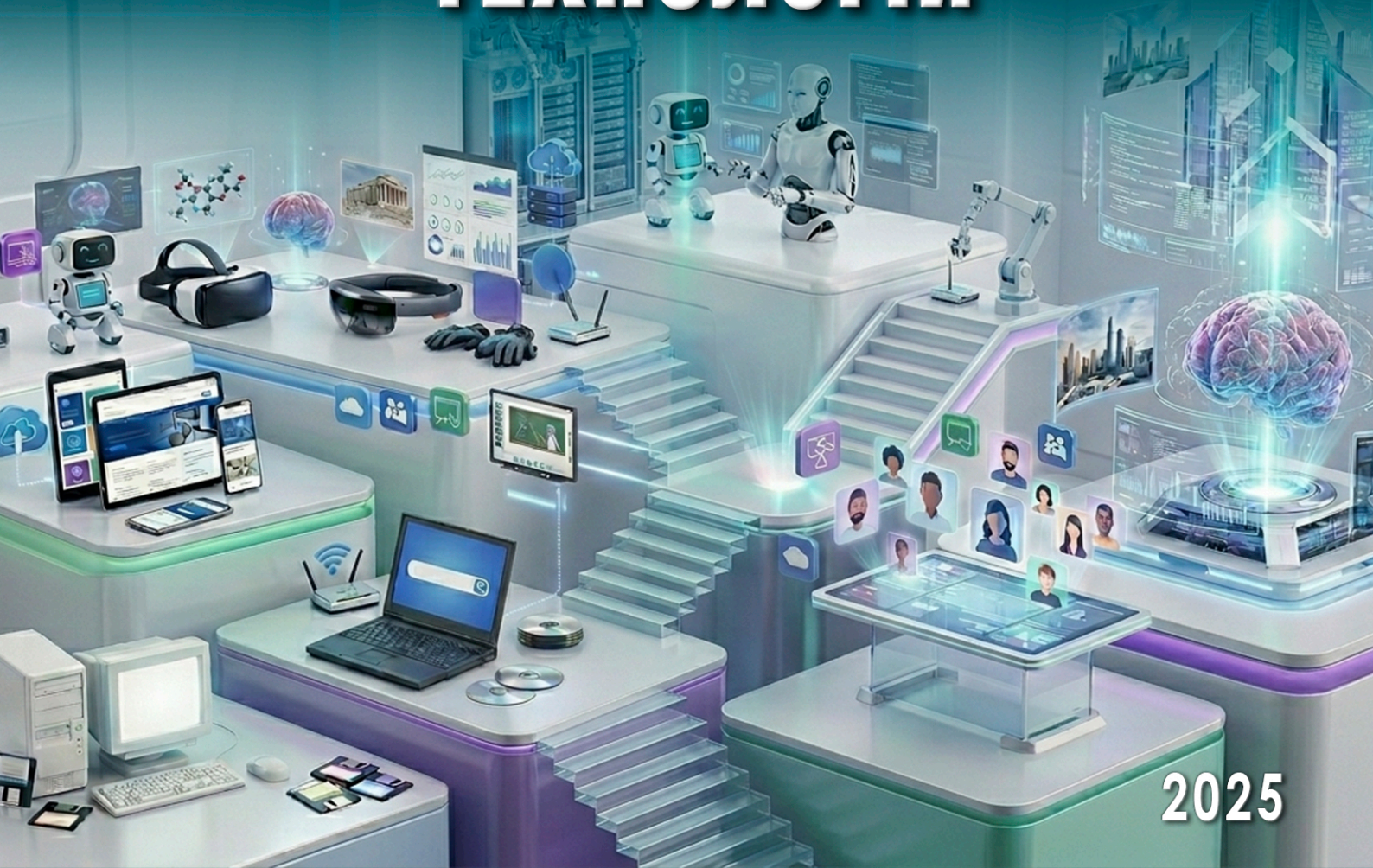
Міністерство освіти і науки України
Державна наукова установа
«Інститут освітньої аналітики»

РОЗВИТОК ІНФОРМАЦІЙНИХ ОСВІТНІХ ТЕХНОЛОГІЙ



2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ОСВІТНЬОЇ АНАЛІТИКИ»

РОЗВИТОК ІНФОРМАЦІЙНИХ ОСВІТНІХ ТЕХНОЛОГІЙ

За редакцією А. О. Литвинчука

Київ – 2025

УДК 37.014.5:004.9
Р 64

Автори:
А. О. Литвинчук (вступ, 2.1, 2.4, 4.5, висновки), А. В. Кир'янов (2.1–2.4, 4.5),
Г. М. Терещенко (вступ, 1.3, 2.1, 2.2, 4.1, 4.5, висновки), Ю. В. Іриневич (1.1, 1.2, 4.2–4.4),
О. В. Кулачинський (3.1–3.4), Н. В. Каменчук (3.1–3.4), Х. С. Ковкрак (2.4), В. В. Лазоренко (3.4),
І. С. Гайдук (1.1, 1.2, 4.2–4.4), Ю. М. Криворучко (4.1, 4.5), П. О. Заверуха (3.1, 3.2),
Я. Д. Сологуб (2.1–2.3, 4.5).

Рецензенти:
Н. І. Версаль – доктор економічних наук, професор, професорка кафедри страхування, банківської справи та ризик-менеджменту Київського національного університету імені Тараса Шевченка;
Т. Л. Дмитренко – доктор економічних наук, старший дослідник, професор ІПО ДННУ «Академія фінансового управління»;
Л. Б. Долінський – доктор економічних наук, доцент, професор кафедри фінансів Національного університету «Києво-Могилянська академія»

Рекомендовано до друку Вченою радою
Державної наукової установи «Інститут освітньої аналітики»
(Протокол № 9 від 1 грудня 2025 р.)

Р 64 **Розвиток інформаційних освітніх технологій** : монографія [Електронний ресурс] / за ред. А. О. Литвинчука ; ДНУ «Інститут освітньої аналітики». Київ, 2025. 199 с.

ISBN 978-617-8421-21-2

Монографію присвячено комплексному дослідженню процесів цифровізації системи освіти України в умовах воєнного стану та євроінтеграції. Актуальність роботи зумовлена необхідністю формування цілісного, інтегрованого та безпечного інформаційного освітнього простору, здатного забезпечити ефективне управління освітою, підвищення прозорості та підзвітності, а також формування доказової державної освітньої політики.

У монографії проаналізовано сучасний стан цифровізації системи освіти України, визначено ключові тенденції розвитку освітніх інформаційних технологій та окреслено проблеми формування інформаційного освітнього простору. Значну увагу приділено дослідженню функціонування національних інформаційних систем управління освітою, їх інтеграції та визначенню критеріїв ефективності. Обґрунтовано напрями модернізації програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту» як базового елемента цифрової інфраструктури галузі.

Окремий розділ присвячено розвитку освітніх платформ в умовах воєнного стану, зокрема аналізу їх функціонування та оцінці ефективності забезпечення доступу до освіти. Досліджено роль цифрових платформ у підтримці безперервності освітнього процесу.

У роботі також розглянуто питання кібербезпеки та захисту персональних даних у сфері освіти, проаналізовано інституційно-правові засади їх забезпечення в Україні та країнах Європейського Союзу, а також визначено напрями їх удосконалення в умовах євроінтеграції.

Результати дослідження можуть бути використані органами державної влади, науковими установами та розробниками інформаційних систем при формуванні та реалізації політики цифровізації освіти, модернізації інформаційної інфраструктури та підвищенні рівня інформаційної безпеки в освітній сфері.

УДК 37.014.5:004.9

ISBN 978-617-8421-21-2

ЗМІСТ

ВСТУП

Актуальність теми монографії зумовлена глибинними трансформаціями системи освіти України, що відбуваються в умовах воєнного стану, прискореної цифровізації та стратегічного курсу на європейську інтеграцію. Активне впровадження цифрових сервісів, освітніх платформ, електронного документообігу та інформаційно-аналітичних систем формує нові вимоги до організації управління освітою та потребує створення цілісного, інтегрованого й безпечного інформаційного освітнього простору. Водночас фрагментарність існуючих цифрових рішень, нерівномірний рівень цифрової спроможності закладів освіти, проблеми інтероперабельності та недостатній рівень захисту даних стримують ефективність управлінських процесів і ускладнюють формування доказової державної освітньої політики.

Особливої актуальності ці питання набувають у контексті інтеграції України до Єдиного освітнього простору Європейського Союзу. Гармонізація національних підходів до цифровізації освіти з європейськими стандартами передбачає впровадження принципів інтероперабельності, стандартизації, ефективного управління даними, а також забезпечення належного рівня кібербезпеки та захисту персональних даних. В умовах воєнного стану ці виклики посилюються зростанням кіберзагроз і підвищеними ризиками втрати або несанкціонованого доступу до чутливої інформації, що обумовлює необхідність комплексного наукового осмислення процесів цифрової трансформації освіти.

Монографію присвячено дослідженню процесів цифровізації системи освіти України в умовах євроінтеграції та воєнного стану, а також обґрунтуванню напрямів їх подальшого розвитку.

Монографія має комплексний міждисциплінарний характер і спрямована на формування цілісної науково обґрунтованої концепції розвитку цифрової інфраструктури освіти України в умовах воєнного стану та євроінтеграційних процесів. У роботі цифровізацію освіти розглянуто як системний багаторівневий

процес, що охоплює технологічні, організаційно-управлінські, інституційно-правові та безпекові компоненти. Особливу увагу приділено ролі державних інформаційних освітніх систем і платформ як ключових інструментів забезпечення ефективного управління освітою, підвищення прозорості та підзвітності, а також формування доказової освітньої політики на основі якісних даних. Обґрунтовано необхідність переходу до інтегрованих, інтероперабельних рішень, що відповідають сучасним європейським підходам до управління даними та цифровими сервісами.

Водночас у монографії акцентовано на необхідності інституційного забезпечення процесів цифрової трансформації, зокрема через удосконалення нормативно-правового регулювання, розвиток механізмів координації між різними рівнями управління освітою та впровадження сучасних підходів до управління інформаційними ресурсами. Важливим напрямом дослідження є інтеграція вимог кібербезпеки та захисту персональних даних у процеси проєктування, впровадження та експлуатації освітніх інформаційних систем відповідно до стандартів Європейського Союзу.

Результати дослідження створюють теоретико-методологічне підґрунтя для подальшого розвитку цифрової трансформації освітньої системи України, а також мають прикладне значення для вдосконалення державної політики у сфері цифровізації освіти, модернізації інформаційних систем та забезпечення сталого функціонування освітньої галузі в умовах сучасних викликів і ризиків.

1. ЦИФРОВІЗАЦІЯ СИСТЕМИ ОСВІТИ УКРАЇНИ В КОНТЕКСТІ ІНТЕГРАЦІЇ В ЄДИНИЙ ОСВІТНІЙ ПРОСТІР ЄС

1.1. Оцінка стану розвитку цифровізації системи освіти України в умовах євроінтеграції

У XXI ст. цифровізація стала домінантною тенденцією в освіті, що визначає нову парадигму навчання, управління та взаємодії між учасниками освітнього процесу. Вона охоплює не лише впровадження електронних ресурсів і технологій, а й глибокі структурні зміни в освітній політиці, управлінні даними, оцінюванні та педагогіці. Світова практика демонструє, що цифрова трансформація освіти є необхідною умовою для забезпечення її доступності, гнучкості, інклюзивності та стійкості. Особливо актуалізувалася ця потреба в умовах пандемії COVID-19, яка виявила слабкі місця у цифровій інфраструктурі та управлінських механізмах у більшості країн.

Україна, як держава, що задекларувала стратегічний курс на євроінтеграцію, має відповідати сучасним європейським стандартам у сфері цифрової освіти. Зобов'язання щодо цифровізації передбачені в рамках Угоди про асоціацію з ЄС, а також конкретизуються через участь у програмах Erasmus+, EU4Digital, eTwinning та ініціативі «Цифрове десятиріччя Європи – 2030» [1].

Одним із ключових напрямів співпраці є адаптація української системи освіти до положень Digital Education Action Plan, який орієнтує країни ЄС на забезпечення цифрової готовності закладів освіти, розвиток цифрових компетентностей громадян та використання цифрових технологій у педагогіці. Таким чином, цифровізація в Україні розглядається не лише як внутрішній модернізаційний процес, а і як вимога зовнішньої інтеграційної політики.

В межах цього процесу реалізуються такі ініціативи, як Єдина освітня екосистема, цифрова сертифікація вчителів, розвиток автоматизованих

інформаційних систем (ЄДЕБО, ПАК «АІКОМ») тощо. Актуальність цифровізації також підтримується через взаємодію з Міністерства освіти і науки України (МОН) з Міністерством цифрової трансформації (МЦТ), яке координує впровадження цифрових сервісів в освітній галузі [2].

Світові аналітичні огляди (зокрема, OECD Digital Education Outlook) свідчать, що країни-лідери в освіті інвестують у цифрову трансформацію як у фактор конкурентоспроможності та соціального добробуту [3].

Україна, попри наявні виклики, має потенціал для ефективного розвитку цифрової освіти – це підтверджується активною участю у міжнародних освітніх дослідженнях, підтримкою цифрових реформ з боку донорів, зростаючим попитом на дистанційне навчання та розвитком EdTech-стартапів. Разом із тим, важливим є не лише впровадження цифрових інструментів, а й глибоке переосмислення їхнього впливу на якість освіти, педагогіку та освітню рівність.

Отже, цифровізація освіти в Україні є не просто технічною модернізацією, а ключовим елементом національної політики в умовах євроінтеграції. Вона покликана не лише підвищити ефективність освітнього процесу, а й забезпечити його прозорість, гнучкість і відповідність глобальним викликам. Актуальність цього напрямку підтверджується як міжнародним контекстом, так і внутрішніми потребами української системи освіти. Цифрова трансформація освіти має здійснюватися системно – з урахуванням нормативної, інституційної, методичної та кадрової складових. Такий підхід дозволить забезпечити сталий розвиток освіти як суспільного блага та інструменту інтеграції України до Європейського освітнього простору [4].

Цифровізація освіти є закономірною відповіддю на виклики сучасного інформаційного суспільства та невід’ємною складовою освітніх реформ. У світовому масштабі використання цифрових технологій в освітньому процесі сприяє підвищенню доступності, якості й гнучкості навчання. Цифрові технології докорінно змінюють освітній ландшафт, відкриваючи нові можливості для інновацій в методиках навчання і в управлінні освітніми установами. Особливо це стало помітно під час пандемії COVID-19, коли

дистанційні платформи дозволили тисячам учнів продовжити навчання вдома. Крім того, в умовах воєнного часу цифрові освітні рішення стали критично важливими для забезпечення безперервності навчання, що ще більше актуалізувало розвиток електронних ресурсів та нормативного врегулювання дистанційних форм здобуття освіти. В Україні цифрова трансформація освіти підтримується на найвищому державному рівні – виділяються необхідні ресурси, реалізуються національні проєкти, а нормативна база постійно вдосконалюється. Україна, інтегруючись в глобальний освітній простір, активно впроваджує стратегії цифрової трансформації освіти, які потребують міцного нормативно-правового підґрунтя.

Фундаментальну основу для цифровізації було закладено Законом України «Про освіту» [5] 2017 року, який визначив стратегічні орієнтири розвитку освітньої системи на засадах компетентнісного підходу. Цей закон закріпив інформаційно-комунікаційну компетентність як одну з ключових компетентностей, необхідних кожній сучасній людині для успішної життєдіяльності. Таким чином, цифрова грамотність стала офіційно визнаною складовою освіти. Фактично, поняття цифрової компетентності увійшло до переліку цілей навчання нарівні зі знанням мов, математичною, природничою, громадянською та іншими компетентностями, що мають опанувати випускники закладів освіти. Такий акцент повністю відповідає європейським підходам: у Рамковій програмі ЄС 2018 року цифрову компетентність також визнано однією з восьми ключових компетентностей для навчання впродовж життя [6]. Включення цифрової грамотності до числа пріоритетних освітніх результатів відображає розуміння законодавцем ролі ІКТ у сучасному освітньому процесі. На виконання Закону України «Про освіту» були розроблені нові державні стандарти освіти. Зокрема, Державний стандарт базової середньої освіти (2020 р.) [7] визначає зміст інформаційно-цифрової компетентності, що передбачає впевнене, критичне та відповідальне використання цифрових технологій для власного розвитку і спілкування.

Таким чином, законодавство забезпечило інтеграцію цифрової складової у зміст освіти на всіх рівнях. Реформа «Нова українська школа», в межах якої ухвалювався цей закон, зробила компетентнісний підхід (включно з цифровими навичками) центральним елементом освітньої політики. Освітні програми всіх рівнів тепер обов'язково містять компоненти, спрямовані на формування інформаційно-комунікаційної компетентності. Система підготовки і підвищення кваліфікації педагогічних працівників також передбачає опанування сучасних цифрових технологій. Більше того, затверджені у 2020 р. професійні стандарти для вчителів визначають володіння цифровими технологіями як одну з ключових вимог до компетентностей педагога. В цілому ЗУ «Про освіту» забезпечив інтеграцію ідей цифрової грамотності на всю вертикаль освіти – від початкової школи до післядипломної підготовки. Це створило основу для подальшої цифрової модернізації освітньої системи. Новий освітній закон також стимулював перехід шкіл на сучасні програми навчання інформатики та активне використання інформаційних технологій у навчальному процесі. Таким чином, норми ЗУ «Про освіту» задали тон подальшим змінам освітніх стандартів і програм з урахуванням викликів цифрової епохи.

Окрім змістовних змін, ЗУ «Про освіту» передбачив і нові організаційні форми здобуття освіти, що стали правовою основою для впровадження електронного навчання. Відповідно до статті 9, особа має право навчатися у різних формах або поєднуючи їх; при цьому серед основних форм здобуття освіти визначено інституційну (очну (денну, вечірню), заочну, дистанційну, мережеву) та індивідуальну (екстернат, сімейна (домашня) освіта тощо) [5]. Таким чином, законодавство вперше офіційно легітимувало дистанційну та мережеву форми навчання нарівні з традиційними. Згідно з визначенням, дистанційна форма здобуття освіти – це індивідуалізований процес, що відбувається переважно за опосередкованої взаємодії віддалених один від одного учасників освітнього процесу у спеціалізованому середовищі, яке функціонує на основі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій. Натомість мережева форма передбачає організацію навчання за

участю кількох закладів чи інших суб'єктів, що взаємодіють між собою на договірних засадах для реалізації однієї освітньої програми. Ці норми закону створили необхідне правове підґрунтя для масового запровадження дистанційного та змішаного навчання у системі освіти. На основі положень ЗУ «Про освіту» МОН розробило підзаконні акти, що детально регламентують організацію дистанційного навчання (зокрема, типове положення про дистанційну форму здобуття освіти було затверджено наказом МОН у 2020 р.). Практична значущість цих норм особливо проявилася під час надзвичайних обставин. Навесні 2020 р., в умовах загальнонаціонального карантину, всі школи та університети перейшли на дистанційне навчання, спираючись на законодавчо визначену можливість такої форми. А у 2022–2023 рр., попри воєнні дії та вимушене переміщення тисяч учнів і студентів, освітній процес продовжився завдяки широкому застосуванню дистанційної та змішаної форм навчання, які вже були передбачені законом. Відтепер дистанційна освіта з вимушеного експерименту перетворилася на повноцінно визнану форму навчання із чітким нормативним статусом, що забезпечує гнучкість і стійкість освітньої системи перед сучасними викликами.

Держава визначила цифрову трансформацію сфери освіти і науки як одну з ключових реформ для створення сучасної ефективної системи освіти. На офіційному рівні цифрова трансформація освіти і науки України трактується як комплексна робота над побудовою екосистеми цифрових рішень у сфері освіти та науки. Тобто, йдеться про системне впровадження інформаційно-комунікаційних технологій у всі аспекти освітньої діяльності – від навчальних методик до управління закладами освіти та освітньою статистикою. Цей процес передбачає, що освітній процес дедалі більше спирається на електронні ресурси (цифрові підручники, онлайн-курси, віртуальні симуляції тощо), а взаємодія учасників освіти відбувається через інтернет-платформи. Відповідно, виникає необхідність перегляду традиційних методик навчання і управління на користь інноваційних, гнучких моделей, орієнтованих на потреби «цифрового покоління».

Зокрема, у 2020 р. МОН запустило національну платформу «Всеукраїнська школа онлайн», адміністратором якої є ДНУ «ІОА», що забезпечує учням доступ до відеоуроків і завдань для дистанційного навчання. Університети також впроваджують електронні кампусні системи. Забезпечуються електронний документообіг для студентів, створюються онлайн-кабінети, впроваджуються цифрові студентські квитки тощо. Для педагогів створюються електронні платформи підвищення кваліфікації та професійні онлайн-спільноти, які сприяють поширенню цифрових методик навчання. Цифрова трансформація освітньої сфери реалізується в тісній співпраці МОН з МЦТ. МЦТ залучає освітню галузь до загальнонаціональних цифрових проєктів – зокрема, через портал державних послуг «Дія» вже надаються окремі освітні електронні послуги (наприклад, електронна подача документів на вступ). При МОН створено окремий структурний підрозділ (директорат), відповідальний за впровадження цифрових рішень у галузі. Втілення цифрових технологій в освітню практику передбачає не лише технічні новації, а й глибинну зміну підходів до навчання, орієнтованих на формування в учнів і студентів необхідних для XXI століття компетентностей. Цифрова трансформація освіти – це не одноразовий проєкт, а безперервний процес. Він вимагає регулярного оновлення технологій та навичок усіх учасників освітнього процесу. В цілому цифрова трансформація охоплює всі рівні освіти – від шкіл до університетів – та передбачає модернізацію і навчального процесу, і освітнього менеджменту.

Комплексна цифровізація освіти включає низку взаємопов’язаних напрямів і завдань, спрямованих на якісні зміни в освітній діяльності. По-перше, одним із найважливіших завдань є створення безпечного електронного освітнього середовища, яке гарантуватиме захищеність даних та комфортну взаємодію всіх учасників освітнього процесу онлайн. Одним з важливих аспектів безпечного цифрового середовища є захист даних та кібербезпека: освітні ІТ-системи повинні відповідати сучасним протоколам безпеки, а користувачів навчають правилам безпечної роботи онлайн. По-друге, важливою умовою цифровізації є оснащення закладів освіти належною цифровою

інфраструктурою – сучасною комп'ютерною технікою, швидкісним інтернет-зв'язком, мультимедійним обладнанням тощо. Для розвитку цифрової інфраструктури держава реалізує спеціальні програми розвитку. Зокрема, забезпечуються школи сучасним комп'ютерним обладнанням та підключенням до Інтернету (у тому числі через проєкти «Ноутбук для вчителя» тощо). По-третє, пріоритетним напрямом виступає підвищення рівня цифрової компетентності педагогів і здобувачів освіти, без чого новітні технології не будуть ефективно використовуватися у навчальному процесі. Підвищення цифрової компетентності учасників освітнього процесу відбувається шляхом оновлення змісту освіти (впровадження викладання ІКТ з початкової школи, курси медіаграмотності тощо). Паралельно здійснюється систематичне підвищення кваліфікації педагогів у сфері цифрових технологій. Далі, значущою складовою є цифрова трансформація управлінських процесів та освітніх послуг – перехід від паперового документообігу до електронного, автоматизація рутинних адміністративних завдань, використання аналітики даних для прийняття управлінських рішень. Наприклад, дедалі ширше застосовуються електронні системи збору звітності, що дозволяє вивільнити час педагогів від заповнення паперових документів. Також у багатьох школах і ЗВО вже запроваджено електронні журнали та щоденники, розклади занять онлайн, електронну реєстрацію вступників – ці рішення спрощують взаємодію між учнями, вчителями і адміністрацією та підвищують прозорість управління. Автоматизація збору та аналізу освітніх даних дає змогу приймати обґрунтовані рішення на основі актуальної інформації. У комплексі всі зазначені заходи ведуть до значного скорочення бюрократичних процедур у сфері освіти та спрощення управління навчальними закладами. Виклики останніх років (пандемія 2020 р. і воєнні дії 2022 р.) лише підкреслили критичну важливість руху в зазначених напрямах. Таким чином, усі ці напрями цифровізації освіти взаємно доповнюють один одного, створюючи синергію ефектів.

3 березня 2021 року Кабінет Міністрів України розпорядженням № 167-р схвалив Концепцію розвитку цифрових компетентностей і затвердив план

заходів щодо її реалізації [8]. Цей документ був розроблений МЦТ у співпраці з МОН. Координатором його реалізації Уряд призначив МЦТ. У пояснювальній частині Концепції відзначено, що стрімке впровадження цифрових технологій у всі сфери життя вимагає підвищення якості підготовки працівників для модернізації економіки країни відповідно до сучасних вимог. Водночас наголошено, що відсутність раніше концептуальних засад державної політики у сфері розвитку цифрових навичок громадян не дозволяла забезпечити розвиток усіх сфер суспільного життя на рівні вимог глобальної цифровізації економіки. Концепція дає офіційне визначення терміна «цифрова компетентність». Згідно з цим документом, цифрова компетентність – це динамічна комбінація знань, умінь, навичок, способів мислення, поглядів та інших особистих якостей у сфері ІКТ і цифрових технологій, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність із використанням таких технологій [8]. Вперше на державному рівні було чітко окреслено, що цифрова грамотність є обов'язковою складовою компетентностей сучасної людини. Прийняття Концепції фактично ліквідувало нормативний вакуум у цій сфері. Воно стало відправною точкою для системної роботи з підвищення цифрової грамотності українців. Концепція також містить затверджений план заходів із чітко визначеними завданнями, строками та відповідальними виконавцями. Документ враховує європейський досвід. Він спирається на рекомендації ЄС щодо розвитку цифрових навичок громадян. Слід відзначити, що низький рівень цифрової компетентності населення визнаний серед чинників, що стримують розвиток держави: зокрема, у Державній стратегії регіонального розвитку на 2021–2027 рр. низький рівень цифровізації регіонів названо одним із загальнонаціональних викликів [9].

Також Концепція розвитку цифрових компетентностей окреслює конкретні завдання та заходи для досягнення поставлених цілей. По-перше, вона передбачає створення умов для здобуття громадянами цифрової освіти за допомогою сучасних інформаційних ресурсів (масових онлайн-курсів, освітніх платформ тощо). По-друге, створено єдиний державний вебпортал цифрової

освіти «Дія.Цифрова освіта» для масового навчання населення цифровим навичкам. Цей портал покликаний стати центральною онлайн-платформою для опанування цифрової грамотності. По-третє, Концепція ставить за мету підвищити обізнаність громадян щодо безпечної роботи в інтернеті та мінімізації кіберризиків. Крім того, документ передбачає запровадження нових цифрових засобів доведення інформації, формування належного правового регулювання розвитку цифрових компетентностей і створення системи індикаторів для моніторингу прогресу у сфері цифрової грамотності [10].

Крім того, реалізація запланованих заходів має зробити життя українців комфортнішим у «цифровій державі» – більше державних послуг надаватиметься онлайн. Також очікується зменшення ризиків, які виникають під час користування Інтернетом, завдяки кращій кіберобізнаності населення. Для держави впровадження Концепції означає синхронізацію підходів до розвитку цифрових компетентностей з європейськими стандартами, зменшення «цифрового розриву» та гармонізацію національного цифрового ринку з ринком ЄС. За рахунок Концепції також закладається основа для формування довгострокової національної стратегії і плану дій щодо розвитку цифрових навичок у суспільстві. Показово, що ухвалення Концепції вже стимулювало активність на місцях: органи місцевого самоврядування та інші інституції почали розробляти власні програми та плани дій з підвищення цифрової грамотності населення, продовжуючи ініціативу, започатковану на центральному рівні [9].

Отже, Концепція розвитку цифрових компетентностей стала стратегічним документом, який визначив державну політику у сфері цифрової грамотності і започаткував масштабні практичні заходи. Концепція орієнтована на всі верстви населення – від школярів і студентів до дорослих різного віку – щоб забезпечити кожному можливість опанувати базові цифрові навички.

Цифровізація освіти неможлива без створення сучасної інформаційної інфраструктури управління, важливою складовою якої є електронні реєстри. Для встановлення єдиних правил ведення державних електронних баз даних (реєстрів), у тому числі освітніх, було ухвалено Закон України «Про публічні

електронні реєстри» [10]. Цей закон визначає правові, організаційні та фінансові засади створення і функціонування публічних електронних реєстрів з метою захисту права та інтересів фізичних і юридичних осіб під час створення, зберігання, оброблення та використання інформації у таких реєстрах. Метою є побудова уніфікованої системи електронних реєстрів шляхом забезпечення організаційної, методологічної і технічної єдності їх функціонування по всій країні. Цим законом також запроваджено єдині принципи ведення різних за призначенням реєстрів та їхньої взаємодії між собою.

Система реєстрів охоплює базові реєстри (найважливіші інформаційні системи держави) та інші реєстри. До базових реєстрів, зокрема, віднесено Єдиний державний демографічний реєстр, Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Державний земельний кадастр, Державний реєстр речових прав на нерухоме майно тощо. До інших належать електронні реєстри, держателями яких є органи державної влади або місцевого самоврядування і які містять усю іншу інформацію (наприклад, про виконавчі документи, нормативні акти, судові рішення тощо). Для забезпечення обміну даними між різними базами передбачено згідно із ЗУ «Про публічні електронні реєстри» функціонування національної системи електронної взаємодії – зокрема, системи «Трембіта», за допомогою якої реєстри безперервно обмінюються інформацією один з одним у режимі реального часу.

Після набрання чинності ЗУ «Про публічні електронні реєстри» держава перейшла до практичної реалізації його норм, у т. ч. в освітній сфері. Зокрема, 1 вересня 2023 р. КМУ затвердив Порядок функціонування Реєстру публічних електронних реєстрів – центральної системи, що містить опис і перелік всіх державних е-реєстрів та координує їх взаємодію [11]. В освітній галузі впровадження єдиних принципів для публічних реєстрів дало змогу інтегрувати освітні інформаційні ресурси у загальнодержавну цифрову інфраструктуру. Так, Єдина державна електронна база з питань освіти (ЄДЕБО), що функціонує з 2012 р. як основна освітня база даних, нині діє за уніфікованими стандартами і взаємодіє з іншими державними інформаційними системами. ЄДЕБО містить,

зокрема, Реєстр суб'єктів освітньої діяльності (перелік усіх закладів вищої, професійної, фахової передвищої та загальної середньої освіти), Реєстр документів про освіту (інформація для перевірки достовірності виданих дипломів, атестатів тощо), Реєстр сертифікатів ЗНО та інші тематичні бази даних [12]. Завдяки включенню ЄДЕБО до загальної системи, освітні дані можуть обмінюватися з іншими державними ресурсами – наприклад, перевірка персональних даних вступників відбувається через взаємодію з демографічним реєстром, а відомості про видані дипломи зіставляються з реєстром актів цивільного стану при працевлаштуванні.

Крім того, на основі освітніх реєстрів надаються нові електронні послуги. Зокрема, через вебпортал «Вступ» абітурієнти можуть подавати заявки до закладів вищої та фахової передвищої освіти онлайн, а приймальні комісії – обробляти їх електронно. Також створено відкриті сервіси для перевірки достовірності документів про освіту – будь-який роботодавець чи громадянин може за кілька секунд переконатися в чинності диплома або студентського квитка, звернувшись до електронного реєстру документів про освіту. Уніфікація освітніх реєстрів підвищує захищеність персональних даних (через єдині стандарти кібербезпеки) та усуває дублювання інформації, адже різні відомства використовують погоджені між собою джерела даних. В результаті створюється єдиний інформаційний простір освіти, у якому дані про учнів, студентів, освітні програми та інші аспекти можуть ефективно використовуватися для аналітики, прийняття управлінських рішень і надання зручних електронних сервісів усім учасникам освітнього процесу.

Отже, нормативно-правове забезпечення цифровізації освіти в Україні сформувало цілісну багаторівневу систему документів – від стратегічних концепцій до конкретних законів, – яка спрямована на всебічну підтримку цифрової трансформації галузі. Державна політика цифрової трансформації освіти і науки окреслила бачення та пріоритети розвитку, заклавши ідеологічні засади переходу до єдиного цифрового освітнього простору. Концепція розвитку цифрових компетентностей доповнила цю політику, зосередившись на

людському капіталі – формуванні в громадян необхідних цифрових навичок і знань – та створивши умови для масового навчання цифрової грамотності. ЗУ «Про освіту» інституційно закріпив необхідність цифрової компетентності та гнучкості освітнього процесу, визнавши цифрову компетентність однією з ключових і відкривши правове поле для дистанційного навчання та освітніх інновацій. ЗУ «Про публічні електронні реєстри» забезпечив фундамент для побудови сучасної ІТ-інфраструктури управління освітою, уніфікувавши принципи ведення освітніх баз даних і їх інтеграцію з іншими державними системами. Усі ці елементи нормативної бази працюють у комплексі, підсилюючи один одного: від підготовки учасників освітнього процесу до цифрової ери – до технічного забезпечення електронного урядування в освіті. Як результат, українська освітня система отримала необхідні юридичні механізми для цифрового розвитку, що вже сьогодні дозволяє впроваджувати цифрові інструменти на практиці та підвищувати стійкість і конкурентоспроможність освіти. Водночас нормативна база продовжує вдосконалюватися у відповідь на виклики часу. Стратегічний курс держави на набуття повноправного членства України в ЄС потребує подальшої адаптації освітнього законодавства до європейського, зокрема у цифровій сфері.

Таким чином, створена в Україні система нормативно-правових актів забезпечує надійне підґрунтя для успішної цифрової трансформації освіти – вона визначає стратегічні орієнтири, встановлює необхідні стандарти і правила та мобілізує ресурси для переведення освітніх процесів на якісно новий цифровий рівень.

1.2. Стан розвитку освітніх інформаційних технологій в Україні

Цифрова інфраструктура закладів освіти в Україні охоплює комп’ютерну техніку, доступ до інтернету та використання сучасних цифрових платформ, що

разом визначають можливості для якісного навчання. В нашій країні розвиток цифрового освітнього середовища проголошений стратегічним пріоритетом.

Більшість закладів освіти вже забезпечені комп'ютерами: загалом 96,9 % шкіл України мають хоча б одну комп'ютерну техніку (96,7 % у міських і 97,1 % у сільських громадах). Проте цього недостатньо – у середньому на один працюючий комп'ютер припадає 16 учнів, а в окремих областях, таких як Рівненська, навантаження сягає 20-21 учень на комп'ютер [13]. Для покращення ситуації держава реалізує програми оновлення техніки: зокрема, у 2021 р. було закуплено понад 60 тисяч ноутбуків для вчителів, що частково компенсувало дефіцит комп'ютерів у школах.

Майже всі школи вже підключені до інтернету – станом на 2023 р. доступ до мережі мають близько 97 % закладів. При цьому 68,9 % шкіл використовують широкосмуговий дротовий інтернет із застосуванням оптоволоконних ліній. Найтиповіша швидкість з'єднання – 30-100 Мбіт/с (таке підключення має 62,5 % закладів), хоча понад чверть шкіл уже отримали інтернет швидкістю понад 100 Мбіт/с. Деякі віддалені або постраждалі від війни школи покладаються на бездротовий доступ – зокрема, супутниковий інтернет Starlink допоміг відновити зв'язок у сільських школах Київщини після бойових дій [13].

Базова ІТ-інфраструктура шкіл охоплює локальні мережі та периферійні пристрої: зокрема, у понад 94 % закладів наявні принтери та копіювальна техніка, а в багатьох облаштовано Wi-Fi для доступу до мережі. Освітні установи дедалі активніше застосовують інтерактивні комплекси (мультимедійні проєктори, інтерактивні дошки тощо) з метою підвищення ефективності навчання. За підтримки міжнародних партнерів впроваджуються рішення і для надзвичайних ситуацій: у 2023 р. в межах проєкту «Цифрові школи» школам передали 1 600 Wi-Fi роутерів та 1 000 вебкамер для обладнання укриттів і кабінетів інформатики [14].

