

DOI [https://doi.org/10.32689/2523-4625-2026-1\(81\)-2](https://doi.org/10.32689/2523-4625-2026-1(81)-2)

УДК 351.77:005.334:37.014.3(477)

## ПРАВОВІ МЕХАНІЗМИ ІНТЕГРАЦІЇ БЕЗПЕКОВИХ КОМПОНЕНТІВ В ОСВІТНЮ ПОЛІТИКУ

Г. О. Кузьменко

### LEGAL MECHANISMS FOR INTEGRATING SECURITY COMPONENTS INTO EDUCATION POLICY

Hanna Kuzmenko

**Анотація.** Стаття розкриває правові механізми інтеграції фізичної, цифрової та психосоціальної безпеки в освітню політику України в умовах воєнного стану та тривалих криз. Мета статті полягає в теоретико-правовому обґрунтуванні освіти як складової критичної інфраструктури та в розробленні багаторівневої рамки узгодження норм матеріального й процесуального права, управлінських процедур, стандартів і показників, що забезпечують безпечне й безперервне функціонування освітньої системи. Методологія дослідження ґрунтується на аналізі й узагальненні національного законодавства України у сфері освіти, цивільного захисту, режиму воєнного стану, публічних закупівель, захисту персональних даних і кібербезпеки, а також на вивченні міжнародних стандартів управління ризиками, інформаційною безпекою та безперервністю діяльності. Аналітичний інструментарій доповнено концепціями “public value” (публічна цінність), “co-governance” (співврядування) та “resilience thinking” (підхід до мислення крізь призму стійкості), що інтегруються із системним, інституційним і ризик-орієнтованим підходами до публічного управління. Наукова новизна отриманих результатів полягає в обґрунтуванні освіти як елемента критичної інфраструктури, від здатності якого підтримувати безперервність навчання, захищати життя, здоров'я та гідність учасників освітнього процесу, забезпечувати довіру громад до публічних інституцій залежить стійкість держави, а також у розробленні матриці правових інструментів, відповідальних суб'єктів і ключових індикаторів безпеки. Показано, що узгоджене застосування вимог цивільного захисту, особливостей правового режиму воєнного стану, процедур публічних закупівель, правил захисту персональних даних і кібербезпеки з інструментами бізнес- та освітньої безперервності формує цілісну архітектуру безпечної освіти на державному, регіональному та інституційному рівнях. Окреслено матрицю, яка охоплює фізичну інфраструктуру (укриття, евакуаційні маршрути, технічну безпеку), цифрові сервіси (електронні журнали, платформи дистанційного навчання, засоби автентифікації), психосоціальну підтримку учасників освітнього процесу, фінансову прозорість і механізми участі громад у прийнятті рішень. У висновках обґрунтовано підхід до моніторингу безпеки освіти, заснований на відкритих даних, співучасті зацікавлених сторін і циклі “плануй – дій – перевірай – коригуй” як умові підзвітності та адаптивності освітньої системи в умовах тривалих криз. Зазначено напрями подальших досліджень, пов'язані з оцінюванням ефективності безпекових інвестицій, валідацією індикаторів, удосконаленням механізмів залучення громад та порівнянням моделей співврядування в різних територіальних громадах.

**Ключові слова:** освітня політика, безпека в освіті, правові механізми, цивільний захист, кібербезпека, захист персональних даних, безперервність навчання, співврядування, публічна цінність.

**Abstract.** The article examines the legal mechanisms for integrating physical, digital and psychosocial security into Ukraine's education policy under martial law and protracted crises. The purpose of the article is to provide a theoretical and legal justification of education as a component of critical infrastructure and to develop a multi-level framework for aligning substantive and procedural legal norms, management procedures, standards and indicators that ensure safe and uninterrupted functioning of the education system. The research methodology is based on the analysis and synthesis of Ukrainian national legislation in the fields of education, civil protection, the legal regime of martial law, public procurement, personal data protection and cybersecurity, as well as on the study of international standards for risk management, information security and business continuity. The analytical toolkit is complemented by the concepts of “public value”, “co-governance” and “resilience thinking”, which are integrated with systemic, institutional and risk-based approaches in public administration. The scientific novelty of the results lies in substantiating education as an element of critical infrastructure whose ability to maintain learning continuity, protect the life, health and dignity of participants in the educational process, and sustain public trust in institutions determines the resilience of the state, and in designing a matrix of legal instruments, responsible actors and key safety indicators. The article demonstrates that the coordinated application of civil protection requirements, specific provisions of the martial law regime, public procurement procedures and rules on personal data protection and cybersecurity, together with business and educational continuity tools, forms an integrated architecture of safe education at national, regional and institutional levels. A matrix is outlined that covers physical infrastructure

