# МІСЦЕВЕ САМОВРЯДУВАННЯ

УДК 351.77:005.334:37.014.3(477)
DOI https://doi.org/10.32782/TNU-2663-6468/2025.5/19

***Кузьменко Г. О.***
Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»

## ЦИФРОВІ СЕРВІСИ ОСВІТИ ЯК ЕЛЕМЕНТ БЕЗПЕКОВОГО ПРОСТОРУ: ПОРІВНЯННЯ НАЦІОНАЛЬНОГО ТА МІЖНАРОДНОГО ДОСВІДУ

*Стаття концептуалізує цифрові сервіси освіти як складову безпекового простору держави, територіальних громад і закладів освіти в умовах воєнного стану в Україні. Обґрунтовано, що платформи дистанційного та змішаного навчання, електронні журнали і щоденники, сервіси електронної ідентифікації та автентифікації, єдині та галузеві реєстри здобувачів освіти і педагогічних працівників, сервіси відеозв'язку, сховища цифрового контенту, системи електронної комунікації з органами влади та постачальниками послуг одночасно є елементами освітньої інфраструктури і критично важливими інформаційними системами. На основі міждисциплінарного аналізу поєднано норми освітнього, інформаційного, адміністративного законодавства, регулювання у сферах електронних документів, електронних довірчих послуг, електронних комунікацій, захисту персональних даних і кібербезпеки, а також підходи публічного врядування та «цифрової трансформації» (перехід до сервісно-платформених моделей управління) для доведення необхідності розглядати цифрові сервіси освіти як елемент національної й локальної безпеки. Здійснено порівняльне зіставлення українських практик із рекомендаціями міжнародних організацій UNESCO, UNICEF, OECD, Світового банку та технічними стандартами ISO/IEC 27001, ISO 22301, ISO/IEC 27701, WCAG 2.1, EN 301 549, матеріалами ENISA і NIST, що застосовуються до захисту освітніх екосистем. Виокремлено ключові групи ризиків: порушення конфіденційності та цілісності даних дітей і педагогів, компрометація облікових записів, недоступність сервісів через технічні збої або кібератаки, невідповідність вимогам доступності, відсутність планів безперервності навчання, фрагментарність управління постачальниками. Сформовано модель інтегрованого управління ризиками, засновану на принципах "security by design" (безпека, закладена у проєктування сервісів), "privacy by design" (приватність, вбудована в процеси обробки даних) та "resilience by design" (стійкість, вбудована у структуру систем); запропоновано систему індикаторів доступності, безперервності, захищеності та прозорості цифрових освітніх сервісів. Розроблено дорожню карту інституціоналізації безпеки цифрових сервісів на рівнях держава – громада – заклад освіти – провайдер, що включає встановлення мінімальних національних вимог до автентифікації та управління доступами, резервного копіювання і відновлення, моніторингу інцидентів, укладання типових договорів з постачальниками з урахуванням стандартів інформаційної безпеки, впровадження локальних політик захисту даних і регулярних навчань із кібергігієни. Доведено, що впровадження такої рамки інтегрує цифрові сервіси освіти в систему безпекового простору, знижує вразливість дітей і педагогів до кіберзагроз, забезпечує безперервність навчання та підвищує довіру до публічних інституцій у воєнний та післявоєнний періоди.*

***Ключові слова:*** *цифрові сервіси освіти, безпековий простір, кібербезпека, захист персональних даних, безперервність навчання, доступність, управління ризиками, публічне врядування, стійкість.*

**Постановка проблеми.** В умовах повномасштабної агресії цифрові сервіси освіти перетворилися на «нервову систему» шкільної та університетської мережі. Збої платформи здатні призвести до зриву навчального процесу в цілому регіоні; витоки даних створюють безпосередні загрози для

дітей, педагогів і об'єктів критичної інфраструктури; недоступність сервісів відтворює та поглиблює освітню нерівність, особливо для внутрішньо переміщених осіб і вразливих груп. Одночасно цифровізація відкриває можливості для інклюзивності, адаптивного навчання, прозорості управління і залучення громадянського суспільства до контролю за якістю освітніх послуг. Це актуалізує потребу розглядати цифрові освітні сервіси не лише як технологічні інструменти, а як елемент безпекового простору, що вимагає цілісних правових рамок, чітких управлінських процедур, узгоджених стандартів та індикаторів ефективності.