Цифрові середовища та освітні онлайн-платформи відіграють дедалі більшу роль у навчальному процесі. В школах активно впроваджуються електронні журнали й системи дистанційного навчання. Державний е-журнал на

початку 2022 р. вже використовували близько 700 шкіл, а платформою «Всеукраїнська школа онлайн» – понад 275 тис. користувачів (учнів і педагогів). В умовах пандемії та війни більшість шкіл опанували інструменти для онлайн-навчання (Zoom, Google Classroom, Moodle тощо), що дозволило продовжувати освітній процес на відстані. Цифрові платформи також широко застосовуються у закладах вищої освіти, де розгорнуто електронні кампуси, бібліотеки та системи управління навчанням.

Забезпеченість цифровою інфраструктурою суттєво різниться між регіонами. У низці областей (зокрема, Черкаській, Одеській, Тернопільській) всі міські школи мають підключення до інтернету, тоді як у прифронтових регіонах цей показник знизився – у Запорізькій області частка шкіл з інтернетом скоротилася на 19 %, у Харківській – на 6 % внаслідок бойових дій. Частка шкільних комп'ютерів, підключених до мережі, перевищує 80 % у ряді західних і центральних областей, водночас у Чернігівській і Житомирській вона не досягає й 60 %. Кількість учнів на один комп'ютер також варіює: якщо на Рівненщині навантаження найбільше (близько 20 учнів на ПК), то в деяких інших регіонах цей показник суттєво нижчий (на Миколаївщині та Сумщині) [13].

За оцінками, близько 772 тис. українських школярів під час війни змінили форму навчання на дистанційну або домашню, що стало можливим лише завдяки наявній цифровій інфраструктурі. Лише 15 % шкіл у 2022/2023 н. р. працювали повністю офлайн; решта перейшли на дистанційне (33 %) чи змішане (51 %) навчання, тож загалом понад 92 % закладів забезпечували освітній процес онлайн у тій чи іншій формі. Для підтримання безперервності освіти залучено різноманітні ІТ-рішення – від платформ відеозв'язку до альтернативних каналів зв'язку. Наприклад, супутниковий інтернет Starlink допоміг відновити навчання у звільнених селах Київщини, а шкільні укриття обладнують Wi-Fi, щоб діти могли навчатися навіть під час повітряних тривог [15].

Особливий виклик становить організація навчання для дітей на тимчасово окупованих територіях (ТОТ), що залишаються поза контролем української влади. Попри ризики, в 2025 р. близько 42 557 українських школярів

продовжують здобувати освіту за українською програмою навіть в окупації [16]. Більшість із них за сприятливих умов підключаються до уроків дистанційно через інтернет, проте постійні проблеми зі зв'язком або безпекою часто унеможливлюють регулярні онлайн-заняття. Для таких випадків МОН запровадило альтернативні формати навчання. Окрім сімейної (домашньої) освіти та екстернату, було організовано систему педагогічного патронажу – індивідуальної роботи вчителя з учнем за гнучким графіком. Педагогічний патронаж дозволяє вчителю вибудувати для дитини індивідуальну траєкторію навчання, підлаштовану під її можливості та обставини (зокрема, уроки проводяться тоді, коли є зв'язок, або маленькими групами дітей, що мешкають по-сусідству). Ця форма освіти визнана МОН оптимальною для дітей в окупації і нині активно впроваджується та роз'яснюється батькам, щоб жодна дитина не залишилася без української школи.

Для підтримки здобувачів освіти в ТОТ та прифронтових зонах держава також розгорнула мережу дистанційних шкіл і надала їм більше автономії. Нині в кожній області України діє принаймні одна дистанційна школа, яка може зарахувати учнів незалежно від їхнього місця проживання. Таким школам дозволено працювати навіть за умови невеликого набору – якщо не вдається сформувати повноцінні класи певної паралелі, навчання все одно проводять індивідуально або в малих групах. Місцева влада отримала право фінансувати групи дистанційного навчання зі зменшеною чисельністю учнів – до 10 осіб на клас у селах та прифронтових чи окупованих територіях (що вдвічі менше від норми). Це рішення дає змогу офіційно продовжувати навчання навіть для невеликої кількості дітей, які залишаються на небезпечних територіях чи в евакуації. Загалом, станом на кінець 2025 р. понад 390 000 українських школярів в Україні та за її межами продовжують здобувати знання дистанційно – ця цифра свідчить про масштаб зусиль, докладених для підтримки освіти кожної дитини незалежно від місця перебування [16].

Масштабне впровадження цифрової освіти в Україні під час війни стало можливим завдяки безпрецедентній міжнародній підтримці. Український уряд

налагодив тісну співпрацю з міжнародними організаціями, донорами та технологічними компаніями, що згуртувалися для порятунку освіти. Цифровізація освітнього процесу в Україні розглядається як частина глобальної стратегії стійкості: зусилля нашої держави узгоджені з Європейським Планом дій з цифрової освіти (2021–2027) [1], а Україна, отримавши статус кандидата в ЄС, отримує значну гуманітарну допомогу на підтримку освітнього сектору. З перших місяців війни міжнародні фонди зосередилися на екстреному забезпеченні українських школярів та вчителів необхідними ресурсами для дистанційного навчання (табл. 1.1).

Таблиця 1.1

Приклади міжнародних ініціатив на підтримку цифрової освіти України

Ініціатива / проєкт	Опис та досягнення
Device Coalition (коаліція пристроїв)	Об'єднання світових виробників комп'ютерної техніки, донорів і НУО під егідою МОН для постачання сучасних ноутбуків і планшетів українським школярам. На 2023 р. було визначено потребу ~330 тис. дітей та 68 тис. учителів у 10 регіонах, які потребують девайсів для онлайн-навчання
Ноутбуки для вчителів (UNESCO + Google)	Спільний проєкт ЮНЕСКО та Google, в рамках якого протягом 2022–2023 рр. українським педагогам було безкоштовно надано 50 000 Chromebook-ноутбуків. Це забезпечило безперервність навчання для десятків тисяч учителів, у т.ч. внутрішньо переміщених, та підвищило якість онлайн-уроків
Digital Learning Centers (UNICEF & GPE)	Створення мережі цифрових освітніх центрів у прифронтових областях за фінансування Глобального партнерства в освіті (GPE) та реалізації UNICEF. Відкрито щонайменше 34 центри на сході й півдні України, які відвідали вже понад 17 000 дітей, надолужуючи навчальну програму у безпечних умовах
Education Cannot Wait (ECW)	Глобальний фонд підтримки освіти в надзвичайних ситуаціях виділив Україні 5 млн дол. США екстреної допомоги (2022 р.) та започаткував програму стійкості з бюджетом 18 млн дол. США на 2024–2026 рр. Кошти спрямовано на забезпечення безперервності навчання, психосоціальну підтримку учнів та відбудову освітнього середовища
Інші проєкти та фонди	ЄС мобілізував близько 3,7 млрд Євро гуманітарної допомоги (2022–2025 рр.), частина якої пішла на освітні потреби. Світовий банк запустив проєкт LEARN (100 млн дол. США) для підвищення безпеки шкіл, перевезення учнів та забезпечення навчальними матеріалами. Coursera відкрила доступ українським студентам до 5 800 онлайн-курсів, а провідні ІТ-компанії надали хмарні сервіси і програмне забезпечення для навчання

Складено авторами за: [18–20].

Завдяки цим міжнародним проєктам українська освіта отримала життєво необхідні ресурси. Зокрема, кошти Global Partnership for Education (GPE) були спрямовані на розгортання цифрових рішень: у квітні 2023 р. GPE виділив Україні 25,5 млн дол. США прискореного гранту, а загальний пакет підтримки склав понад 51 млн дол. США. Це фінансування дозволило закупити тисячі пристроїв, профінансувати навчальні центри та тренінги для вчителів. Так само, фонд Education Cannot Wait ще з березня 2022 р. інвестує в підтримку освітніх потреб українських дітей, забезпечуючи як негайну допомогу, так і довгострокову відбудову системи. Важливу роль відіграють і прямі гуманітарні внески урядів різних держав та ЄС: зусиллями європейських партнерів українські школи отримали сучасне обладнання, навчальні матеріали і доступ до інтернету навіть у кризових умовах [17].

Міжнародна підтримка не обмежується матеріально-технічними ресурсами – також надається експертна допомога у впровадженні освітніх реформ і підвищенні стійкості системи. Під час UNESCO Digital Learning Week 2023 світові експерти відзначили український досвід як зразок освітньої стійкості завдяки EdTech-рішенням. На основі українських уроків для урядів інших країн, що переживають кризи, сформульовано рекомендації – інвестувати в цифрову інфраструктуру завчасно, будувати партнерства з ІТ-сектором під державною координацією та поєднувати гнучкість із підзвітністю під час реагування на кризи. Таким чином, підтримка міжнародної спільноти не лише допомогла Україні втримати освітній процес під час війни, але й сприяє трансформації освіти, роблячи її більш технологічно оснащеною, інклюзивною та стійкою до викликів майбутнього.

Оцінювання рівня цифрової компетентності вчителів спирається на спеціально розроблені рамки та стандарти. На європейському рівні ключовим орієнтиром є Європейська рамка цифрових компетентностей для педагогів DigCompEdu, яка визначає 6 різних сфер компетентностей та загалом 22 компетентності, необхідні сучасному вчителю. DigCompEdu пропонує також 6 рівнів професійної майстерності – від A1 (новачок) до C2 (піонер), що дозволяє

педагогам оцінити власний прогрес від базового до експертного володіння цифровими навичками. Рамка DigCompEdu акцентує увагу на тому, що вчитель має володіти цифровими технологіями для впровадження ефективних, інклюзивних та інноваційних стратегій навчання [21].

У 2021 р. в Україні було адаптовано й впроваджено національну рамку цифрової компетентності педагогічних працівників, розроблену на основі європейських підходів. Національна рамка цифрової компетентності педагогічних і науково-педагогічних працівників охоплює 5 сфер компетентностей (замість шести в DigCompEdu) і містить 22 конкретизовані компетентності, а також визначає 5 рівнів оволодіння цифровими навичками. Цей документ слугує інструментом для розробки освітніх стандартів і програм підвищення кваліфікації в Україні, а також для самооцінювання вчителів щодо їхньої цифрової компетентності [22].

В табл. 1.2 наведено порівняльний опис основних параметрів європейської та української рамок цифрової компетентності педагогів.

Таблиця 1.2

Порівняння європейської та української рамок цифрової компетентності педагогів

Рамка компетентностей	Сфери/області	Кількість компетентностей	Рівні володіння
Європейська DigCompEdu (European Commission, 2017 р.)	6 сфер	22	6 (A1–C2)
Українська рамка (МЦТ, 2021 р.)	5 сфер	22	5

Складено авторами за: [21].

Дослідження останніх років показують, що цифрові навички українських освітян помітно різняться за напрямами. Зокрема, результати всеукраїнського опитування 2022–2023 рр. засвідчили, що у сферах комунікації та співпраці та створення цифрового контенту більшість учителів продемонстрували високий рівень компетентності (понад 60 % опитаних), тоді як у сфері розв’язання проблем рівень в середньому наближається до 46 % (середній показник).

Натомість у сфері цифрової безпеки та базового програмування частка впевнених користувачів залишається меншою за 36 %, що вказує на прогалини у цих напрямах. Лише близько 15 % педагогів виявили зацікавленість та навички у використанні сучасних інструментів штучного інтелекту для професійних цілей [23]. Отже, попри загальне підвищення цифрової грамотності, існують специфічні області, де педагоги потребують подальшого розвитку навичок.

Розуміючи важливість цифрових навичок, держава та освітні інституції впроваджують програми професійного розвитку для педагогів. МОН включило цифрову компетентність до переліку ключових навичок у професійному стандарті вчителя та директора школи. Це закріплено нормативно, зокрема наказом МОН від 15.01.2019 № 38 [24], який передбачив розробку професійних ІКТ-компетентностей учителів. У співпраці з технологічними компаніями та громадськими організаціями МОН регулярно організовує масові тренінги й вебінари для освітян. За останні роки за підтримки партнерів (наприклад, корпорації Google, Microsoft) було проведено декілька масштабних навчальних проєктів, охопивши тисячі вчителів по всій Україні. Такі заходи спрямовані на оволодіння сучасними інструментами онлайн-навчання, інтерактивними платформами, методиками змішаного і дистанційного навчання тощо.

Попри виклики, цифрова інфраструктура української освіти поступово відновлюється і розвивається. Держава разом із партнерами реалізує стратегію цифрової трансформації освіти [25], впроваджуючи проєкти на кшталт «Цифрові школи» для оснащення закладів технікою, високошвидкісним інтернетом та електронним контентом. Останні роки – від пандемії до війни – переконливо довели критичну важливість інвестицій у цифрові технології, аби освітній процес залишався стійким і доступним за будь-яких обставин.

Цифровізація освіти в Україні супроводжується впровадженням різних інформаційних систем для закладів освіти. Крім основних централізованих платформ, діють і інші державні освітні інформаційні системи – серед них, зокрема, автоматизована система «Школа» (АС «Школа»), а також розгалужені рішення типу електронних журналів і щоденників. Такі системи покликані

підвищити ефективність управління освітою та замінити застарілий паперовий документообіг на цифровий аналог. Наприклад, впровадження стандарту електронного класного журналу дозволяє відмовитися від ведення до 16 паперових документів у школі [26], а платформи електронного журналу й щоденника дають можливість фіксувати відвідування та оцінки онлайн, забезпечуючи доступ до даних учням, батькам і вчителям у режимі реального часу.

АС «Школа» є прикладом державної інформаційної системи, розробленої для закладівзагальної середньої освіти. Ця система автоматизує ключові процеси діяльності школи – від планування розкладу й обліку успішності до формування статистичної звітності [27]. Важливо, що АС «Школа» інтегрується з національними освітніми реєстрами та базами даних: забезпечено повну взаємодію з ЄДЕБО, Українським центром оцінювання якості освіти (УЦОЯО) та іншими відомчими системами. Таким чином, дані про учнів, навчальні плани і успішність синхронізуються з центральними ресурсами МОН, створюючи єдиний інформаційний простір. Крім того, система «Школа» дозволяє автоматично формувати заявки на виготовлення документів про освіту державного зразка (атестатів, учнівських квитків), що значно спрощує діловодство закладу.

Окремої уваги заслуговують електронні журнали та щоденники, що фактично стали обов’язковим атрибутом сучасної школи. Державні та приватні розробники пропонують численні варіанти таких систем. Зокрема, існує державний е-журнал, який школи можуть використовувати безкоштовно, або альтернативні рішення від приватних компаній, за умови відповідності останніх вимогам законодавства. Функціонально ці інструменти повністю дублюють і розширюють можливості паперових класних журналів. Приміром, платформа «Єдина школа» після підключення до державної бази даних ПАК «АІКОМ» стала цифровим аналогом шкільного журналу і щоденника: вона дозволяє занотовувати зміст уроків, виставляти оцінки та вести розклад онлайн [28]. Таким чином, школярі і їхні батьки можуть оперативно отримувати інформацію

про успішність, а вчителі – спростити рутинну звітність. Більшість сучасних е-журналів також мають функціонал електронного щоденника, де фіксуються домашні завдання, оголошення та зауваження, що робить комунікацію між школою і родиною прозорішою і ефективнішою. В цілому розмаїття державних ІТ-систем – від великих комплексів до точкових застосунків – створює основу для переведення освітнього процесу на цифрові рейки на всіх рівнях.

Інтеграція освітніх інформаційних систем із системами електронної ідентифікації є важливим напрямом цифрової трансформації. Використання платформ на кшталт ID.GOV.UA (Інтегрованої системи електронної ідентифікації) дозволяє надійно підтверджувати особу користувача під час доступу до освітніх онлайн-сервісів [29]. Система ID.GOV.UA виступає єдиною точкою входу, через яку учні, батьки чи педагоги можуть проходити автентифікацію за допомогою банківської ідентифікації (BankID), електронного підпису чи інших засобів, перш ніж отримати доступ до персональних даних або електронних послуг. Наприклад, нова державна освітня екосистема «Мрія» реалізує вхід користувачів саме через портал ID.GOV.UA: при спробі авторизації система перенаправляє на відповідний сервіс eID для підтвердження особи [30]. Це гарантує, що до чутливої інформації (успішність учня, контактні дані тощо) отримують доступ тільки належним чином ідентифіковані та уповноважені особи.

Крім автентифікації користувачів, інтеграція з цифровими ідентифікаційними сервісами відкриває можливості для юридично значимих електронних транзакцій у сфері освіти. Зокрема, впроваджується Дія.Підпис – кваліфікований електронний підпис, доступний через мобільний застосунок «Дія», який користувач може отримати онлайн та використовувати для підписання документів [31]. Використання Дія.Підпису та інших засобів електронного підпису у взаємодії з освітніми інформаційними системами дозволяє переводити в електронну форму такі процедури, як підписання класних журналів, заяв на зарахування або звітних документів. Наприклад, учитель або директор школи можуть накласти свій електронний підпис (сертифікат) на

семестровий звіт успішності чи наказ по школі, після чого цей документ матиме таку саму юридичну силу, як паперовий із «мокрою» печаткою. Це істотно спрощує документообіг і прискорює обмін інформацією. Важливо, що платформи типу ID.GOV.UA забезпечують дотримання законодавчих вимог щодо захисту інформації під час таких операцій, а також сумісність із європейськими стандартами транскордонної електронної ідентифікації. Отже, зв'язка «освітні системи – BankID – Дія.Підпис» нині стає основою для безпечної та зручної роботи користувачів у цифровому освітньому середовищі.

Не менш значущою є роль приватних ІТ-рішень у підтримці освітнього процесу. Комерційні компанії та ІТ-стартапи активно доповнюють державні ініціативи, пропонуючи школам і університетам сучасні програмні продукти – від електронних журналів до повнофункціональних систем управління навчанням (LMS) і CRM-платформ для освітніх закладів. Часто такі рішення впроваджуються швидше та гнучкіше, враховуючи специфічні потреби користувачів. Приміром, протягом пандемії COVID-19 багато шкіл перейшли на використання приватних сервісів на кшталт Google Classroom або Moodle для організації дистанційного навчання. Ці системи дозволяють створювати онлайн-курси, розміщувати навчальні матеріали, проводити тести і відстежувати прогрес учнів у режимі реального часу. Паралельно, низка вітчизняних компаній розробила власні платформи електронного журналу і щоденника, що конкурують за зручністю та функціоналом. Деякі з них, як-от вже згадані «Єдина школа» чи «Eddy», були інтегровані з державною системою ПАК «АІКОМ» і передають дані до центральної бази МОН [32]. Завдяки цьому школи отримують сучасний інтерфейс та розширені можливості від приватного продукту, і водночас гарантію, що всі необхідні дані автоматично надходять до державної звітності (табл. 1.3).

Як видно з табл. 1.3, приватні рішення часто охоплюють різні аспекти освітнього процесу. Зокрема, платформа «HUMAN Школа» позиціюється як комплексна CRM-система для школи, що одночасно включає в себе і функції е-журналу, і модулі дистанційного навчання. У 2022 р. розробники «HUMAN»

запропонували українським школам безоплатно користуватися їхньою системою під час воєнного стану, щоб підтримати безперервність навчання. Ця платформа дає змогу цифровізувати як очне, так і дистанційне навчання, зменшуючи навантаження на вчителів шляхом автоматизації рутинних процесів. Зокрема, система аналізує освітню траєкторію кожного учня та надає адміністрації інструменти для індивідуальної підтримки: на основі зібраних даних про оцінки і прогрес можна вчасно виявити тих, хто відстає, і запропонувати їм додаткові ресурси або консультації. Для самих учнів платформи типу HUMAN створюють безпечне внутрішнє середовище спілкування і доступ до матеріалів, що є особливо актуальним у разі вимушеного переїзду чи навчання з-за кордону під час війни.

Таблиця 1.3

Приватні ІТ-рішення для підтримки освіти

Категорія рішення	Приклади	Призначення в освітньому процесі
Електронний журнал та щоденник	«Human Школа», «Єдина школа», «Нові знання», «Всеосвіта»	Ведення електронного класного журналу: облік відвідування, оцінок, домашніх завдань; забезпечення комунікації між учителями, учнями і батьками; повна заміна паперової документації
Система управління навчанням (LMS)	Google Classroom, Moodle, Classtime	Організація дистанційного та змішаного навчання: розміщення матеріалів, проведення онлайн-занять і тестувань; відстеження успішності і залученості учнів; підтримка спільної роботи над проєктами
CRM та комплексні шкільні платформи	«HUMAN Школа», «Моя Школа», «School Champion»	Централізоване управління закладом освіти: ведення баз даних учнів і працівників, електронний документообіг (накази, розклади, звіти); аналітика показників (успішності, відвідування); інструменти для внутрішньої комунікації та оповіщень

Складено авторами

Як видно з табл. 1.3, приватні рішення часто охоплюють різні аспекти освітнього процесу. Зокрема, платформа «HUMAN Школа» позиціюється як комплексна CRM-система для школи, що одночасно включає в себе і функції е-журналу, і модулі дистанційного навчання. У 2022 р. розробники «HUMAN» запропонували українським школам безоплатно користуватися їхньою системою

під час воєнного стану, щоб підтримати безперервність навчання. Ця платформа дає змогу цифровізувати як очне, так і дистанційне навчання, зменшуючи навантаження на вчителів шляхом автоматизації рутинних процесів. Зокрема, система аналізує освітню траєкторію кожного учня та надає адміністрації інструменти для індивідуальної підтримки: на основі зібраних даних про оцінки і прогрес можна вчасно виявити тих, хто відстає, і запропонувати їм додаткові ресурси або консультації. Для самих учнів платформи типу HUMAN створюють безпечне внутрішнє середовище спілкування і доступ до матеріалів, що є особливо актуальним у разі вимушеного переїзду чи навчання з-за кордону під час війни.

Неодмінною умовою сучасного управління освітою є використання аналітичних систем і великих даних (Big Data). Зростання обсягів інформації відкриває перед освітніми установами нові можливості для прийняття рішень на основі даних. Аналітика даних дозволяє переходити від інтуїтивного управління до доказового (evidence-based) – коли рішення приймаються на підставі статистичних показників, трендів і прогнозів. Інтеграція технологій Big Data в освітній процес обіцяє справжню революцію у навчанні, оскільки надає глибоке розуміння поведінки учнів, рівня їхньої успішності та дозволяє оптимізувати навчальні стратегії.

Наповнене даними освітнє середовище генерує величезні масиви різнорідної інформації – від оцінок і результатів тестів до журналів відвідування, активності учнів у електронних системах і навіть їхніх вподобань при виборі факультативів. Сучасні аналітичні платформи здатні збирати ці дані в реальному часі, очищувати, агрегувати їх і наочно представляти у вигляді діаграм, панелей індикаторів (dashboard), звітів тощо. Для керівників освіти це означає можливість оперативно відстежувати ключові показники – наприклад, середній бал по школі чи районі, результати НМТ, статистику відвідування – і виявляти проблемні зони, що вимагають реагування.

Великі дані відкривають шлях до більш персоналізованого та адаптивного навчання. На рівні класу та окремого учня аналітичні інструменти дають

педагогам детальні підказки для коригування методики. Скажімо, якщо система бачить, що учень систематично витрачає більше часу на виконання завдань з математики та отримує нижчі оцінки, вона може рекомендувати вчителю надати цьому учневі додаткові матеріали або консультації. У впроваджених системах Big Data вчителі отримують детальну аналітику успішності учнів на основі їхніх оцінок, часу виконання домашніх завдань і активності в онлайн-курсах, що дозволяє адаптувати навчальну програму під потреби конкретного класу чи навіть учня. З іншого боку, самі учні можуть отримувати індивідуальні рекомендації щодо тем або ресурсів для додаткового опанування – на основі виявлених прогалин у знаннях чи, навпаки, виявлених обдарувань у певній сфері. Такий підхід значно підвищує ефективність навчання, роблячи його більш гнучким і орієнтованим на особистість дитини. Вже зараз у світі існують системи раннього попередження про академічну неуспішність, що аналізують великі дані (відвідування, бали, поведінкові фактори) і сигналізують про ризик відрахування чи потребу в додатковій підтримці конкретного учня.

Аналітичні системи корисні не лише на рівні школи, а й для органів управління освітою. Агреговані «великі дані» на рівні міста чи країни допомагають планувати освітню політику, розподіляти ресурси та оцінювати вплив нововведень. В Україні з 2023 р. розгорнуто нову версію ПАК (АІКОМ) – ПАК «АІКОМ 2.0», який акумулює дані шкільної мережі для потреб МОН і місцевих управлінь. До ПАК «АІКОМ 2.0» підключаються різні освітні платформи, і завдяки цьому централізована база даних отримує актуальні відомості з кожної школи автоматично. Такий підхід дозволяє автоматизувати збір і обробку статистичних даних, істотно скоротивши навантаження на вчителів у частині звітності. Замість того, щоб множити паперові форми або вручну дублювати інформацію в кількох системах, достатньо один раз внести дані в електронний журнал – і вони вже доступні для аналізу на верхніх рівнях. Наприклад, показники охоплення дітей освітою, наповнюваності класів, забезпеченості підручниками чи результати державної підсумкової атестації

можуть збиратися в режимі реального часу через електронні системи і відображатися на аналітичних панелях для керівників.

Широке застосування великих даних порушує і нові питання – зокрема, проблеми сумісності, стандартизації та захисту даних. Через історично фрагментований підхід різні школи використовували різноманітні програмні продукти, які не завжди «вміли» обмінюватися інформацією між собою. Це створювало проблеми сумісності: відсутність єдиних стандартів даних ускладнювала перенос даних з однієї системи в іншу і вимагала дублювання роботи. Сьогодні вирішення цієї проблеми лежить у площині впровадження уніфікованих державних стандартів та інтеграційних платформ. Процес, започаткований МОН через ПАК «АІКОМ», саме спрямований на забезпечення інтероперабельності – зовнішні освітні системи проходять процедуру тестування і підключення, після чого їхні дані автоматично синхронізуються з центральною базою. Таким чином, поступово формується стандарт взаємодії: щоб програмний продукт міг використовуватися у закладах освіти, він має підтримувати визначені державою формати даних, протоколи обміну і рівень захисту інформації.

Стандартизація стосується не лише форматів файлів чи протоколів, а й самих довідників та класифікаторів освітньої інформації. Для коректного об’єднання даних необхідно, щоб всі системи трактували базові сутності (учень, клас, предмет, оцінка тощо) однаково. З цією метою затверджуються єдині довідники навчальних закладів, спеціальностей, навчальних планів, які мають використовувати різні інформаційні системи. Ініціативи на кшталт відкритих наборів даних про заклади освіти або реєстру учнів допомагають створити спільне інформаційне поле, де кожному учню чи школі відповідає унікальний ідентифікатор. У майбутньому перехід на міжнародні стандарти (наприклад, Experience API для навчальних даних чи стандарт Learning Analytics Interoperability) дозволить українським системам легко інтегруватися зі світовими платформами. Вже зараз у рамках ЄС триває робота над

забезпеченням сумісності національних освітніх реєстрів для обміну даними, і Україна, цифровізуючи свою освіту, враховує ці глобальні тренди.

Для успішної цифрової трансформації освітньої сфери визначено кілька пріоритетних напрямів розвитку:

- Розширення цифрової інфраструктури: забезпечення закладів освіти необхідною технікою та інтернет-підключенням, створення мережі центрів для доступу до цифрових ресурсів у громадах.
- Доступ до якісного цифрового контенту: розробка і впровадження онлайн-ресурсів для навчання.
- Підвищення цифрових навичок учасників освіти: масштабне навчання педагогів цифровій грамотності і розвиток цифрової та медіаграмотності учнів.
- Цифрове управління та електронні послуги: модернізація освітніх інформаційно-управлінських систем та розвиток електронних сервісів для освіти [17].

До 2030 р. очікується реалізація ключових ініціатив у сфері освіти в Україні, які закладуть основу для цифрової освіти майбутнього. Серед пріоритетних кроків – оснащення закладів освіти (особливо у прифронтових та сільських регіонах) сучасними комп'ютерами, мультимедійним обладнанням і швидкісним інтернетом, модернізація шкільної інфраструктури за принципом «відбудувати краще, ніж було» (*build back better*), а також створення широкого спектру інтерактивного цифрового контенту для забезпечення доступності, інклюзивності й інноваційності навчання. Очікувані результати цифровізації освіти до 2030 р. включають підвищення якості та гнучкості освітнього процесу, подолання цифрового розриву між різними групами населення, а також сформовану культуру безперервного розвитку цифрових навичок у вчителів і учнів.

В найближчій перспективі можна очікувати, що освітня система стане більш стійкою до зовнішніх викликів та гнучкою до змін. Практично всі школи матимуть доступ до швидкісного інтернету, а цифрові технології будуть повсякденно інтегровані в навчальний процес. Учні отримають рівні можливості

доступу до якісного е-контенту незалежно від місця проживання, що сприятиме освітній рівності. Педагоги широко використовуватимуть інструменти ШІ для персоналізації навчання та аналізу успішності, що дозволить підвищити навчальні результати школярів. Участь у європейському цифровому освітньому просторі забезпечить визнання українських електронних сертифікатів і взаємообмін освітніми ресурсами з країнами ЄС. Таким чином, до 2030 року цифрова трансформація освіти має призвести до якісно нового рівня організації навчання – більш ефективного, інклюзивного, безпечного та орієнтованого на потреби суспільства майбутнього.

1.3. Проблеми формування інформаційного освітнього простору України

Формування інформаційного освітнього простору – це комплексний процес створення середовища, яке сприяє доступу до інформації, розвитку навичок критичного мислення, аналізу та креативності серед громадян. Цей простір має на меті не лише передачу знань, але і навчання людей критично оцінювати інформацію, використовувати її в різних контекстах та приймати обґрунтовані рішення.

Аналітики відзначають, що головним досягненням нинішнього етапу інформатизації загальної середньої освіти є впровадження дистанційної форми навчання як системи засобів відкритого доступу до інформаційних ресурсів, самостійної роботи учасників навчального процесу та їх інтенсивного спілкування. Інформаційний освітній простір стає новою організаційно-педагогічною системою функціонування загальноосвітнього навчального закладу з можливостями відкритого й віддаленого доступу до навчальних ресурсів, інноваційної професійної діяльності педагогічних колективів, постійного моніторингу здобутих учнями знань, набутих умінь і навичок та інтерактивної взаємодії суб’єктів освітнього процесу.

Основні аспекти формування інформаційного освітнього простору включають:

По-перше, забезпечення широкого доступу до різноманітної, достовірної та актуальної інформації.

По-друге, навчання навичкам розуміння, аналізу та взаємодії з різноманітними медійними форматами дозволяє розпізнавати фейки та маніпуляції інформацією.

По-третє, розвиток навичок критичного мислення для аналізу інформації, оцінки її джерел та визначення обґрунтованості думок і точок зору.

По-четверте, освоєння розуміння принципів роботи Інтернету, використання електронних ресурсів та інструментів ля збору та обробки інформації.

По-п’яте, створення умов для розвитку творчості та самовираження учнів шляхом використання інформаційних технологій, медійних платформ та інших ресурсів.

По-шосте, розвиток навичок співпраці та комунікації, що сприяє розвитку ефективної комунікації та співпраці в інформаційному середовищі.

Ці аспекти взаємодіють між собою і сприяють створенню освітнього середовища, яке дозволяє учням ефективно використовувати інформацію для власного розвитку та для участі в суспільстві.

Мета, завдання та функції створення єдиного інформаційного простору наведено на рис. 1.1–1.3.

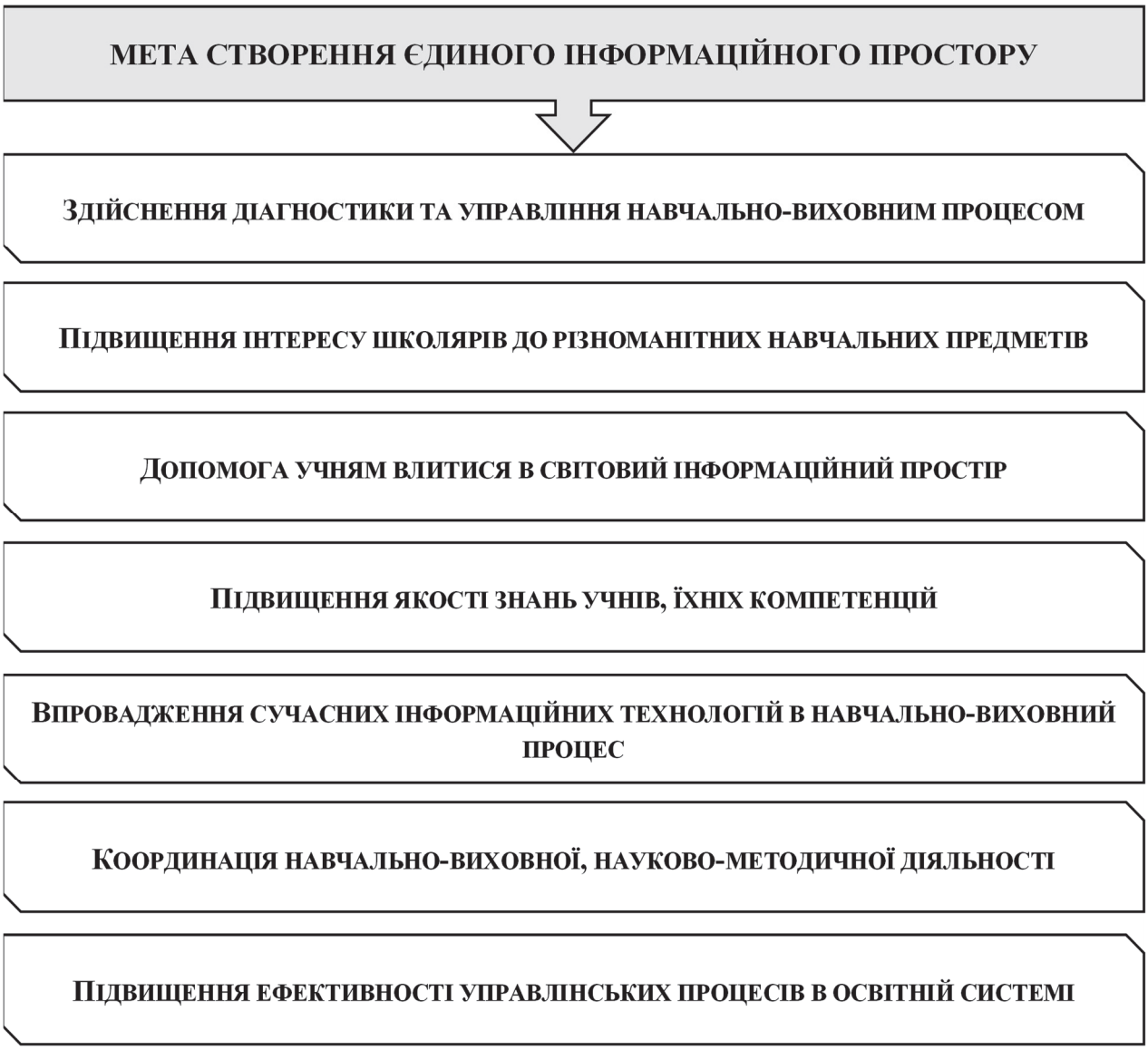


Рис. 1.1. **Мета створення єдиного інформаційного простору**
Побудовано авторами.