(shelters, evacuation routes, technical safety), digital services (electronic gradebooks, distance learning platforms, authentication tools), psychosocial support for learners and staff, financial transparency and mechanisms for community participation in decision-making. The conclusions substantiate an approach to monitoring safety in education based on open data, stakeholder co-participation and the “plan – do – check – act” cycle as a prerequisite for accountability and adaptability of the education system in protracted crises. The article also identifies directions for further research related to assessing the effectiveness of safety investments, validating indicators, improving mechanisms for community engagement and comparing co-governance models across territorial communities.

**Key words:** education policy, safety in education, legal mechanisms, civil protection, cybersecurity, personal data protection, learning continuity, co-governance, public value.

**1. Вступ.** В умовах воєнного стану питання безпеки в освіті набуває системного характеру: від укриттів і евакуаційних протоколів до кіберстійкості платформ, захисту персональних даних та психосоціальної підтримки. Фрагментарні рішення не забезпечують ні якості, ні довіри. Потрібні правові механізми, які інтегрують вимоги різних секторів (освіта, цивільний захист, охорона здоров'я, цифрова трансформація, соціальний захист) у єдину політику з чіткими ролями, ресурсами, процедурами та індикаторами. Запит на таку інтеграцію зумовлений необхідністю безперервності навчання, справедливого доступу для вразливих груп, прозорості використання коштів і захисту прав учасників освітнього процесу.

**Огляд публікацій і досліджень.** Концепції резильєнтності (С. Голлінг; Б. Волкер і Д. Сольт) та управління кризами (А. Боін, П. 'т Харт) задають теоретичні координати для системного підходу до ризиків і відновлення в освіті [16; 17; 31]. Сенсмейкінг К. Вейка пояснює, як організації інтерпретують невизначеність і навчаються діючи [18]. Рамки співврядування (К. Анселл, А. Геш; Є. Торфінг), публічної цінності (Дж. Брайсон та співавт.) і копродукції (Т. Боваєрд, Е. Леффлер) демонструють, як державні і недержавні актори можуть спільно формувати політики безпеки в освіті [20; 21; 19; 25]. Міжнародні стандарти ISO 22301 (безперервність), ISO 31000 (ризик-менеджмент), ISO/IEC 27001 (інформаційна безпека) та керівні документи UNDRR (Sendai Framework), GADRRRES (Comprehensive School Safety Framework 2022–2030), а також огляди UNESCO/UNICEF/OECD/World Bank пропонують перевірені практики інтеграції безпеки у шкільну політику [28; 29; 27; 11; 12; 13; 14; 15].

В українському контексті правові вимоги розпорошені між законами про освіту, цивільний захист, кібербезпеку, персональні дані, воєнний стан, інформацію та публічні закупівлі. Невирішеним лишається питання операційної інтеграції: хто, на якій підставі й за якими індикаторами ухвалює рішення; як забезпечити прозорість, підзвітність і баланс прав під час обмежень воєнного стану [1; 2; 3; 5; 6; 7; 10].

**Мета статті:** обґрунтувати особливості рамки інтеграції безпекових компонентів в освітню політику України, визначити інструменти імплементації на державному, регіональному та інституційному рівнях, а також запропонувати систему індикаторів моніторингу виконання.

**2. Матеріали і методи.** Інтеграція безпекових компонентів в освітню політику передбачає узгодження трьох шарів: (норми права (загальні та спеціальні), управлінські процедури та інститути (ролі, регламенти, бюджети), стандарти й індикатори (операційні вимоги, моніторинг). Теоретично ця інтеграція спирається на співврядування як інституційну логіку колективних дій і на рамку публічної цінності для оцінювання рішень за критеріями суспільної корисності, легітимності/підтримки та операційної спроможності [20; 21; 19].

