Олександр ЩИРОВ,
здобувач вищої освіти другого року навчання,
спеціальність 081 - Право, третій освітньо-науковий рівень
доктор філософії права (PhD) гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна
e-mail: o.s.shchyrov@khai.edu
ORCID: 0009-0004-4828-6180

Науковий керівник: Наталія ФІЛІПЕНКО,
доктор юридичних наук, професор,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут»,
Харків, Україна
e-mail: n.filipenko@khai.edu
ORCID: 0000-0001-9469-3650

DOI: https://doi.org/10.32620/pls.2024.5.25

ЗАХИСТ ТА СТІЙКІСТЬ ОСВІТНЬОГО СЕРЕДОВИЩА: ПРАВОВИЙ ВИМІР У ГЛОБАЛІЗОВАНОМУ СВІТІ

Анотація: *У статті розглядаються правові аспекти забезпечення стійкості освітнього середовища в умовах глобалізації, зокрема через призму його захисту як частини критичної інфраструктури. Аналізуються ключові міжнародні та національні нормативні акти, а також практичні аспекти їх реалізації. Особлива увага приділяється питанням кіберзахисту, цифровізації та управління ризиками в освітніх установах. У статті розглянуто роль інноваційних технологій, зокрема «розумних кампусів» та VR-інструментів, у забезпеченні безпеки та адаптації освітнього процесу до викликів сучасності. Окремо аналізуються програми емоційної підтримки учасників освітнього процесу як елемент забезпечення психологічної стійкості. Висновки містять рекомендації щодо вдосконалення правового регулювання та підвищення ефективності управління освітніми установами у кризових умовах.*

Ключові слова: *освітнє середовище, стійкість, критична інфраструктура, кіберзахист, інновації, цифровізація, міжнародне право.*

Сучасні глобальні виклики, серед яких війни, кіберзагрози, пандемії та кліматичні зміни, загострюють питання безпеки і стійкості освітнього середовища. Освітні заклади, як складова критичної інфраструктури, стають не лише об'єктами впливу, але й активними учасниками трансформаційних процесів. У цьому контексті постає необхідність аналізу правових механізмів, які забезпечують їхню стійкість.

Освітні установи виконують дві ключові функції: забезпечення освітніх послуг і формування соціальної стійкості. Отже, й освітнє середовище є об'єктом правового захисту. Згідно з рекомендаціями ЮНЕСКО, вони класифікуються як частина соціальної критичної інфраструктури, що потребує особливого правового регулювання.

Міжнародними стандартами, основою правового захисту освітнього середовища є міжнародні акти:

Загальна декларація прав людини, яка гарантує право на освіту (ст. 26) [1];

Конвенція ООН про права дитини (ратифіковано Постановою ВР № 789-XII від 27.02.1991 р.), що наголошує на обов'язку держав забезпечити доступ до якісної освіти навіть в умовах криз [2];

У вересні 2015 року всі 193 члени Організації Об'єднаних Націй ухвалили план досягнення спільного кращого майбутнього. Наступні 15 років спільні зусилля спрямовано на подолання крайньої бідності, боротьбу з нерівністю і несправедливістю та на захист нашої планети. У центрі «Порядку денного 2030» є 17 Цілей сталого розвитку (ЦСР), зокрема у програмах, присвячених «Якісній освіті» (Ціль 4) та «Інноваціям та інфраструктурі (Ціль 9) [3].

В національному контексті, українське законодавство враховує рекомендації міжнародних організацій. Наприклад, Закон України «Про освіту» визначає, що цифровізація освіти є одним із ключових напрямів її модернізації [4]. Реалізація

освітніх ініціатив під час війни, таких як Всеукраїнська школа онлайн, стала можливим завдяки нормативній базі, що передбачає гнучкість освітнього процесу.