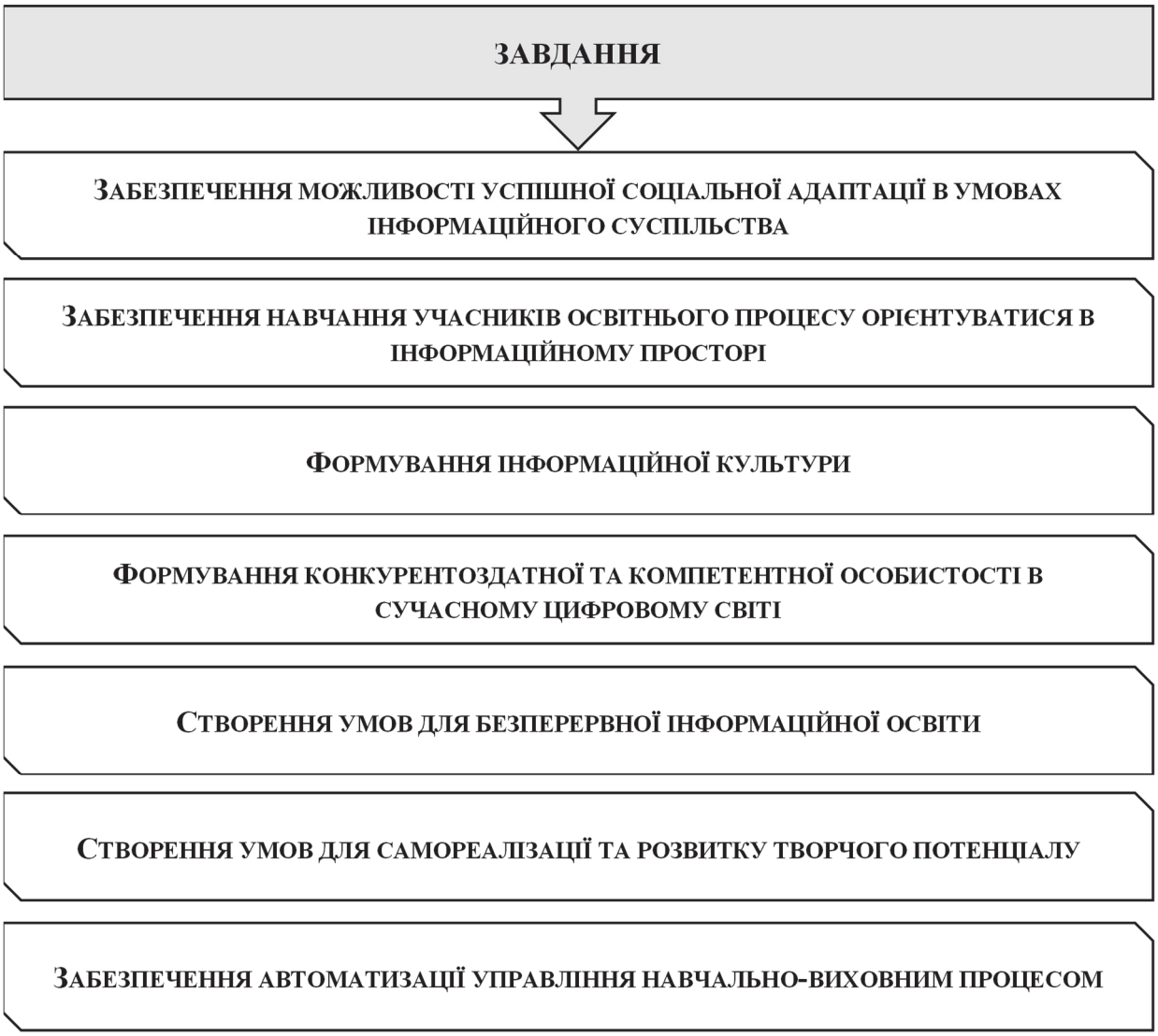


Рис. 1.2. **Завдання створення єдиного інформаційного простору**

Побудовано авторами.

Рис. 1.3. **Функції єдиного інформаційного простору**

Побудовано авторами.

Формування інформаційного освітнього простору в Україні – це комплексний процес, який включає в себе створення та розвиток системи освіти, доступу до інформації, а також підтримку та розвиток інформаційних технологій.

Формування інформаційного освітнього простору в Україні відбуваються відповідно до умов розвитку освітньої системи, а також знаходиться під впливом низки чинників, зокрема:

- розвиток інформаційно-комунікаційних технологій (ІКТ) в навчальних закладах;
- забезпечення доступу до сучасних технологій у навчальних закладах;
- впровадження інтерактивних методів навчання з використанням сучасних засобів технічної оснастки;
- стимулювання інновацій в освіті, включаючи впровадження електронних підручників та онлайн-курсів;
- наявність програм підвищення кваліфікації вчителів у галузі ІКТ;
- розвиток платформ для дистанційного навчання та самонавчання;
- забезпечення доступу до електронних ресурсів для навчання, онлайн-курсів та дослідження;
- розвиток електронних бібліотек та інтерактивних навчальних матеріалів;
- розробка та впровадження програм інформаційної грамотності в освітніх закладах;
- забезпечення доступу до навчальних матеріалів для розвитку навичок критичного мислення та оцінки інформації;
- забезпечення широкого доступу до Інтернету для учнів та студентів;
- розвиток інфраструктури для забезпечення якісного Інтернет-з’єднання;
- підтримка стартапів та інноваційних проектів в галузі освіти та технологій;
- впровадження новітніх методик та технологій у навчальний процес;

- наявність тренінгів та курсів для вчителів щодо ефективного використання медіа ресурсів у навчальному процесі;

- забезпечення співпраці з ІТ-компаніями, громадськими організаціями та урядовими структурами для спільного розвитку інформаційного освітнього простору;

- включення питань інформаційної безпеки у навчальні програми;

- проведення інформаційних кампаній щодо захисту особистих даних та безпеки в Інтернеті;

- залучення до вивчення інформаційного мислення як навички критичного та аналітичного мислення.

Вищезазначене створює умови до ефективного користування інформаційними ресурсами та адаптації до змін у сучасному інформаційному середовищі. Завдяки цьому можна створити освітній простір, де учасники освітнього процесу зможуть ефективно користуватися інформацією, розуміти її та адекватно реагувати на виклики сучасності. Розвиток інформаційного освітнього простору є важливим аспектом для підготовки учнів до викликів сучасного світу, де інформація та технології швидко змінюються.

Поряд із зазначеним, формування інформаційного освітнього простору в Україні може зіткнутися з різними проблемами, які відображають сучасний стан суспільства та освітніх систем, зокрема:

1. Наявність доступу до інформації. Не всі учасники освітнього процесу мають однаковий доступ до інформації через різницю в рівнях технічної грамотності та доступу до інтернету. Це може створювати нерівності в можливостях отримання освіти через інтернет.

2. Недостатнє фінансування освіти може обмежувати можливості впровадження сучасних технологій та методик викладання. Нестача коштів може впливати на розвиток інформаційно-технологічних інфраструктур та професійну підготовку вчителів тощо.

3. Наявність цифрового розриву. Розрив між тими, хто має доступ до технологій і може вільно користуватися інтернетом, і тими, хто цього не може,

може зростати. Це стосується як міських, так і сільських областей, де інфраструктура може бути менше розвиненою.

4. Низька якість інформаційної освіти. Слід зважати, що не завжди інформаційна освіта в школах та вишах відповідає сучасним вимогам. Нестача актуального змісту та методологій, які сприяють розвитку критичного мислення та навичок аналізу, може стати перешкодою для вивчення сучасних технологій та інформаційної грамотності.

5. Недостатній рівень підготовки вчителів. Вчителі повинні мати необхідні знання та навички для викладання інформаційних технологій. Програми підготовки вчителів повинні включати актуальні педагогічні та інформаційно-технологічні аспекти.

6. Зростання десинформації та кіберзагроз може ускладнювати формування інформаційного освітнього простору. Учасники освітнього процесу повинні мати навички розпізнавання недостовірної інформації та вміти забезпечувати свою кібербезпеку.

Розв’язання цих проблем вимагає комплексного підходу, який включає в себе покращення фінансування освіти, розробку та впровадження сучасних програм та методик викладання, підтримку вчителів та розвиток доступу до інтернету. Також важливо зосередитися на розвитку критичного мислення та навичок аналізу в освітньому процесі.

2. МОДЕРНІЗАЦІЯ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ ОСВІТНІХ СИСТЕМ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ОСВІТОЮ В УКРАЇНІ

2.1. Національні інформаційні системи управління освітою

В Україні функціонують інформаційні та освітні платформи у різних складниках освіти: дошкільна, повна загальна середня, професійна (професійно-технічна), вища. Нижче подано опис основних освітніх інформаційних систем.

ПАК «АІКОМ» [26] – національна інформаційно-аналітична система, призначена для використання суб'єктами освітньої діяльності з метою ефективного управління закладом освіти у сфері дошкільної, загальної середньої, позашкільної, професійної (професійно-технічної) та фахової передвищої освіти.

У ПАК «АІКОМ» накопичується, зберігається та здійснюється автоматизоване оброблення освітньої статистики для розподілу коштів освітньої субвенції, ведення обліку дітей дошкільного та шкільного віку, формування переліку підручників, обраних закладами освіти для їх подальшого розподілу та доставки до закладів освіти, ведення обліку закладів дошкільної освіти, ведення електронних щоденників і журналів (e-journal) та електронного документообігу, ведення фінансової звітності закладів освіти, ведення обліку закладів позашкільної освіти, підвищення кваліфікації педагогічних працівників, ведення обліку учнів, слухачів, педагогічних працівників та матеріально-технічного забезпечення закладів професійної (професійно-технічної) освіти.

Користувачами інформаційної системи є усі учасники освітнього процесу та управлінці.

Функції АІКОМ:

- збір достовірних, актуальних даних про стан системи освіти за затвердженою системою показників та автоматичною генерацією звітності;

- забезпечення органів управління і громадськості статистичними даними для прийняття ефективних управлінських рішень щодо підвищення доступності та якості освіти, ефективності використання державних коштів;

- реалізація можливості взаємодії ПАК «АІКОМ» з різними освітніми системами, базами даних та державними реєстрами;

- розвантаження освітян від необхідності заповнення різних форм звітності та паперової роботи;

- запровадження національного обліку дітей дошкільного та шкільного віку;

- запровадження процесів зарахування, відрахування та переведення учнів до закладів загальної середньої освіти на базі ПАК «АІКОМ»;

- створення електронних сервісів та послуг для батьків.

ЄДЕБО (Єдина державна електронна база з питань освіти) [33].

Централізована електронна система, що містить дані про заклади освіти, учнів, студентів, педагогічних працівників, результати навчання та освітні документи. Вона забезпечує автоматизований облік і контроль у сфері освіти, а також використовується для вступної кампанії, видачі дипломів і сертифікатів. ЄДЕБО є основою для прийняття рішень у сфері державної освітньої політики. Система ЄДЕБО переважно працює в складнику вищої освіти. До основного функціоналу ЄДЕБО належить:

- забезпечення інформаційного супроводження вступної кампанії до закладів вищої освіти;

- використання даних ЄДЕБО для виготовлення студентських (учнівських) квитків державного зразка;

- використання даних ЄДЕБО для виготовлення документів про вищу та професійну (професійно-технічну) освіту.

Інформація, що міститься в Єдиній державній електронній базі з питань освіти, крім персональних даних та інформації з обмеженим доступом, є доступною у форматі відкритих даних, у тому числі з урахуванням потреб осіб з

порушенням зору. Особа має повний доступ до всіх відомостей про себе, внесених до ЄДЕБО.

ІСУО (Інформаційна система управління освітою) [34]. Система охоплює усі заклади освіти та дозволяє співробітникам місцевих органів управління освітою автоматично сформувати статистичні звіти. Для потреб органу управління освітою та закладів освіти був розроблений додатковий функціонал «Конструктор форм», який дозволяє створити будь-які внутрішні звітності (кількість комп'ютерного забезпечення, паспорт навчальних закладів і т.п.) та автоматично отримувати інформацію від установ в електронному вигляді. ІСУО має трирівневу архітектуру і складається з клієнтського ПЗ, веб-порталів та бази даних. ІСУО має масштабовану архітектуру, що не залежить від архітектури апаратного забезпечення і типу операційної системи. Це дозволяє збільшення кількості користувачів та об’єму даних без втрати працездатності під час інтенсивного навантаження.

«Eddy» – це онлайн-сервіс для шкіл, який надає інструменти для ведення електронних щоденників, журналів, розкладів і комунікації між учнями, батьками та вчителями [35]. До функціоналу «Eddy» належить:

- інструменти для адміністрування навчальних матеріалів та контролю проведення онлайн-занять;
- для подання всіх необхідних документів та проходження всіх етапів під час вступу до вашого закладу;
- для наповнення та налаштувань сторінок платформи, публікації новин, подій та інших презентаційних матеріалів вашого закладу;
- для контролю та агрегації всіх даних успішності учнів вашого закладу;
- для налаштування, внесення та редагування інтерактивного розкладу для всіх користувачів;
- адміністрування класів та додаткових груп для проведення факультативів тощо.

Зручні інструменти для класних керівників; можливість підключення повноцінної системи контролю звітності, документообігу та організаційних

питань; модуль для проведення організаційних онлайн-нарад або зустрічей з колегами без часових обмежень.

«Human Школа» – це хмарна система для організації навчального процесу з електронним журналом, тестуванням, аналітикою і внутрішнім чатом [36]. «Human» поєднує в собі такий функціонал:

- комунікація (об'єднання користувачів в окремих тематичних просторах); навчальні матеріали;
- календарно-тематичне планування;
- перевірка знань; оцінювання та відвідуваність;
- учні і батьки можуть переглядати розклад уроків, отримані оцінки, відсутність та запізнення, дедлайни по завданням і статуси їх виконання;
- класний керівник може занотовувати в систему інформацію про щоденну активність учня;
- система надає можливість для ведення, формування і друку всієї необхідної звітності відповідно чинного законодавства; дозволяє переглядати динаміку і рівень успішності учнів, вчителів, класів, курсів і закладу в цілому;
- система надає можливість створювати необмежену кількість розкладів уроків з різними правилами повторюваності і тривалості уроків, та використовувати архівні розклади тощо.

«Моя школа» – це онлайн-платформа для електронного документообігу в школі, створення електронних журналів та індивідуальних навчальних планів [37]. «Моя школа» має наступний функціонал:

- доступ до навчальних матеріалів, домашніх завдань, розкладу уроків;
- можливість ділитися навчальними матеріалами з однокласниками, простір для дискусій, обговорень, спільної роботи;
- можливість відстежувати оцінки, домашні завдання, порівняльний аналіз успішності дитини, тенденції, відвідуваність;
- спілкування з класними керівниками та керівництвом школи;
- дозволяє обирати системи навчання, тривалість занять, рівні навчання, системи оцінок;

- учителям надані умови для складання планів навчання на кожен урок, триместр/семестр і навчальний рік;

- вчителі можуть стежити за успішністю свого виховного класу, організовувати позакласну діяльність, батьківські збори, проводити опитування, голосування, спонукати батьків до участі в житті класу і школи;

- керівники шкіл завжди мають доступ до інформації про плани навчання та успішності учнів; широкий спектр звітів дозволяє одержувати результати на рівні класу і школи та порівнювати їх з попередніми періодами.

«Всеосвіта» є освітньою платформою для вчителів і учнів із матеріалами, тестами, вебінарами, онлайн-курсами та конкурсами [38]. «Всеосвіта» Орієнтована на підтримку педагогів і неформальну освіту. Основний функціонал платформи «Всеосвіта»:

- бібліотека навчальних матеріалів (доступ до тисяч розробок уроків та можливість публікувати власні авторські матеріали);

- онлайн-тестування та перевірка знань; курси підвищення кваліфікації для педагогів; журнали та планування (частково);

- конкурси, олімпіади та інші активності;

- комунікація та професійна спільнота (внутрішні групи, обговорення, новини освіти, блоги та форуми для педагогів) [38].

«OIC Prosvita» – це система автоматизації документообігу та освітніх процесів у школах (щоденники, журнали, комунікація, розклади) [39]. Функціонал «OIC Prosvita»:

- електронний журнал та щоденник (ведення оцінок, обліку відвідуваності, домашніх завдань та коментарів учителів.

- учні та батьки мають доступ до поточної успішності в режимі онлайн);

- електронний розклад (автоматизоване створення розкладів занять, гнучке редагування для адміністрації та відображення для учнів і педагогів);

- адміністрування школи (ведення обліку класів, учнів, працівників, навчальних планів та розкладів, генерація внутрішньої документації: наказів, табелів, звітів для закладу);

- комунікація (інтегровані повідомлення між учасниками освітнього процесу (учні, батьки, вчителі, адміністрація), повідомлення про оцінки, завдання, події);

- аналітика та звітність (внутрішня) (статистика по класах, предметах, відвідуваності, успішності);

- особисті кабінети (розмежування ролей (вчитель, учень, батько, адміністратор) з відповідним функціоналом для кожного).

«Мрія» – державна онлайн-платформа для дистанційного навчання з курсами, відеоуроками, електронними матеріалами.

Основний функціонал платформи «Мрія»:

- цифрова бібліотека відеоуроків;
- розробки уроків та методичні рекомендації (презентації, тести, завдання, інструкції з організації дистанційного навчання);
- платформа для учнів (доступна навігація за класами, предметами, темами);
- адаптація контенту для різного рівня технічного забезпечення тощо.

«Мрія» ще знаходиться на стадії розробки [30].

«Єдина школа» є підсистемою ІСУО для ведення електронних журналів, щоденників, розкладів, заяв на зарахування. Портал надає такі інструменти різним зацікавленим сторонам, зокрема [34]:

– можливість для батьків переглянути інформацію по ЗЗСО та подати заяву на реєстрацію в один чи декілька ЗЗСО;

– для закладів загальної середньої освіти можливість отримувати та обробляти заяви батьків он-лайн режимі (роздруковувати готові форми заяв, згоди на обробку персональних даних, тощо);

– автоматизувати розподіл заяв на першочергові та другочергові;

– отримати журнал заяв як електронний архів, імпортувати дані в Excel;

– надавати попередню інформацію про заклад (гуртки, секції, особливості навчання, профілі, мови навчання тощо);

– для обласних управлінь освіти збирати статистику по кількості заяв до першого класу в розрізі шкіл;

– переглядати наповнюваність закладів загальної середньої освіти; отримувати інформацію по кількості вільних місць в закладах;

– аналізувати статистику заяв та наповнюваність закладів для їх подальшого розвитку та модернізації.

«SMART школа» – освітня онлайн-платформа, що пропонує модулі для електронних журналів, системи домашніх завдань, електронних бібліотек, комунікації, електронного документообігу та звітності всередині школи. Ця платформа з відеоуроками, розроблена за підтримки МОН для дистанційного навчання в умовах війни.

До основного функціоналу SMART школи належать різні сервіси, зокрема:

- формування розкладу навчальних занять;
- доступ до журналів успішності всіх класів (академічних груп);
- електронний щоденник;
- всі уроки на одному сайті;
- доступ до матеріалів уроку згідно розкладу занять;
- нагадування про створення нових уроків та наповнення їх навчальним матеріалом; збереження історії;
- електронні журнали;
- швидке створення уроку та доповнення матеріалами;
- здобувачі освіти завантажують результати роботи на особисту сторінку для їх подальшої перевірки;
- перегляд історії активності здобувачів освіти;
- єдина платформа для організації та проведення уроків в онлайн режимі;
- перегляд послідовності створених уроків та їх наповнення;
- керування списками учнів, батьків та викладачів;
- тарифікація викладачів;
- розподіл робочого часу викладачів;
- доступ до всіх типів звітності;

- ведення повної статистики (оцінки, активність здобувачів освіти, активність вчителів, класи, предмети) тощо [40].

ОІС «Навчання і Технології» [41] – це освітня інформаційна система, орієнтована на автоматизацію навчального процесу, ведення шкільної документації, електронних журналів, табелів успішності та розкладів. Також передбачена функція комунікації між усіма учасниками освітнього процесу. Функціонал ОІС «Навчання і Технології» включає в себе:

- електронні журнали та щоденники: ведення поточної успішності, облік відвідуваності, тем уроків та домашніх завдань, окремі кабінети для учнів, вчителів і батьків із доступом до навчального процесу;

- автоматизоване створення та ведення розкладу: інструменти для формування розкладу занять з урахуванням навантаження, кабінетів і обмежень, можливість редагування та оперативного оновлення змін;

- документообіг і управлінська діяльність школи: формування звітів, табелів, аналітики щодо навчального процесу, контингенту та навантаження, внутрішні накази, облік кадрів та інше адміністрування;

- комунікація: система повідомлень між школою, учнями та батьками, оголошення, нагадування, сповіщення про зміни в розкладі або оцінки;

- мобільний додаток: окремий зручний додаток для смартфонів із базовими функціями електронного щоденника.

Портал послуг е-школа – це державний портал, який надає адміністративні освітні послуги для громадян, зокрема: заяви на зарахування до школи, переведення, електронні витяги, сервіси для батьків і закладів. Створений у межах цифровізації освіти, інтегрований з ЄДЕБО [42].

До основного функціоналу належить:

1) електронний журнал, доступ до нього мають вчителі-предметники, класний керівник, директор;

2) електронний щоденник (на підставі даних, внесених вчителями до журналів, для кожного учня формується його електронний щоденник; у щоденнику відображено все, що вчителі внесли до журналу (відмітки,пропуски,

коментарі тощо), а також поведінка і зауваження за кожен тиждень; для батьків є можливість «підписувати» щоденник своєї дитини. Батьки учня мають доступ до всіх даних тільки своєї дитини);

3) таблиця успішності (для кожного учня є зведена таблиця всіх відміток, отриманих за чверть з усіх предметів; у таблиці містяться також усі пропуски, середній бал і четвертна відмітка по кожному предмету);

4) графіки успішності (для кожного учня і кожного класу доступна статистика успішності в графічному вигляді);

5) розклад уроків учня і вчителя; розклад шкільних дзвінків, чвертей і канікул; персональні сторінки кожного користувача; спілкування всередині школи (табл. 2.1).

Таблиця 2.1

Порівняльна характеристика освітніх інформаційних систем в Україні

Система	Тип / рівень	Сегмент освіти	Ключові функції	Основні користувачі	Статус
ПАК «АІКОМ»	Національна інформаційно-аналітична система (національний рівень)	Дошкілля, ЗЗСО, позашкілля, П(ПТ)О	Освітня статистика; е-документообіг; е-журнали/щоденники; аналітика; облік дітей і закладів; інтеграція з реєстрами	МОН, органи управління, заклади освіти, вчителі, батьки, громадськість	Державна
ЄДЕБО	Державна реєстрова ІС (національний рівень)	Переважно **вища** + частково П(ПТ)О	Вступна кампанія; облік; формування/замовлення документів; відкриті дані (без персональних)	МОН/органи, ЗВО/ЗПТО, вступники	Державна
ІСУО	Управлінська ІС + звітність (нац./регіональний рівні)	Дошкілля + ЗЗСО (+ частково інше)	Статзвітність (76-РВК, 83-РВК тощо) з ЕЦП; конструктор форм; модулі обліку дітей, підручники, ліцензування	ОУО, заклади, ОДА	Приватна
Єдина школа (school.isuo.org)	Підсистема ІСУО (локальний рівень закладу)	ЗЗСО	Е-журнал/щоденник/розклад; заяви на зарахування; кабінети для батьків і шкіл; статистика для ОУО	Батьки, школи, ОУО/ОДА	Приватна
Портал послуг (e-schools.info)	Державний сервіс/портал послуг	ЗЗСО (адмінпослуги)	Заяви/витяги/сервіси для громадян; журнал/щоденник/успішність (за описом)	Батьки, учні, школи, органи	Державна
Eddy	Хмарна шкільна платформа (локальний рівень)	ЗЗСО	Е-журнал/щоденник/розклад; комунікація; аналітика успішності; адміністрування; CRM-елементи	Школи, вчителі, батьки, учні	Приватна
Human Школа	Хмарна шкільна платформа (локальний рівень + кабінет департаменту)	ЗЗСО	Е-журнал; тестування; аналітика; чат; планування; звітність; адміністрування; кабінет управління	Школи, вчителі, батьки, учні, управління	Приватна
Моя школа (moiashkola.ua)	Платформа для документообігу/журналів (локальний рівень)	ЗЗСО	Е-журнали; індивідуальні плани; навчальні матеріали; аналітика успішності; інструменти для керівників	Учні/батьки/вчителі/адміністрація	Приватна
ОІС Prosvita	Шкільна ОІС (локальний рівень)	ЗЗСО	Е-журнал/щоденник; розклад; адміністрування; комунікація; внутрішня звітність	Школи, вчителі, батьки, учні	Приватна
Мрія (mriya.education)	Державна платформа контенту/дистанційного навчання	ЗЗСО (підтримка дистанційного)	Відеоуроки; навчальні матеріали; бібліотека; доступ 24/7; партнерства	Учні, вчителі, батьки	Державна
Всеосвіта	Освітня платформа контенту/підвищення кваліфікації	Переважно ЗЗСО (педагоги/учні)	Бібліотека матеріалів; тестування; вебінари/курси; конкурси; спільнота	Вчителі, учні	Приватна/ громадська платформа

Складено авторами за: [26; 33–42].

Проведений аналіз дає змогу нам говорити, що на сьогодні в Україні немає повноцінного аналога ПАК «АІКОМ».

Жодна з існуючих освітніх інформаційних систем, як державних, так і комерційних, не охоплює настільки широкий набір функцій, який поєднує управлінські, аналітичні, звітні та сервісні можливості одночасно для кількох рівнів освіти від дошкільної до фахової передвищої. ПАК «АІКОМ» є єдиною системою, яка забезпечує інтеграцію з державними реєстрами.

Інші платформи, такі як ІСУО, Human, Eddy або Всеосвіта, здебільшого орієнтовані на організацію навчального процесу, облік успішності або підтримку дистанційного навчання. Водночас вони не забезпечують централізованого збору та перевірки статистичних даних, необхідних для цілей державного управління освітою.

На відміну від них, ПАК «АІКОМ» є державним інструментом стратегічного рівня, призначеним для підтримки прийняття управлінських рішень, прозорого розподілу ресурсів та надання публічних освітніх сервісів. Завдяки модульній архітектурі та нормативній інтегрованості ПАК «АІКОМ» відіграє важливу роль у цифровій трансформації системи освіти України.

Загалом в Україні сформувалася різноманітна система національних і локальних освітніх інформаційних систем, які виконують різні функції на рівні держави, органів управління освітою та закладів освіти.

Державні системи забезпечують облік, управління та надання адміністративних освітніх послуг, тоді як локальні та комерційні платформи зосереджені на організації навчального процесу й комунікації між учасниками освіти. Сукупність таких систем створює основу для цифровізації управління освітою, однак водночас актуалізує питання їх інтеграції, узгодженості даних і застосування системного аналізу для подальшого розвитку.

2.2. Основні проблеми функціонування та інтеграції національних освітніх інформаційних систем

Попередній аналіз проведений у першому та другому розділах дали змогу виокремити низку проблем функціонування та інтеграції національних освітніх інформаційних систем.

По-перше, фрагментарність інформаційних систем. Однією з ключових проблем є наявність великої кількості окремих освітніх інформаційних систем, які розроблялися у різний час, для різних цілей і без єдиної архітектурної концепції. У результаті дані зберігаються в різних системах, дублюються або не узгоджуються між собою, що ускладнює формування цілісної картини стану освіти.

По-друге, низький рівень інтеграції між системами. Багато освітніх ІС не мають налагоджених механізмів обміну даними між собою та з державними реєстрами. Це призводить до необхідності багаторазового введення одних і тих самих даних на різних рівнях управління, підвищує ризик помилок і знижує ефективність використання інформації.

По-третє, дублювання даних і навантаження на користувачів. Працівники закладів освіти та органів управління часто змушені заповнювати однакову або подібну інформацію в кількох системах одночасно. Таке дублювання не лише збільшує адміністративне навантаження, а й негативно впливає на якість даних через різні формати та строки подання звітності.

По-четверте, проблеми якості та повноти даних. Ще однією суттєвою проблемою є недостатня якість освітніх даних, що проявляється у помилках, неповноті або застарілості інформації. Причинами цього є як людський фактор, так і відсутність автоматизованих механізмів перевірки та верифікації даних під час їх внесення до систем.

По-п’яте, відсутність уніфікованих стандартів даних. У національних освітніх інформаційних системах часто використовуються різні підходи до структури показників, форматів даних і класифікаторів. Це ускладнює

порівняння інформації між системами, регіонами та рівнями освіти, а також обмежує можливості аналітичної обробки даних.

По-шосте, обмежені аналітичні можливості систем. Багато освітніх ІС орієнтовані переважно на облік і звітність, але мають недостатньо розвинені інструменти аналітики. У результаті зібрані дані використовуються не в повному обсязі для прогнозування, оцінювання ефективності рішень та планування розвитку освіти.

По-сьоме, проблеми нормативного та організаційного характеру. Функціонування та інтеграція освітніх інформаційних систем часто ускладнюються через недосконаліть нормативно-правового регулювання, часті зміни вимог до звітності та нечіткий розподіл відповідальності між різними суб'єктами. Це створює додаткові труднощі для стабільної роботи систем.

По-восьме, питання захисту персональних даних та інформаційної безпеки. Інтеграція освітніх ІС пов'язана з обробкою значних обсягів персональних даних учнів і педагогічних працівників. Не всі системи однаковою мірою відповідають вимогам інформаційної безпеки, що створює ризики витоку даних та обмежує можливості обміну інформацією між системами.

Вважаємо за потрібне більш детально зупинитися саме на питання захисту персональних даних та інформаційній безпеці. Адже в умовах широкомасштабної війни це набуває виключно важливого значення.

На сучасному етапі розвитку інформаційно-комунікаційних технологій питання кібербезпеки стають однією з найбільш проблемних сфер, зокрема в системі освіти, яка активно переходить у цифровий формат. Впровадження освітніх інформаційних систем в Україні супроводжується накопиченням значних обсягів персональних і службових даних, таких як інформація про учнів, педагогічних працівників і діяльність закладів освіти. За умов недостатнього рівня захисту інформації це створює серйозні ризики несанкціонованого доступу, витоку або неправомірного використання даних, що негативно впливає на довіру до цифрових сервісів у сфері освіти [43].

Проблемність інформаційної безпеки посилюється тим, що освітній процес, управління закладами освіти та аналітична діяльність усе більше залежать від електронних платформ і цифрових сервісів. Не всі наявні освітні інформаційні системи забезпечують достатній рівень технічного та організаційного захисту даних, що робить їх вразливими до кіберзагроз. У результаті виникає проблема забезпечення безпечного обміну інформацією між системами та надійного збереження персональних даних учасників освітнього процесу.

Додатковою проблемою є необхідність приведення національних освітніх інформаційних систем у відповідність до європейських вимог у сфері захисту персональних даних. У межах євроінтеграційних процесів Україна зобов'язана адаптувати свої підходи до положень Загального регламенту ЄС про захист даних (GDPR), що вимагає значних організаційних, правових і технічних змін. Недостатня підготовленість окремих освітніх установ і користувачів до таких вимог ускладнює практичну реалізацію цих стандартів.

Так, питання захисту персональних даних та інформаційної безпеки є однією з ключових проблем функціонування та інтеграції національних освітніх інформаційних систем. Її невирішеність стримує подальший розвиток цифрової освіти та потребує комплексного підходу, що поєднує технічні рішення, нормативне регулювання та підвищення цифрової грамотності користувачів.

2.3. Визначення критеріїв та показників ефективності освітніх інформаційних систем

У ході дослідження було встановлено, що архітектура освітніх інформаційних систем України є досить фрагментованою. Це проявляється у розпорошеності даних, дублюванні окремих функцій та відсутності єдиного підходу до взаємодії між різними підсистемами. Більшість освітніх ІС створювалися у різні періоди та за різними організаційними підходами, часто без

узгодження з єдиною державною цифровою стратегією. У результаті це призвело до неузгодженості та дисбалансу в структурі систем. Так, ЄДЕБО зосереджена переважно на вищій освіті та проведенні вступних кампаній, ПАК «АІКОМ» виконує функції управлінської аналітики й забезпечує збір адміністративної звітності у сфері дошкільної, загальної середньої та позашкільної освіти, тоді як більшість приватних систем виконують окремі, обмежені функції, зокрема ведення електронних журналів і щоденників, не маючи доступу до всіх первинних даних.

Ефективність освітніх інформаційних систем доцільно оцінювати на основі чітко визначених критеріїв і кількісних показників, які відображають реальний стан їх функціонування та рівень впливу на управління освітою. В умовах фрагментованості національного цифрового освітнього середовища особливо важливо перейти від описового аналізу до формалізованого оцінювання, що дозволяє порівнювати різні системи між собою та відстежувати динаміку їх розвитку.

На основі системного аналізу освітніх ІС України можна виділити п’ять ключових груп критеріїв ефективності:

- інтероперабельність;
- якість даних;
- рівень інтеграції;
- економічна доцільність;
- надійність функціонування.

Саме ці критерії найбільш повно відображають проблеми, пов’язані з дублюванням даних, паралельним веденням звітності та обмеженою аналітичною спроможністю систем.

Першим критерієм є рівень інтероперабельності (I_s), який характеризує здатність освітньої ІС обмінюватися даними з іншими системами та державними реєстрами. Його можна визначити як частку реалізованих стандартних каналів обміну даними (API, інтеграція через Trembita, підтримка JSON/XML) від їх загальної кількості, необхідної для повноцінного функціонування системи:

$$I_s = \frac{N_{int}}{N_{req}}, \quad (2.1)$$

де N_{int} – кількість реалізованих інтеграційних інтерфейсів; N_{req} – необхідна кількість інтеграцій відповідно до функціонального призначення системи.

Другим важливим критерієм є якість даних (Q_d), яка визначає достовірність, актуальність і повноту інформації, що зберігається в системі. З урахуванням проблем дублювання та розбіжностей у звітності, цей показник доцільно обчислювати як частку перевірених і актуальних записів у загальному обсязі даних:

$$Q_d = \frac{D_{valid}}{D_{total}}, \quad (2.2)$$

де D_{valid} – кількість верифікованих та актуальних записів; D_{total} – загальна кількість записів у системі.

Третім критерієм є ступінь інтеграції (C_i), який відображає рівень взаємодії освітньої ІС з іншими інформаційними системами та підсистемами управління. Цей показник може бути оцінений як відношення кількості реально інтегрованих підсистем до загальної кількості систем, з якими необхідна взаємодія:

$$C_i = \frac{S_{int}}{S_{all}}, \quad (2.3)$$

де S_{int} – кількість інтегрованих підсистем; S_{all} – загальна кількість релевантних систем у освітньому середовищі.

Економічний аспект ефективності відображається через вартість технічного обслуговування (C_t), яка включає витрати на підтримку інфраструктури, оновлення програмного забезпечення та адміністрування. У поєднанні з цим показником враховуються ризики функціональної невідповідності (R_f), які пов'язані з технічними збоями, відсутністю інтеграції та потенційними втратами даних.

З урахуванням наведених критеріїв узагальнену ефективність освітньої інформаційної системи запропоновано оцінювати за інтегральною формулою:

$$E = \frac{I_s \times Q_d \times C_i}{C_t + R_f}, \quad (2.4)$$

де E – інтегральний показник ефективності освітньої ІС.

Максимізація значення E досягається шляхом підвищення рівня інтероперабельності, якості даних та інтеграції систем за одночасного зменшення витрат і ризиків.

Запропонована система критеріїв дозволяє не лише порівнювати різні освітні інформаційні системи, але й формувати ключові показники ефективності (KPI) для оцінювання цифрової трансформації освіти. Вона створює методичну основу для переходу до управління освітою на основі даних та підтримує розроблення цільової архітектури національної освітньої інформаційної системи.

Узагальнення критеріїв та показників оцінювання ефективності освітніх інформаційних систем наведено в табл. 2.2.

Таблиця 2.2

Критерії та показники оцінювання ефективності освітніх ІС

Критерій	Показник	Формула	Інтерпретація
Інтероперабельність	Рівень інтероперабельності (I_s)	$I_s = \frac{N_{int}}{N_{req}}$	Показує, наскільки система здатна обмінюватися даними з іншими ІС і державними реєстрами
Якість даних	Якість даних (Q_d)	$Q_d = \frac{D_{valid}}{D_{total}}$	Відображає достовірність, актуальність і повноту даних
Інтеграція	Ступінь інтеграції (Ci)	$C_i = \frac{S_{int}}{S_{all}}$	Характеризує рівень включеності системи в єдине освітнє цифрове середовище
Економічна ефективність	Вартість обслуговування (Ct)	експертна / фінансова оцінка	Витрати на підтримку, адміністрування та розвиток системи
Надійність	Ризик функціональної невідповідності (R_f)	експертна шкала (0–1)	Враховує ризики збоїв, втрати даних, відсутності оновлень
Інтегральна оцінка	Ефективність ІС (E)	$E = \frac{I_s \times Q_d \times C_i}{C_t + R_f}$	Дає змогу порівнювати різні ІС між собою

Складено авторами.

Наведемо умовний приклад розрахунку ефективності – порівняння ПАК «АІКОМ» та приватних освітніх ІС (Human / Eddy).

Доцільно підкреслити, що значення є умовними та використовуються для методичної ілюстрації застосування розроблених критеріїв.

Вхідні дані для оцінки освітніх інформаційних систем наведено в табл. 2.3.