По-перше, фізична безпека. Кодекс цивільного захисту визначає обов'язки щодо укриттів, евакуаційних шляхів та навчальних тривог, а також координацію зі службами цивільного захисту [4]. На рівні політики це означає: обов'язкові плани евакуації, регулярні тренування, аудит укриттів, інтеграцію навчальних планів із безпековими інструктажами. Sendai Framework підкреслює зниження ризиків через планування, раннє попередження та готовність, а Comprehensive School Safety Framework пропонує три стовпи безпечної школи: безпека та структурна стійкість, управління ризиками та безперервність навчання, освіта з питань ризиків і безпеки [11; 27]. У поєднанні з національними вимогами це формує обов'язковий мінімум для закладів: укриття, маршрути евакуації, інструктажі, взаємодія з ДСНС, фіксація і перевірка протоколів [4; 10].

По-друге, цифрова безпека та захист даних. Закон про кібербезпеку визначає засади національної системи кіберзахисту, а закон про персональні дані – права суб'єктів і вимоги до обробки [6; 5]. На рівні школи та громади це означає політики доступу, мінімізацію даних, управління згодами, двофакторну автентифікацію, журналювання доступів, резервне копіювання, план відновлення після інцидентів і регулярні навчання користувачів. ISO/

ІЕС 27001 пропонує рамку для побудови системи менеджменту інформаційної безпеки, а ISO 22301 – для системи безперервності діяльності, що критично для підтримки дистанційного чи змішаного навчання [28; 29]. У сучасних умовах цифрова безпека невіддільна від педагогічних рішень: платформи та контент мають відповідати принципам *privacy-by-design* і *security-by-design*, а учні – здобувати навички цифрової гігієни [12; 15].

По-третє, психосоціальна безпека та інклюзія. Освітня політика має забезпечувати доступ до психологічної підтримки, програм соціально-емоційного навчання, адаптацій для учнів із ООП і підтримки ВПО. Міжнародні огляди наголошують, що без цих компонентів неможливо забезпечити сталу відвідуваність, навчальні результати й довіру до інституцій [12; 14; 15]. Правові підстави – у загальних гарантіях права на освіту, недискримінації й безпеки, конкретизованих у підзаконних актах і локальних політиках закладів [1; 2].

По-четверте, прозорість і підзвітність. Вимоги законів про інформацію та доступ до публічної інформації забезпечують відкритість даних про безпекові заходи, закупівлі, інциденти та результати моніторингу [8; 7]. На практиці це означає публічні реєстри потреб, звіти про стан укриттів, витрати на безпеку, панелі індикаторів відвідуваності й безперервності навчання. Прозорість зменшує асиметрію інформації й підвищує довіру до рішень, що особливо важливо в умовах обмежень воєнного стану [3; 13].

По-п'яте, фінансова архітектура. Бюджетний кодекс і закон про публічні закупівлі створюють інструменти для фінансування заходів безпеки, співфінансування з донорами та прозорої конкуренції між постачальниками [9; 13]. Це потребує стандартизованих технічних завдань (укриття, енергостійкість, обладнання), планів безперервності з бюджетами, контрактів із вимогами до SLA і KPI, а також відкритих звітів.

З огляду на наведене, доцільно запропонувати матрицю правових механізмів інтеграції безпеки (табл. 1).

Ключовим елементом правової інтеграції є розподіл відповідальності й процедур ухвалення рішень. Співврядування передбачає залучення НУО, батьківських і учнівських спільнот, місцевого бізнесу до циклів «планування – реалізації – моніторингу». Правові механізми для такого залучення – консультативні органи при відділах освіти, наглядові ради шкіл, публічні консультації, бюджети участі, договори про співфінансування й меморандуми про партнерство [20; 21; 25]. У поєднанні з прозорими даними це створює підзвітність і довіру, що критично для довгострокового фінансування безпеки [7; 9].

Окрема увага – узгодженню норм у колізійних ситуаціях. Під час воєнного стану можуть діяти обмеження прав і спрощені процедури. Політика безпеки має забезпечувати пропорційність втручань і документування рішень для постфактум-аудиту, що відповідає принципам публічної цінності та верховенства права [3; 19].

