

УДК 004.056

*Іван Голуб, науковий співробітник відділу
цифрових освітніх ресурсів,
Інститут професійної освіти НАПН України,
м. Київ, Україна*

НОРМАТИВНО-ПРАВОВА БАЗА КІБЕРБЕЗПЕКИ УКРАЇНИ ТА ЇЇ РЕЛЕВАНТНІСТЬ ДЛЯ НАУКОВИХ УСТАНОВ

Анотація. Автор досліджує нормативно-правову базу кібербезпеки в Україні, підкреслюючи її важливість для наукових установ. Обговорюється Національна стратегія кібербезпеки до 2025 року, визначаючи її пріоритети захисту та координацію зусиль через Національний координаційний центр кібербезпеки та Держспецзв'язку. Текст аналізує ключові закони та постанови Кабінету Міністрів України, такі як закони «Про основні засади забезпечення кібербезпеки України» та «Про інформацію», що регулюють захист даних, включаючи персональні та наукові. Особлива увага приділяється обов'язку наукових організацій дотримуватися законодавчих вимог, включаючи створення комплексних систем захисту інформації (КСЗІ) та планів реагування на кіберінциденти. Стаття також згадує нормативні акти Держспецзв'язку щодо КСЗІ та криптографічного захисту, а також рекомендації CERT-UA для освітнього сектору.

Ключові слова: кіберзахист, наукові установи, нормативні документи.

Abstract. The author examines the regulatory framework for cybersecurity in Ukraine, emphasizing its importance for scientific institutions. The National Cybersecurity Strategy until 2025 is discussed, identifying its protection priorities and coordinating efforts through the National Cybersecurity Coordination Center and the State Service for Special Communications. The text analyzes key laws and resolutions of the Cabinet of Ministers of Ukraine, such as the laws “On the Basic Principles of Ensuring Cybersecurity of Ukraine” and “On Information”, which regulate data protection, including personal and scientific data. Particular attention is paid to the obligation of scientific organizations to comply with legislative requirements, including the creation of comprehensive information protection systems (CSIS) and cyber incident response plans. The article also mentions the State Service for Special Communications’ regulatory acts on CISS and cryptographic protection, as well as CERT-UA recommendations for the education sector.

Keywords: cyber defense, scientific institutions, regulatory documents.

Розбудова ефективної системи кібербезпеки в Україні передбачає наявність чітко визначеної нормативно-правової бази. Вона регулює засади національної кібербезпеки, діяльність уповноважених органів, а також вимоги до захисту інформаційних систем у різних секторах, включаючи наукову та освітню сфери [1; 2; 3].

Відслідковуючи прийняті закони можна побачити, як формується Національна стратегія та координація в цій сфері. На основі ухваленої в серпні 2021 року Стратегії кібербезпеки (розрахованої до 2025 р.) [4; 5; 6] держава визначила пріоритети кіберзахисту, зокрема створення кібервійськ та побудову національної системи реагування на інциденти. Для координації зусиль діє Національний координаційний центр кібербезпеки при РНБО, а Держспецзв'язку (Державна служба спеціального зв'язку та захисту інформації) відіграє провідну роль у формуванні і реалізації політики [7]. Наприклад, у 2022 році кількість зафіксованих кіберінцидентів зростає у 2,8 рази проти попереднього, які спонукали до посилення моніторингу та обміну інформацією між усіма суб'єктами кібербезпеки [8; 9].

Установи Національної академії педагогічних наук України, як наукові організації державної форми власності, зобов'язані дотримуватись вимог законодавства в частині захисту інформаційних активів, у тому числі персональних даних, наукової інформації, інтелектуальної власності та критичних ІТ-систем.

1. Закон України «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII) [10]. Цей закон є ключовим документом, який визначає національні пріоритети та інституційну модель кіберзахисту.

Впровадження закону в наукових установах:

- *Визначено обов'язок суб'єктів (у тому числі освітньо-наукових) впроваджувати заходи з кіберзахисту.*
- *Прямо згадується сфера освіти та науки як частина національного кіберпростору.*

2. Закон України «Про інформацію» (із змінами, 2022) [11; 12]. Він регламентує доступ до інформації, її класифікацію, вимоги до зберігання та захисту.

Для наукових установ:

- *Наукові установи обробляють не лише відкриту, а й обмежену за доступом інформацію, яка підпадає під дії цього закону, зокрема у частині персональних даних, авторських прав, конфіденційної інформації.*

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [11; 12; 13]. Цей закон зобов'язує всі суб'єкти, які використовують ІКТ, забезпечити технічний захист інформації, зокрема шляхом створення комплексної системи захисту (КСЗІ). [14; 15].

Для наукових установ КСЗІ рекомендовано створювати для:

- *захисту інформації з обмеженим доступом (проектні дані, персональні архіви);*
- *внутрішніх баз студентів, наукових кадрів, розрахунків.*

4. Постанова КМУ № 518 «Про затвердження Порядку реагування на кіберінциденти» (2018) [16]. Вона регламентує порядок взаємодії з CERT-UA, фіксацію та документування кіберінцидентів.