Таблиця 2.3

Вхідні дані для оцінки освітніх інформаційних систем

Показник	АІКОМ	Приватна ІС
I_s (інтероперабельність)	0,85	0,30
Q_d (якість даних)	0,90	0,70
C_i (інтеграція)	0,80	0,40
C_t (вартість обслуговування)	0,40	0,20
R_f(ризики)	0,10	0,30

Складено авторами.

Розрахунок ефективності освітніх інформаційних систем буде виглядати наступним чином:

Для ПАК «АІКОМ»:

$$E_{AICOM} = \frac{0{,}85 \times 0{,}90 \times 0{,}80}{0{,}40 + 0{,}10} = \frac{0{,}612}{0{,}50} = 1{,}22. \quad (2.5)$$

Для приватної ІС:

$$E_{private} = \frac{0{,}30 \times 0{,}70 \times 0{,}40}{0{,}20 + 0{,}30} = \frac{0{,}084}{0{,}50} = 0{,}17. \quad (2.6)$$

Отримані результати свідчать, що інтегральний показник ефективності ПАК «АІКОМ» суттєво перевищує аналогічний показник приватних освітніх інформаційних систем. Це пояснюється вищим рівнем інтероперабельності, кращою якістю даних та глибшою інтеграцією з державними реєстрами. Приватні ІС, хоча й мають нижчу вартість обслуговування, поступаються за системною ефективністю через обмежену інтеграцію та підвищені ризики функціональної невідповідності.

2.4. Модернізація програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту»

На сьогодні, модернізація ПАК «АІКОМ» осмислюється як глибока трансформація інструментів інформаційного забезпечення управління освітою, що виходить за межі технічного оновлення програмного забезпечення. Йдеться

про перехід до нової якості управлінських процесів, у яких дані стають основою планування, моніторингу та оцінювання освітньої політики. У цьому контексті ПАК «АІКОМ» формується як системоутворюючий елемент державної освітньої інфраструктури, здатний забезпечити сталі, відтворювані та прозорі механізми управління. Фактично ми говоримо про модернізовану версію ПАК «АІКОМ» – АІКОМ 2.

Мета розробки та впровадження програмних модулів АІКОМ 2 зумовлена необхідністю створення сучасного інформаційного середовища освітнього менеджменту, що забезпечує централізований збір, обробку, зберігання та аналіз освітніх даних з метою підвищення ефективності управління, прозорості та якості освітніх послуг, а також інтеграцію із державними реєстрами та електронними платформами.

Цілі розробки та впровадження програмних модулів АІКОМ 2:

1. Забезпечити розробку та впровадження функціоналу для централізованого збору та аналізу освітніх даних, зокрема обліку учнів, педагогічних працівників, закладів освіти та їх філій.

2. Розширити функціонал АІКОМ 2 для автоматизації процесів формування, подання, моніторингу та аналізу звітності до органів управління освітою з можливістю подальшого масштабування.

3. Забезпечити інтеграцію АІКОМ 2 із державними реєстрами, включаючи ЄДР, ДРАЦС, ДРФО та платформою «Трембіта».

4. Підтримати електронний документообіг та стандарти відкритих даних у системі освіти.

5. Забезпечити захист персональних даних і відповідність інформаційно-комунікаційним стандартам.

6. Забезпечити підтримку децентралізованого управління освітою через доступ до достовірних даних на всіх рівнях управління, що сприятиме прийняттю ефективних управлінських рішень і підвищенню прозорості процесів.

Завдання розробки та впровадження програмних модулів АІКОМ 2:

1. Забезпечити розробку та впровадження функціоналу для централізованого збору та аналізу освітніх даних, зокрема обліку учнів, педагогічних працівників, закладів освіти та їх філій.

1.1. Розробити модуль управління користувачами, включаючи функції створення облікових записів, налаштування доступів та верифікації через ЕЦП.

1.2. Розробити модуль обліку учнів із функціями зарахування, переведення, відрахування та ведення профілів учнів.

1.3. Розробити модуль обліку закладів освіти для управління інформацією про заклади, філії, освітні параметри та навчальні роки.

1.4. Розробити модуль обліку педагогічних працівників із можливістю управління профілями працівників, кваліфікаціями та плануванням навантаження.

2. Розширити функціонал АІКОМ 2 для автоматизації процесів формування, подання, моніторингу та аналізу звітності до органів управління освітою з можливістю подальшого масштабування.

2.1. Реалізувати модуль звітності для автоматизованого формування, подання та аналізу даних за такими напрямами:

- контингент (облік учнів та працівників);

- мережа закладів освіти та їх структурних підрозділів;

- використання державних субвенцій;

- показники діяльності загальноосвітніх навчальних закладів.

3. Забезпечити інтеграцію АІКОМ 2 із державними реєстрами, включаючи ЄДР, ДРАЦС, ДРФО та платформою «Трембіта».

3.1. Інтегрувати систему з національними реєстрами, включаючи ЄДР, ДРАЦС, ДРФО, ЄДЕБО та платформу «Трембіта», з метою забезпечення актуальності даних і безперебійного обміну інформацією.

3.2. Реалізувати інтеграцію з онлайн-сервісом «Мрія», включаючи:

- використання REST API для пошуку, отримання та збереження даних учнів, вчителів, законних представників;

- забезпечення обміну даними через стандартизовані формати JSON/XML.

3.3. Інтегрувати АІКОМ 2 зі сторонніми освітніми інформаційними системами (ОІС) шляхом:

- розробки API для обміну даними про заклади освіти, співробітників, учнів;

- забезпечення доступу до статистичних звітів для аналізу даних.

4. Підтримати електронний документообіг та стандарти відкритих даних у системі освіти.

5. Забезпечити захист персональних даних і відповідність інформаційно-комунікаційним стандартам.

5.1. Реалізувати механізми захисту персональних даних відповідно до стандартів ДСТУ ISO/IEC включаючи шифрування, резервування даних та аудит доступу.

6. Забезпечити підтримку децентралізованого управління освітою через доступ до достовірних даних на всіх рівнях управління, що сприятиме прийняттю ефективних управлінських рішень і підвищенню прозорості процесів.

6.1. Забезпечити функціонал для експорту даних у стандартизованих форматах (Excel, CSV).

Концептуальним підґрунтям модернізації є визнання освітніх даних стратегічним нематеріальним активом держави. Дані розглядаються не як побічний результат адміністративної звітності, а як самостійний об’єкт управління, що потребує цілеспрямованого планування, стандартизації та аналітичної інтерпретації. Такий підхід відповідає сучасним теоріям evidence-based policy та дозволяє перейти від інтуїтивних управлінських рішень до науково обґрунтованих.

Об’єктом автоматизації в АІКОМ 2 є процеси управління освітою на всіх рівнях, включаючи дошкільну, загальну середню, позашкільну та професійно-технічну освіту. Система автоматизує облік учнів, педагогів, закладів освіти та їхніх філій, а також процеси формування, подання та аналізу звітності. Вона

забезпечує інтеграцію з державними реєстрами, такими як ДРАЦС, та іншими, створюючи єдиний інформаційний простір для освітньої сфери.

Суб'єктами автоматизації АІКОМ 2 є освітні заклади, їхні керівники, адміністратори та педагогічні працівники, здобувачі освіти й їхні законні представники, а також органи управління освітою всіх рівнів – від місцевих до центральних, включно з Міністерством освіти і науки України. До суб'єктів також належать адміністратори системи, такі як Державна наукова установа «Інститут освітньої аналітики», і державні реєстри, інтегровані з АІКОМ 2 (ДРАЦС тощо).

Конфігурація та топологія АІКОМ 2 полягає у тому, що модернізована система має бути побудована на базі локальної обчислювальної мережі центрального вузла та віддалених автоматизованих робочих місць користувачів управлінь та закладів освіти, які мають підключення до комунікаційної мережі загального користування Інтернет. Структура передбачає централізоване зберігання даних та доступ користувачів через захищене з'єднання з Інтернетом.

Характеристика апаратного та програмного забезпечення АІКОМ 2:

Центральний вузол АІКОМ 2 має бути розташований на базі Інформаційної системи «Програмна платформа для розгортання та супроводження державних електронних реєстрів» (далі – Платформа Реєстрів) державного підприємства «Українські спеціальні системи» (далі – ДП «УСС»).

Платформа Реєстрів забезпечує ядро архітектури АІКОМ 2, зокрема її функціональні та інфраструктурні компоненти.

Основними особливостями Платформи, які використовуються для реалізації АІКОМ 2, є:

● Централізоване управління даними: центральна база даних (ЦБД) АІКОМ 2 базується на Платформі Реєстрів, яка забезпечує зберігання, обробку та доступ до даних про заклади освіти, учнів, педагогічних працівників тощо.

● Бізнес-логіка та процеси: усі ключові функції АІКОМ 2, включаючи облік, звітність та управління користувачами, реалізовані за допомогою мікро сервісів, що надаються платформою.

● Безпека: платформа побудована відповідно до принципів Zero-Trust, що забезпечує шифрування даних, автентифікацію та авторизацію на всіх рівнях.

Технологічні особливості Платформи Реєстрів:

● Модульність: платформа розроблена як сукупність мікро сервісів, що дозволяє легко додавати новий функціонал або змінювати існуючий.

● Контейнерна оркестрація: використання Kubernetes та OpenShift забезпечує автоматичне масштабування, розгортання та управління ресурсами.

● Інтеграційні можливості: платформа підтримує інтеграцію з іншими державними реєстрами через стандартні API (REST, SOAP) або захищену транспортну шину «Трембіта».

● Автоматизація: впровадження GitOps підходу для централізованого управління оновленнями та розгортання системи.

До складу центрального вузлу АІКОМ 2 має входити сервер додатків та баз даних. Для забезпечення мережевого зв'язку серверу має використовуватися відповідне комутаційне обладнання (в тому числі, міжмережевий екран) зі складу центру обробки даних ДП «УСС» (далі – ЦОД).

Сервер додатків та баз даних має бути призначений для надання користувачам АІКОМ 2 графічного інтерфейсу для виконання покладених на них функціональних обов'язків, для забезпечення виконання функціональних завдань з обробки інформації, що покладені на АІКОМ 2, для розміщення та управління базами даних інформаційних об'єктів, що зберігаються та обробляються в АІКОМ 2, для забезпечення функціонування прикладного програмного забезпечення АІКОМ 2, а також для надання доступу до загальнодоступної інформації про заклади освіти та статистичних відомостей щодо їх діяльності.

Веб-сервер, сервер баз даних, сервер аналітики, портал відкритих даних мають бути розгорнуті на сервері додатків та баз даних в якості окремих компонентів прикладного програмного забезпечення.

Робочі місця системних адміністраторів мають бути призначені для:

● централізованого управління налаштуваннями програмного та апаратного забезпечення серверів АІКОМ 2 та комутаційного обладнання;

● управління обліковими записами обслуговуючого персоналу на технічних засобах АІКОМ 2, а також для перегляду протоколів подій в АІКОМ 2.

Робочі місця технічних адміністраторів мають бути призначені для:

● управління налаштуваннями прикладного програмного забезпечення, обліковими записами адміністраторів та респондентів управлінь освітою обласного, районного, територіального (ОТГ), місцевого та міського (населений пункт) рівнів, користувачів МОН та рівня загальноосвітніх закладів середньої освіти та їх правами доступу до інформаційних об’єктів;

● формування інформаційних звітних даних з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця адміністраторів управлінь освітою обласного рівня мають бути призначені для:

● управління обліковими записами респондентів власного управління освітою, адміністраторів управлінь освітою районного та територіального рівнів (ОТГ), а також рівня загальноосвітніх закладів середньої освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до інформаційних об’єктів;

● подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та звітів, поданих адміністраторами управлінь освітою районного рівня (відповідно до адміністративної підпорядкованості) з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця респондентів управлінь освітою обласного рівня мають бути призначені для формування статистичної звітної інформації на обласному рівні для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до ДНУ «ІОА».

Автоматизовані робочі місця адміністраторів управлінь освітою районного рівня мають бути призначені для:

● управління обліковими записами респондентів власного управління освітою, управління освітою рівня територіальної громади, адміністраторів закладів освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до інформаційних об’єктів;

● подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та даних, поданих адміністраторами закладів освіти (відповідно до адміністративної підпорядкованості) з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця респондентів управлінь освітою районного рівня мають бути призначені для формування статистичної звітної інформації на районному рівні для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до управління освітою обласного рівня (відповідно до адміністративної підпорядкованості).

Автоматизовані робочі місця адміністраторів управлінь освітою рівня територіальної громади (ОТГ) мають бути призначені для:

● управління обліковими записами респондентів власного управління освітою,, місцевого управління освітою, адміністраторів закладів освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до інформаційних об’єктів;

● подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та даних, поданих адміністраторами закладів освіти (відповідно до адміністративної підпорядкованості) та органами управління освітою місцевого рівня з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця респондентів управлінь освітою рівня територіальної громади мають бути призначені для формування звітної

інформації на рівні територіальної громади для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до управління освітою районного рівня (відповідно до адміністративної підпорядкованості).

Автоматизовані робочі місця адміністраторів управлінь освітою місцевого рівня мають бути призначені для:

● управління обліковими записами респондентів власного управління освітою, управління освітою рівня міста, адміністраторів закладів освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до інформаційних об’єктів;

● подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та даних, поданих адміністраторами закладів освіти (відповідно до адміністративної підпорядкованості) та органами управління освітою рівня міста з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця респондентів управлінь освітою місцевого рівня мають бути призначені для формування звітної інформації на місцевому рівні для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до управління освітою рівня територіальної громади (відповідно до адміністративної підпорядкованості).

Автоматизовані робочі місця адміністраторів управлінь освітою міського рівня мають бути призначені для:

● управління обліковими записами респондентів власного управління освітою та адміністраторів закладів освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до інформаційних об’єктів;

● подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та даних, поданих адміністраторами закладів освіти (відповідно до адміністративної підпорядкованості) з використанням прикладного програмного забезпечення відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця респондентів управлінь освітою міського рівня мають бути призначені для формування звітної інформації на рівні міста для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до управління освітою місцевого рівня (відповідно до адміністративної підпорядкованості).

Автоматизовані робочі місця респондентів закладів освіти мають бути призначені для формування статистичної звітної інформації на рівні закладу освіти для подальшої подачі відповідних інформаційних звітів адміністратором свого закладу освіти до управління освіти міського / місцевого / територіального / районного / обласного рівня (відповідно до підпорядкованості).

Всі наведені автоматизовані робочі місця адміністраторів та респондентів мають являти собою окремі електронні обчислювальні машини, що мають підключення до мережі Інтернет.

На центральному вузлі АІКОМ 2 має використовуватися наступне програмне забезпечення:

- операційна система серверу – Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-145-generic x86_64);
- операційні системи робочих місць адміністраторів ДНУ «ІОА» – сімейства Microsoft Windows;
- операційні системи робочих місць адміністраторів та респондентів управлінь освітою та закладів освіти – сімейства Microsoft Windows;
- прикладне програмне забезпечення;
- прикладне програмне забезпечення веб-серверу nginx 1.10.3;
- система управління базами даних PostgreSQL 6.18.

Центральний вузол АІКОМ 2 має розгортатися з використанням технічних засобів ЦОД ДП «УСС» на підставі договору №11.945/24 від 01.05.2024 між ДП «УСС», ДНУ «ІОА» та ГО «Офіс ефективного реагування», у якому зафіксоване наступне:

- ДП «УСС» надає послуги з розміщення серверного обладнання ДНУ «ІОА» в придатному для монтажу корпусі в комунікаційну шафу,

підключення його до мережі безперебійного живлення і забезпечення напругою 220 В змінного струму;

● ДП «УСС» забезпечує захищене підключення серверного обладнання ДНУ «ІОА» до мережі Інтернет та захист від мережевих атак з боку зазначеної мережі відповідно до вимог законодавства України та нормативно технічної документації в галузі технічного захисту інформації з використання захищеного вузлу інтернет-доступу (атестат відповідності комплексної системи захисту інформації вимогам нормативних документів системи технічного захисту інформації № 21662 від 09.06.2020);

● ДП «УСС» забезпечує технічне обслуговування встановленого серверного обладнання ДНУ «ІОА» в обсязі включення і виключення електроживлення, а також запуску його на перевантаження.

Формування єдиного ядра освітніх даних є ключовим напрямом модернізації, оскільки саме фрагментація та дублювання інформації є однією з головних проблем управління освітою. Централізоване ядро забезпечує уніфіковані правила опису даних, їх валідації та актуалізації. У науковому сенсі це створює умови для підвищення валідності статистичних і аналітичних висновків.

Відзначимо, що функціональна модернізація АІКОМ орієнтується на відображення освітньої системи як динамічного соціального процесу. Замість фіксації окремих показників у певний момент часу система поступово набуває здатності відстежувати зміни, переходи та взаємозв’язки. Це відкриває можливості для використання методів порівняльного, трендового та факторного аналізу в управлінні освітою.

Архітектурна модернізація ПАК «АІКОМ» спрямована на подолання обмежень ієрархічних, жорстко зв’язаних систем, які не здатні адаптуватися до динамічних змін у сфері освіти. Модульний підхід дозволяє розглядати систему як сукупність взаємопов’язаних, але автономних компонентів, кожен з яких може розвиватися без порушення цілісності всієї платформи. Це створює передумови для довгострокової еволюції системи.

Опишемо технічну архітектуру АІКОМ 2.

Технічна архітектура АІКОМ 2:

Архітектура АІКОМ 2 має бути відкритою, модульною та інтегрованою, що дозволяє забезпечувати масштабованість, легкість інтеграції з іншими державними системами та високу продуктивність. Система має бути побудована щонайменше з таких основних компонентів, які наведені в принциповій схемі технічної архітектури (рис. 2.1).

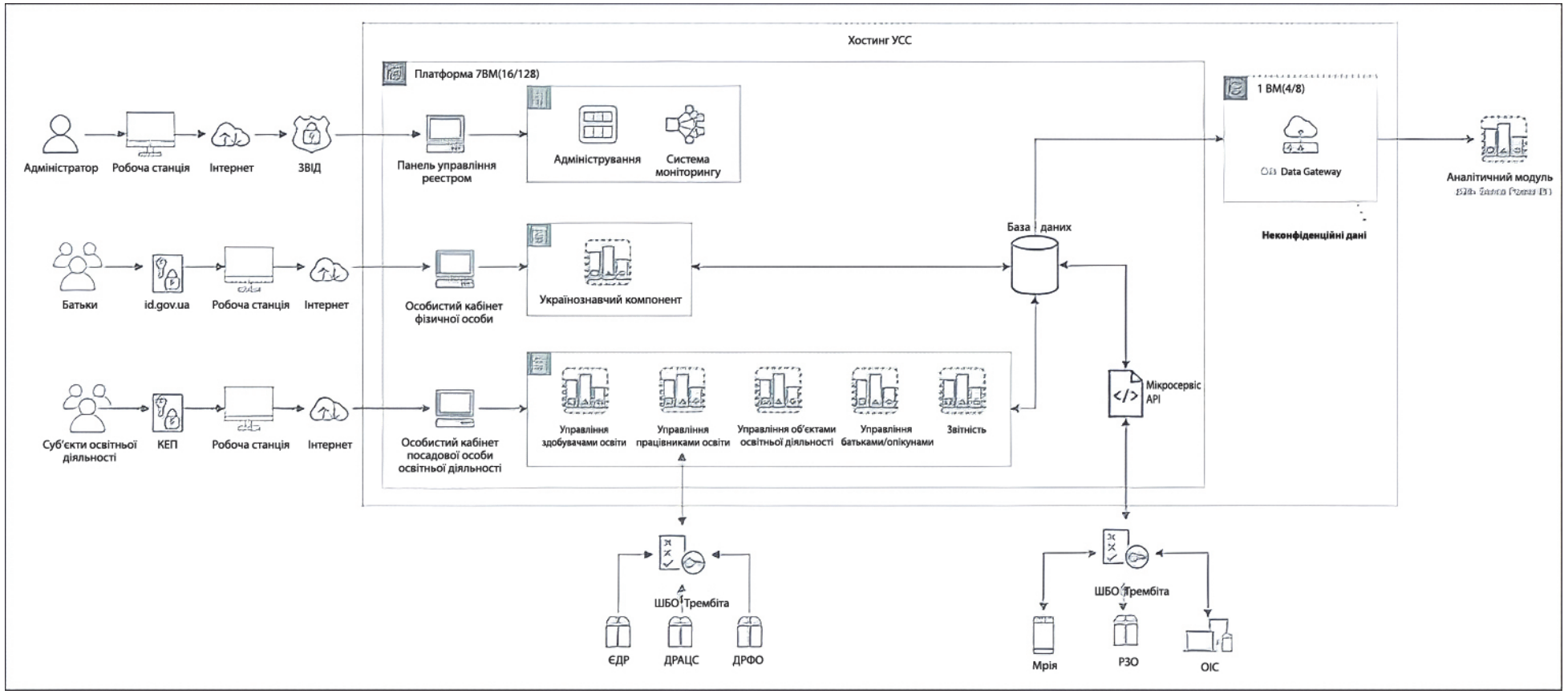


Рис. 2.1. **Архітектура АІКОМ 2**

Побудовано авторами.

Центральна база даних (ЦБД): ЦБД має бути основним сховищем даних про заклади освіти, учнів, педагогічних працівників та інші ключові дані. База має бути побудована за принципами реляційної моделі з підтримкою масштабованості та високої доступності. Для роботи з ЦБД передбачено механізми кешування запитів, що оптимізують продуктивність системи.

Далі опишемо функціональні модулі. Так, функціональність АІКОМ 2 має реалізовуватися через набір логічних модулів, кожен із яких виконує окремі завдання та розміщено в кабінеті користувача на Платформі:

● Модуль адміністрування: відповідає за створення, редагування та управління обліковими записами користувачів різних рівнів, а також за контроль доступу до функціоналу системи.

● Модуль обліку закладів загальної середньої освіти: має забезпечувати реєстрацію, оновлення даних і управління інформацією про заклади освіти та їх філії, зокрема параметрами закладів, дані про матеріально-технічний стан закладів, інформацію про навчальні роки і класи.

● Модуль обліку працівників закладів загальної середньої освіти: відповідає за облік персоналу, включаючи створення, оновлення профілів працівників, планування навантаження.

● Модуль обліку учнів та дітей шкільного віку: автоматизує процеси обліку дітей шкільного віку, а також зарахування, переведення, відрахування та ведення освітніх профілів учнів, включаючи облік їхніх медичних документів та пільг.

● Модуль звітності: має забезпечувати формування агрегованих статистичних звітів для закладів освіти, органів управління освітою та інших зацікавлених сторін.

● Модуль Українознавчого компоненту: має забезпечувати автоматизацію процесів подання заяви та обробку заяв для зарахування на програму.

Автоматизовані робочі місця користувачів (електронні кабінети користувачів).

Особисті електронні кабінети мають забезпечувати доступ користувачів до функціоналу системи. Кабінети мають бути адаптовані відповідно до ролей користувачів. Доступ користувачів має забезпечуватися через сервіс авторизації з використанням інструментів ЕЦП.

Сервіси інтеграції:

АІКОМ 2 має забезпечувати інтеграції АІКОМ 2 з іншими державними інформаційними системами та сервісами через стандартизовані протоколи взаємодії (REST, SOAP). Він відповідає за налаштування інформаційного обміну даними між системами, забезпечення їх сумісності та захисту інформації під час передачі.

Додаткові сервіси: Система забезпечує інтеграцію з платформами освітніх інформаційних систем (ОІС) для обміну даними. Через інтеграцію з державною цифровою екосистемою «Мрія» здійснюється обмін даними між системами для надання освітніх послуг.

Функціональна схема АІКОМ 2 визначає логічну структуру системи, взаємозв'язки між її компонентами та основні функціональні можливості. Далі опишемо вимоги до організації функціональних модулів, таких як модуль управління користувачами, модуль обліку закладів освіти, модуль педагогічних працівників, модуль обліку учнів, модуль звітності та сервісів API інтеграцій. Описи охоплюють функціональність кожного модуля, включаючи їхню здатність виконувати конкретні завдання, інтегруватися з іншими модулями системи та зовнішніми інформаційними ресурсами. Окрема увага приділяється забезпеченню гнучкості та масштабованості модулів, що дозволяє адаптувати їх до змін у нормативно-правовій базі або потреб користувачів.

Модуль управління користувачами.

Модуль управління користувачами є ключовим компонентом системи, що має забезпечувати створення, оновлення та підтримку даних облікових записів користувачів на різних рівнях управління освітою. Модуль має бути спрямований на реалізацію функціоналу для створення нових облікових записів, редагування наявних даних, онбордингу користувачів, а також вибору і

керування записами про освітні інформаційні системи та органи управління освітою.

Модуль має забезпечувати виконання наступних ключових функцій:

● Створення та оновлення облікових записів – реєстрація нових користувачів, редагування персональних даних, налаштування ролей і доступів у системі.

● Управління правами доступу користувачів – налаштування рівнів доступу відповідно до ролей і контроль за їх використанням.

● Реалізація процесу онбордингу для нових користувачів – забезпечення первинної реєстрації, автентифікації та налаштування облікових записів.

Модуль має забезпечувати автоматичну валідацію введених даних, інтеграцію з іншими компонентами системи для забезпечення синхронізації інформації, логування дій користувачів і генерацію інформаційних повідомлень.

Схему компонентів модуля наведено на рис. 2.2.

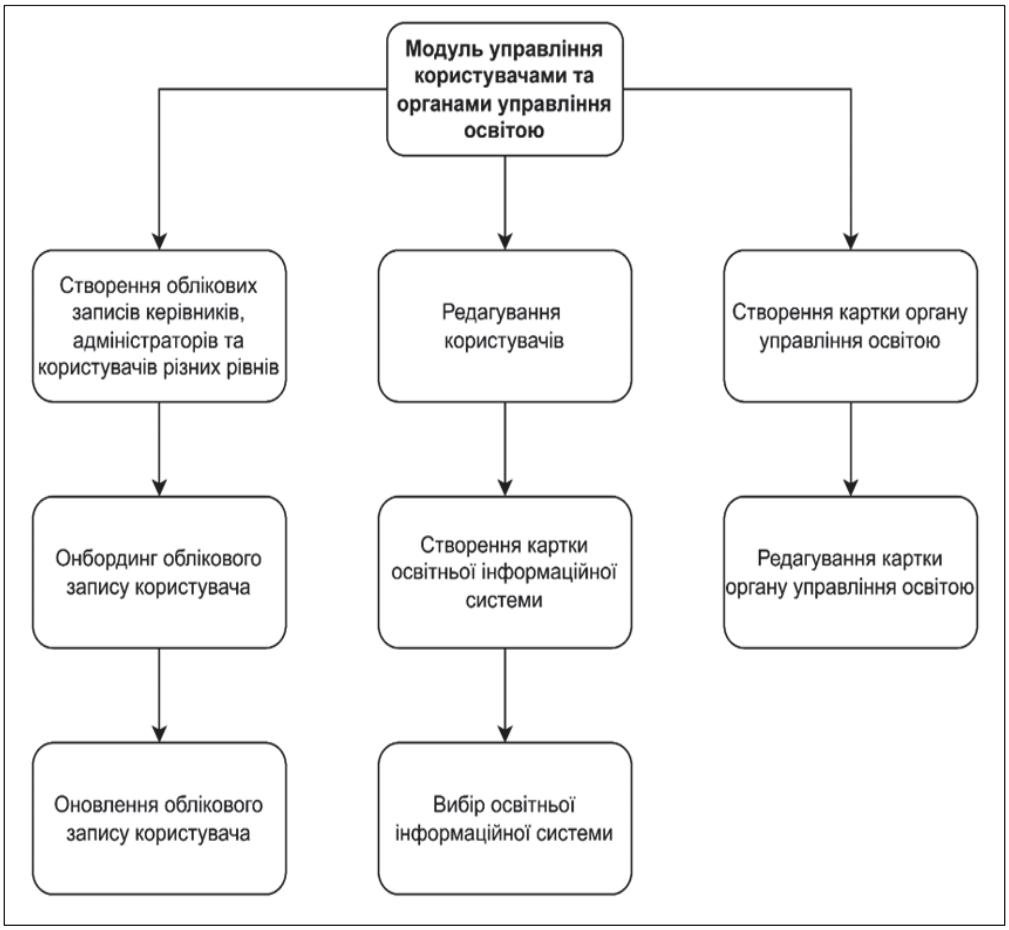


Рис. 2.2. **Схема компонентів модуля управління користувачами**
Побудовано авторами.

Рольова модель доступу розглядається як інструмент не лише інформаційної безпеки, а й управлінської відповідальності. Чітке розмежування повноважень дозволяє формувати персоніфіковану відповідальність за якість даних, а також забезпечує прозорість дій користувачів. У науковому контексті це відповідає принципам good governance та інституційної підзвітності.

Модуль закладів загальної середньої освіти.

Модуль закладів загальної середньої освіти (ЗЗСО) має бути інтегрованою частиною автоматизованої інформаційної системи, призначеної для управління освітнім процесом у закладах загальної середньої освіти та їхніх філіях. Модуль має забезпечувати виконання наступних ключових функцій:

● Реєстрація та оновлення даних про заклади освіти – внесення інформації про заклади, їхні параметри та філії з можливістю редагування.

● Структуризація даних про заклади, філії, класи та паралелі – упорядкування інформації про освітню мережу для зручного управління.

● Управління навчальними роками, гуртками та групами продовженого дня – створення, налаштування та ведення параметрів освітнього процесу.

Облік закладів освіти в АІКОМ 2 перетворюється на інструмент аналізу освітньої інфраструктури як складної територіально організованої системи. Це дозволяє оцінювати щільність мережі, доступність освіти, ефективність використання ресурсів та обґрунтовувати управлінські рішення щодо оптимізації мережі закладів.

Схему компонентів модуля наведено на рис. 2.3.

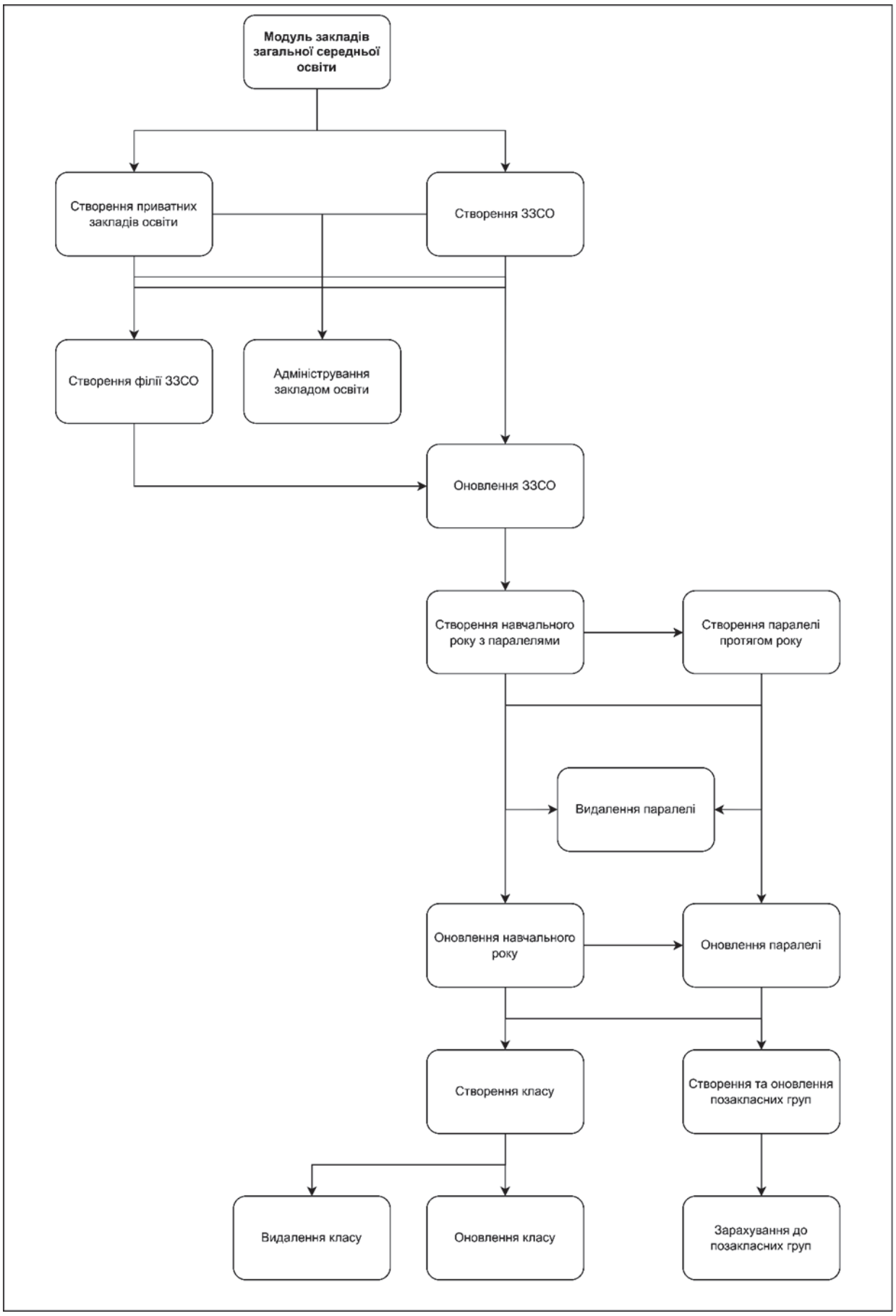


Рис. 2.3. **Схема компонентів модуля ЗЗСО**

Побудовано авторами.

Модуль педагогічних працівників закладів загальної середньої освіти.

Модуль педагогічних працівників закладів загальної середньої освіти має бути інтегрованою частиною автоматизованої інформаційної системи, призначеної для управління інформацією про працівників закладів освіти, включаючи їхній облік, навантаження та історію працевлаштування. Основна мета модуля – забезпечення автоматизації процесів створення, оновлення, збереження та аналізу даних про персонал, а також підтримки ключових бізнес-процесів, пов’язаних із їхньою діяльністю.

Модуль педагогічних працівників має забезпечувати виконання наступних ключових функцій:

1. Управління картками працівників – створення, оновлення та збереження інформації про працівників, включаючи персональні дані, контактну інформацію, кваліфікації та документи.

2. Навантаження педагогічних працівників – облік навчального навантаження педагогів, у тому числі за класами, предметами, гуртками та ставками.

3. Облік звільнення працівників – внесення та обробка даних про звільнення співробітників із відповідним обліком у системі.

Модуль має забезпечувати автоматичну валідацію введених даних, інтеграцію з іншими компонентами системи для забезпечення синхронізації інформації, логування дій користувачів і генерацію інформаційних повідомлень.

Схему компонентів модуля наведено на рис. 2.4.

