

ГАРМОНІЗАЦІЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА З ACQUIS ЄС У СФЕРІ КІБЕРБЕЗПЕКИ: ОСНОВНІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ ДИРЕКТИВИ ЄС NIS2

Вінницький національний технічний університет

Анотація

У доповіді проаналізовано основні аспекти імплементації Директиви ЄС NIS2 в законодавство України. З'ясовано, що впровадження положень Директиви NIS2 є важливим етапом гармонізації українського законодавства з acquis ЄС у сфері кібербезпеки. Реалізація вимог NIS2 сприятиме підвищенню рівня захисту критичної інфраструктури, зміцненню кіберстійкості держави, інтеграції України до європейського цифрового простору та розвитку механізмів міжнародного співробітництва у сфері кібербезпеки. Обґрунтовано, що ефективна адаптація положень Директиви потребує комплексного оновлення законодавства, розвитку інституційної спроможності держави та формування сучасної культури кібербезпеки як у державному, так і в приватному секторах.

Ключові слова: кібербезпека, імплементація права ЄС, Директива NIS2, кіберстійкість, європейська інтеграція.

Abstract

The report analyzes the main aspects of the implementation of the EU NIS2 Directive into the legislation of Ukraine. It has been established that the implementation of the provisions of the NIS2 Directive constitutes an important stage in the harmonization of Ukrainian legislation with the EU acquis in the field of cybersecurity. The implementation of the NIS2 requirements will contribute to enhancing the protection of critical infrastructure, strengthening the cyber resilience of the state, integrating Ukraine into the European digital space, and developing mechanisms for international cooperation in the field of cybersecurity. It is substantiated that the effective adaptation of the Directive's provisions requires comprehensive legislative reform, the development of the institutional capacity of the state, and the formation of a modern cybersecurity culture in both the public and private sectors.

Keywords: cybersecurity, implementation of EU law, NIS2 Directive, cyber resilience, European integration.

Вступ

28 лютого 2022 року – визначна дата в історії України. Саме цього дня, на п'ятий день повномасштабного вторгнення Росії, президент України офіційно підписав заявку на вступ до Європейського Союзу. Це рішення стало не лише рішучим кроком у напрямку європейської інтеграції, а й відповіддю на військову агресію, що загрожувала існуванню української державності. З моменту здобуття незалежності у 1991 році Україна неодноразово декларувала свій європейський вибір. Під час Революції Гідності 2013–2014 років, українці виступили проти відмови тодішньої влади підписати Угоду про асоціацію з ЄС. З того часу Україна прискорила реформи, спрямовані на євроінтеграцію [1]. Власне, в статті 124 в Угоді про асоціацію з ЄС (2014) зазначено, що «сторони визнають важливість наближення чинного законодавства України до права Європейського Союзу. Україна забезпечує поступове приведення своїх чинних законів та майбутнього законодавства у відповідність до acquis ЄС. Таке наближення розпочинається з дати підписання цієї Угоди та поступово поширюватиметься на всі елементи acquis ЄС» [2]. Отже, гармонізація національного законодавства з acquis ЄС в сфері кібербезпеки є нагальним процесом, зокрема: з положеннями Директиви Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року (Директива NIS2) [3].

Результати дослідження

Імплементація положень Директиви NIS2 [3] в українське законодавство має враховувати такі основні аспекти:

