УДК 340(477):004.056

ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Новік Т.О.
e-mail: taisiia.novik@nure.ua
Харківський національний університет радіоелектроніки, каф. філософії
м. Харків, Україна

In today's world, where digital technologies have become an integral part of society, cybersecurity is critically important. Ukraine is actively developing its legal framework for cybersecurity as part of its European integration and efforts to strengthen national security. The relevance of this topic is underscored by the growing number of cyber threats and their potential impact on national security, the economy, and citizens' rights. In 2023, there was a significant rise in cyber incidents, which calls for an enhancement of Ukraine’s cybersecurity system. Ukraine’s legal progress in cybersecurity aligns with European standards, but further harmonization and cooperation are needed for more comprehensive protection.

У сучасному світі, де цифрові технології стали невід'ємною частиною суспільного життя, питання кібербезпеки набуває критичного значення. Україна, прагнучи до європейської інтеграції та зміцнення своєї національної безпеки, активно розвиває правові засади кібербезпеки. Важливість цієї теми підкреслюється зростаючою кількістю кіберзагроз та їх потенційним впливом на національну безпеку, економіку та права громадян.

За даними Оперативного центру реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України, у другій половині 2023 року кількість подій інформаційної безпеки категорії «02 Шкідливий програмний код» зросла на 95,8%, а категорії «03 Збір інформації зловмисником» – на 35,8% порівняно з першою половиною 2023 року [1]. Це різке зростання може бути наслідком збільшення активності кіберзлочинців в умовах сучасних викликів, таких як військова агресія, що робить необхідним удосконалення системи кіберзахисту в Україні.

Основоположним нормативно-правовим актом, який регулює кібербезпеку в Україні, є Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий у 2017 році. Цей закон визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору» [2]. Закон став основою для подальшого розвитку нормативної бази у сфері кіберзахисту.

У 2021 році в законодавство були внесені важливі поправки, спрямовані на посилення захисту критичної інфраструктури та залучення приватного сектору до загальної системи кібербезпеки. Окрім того, у 2021

році була прийнята Національна стратегія кібербезпеки на період 2021-2025 років, яка передбачає більш активне використання сучасних технологій для протидії кіберзагрозам та підвищення рівня координації між державними установами і приватним сектором.

Серед ключових нововведень можна виділити запуск платформи для швидкого реагування на інциденти кібербезпеки, що підтримується Державною службою спеціального зв'язку та захисту інформації України, а також створення Національного координаційного центру кібербезпеки при РНБО України у 2022 році [3].

Українське законодавство з кібербезпеки значною мірою орієнтується на європейські стандарти. Особливо важливу роль відіграє імплементація положень Європейської директиви NIS (Network and Information Systems), яка встановлює основні вимоги до безпеки мереж та інформаційних систем у країнах ЄС [4]. Українські законодавці значною мірою врахували ці вимоги під час розробки національних стандартів захисту критичної інфраструктури.

Проте Україна ще має значний шлях до гармонізації з іншими європейськими регламентами, такими як GDPR (General Data Protection Regulation), що регулює захист персональних даних. В той час як у Європі ці стандарти вже впроваджені на високому рівні, в Україні законодавча база з цього питання потребує вдосконалення, особливо у сфері приватного сектору.

Крім того, хоча міжнародні стандарти, такі як ISO/IEC 27001 (стандарт управління інформаційною безпекою), впроваджуються в державних установах, їх використання в приватному секторі залишається обмеженим. Це становить ризик для загальної кібербезпеки країни, особливо з огляду на важливість приватних компаній у загальній мережевій інфраструктурі.

За останні роки Україна досягла значного прогресу у сфері кібербезпеки. До ключових нововведень можна віднести:

1) Прийняття Стратегії кібербезпеки України у 2021 році, яка враховує сучасні виклики та загрози в кіберпросторі.

2) Створення Національного координаційного центру кібербезпеки при РНБО у 2022 році, що посилило координацію дій різних відомств у сфері кіберзахисту [3].

3) Запровадження системи захисту критичної інформаційної інфраструктури. Станом на 2023 рік, до реєстру об'єктів критичної інформаційної інфраструктури включено понад 500 об'єктів [5].

4) Розвиток державно-приватного партнерства, включаючи підписання меморандумів з провідними IT-компаніями щодо обміну інформацією про кіберзагрози.

Попри це, Україна все ще має низку викликів. Серед них:

1) Гармонізація законодавства з вимогами NIS2 Директиви ЄС, яка включає детальніші вимоги до кібербезпеки у різних секторах економіки.

2) Посилення міжнародної співпраці, особливо в контексті обміну інформацією про кіберзагрози та спільного реагування на кіберінциденти.

3) Розвиток системи підготовки фахівців з кібербезпеки. Дефіцит кваліфікованих кадрів може стати загрозою для національної безпеки в довгостроковій перспективі [6].

4) Вдосконалення системи аудиту кібербезпеки та відповідальності за порушення вимог кіберзахисту.

Україна зробила значні кроки в розвитку правових засад кібербезпеки та частковій інтеграції міжнародних стандартів у національне законодавство. Проте для подальшого вдосконалення необхідно розширити використання європейських стандартів, таких як GDPR та ISO/IEC 27001, підвищити рівень підготовки фахівців з кібербезпеки та поглибити міжнародну співпрацю. Удосконалення координації між державними органами та приватним сектором також стане важливим елементом зміцнення кібербезпеки в Україні.

Список використаних джерел

1. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв’язку та захисту інформації України. URL: https://scpc.gov.ua/api/files/e4eaafb7-99de-4a60-89f2-f0c05b777b69

2. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Про Національний координаційний центр кібербезпеки : Указ Президента України від 28.01.2022 № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289

4. Директива NIS (Network and Information Security) 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

5. Державна служба спеціального зв'язку та захисту інформації України. Реєстр об'єктів критичної інформаційної інфраструктури. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veresnya-2023-roku-793

6. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. – К., 2024.– №2(лютий).– 253 с.