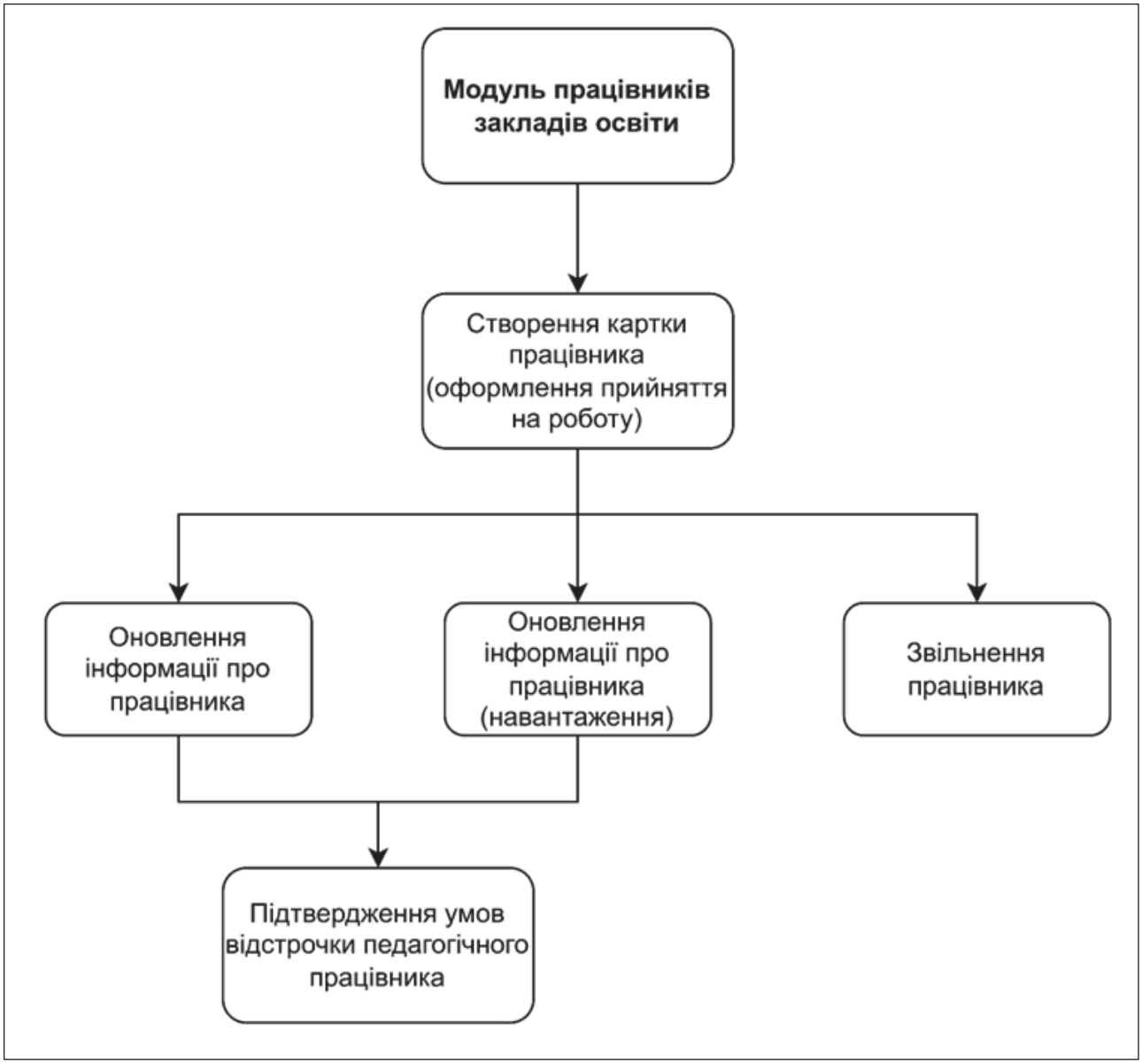


Рис. 2.4. **Схема компонентів модуля педагогічних працівників закладів загальної середньої освіти**

Побудовано авторами.

Кадровий компонент АІКОМ 2 розвивається у напрямі аналітичного дослідження людського потенціалу освіти. Дані про педагогічних працівників стають основою для оцінювання кадрових ризиків, прогнозування дефіцитів та розроблення політик професійного розвитку. Це відповідає сучасним підходам до управління людським капіталом у публічному секторі.

Модуль обліку учнів.

Модуль обліку учнів має бути інтегрованою частиною автоматизованої інформаційної системи, призначеної для управління інформацією про учнів

закладів освіти. Його функціональність має забезпечувати створення, оновлення та зберігання даних про освітні профілі учнів, медичні документи, інформацію про пільги, а також організацію процесів зарахування та переведення. Функціонал модуля має охоплювати:

● Створення та оновлення освітніх профілів – введення базової інформації про учнів і підтримка її актуальності.

● Медична документація – створення та оновлення медичних записів із дотриманням правил доступу.

● Пільги учнів – реєстрація документів, що підтверджують право на пільги.

● Організація зарахування – підтримка процесу прийому учнів, включаючи випадки відсутності попередніх записів у системі.

● Переведення учнів між закладами, класами або паралелями відповідно до нормативів.

● Управління даними законних представників – оновлення даних про осіб, що представляють інтереси учня.

Схему компонентів модуля наведено на рис. 2.5.

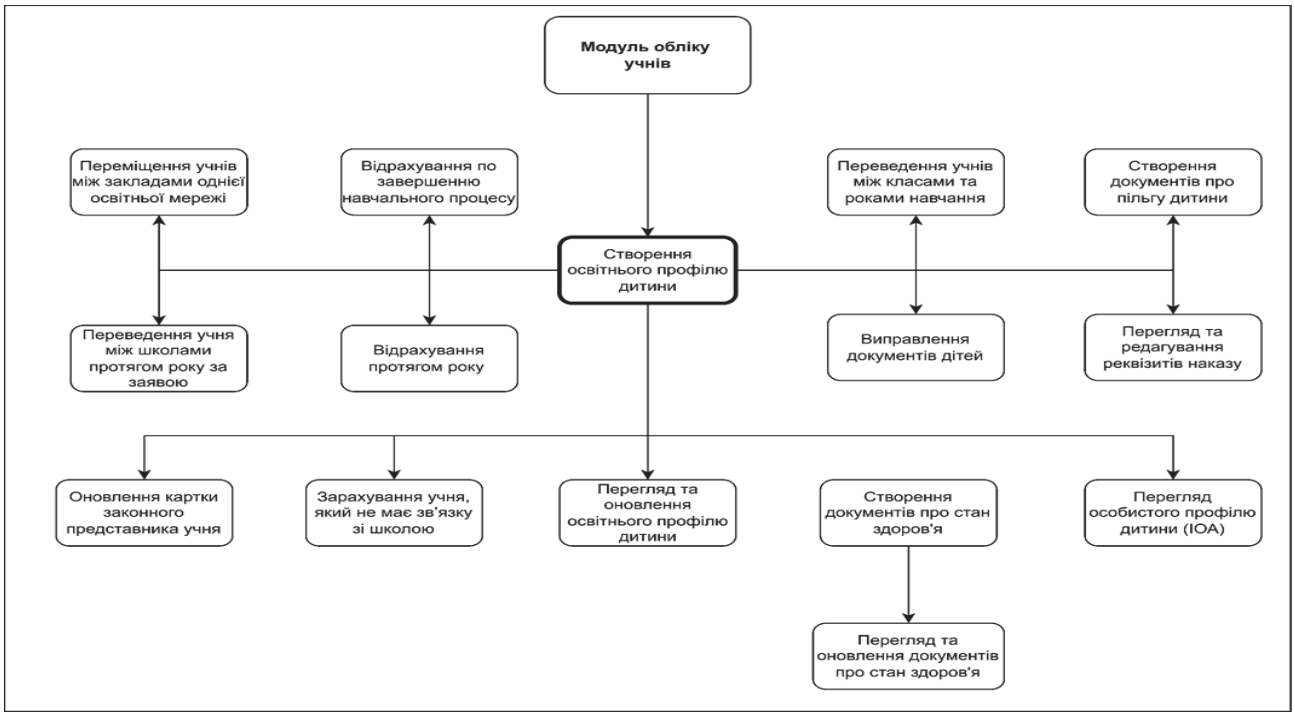


Рис. 2.5. **Схема компонентів модуля обліку учнів**

Побудовано авторами.

Облік учнів у межах модернізації набуває ознак інструменту соціально-демографічного аналізу. Відстеження освітніх траєкторій дозволяє досліджувати вплив соціальних, територіальних і економічних факторів на доступ до освіти. Таким чином, АІКОМ стає джерелом емпіричних даних для освітньої соціології та демографії.

Модуль звітності.

Модуль звітності є компонентом системи, призначеним для формування, обробки та надання звітів для закладів освіти, органів управління освітою та інших зацікавлених сторін. Основна мета модуля – забезпечити швидкий, зручний та автоматизований процес отримання звітності, необхідної для аналізу та прийняття управлінських рішень.

Функціонал модуля має включати:

● Автоматичне формування звітів – генерація стандартних форм звітів, таких як «Контингент», «Мережа», «Звіт по субвенціях», «Класи та учні».

● Інтеграція з іншими модулями – автоматичне збирання даних із модулів обліку учнів, педагогічних працівників, закладів освіти.

● Експорт звітів – підтримка різних форматів (Excel, PDF, CSV) для подальшого аналізу.

● Доступ до історичних даних – можливість перегляду та аналізу звітів за попередні періоди.

● Логування дій – відстеження змін у звітах для забезпечення прозорості.

Модуль звітності має підтримувати стандартизовані шаблони, визначені законодавством, та забезпечувати гнучкість у налаштуваннях (рис. 2.6).

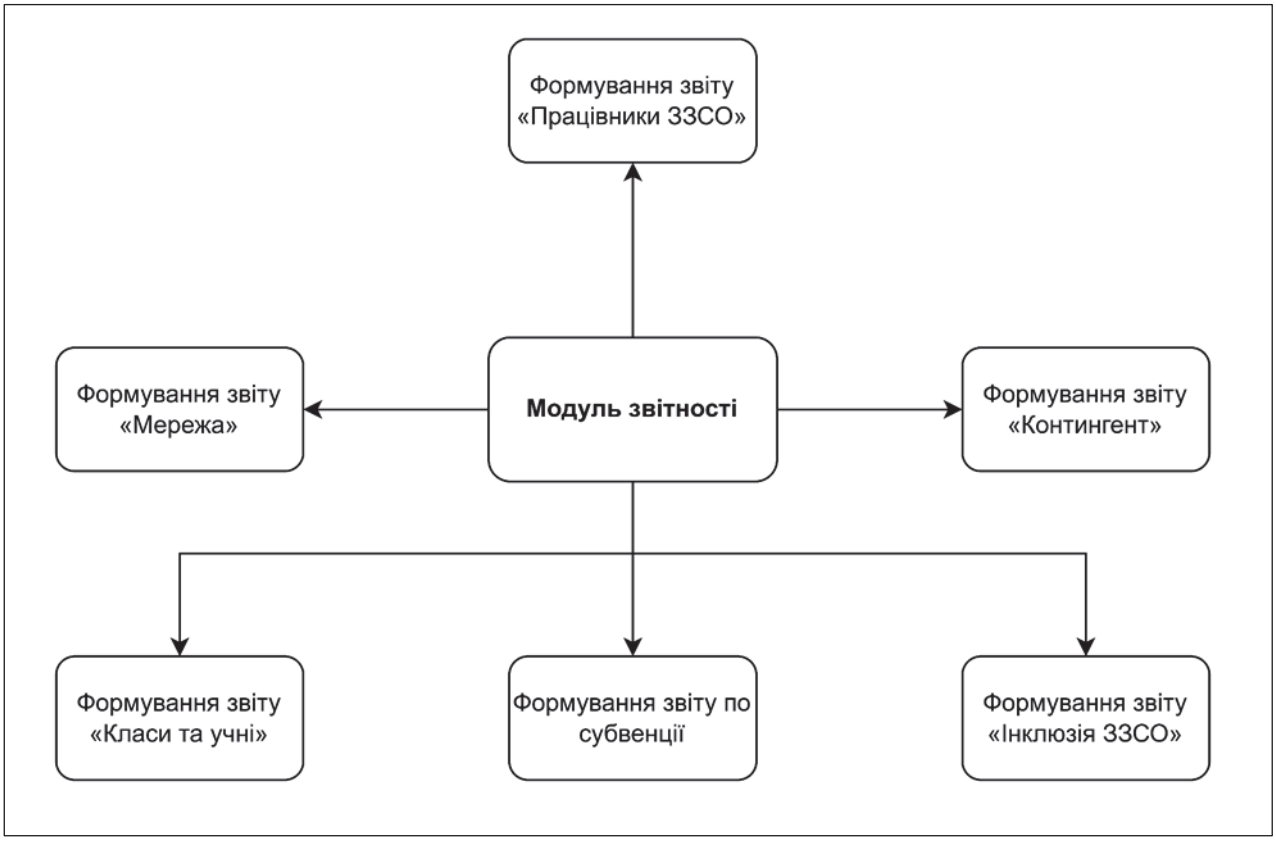


Рис. 2.6. **Схема компонентів модуля звітності**
Побудовано авторами.

Відзначимо, що аналітична складова АІКОМ 2 розвивається від регламентованої статистики до гнучкої системи підтримки управлінських рішень. Це означає перехід від підготовки звітів «заради звітів» до формування аналітичних продуктів, орієнтованих на конкретні управлінські запити. У науковому сенсі це створює передумови для використання багатовимірного аналізу.

У свою чергу, інтеграційна спроможність системи розглядається як умова формування цілісного інформаційного простору держави. Освітні дані в такій моделі перестають бути ізольованими та можуть використовуватися у міжсекторальних дослідженнях. Це суттєво підвищує аналітичну цінність інформації. Зокрема, сервіс API-інтеграцій має забезпечувати функціональність інтеграції АІКОМ 2 з іншими державними інформаційними системами та платформами через стандартизовані інтерфейси.

Основні функції сервісу:

- Обмін даними: підтримка інтеграції з державними реєстрами (ЄДР, ДРАЦС, ДРФО) через REST/SOAP API.
- Захист інформації: забезпечення безпеки передачі даних через TLS/SSL-протоколи та механізми аутентифікації (OAuth 2.0, JWT).
- Підтримка форматів даних: робота з JSON та XML для забезпечення сумісності з іншими системами.
- Інтеграція з платформою «Трембіта»: забезпечення автоматизованого обміну інформацією через захищену транспортну шину.
- Моніторинг та аудит: логування всіх інтеграційних запитів для подальшого аналізу та виявлення помилок.
- Сумісність із освітніми інформаційними системами (OIC): надання API для обміну даними між закладами освіти та іншими платформами.

Сервіс має бути гнучким у налаштуваннях для забезпечення адаптації до нових вимог законодавства чи змін у зовнішніх інформаційних системах.

Слід відзначити, що технологічна модернізація ґрунтується на принципах масштабованості, відмовостійкості та гнучкості, що дозволяє забезпечити безперервність функціонування системи. У науковому контексті це відповідає системному підходу до управління складними соціально-технічними системами. Стандартизація даних є необхідною умовою їх наукової інтерпретації та порівнюваності. Єдині підходи до класифікацій і показників забезпечують можливість довгострокових досліджень та міжнародних порівнянь, що є критично важливим у контексті європейської інтеграції освіти.

Користувацький інтерфейс розглядається як елемент організаційної ефективності. Його спрощення та логічна структурованість сприяють зниженню транзакційних витрат у системі управління освітою та підвищують якість первинних даних.

Орієнтація на життєвий цикл даних дозволяє впровадити науково обґрунтований підхід до управління інформацією. Кожен етап – від створення до використання в аналітиці – розглядається як об’єкт управління, що підвищує загальну ефективність системи.

Загалом модернізація ПАК «АІКОМ» сприяє формуванню культури роботи з даними в освітній сфері. Це означає зміну управлінських практик і підвищення аналітичної компетентності учасників освітнього управління. Міжсекторальний потенціал АІКОМ 2 дозволяє використовувати освітні дані в комплексних соціально-економічних дослідженнях. Це підвищує роль системи як національного аналітичного ресурсу. Розширення охоплення системи на інші рівні освіти формує основу для аналізу освітнього шляху людини впродовж життя. Такий підхід відповідає концепції навчання впродовж життя та розвитку людського капіталу. У підсумку модернізація ПАК «АІКОМ» постає як інституційна та науково обґрунтована трансформація управління освітою, що забезпечує перехід від адміністративної моделі до аналітичної, орієнтованої на розвиток, стійкість і стратегічне планування державної освітньої політики.

3. РОЗВИТОК ОСВІТНІХ ПЛАТФОРМ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Функціонування інформаційної платформи «Освіта для ветеранів»

За останнє десятиліття Україна зіткнулася з численними викликами, зокрема з військовою агресією з боку Російської Федерації, пандемією COVID-19, а з 2022 року – з повномасштабним вторгненням. Ці події зумовили трансформацію ринку праці, поглибили наявні дисбаланси та актуалізували потребу в системній підтримці окремих груп населення, зокрема ветеранів війни.

Після початку АТО у 2014 році країна втратила частину територій разом із промисловими об’єктами, а значна частина громадян залишилася без роботи через зупинку підприємств. Крім того, відбулася втрата кваліфікованих кадрів унаслідок мобілізації, що ускладнило функціонування національного ринку праці.

У 2016 році спостерігалося певне поліпшення ситуації: зросла кількість вакансій, активізувалася діяльність роботодавців. Проте на перший план вийшла проблема професійної адаптації демобілізованих військовослужбовців – багато з них не мали змоги повернутися до попередньої діяльності через стан здоров’я або зміну професійних вимог.

Міністерство соціальної політики ще з середини 2010-х років реалізовувало державні програми професійної адаптації ветеранів. За підтримки Міжнародного фонду соціальної адаптації, НАТО, а також за участі Державної служби зайнятості в Україні почали функціонувати центри перекваліфікації. Проте цим ініціативам бракувало єдиного системного підходу – зусилля залишалися фрагментарними та часто неузгодженими між собою [44].

Після стабілізації ситуації на сході України у 2016 р. чисельність військовослужбовців почала поступово зменшуватися. Водночас зростали вимоги роботодавців до кваліфікації кандидатів, а також до їхніх соціальних

навичок. Багато ветеранів зіштовхнулися з неможливістю повернення до попереднього місця роботи.

Початок повномасштабної війни у 2022 р. спричинив масштабні зміни в економіці України та на ринку праці. Захоплення ворогом великої території країни, руйнування підприємств, вимушене переміщення населення та загальна економічна нестабільність призвели до різкого зростання рівня безробіття. Внутрішня міграція також поглибила дисбаланс між попитом і пропозицією робочої сили, зокрема через невідповідність наявної кваліфікації внутрішньо переміщених осіб (ВПО) потребам ринку праці через спрямованість на розвиток різних напрямків економічної діяльності у східних та західних регіонах.

Проблема працевлаштування ветеранів набула ще більшої актуальності. Оскільки значна частина військовослужбовців після демобілізації мають обмеження за станом здоров’я та недостатній рівень цивільних навичок, питання їхньої професійної реінтеграції стало стратегічно важливим. Виникла потреба в інституційно підтриманих, технологічно сучасних та інклюзивних рішеннях у сфері освіти й зайнятості.

За даними Державної служби зайнятості, з початку повномасштабного вторгнення і до 30 березня 2023 року послугами служби скористалися 8 911 ветеранів, з яких 2 362 були працевлаштовані, а 118 пройшли професійне навчання [45].

Соціологічні дослідження також свідчать, що проблеми адаптації ветеранів мають як зовнішній (упередженість роботодавців), так і внутрішній (невпевненість самих ветеранів) характер. Згідно з опитуванням, проведеним у межах Програми реінтеграції ветеранів IREX, 32 % респондентів стикалися з дискримінацією з боку роботодавців через свій статус. Крім того, ветерани самостійно вказували на такі бар’єри, як: відсутність розуміння, як адаптувати військовий досвід до умов цивільного ринку праці; невпевненість у власній кваліфікації; труднощі з налагодженням соціальних контактів після повернення до цивільного життя.

У межах іншого дослідження, проведеного в червні-липні 2023 року [45], роботодавці підтверджували, що багато демобілізованих мають проблеми зі здоров'ям, що унеможливлює повернення до попередніх посад. Водночас результати засвідчують готовність бізнесу: розглядати ветеранів на нові посади – зокрема в галузях будівництва, інженерії, автомобільного сервісу; брати участь у перекваліфікації працівників, які втратили здатність виконувати попередні обов'язки; активно формувати запити до центрів зайнятості, попри критику якості їхньої роботи та невідповідність освітніх послуг реальним потребам ринку.

Дослідження також зафіксувало такі дані: лише 41,6 % ветеранів зверталися до Державної служби зайнятості; 65,8 % опитаних заявили про потребу в професійній адаптації; 53,3 % висловили бажання змінити кваліфікацію, а 48,2 % – здобути додаткову освіту.

Це свідчить про високу потребу в заходах, спрямованих на професійне навчання, перепідготовку та трудову інтеграцію ветеранів, в умовах економічних трансформацій, спричинених війною.

Зважаючи на постійне зростання кількості громадян, які проходять військову службу, нагальним завданням у довгостроковій перспективі є розроблення комплексних механізмів підтримки трудової інтеграції ветеранів для забезпечення сталого повоєнного відновлення країни.

Окремим напрямом стала цифровізація процесів обліку та обслуговування ветеранів, що відповідає загальнодержавному курсу на діджиталізацію. У 2019 р. Міністерство у справах ветеранів України ініціювало створення Єдиного державного реєстру ветеранів війни, який набув повної функціональності в лютому 2023 р. відповідно до наказу Мінветеранів від 09.02.2023 № 26 [46]. Інформаційно-комунікаційна система реєстру не лише забезпечує накопичення даних про ветеранів, але й дає змогу оформлювати пільги та координувати взаємодію між центральними та місцевими органами влади.

Наступним етапом цифрової трансформації стало впровадження системи «Є-Ветеран» – електронного кабінету, який консолідує інформацію про

соціальні гарантії, забезпечує можливості взаємодії з органами влади та доступ до пільг і послуг в електронному форматі.

Євроінтеграційний курс України, який активізувався після 2022 р., відкрив нові можливості для залучення міжнародної допомоги у сфері соціальної підтримки населення, зокрема ветеранів. В межах програм, що фінансуються Європейським Союзом (ЄС) та країнами-партнерами, формується нова модель взаємодії держави, роботодавців і громадян з метою створення сприятливих умов для післявоєнного відновлення України.

В Україні реалізується низка проєктів за підтримки ЄС та країн-партнерів, спрямованих на побудову цілісної системи професійної реінтеграції ветеранів.

У цьому контексті варто відзначити низку ініціатив, реалізованих після початку повномасштабного вторгнення. Однією з ключових програм стала «EU4Recovery – Розширення можливостей громад в Україні», започаткована у жовтні 2022 р. Програмою розвитку ООН (ПРООН) за фінансування Європейського Союзу [47]. Програма охоплює п’ять компонентів, серед яких особливу увагу приділено реінтеграції ветеранів. Основною метою є створення сприятливих умов для повернення ветеранів до цивільного життя, зокрема у професійній сфері.

Проєкт також підтримує цифровізацію послуг: передбачається створення та вдосконалення онлайн-інструментів для обслуговування ветеранів і членів їхніх родин. Зокрема, у Дніпропетровській області впроваджено систему «Я – ветеран», яка забезпечує комплексну соціальну, правову, медичну та психологічну підтримку на місцевому рівні. Платформа була адаптована для використання в Центрах надання адміністративних послуг (ЦНАП), а кількість доступних послуг розширено зі 100 до 300. Завдяки цьому ветерани можуть отримувати допомогу швидко та без черг. Станом на сьогодні системою скористалися понад 20 000 ветеранів області.

Ще одним важливим проєктом, реалізованим за підтримки GIZ, є «Skills4Recovery – Навчання та перепідготовка кваліфікованої робочої сили для відбудови України». Цей проєкт має більш вузьке спрямування, орієнтоване на

відновлення кадрового потенціалу в контексті післявоєнного відновлення країни. Його мета – розвиток робітничих професій, які є критично важливими для майбутньої відбудови.

Офіційно проєкт «Skills4Recovery» стартував у вересні 2023 р. і розрахований до середини 2026 р. Одним із ключових завдань проєкту є налагодження взаємодії між державними інституціями для планування освітніх програм відповідно до актуальних потреб ринку праці [48].

У межах цього проєкту було створено платформу «Освіта для ветеранів», що покликана стати інструментом допомоги у професійній адаптації колишніх військових. Платформа надає інформацію про доступні освітні можливості й допомагає ветеранам знайти новий професійний шлях у випадках, коли продовження роботи за попереднім фахом є неможливим [49].

Ініціатива реалізована у партнерстві з МОН, Міністерством економіки України, Національним агентством кваліфікацій, Державною службою зайнятості, військовими адміністраціями, закладами освіти та іншими постачальниками освітніх послуг.

Платформа має на меті систематизацію та узагальнення інформації про освітні можливості, що є вкрай важливим у контексті задоволення поточного попиту на ринку праці, а також сприяння адаптації ветеранів до цивільного життя.

Платформа «Освіта для ветеранів» стала відповіддю на потребу підвищення інформованості ветеранів про наявні можливості перекваліфікації та здобуття актуальних професій, а також – засобом популяризації робітничих професій, затребуваних на ринку праці.

Ініціатива стала частиною виконання «Стратегії переходу та інтеграції українських ветеранів до освіти і ринку праці», розробленої ГО «Українська асоціація маркетингу» в межах проєкту «Skills4Recovery». Стратегія охоплює чотири ключові напрями: розширення доступу до якісної освіти; підвищення рівня працевлаштування; розвиток ветеранського підприємництва; підтримка соціальної адаптації.

Платформа «Освіта для ветеранів» представлена у форматі каталогу освітніх можливостей різних рівнів і напрямів, що, станом на кінець 2024 р., містить понад 1 200 актуальних програм. Сайт має адаптивний, інклюзивний інтерфейс для осіб із порушеннями зору й включає: зручний інформаційний пошук із можливістю фільтрації за різними критеріями; блоки з описом рівнів освіти; аналітику щодо потреб ринку праці; прогнози щодо затребуваних професій [49].

Окрім функції агрегування освітніх можливостей, платформа «Освіта для ветеранів» виконує низку додаткових завдань, серед яких: збір статистичних даних щодо популярності програм, взаємодія з користувачами, верифікація закладів освіти та модерація контенту.

Платформа надає користувачам можливість підбору навчальних програм за низкою критеріїв, таких як: напрям підготовки, рівень освіти, тривалість навчання, вартість, форма навчання та географічне розташування навчального закладу. Це дозволяє ветеранам обрати саме ті освітні програми, які відповідають їхнім потребам і є актуальними в умовах сучасного ринку праці.

Складові платформи зображені на рис. 3.1–3.2.

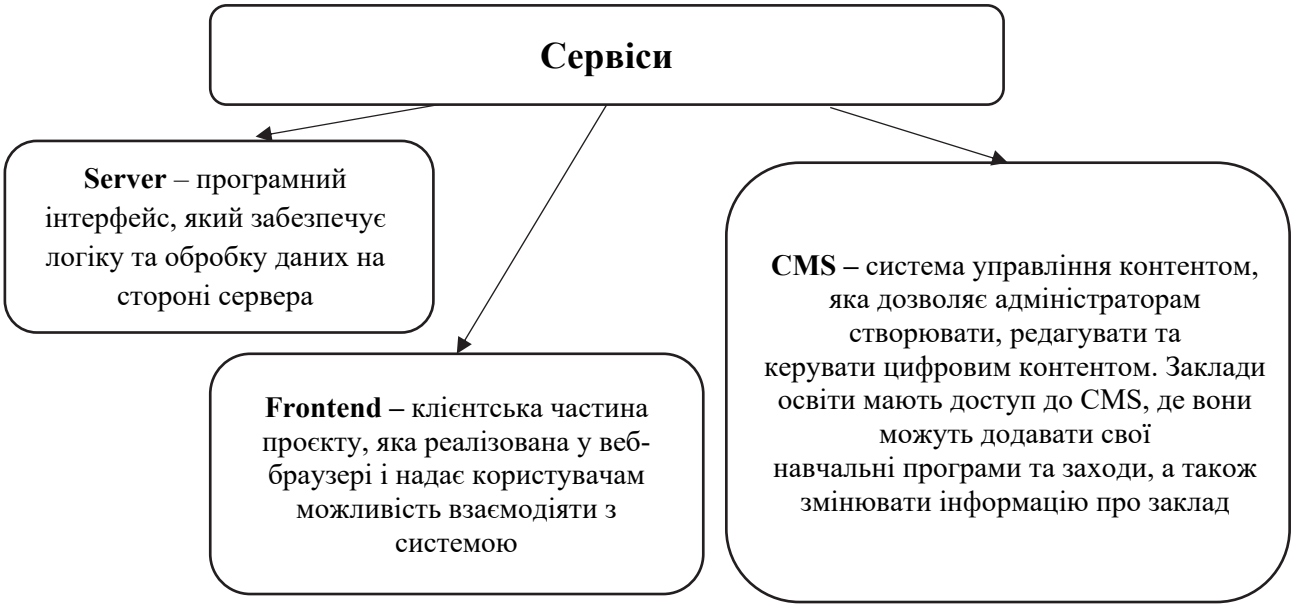


Рис. 3.1. **Сервіси платформи «Освіта для ветеранів»**
Побудовано авторами.

Рис. 3.2. **Сутності платформи «Освіта для ветеранів»**
Побудовано авторами.

Кожна складова відповідає за певний функціонал платформи:

– Server здійснює обробку запитів, управління даними, відповідає за автентифікацію та авторизацію, інтеграцію зі сторонніми сервісами, моніторинг та логування;

– CMS здійснює управління наповненням платформи, користувачами, освітніми програмами, формує звіти та аналітику, здійснює контроль доступу;

– Frontend відповідає за відображення компонентів, в тому числі освітніх програм та заходів, пошук та фільтрацію, автентифікацію і авторизацію, взаємодію користувача з освітніми закладами, моніторинг навчання.

Платформа використовує систему аутентифікації користувачів на основі JWT-токенів. Якщо користувач аутентифікувався, сервер генерує JWT-токен, що містить дані про користувача та його рівень доступу. При повторній аутентифікації сервер перевіряє JWT-токен і, якщо дані ведено правильно, надає користувачу права доступу відповідно до ролі керівника закладу або адміністратора (рис. 3.3).

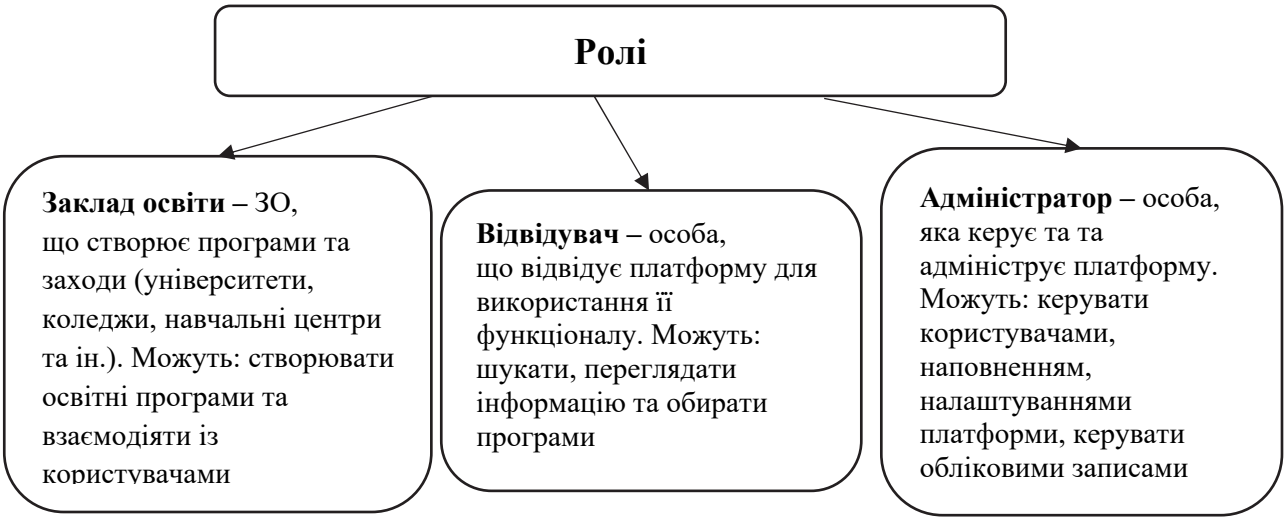


Рис. 3.3. **Ролі користувачів платформи «Освіта для ветеранів»**
Побудовано авторами.

Адміністратор платформи здійснює керування через панель адміністратора. Після вдалої автентифікації, адміністратор має доступ до особистого кабінету, де може переглядати дані свого акаунту, список закладів, що пропонують освітні програми на платформі та дані користувачів, може скористатись професійним словником.

На сторінці «Дашборд» можна переглядати статистику перегляду освітніх програм та контактів організацій, що їх надають, у вигляді графіків чи діаграми. Отримані дані дають можливість оцінити привабливість програми для відвідувачів сайту, а, відповідно, оцінити рівень зацікавленості.

Сторінка «Заклади» містить перелік всіх навчальних закладів, що зареєстровані на платформі. Під час реєстрації, кожному закладу присвоюється унікальний ID, назва, місто, статус закладу. Кожен заклад має картку, де зафіксована інформація про нього. Також, картка містить позначку про статус перевірки закладу та програм. Адміністратор перевіряє профілі створених закладів, за потреби, може редагувати інформацію про заклади, перевіряти статус перевірки навчальних програм та вносити зміни у внесені данні програми. Також, адміністратор може вносити зміни у навчальні програми, що вже є на сайті та додавати нові. Адміністратор може видалити на актуальну інформацію про заклади та навчальні програми. Також, адміністратор може керувати

освітніми заходами, що розміщуються на платформі. Таким чином, забезпечується актуальність та достовірність даних, що представлені на платформі.

Сторінка «Користувачі» містить перелік всіх зареєстрованих користувачів. Під час реєстрації, користувачам також присвоюється номер ID, роль та адреса електронної пошти. Для забезпечення доступу, адміністратор може змінити пароль адміністратора.

Сторінка «Словники» містить інформацію про всі освітні заклади, професії, документи та інше. Адміністратор може додавати або змінювати інформацію про професії, спеціалізації, форми власності закладів, категорії, підтверджуючі документи про освітні програми, можливі форми оплати, типи та тривалість освітніх програм, форми навчання та формати проведення навчання.

Освітні програми та заходи на платформі акумулюються від різних закладів освіти (ЗО) та організацій. Для забезпечення достовірності представленої інформації, реєстрація та розміщення навчальних програм відбуваються виключно через адміністратора платформи. Зацікавлений заклад або організація має отримати посилання на реєстраційну форму, заповнення якої надає можливість розміщення відповідних освітніх продуктів.

Після додавання програми, вона проходить процедуру верифікації адміністратором платформи, представником МОН. Лише після підтвердження відповідності програма стає доступною для перегляду користувачами. Адміністратор має можливість переглядати, редагувати чи видаляти програми або інформацію про заклади, що дозволяє підтримувати актуальність, точність і якість контенту. Аналогічна процедура верифікації застосовується і у випадку змін у даних про програму чи заклад. До моменту проходження повторної модерації оновлена інформація не відображатиметься в результатах пошуку. Це запобігає появі недостовірних або сумнівних ініціатив на платформі.

Функціонал платформи також включає моніторинг популярності програм серед користувачів, що дозволяє визначати напрями з найвищим попитом. Аналіз запитів дає змогу ідентифікувати найцікавіші освітні пропозиції та

визначити ключові критерії вибору програм, що, у свою чергу, може бути використано для формування державної політики у сфері освіти. Зокрема, такі дані корисні для стратегічного планування, удосконалення змісту освітніх програм і коригування державного замовлення відповідно до потреб ринку праці.

З урахуванням потреб цільової аудиторії, платформа має адаптивний інтерфейс, зокрема – опції кастомізації для осіб з порушеннями зору. Користувач може змінити дизайн сайту на чорно-білий, налаштувати розмір шрифту, міжлітерний інтервал, збільшити курсор, активувати лінію для зручного читання, підкреслення посилань тощо. Це суттєво підвищує доступність платформи для широкого кола користувачів і сприяє залученню осіб з інвалідністю до процесу професійної адаптації.

Головна сторінка платформи структурована у вигляді інформаційних блоків, що допомагають користувачу сформувати власний запит і зорієнтуватися в наявних можливостях. Зокрема, містяться: розділ про сам проєкт; блок «Рівні освіти» з коротким описом рівнів національної системи освіти та специфіки здобуття освіти на кожному з них; блок «Інфографіка», який містить аналітичні дані про прогнозований попит на ринку праці та найбільш затребувані професії; розділ «Популярні питання», що містить відповіді на поширені запити й орієнтує користувача щодо використання функціоналу платформи.

Таке наповнення платформи сприяє полегшенню пошуку інформації, формулюванню індивідуального запиту та ухваленню освітнього рішення, що відповідає особистим потребам та життєвим обставинам ветерана.

На головній сторінці розміщено блок «Що шукаєте?», який являє собою систему пошуку із можливістю налагодження параметрів сортування за регіоном та ключовими словами, при натискання кнопки «Знайти освіту», користувач переходить на сторінку розширеного пошуку, де можна обрати більш детальні параметри пошуку: заклад освіти, професія, спеціальність, тривалість, наявність інклюзивних умов у закладі та тип освіти. Цей функціонал дає можливість персоналізувати запит під потреби користувача та відібрати найбільш відповідні пропозиції навчальних програм.

Блок «Рівні освіти» допомагає користувачу ознайомитись із різницею умов зарахування, тривалістю навчання та специфікою навчальних закладів, що надають освітні послуги різних рівнів. Цей інформаційний блок створений для допомоги користувачу у подальшій орієнтації у навчальних програмах, що пропонуються та визначені того типу навчання, що цікавить конкретного шукача.