**Аналіз останніх досліджень і публікацій.** Підходи «цифрового врядування», запропоновані П. Данліві, Х. Марґеттс, І. Мергель, С. Озборном та ін., підкреслюють перехід від відомчих інформаційних систем до платформних моделей, у яких дані та сервіси стають базою для співпраці держави, громад і користувачів. Концепції публічного врядування і співтворення публічних послуг, розвинуті Дж. Брайсоном, Б. Кросбі, Л. Блумберг, Т. Бовaердом, Е. Леффлером, пояснюють, як цифрові інструменти можуть посилювати публічну цінність за умови прозорості й підзвітності. У галузі "ICT4D" Р. Гікс наголошує на залежності ефективності цифрових рішень від інституційної спроможності та соціальної інклюзії. Якість онлайн-освіти та роль інфраструктури ґрунтовно досліджено у працях Б. Мінз, Т. Андерсона, Д. Гаррісона. Міжнародні організації UNESCO, UNICEF, OECD, Світовий банк розробили рекомендації щодо безперервності навчання, захисту дітей в онлайні, цифрової інклюзії та стійкості систем освіти. Стандарти ISO/IEC 27001, ISO 22301, ISO/IEC 27701, настанови ENISA та рамки NIST визначають вимоги до захисту інформації, управління безперервністю та приватністю. В українському науковому дискурсі приділяється увага цифровій трансформації публічного управління, відкритим даним та кібербезпеці, проте інтегроване управління ризиками цифрових освітніх сервісів, зокрема щодо поєднання вимог доступності, безперервності, захисту персональних даних і правового статусу постачальників, висвітлено фрагментарно. Наявний розрив між технічними рекомендаціями та формальним дотриманням законодавства у практиці закладів освіти і громад обґрунтовує необхідність систематизації підходів.

**Постановка завдання.** Мета статті – обґрунтувати цілісну рамку розгляду цифрових сервісів освіти як елемента безпекового простору, порівняти національні і міжнародні підходи до їх правового та організаційного забезпечення і запропонувати практичні інструменти інституціоналізації безпеки, доступності та безперервності зазначених сервісів у системі публічного врядування освітою.

Методологія дослідження. Дослідження здійснено як міждисциплінарне, що поєднує таксономію цифрових освітніх сервісів, критичний аналіз законодавства України у сферах освіти, електронних документів та довірчих послуг, електронних комунікацій, захисту персональних даних, інформаційної безпеки, а також нормативних актів воєнного періоду. Використано компаративний аналіз міжнародних документів UNESCO, UNICEF, OECD, Світового банку та технічних стандартів ISO/IEC, EN, рекомендацій ENISA і NIST. Застосовано інструменти операціоналізації понять доступності, безперервності та безпеки цифрових сервісів через систему індикаторів, а також логіку побудови «дорожньої карти» імплементації на рівнях держава – громада – заклад освіти – провайдер. Обмеження дослідження полягають у відсутності суцільних емпіричних вимірювань і спиранні на доступні офіційні дані, аналітичні звіти та пілотні практики.

Нормативно-правове поле. Правові засади організації освіти, прав і обов'язків учасників освітнього процесу, академічної автономії закладів та відповідальності засновників визначаються Законом України «Про освіту» і Законом України «Про повну загальну середню освіту» [1; 2]. Юридичну силу електронних документів та електронного документообігу забезпечує Закон України «Про електронні документи та електронний документообіг», а функціонування кваліфікованих електронних підписів і печаток – Закон України «Про електронні довірчі послуги» [3; 4]. Стандарти електронних комунікацій і вимоги до мереж та послуг, у тому числі критичних для освітніх платформ, встановлює Закон України «Про електронні комунікації» [6]. Захист персональних даних учнів, батьків, педагогів та інших користувачів цифрових сервісів визначається Законом України «Про захист персональних даних», а системні вимоги до побудови кібербезпеки – Законом України "Про основні засади забезпечення кібербезпеки України» [5; 7]. Інформаційна відкритість і підзвітність провайдерів освітніх послуг і органів управління освітою ґрунтується на Законах України «Про інформацію» та «Про доступ до публічної інформації» [8; 9]. Організацію здобуття загальної середньої освіти й освітнього процесу в умовах воєнного стану деталізовано наказом Міністерства освіти