Кіберзахист має високу пріоритетність у сфері освіти. Оскільки цифровізація стала невід'ємною частиною освітнього процесу, важливим аспектом є забезпечення кібербезпеки. Велика кількість освітніх закладів у світі стикаються з ризиками витоку даних або кібератаками. У 2023 році хакери атакували цифрові платформи шкіл США, заблокувавши доступ до онлайн-уроків. Інцидент викликав необхідність розробки додаткових протоколів безпеки та боротьби з кіберзагрозами. Слід дотримуватися рекомендацій з кіберзахисту: впроваджувати національні стандарти безпеки, зокрема рекомендації НБУ для освітніх ІТ-систем; регулярно моніторити цифрові платформи, що використовуються в навчанні; користуватися ресурсами та освітніми програми з кіберграмотності для викладачів і студентів.

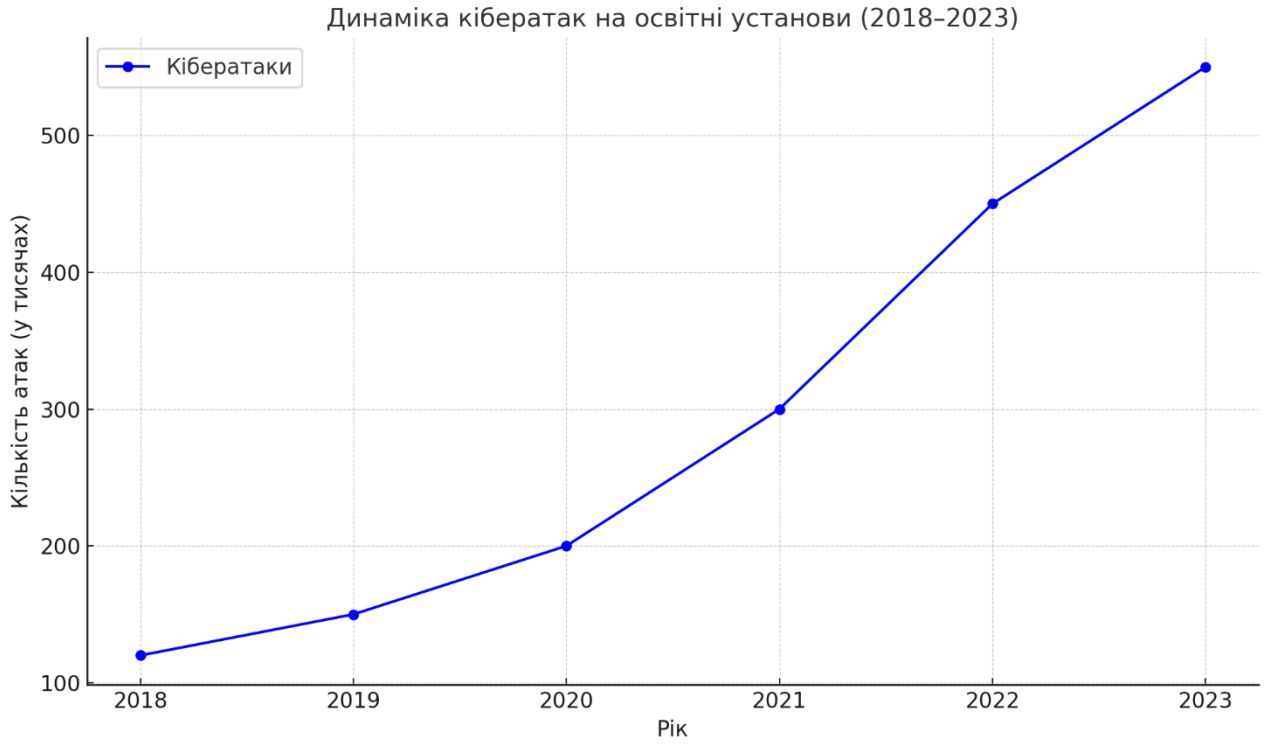

Рис. 1. Рівень кібератак на освітні установи у світі за 2018–2023 роки (графік додається)