Блок «Інфографіка» репрезентує прогнозовану потребу у кадрах на ринку праці у поточному та наступних роках. Доповнює вказану інформацію блок «Очікувано затребувані професії», який демонструє спеціальності, що користуються найбільшим попитом серед роботодавців. Ці блоки мають за мету інформування про тенденції ринку праці та допомагають шукачу співставити свої навички, бажання та наявні тенденції задля найкращого вибору шляху у навчанні.

Станом на сьогодні платформа функціонує в режимі дослідної експлуатації та перебуває у процесі вдосконалення. Попри це, вона вже виконує роль акумулятора актуальних освітніх можливостей для ветеранів, допомагаючи їм визначитися з професійним напрямом у нових соціально-економічних реаліях. У табл. 3.1 продемонстровані основні переваги впровадження у широке використання платформи «Освіта для ветеранів».

Таблиця 3.1

Переваги від впровадження платформи «Освіта для ветеранів»

Зацікавлені сторони	**Переваги від впровадження платформи «Освіта для ветеранів»**
Ветерани (Користувачі)	- Доступ до актуальних та перевірених освітніх програм різного рівня та напрямку; - Можливість індивідуального підбору програм за критеріями (географія, напрям, тривалість, форма, вартість тощо); - Адаптивний інтерфейс для людей з інвалідністю; - Інформаційна підтримка щодо ринку праці та затребуваних професій; - Сприяння професійній реінтеграції, перекваліфікації та соціальній адаптації; - Підвищення обізнаності про доступні освітні можливості та зниження бар’єрів до навчання.
Заклади освіти	- Безкоштовне розміщення програм на платформі з офіційною модерацією та верифікацією; - Залучення нової аудиторії – ветеранів, як здобувачів освіти; - Можливість отримувати зворотний зв’язок через аналітику запитів; - Посилення прозорості та довіри до програм закладу.

Зацікавлені сторони	Переваги від впровадження платформи «Освіта для ветеранів»
Державні органи	- Інструмент реалізації державної політики реінтеграції ветеранів та освіти дорослих; - Управлінсько-аналітична підтримка на основі даних з платформи (попит, популярність програм, освітні потреби); - Підвищення ефективності міжвідомчої взаємодії між МОН, Мінветеранів, службою зайнятості тощо; - Підтримка цифровізації послуг.
Роботодавці	- Наявність інформації про актуальні освітні програми для майбутніх працівників; - Підвищення кваліфікації ветеранів відповідно до потреб ринку; - Потенційне зменшення дефіциту кадрів у критичних галузях (будівництво, інженерія, ІТ тощо); - Можливість формування запитів щодо змісту освітніх програм та участі в їхньому наповненні

Складено авторами.

Платформа «Освіта для ветеранів» демонструє динамічний розвиток і потенціал подальшого масштабування. Серед актуальних напрямів удосконалення – підвищення інтеграції з закладами освіти для розширення доступу до інформації та поглиблення співпраці. Зокрема, важливим кроком є реалізація можливості прямого переходу на вебсайти ЗО зі сторінок освітніх програм, розміщених на платформі. Це дозволить користувачам оперативно ознайомлюватися з детальною інформацією про заклад, умови вступу та особливості навчального процесу. Водночас, позначки на офіційних вебсайтах освітніх закладів про їхню участь у платформі «Освіта для ветеранів» підвищуватимуть видимість цієї ініціативи та інформованість цільової аудиторії.

На цьому етапі свого розвитку платформа є перспективним інструментом трудової реінтеграції та підвищення інформованості ветеранів про наявні освітні можливості. Вона має потенціал стати комунікаційним містком між потребами ветеранів, можливостями освітніх закладів і запитами ринку праці. Популяризація програм, які відповідають сучасним вимогам роботодавців, сприятиме зниженню кадрового дефіциту в галузях, що зазнали найбільших втрат унаслідок війни, а також підтримуватиме формування економічно активного населення серед демобілізованих громадян.

3.2. Функціонування інформаційної платформи «Позашкілля»

Позашкільна освіта є важливою невід'ємною частиною системи освіти України [5]. Так само, як і інші складники національної системи освіти, позашкільна освіта відіграє важливу роль у формуванні компетентностей дітей [50]. Завданнями позашкільної освіти є не тільки освіта вихованців, учнів і слухачів, а ще й виховання свідомих громадян України, навчання розуміння важливості прав і свобод людини, відповідальності за свої вчинки; надання можливості вільного розвитку особистості відповідно до інтересів та здібностей; виховання патріотизму, любові до України; створення можливостей для творчого, фізичного, інтелектуального розвитку, здобуття професійних навичок; задоволення освітніх потреб, що не можуть бути забезпечені іншими рівнями системи освіти [51].

Тож, важко недооцінити значимість цієї складової системи освіти України, як додаткового засобу розвитку, а також її вплив на формування не тільки більш поглиблених професійних навичок, а й здобуття соціальних навичок, розуміння себе як частини команди, соціуму, виховання свідомих представників громадянського суспільства.

Через політично-економічні труднощі, які переживає наша країна останні роки, сфера позашкільної освіти зазнала значного удару – зокрема пандемія COVID-19 та повномасштабне вторгнення рф суттєво вплинули на цю сферу, що призвело до скорочення кількості закладів позашкільної освіти (ЗПО) та вихованців, учнів і слухачів (табл. 3.2).

Таблиця 3.2

Динаміка розвитку позашкільної освіти в Україні у 2019–2025 рр.

Кількість станом на початок року	2019 р.	2020 р.	2021 р.	2022 р.	2023 р.	2024 р.	2025 р.
Закладів позашкільної освіти, *од.*	1 382	1 389	1 351	1 263	1 153	1 170	1 151
Вихованців, *осіб*	1 275 253	1 190 490	1 138 171	1 014 981	790 834	798 854	781 388
Гуртків, груп, класів, *од.*	77 960	73 739	71 468	63 972	50 765	51 869	51 323

Складено авторами за: [52].

Дані табл. 3.2 підтверджують поступове скорочення кількості ЗПО та кількості вихованців, учнів і слухачів за період 2019-2025 рр. Пандемія, у 2019-2022 рр. спричинила скорочення кількості функціонуючих закладів через неможливість організації безпечного процесу надання освітніх послуг. Як відповідь на цей виклик, напрямок розвитку позашкільної освіти було зосереджено на забезпечення можливості отримання якісної позашкільної освіти вихованцями у безпечних умовах. МОН забезпечило отримання освітніх послуг дистанційно за допомогою використання сучасних інформаційних технологій та розвитку інтегрованих інформаційних систем для функціонування позашкільної освіти онлайн [53].

Для організації роботи ЗПО в умовах пандемії МОН розробило організаційно-методичні рекомендації щодо дистанційного навчання в позашкільній освіті [54]. У цьому документі вказано принципи організації дистанційного навчання у закладах позашкільної освіти, зазначено інформацію щодо інструментів дистанційного навчання. Також, було надано методичні рекомендації щодо організації безпечного освітнього процесу ЗПО в очному форматі у 2021/2022 н. р. ЗПО, що підпорядковані МОН, стали прикладом реалізації рекомендацій щодо дистанційної роботи. Вони зібрали та розмістили на своїх офіційних веб-сайтах інформацію стосовно організації дистанційного навчання та ефективні приклади реалізації даного формату навчання [55].

Найбільше скорочення кількості ЗПО та вихованців, припадає на час повномасштабного вторгнення, що пов’язано з великою кількістю нових викликів, спричинених війною, таких як міграція вихованців, педагогічного персоналу, питання організації безпечного освітнього процесу, руйнування інфраструктури та ін. У лютому 2022 р. освітній процес зупинився у більшості закладах освіти.

Моніторингове дослідження щодо забезпечення доступу до якісної позашкільної освіти, що проводилося Державною службою якості освіти навесні 2023 р., так само показало скорочення кількості ЗПО на 10 % за 2021–2023 рр. [56].

Опитування Служби освітнього омбудсмена, проведене у серпні 2022 р., показало, що 52,3 % опитаних не відвідували ЗПО до повномасштабного вторгнення, а 49,4 % з тих, хто відвідував, вказали, що припинили заняття через війну [57].

Постало питання відновлення освітнього процесу у найбільш безпечному форматі з огляду на нові реалії. Зважаючи на це, МОН спрямувало усі зусилля для відновлення освітнього процесу у дистанційному форматі. Розроблено методичні рекомендації щодо підготовки закладів освіти до 2022/2023 н. р. в умовах військового стану [58]. Вдалося досягти відновлення роботи більшості закладів країни.

У березні 2023 р. благодійним фондом «Клуб добродіїв» було проведене дослідження «Підлітки та їхнє життя під час війни». Згідно з результатами дослідження, 85 % підлітків мають хобі. 48 % опитаних вбачають зв'язок між хобі та самореалізацією у майбутньому, а 16 % мріють у майбутньому перетворити хобі на професію [59].

Незважаючи на скорочення кількості закладів й труднощі у роботі, спричинені війною, позашкільна освіта залишається важливим складником системи освіти, особливо цінним в нових реаліях, адже заняття у гуртках, підтримка однодумців виконують, також, терапевтичну функцію та дають можливість покращити психологічний стан сучасної молоді [60].

Наявність попиту та неможливість державних закладів повністю задовільнити його сприяли поширенню кількості приватних закладів позашкільної освіти, що формально не підпорядковуються органам державної влади або місцевого самоврядування, не зобов'язані отримувати ліцензію для здійснення освітньої діяльності та функціонують повністю автономно. Такий процес має як позитивні, так і негативні наслідки. З одного боку, наявність великої кількості представників малого бізнесу сприяє розбудові економіки, задовольняє попит на послуги високої якості, розширює перелік освітніх послуг. Проте, повна автономність позбавляє можливості репрезентативного аналізу та збору статистичних даних про вихованців таких закладів через відсутність

необхідності звітування та передачі інформації державним органам, а також контролювання контексту та цінностей які розповсюджуються приватними закладами, їх відповідність загальнонаціональному вектору розвитку та цілям національної системи освіти. Саме тому пошук засобів моніторингу діяльності ЗПО, що не підпорядковані органам державної влади, є актуальним, особливо враховуючи нинішню соціально-політичну ситуацію в нашій країні.

У часи цифровізації та реформування української системи освіти в цілому, позашкільна освіта теж не може знаходитися осторонь цього процесу. Тож, позашкільна освіта також поступово зазнає змін і осучаснення.

На хвилі впровадження інформаційних технологій у закладах освіти, починають з'являтися репрезентативні сайти закладів освіти. Були створені сайти Державної служби молоді та спорту, Федерації дитячих організацій України, всесвітнього скаутського бюро та ін. [61]. Для цього періоду характерні перші проби упорядкування інформації щодо ЗПО у вигляді каталогів на місцевих сайтах з описом та контактними даними. Проте, у діях присутня хаотичність і локальність збору даних, відсутність системного підходу до висвітлення інформації.

З 2009 р. в системі освіти було запроваджено електронний формат подання звітності за допомогою електронної пошти. Директори закладів надсилали електроні звіти у форматі Excel або Word та допоміжних програм локального рівня. Таким самим чином відбувалася передача звітності і у позашкільній освіті, проте основна маса закладів все ще використовувала паперову форму звітності, а при використанні електронного варіанту відбувалося дублювання у паперовому форматі.

У 2010-2015 рр. стали з'являтися локальні ініціативи цифрового обліку гуртків, але без системності викладу інформації та уніфікації. У деяких регіонах створюються електронні каталоги гуртків (наприклад, обласні сайти з переліком секцій і гуртків). Вперше починають використовуватися електронні журнали у роботі окремих гуртків. Починає налагоджуватись процес подачі звітності в

електронному вигляді на регіональному рівні. У цей період відбуваються перші спроби цифровізації документації та створення реєстрів на регіональному рівні.

У 2017 р. було створено сторінку «Позашкільні заклади та освітні центри» на офіційному сайті Київської міської державної адміністрації (КМДА) [62]. Сервіс надає можливість пошуку гуртка за інтересами, районом, віком, зробити онлайн-запис на гуртки, переглянути рейтинг популярності програм, дані про заклад, графік занять, вік дітей, викладача.

Львівською міською радою був створений Портал відкритих. Це ресурс з десятками наборів даних серед яких у 2019 р. з'явилися і переліки закладів освіти, в тому числі позашкільної. Портал містить переліки секцій та гуртків Львову та Львівської територіальної громади з інформацією про них. Портал не надає можливості пошуку гуртка або запису на заняття, проте містить каталог ЗПО і спортивних секцій державної та комунальної власності та їх контактною інформацією [63].

Війна стала додатковим фактором, що активізував інтеграцію національної освітньої системи у європейський освітній простір. Підсилилася співпраця з європейськими партнерами на всіх рівнях: від консультацій стосовно розробки нормативних актів, до оновлення матеріально-технічної бази закладів освіти.

У лютому 2023 р., було презентовано спільний план роботи МОН та Міжнародної асоціації позашкільної освіти на 2023 рік. Головними пріоритетами на шляху розвитку позашкільної освіти, згідно з планом, стало: налагодження державно-громадського партнерства, аналіз міжнародного досвіду розвитку компетентностей вихованців, цифровізація сфери позашкільної освіти у рамках євроінтеграції освіти [64].

Проте, ще до початку повномасштабного вторгнення, відбувалося активне обговорення питання трансформації позашкільної освіти у рамках загального процесу цифровізації. Створений у 2021 р. директорат цифрової трансформації МОН від самого заснування розпочав роботу над питаннями розробки засобів цифровізації освіти. Було розпочато низку проєктів, що стосувалися різних складників освіти, таких як професійна (професійно-технічна) освіта (створення

EMIS – модулю збору статистичної та звітної інформації закладів професійної (професійно-технічної) та позашкільної освіти (створення і запуск інформаційно-аналітичної системи «Позашкілля») [65].

Наказ МОН від 06.09.2022 № 795 [66] зобов'язав департаменти (управління) освіти і науки обласних, Київської міської військових (державних) адміністрацій перевірити наявність та достовірність даних про органи управління у сфері освіти за їх місцезнаходженням відповідної адміністративно-територіальної одиниці, достовірність та повноту переліку закладів дошкільної освіти (ЗДО), ЗЗСО, ЗПО, закладів професійної (професійно-технічної) та фахової передвищої освіти, які забезпечують здобуття повної загальної середньої освіти у функціонуючій програмно-апаратний комплекс «Автоматизований інформаційний комплекс освітнього менеджменту» (ПАК «АІКОМ»). З цього часу ЗПО офіційно доєдналися до загальної електронної мережі з повним переліком закладів, що підпорядковуються органам управління освітою.

З метою збору та поширення інформації про ЗПО різних форм власності та підпорядкування, враховуючи і приватні заклади, що не ліцензуються і не підпорядковуються органам управління освітою, навесні 2021 року МОН разом із SoftServe, що є найбільшою ІТ-компанією українського походження, розпочали проєкт по створенню порталу «Позашкілля». Метою співпраці став розвиток позашкільної освіти у бік цифровізоції. SoftServe розробили інформаційно-аналітичну систему для всіх закладів, що надають послуги позашкільної освіти [67].

Мета порталу «Позашкілля» створити систему, що акумулюватиме більш розширені дані про заклади і гуртки всіх форм власності, що надають освітні послуги.

Створення інформаційно-аналітичної системи «Позашкілля» є відповіддю на нагальні потреби модернізації та цифровізації галузі. Наразі портал функціонує у режимі дослідної експлуатації [68].

Система «Позашкілля» – це інформаційно-аналітична система реалізована у вигляді сервісного порталу, зручного користувачу для пошуку гуртків, запису

дітей та дорослих, відслідковування чисельності вихованців та їх досягнень, а для державних структур – отримання статистичних показників. Також портал дозволяє відслідковувати результати обдарованих дітей у всеукраїнських та міжнародних конкурсах, олімпіадах, а також дітей, які отримали гранти за досягнення. Така функція дає можливість заохочувати талановитих дітей та зменшити відтік обдарованої молоді.

Структура порталу складається з таких частин: кабінету споживача послуг, кабінету надавача послуг та кабінету адміністраторів різного рівня. Також, можливе використання порталу сторонніми користувачами, що не зареєстровані у системі.

Функціонал порталу «Позашкілля» спрямований на те, щоб спростити взаємодію на різних рівнях, тому ієрархічна структура ролей та функціонал адміністраторів порталу відображає структуру органів управління позашкільною освітою, що робить користування порталу зрозумілим для адміністраторів. Структурна ієрархія адміністраторів порталу зображена на рис. 3.4.

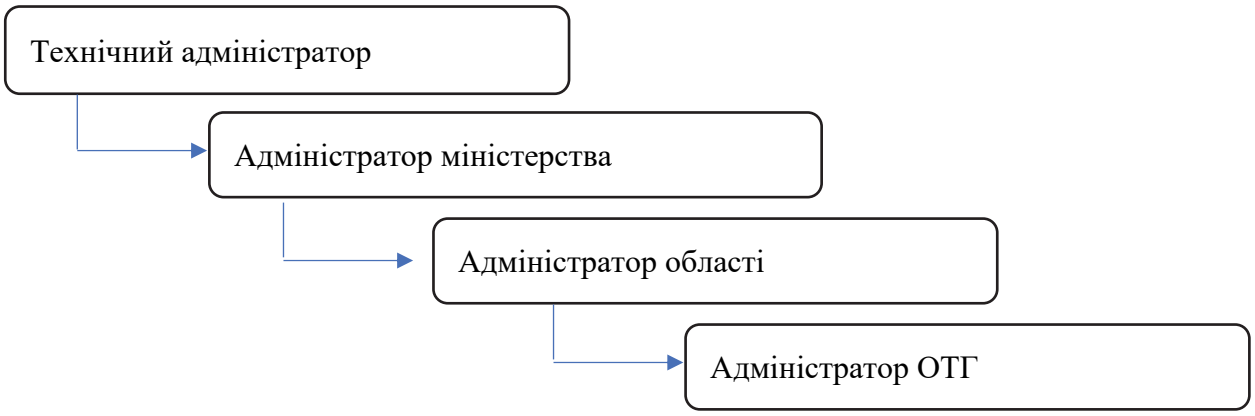


Рис. 3.4. **Ієрархічна структура адміністраторів порталу «Позашкілля»**
Побудовано авторами.

Адміністратори всіх рівнів взаємодіють з платформою через особисті кабінети. Для підтвердження особи адміністратора та додаткового захисту інформації, у кабінеті адміністратора використовується КЕП-ключ.

Технічний адміністратор є вищим щаблем керування іншими користувачами порталу. З огляду та те, що платформа «Позашкілля» була передана в адміністрування ДНУ «ІОА», як основному реципієнту статистичних

даних, саме представник інституту виконуватиме роль технічного адміністратора. Це дозволить оперативно отримувати необхідні статистичні дані відповідно до потреб.

Технічний адміністратор має широкий функціонал адміністративного і технічного характеру для керування як адміністративною структурою, так і коректним функціонуванням порталу. Серед основних функцій технічного адміністратора слід виділити: створення та керування адміністраторами міністерств, області (за потреби), керування адміністраторами області, створенеми технічним адміністратором, створення надавачів послуг державної або комунальної форми власності або підтвердження реєстрації приватних закладів та затвердження їх ліцензій за наявності, керування надавачами послуг, створення напрямку навчання. Ці можливості допоможуть забезпечити адміністративну ієрархію порталу, що відповідатиме адміністративній структурі у сфері позашкільної освіти та враховуватиме специфіку підпорядкування.

За допомогою вибудованої структури адміністрування, технічний адміністратор зможе переглядати, сортувати за критеріями і підпорядкуванням заклади освіти, вивантажувати статистичні данні про здобувачів освіти, власне заклади, педагогів. Статистика, що відображається, залежить від рівня доступу адміністратора. Технічний адміністратор може переглядати та завантажувати статистичні дані усіх користувачів порталу, незалежно від підпорядкування.

Залежно від напрямку, ЗПО державної форми власності підпорядковуються різним міністерствам. Відповідно до ієрархії порталу «Позашкілля», адміністратор міністерства має доступ до керування даними і перегляду, вивантаження статистики тих закладів, що підпорядковані його міністерству, але не може переглядати статистику інших міністерств та приватних ЗПО. У кабінеті адміністратор міністерства створює та керує даними і статусом адміністраторів областей для ефективного управління на місцях.

Адміністратор області та адміністратор ОТГ (об’єднаної територіальної громади) мають схожі функціональні можливості, які поширюються за таким самим принципом, як і у адміністраторів міністерств – кожен обласний

адміністратор може керувати, бачити та вивантажувати статистичні дані ЗПО, що підпорядковані відповідному регіону, та не може керувати, вносити зміни чи бачити статистичні дані ЗПО, що відносяться до інших територіальних одиниць.

Таким чином, структура адміністрування розроблена з урахуванням відображення реальної адміністративної структури позашкільної освіти та зручного розподілу функціоналу відповідно до рівнів доступу.

Для користувачів портал «Позашкілля» поділяється на 2 частини: кабінет користувача (дитина або її батьки) та кабінет надавача послуг (директор ЗПО). Також, пересічний користувач, який не зареєстрований у системі, може звертатися до порталу, як до каталогу щоб знайти, переглянути та обрати варіанти гуртків для себе чи дитини.

Надавачі послуг можуть керувати гуртками, відкривати та закривати набір вихованців, учнів, слухачів, формувати групи, збирати статистику про користувачів, що відвідують гуртки надавача, відмічати особливо талановитих дітей на сторінці закладу у розділі «Досягнення».

Можливість листування між надавачем послуг і користувачем є інструментом вибудови ефективного зв’язку між користувачами порталу шляхом вчасного розповсюдження корисної інформації, що стосується вихованців, розкладу занять чи змін у роботі гуртків.

Система оцінок і коментарів є додатковим засобом заохочення та відображає цікавість користувачів до тих чи інших занять.

Портал має стати ефективним маркетинговим засобом для ЗПО завдяки поширенню інформації про гуртки закладу, відкриті набори та можливості. Враховуючи загальну діджиталізацію та зміну способів пошуку й отримання інформації громадянами, портал «Позашкілля» стане не тільки засобом адміністрування та збору статистичних даних, а й слугуватиме підвищенню обізнаності й зацікавленості до ЗПО у сучасних батьків та дітей, що стимулює популяризацію серед населення позашкільної освіти, як важливого складника освіти протягом життя.

Поширення використання порталу «Позашкілля», як інформаційної освітньої системи, має ряд переваг різного спрямування. Основні переваги зображено на рис. 3.5.

Рис. 3.5. **Переваги використання порталу «Позашкілля»**
Побудовано авторами.

Сучасний розвиток інформаційних технологій відіграє ключову роль у трансформації освітнього середовища, зокрема у сфері позашкільної освіти. Упровадження цифрових рішень, таких як портал «Позашкілля», забезпечує значне покращення управлінських процесів, підвищує рівень доступності освітніх послуг та сприяє ефективному використанню ресурсів.

Основними перевагами використання порталу є автоматизація збору, даних всіх надавачів послуг позашкільної освіти різної форми власності та підпорядкування, що дозволяє оперативно реагувати на виклики у сфері

позашкільної освіти. Завдяки цифровізації адміністратори отримують зручний інструмент для моніторингу діяльності закладів, оцінки ефективності програм та формування звітності. Впровадження у широке використання порталу «Позашкілля» сприятиме створенню єдиного інформаційного простору, що значно покращує взаємодію між державними органами, закладами освіти, педагогами, вихованцями, учнями й слухачами та їхніми батьками.

Система рейтингів та заохочень порталу може допомогти виділяти ті заклади, що мають найкращі показники, а інформація про ліцензування – підштовхнути приватні заклади до впровадження державних вимог до освітнього процесу та отримання ліцензій.

Слід зазначити, що незважаючи на переваги впровадження порталу «Позашкілля», є ряд перепон для реалізації цього проєкту. З огляду на те, що приєднання до платформи не є обов'язковим на законодавчому рівні та відсутності механізмів впливу на заклади приватної форми власності, що не підпорядковані національній системі освіти, стає актуальним питання шляхів популяризації та висвітлення переваг використання платформи саме як маркетингового інструменту та засобу зручного адміністрування діяльності закладу.

Запровадження таких інформаційних платформ підвищує прозорість управління освітніми процесами, спрощує доступ до позашкільної освіти для широкого кола користувачів та сприяє підвищенню якості освітніх послуг.

Таким чином, цифрові технології в освіті є не лише інструментом оптимізації управлінських процесів, а й важливим чинником підвищення ефективності та доступності освіти загалом і дошкільної освіти зокрема.

Портал «Позашкілля» спрямований на поширення інформації, спрощення комунікації між надавачами та отримувачами освітніх послуг закладів всіх форм власності та підпорядкування. Це інструмент збору та накопичення інформації не тільки про ЗПО, що підпорядковані державним органам управління, а і приватних надавачів послуг, що функціонують без ліцензування.

Збір інформації про всіх надавачів послуг позашкільної освіти допоможе створити більш репрезентативну базу даних для подальшого аналізу і досліджень в освітній сфері.

Подальші дослідження можуть бути спрямовані на вивчення можливостей інтеграції інформаційних систем, розширення можливостей взаємодії порталу «Позашкілля» з іншими освітніми та державними інформаційними системами, впливу інтеграції інформаційних ресурсів на ефективність управління позашкільною освітою, впливу цифрових технологій на якість освіти, розробку методів та засобів поширення інформації та популяризації використання порталу серед потенційних надавачів та отримувачів послуг в позашкіллі.

3.3. Функціонування інформаційної платформи про здорове шкільне харчування «ЗнаЇмо»

Наприкінці 2021 р. в Україні розпочала роботу платформа про здорове харчування у школах «Знаїмо». Вона є частиною реформи системи шкільного харчування, яка відбувається в Україні за ініціативи першої леді Олени Зеленської.

За цей час, платформа стала інформаційним вісником реформи, зібрала в одному місці усі матеріали, законодавчу базу, поради, новини розвитку реформи, позитивні практики та настанови.

Назва «Знаїмо» розшифровується як «знаємо, що їмо» (рис. 3.6).

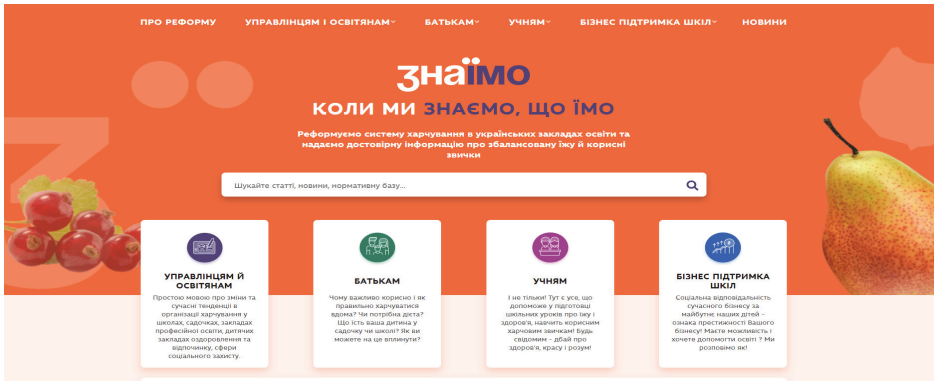


Рис. 3.6. **Платформа «Знаїмо»**

Джерело: [69].

Мета платформи – покращення культури харчування дітей та надання інструментів для організації якісного та здорового харчування в закладах освіти.

Сайт містить понад 200 текстових матеріалів, близько сотні презентацій, анімаційних об’єктів, інструкцій та відповідей на актуальні питання щодо реформи шкільного харчування.

В межах своєї мети, портал виконує наступні основні завдання:

– надання достовірної інформації про здорове харчування;

– ноз’яснення нових стандартів шкільного харчування та норм харчового забезпечення;

– допомога освітянам у впровадженні нових підходів до харчування;

– залучення батьків до контролю якості харчування дітей;

– створення платформи для навчання кухарів і персоналу шкільних їдалень.

Портал розподілений на тематичні блоки за цільовою аудиторією і буде корисний таким категоріям як:

– учні можуть отримати інформацію як правильно харчуватися, отримати цікаві матеріали про здоровий спосіб життя;

– батьки – отримати поради щодо організації здорового харчування вдома та в школі;

– освітяни – навчитися впроваджувати нові стандарти харчування та систему НАССР (контроль безпечності харчових продуктів);

– управлінці – знайти методичні рекомендації щодо модернізації харчоблоків та закупівель;

– представники бізнесу – зрозуміти, як підтримати реформу шкільного харчування через партнерські проєкти.

Розділи платформи розділені за групами відвідувачів на тематичні блоки, кожен з яких містить усі напрацювання реформи за тематикою.

Так, у розділі «Управлінцям й освітянам» зібрано інформацію для освітніх управлінців та керівників закладів освіти про нормативно-правові акти, які стосуються реформи шкільного харчування, роз’яснення з організації

харчування у школах, закупівель продуктів та обладнання, приклади успішних практик тощо. Розділ містить інтерактивний калькулятор обладнання, який дозволяє прорахувати кількість різного за видом обладнання, необхідного харчоблоку в залежності від структури харчоблоку та кількості дітей, що потребують харчування. Ці матеріали спрямовані допомогти проводити зміни на місцях і забезпечувати школярів здоровим харчуванням (рис. 3.7).

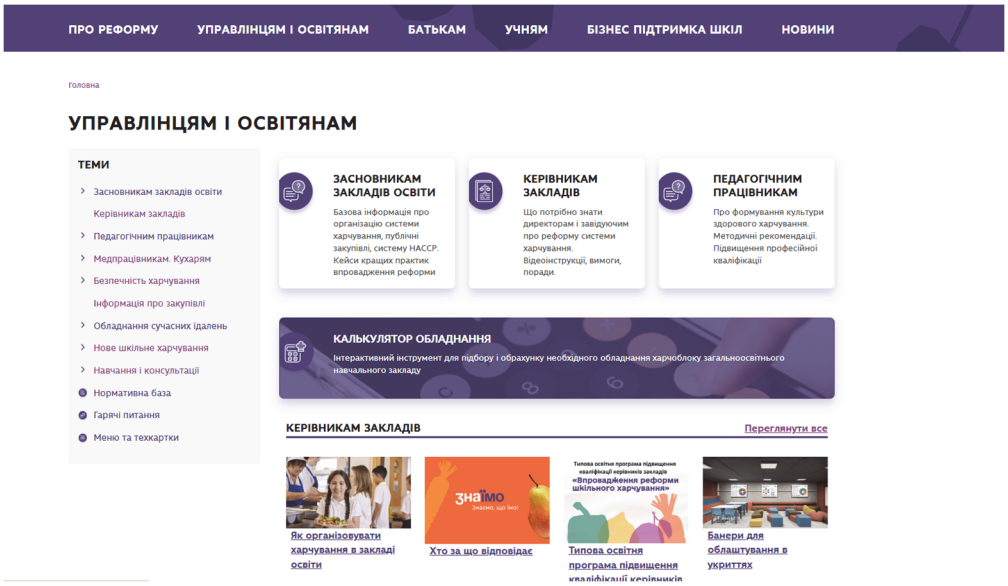


Рис. 3.7. **Інформація для управлінців та освітян**

Джерело: [69].

Підрозділ «Засновникам закладів освіти» має на меті скоординувати засновників ЗЗСО та ЗДО у ключових питаннях реформування харчування. Підрозділ містить корисні статті що до питань організації харчування за сучасними вимогами, приклади кращих практик у впровадженні реформи, рекомендації що до організації закупівель та рекомендації по впровадженню та підтримці сисетми HACCP в закладах.

Підрозділ «Педагогічним працівникам» зібрав навчальні матеріали та курси для підвищення кваліфікації та отримання нових навичок педагогічного персоналу, матеріали для проведення уроків з учнями, інформаційні банери для облаштування класів та укриттів. Також, у цьому підрозділі містяться корисні матеріали для шкільного психолога про харчові розлади та рекомендації що до формування здорових відносин з їжею та сприйняття свого тіла.

Підрозділ «Медпрацівникам та кухарям» містить збірники рецептур, поради що до методів приготування та вибору продуктів, а також відеоінстрікції з організації технологічних процесів під час приготування їжі.

У підрозділі «Безпечність харчування» зібрані матеріали на тему впровадження системи HACCP: рекомендації, поради та інструкції.

У підрозділі «Інформація про закупівлі» можна знайти рекомендації з користування сервісом Prozorro Market та корисні статті що організації закупівельного процесу.

Підрозділ «Обладнання сучасних їдалень» містить корисну інформацію що до модернізації їдалень з урахуванням сучасних норм: нормативну базу, методичні рекомендації, поради по плануванню і проведенню робіт з переоснащення.

Підрозділ «Нове шкільне харчування» наповнений статтями, спрямованими на популяризацію реформи та роз'яснення спірних питань та змін, що відбуваються внаслідок її впровадження.

У підрозділі «Навчання і консультації» зібрав матеріали стосовно підвищення кваліфікації, формування сучасних знань про шкільне хар чування управлінців та освітян за різними напрямками. Також, цей розділ містить відеоматеріали для учнів на тему здорового харчування, які рекомендовано використовувати в освітньому процесі.

На платформі розміщено, також, підбірку нормативної бази що до шкільного харчування, гарячі питання для публічного обговорення, рекомендовані меню для шкіл і технологічні картки приготування страв.

У розділі «Батькам» міститься калькулятор індексу маси тіла для виявлення проблем із зайвою вагою у дитини. Розділ для батьків учнів містить матеріали та корисні поради що до організації здорового харчування вдома, спрямовані на навчання дітей харчуватись правильно не тільки в стінах навчального закладу, а формувати правильні харчові звички протягом життя. Цей розділ, також, містить інформацію що до організації харчування дітей з

особливими дієтичними потребами. Розділ також містить поради, як допомогти дітям призвичаїтись їсти корисно (рис. 3.8).

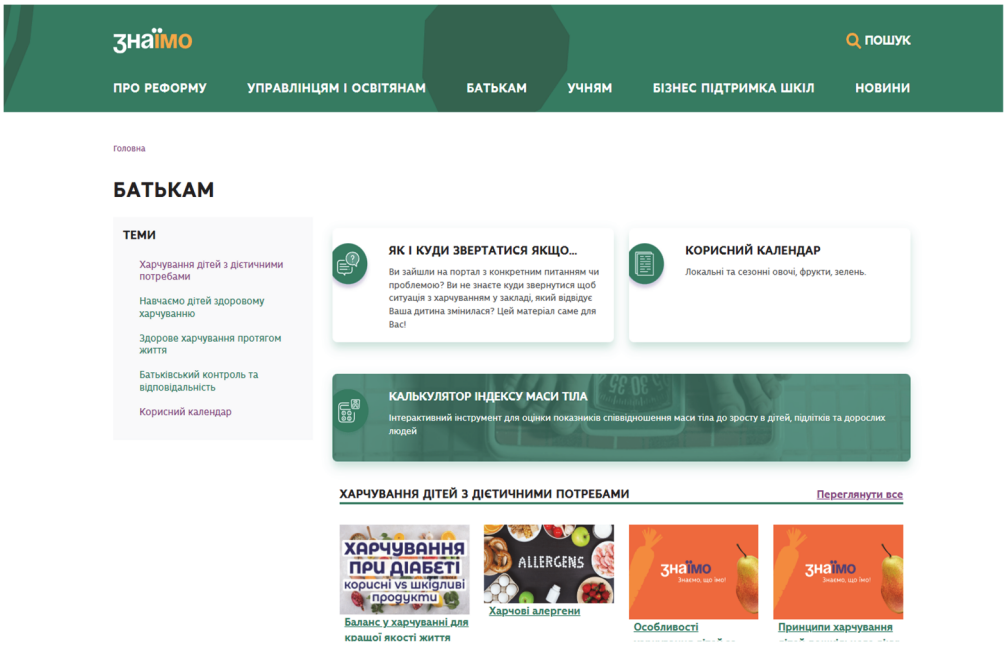


Рис. 3.8. **Інформація для батьків**

Джерело: [69].

Розділ із навчальними та інформаційними матеріалами «Учням» стане в нагоді учням та педагогам. Матеріали розділу допомагають учням більше дізнаватись про здорове харчування, вивчаючи різні предмети у школі (рис. 3.9).