і науки України від 28 березня 2022 року № 274 «Про деякі питання організації здобуття загальної середньої освіти та освітнього процесу в умовах воєнного стану в Україні» [10]. Сукупність зазначених норм, у поєднанні з міжнародними стандартами інформаційної безпеки та доступності, створює правову і методичну основу для інтегрованого управління ризиками цифрових освітніх сервісів.

**Виклад основного матеріалу.** Цифрові сервіси освіти доцільно розглядати як взаємопов'язану екосистему, у якій технологічні рішення поєднані з правовими, організаційними та безпековими вимогами. До цієї екосистеми належать платформи управління навчанням "LMS" (системи управління навчальним процесом), персоналізовані середовища "LXP" (платформи навчального досвіду), електронні журнали та щоденники, сервіси електронної ідентифікації й автентифікації "eID", реєстри здобувачів освіти і педагогічних працівників, засоби відеоконференц-зв'язку, сховища навчальних матеріалів, сервіси електронної комунікації між школами, батьками, органами влади та постачальниками послуг. У воєнний час ця екосистема набуває подвійної природи: педагогічної, що забезпечує доступ до змісту, оцінювання, комунікацію й підтримку безперервного навчання, та безпекової, пов'язаної із захистом життя і гідності дітей, збереженням даних про місцезнаходження, статус внутрішньо переміщених осіб та особливі освітні потреби, гарантуванням стійкості навчального процесу в умовах обстрілів, окупації, евакуації та вимушеного переміщення [1; 2; 11; 14; 18]. Наявні дослідження цифрового врядування та "digital era governance" підкреслюють, що такі платформи фактично виконують функції публічної інфраструктури, де якість сервісу і безпека стають складовими публічної цінності [15; 16; 29].

Порівняльний аналіз міжнародних підходів дозволяє виокремити три базові принципи проєктування і функціонування цифрових сервісів освіти. Перший принцип – "security by design" – передбачає інтеграцію вимог безпеки вже на етапі архітектурних рішень: мінімізація обсягів даних, що збираються, чітке визначення ролей і прав доступу, використання автентифікації з підвищеним рівнем довіри, обов'язкове журналювання операцій, шифрування даних під час зберігання і передавання, регулярні аудити й тестування захищеності [24; 25; 28]. Цей підхід відповідає вимогам законодавства щодо захисту персональних даних і кібербезпеки та зменшує вразливість сервісів до типових загроз, виділених ENISA та NIST, таких як фішинг, "ransomware", несанкціонований доступ до облікових записів чи порушення цілісності баз даних [7; 24; 27; 28]. Другий принцип – "privacy by design" – фокусується на дотриманні прав суб'єктів персональних даних відповідно до національного законодавства: обробка даних дітей і педагогів має здійснюватися на визначених законом підставах, з чітко окресленою метою, пропорційним обсягом і строками зберігання, передбачуваними процедурами доступу, виправлення та видалення інформації [5; 8; 9; 26]. Для нових функцій платформ доцільним є застосування оцінювання впливу на приватність за логікою ISO/IEC 27701 і міжнародних рекомендацій щодо захисту дітей в цифровому середовищі [12; 26]. Третій принцип – "resilience by design" – орієнтований на вбудовану стійкість: використання резервних копій, географічно розподіленої інфраструктури, альтернативних каналів доступу, наявність затверджених планів безперервності діяльності і сценаріїв відновлення, відповідно до вимог ISO 22301 і практик забезпечення безперервності навчання, які фіксуються у звітах UNESCO, OECD та Світового банку [13; 14; 18; 25]. Дотримання цих трьох принципів перетворює цифрові освітні сервіси з технічного інструменту на захищений публічний сервіс, що здатен функціонувати в умовах кризи.