Для забезпечення стійкості слід підходити інноваційно, впроваджувати методи стійкого управління, розвивати моделі «розумних кампусів», які інтегрують технології IoT (Internet of Things – Інтернет речей), дозволяє оптимізувати ресурси і забезпечувати контроль безпеки на території закладу. Таким прикладом є досвід Сінгапуру у створенні «розумних університетів», де впроваджуються енергозберігаючі системи, автономне відеоспостереження і моніторинг здоров'я студентів. Також слід зауважити про міжнародні кейси впровадження заходів стійкості, як Програма «CyberSmart! Education»: її вплив на зниження ризиків кіберзагроз у школах і університетах. Програма була впроваджена в США для підвищення рівня кібербезпеки серед учнів і персоналу навчальних закладів. Її метою є навчання базовим принципам захисту інформації, протидії фішинговим атакам та безпечної роботи з мережами. В результаті, у 2021 році після реалізації програми в кількох штатах США кількість успішних фішингових атак на школи зменшилася на 40%. Досвід Нідерландів із впровадження законодавства, яке забезпечує кібербезпеку як невід'ємну частину управління освітніми установами. Національний досвід України: інтеграція освітньої платформи «Дія.Освіта» для підвищення цифрової грамотності учасників освітнього процесу. Україна, в умовах цифрової трансформації та зростання загроз кібербезпеці, розробила платформу "Дія.Освіта", яка є частиною масштабної ініціативи цифровізації країни. До ключових завдань платформи належать: проведення курсів із цифрової грамотності для вчителів і студентів; ознайомлення персоналу закладів освіти із сучасними інструментами для захисту інформації; інтеграція елементів STEM-освіти з акцентом на кібербезпеку. У 2022 році, після пілотного запуску платформи в регіонах, які постраждали від військових дій, понад 25 тисяч педагогів успішно пройшли навчання з основ кіберзахисту. Це дало змогу уникнути витоку

персональних даних у багатьох школах і університетах. Висновок: Платформа є яскравим прикладом ефективної національної ініціативи, яка спрямована на підвищення стійкості освітнього середовища. Інші країни можуть запозичити цей досвід для побудови аналогічних систем.

Також існують ініціативи із фізичної та психологічної підтримки в освітніх установах, такі як програма «Безпечна школа» у регіонах, які постраждали від військових дій. Стійкість освітнього середовища залежить не лише від технологій, а й від психологічного добробуту його учасників. Тому психологічна стійкість учасників освітнього процесу є вкрай важливим фактором. В Україні активно розвиваються програми емоційної підтримки для школярів у рамках ініціатив ЮНІСЕФ.

Стійкість освітнього середовища в Україні базується на низці законодавчих актів та стратегій. Серед ключових документів:

Закон України «Про освіту» (2017): закріплює право на безпечні умови навчання, включаючи захист персональних даних студентів та викладачів [4];

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

Стратегія кібербезпеки України: передбачає посилення кіберзахисту критичної інфраструктури, до якої відносяться й освітні заклади [6];

Закон України «Про критичну інфраструктуру»: вимагає від закладів освіти розробки заходів для забезпечення функціонування у надзвичайних ситуаціях [7].

Згідно з міжнародними стандартами (наприклад, ISO/IEC 27001), важливим аспектом є впровадження систем управління інформаційною безпекою (СУІБ). Однак забезпечення належного рівня програмного забезпечення для захисту даних в освітніх закладах України залишається проблематичним. За попередніми дослідженнями міжнародних організацій та експертів, рівень цифрової готовності українських освітніх закладів залишається низьким. Особливо це стосується питань кібербезпеки та захисту даних, що вимагає суттєвих інвестицій та модернізації.

Юридична відповідальність за недотримання заходів кібербезпеки відповідно до законодавства України показує, що заклади освіти та їхні співробітники можуть бути притягнуті до відповідальності за порушення вимог інформаційної безпеки. Адміністративна відповідальність передбачена статтями Кодексу України про адміністративні правопорушення, зокрема за недотримання порядку зберігання даних. Кримінальна відповідальність – згідно зі статтею 361 Кримінального кодексу України, за несанкціоноване втручання в роботу інформаційних систем освітніх установ.