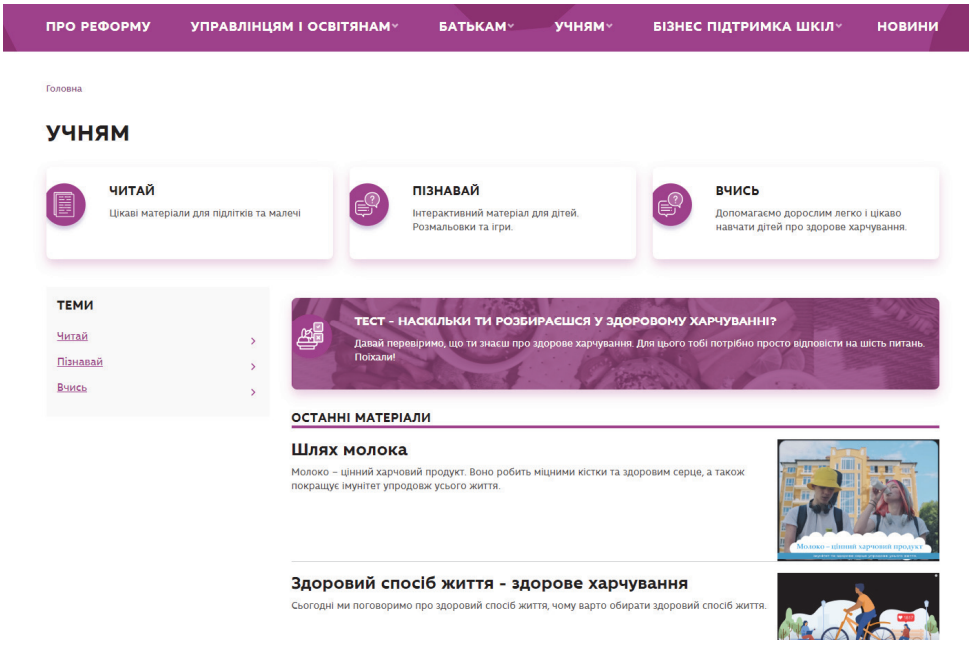


Рис. 3.9. **Інформація для учнів**

Джерело: [69].

Крім того, у відповідному розділі платформи «Бізнес підтримка шкіл» розміщено матеріали, які допоможуть бізнесу зрозуміти доцільність і переваги допомоги школам, що змінюють систему харчування (рис. 3.10).

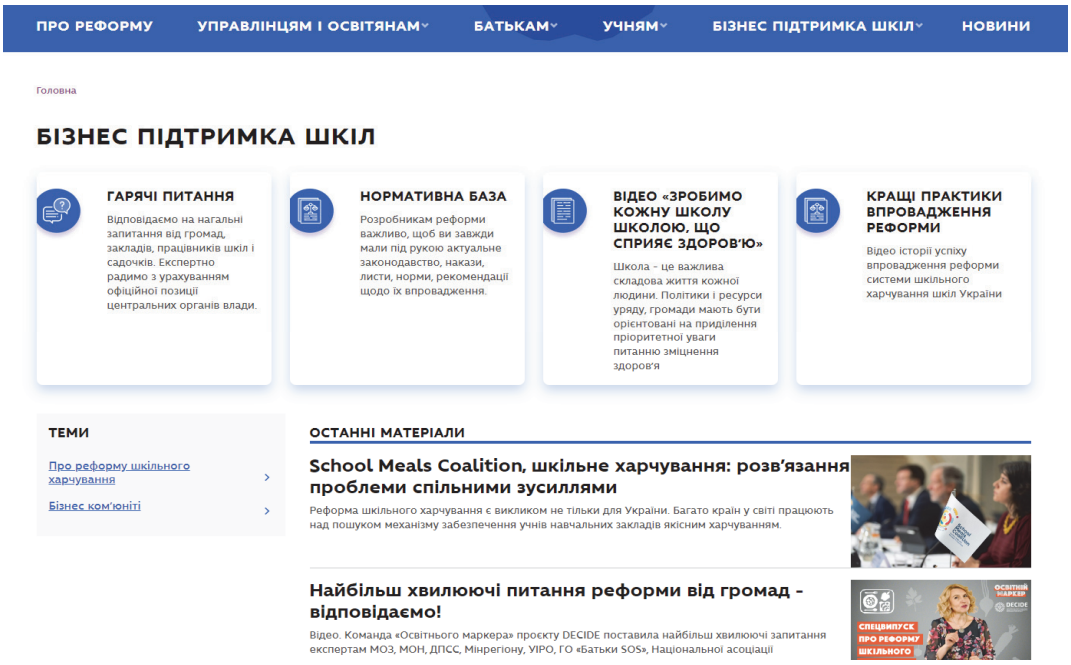


Рис. 3.10. **Бізнес підтримка шкіл**

Джерело: [69].

Наразі інформація на порталі регулярно оновлюється і доповнюється новими матеріалами. Портал є засобом комунікації та збірником напрацювань реформи, який містить доступну інформацію для всіх зацікавлених категорій з будь-яким рівнем обізнаності що до здорового харчування.

Платформа «Знаймо» є результатом міжсекторальної співпраці державних інституцій України, міжнародних організацій, громадських об'єднань та приватного сектору в межах реалізації реформи системи шкільного харчування. Розроблення платформи здійснювалося за участю Міністерства освіти і науки України, Міністерства охорони здоров'я України, Міністерства економіки України, Державної служби України з питань безпечності харчових продуктів та захисту споживачів, експертів з підтримки реформ при МОН, а також Центру громадського здоров'я України.

Ініціатива реалізована за підтримки Дитячого фонду ООН (ЮНІСЕФ) в Україні, швейцарсько-українського проєкту DECIDE («Децентралізація для

розвитку демократичної освіти»), який упроваджується консорціумом громадської організації DOCCU («Розвиток громадянських компетентностей в Україні») та Цюрихського педагогічного університету (PH Zurich, Швейцарія), а також українсько-швейцарського проєкту «Діємо для здоров'я» («Скорочення поширеності факторів ризику неінфекційних захворювань в Україні»).

Реалізацію проєкту «Діємо для здоров'я» забезпечує консорціум, до складу якого входять GFA Consulting Group, Женевські університетські клініки (Hôpitaux Universitaires de Genève), Благодійний фонд «Здоров'я жінки і планування сім'ї» та компанія One Health за підтримки Швейцарської Конфедерації. У розробленні платформи також брали участь Асоціація дієтологів України та команда Євгена Клопотенка.

Технічну реалізацію інформаційного ресурсу забезпечила українська IT-компанія SoftServe [70].

Складові реформи наведено на рис. 3.11.

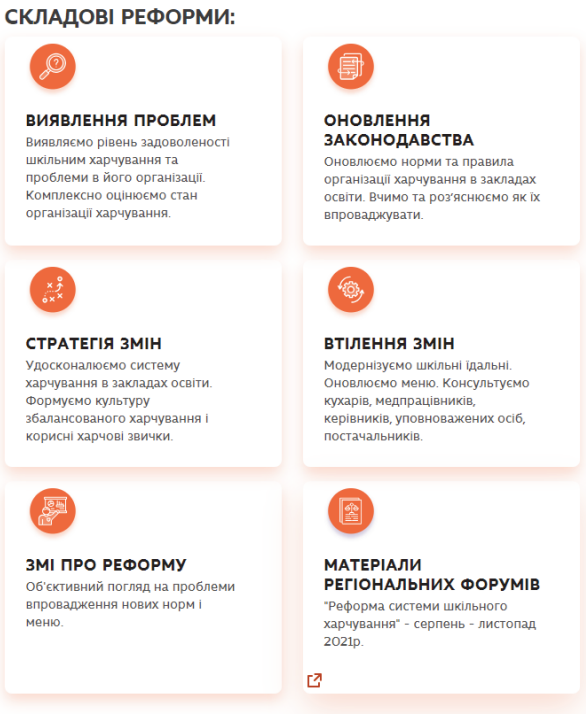


Рис. 3.11. **Складові реформи харчування**

Джерело: [69].

Починаючи із січня 2022 р., МОН здійснювало систематичний моніторинг упровадження реформи шкільного харчування. Оцінювання ефективності

реалізації відбувалося за такими показниками, як ступінь готовності оновлених меню, кількість модернізованих харчоблоків у закладах загальної середньої освіти, а також результати опитувань керівників цих закладів щодо відгуків учнів і батьків.

За підсумками проведеного моніторингу станом на 31 січня 2022 року, нове меню, розроблене в межах реформи системи шкільного харчування, було впроваджено у 13 403 закладах загальної середньої освіти України, що становить 96,6 % від їх загальної кількості [71].

На жаль, широкомасштабна збройна агресія рф проти України загальмувала реформу харчування у закладах загальної середньої освіти.

У 2023 р., після прийняття рішення про продовження реформи шкільного харчування, важливим кроком стала розробка Стратегії реформування системи шкільного харчування, що охоплювала б не тільки нові вимоги до харчоблоків, а й надавала інструменти для вирішення організаційних проблем та ключових напрямків, що потребують уваги [72]. Стратегія визначає поетапний план реалізації реформи шкільного харчування на період 2023-2027 рр. та розділена на 2 етапи: 2023-2024 рр. та 2025-2027 рр.

У лютому 2023 р. була проведена робоча нарада «Реформа шкільного харчування: пріоритетні напрямки розвитку в умовах війни та повоєнного відновлення України», на якій було вперше презентовано Стратегію реформування системи шкільного харчування на 2023-2027 р. 27.10.2023 доопрацьована Стратегія була схвалена розпорядженням Кабінету Міністрів України [73]. Вона містить план впровадження реформи та конкретні завдання як для реалізації реформи на центральному рівні, так і на регіональному. Основний акцент Стратегії спрямовано на забезпечення доступності всіх школярів до якісного здорового харчування, показниками досягнення цілі визначено: зниження відсотка ожиріння серед дітей; рівень задоволеності дітей харчуванням у школі; зміна раціону школярів на більш здоровий; збільшення відсотку учнів, що харчуються у закладах освіти, відсоток модернізованих або відновлених харчоблоків шкіл.

Документ містить стратегічні цілі, в рамках поставленої мети, що розділені на конкретні операційні кроки за чотирма напрямками: фінансове забезпечення закупівель харчових продуктів; відбудова та модернізація харчоблоків з можливістю організувати технологічні процеси відповідно до вимог системи НАССР; забезпечення кваліфікованим персоналом шкільних харчоблоків; підвищення обізнаності школярів що до здорового харчування та зміна харчових уподобань.

Для оцінки досягнень першого етапу реформи шкільного харчування, що проходив у 2023–2024 рр. було проаналізовано встановлені Стратегією цілі та заходи, що були виконані за цей період. Результати наведені у табл. 3.3.

Таблиця 3.3

Цілі та заходи, що були виконані на першому етапі реформи шкільного харчування (2023–2024 рр.)

Стратегічна ціль 1. Достатність фінансового ресурсу у замовників для закупівель харчових продуктів чи послуг з організації харчування та здійснення закупівель просто та ефективно	
Операційна ціль 1. Забезпечення достатнього фінансування для якісних закупівель	
Заплановані заходи	Реалізовані заходи
1. Комунікація з представниками місцевого самоврядування щодо особливостей і вимог до забезпечення харчування в закладах освіти.	3 партнерські зустрічі та 19 регіональних форумів з представниками Обласних військових адміністрацій (ОВА) з метою обміну досвідом та демонстрації вдалих напрацювань, розробка регіональних Стратегій реформи.
2. Установлення нижньої межі вартості харчування на одну дитину.	Встановлено ціну вартості одноразового харчування для учнів 1–4 класів у 2024 році на рівні 50 грн на день.
3. Сприяння залученню коштів до місцевих бюджетів у вигляді субвенції з державного бюджету для забезпечення харчування в закладах освіти дітей пільгових категорій.	Організовано фінансування 1-но разового гарячого харчування для всіх учнів початкових класів за рахунок державної субвенції з 2024–2025 н. р.
4. Розгляд питання щодо можливості розширення переліку категорій дітей, що забезпечуються безоплатним харчуванням у закладах освіти.	Проведення зустрічі для зацікавлених сторін що до обговорення аналітичної довідки ВООЗ «Розширення національної програми шкільного харчування в Україні». Особливо підкреслено важливіть організації забезпечення безоплатним харчуванням усіх учнів. З жовтня 2024 року всі учні 1–4 класів були забезпечені одноразовим безкоштовним харчуванням за рахунок субвенції.
5. Сприяння залученню додаткових інвестицій, спрямованих на покращення харчування в закладах освіти.	Підписання Меморандуму про взаєморозуміння та співпрацю між Всесвітньою продовольчою організацією (ВПП) та МОН щодо впровадження реформи шкільного харчування. Фінансування ВПП 30 % вартості харчування учнів початкової школи у 15 областях.

Операційна ціль 2. Зрозумілість і доступність процедури закупівель для замовників, а також механізмів впливу на постачальників харчових продуктів/послуг харчування	
6. Внесення змін до примірної тендерної документації та примірних договорів.	Перенесено на 2 етап.
7. Здійснення підвищення кваліфікації закупівельників.	Проведено вебінар для постачальників та виробників харчових продуктів «Як стати постачальником продуктів харчування для фабрики-кухні в Бучі: Прозорість закупівель в межах реформи шкільного харчування».
8. Забезпечення розвитку електронного каталогу «Prozorro Market».	23.08.2024 р. Була проведена нарада що вдосконалення роботи «Prozorro Market».
Операційна ціль 3. Заінтересованість підприємств та підприємців у роботі із закладами освіти	
9. Популяризація електронного каталогу «Prozorro Market».	13.09.2024 р. проведена нарада що до державно-приватного партнерства з метою залучення бізнесів до співпраці через «Prozorro Market». 30.09.2024 р. проведеня форуму «Prozorro Market: win-win для держави на бізнесу».
Стратегічна ціль 2. Відновлення та модернізація харчоблоків закладів освіти з використанням новітніх технологічних процесів, покращення показників енергоефективності та дотримання принципів системи аналізу небезпечних факторів та контролю у критичних точках (HACCP)	
Операційна ціль 1. Завдяки відновленій та модернізованій мережі харчоблоків закладів освіти із застосуванням трьох технологічних моделей забезпечення учнів повноцінним, безпечним та різноманітним харчуванням (та інших груп населення за потреби та можливості)	
10. Визначення потреб закладів освіти, зокрема щодо модернізації харчоблоків, що дасть змогу передбачити пріоритетність проектів.	Проведення аудитів 30 ЗЗСО та 44 ЗДО у м. Чернігові з метою визначення основних пріоритетних напрямків оптимізації системи харчування. Створення Дашборду потреб територіальних громад.
11. Встановлення нормативних вимог до проектування приміщень харчоблоків закладів освіти.	Затвердження Наказом ДП «УкрНДНЦ» № 98 від 25.03.2024 «Настанови з проєктування при будівництві приміщень харчоблоків закладів дошкільної та загальної середньої освіти, дитячих закладів оздоровлення та відпочинку відповідно до моделей організації харчування».
12. Оновлення посібника для проектувальників та архітекторів (рекомендації для комплексної модернізації та технологічного переоснащення харчоблоку закладу загальної середньої освіти, в основі яких лежить сучасний технологічний процес, що забезпечує дотримання норм на принципах системи HACCP, та приготування якісної та безпечної їжі в асортименті).	Восени 2023 р. оприлюднено розроблені «Українським інститутом розвитку освіти» «Методичні рекомендації щодо облаштування харчоблоків у закладах загальної середньої освіти».
13. Забезпечення спрямування коштів державного, місцевих бюджетів і коштів, залучених від донорських організацій, на відновлення та розвиток освітньої інфраструктури.	Реалізація проекту з побудови фабрик-кухонь «Готуїмо» м. Буча Київської та м. Лозова Харківської областей завдяки фінансуванню Говарда Г. Баффета. Організація інформаційних зустрічей та воркшопів з представниками громад щодо розподілу субвенцій на ремонт, будівництво і модернізацію харчоблоків. Виділення коштів з державного бюджету на реконструкцію та побудову харчоблоків.

14. Впровадження проектів з будівництва/ відновлення/модернізації харчоблоків у закладах загальної середньої освіти, в основі яких лежить сучасний технологічний процес, що забезпечує дотримання норм на принципах системи НАССР, та приготування якісної та безпечної їжі в асортименті.	Створеня фабрики-кухні у м. Буча Київської області, м. Лозова Харківської області, Проведення конкурсу проєктів реконструкції та будівництва шкільних харчоблоків за кошти державної субвенції.
Операційна ціль 2. Спроможність закладів освіти впровадити та підтримувати дієву систему НАССР	
15. Визначення цільових груп для комунікації та сприяння проведенню спільної інформаційно-комунікаційної кампанії.	Організація підвищення кваліфікації кухарів системи шкільного харчування з метою створення групи «агентів змін» для поширення знань про безпеку харчування. Проведення тренінгу «Організація якісного та безпечного харчування в закладах освіти».
16. Забезпечення системності та регулярності підвищення кваліфікації, оновлення знань.	Створення онлайн-курсів базового «Практичні аспекти виконання закладами освіти вимог харчового законодавства» та поглибленого «Впровадження у харчоблоках закладів освіти процедур, заснованих на принципах НАССР» рівня.
17. Створення умов для перевірки знань, зокрема з використанням тестування на онлайн-платформах.	Не реалізовано.
Стратегічна ціль 3. Забезпечення органів місцевого самоврядування і закладів освіти достатнім штатом кваліфікованих працівників, які якісно та безпечно організовують харчування і сприяють формуванню в учнів здорових харчових звичок	
Операційна ціль 1. Забезпечення закладів освіти мотивованими та професійними медичними працівниками та працівниками харчоблоків	
18. Перегляд умов оплати праці працівників харчоблоків і сестер медичних у закладах освіти.	Затвержено Постанову КМУ «Деякі питання оплати праці працівників державних та комунальних закладів охорони здоров'я».
19. Перегляд типових штатних нормативів щодо працівників, які забезпечують організацію харчування в закладах освіти (зокрема щодо сестер медичних з дієтичного харчування).	Перегляд Наказу МОН № 1205 від 06.12.2019 р. «Про затвердження Типових штатних нормативів закладів загальної середньої освіти». Наказ МОН № 1414 від 02.10.2024 р. та № 1487 від 22.10.2024 р.
20. Забезпечення підготовки/підвищення кваліфікації кухарів через відповідні регіональні та/або місцеві програми.	Побудова та розширення мережі кулінарних хабів для навчання, перекваліфікації та підвищення кваліфікації кухарів.
21. Підготовка кухарів за новими програмами в закладах професійної (професійно-технічної) освіти (ЗП(ПТ)О).	Створення кулінарних 3 хабів на базі ЗП(ПТ)О.
22. Розроблення професійного стандарту освіти за професією «Кухар закладу освіти».	Внесення в реєстр класифікацій професійного стандарту «Кухар закладу освіти» у березні 2024 р.
23. Затвердження програм з підвищення кваліфікації з питання щодо реформування системи шкільного харчування, розроблення нових навчальних матеріалів та оновлення існуючих.	14 травня 2024 р. затверджено Типову освітню програму підвищення кваліфікації керівників закладів освіти за напрямом «Впровадження реформи шкільного харчування»
24. Розвиток навчально-практичних центрів, що здійснюють підготовку кухарів, а також створення мережі центрів підвищення кваліфікації кухарів на базі ЗП(ПТ)О.	Створено навчально-практичні центри для підготовки кухарів системи шкільного харчування. На кінець 2024 р. створено 11 кулінарних хабів в різних областях, 3 з яких засновано на базі ЗП(ПТ)О.

25. Інформування про переваги співпраці органів місцевого самоврядування із ЗП(ПТ)О з питань перепідготовки кухарів.	Висвітленя позитивних прикладів співпраці місцевої влади і ЗП(ПТ)О.
Операційна ціль 2. Набуття педагогічними працівниками та керівниками закладів освіти, науково-педагогічними працівниками інститутів післядипломної освіти відповідних компетентностей і сприяння формуванню навичок здорового харчування учнів та їх батьків	
26. Навчання працівників закладів освіти, залучених до підвищення кваліфікації вчителів (здоров'язбережувальна галузь).	Проведення онлайн-навчання «Сучасні підходи та виклики в організації шкільного харчування».
27. Оновлення програм підвищення кваліфікації педагогічних працівників (здоров'язбережувальна галузь) закладів освіти.	Полтавською академією неперервної освіти ім. М. В. Остроградського розроблено та введено в дію освітню програму підвищення кваліфікації «Розвиток професійних компетентностей учителів інтегрованих курсів соціальної і здоров'язбережувальної освітньої галузі»
28. Навчання керівників закладів освіти організації харчування та формування навичок здорового харчування в закладах освіти.	Проведення онлайн-курсів базового «Практичні аспекти виконання закладами освіти вимог харчового законодавства» та поглибленого «Впровадження у харчоблоках закладів освіти процедур, заснованих на принципах HACCP» рівня. 29 серпня 2024 р. проведено онлайн-вебінар «Особливості організації харчування в укриттях, розташованих у закладах освіти»
Операційна ціль 3. Ефективне впровадження органами місцевого самоврядування реформи системи шкільного харчування	
29. Забезпечення надання консультацій і роз'яснень щодо впровадження реформи системи шкільного харчування посадовим особам місцевого самоврядування та депутатам місцевих рад.	Проведення онлайн-семінару «Організація шкільного харчування у країнах Європи», організовано та проведено вебінари та тренінги з питань ввпровадження реформи з представниками громад та депутатами місцевої влади.
30. Розгляд питання щодо можливості введення посади технолога громадського харчування у структурному підрозділі з питань освіти виконавчого органу сільської, селищної, міської ради/закладі освіти та сприяння розвитку надання відповідних послуг.	Перенесено на 2 етап.
31. Створення цифрових інструментів для зниження бюрократичного навантаження на посадових осіб місцевого самоврядування, до компетенції яких належать питання організації харчування у закладах освіти, і працівників закладів освіти щодо впровадження реформи системи шкільного харчування (зокрема щодо формування меню та аналізу його дотримання, потреб у закупівлях).	Створено Порадники для посадових осіб з питань закупівель та впровадження системи HACCP.
Стратегічна ціль 4. Свідоме обрання українцями здорового харчування	
Операційна ціль 1. Повноцінне, збалансоване харчування учнів у закладах освіти, яке відповідає затвердженим нормам	
32. Затвердження примірних чотиритижневих сезонних меню для закладів освіти.	Про затвердження рекомендованого Примірного чотиритижневого сезонного меню, рекомендованого для організації одноразового харчування дітей віком від 6 до 18 років в закладах освіти та інших організованих дитячих колективах

	на осінній період Наказом № 243 Міністерства охорони здоров'я.
33. Розширення переліку страв і технологічних карток (рецептури) для харчування в закладах освіти.	Розробка та презентація оновленого збірника рекомендованих рецептур для харчування дітей у закладах освіти.
34. Розроблення рекомендацій і нормативно-правових актів щодо організації харчування в закладах освіти на період воєнного стану.	Прийняття постанови КМУ «Про внесення змін до постанови КМУ від 24.03.2021 р. № 305». (Про затвердження норм та Порядку організації харчування у закладах освіти та дитячих закладах оздоровлення та відпочинку»).
35. Забезпечення організації харчування в закладах освіти органами місцевого самоврядування.	На селекторній нараді 14.06.2024 р. було обговорено подальший розвиток реформи та перехід її реалізації на рівень областей та громад. Розробка втілення регіональних програм.
Операційна ціль 2. Сприяння свідомому вибору здорового харчування через освіту	
36. Підготовка та поширення дидактичних та освітніх матеріалів про принципи здорового харчування та збереження фізичного здоров'я.	Організовано комунікаційну кампанію для популяризації здорового харчування черех диджитал-канали. Охоплення 2 095 557 людей. Проведено комунікаційну кампанію «Головне – що всередині», до якої долучилося 7 591 000 людей. Розробка інформаційних банерів на тему здорового харчування для розміщення в укриттях навчальних закладів.
37. Підготовка та поширення матеріалів про вплив здорового харчування на покращення психологічного стану.	Проведення дослідження що до впровадження комплексної національної програми шкільного харчування. У висновках підкреслено переваги для фізичного та психічного здоров'я.
38. Формування в освітньому середовищі інформаційного поля для розуміння навичок здорового харчування та збереження здоров'я шляхом застосування нових форм передачі знань (навчальні візити, майстер-класи, дегустації тощо).	Запущено онлайн-курс «Основи здорового харчування для учнів 1–4 класів». На червень 2024 року, його пройшли 4 553 вчителя. Забезпечення вчителів 774 інтерактивними ігровими наборами для проведення уроків, розрахованих на 23 220 школярів.
Операційна ціль 3. Доступність та зрозумілість інформації про здорове харчування	
39. Розвиток функціоналу та поширення інформації про веб-портал «ЗнаЇмо».	На червень 2024 року зафіксовано 510 519 користувачів платформи. Розроблено інформаційні матеріали, відео-інструкції.
40. Залучення лідерів думок, «спікерів реформи» до підвищення рівня поінформованості про зміни.	О. Зеленська, Є. Клопотенко, О. Степанюк, В. Полторак, В. Ляшко, та ін. «спікери реформи» активно долучені до процесу реформування на кожному етапі. На кінець 2024 р. TikTok-канал про здорове харчування HRAIMO охопив 1 750 000 користувачів. Запущено подкаст Cult [Food] про здорове харчування.

Складено авторами за: [74–76].

Аналіз виконання операційного плану Стратегії реформування системи шкільного харчування на 2023–2024 рр. засвідчує, що реалізація першого етапу відбувалася системно та охопила всі чотири стратегічні напрями: фінансове

забезпечення, модернізацію харчоблоків, кадровий розвиток і формування культури здорового харчування. Попри складні умови воєнного стану, більшість запланованих заходів було виконано або розпочато, що свідчить про дієвість міжвідомчої координації та партнерських механізмів управління реформою.

У сфері фінансового забезпечення досягнуто значного результату. Вперше на державному рівні встановлено мінімальну вартість одноразового харчування для учнів початкової школи – 50 грн на день, що стало орієнтиром для формування місцевих бюджетів. Запроваджено державну субвенцію, яка з 2024/2025 н. р. гарантує безоплатне гаряче харчування всім учням 1–4 класів. У межах міжнародної співпраці підписано Меморандум між Міністерством освіти і науки України та ВПП, що передбачає співфінансування вартості харчування у 15 областях. Водночас частину технічних завдань, зокрема оновлення тендерної документації та спрощення закупівельних процедур, перенесено на другий етап (2025–2027 рр.).

У напрямі модернізації матеріально-технічної бази створено нормативну основу для відновлення і будівництва харчоблоків. Розроблено нові настанови з проєктування приміщень закладів освіти, оновлено методичні рекомендації щодо оснащення харчоблоків відповідно до принципів системи HACCP. Проведено аудит потреб закладів освіти, створено електронний дашборд для моніторингу потреб громад. Практичним результатом стала реалізація пілотних проєктів фабрик-кухонь у містах Буча (Київська обл.) та Лозова (Харківська обл.), які стали прикладом сучасної моделі організації шкільного харчування.

Кадровий блок реформи зосередився на формуванні професійного потенціалу системи. Затверджено професійний стандарт «Кухар закладу освіти», оновлено типові штатні нормативи та умови оплати праці працівників харчоблоків. Розбудовується мережа кулінарних хабів і навчально-практичних центрів – станом на кінець 2024 р. їх функціонувало 11 у різних регіонах, три з них – на базі ЗП(ПТ)О. Відпрацьовано нові програми підвищення кваліфікації кухарів і керівників закладів освіти, що охоплюють питання впровадження

системи HACCP, здорового харчування та організації освітнього процесу під час воєнного стану.

Особливу увагу приділено формуванню культури здорового харчування серед дітей, батьків і педагогів. У межах просвітницької роботи проведено масштабні комунікаційні кампанії «Головне – що всередині» та інформаційні заходи у співпраці з лідерами думок і медіа. Запущено освітні онлайн-курси з основ здорового харчування для вчителів початкової школи, підготовлено інтерактивні матеріали та дидактичні набори для проведення тематичних занять. Важливим досягненням став розвиток інформаційної платформи «ЗнаЇмо», яка стала основним ресурсом реформи. Станом на червень 2024 р. портал нараховував понад 510 тис. користувачів, забезпечував доступ до навчальних матеріалів, нормативної бази та інструкцій для освітян.

Проте, не всі задачі операційного плану виконано у повній мірі. Під час дослідження виявлено наступні перепони на шлюху до повної реалізації плану заходів:

– воєнний стан і безпекові обмеження;

– фінансова неспроможність окремих територіальних громад попри запровадження державних субвенцій;

– недостатня узгодженість нормативно-правових актів, зокрема типові договори закупівель, тендерна документація та рекомендації для органів місцевого самоврядування, перебувають у процесі оновлення;

– кадровий дефіцит та низький рівень професійної підготовки персоналу;

– нерівномірність технічної модернізації шкіл;

– низький рівень поінформованості та мотивації на місцевому рівні;

– обмежена цифровізація управлінських процесів: відсутність єдиних цифрових інструментів для планування меню, обліку закупівель;

– супротив частини батьків і учнів новим підходам.

У підсумку, перший етап реформи продемонстрував ефективність державного управління у складних умовах, налагоджену взаємодію центральних і місцевих органів влади, міжнародних організацій та громадського сектору.

Закладено нормативно-правову, фінансову та кадрову основу для продовження реформи у 2025–2027 рр. На наступному етапі пріоритетами залишаються подальша діджиталізація процесів, повна модернізація харчоблоків у громадах і розширення програм з формування здорових харчових звичок.

Допоміжним засобом на шляху до виконання поставлених завдань, стала платформа «Знаїмо», що накопичує та акумулює новини, досягнення, створені у процесі реформи навчальні матеріали.

3.4. Аналіз ефективності функціонування платформи дистанційної освіти «Всеукраїнська школа онлайн»

Пандемія COVID-19 стала рушійною силою глибокого переосмислення освітніх практик в Україні та світі. У 2020 р., коли були введені карантинні обмеження, сотні школярі всього світу опинилися без фізичного доступу до класів, а організація дистанційного навчання стала нагальною необхідністю. Багато учнів не мали альтернативи – вони залишились вдома, не маючи можливості отримувати освіту, що стимулювало держави шукати рішення для забезпечення безперервності освіти.

У дуже короткий термін вчителям та учням довелося опановувати цифрові навички, що супроводжувалося рядом труднощів: втомою від постійного перебування перед екранами моніторів, неможливістю отримувати повноцінне навчання учнями, що не мали технічного забезпечення, втрата інтересу до навчання учнів, що не мали навичок самостійного навчання поза колективом.

У 2020 р. Міжнародна комісія ЮНЕСКО щодо майбутнього освіти (International Commission on the Futures of Education) опублікувала звіт «Освіта у світі після COVID: Дев’ять ідей для суспільних дій», він окреслює 9 пріоритетних напрямків для розвитку освіти у майбутньому, враховуючи досвід пандемії. Ці 9 ідей, описані комісією для використання у державних політиках,

соціальних дискусіях, включення до пріоритетних напрямків розвитку освітньої сфери з метою підвищення доступності освіти в будь-яких умовах.

Одним з запропонованих напрямків є: надання педагогам та учням вільного доступу до технологій з відкритим вихідним кодом. Надавати підтримку розробці відкритих освітніх ресурсів і цифрових інструментів. Автори наголошують, що освіта має бути доступна всім і не може бути залежна ні від обставин, відсутності фізичного доступу до навчальних закладів, ні від приватних комерційних освітніх рішень.

Автори закликають до глобальної співпраці між державами, благодійними та некомерційними організаціями з метою розробки та популяризації відкритих освітніх ресурсів, платформ, але наголошують, що саме держава має взяти на себе ключову роль з надання освітніх послуг у цифровому форматі для забезпечення збереження визначених державою напрямків розвитку учнів [77].

Також, у 2020 р., глобальна коаліція ЮНЕСКО з питань освіти (UNESCO Global Education Coalition) опублікувала Стратегію дистанційного навчання як ключовий елемент забезпечення безперервності освіти. В стратегії, насамперед, визначено різні засоби для організації дистанційного навчання, що можуть використовуватись окремо або комплексно, в залежності від рівня цифрових навичок. Серед запропонованих засобів, зокрема, представлені: пошта та адресна розсилка, телебачення/радіо, електронна пошта або текстові повідомлення, інтернет платформи, адаптоване програмне забезпечення, відеоконференції. Також, документ містить поради що до організації дистанційного навчання, заходи для адаптації вчителів, учнів та їх родин [78].

Ці рекомендації дали поштовх розвитку цифрових навчальних інструментів у всьому світі, а використання інтернету та веб ресурсів стало частиною засобів навчання. Саме тому, важливою темою є створення освітніх ресурсів, що містять достовірні та актуальні матеріали, схвалені державою.

Використання олайн засобів навчання стало рятівним рішенням для світу у часи пандемії. Цей досвід спонукав державні системи освіти знаходити оптимальні рішення що до організації онлайн та гібридного режиму навчання.

Для України таким рішенням став телевізійний проєкт ВШО, який трансформувався у національну освітню платформу. Платформа стала дієвим заходом для організації онлайн навчання не тільки під час карантинних обмежень і з початком повномасштабного вторгнення. Завдяки цьому рішенню, школярі можуть продовжувати навчання в умовах відсутності можливості фізичного відвідування шкіл, що забезпечує безперервність навчання протягом життя.

Проблема безперервності навчання, у зв'язку з військовими діями, залишається актуальною для учнів України, саме тому ВШО залишається дієвим засобом забезпечення доступу до знань.

ВШО є державною вебплатформою дистанційного та змішаного навчання, створеною з метою забезпечення рівного, вільного і безоплатного доступу здобувачів загальної середньої освіти до якісних освітніх матеріалів, а також методичної підтримки педагогічних працівників у процесі організації освітнього процесу в цифровому середовищі [79].

Запровадження платформи у 2020 р. відбулося в умовах поширення пандемії COVID-19 та стало відповіддю держави на потребу швидкого переходу системи освіти до дистанційного формату. Водночас створення ВШО не обмежувалося ситуативним реагуванням на кризові обставини, а відповідало стратегічному курсу цифрової трансформації освіти та необхідності забезпечення сталості освітнього процесу незалежно від зовнішніх чинників.

Особливої актуальності функціонування ВШО набуло в умовах воєнного стану. Платформа фактично стала одним із ключових інструментів забезпечення доступу до української загальної середньої освіти для учнів, які перебувають за межами країни, проживають на тимчасово окупованих територіях або навчаються в умовах обмеженої фізичної доступності закладів освіти. Важливою перевагою платформи є наявність навчального контенту українською мовою, який відповідає державним освітнім стандартам.

Для розширення можливостей користування ВШО функціонує мобільний застосунок, що забезпечує доступ до всіх навчальних курсів і матеріалів

платформи, участь у навчальних активностях та комунікацію між учасниками освітнього процесу. Це сприяє підвищенню гнучкості навчання та адаптації освітнього процесу до різних умов і технічних можливостей користувачів.

Платформа забезпечує учнів комплексним навчальним контентом, що включає відеоуроки, текстові конспекти, тестові завдання для перевірки знань, а також інструменти для відстеження індивідуального навчального прогресу. Для педагогічних працівників передбачено методичні рекомендації та приклади використання матеріалів ВШО в умовах дистанційного і змішаного навчання (рис. 3.12).

Рис. 3.12. **Перелік навчальних курсів ВШО**

Джерело: [79].

Станом на поточний період платформа містить відеоуроки, тести і матеріали для самостійної роботи з 18 базових навчальних предметів для учнів 2–11 класів, зокрема з української мови та літератури, математики, природничих дисциплін, історії та іноземних мов. ВШО може використовуватися як основний інструмент дистанційного навчання, так і як допоміжний ресурс для надолуження навчальних втрат або самостійного опрацювання окремих тем.

За даними Міністерства освіти і науки України, кожен п’ятий учитель-предметник користується матеріалами ВШО. Загальна кількість зареєстрованих користувачів платформи становить понад 422 тис. осіб, включаючи мешканців тимчасово окупованих територій. Загалом ВШО використовується у 119 країнах світу, що свідчить про її значний транснаціональний освітній потенціал.

Нормативно-правове забезпечення функціонування ВШО здійснюється відповідно до Положення про вебплатформу дистанційного навчання «Всеукраїнська школа онлайн», затвердженого наказом МОН від 16.06.2023 № 746 [80]. Документ визначає цілі, завдання та функціональні можливості платформи, порядок експертизи освітніх матеріалів, а також механізми захисту інформації й персональних даних користувачів.

