I. M. Digital sovereignty in practice: analyzing the EU's NIS2 directive. *International Journal of Information Security*. 2025. Vol. 24, Iss. 4. Art. 167. DOI: https://doi.org/10.1007/s10207-025-01090-4

11. Ristvej J., Tonhauser M., Chovanec D., Kubáš J., Kollár B., Zamiar Z. Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*. 2025. Vol. 15. Art. 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3

12. Chiara P. G. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*. 2024. Vol. 53. Art. 105961. DOI: https://doi.org/10.1016/j.clsr.2024.105961

13. Rampášek M., Mesarčík M., Andraško J. Evolving cybersecurity of AI-featured digital products and services: rise of standardisation and certification? *Computer Law & Security Review*. 2025. Vol. 56. Art. 106093. DOI: https://doi.org/10.1016/j.clsr.2024.106093

14. Khurshid A., Alsaaidi R., Aslam M., Raza S. EU Cybersecurity Act and IoT certification: landscape, perspective and a proposed template scheme. *IEEE Access*. 2022. Vol. 10. P. 129932–129948. DOI: https://doi.org/10.1109/ACCESS.2022.3225973

15. Villani S. The Cyber Solidarity Act: framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system. *European Journal of Risk Regulation*. 2025. DOI: https://doi.org/10.1017/err.2025.24

16. Shopina I., Khomiakov D., Khrystynchenko N., Zhukov S., Shpenov D. Cybersecurity: legal and organizational support in leading countries, NATO and EU standards. *Journal of Security and Sustainability Issues*. 2020. Vol. 9, Iss. 3. P. 977–992. DOI: https://doi.org/10.9770/jssi.2020.9.3(22)

17. Kovaliv M., Skrynkovskyy R., Nazar Y., Yesimov S., Krasnytskyi I., Kaydrovych K., Kniaz S., Kemska Y. Legal support of cybersecurity of critical information infrastructure of Ukraine. *Path of Science*. 2021. Vol. 7, Iss. 12. P. 2011–2018. DOI: https://doi.org/10.22178/pos.69-12

18. Svintsytskyi A. The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova*. 2022. Vol. 20, No. 38. DOI: https://doi.org/10.21830/19006586.903

19. Davydiuk A., Zubok V. Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*. Tallinn, 2023. P. 121–139. DOI: https://doi.org/10.23919/cycon58705.2023.10181813

20. Mentzelou K., Chountalas P. T., Kitsios F. C., Magoutas A. I., Dasaklis T. K. Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *J. Cybersecur. Priv.* 2025. Vol. 5. P. 97. DOI: https://doi.org/10.3390/jcp5040097

21. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. *Zbierka zákonov Slovenskej republiky*. 2018. URL: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

22. Zákon č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. *Zbierka zákonov Slovenskej republiky*. 2024. URL: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html

23. Commission calls on 19 Member States to fully transpose the NIS2 Directive: press release. *European Commission, Shaping Europe's digital future*. 2025. URL: https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive

24. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

25. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016

26. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 6. Ст. 42. URL: https://zakon.rada.gov.ua/laws/show/1882-20

27. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-IX

28. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. *Офіційний вісник України*. 2014. № 75, Т. 1. Ст. 2125. URL: https://zakon.rada.gov.ua/laws/show/984_011

29. Україна пройшла скринінг ЄС за розділом 10 «Цифрова трансформація та медіа». *Центр демократії та верховенства права*. URL: https://cedem.org.ua/news/ukrayina-proyshla-skryning/

30. Пролорензо А. Політико-правові засади гармонізації системи кібербезпеки України із законодавством Європейського Союзу: імплементація NIS2 та інституційна спроможність. *Вісник Прикарпатського університету. Серія «Політологія».* 2026. № 23. С. 184–196. DOI: https://doi.org/10.32782/2312-1815/2026-23-19

## REFERENCES

1. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80–152. Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

2. Tarasov, O. V. (2016). Adaptatsiia, implementatsiia chy harmonizatsiia prava YeS? [Adaptation, implementation or harmonisation of EU law?]. In *Yevropeiska intehratsiia v konteksti suchasnoi heopolityky* [European integration in the context of modern geopolitics] (pp. 30–39). Pravo. https://dspace.nlu.edu.ua/bitstreams/65ab0a50-5c9a-4349-8c7a-a01edaa8e9cf/download [in Ukrainian].

3. Zubok, V., Davydiuk, A., & Klymenko, T. (2023). Cybersecurity of critical infrastructure in Ukrainian legislation and in Directive (EU) 2022/2555. *Elektronne modeliuvannia* [Electronic Modeling], *45*(5), 54–66. https://doi.org/10.15407/emodel.45.05.054

4. Fediienko, O. P. (2024). Yevropeiskyi dosvid zakonodavchoho zabezpechennia posylennia kiberstiikosti [European experience of legislative support for strengthening cyber resilience]. *Informatsiia i pravo* [Information and Law], (2(49)), 178–189. https://il.ippi.org.ua/article/download/306208/345660 [in Ukrainian].

5. Krainiuk, O., Yevseiev, S., Didenko, N., & Piksasov, M. (2025). Transformatsiia normatyvno-pravovoho polia kiberbezpeky Ukrainy: analiz vidpovidnosti vymoham dyrektyvy NIS2 ta Zakonu pro kiberbezpeku [Transformation of the regulatory field of cybersecurity of Ukraine: Analysis of compliance with the requirements of the NIS2 Directive and the Cybersecurity Act]. *Terytoriia bezpeky* [Territory of Security], *1*(3), 40–48. https://doi.org/10.20998/3083-6298.2025.03.05 [in Ukrainian].