Для закладів освіти з обмеженими ресурсами актуальними є такі рішення:

використання відкритих платформ для управління ризиками кібербезпеки (наприклад, CIS Controls);

створення базових політик безпеки: розробка інструкцій для викладачів та студентів щодо поводження з даними;

навчальні тренінги для персоналу щодо правил користування інформаційними системами;

пошук зовнішнього фінансування: наприклад, через грантові програми.

Таблиця: Основні проблеми та рекомендації з правового забезпечення кібербезпеки

Проблема	**Юридичне регулювання**	**Рекомендація**
Низький рівень автоматизації	ЗаконУкраїни «Про освіту», Національна стратегія кібербезпеки	Використання базових ІТ-рішень
Недостатнє розуміння кіберризиків	Відсутність обов’язкових тренінгів	Запровадження коротких курсів кібергігієни
Відсутність внутрішніх політик	Закон «Про захист інформації в інформаційно-телекомунікаційних системах», ISO/IEC 27001	Розробка університетських правил безпеки
Обмеженість ресурсів	Бюджетні обмеження	Використання безкоштовного ПЗ, отримання грантів.

Стійкість освітнього середовища потребує не лише технічних рішень, але й вдосконалення нормативно-правової бази. Освітні заклади повинні активно співпрацювати з державними органами та міжнародними організаціями для інтеграції сучасних стандартів безпеки. Юридичне забезпечення таких процесів є ключовим елементом успішної трансформації системи освіти в умовах глобальних викликів. Правовий захист освітнього середовища є важливою складовою

забезпечення його стійкості. Це передбачає комплексний підхід, що включає впровадження інновацій, забезпечення кібербезпеки і захист прав учасників освітнього процесу. Особливу роль відіграє адаптація міжнародних стандартів до національного контексту.

Бібліографічні посилання

1. Universal Declaration of Human Rights. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 A (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. Офіційний переклад. URL: https://www.ohchr.org/en/human-rights/universal-declaration/translations/ukrainian-ukrayinska.

2. UN Convention on the Rights of the Child. Конвенція про права дитини. Редакція зі змінами, схваленими резолюцією 50/155 Генеральної Асамблеї ООН від 21 грудня 1995 року. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text.

3. Глобальний договір ООН в Україні. 17 Цілей сталого розвитку. URL: https://globalcompact.org.ua/tsili-stijkogo-rozvytku/.

4. Про освіту. Закон України від 05.09.2017 р. № 2145-VIII. База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text.

5. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 р. № 80/94-ВР. База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указом Президента України від 26.08.2021 р. № 447/2021. База даних «Законодавство України»/ВР України. URL: Про рішення Ради національн... | від 26.08.2021 № 447/2021.

7. Про критичну інфраструктуру. Закон України від 16.11.2021 р. № 1882-IX. База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

O. Shchyrov, N.Filipenko

Protection and resilience of the educational environment: Legal dimension in a globalized world.

Abstract: The article examines the legal aspects of ensuring the resilience of the educational environment in the context of globalization, in particular through the prism of its protection as part of critical infrastructure. Key international and national regulatory frameworks, as well as their practical applications, are analyzed. Particular attention is given to issues of cybersecurity, digitalization, and risk management in educational institutions. The article examines the role of innovative technologies, including smart campuses and VR tools, in ensuring security and adapting the educational process to the challenges of our time. Programs of emotional support for participants in the educational process are also analyzed as a key element of psychological resilience. The conclusions include recommendations for improving legal regulation and enhancing the efficiency of managing educational institutions under crisis conditions.

Keywords: educational environment, resilience, critical infrastructure, cybersecurity, innovation, digitalization, international law.

Зразок для цитування:
Щиров О., Філіпенко Н. Захист та стійкість освітнього середовища: правовий вимір у глобалізованому світі. Пропілеї права та безпеки: наук. журнал. Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2024. № 5. С. 88-91. DOI: https://doi.org/10.32620/pls.2024.5.25.