У національному контексті виявляються низка системних викликів. Досвід громад і закладів освіти підтверджує фрагментацію використаних платформ, різну зрілість управлінських та IT-процесів, нерівномірне дотримання вимог захисту персональних даних, обмежені ресурси на кіберзахист і навчання персоналу [17; 18; 19]. Часто відсутні формалізовані політики інформаційної безпеки, реєстри обробок даних, процедури управління інцидентами, а договори з провайдерами не містять чітко визначених вимог щодо шифрування, журналювання, резервного копіювання та відповідальності за порушення [5; 7; 24]. Це призводить до розриву між нормами законодавства і фактичними гарантіями безпеки учасників освітнього процесу, особливо в умовах воєнного стану, коли дані про місцезнаходження, маршрути евакуації, належність до вразливих груп набувають особливої чутливості [6; 7; 14].

Для подолання цього розриву на рівні держави обґрунтованим є встановлення мінімальних обов'язкових вимог до цифрових освітніх сервісів. До такого базового переліку, спираючись на стандарти ISO/IEC 27001, ISO 22301, ISO/IEC 27701, рекомендації ENISA, NIST та практику країн ЄС, доцільно віднести вимоги щодо використання

надійних засобів електронної ідентифікації, підтримки багатофакторної автентифікації, ведення журналів доступу, криптографічного захисту, проведення регулярних аудитів безпеки, наявності планів безперервності діяльності, відповідності вимогам доступності WCAG 2.1 та EN 301 549 і прозорого інформування про інциденти [23; 24; 25; 27; 28; 30]. Уніфікація таких вимог на національному рівні дозволить зменшити технологічну фрагментацію, спростити контроль і забезпечити більш рівні умови для всіх закладів освіти.

На рівні територіальних громад результати досліджень цифрової трансформації публічного управління свідчать про важливість інституційних спроможностей «посередників»: саме громади здатні координувати вибір платформ, забезпечувати сегментацію і захист локальних мереж, організовувати спільні закупівлі, створювати центри цифрових компетентностей для закладів освіти [16; 17; 19]. Практика країн ЄС демонструє ефективність регіональних центрів підтримки шкіл з питань кібербезпеки, управління даними та доступності, які забезпечують типові політики, шаблони договорів із провайдерами, консультації та моніторинг інцидентів [19; 27; 29]. Формування таких центрів або міжмуніципальних сервісних структур в Україні може бути інструментом масштабування кращих практик та підтримки малих громад.

На рівні закладу освіти цифрові сервіси стають частиною внутрішньої системи забезпечення якості. Необхідними елементами є затверджена політика захисту даних, призначення відповідальної особи або команди, ведення реєстру інформаційних активів та обробок персональних даних, мінімізація прав доступу відповідно до ролей, регламенти резервного копіювання, періодичні тренування персоналу щодо дій у разі кіберінциденту [5; 7; 24; 26]. Міжнародні дослідження підкреслюють, що поєднання технічних засобів безпеки з системним навчанням педагогів і адміністрацій знижує частоту інцидентів і покращує готовність до кризових ситуацій [18; 20; 21]. Для українських закладів освіти, які працюють під обстрілами або приймають значну кількість внутрішньо переміщених учнів, така інституційна впорядкованість стає не лише нормативною вимогою, а й умовою довіри батьків і партнерів.

Особливу групу становлять дані про дітей та інші чутливі відомості. Йдеться про результати навчання, інформацію про стан здоров'я, статус дитини з особливими освітніми потребами, належність до ВПО, а також геодані укриттів і маршрутів евакуації. Відповідно до Закону України «Про захист персональних даних» та принципів ISO/IEC 27701 такі дані мають оброблятися з урахуванням підвищеного рівня захисту: обмежене коло осіб, яким надається доступ; технічні обмеження копіювання та експорту; чітко визначені строки зберігання; процедури анонімізації для аналітичних цілей [5; 26]. Запровадження єдиної національної таксономії освітніх даних із визначенням категорій чутливості та режимів доступу могло б зменшити ризики довільного трактування вимог безпеки на локальному рівні.