Для наукових установ:

- *Кожна установа в державному секторі, повинна призначити відповідального за кібербезпеку.*
- *Необхідне впровадження внутрішнього плану реагування на інциденти.*

5. Постанова КМУ № 439 «Про затвердження Стратегії кібербезпеки України» (2021) [6]. Це стратегічний документ, який визначає пріоритети кіберзахисту на період до 2025 року.

- *Для освітніх установ рекомендовано впровадження освітніх програм з кібергигієни для персоналу. Стратегія передбачає і співпрацю наукових установ з державними органами в рамках підвищення загального рівня стійкості.*

6. Нормативні документи Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ).

- Методичні рекомендації щодо побудови КСЗІ (2021) [14; 15]. Вони містять інструкції зі створення комплексної системи захисту для ІТ-систем. Їх основу можна використати, як базовий документ для проектування ІТ-безпеки в наукових інформаційних мережах.

- Вимоги до криптографічного захисту інформації (КЗІ) [17]. Для роботи з інформацією, яку потрібно зашифрувати (наприклад, дані учасників наукових досліджень, проєктів).

- Галузеві рекомендації CERT-UA. Періодично публікуються рекомендації, приклади атак та методи реагування для освітнього сектору.

Висновок: Нормативно-правова база кібербезпеки України є всеохоплюючою та постійно розвивається. Наукові установи, як суб'єкти національного кіберпростору та власники цінної інформації, мають чіткі зобов'язання щодо її захисту. Дотримання вимог законодавства, впровадження відповідних заходів та співпраця з державними органами є критично важливими для забезпечення стійкості наукової сфери до кіберзагроз. Особлива увага має бути приділена захисту інформації з обмеженим доступом, персональних даних та інтелектуальної власності.

Список використаних джерел

1. Про освіту : Закон України від 5 вересня 2017 р. № 2145-VIII. *Відомості Верховної Ради України*. 2017. № 38–39. Ст. 380. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2145-19> (дата звернення 10.05.2025).
2. Про вищу освіту : Закон України від 1 лип. 2014 р. № 1556-VII. *Відомості Верховної Ради України*. 2014. № 37–38. Ст. 2004. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/1556-18> (дата звернення 10.05.2025).
3. Про наукову і науково-технічну діяльність: Закон України від 26 листоп. 2015 р. № 848-VIII. *Відомості Верховної Ради України*. 2016. № 3. Ст. 25. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/848-19> (дата звернення 10.05.2025).

4. The President of Ukraine approved a new Cybersecurity Strategy of Ukraine. [Електронний ресурс]. URL: <https://www.rnbo.gov.ua/en/Diialnist/4976.html> (дата звернення 03.05.2025).
5. Про схвалення Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 26 трав. 2021 р. № 518-р. *Офіційний вісник України*. 2021. № 50. Ст. 3085. [Електронний ресурс]. URL: <https://www.kmu.gov.ua/npas/pr-skhlavennya-strategiyi-kiberbezpeki-518-260521> (дата звернення 10.05.2025).
6. Про затвердження Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 17 черв. 2021 р. № 439-р. *Офіційний вісник України*. 2021. № 50. Ст. 3085. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/439-2021-p> (дата звернення 10.05.2025).
7. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо політик інформаційної безпеки. 2022. [Електронний ресурс]. URL: <https://cip.gov.ua> (дата звернення 10.05.2025).
8. 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 (NIS 2 Directive). [Електронний ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555> (дата звернення 10.05.2025).
9. Рада національної безпеки і оборони України. Cyber Digest. Стан кіберзагроз: січень 2024. Київ : РНБО України, 2024. 16 с. [Електронний ресурс]. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf (дата звернення 10.05.2025).
10. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2018. № 5. Ст. 36. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення 10.05.2025).
11. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення 10.05.2025).
12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/80/94-vr> (дата звернення 10.05.2025).
13. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення 10.05.2025).
14. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо побудови комплексної системи захисту інформації (КСЗІ). 2021. [Електронний ресурс]. URL: <https://cip.gov.ua/ua/publikacii/metodichni-rekomendacii> (дата звернення 10.05.2025).
15. Державна служба спеціального зв'язку та захисту інформації України. Типові політики КСЗІ для критичної інфраструктури. 2022. [Електронний ресурс]. URL: <https://cip.gov.ua> (дата звернення 10.05.2025).

16. Про затвердження Порядку реагування на кіберінциденти : постанова Кабінету Міністрів України від 24 лип. 2018 р. № 518. *Офіційний вісник України*. 2018. № 61. Ст. 2112. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/518-2018-п> (дата звернення 10.05.2025).
17. Державна служба спеціального зв'язку та захисту інформації України. Вимоги до криптографічного захисту інформації. 2021. [Електронний ресурс]. URL: <https://cip.gov.ua> (дата звернення 10.05.2025).