Таблиця 1

**Матриця правових механізмів інтеграції безпекових компонентів в освітню політику**

Рівень системи	Нормативна основа	Механізми імплементації	Компоненти безпеки	Ключові індикатори
Держава	Закони, кодекси, нац. стандарти	Державні стандарти, нац. панель даних, ВСМ-вимоги, керівництва	фізична, цифрова, психосоціальна	частка уроків, що відбулися; % шкіл з укриттями; інциденти кібербезпеки/місяць
Область/громада	Регіональні програми, рішення ОМС	Координаційні штаби, бюджети безпеки, каталоги потреб, партнерства	фізична, цифрова, психосоціальна	час реагування; виконання планів відновлення; прозорість закупівель
Заклад освіти	Локальні політики, інструкції	Плани евакуації, навчальні тривоги, ISMS, резервне копіювання, ППК	фізична, цифрова, психосоціальна	відвідуваність; час відновлення; задоволеність учасників
Клас/учень	Індивідуальні плани, правила	Навчання з безпеки, цифрова гігієна, ПСС, адаптації	психосоціальна, цифрова	прогрес учнів; охоплення ПСС; частка користувачів із 2FA

Сформовано на основі [11; 12; 13; 14; 15; 16; 17; 18; 19; 20; 21; 25; 27; 28; 29].

Запровадження систем безперервності (ВСМ) в освіті вимагає поєднання правових і управлінських інструментів: аналіз впливу на діяльність (ВІА), реєстри критичних процесів (навчання, комунікація, захист даних), сценарне планування, регулярні стрес-тести та навчальні симуляції. Імплементация на рівні закладів може здійснюватися через локальні накази, політики інформаційної безпеки, угоди про рівень сервісу та внутрішній аудит [28; 29].

Нарешті, освітня політика має містити компонент освіти з питань безпеки: інтеграція тем цивільного захисту, медіагігієни, кібербезпеки й психосоціального благополуччя у стандарти, курикулум і позакласну діяльність. Це зміцнює «культуру безпеки» і знижує ризики довгостроково [11; 12; 15].

**3. Висновки і перспективи подальших досліджень.** Інтеграція безпекових компонентів в освітню політику вимагає узгодження норм права, управлінських процедур і стандартів із чітким розподілом відповідальності

та відкритими даними. Цілісна рамка включає: фізичну безпеку (укриття, евакуація), цифрову безпеку (ISMS, ВСМ, захист даних), психосоціальну підтримку й інклюзію, а також прозорі фінансові механізми й партнерства. На практиці це реалізується через локальні політики, плани безперервності, індикатори і цикли «плануй-роби-перевір-дій». Подальші дослідження доцільно спрямувати на оцінювання економічної ефективності безпекових інвестицій, валідацію індикаторів та порівняння моделей співврядування у різних громадах.

**Конфлікт інтересів.** Відсутній.

**Фінансування.** Дослідження проводилося без фінансової підтримки.

**Доступність даних.** Рукопис не має пов'язаних даних.

**Використання засобів штучного інтелекту.** Автор підтверджує, що не використовував технології штучного інтелекту під час створення представленої роботи.