Доступність цифрових сервісів прямо пов'язана з реалізацією права на освіту для осіб з інвалідністю, дітей з особливими освітніми потребами, внутрішньо переміщених осіб та інших вразливих груп. Вимоги WCAG 2.1 та EN 301 549 встановлюють стандарти сприйнятності, керованості, зрозумілості та надійності інтерфейсів; емпіричні дослідження показують, що невідповідність цим стандартам призводить до фактичного виключення частини користувачів з освітнього процесу [23; 30]. Тому цифрові платформи, що закуповуються або розробляються для системи освіти, мають проходити оцінку доступності; в іншому разі держава і громади відтворюють нерівність, суперечливу до задекларованих принципів інклюзії [1; 2; 11].

Безперервність навчання у воєнний час є інтегральним індикатором стійкості цифрових сервісів. Практика, узагальнена OECD та Світовим банком, демонструє ефективність застосування методології "business continuity management": ідентифікація критичних процесів (проведення уроків, комунікація з батьками, виставлення оцінок), визначення припустимого часу відновлення та максимально припустимих втрат даних, відпрацювання сценаріїв переходу на резервні канали (офлайн-матеріали, альтернативні платформи, асинхронні формати) [13; 14; 25]. Публічні індикатори – частка занять, проведених за розкладом, середній час простою сервісів, кількість задокументованих інцидентів – стають механізмом підзвітності провайдерів і органів управління освітою та дозволяють громадам оцінювати реальну стійкість цифрового середовища.

Порівняльний досвід країн ОЕСР засвідчує, що найбільш захищені й ефективні системи виникають там, де освітні платформи інтегровані з державними системами електронної ідентифікації, де укладаються стандартизовані договори з постачальниками із закріпленими вимогами до сертифікації інформаційної безпеки, процедури

аудиту, прозорого повідомлення про інциденти та гарантії перенесення даних під час зміни провайдера [19; 24; 27; 29]. Такий підхід мінімізує залежність від окремих комерційних рішень і дозволяє поєднати технологічну гнучкість зі стабільністю і підзвітністю публічної інфраструктури. Адаптація цих механізмів в Україні через типові умови договорів та добровільні програми відповідності стандартам інформаційної безпеки для провайдерів освітніх сервісів може стати реалістичним кроком до зміцнення безпекового простору освіти.

**Висновки.** Цифрові сервіси освіти в умовах воєнного стану є складовою безпекового простору, а не лише інструментом навчання. Їх надійність, захищеність, доступність і безперервність безпосередньо впливають на реалізацію права на освіту, захист дітей і довіру до публічної влади. Аналіз українського законодавства та міжнародних стандартів свідчить про наявність достатньої нормативної бази для побудови інтегрованої системи управління ризиками, однак практична імплементація потребує унормування мінімальних вимог до сервісів, посилення відповідальності постачальників, розвитку інституційних спроможностей громад і закладів освіти та формування культури кібергігієни.

**Список літератури:**

1. Про освіту. Закон України від 05.09.2017 № 2145-VIII. *Відомості Верховної Ради України*, 2017, № 38–39, ст. 380.

2. Про повну загальну середню освіту. Закон України від 16.01.2020 № 463-IX. *Відомості Верховної Ради України*, 2020, № 31, ст. 226.

3. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV. *Відомості Верховної Ради України*, 2003, № 36, ст. 275.

4. Про електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної Ради України*, 2017, № 45, ст. 403.

5. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*, 2010, № 34, ст. 481.

6. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. *Відомості Верховної Ради України*, 2021, № 15, ст. 120.

7. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*, 2017, № 45, ст. 403.

8. Про інформацію. Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*, 1992, № 48, ст. 650.

9. Про доступ до публічної інформації. Закон України від 13.01.2011 № 2939-VI. *Відомості Верховної Ради України*, 2011, № 32, ст. 314.

10. Про деякі питання організації здобуття загальної середньої освіти та освітнього процесу в умовах воєнного стану в Україні. Наказ Міністерства освіти і науки України від 28.03.2022 № 274.

11. UNESCO. Global Education Monitoring Report 2023: Technology in Education. Paris: UNESCO, 2023. 476 p.

12. UNICEF. Child Online Protection in Times of COVID-19 and Beyond. New York: UNICEF, 2021. 36 p.

13. OECD. Education Policy Outlook 2021: Shaping Responsive and Resilient Education. Paris: OECD Publishing, 2021. 300 p.