6. Sievers, T. (2021). Proposal for a NIS directive 2.0: Companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*, *2*(2), 223–231. https://doi.org/10.1365/s43439-021-00033-8

7. Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), Article 105336. https://doi.org/10.1016/j.clsr.2019.06.007

8. Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1), Article tyad009. https://doi.org/10.1093/cybsec/tyad009

9. Casarosa, F., & Comandé, G. (2026). Implementing the NIS 2 Directive: Towards harmonisation or further fragmentation? *CEUR Workshop Proceedings*, *4198*, Paper 19. https://ceur-ws.org/Vol-4198/paper19.pdf

10. Kianpour, M., Earls Davis, P. A., & Windekilde, I. M. (2025). Digital sovereignty in practice: Analyzing the EU's NIS2 directive. *International Journal of Information Security*, *24*(4), Article 167. https://doi.org/10.1007/s10207-025-01090-4

11. Ristvej, J., Tonhauser, M., Chovanec, D., Kubáš, J., Kollár, B., & Zamiar, Z. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*, *15*, Article 26902. https://doi.org/10.1038/s41598-025-12829-3

12. Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, *53*, Article 105961. https://doi.org/10.1016/j.clsr.2024.105961

13. Rampášek, M., Mesarčík, M., & Andraško, J. (2025). Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? *Computer Law & Security Review*, *56*, Article 106093. https://doi.org/10.1016/j.clsr.2024.106093

14. Khurshid, A., Alsaaidi, R., Aslam, M., & Raza, S. (2022). EU Cybersecurity Act and IoT certification: Landscape, perspective and a proposed template scheme. *IEEE Access*, *10*, 129932–129948. https://doi.org/10.1109/ACCESS.2022.3225973

15. Villani, S. (2025). The Cyber Solidarity Act: Framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.24

16. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards. *Journal of Security and Sustainability Issues*, *9*(3), 977–992. https://doi.org/10.9770/jssi.2020.9.3(22)

17. Kovaliv, M., Skrynkovskyy, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Kaydrovych, K., Kniaz, S., & Kemska, Y. (2021). Legal support of cybersecurity of critical information infrastructure of Ukraine. *Path of Science*, *7*(12), 2011–2018. https://doi.org/10.22178/pos.69-12

18. Svintsytskyi, A. (2022). The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova*, *20*(38). https://doi.org/10.21830/19006586.903

19. Davydiuk, A., & Zubok, V. (2023). Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 121–139). https://doi.org/10.23919/cycon58705.2023.10181813

20. Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., & Dasaklis, T. K. (2025). Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy*, *5*(4), 97. https://doi.org/10.3390/jcp5040097

21. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov [Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain acts]. (2018). *Zbierka zákonov Slovenskej republiky*. https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

22. Zákon č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony [Act No. 366/2024 Coll. amending and supplementing Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain acts, as amended, and amending and supplementing certain acts]. (2024). *Zbierka zákonov Slovenskej republiky*. https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html

23. European Commission. (2025). *Commission calls on 19 Member States to fully transpose the NIS2 Directive* [Press release]. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive

24. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity of Ukraine], Zakon Ukrainy No. 2163-VIII. (2017, October 5). *Vidomosti Verkhovnoi Rady Ukrainy*, (45), Art. 403. https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

25. Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky [On the National Cybersecurity Coordination Center], Ukaz Prezydenta Ukrainy No. 242/2016. (2016, June 7). https://zakon.rada.gov.ua/laws/show/242/2016 [in Ukrainian].

26. Pro krytychnu infrastrukturu [On critical infrastructure]. Zakon Ukrainy No. 1882-IX. (2021, November 16). *Vidomosti Verkhovnoi Rady Ukrainy*, 2022, (6), Art. 42. https://zakon.rada.gov.ua/laws/show/1882-20 [in Ukrainian].

27. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury [On amendments to certain laws of Ukraine regarding information protection and cyber defence of state information resources and critical information infrastructure facilities], Zakon Ukrainy No. 4336-IX. (2025, March 27). https://zakon.rada.gov.ua/laws/show/4336-IX [in Ukrainian].

28. Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony [Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part]. (2014). *Ofitsiinyi visnyk Ukrainy*, (75), Vol. 1, Art. 2125. https://zakon.rada.gov.ua/laws/show/984_011 [in Ukrainian].

29. Tsentr demokratii ta verkhovenstva prava. (n.d.). *Ukraina proishla skryninh YeS za rozdilom 10 «Tsyfrova transformatsiia ta media»* [Ukraine passed the EU screening under Chapter 10 «Digital Transformation and Media»]. https://cedem.org.ua/news/ukrayina-proyshla-skryning/ [in Ukrainian].

30. Prolorenzo, A. (2026). Polityko-pravovi zasady harmonizatsii systemy kiberbezpeky Ukrainy iz zakonodavstvom Yevropeiskoho Soiuzu: implementatsiia NIS2 ta instytutsiina spromozhnist [Political and legal principles of harmonizing Ukraine's cybersecurity system with European Union legislation: Implementation of NIS2 and institutional capacity]. *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia* [Bulletin of the Precarpathian University. Series: Political Science], (23), 184–196. https://doi.org/10.32782/2312-1815/2026-23-19 [in Ukrainian].

*Дата першого надходження статті до видання: 15.09.2026*
*Дата прийняття статті до друку після рецензування: 02.10.2026*
*Дата публікації (оприлюднення) статті: 16.11.2026*