#### References:

1. Pro osvitu: Zakon Ukrainy vid 05.09.2017 № 2145-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 2017, № 38–39, st. 380. [On Education] [in Ukrainian].
2. Pro povnu zahalnu seredniu osvitu: Zakon Ukrainy vid 16.01.2020 № 463-IX. Vidomosti Verkhovnoi Rady Ukrainy, 2020, № 31, st. 226. [On Complete General Secondary Education] [in Ukrainian].
3. Pro pravovyi rezhym voiennoho stanu: Zakon Ukrainy vid 12.05.2015 № 389-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 2015, № 28, st. 250. [On the Legal Regime of Martial Law] [in Ukrainian].
4. Kodeks tsyvilnoho zakhystu Ukrainy: Zakon Ukrainy vid 02.10.2012 № 5403-VI. Vidomosti Verkhovnoi Rady Ukrainy, 2013, № 34–35, st. 458. [Code of Civil Protection of Ukraine] [in Ukrainian].
5. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 № 2297-VI. Vidomosti Verkhovnoi Rady Ukrainy, 2010, № 34, st. 481. [On Personal Data Protection] [in Ukrainian].
6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 2017, № 45, st. 403. [On the Basic Principles of Ensuring Cybersecurity of Ukraine] [in Ukrainian].
7. Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011 № 2939-VI. Vidomosti Verkhovnoi Rady Ukrainy, 2011, № 32, st. 314. [On Access to Public Information] [in Ukrainian].
8. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 № 2657-XII. Vidomosti Verkhovnoi Rady Ukrainy, 1992, № 48, st. 650. [On Information] [in Ukrainian].
9. Biudzhetni kodeks Ukrainy: Kodeks Ukrainy vid 08.07.2010 № 2456-VI. Vidomosti Verkhovnoi Rady Ukrainy, 2010, № 50–51, st. 572. [Budget Code of Ukraine] [in Ukrainian].
10. Pro zatverdzhennia Poriadku orhanizatsii osvitnoho protsesu v umovakh voiennoho stanu: Postanova Kabinetu Ministriv Ukrainy vid 23.09.2022 № 1117. Ofitsiyni visnyk Ukrainy, 2022, № 76. [On Approval of the Procedure for Organizing the Educational Process under Martial Law] [in Ukrainian].
11. UNDRR. Sendai Framework for Disaster Risk Reduction 2015–2030. Geneva: United Nations Office for Disaster Risk Reduction, 2015. [in English].
12. GADRRRES. Comprehensive School Safety Framework 2022–2030. Global Alliance for Disaster Risk Reduction and Resilience in the Education Sector, 2022. [in English].
13. Pro publichni zakupivli: Zakon Ukrainy vid 25.12.2015 № 922-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 2016, № 9, st. 89. [On Public Procurement] [in Ukrainian].
14. UNESCO. Global Education Monitoring Report 2023: Technology in Education. Paris: UNESCO, 2023. [in English].
15. OECD. Strengthening the Resilience of Education Systems. Paris: OECD Publishing, 2022. [in English].
16. Holling C. S. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1973, 4, 1–23. [in English].

17. Walker B., Salt D. Resilience Thinking: Sustaining Ecosystems and People in a Changing World. Washington, DC: Island Press, 2006. [in English].
18. Weick K. E. Sensemaking in Organizations. Thousand Oaks: Sage, 1995. [in English].
19. Bryson J. M., Crosby B. C., Bloomberg L. Public value governance: Moving beyond traditional public administration and the new public management. *Public Administration Review*, 2014, 74(4), 445–456. [in English].
20. Ansell C., Gash A. Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 2008, 18(4), 543–571. [in English].
21. Torfing J., Peters B. G., Pierre J., Sørensen E. *Interactive Governance: Advancing the Paradigm*. Oxford: Oxford University Press, 2012. [in English].
22. Heifetz R., Grashow A., Linsky M. *The Practice of Adaptive Leadership*. Boston: Harvard Business Press, 2009. [in English].
23. Heeks R. *Information and Communication Technology for Development (ICT4D)*. London: Routledge, 2018. [in English].
24. World Bank. *Resilient Education Systems in Ukraine: Policy Note*. Washington, DC: The World Bank, 2023. [in English].
25. Bovaird T., Loeffler E. From engagement to co-production: The contribution of users and communities to outcomes and public value. *Voluntas*, 2012, 23, 1119–1138. [in English].
26. UNICEF. *Ukraine Humanitarian Situation Report: Education, 2023*. New York: United Nations Children's Fund, 2023. [in English].
27. ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. Geneva: ISO/IEC, 2022. [in English].
28. ISO 22301:2019. *Security and Resilience – Business Continuity Management Systems – Requirements*. Geneva: International Organization for Standardization, 2019. [in English].
29. ISO 31000:2018. *Risk Management – Guidelines*. Geneva: International Organization for Standardization, 2018. [in English].
30. Boin A., 't Hart P., Stern E., Sundelius B. *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge: Cambridge University Press, 2005. [in English].

#### ВІДОМОСТІ ПРО АВТОРА

**Кузьменко Ганна Олександрівна**  
*доктор філософії в галузі публічного управління та адміністрування, доцент, доцент кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом, ORCID: 0000-0003-0672-7633*

**Kuzmenko Hanna**  
*Doctor of Philosophy in Public Administration and Management, Associate Professor at the Department of Public Administration, Interregional Academy of Personnel Management ORCID: 0000-0003-0672-7633*

Дата надходження статті: 02.04.2026

Дата надходження виправленої версії статті: 16.04.2026

Дата прийняття статті: 20.04.2026

Дата публікації статті: 09.06.2026