14. World Bank. Resilient Education Systems in Ukraine: Policy Note. Washington, DC: The World Bank, 2023. 48 p.

15. Dunleavy P., Margetts H., Bastow S., Tinkler J. Digital Era Governance: IT Corporations, the State, and E-Government. Oxford: Oxford University Press, 2006. 288 p.

16. Osborne S. P. The New Public Governance? Emerging Perspectives on the Theory and Practice of Public Governance. London: Routledge, 2010. 448 p.

17. Heeks R. Information and Communication Technology for Development (ICT4D). London: Routledge, 2018. 190 p.

18. UNESCO; UNICEF; World Bank; OECD. What Have We Learnt? Overview of Findings from a Survey of Teachers and School Leaders during the COVID-19 Pandemic. Paris: OECD Publishing, 2021. 68 p.

19. European Commission. Digital Education Action Plan 2021–2027. Brussels: European Commission, 2020. 31 p.

20. Means B., Bakia M., Murphy R. Learning Online: What Research Tells Us about Whether, When and How. New York: Routledge, 2014. 240 p.

21. Anderson T. (ed.). The Theory and Practice of Online Learning. 2nd ed. Edmonton: AU Press, 2008. 472 p.

22. Garrison D. R., Anderson T., Archer W. Critical Inquiry in a Text-Based Environment: Computer Conferencing in Higher Education. *The Internet and Higher Education*, 2000, 2(2–3), 87–105.

23. W3C. Web Content Accessibility Guidelines (WCAG) 2.1. World Wide Web Consortium, 2018. 298 p.
24. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva: ISO/IEC, 2022. 31 p.
25. ISO 22301:2019. Security and Resilience – Business Continuity Management Systems – Requirements. Geneva: ISO, 2019. 24 p.
26. ISO/IEC 27701:2019. Security Techniques – Extension to ISO/IEC 27001 and 27002 for Privacy Information Management – Requirements and Guidelines. Geneva: ISO/IEC, 2019. 66 p.
27. ENISA. Threat Landscape for the Education Sector. Athens: European Union Agency for Cybersecurity, 2022. 52 p.
28. NIST. Security and Privacy Controls for Information Systems and Organizations (SP 800-53, Revision 5). Gaithersburg, MD: NIST, 2020. 482 p.
29. Mergel I., Edelmann N., Haug N. Defining Digital Transformation: Results from Expert Interviews. *Government Information Quarterly*, 2019, 36(4), 101385.
30. ETSI. EN 301 549 V3.2.1 (2021-03). Accessibility Requirements for ICT Products and Services. Sophia Antipolis: ETSI, 2021. 180 p.

**Kuzmenko H. O. DIGITAL EDUCATION SERVICES AS A COMPONENT OF THE SECURITY SPACE: NATIONAL AND INTERNATIONAL EXPERIENCE COMPARED**

*The paper conceptualizes digital education services as a component of the security space for the state, local communities and educational institutions under martial law in Ukraine. It argues that learning platforms, e-registers, identification and authentication services, education databases and data exchange channels function simultaneously as education infrastructure and security-relevant information systems. The study is based on an interdisciplinary analysis of Ukrainian legislation on education, electronic documents and trust services, electronic communications, personal data protection and cybersecurity, as well as on a comparative review of international guidelines (UNESCO, UNICEF, OECD, World Bank) and technical standards (ISO/IEC 27001, ISO 22301, ISO/IEC 27701, WCAG 2.1, EN 301 549, ENISA, NIST). The article identifies key risks related to confidentiality, integrity, availability and continuity of digital services and proposes an integrated risk management model grounded in the principles of security by design, privacy by design and resilience by design. A set of indicators for availability, continuity, security and transparency is suggested, together with a roadmap for institutionalizing security of digital education services at the levels of state, community, school and provider. The implementation of this framework is argued to reduce the exposure of children and teachers to cyber threats, safeguard uninterrupted learning and strengthen trust in public authorities and education providers in wartime and post-war recovery.*

***Key words:*** *digital education services, security space, cybersecurity, data protection, accessibility, business continuity, governance, resilience.*

Дата надходження статті: 31.10.2025
Дата прийняття статті: 20.11.2025
Опубліковано: 29.12.2025