- *гармонізація з *acquis* ЄС* (Україна має адаптувати правові норми у сфері кібербезпеки відповідно до вимог цієї директиви, зокрема щодо обов'язків суб'єктів щодо управління ризиками, звітування та співпраці);
- *визначення секторів та суб'єктів* (необхідно створити перелік секторів високої критичності, зокрема енергетики, транспорту, фінансів, охорони здоров'я, цифрової інфраструктури тощо; також визначити відповідних суб'єктів, що належать до категорій основних і важливих);
- *національна стратегія безпеки* (в Україні необхідно привести у відповідність до вимог директиви національну стратегію кібербезпеки, зокрема щодо цілей, пріоритетів, управлінської системи, механізмів ідентифікації активів, оцінювання ризиків, заходів реагування та відновлення);
- *організаційна структура* (передбачити створення/укомплектування компетентних органів, єдиних контактних пунктів, а також формування мережі CSIRT і EU-CyCLONe для забезпечення транскордонної та міжсекторальної співпраці);
- *обов'язки щодо управління ризиками та звітування* (впровадити обов'язки для суб'єктів щодо управління ризиками, проведення оцінки вразливостей тощо; створення процедур скоординованого оприлюднення вразливостей та використання європейських схем сертифікації кібербезпеки);
- *механізми обміну інформацією* (впровадити механізми добровільного та обов'язкового обміну інформацією між суб'єктами, CSIRT, компетентними органами та ENISA, з урахуванням захисту конфіденційної та таємної інформації; забезпечити інтеоперабельність систем);
- *реєстри та бази даних* (створити та підтримувати реєстри основних і важливих суб'єктів, а також бази даних реєстрації доменних імен, що відповідають стандартам захисту даних та забезпечать прозорість і доступність інформації для легітимних користувачів);
- *юрисдикція та відповідальність* (визначити юрисдикцію; забезпечити невідворотну відповідальність за порушення в сфері кібербезпеки через адміністративні штрафи та/або інші правозастосовні практики);
- *нагляд та санкції* (встановити механізми нагляду, процедурні гарантії, санкції та відповідальність за порушення вимог, з урахуванням принципів пропорційності та ефективності);
- *міжнародна співпраця* (забезпечити участь України у міжнародних угодах, співпрацю з третіми країнами та міжнародними організаціями у сфері кібербезпеки, обмін розвідданими та досвідом тощо);
- *перегляд та оновлення* (встановити механізм періодичного перегляду національної системи кібербезпеки відповідно до змін у технологічному, політичному та правовому середовищі, з урахуванням рекомендацій та звітів ENISA, мережі CSIRT та інших стейкхолдерів);
- *технічна гармонізація та стандартизація* (заохочувати використання європейських і міжнародних стандартів, технічних специфікацій і схем сертифікації для забезпечення сумісності та високого рівня кібербезпеки);
- *захист персональних даних* (враховувати положення Регламенту ЄС 2016/679 [4] та інших нормативно правових актів щодо захисту персональних даних при опрацюванні інформації, що стосується інцидентів, вразливостей і обміну даними).

Висновок

Імплементація Директиви NIS2 [3] є важливим етапом гармонізації українського законодавства з *acquis* ЄС в сфері кібербезпеки. Вона сприятиме: підвищенню рівня захисту критичної інфраструктури; зміцненню кіберстійкості держави; інтеграції України до європейського цифрового простору; розвитку механізмів міжнародного співробітництва у сфері кібербезпеки. Ефективна адаптація положень NIS2 потребує комплексного оновлення законодавства, розвитку інституційної спроможності держави та формування сучасної культури кібербезпеки як у державному, так і в приватному секторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 28 лютого 2022 року: день, коли Україна офіційно подала заявку на вступ до ЄС. *Комітет з питань інтеграції України до Європейського Союзу. Верховна Рада України*. URL: <https://comeuroint.rada.gov.ua/print/75117.html> (дата звернення: 25.05.2026)

2. 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 від 26.09.2014 року, №75, том 1, стор. 83, стаття 2125*. URL: https://zakon.rada.gov.ua/laws/card/984_011 (дата звернення: 25.05.2026)
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 вісник Європейського Союзу від 27.12.2022 року, /L333/, стор. 80*. URL: https://zakon.rada.gov.ua/laws/card/9a3_001-22 (дата звернення: 25.05.2026)
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вісник Європейського Союзу від 04.05.2016 року, /L119/, стор. 1*. URL: https://zakon.rada.gov.ua/laws/card/984_008-16 (дата звернення: 25.05.2026)

Лівандовська Анастасія Олегівна – студентка групи 1БКС-23Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: anastasiativandovska@gmail.com

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: Imaidanevych@gmail.com

Livandovska Anastasiia – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: anastasiativandovska@gmail.com

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: Imaidanevych@gmail.com