УДК 004.056

В. О. Демченко
Л. О. Майданевич

НОРМАТИВНЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ ПІД ЧАС ВОЄННОГО СТАНУ: ОСОБЛИВІ АСПЕКТИ

Вінницький національний технічний університет

Анотація

В доповіді проаналізовані окремі аспекти унормування кібербезпеки в Україні в умовах воєнного стану. Обґрунтовано, що воєнний стан зумовив підвищення вимог до кіберстійксті держави, оперативності реагування на кіберінциденти, удосконалення інформаційного обміну задля більш ефективного захисту критичних систем. Визначено потребу у подальшій гармонізації підзаконної бази, уточненні процедур взаємодії суб'єктів та посиленні їх відповідальності за порушення кіберзахисту. Зроблено висновок , що ефективність нормативного регулювання кібербезпеки під час воєнного стану визначається не лише наявністю законодавчих приписів, а й їх дієвим застосуванням.

Ключові слова: кібербезпека, кіберзахист, об'єкти критичної інфраструктури, воєнний стан.

Abstract

The report analyzes certain aspects of the regulation of cybersecurity in Ukraine under martial law. It is substantiated that martial law has led to increased requirements for the state's cyber resilience, the speed of response to cyber incidents, and the improvement of information exchange for more effective protection of critical systems. The need for further harmonization of the regulatory framework, clarification of the procedures for interaction between entities, and strengthening their responsibility for violations of cyber protection is identified. It is concluded that the effectiveness of regulatory regulation of cybersecurity during martial law is determined not only by the presence of legislative provisions, but also by their effective application.

Key words: cybersecurity, cyber defense, critical infrastructure facilities, martial law.

Вступ

У сучасних умовах гібридної війни Україна щодня зазнає масованих кібератак на об'єкти критичної інфраструктури. За даними CERT-UA, у 2025 році зафіксовано майже 6000 кібератак (це на 37% більше ніж в попередньому році). Головною цілю в цих випадках є державні реєстри, енергетична та інша інфраструктура, яка забезпечує життєво важливі функції та послуги держави. Захист критичної інфраструктури став невід'ємною частиною національної оборони, а нормативне регулювання кібербезпеки в умовах воєнного стану – це питання національного виживання.

Результати дослідження

Оскільки наша країна знаходиться у стані війни, тому звичайного захисту критичних інфраструктур є недостатньо. В цьому випадку життєво необхідним є дотримання законів про кібербезпеку. В нашій доповіді ми звернемо увагу на такі закони:

1. Закон України «Про основні засади забезпечення кібербезпеки України» [2] визначає правові та організаційні основи забезпечення кібербезпеки в країні, зокрема у контексті викликів, пов'язаних із воєнним станом. Закон закріплює принципи застосування норм, що передбачають баланс між забезпеченням національної безпеки та захистом прав і свобод громадян, а також баланс між відповідальністю та пропорційністю заходів. Він визначає, що у разі воєнного стану можливо застосування заходів, спрямованих на запобігання використанню кіберпростору у протиправних цілях, у тому числі у воєнних цілях, та реагування на кіберзагрози і кіберінциденти. Закон передбачає, що заходи у сфері кібербезпеки мають бути необхідними і мінімально достатніми для досягнення цілей забезпечення безпеки, що є важливим у контексті викликів воєнного стану. Також закон встановлює порядок реагування на кризові ситуації у сфері

кібербезпеки, що виникають у зв’язку з воєнним станом, та визначає роль суб'єктів забезпечення кібербезпеки у таких умовах. Таким чином, нормативне регулювання у цій сфері враховує виклики воєнного стану і передбачає механізми реагування та забезпечення кібербезпеки в умовах збройної агресії.

2. Закон України «Про критичну інфраструктуру» [3] визначає правові та організаційні засади створення і функціонування національної системи захисту критичної інфраструктури, яка є складовою частиною законодавства у сфері національної безпеки. Закон визначає, що законодавство у цій сфері складають Конституція України, цей Закон, міжнародні договори, ратифіковані Верховною Радою, а також інші нормативно-правові акти. Регулювання відносин у сфері функціонування та захисту критичної інфраструктури здійснюється у мирний час, а особливості захисту у надзвичайних ситуаціях, воєнному та особливому періоді регулюються відповідними законами.

Закон встановлює рівні управління системою: загальнодержавний, регіональний, місцевий та об’єктовий; а також визначає принципи її функціонування (зокрема єдність, координованість, державно-приватне партнерство, міжнародне співробітництво). Управління системою здійснюється через відповідні органи, зокрема: Кабінет Міністрів України, уповноважений орган у сфері захисту критичної інфраструктури, секторальні та функціональні органи, оператори критичної інфраструктури.

Об’єкти критичної інфраструктури можуть бути віднесені до категорій критичності: I (особливо важливі), II (життєво важливі), III (важливі), IV (необхідні). Віднесення здійснюється відповідно до критеріїв, визначених цим Законом, та за процедурою, встановленою Кабінетом Міністрів. Ведеться реєстр таких об’єктів, який є відкритим і доступним для громадськості, крім інформації з обмеженим доступом.

Також цей закон передбачає особливий режим дії встановлений під час воєнного стану та протягом двох років після його припинення: забороняється вилучення, накладення арешту або обмеження прав держави щодо об’єктів критичної інфраструктури, що перебувають у державній власності, а також накладення арештів або припинення зобов’язань щодо господарських товариств – операторів критичної інфраструктури (якщо їх частки належать державі або були відчужені під час воєнного стану). Також забороняється відкриття проваджень у справах про банкрутство таких товариств, а арешти та обмеження щодо їх майна підлягають зняттю або скасуванню.

Загалом, цей Закон створює правову базу для системної організації, управління та захисту об’єктів критичної інфраструктури України, враховуючи особливості воєнного стану та необхідність забезпечення національної безпеки.

Висновки

Проведений аналіз Закону України «Про основні засади забезпечення кібербезпеки України» та Закону України «Про критичну інфраструктуру» засвідчує, що в умовах воєнного стану нормативне регулювання кібербезпеки набуває особливої системоутворюючої ролі. Перший закон формує загальну модель національної системи кібербезпеки, визначає суб’єктів, їх повноваження та механізми координації, тоді як другий встановлює спеціальний режим захисту об’єктів критичної інфраструктури (як ключових елементів стійкості держави).

Воєнний стан актуалізував необхідність підвищення рівня кіберстійкості, оперативного обміну інформацією про кіберінциденти, розширення повноважень уповноважених органів та впровадження ризик-орієнтованого підходу до захисту критичних систем. Водночас практична реалізація зазначених законів виявляє потребу у подальшій гармонізації підзаконної бази. Уточненні процедур взаємодії між державними органами та суб’єктами господарювання, а також у посиленні відповідальності за порушення вимог кіберзахисту.

Таким чином, ефективність нормативного регулювання кібербезпеки під час воєнного стану визначається не лише наявністю законодавчих приписів, а й їх дієвим застосуванням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Апарат РНБО представив досвід кібероборони в умовах війни під час слухань у Європейському парламенті. URL: https://www.rnbo.gov.ua/ua/Diialnist/7392.html?PRINT (дата звернення: 19.02.2026).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 19.02.2026).
3. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 19.02.2026).

Демченко Вероніка Олександрівна – студентка групи 1БКС-23Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: vdemchenkoo.ol@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: lmaidanevych@gmail.com

Demchenko Veronika – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vdemchenkoo.ol@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: lmaidanevych@gmail.com