Також Положення визначає основними завданнями Платформи, серед яких:

1) забезпечення учасників освітнього процесу вільним онлайн доступом до освітніх матеріалів, зокрема для організації навчання в різних формах;

2) забезпечення методичної підтримки педагогічних працівників під час здійснення освітнього процесу та можливості їх професійного розвитку засобами Платформи;

3) забезпечення можливості вимірювання та надолуження прогалин у знаннях здобувачів освіти засобами Платформи;

4) захист даних (у тому числі персональних), що розміщуються на Платформі, від несанкціонованого доступу, знищення, модифікації;

5) інші завдання, визначені законодавством.

Відповідно до основних завдань Платформа має такі функціональні можливості:

1) створення, розміщення та оприлюднення освітніх матеріалів;

2) створення та використання особистих електронних кабінетів користувачів після реєстрації та авторизації за допомогою особистих ідентифікаторів доступу до електронного кабінету користувача (логіна та паролю);

3) зміна даних у особистому електронному кабінеті користувача, зокрема даних про прізвище, ім’я, по батькові (за наявності);

4) надання всім чи окремим користувачам доступу до освітніх матеріалів;

5) забезпечення можливості перевірки/самоперевірки отриманих знань після використання користувачем освітніх матеріалів;

6) забезпечення можливості вимірювання та надолуження прогалин у знаннях здобувачів освіти;

7) забезпечення можливості здійснення експертизи освітніх матеріалів засобами Платформи;

8) забезпечення комунікації користувачів між собою;

9) забезпечення можливості розподілу користувачів за відповідними класами, групами;

10) застосування інтерфейсів, адаптованих для осіб із особливими освітніми потребами;

11) розміщення освітніх матеріалів державною мовою, а також іншими мовами, зокрема жестовою, відповідно до законодавства;

12) інтеграція складових Платформи до інших інформаційно-комунікаційних систем;

13) систематизація та пошук освітніх матеріалів, розміщених і оприлюднених на Платформі;

14) користування Платформою через комп’ютер, мобільний застосунок, інші електронні носії, функціональні можливості яких дають можливість використовувати Платформу;

15) оброблення інформації в режимі реального часу;

16) забезпечення трансляції аудіовізуальної інформації в режимі реального часу;

17) розмежування доступу до інформації, яка розміщена на Платформі, і забезпечення контролю за таким доступом;

18) проведення моніторингу відвідувань, реєстрації подій, що відбуваються на Платформі та стосуються її безпеки;

19) блокування несанкціонованих дій щодо захищених ресурсів і автоматичне інформування Технічного адміністратора про вчинення таких дій;

20) надання інформації та/або консультацій користувачам;

21) інші функціональні можливості, необхідні для виконання основних завдань Платформи.

З технічної точки зору ВШО функціонує як складна інформаційно-комунікаційна система, що включає основний і резервний центральні вузли, систему віртуалізації, сервери різного функціонального призначення та мережеву інфраструктуру з використанням хмарних технологій. Структурну схему інформаційно-комунікаційної системи ВШО наведено на рис. 3.13.

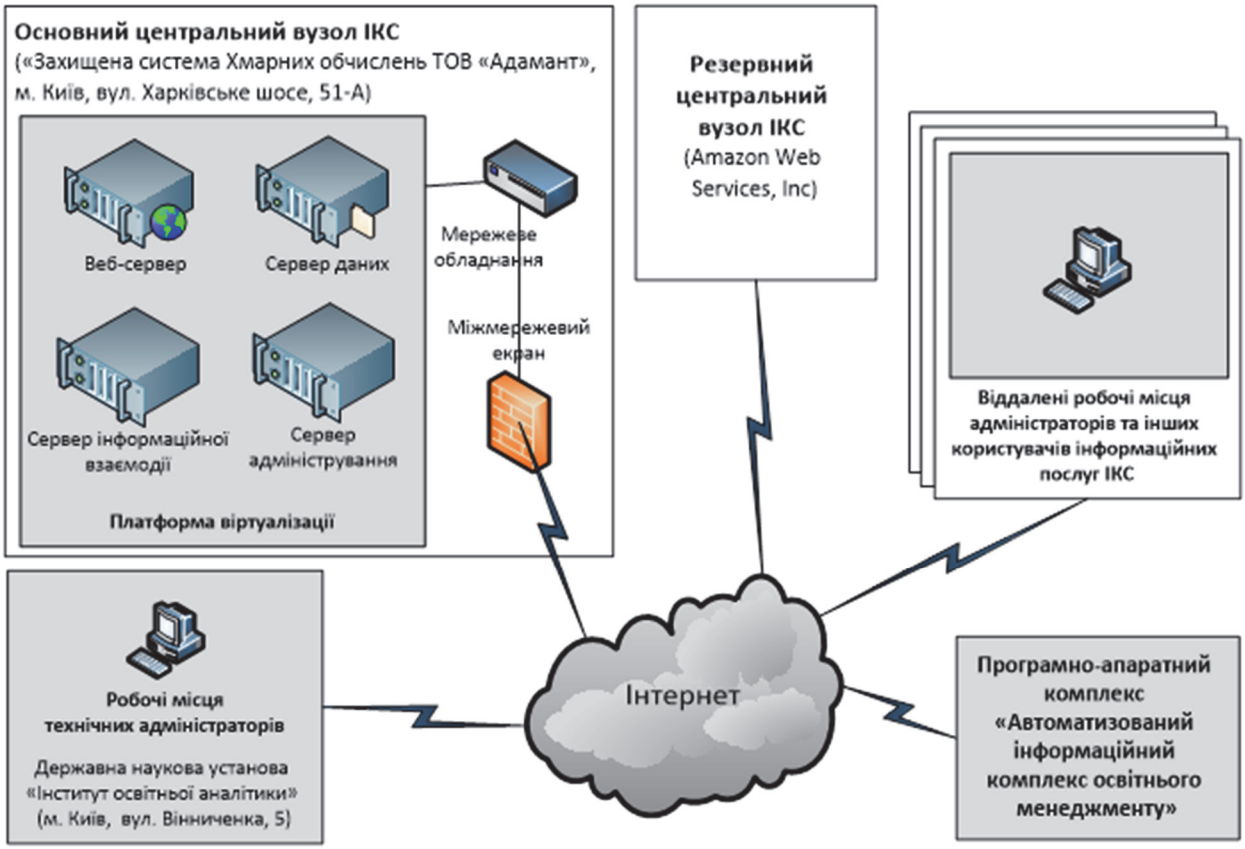


Рис. 3.13. **Структурна схема ІКС**

Побудовано авторами.

До складу основного центрального вузлу ІКС входять:

– платформа віртуалізації (надається як послуга з боку хостинг-провайдера), на якій в якості віртуальних серверів функціонують наступні сервери:

– веб-сервер;

– сервер даних;

– сервер інформаційної взаємодії;

– сервер адміністрування;

– комутаційне обладнання (в тому числі, міжмережевий екран).

Веб-сервер призначений для надання користувачам ІКС графічного інтерфейсу для виконання покладених на них функціональних обов'язків, обробки запитів та логування дій користувачів.

Сервер даних призначений для розміщення та управління інформаційними об'єктами (представлених у вигляді файлів та об'єктів баз даних), що зберігаються та обробляються в ІКС.

Сервер інформаційної взаємодії призначений для забезпечення інформаційної взаємодії з програмно-апаратним комплексом «Автоматизований інформаційний комплекс освітнього менеджменту».

Сервер адміністрування призначений для забезпечення захищеного віддаленого підключення обслуговуючого персоналу (технічних адміністраторів) з метою адміністрування прикладного програмного забезпечення, баз даних, а також іншими налаштуваннями прикладного програмного забезпечення та систем керування базами даних ВШО.

Резервний центральний вузол розгорнутий на базі обчислювальної та мережевої інфраструктури хостинг-провайдера (компанія Amazon Web Services, Inc), в межах якої розгорнуто середовище контейнеризації (Kubernetes), на якому в якості ізольованих логічних контейнерів функціонують такі контейнери прикладного програмного забезпечення ІКС.

Робочі місця технічних адміністраторів призначені для:

– централізованого управління налаштуваннями програмного та апаратного забезпечення серверного та мережевого обладнання центральних вузлів ІКС;

– управління обліковими записами обслуговуючого персоналу (на рівні системного програмного забезпечення) та користувачів (з ролями

«адміністратор», «адміністратор модулю «Додаткові матеріали», «експерт модулю «Додаткові матеріали», на рівні прикладного програмного забезпечення);

– технічних засобах ІКС, а також для перегляду протоколів подій в ІКС;

– оновлення системного, антивірусного та прикладного програмного забезпечення.

Віддалені робочі місця адміністраторів та інших користувачів інформаційних послуг ІКС призначені для адміністрування (створення, управління контентом) навчальних матеріалів та їх використання в навчальному процесі користувачами інформаційних послуг ІКС.

Віддалені робочі місця адміністраторів та інших користувачів інформаційних послуг ІКС являють собою сукупність ЕОМ, організованих у вигляді окремих автоматизованих робочих місць користувачів або у вигляді обчислювальних мереж. Припускається використання персональних ЕОМ, мобільних ЕОМ (ноутбуків), а також планшетних комп'ютерів та смартфонів.

Віддалені робочі місця адміністраторів та інших користувачів інформаційних послуг ІКС працюють в режимі «тонкого» клієнта, який не передбачає можливості зберігання будь-яких даних на таких робочих місцях. Всі дані, що обробляються в ІКС, зберігаються виключно в межах центральних вузлів та / або передаються для подальшої обробки та зберігання до програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту».

Таким чином, Всеукраїнська школа онлайн є комплексним цифровим освітнім середовищем, яке поєднує якісний навчальний контент, нормативно врегульовану організаційну модель і сучасну технічну інфраструктуру. Її функціонування забезпечує безперервність освітнього процесу в умовах кризових викликів та створює підґрунтя для подальшого розвитку дистанційної й змішаної освіти в Україні.

4. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВОЄННОГО СТАНУ ТА ЄВРОІНТЕГРАЦІЇ

4.1. Огляд наукових підходів до забезпечення інформаційної безпеки в умовах цифровізації освіти

На сучасному етапі розвитку ІКТ в світі питання кібербезпеки стають одними із ключових, зокрема й у сфері освіти, особливо в умовах поглиблення цифровізації. Цифрова трансформація освіти в Україні супроводжується активним упровадженням освітніх інформаційних систем, що акумулюють значні обсяги чутливої інформації: від особистих даних учнів та вчителів до статистичних відомостей про заклади.

Водночас, недостатній рівень захисту таких систем створює потенційні ризики витоку, зловживання або неправомірного доступу до даних, що може спричинити серйозні наслідки як на інституційному, так і на особистісному рівні. У сучасних умовах навчальний процес, управління закладами освіти та аналітика даних дедалі частіше базуються на використанні електронних платформ, інформаційно-комунікаційних систем і цифрових сервісів. Це зумовлює необхідність забезпечення належного рівня інформаційної безпеки, особливо з огляду на збереження та захист персональних даних учасників освітнього процесу.

У контексті євроінтеграції Україна бере на себе зобов’язання щодо гармонізації національного законодавства з європейськими нормами, зокрема в частині захисту персональних даних. Вимоги Загального регламенту ЄС про захист даних – General Data Protection Regulation (GDPR) актуалізують необхідність адаптації українських освітніх інформаційних систем до високих стандартів прозорості, надійності та відповідальності. Це вимагає не лише технічних рішень, а й розвитку культури цифрової грамотності та правової обізнаності у сфері захисту даних.

Тож можна стверджувати, що актуальність проведення наукових досліджень у сфері кібербезпеки та інформаційної безпеки в освітніх інформаційних системах в умовах цифрової трансформації та євроінтеграції: аспекти захисту персональних даних, обумовлена зростаючим значенням цифрових технологій у сфері освіти, а дослідження проблематики інформаційної безпеки в освітньому середовищі є надзвичайно важливим і своєчасним. Це сприятиме розумінню викликів і можливостей цифровізації освіти, а також формуванню комплексного підходу до захисту персональних даних у відповідності до сучасних європейських стандартів.

Проблематика інформаційної безпеки в освіті в умовах цифрової трансформації та євроінтеграції є предметом активних наукових досліджень, в яких висвітлюються різні аспекти цієї проблематики.

Зокрема, у статті «Інформаційна безпека цифрової трансформації» визначено особливості інформаційної безпеки в процесі цифрової трансформації та шляхи її забезпечення. Автор формулює визначення цифрової трансформації, розглядаючи її в телеологічному та діяльнісному аспектах. Наголошується на необхідності активного застосування заходів інформаційної безпеки через зростання кількості та інтенсивності інформаційних загроз у сферах, де цифрова трансформація відбувається найшвидше [81].

Вартий уваги збірник матеріалів наукової конференції Інституту цифровізації освіти НАПН України, що містить доповіді, присвячені розвитку цифрових технологій у відкритій освіті та науці. Учасники конференції описують теоретичні та практичні аспекти проєктування і використання сучасних засобів навчання в комп'ютерно орієнтованому середовищі, зокрема застосування хмарних та імерсивних технологій. Окрему увагу приділено питанням інформаційної безпеки та захисту персональних даних в умовах цифрової трансформації освітнього процесу [82].

Стаття «Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії» присвячена розробці ефективного підходу до протидії загрозам, пов’язаним із соціальною інженерією в цифровому

середовищі [83]. Так, питання інформаційної безпеки в умовах цифрової трансформації освіти набуває дедалі більшої актуальності в наукових дослідженнях. У працях наголошуються на необхідності створення безпечного інформаційного середовища для реалізації цифрових прав громадян і розвитку сучасної освітньої інфраструктури, з урахуванням новітніх технологій.

Стосовно конкретних заходів захисту в інформаційних системах, то цій проблематиці присвячено чимало публікацій українських вчених. Зокрема у збірнику тез доповідей конференції Державної наукової установи «Інститут освітньої аналітики» серед ключових тем розглядаються питання інформаційної безпеки, цифрової трансформації освітніх процесів та інтеграції в європейський освітній простір, що включає аспекти захисту персональних даних в освітніх інформаційних системах [84].

Публікація «Заходи захисту персональних даних в інформаційних системах» присвячена аналізу основних і додаткових заходів захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах [85].

Стаття «Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах» присвячена аналізу особливостей захисту персональних даних в умовах стрімкого розвитку інформаційно-телекомунікаційних технологій [86].

У роботі розглядаються актуальні загрози, пов’язані з обробкою персональної інформації, та пропонуються технічні й організаційні заходи для забезпечення її безпеки. Особлива увага приділяється впровадженню комплексних систем захисту, що враховують специфіку телекомунікаційних технологій та дотримання чинного законодавства у сфері захисту персональних даних [87].

У публікації «Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах» розглянуто питання необхідності захисту персональних даних, які створюються і обробляються прикладним програмним забезпеченням в автоматизованих системах. Авторами

запропоновано базову модель представлення параметрів ризику, які визначені на установлених законодавством критеріях у сфері забезпечення захисту персональних даних. Розроблено метод оцінки ризиків за результатами якого надаються рекомендації щодо вибору політики безпеки для захисту персональних даних, доповнення стандартного функціонального профілю захищеності необхідними послугами безпеки, визначення величини нанесеної шкоди людині, суспільству, державі у разі втрати таких персональних даних [88].

Стаття «Захист інформації в прикладних інформаційних системах» присвячена аналізу сучасних методів захисту персональних даних в інформаційних системах, зокрема в контексті мобільних платформ. У публікації розглядаються статистичні дані щодо витоків персональних даних, де зазначається, що близько 75 % випадків витоку конфіденційної інформації у 2019 році становили саме персональні дані. Автори підкреслюють важливість впровадження ефективних заходів захисту для запобігання таким інцидентам. Автори наголошують на необхідності поєднання технічних рішень та обізнаності розробників у виборі відповідних методів захисту для забезпечення безпеки персональних даних в сучасних інформаційних системах [89].

Стаття О. О. Бакаєва та Г. В. Суського присвячена аналізу та обґрунтуванню ефективності знеособлення (анонімізації) як методу захисту персональних даних в умовах сучасного цифрового середовища. Автори розробили методику та правила обробки знеособлених даних із залученням зовнішніх операторів, що дозволяє забезпечити конфіденційність інформації як на рівні оператора, так і користувача. Запропонований підхід особливо актуальний для малобюджетних організацій, які використовують дата-центри та хмарні технології, оскільки дозволяє знизити витрати на захист даних без шкоди для безпеки [90].

Тож, у сучасних українських наукових публікаціях значна увага приділяється заходам захисту персональних даних в інформаційних системах, зокрема в контексті цифровізації освітнього простору, розвитку телекомунікаційних технологій та підвищення кіберзагроз. Дослідники

аналізують як загальні принципи і моделі захисту, так і практичні методи. Окрему увагу приділено впровадженню комплексних систем безпеки та адаптації підходів до умов роботи хмарних технологій.

У контексті євроінтеграції України, огляд сучасних досліджень засвідчує зростаючу увагу до питань інформаційної безпеки в умовах цифрової трансформації освіти, зокрема в аспектах захисту персональних даних, гармонізації з європейськими стандартами (зокрема Загальному регламенту захисту даних ЄС (GDPR) та розвитку цифрової компетентності.

Так, стаття Легкої О. В. присвячена розгляду позитивного міжнародного досвіду щодо законотворчої діяльності з питань захисту персональних даних. Проаналізовано основні норми міжнародних та вітчизняних нормативно-правових документів, які регулюють питання захисту персональних даних. Досліджено основні нововведення Загального регламенту про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (GDPR), положення про екстратериторіальність дії GDPR у контексті можливості його застосування щодо фізичних та юридичних осіб України. Надано пропозиції щодо основних шляхів адаптації вітчизняного законодавства про захист персональних даних до міжнародних стандартів [91].

Стаття «Нормативні вимоги України в сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах у порівнянні з вимогами США та ЄС» присвячена аналізу та порівнянню нормативно-правових актів, що регулюють захист персональних даних в Україні, США та ЄС. Автори підкреслюють, що українське законодавство, зокрема Закон «Про захист персональних даних», потребує оновлення та гармонізації з міжнародними стандартами, такими як GDPR та CCPA. У статті також розглядаються прогалини в українському законодавстві, зокрема відсутність чітких вимог до кіберзахисту інформаційно-комунікаційних систем, в яких обробляються персональні дані. Автори наголошують на необхідності впровадження кращих світових практик для підвищення рівня довіри громадян та бізнесу до державних інституцій, а також для стимулювання розвитку цифрової економіки України [92].

Також порівняльній характеристиці нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах присвячена стаття В. Кальченка та В. Ободяка. Автори аналізують відмінності між українським законодавством і європейським регламентом GDPR щодо захисту персональних даних. У статті підкреслюється необхідність адаптації українських нормативних актів до стандартів ЄС для підвищення ефективності захисту персональних даних та розвитку цифрової інфраструктури країни [93].

У контексті євроінтеграційного курсу України, сучасні наукові дослідження акцентують увагу на необхідності гармонізації національного законодавства у сфері захисту персональних даних із європейськими та міжнародними стандартами, насамперед GDPR. Акцентується увага на існуючих прогалинах в українському правовому полі, зокрема у сфері кіберзахисту інформаційно-комунікаційних систем, що обробляють персональні дані, й підкреслюються потреба впровадження ефективних правових та організаційних механізмів.

Зарубіжні публікації присвячені актуальним викликам у сфері захисту персональних даних, інформаційної безпеки та правового регулювання в умовах стрімкої цифровізації. Основну увагу дослідники приділяють таким темам, як: захист приватності в Інтернеті речей (IoT) та необхідність нових підходів до цифрової ідентифікації [94]; прогалини у регулюванні штучного інтелекту в рамках ЄС і необхідність узгодження його з положеннями GDPR [95]; кримінально-правова відповідальність за кібершахрайство в епоху edge computing і виклики, пов’язані із захистом персональної інформації [96]. Вищезазначені та інші чисельні публікації формують цілісну картину міжнародного досвіду з питань забезпечення інформаційної безпеки, підкреслюючи необхідність міждисциплінарного підходу, нормативної адаптації та інтеграції захисту даних у всі сфери цифрової діяльності.

4.2. Інституційно-правові засади кібербезпеки та захисту персональних даних в Україні

Конституція України (КУ), закріплюючи систему основоположних прав і свобод людини, створює принципову правову рамку для розвитку законодавства у сферах захисту персональних даних, інформаційної безпеки та цифрових прав. Основні конституційні положення, що закладають фундамент кібербезпеки, належать до розділу II «Права, свободи та обов'язки людини і громадянина» та регулюють приватність, інформаційний суверенітет особи та обмеження державного втручання [97].

Стаття 32 КУ містить ключові гарантії, що стосуються персональних даних. Частина перша встановлює: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України» [97]. Це формує базовий принцип недоторканності приватного простору, який у цифрову епоху охоплює як фізичні, так і електронні прояви приватності. Частина друга забороняє «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди», за винятком випадків, визначених законом і лише «в інтересах національної безпеки, економічного добробуту та прав людини». Ця норма створює безумовний пріоритет згоди суб'єкта даних та делегує законодавцю обмежені умови, за яких можлива легітимна обробка персональних даних без такої згоди, одночасно перешкоджаючи надмірному збиранню даних державою. Частина третя гарантує право кожного «знати, які відомості про нього збираються», а також передбачає право на доступ до таких відомостей та право вимагати їх виправлення. Це положення формує основу сучасної концепції інформаційного самоврядування (informational self-determination), що є необхідною передумовою функціонування будь-якої системи захисту персональних даних. Частина четверта встановлює право на судовий захист у разі порушення цих норм, що забезпечує конституційні гарантії ефективного правового засобу захисту.

Стаття 31 КУ гарантує таємницю комунікацій. У ній зазначено: «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції». Формула «інша кореспонденція» охоплює всі сучасні форми цифрової комунікації, включно з електронною поштою, месенджерами, хмарними сервісами та іншими каналами передачі інформації. Друга частина статті встановлює, що «винятки можуть бути встановлені лише судом у випадках, передбачених законом». Це створює конституційний бар'єр перед неконтрольованими формами електронного стеження, а також зобов'язує органи державної влади застосовувати будь-які заходи цифрового перехоплення тільки в рамках судового контролю й пропорційності. Таким чином, стаття 31 є прямою базою для обмеження діяльності спецслужб у кіберпросторі та регулювання оперативно-розшукових і технічних заходів.

Стаття 34 КУ закріплює право на свободу інформації, проголошуючи право кожного «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб». Ця гарантія, однак, супроводжується частиною третьою, яка дозволяє встановлювати обмеження законом «в інтересах національної безпеки, територіальної цілісності або громадського порядку» та інших визначених Конституцією підстав. Для сфери кібербезпеки це створює необхідний баланс між свободою інформації та захистом критичної інформаційної інфраструктури. Водночас ця норма забезпечує легітимність державних вимог щодо безпечного поводження з інформацією, у тому числі персональною.

Право на невтручання у приватне життя отримує додаткове укріплення в статті 28 КУ, яка гарантує, що «кожен має право на повагу до його гідності». У контексті цифрових прав це означає, що обробка персональних даних, цифрове спостереження або автоматизоване прийняття рішень не можуть принижувати гідність людини чи перетворювати особу на об'єкт неконтрольованого стеження. Повага до гідності стає ключовим критерієм допустимості цифрових технологій.

Стаття 40 КУ, яка гарантує право звернення до органів державної влади, побічно стосується кібербезпеки шляхом установлення обов'язку держави

забезпечувати безпечні та надійні канали комунікації між громадянами і державними органами, включаючи електронні сервіси. Це створює основу для розвитку державних платформ цифрової взаємодії.

Стаття 17 КУ визначає забезпечення «державної безпеки та захисту державного кордону» як найважливіші функції держави. У сучасних умовах це поняття охоплює й кібербезпеку, оскільки цифрові загрози становлять одну з ключових компонент національної безпеки. Конституційний обов'язок держави забезпечувати безпеку включає захист інформаційного простору, критичної інфраструктури та цифрового суверенітету.

Таким чином, КУ формує комплексну і внутрішньо узгоджену систему конституційних гарантій у сфері цифрової безпеки, захисту персональних даних і приватності. Статті 31 і 32 закріплюють фундаментальні права на недоторканність приватного життя й таємницю комунікацій, визначаючи межі й процедури можливого втручання. Стаття 34 забезпечує свободу інформації у поєднанні з легітимними механізмами її обмеження. Стаття 17 визначає обов'язок держави захищати інформаційний простір як складову національної безпеки. Разом ці положення створюють конституційне підґрунтя, на якому базується спеціальне законодавство України про персональні дані, інформаційну та кібернетичну безпеку.

Закон України «Про інформацію» [98] встановлює правові засади інформаційних відносин і правовий режим інформації як ключового ресурсу суспільства. Він є одним із центральних загально-галузевих актів, на якій базуються спеціальні закони (наприклад, про персональні дані, електронні комунікації, інформаційну безпеку).

Визначення предмета правового регулювання вказано в Статті 1: під «інформацією» розуміються деталі і/або дані, які можуть зберігатися на фізичних носіях або відображатися електронно. Це універсальне визначення охоплює як традиційні форми інформації, так і її цифрові втілення в базах даних, інформаційних системах та мережах. Закон визначає також поняття захисту інформації як сукупність правових, адміністративних, організаційних, технічних

та інших заходів, що забезпечують збереження, цілісність та порядок доступу до інформації. Така дефініція має прямий вплив на подальше законодавство в сфері кібербезпеки та захисту інформації загалом, оскільки вказує на комплексність і багатовимірність захисних заходів, які повинні бути предметом регулювання.

Стаття 2 закріплює основні принципи інформаційних відносин, серед яких забезпечення прав на інформацію, публічність і доступність, свободу обміну та отримання інформації, законність отримання й використання інформації, а також безпеку особи від втручання в особисте і сімейне життя. Ці принципи не лише декларативні, а й слугують методологічною основою для тлумачення інших правових норм, зокрема щодо доступу до відкритих даних, захисту персональної інформації та обмежень у сфері обробки інформації заради суспільних чи державних інтересів.

Стаття 3 закладає державну інформаційну політику, яка має включати забезпечення кожному доступу до інформації, створення умов для вільного обміну та використання інформації, розвиток інформаційних систем і мереж, впровадження електронного урядування, збереження національних інформаційних ресурсів й забезпечення інформаційної безпеки України. Формулювання про інформаційну безпеку є принциповим: воно ставить завдання державі формувати та реалізовувати політику, покликану гарантувати захист інформаційних ресурсів та інформаційного простору, що включає і кібернетичний вимір у сучасних умовах.

У Статті 5 міститься гарантоване кожному право на інформацію, яке охоплює можливість вільно отримувати, використовувати, поширювати, зберігати й захищати інформацію, необхідну для реалізації своїх прав і легітимних інтересів. Законом далі встановлено, що реалізація цього права не повинна порушувати законні права інших осіб чи суспільні інтереси, тим самим вводиться принцип збалансованості доступу до інформації та захисту інших прав (наприклад, приватності чи безпеки).

Стаття 6 визначає механізми забезпечення права на інформацію, включно з створенням умов для доступу до різних джерел інформації, обов’язком органів

влади інформувати суспільство та забезпечувати доступ до їхньої діяльності, встановленням відповідальності за порушення законодавства про інформацію. Частина друга цієї статті прямо передбачає, що право на інформацію може бути обмежене законом у інтересах національної безпеки, громадського порядку, захисту прав інших осіб тощо – це юридично важлива норма, яка служить законодавчою підставою для обмежень доступу до інформації з міркувань захисту та безпеки, включно з кібербезпекою та захистом персональних даних.

Важливим є розділ про класифікацію інформації. Зокрема, Стаття 10 та Стаття 11 виділяють інформацію про індивіда (персональні дані) як окремий тип інформації. Закон встановлює, що збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди не допускається, за винятком випадків, передбачених законом і лише в інтересах національної безпеки, економічного добробуту чи захисту прав людини. Це положення перегукується і підсилює конституційну норму про захист персональних даних, закріплену в Статті 32 КУ, та є прямою юридичною підставою для спеціального законодавства про персональні дані. Аналогічні принципи закріплено й для доступу кожного до власної інформації, за винятком випадків, обумовлених законом.

Далі Статті 20-21 встановлюють правовий режим доступу до інформації, розділяючи її на публічно доступну та обмежену, де обмеженою визнається конфіденційна, таємна та службова інформація. Закон визначає, що конфіденційна інформація може бути розповсюджена лише з дозволу власника або у випадках, передбачених законом, що створює правовий механізм захисту інформації, яка має обмежений доступ, включно з персональними даними.

Статті, що стосуються діяльності журналістів та медіа, регулюють професійні відносини і заборону на цензуру, але також прямо вказують на права та обов’язки щодо доступу до інформації та її захисту.

Нарешті, розділ про відповідальність передбачає, що порушення законодавства про інформацію тягне за собою дисциплінарну, цивільну, адміністративну або кримінальну відповідальність. Це особливо важливо з

огляду на сучасні стандарти відповідальності за неправомірне розголошення, несанкціонований доступ або обробку інформації, зокрема персональних даних чи інших обмежених відомостей.

У сукупності норми Закону України «Про інформацію» створюють правову основу для захисту інформаційних прав суб'єктів, збалансований доступ до інформації, режим класифікації інформації і механізми її захисту. Цей закон слугує базовою платформою для розвитку спеціального законодавства з кібербезпеки, захисту персональних даних та безпеки інформаційних систем в Україні.

Закон України «Про основні засади забезпечення кібербезпеки України» [99] формує нормативну рамку, у межах якої держава, суспільство й приватний сектор координують свої зусилля у захисті цифрового середовища. Його ключові статті визначають поняття, принципи та інституційні механізми, що задають логіку побудови сучасної національної системи кіберзахисту. Уже Стаття 1 окреслює базову термінологію, яка стає основою для подальшого правозастосування: кіберпростір трактується як глобальне середовище функціонування інформаційно-комунікаційних систем, а кібербезпека – як стан захищеності життєво важливих інтересів держави, суспільства й громадянина, що може бути порушений через кібератаки, кіберінциденти та інші форми цифрових загроз. У цих визначеннях помітна інтеграція національного підходу з міжнародними стандартами безпеки, що надає правовому регулюванню належної концептуальної узгодженості.

Подальші положення Закону розкривають його функціональну спрямованість. У Статті 2 сформульовано принципи, на яких ґрунтується національна політика у сфері кібербезпеки. Йдеться про верховенство права, пропорційність заходів безпеки, дотримання балансу між необхідністю захисту та повагою до прав і свобод людини, а також про важливість превентивних механізмів та багаторівневої взаємодії з усіма суб'єктами цифрових відносин. Таким чином, закон не лише визначає правила, а й задає етичний вимір державної діяльності у цифровому просторі.

Стаття 3 закріплює правові основи функціонування кібербезпеки, підкреслюючи, що ця сфера ґрунтується на Конституції, профільних законах, міжнародних договорах і стратегічних документах, які формують цілісний нормативний контекст. Кібербезпека у цьому розумінні постає як комплекс політик і процедур, орієнтованих не тільки на реагування на загрози, а й на їх завчасне виявлення, оцінювання ризиків і стратегічне планування захисту.

Особливе значення має Стаття 4, яка описує об'єкти кібербезпеки та кіберзахисту. До них належать інформаційні ресурси, комунікаційні системи, інформаційно-телекомунікаційні системи та інфраструктура, від функціонування якої залежить стабільність держави. Уведення поняття критичної інформаційної інфраструктури відображає світову тенденцію до підвищеної уваги щодо систем, які забезпечують енергетику, транспорт, фінансову діяльність, державне управління та інші сфери життєзабезпечення.

Стаття 5 формує коло суб'єктів, відповідальних за реалізацію політики кібербезпеки. До цього кола входять державні органи, спеціалізовані служби, органи місцевого самоврядування, підприємства та організації різних форм власності, а також громадяни. Закон тим самим створює поліцентричну модель кіберзахисту, у якій функції держави доповнюються обов'язками власників інформаційних систем та користувачів цифрових ресурсів. У Статті 5-1 розширено вимоги щодо інституціоналізації кіберзахисту всередині організацій шляхом створення підрозділів або призначення керівників, відповідальних за організацію і контроль заходів безпеки. Це свідчить про розуміння кібербезпеки як управлінської функції, що вимагає професійної компетентності й системності.

Стаття 6 визначає обов'язок суб'єктів критичної інфраструктури підтримувати високий рівень готовності до протидії кіберзагрозам. Тут підкреслюється, що такі суб'єкти повинні забезпечувати не лише технічну стійкість своїх систем, а й організаційно-процедурну узгодженість дій, зокрема у питаннях моніторингу, повідомлення про інциденти та оперативного реагування. У цьому контексті кібербезпека набуває характеру неперервного процесу управління ризиками.

У Статтях 7-9 відображено концепцію національної системи кібербезпеки, яка передбачає взаємодію державних органів, операторів інфраструктури, експертного середовища та приватного сектору для виявлення й нейтралізації загроз. Окрема увага приділяється створенню механізмів реагування на кіберінциденти та забезпеченню сталої здатності інституцій до відновлення функціонування після атак. У цих положеннях проявляється ідея колективної кіберстійкості, яка є фундаментальною у сучасних підходах до захисту цифрових систем.

Стаття 9-1 закладає основу для функціонування національної системи обміну інформацією про кіберзагрози та кіберінциденти. Закон наголошує, що цей обмін має здійснюватися з дотриманням законодавства про захист персональних даних, що є принципово важливим з огляду на необхідність запобігти надмірному втручанню у приватність та забезпечити відповідність міжнародним стандартам, включно з європейськими. У цьому положенні чітко простежується ідея співвідношення безпеки та прав людини: кіберзахист не може бути підставою для необмеженої обробки інформації про особу.

Далі Стаття 10 окреслює засади державно-приватної взаємодії, яка стає ключовим чинником ефективності кібербезпеки в умовах цифрової економіки. Приватний сектор володіє значною частиною технологічних ресурсів, а тому його залучення до механізмів виявлення, класифікації та нейтралізації загроз є необхідним елементом безпекової інфраструктури держави.

Стаття 11 підкреслює роль держави у створенні сприятливих умов для розвитку кібербезпеки, включно зі стимулюванням наукових досліджень, підготовки кадрів, технічного переоснащення та інновацій. Ця стаття підносить кібербезпеку до рівня стратегічної галузі знань і практики, що потребує довгострокової політики розвитку.

Нарешті, Стаття 12 встановлює вимоги до контролю за законністю заходів із кіберзахисту. Акцент на контролі є необхідною гарантією того, що діяльність у сфері кібербезпеки не стане підставою для порушення конституційних прав громадян. Тут проявляється демократичний характер регулювання, який

обмежує державне втручання рамками законності, пропорційності та обґрунтованості.

У сукупності ці статті формують цілісний концептуальний каркас національної системи кібербезпеки. Закон поєднує стратегічне бачення із практичними механізмами реалізації та підкреслює, що ефективний кіберзахист у XXI ст. можливий лише за умови збалансованої взаємодії держави, суспільства та бізнесу, а також неухильного дотримання прав людини й принципів захисту персональних даних.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» [100] є одним із фундаментальних джерел правового регулювання захисту інформації в автоматизованих системах і має безпосереднє значення для становлення інформаційної безпеки в Україні.

Закон формує комплексне правове поле для відносин, пов'язаних із захистом інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – системи). Він встановлює предмет регулювання, ключові терміни, а також підґрунтя для визначення правового режиму доступу до інформації, обов'язків щодо її захисту, ролей суб'єктів та повноважень державних органів.

У самому початку, в Статті 1, закон вводить терміни, що визначають предмет і обсяг регулювання: блокування – як дії, що унеможливлюють доступ до інформації; витік – як доступ до інформації осіб, які не мають на це права; володілець інформації – як особа, якій належать права на інформацію; власник системи – як особа, яка володіє технічним засобом обробки інформації; та поняття обробки, доступу, несанкціонованих дій, криптографічного захисту, порушення цілісності тощо. Ці терміни формують загальні семантичні координати для всіх подальших норм.

Подальні статті розвивають ці визначення у площині правового статусу об'єктів і суб'єктів. Статті 2-3 окреслюють об'єкти захисту та суб'єктів відносин: першими виступають системи і інформація як така, другими – користувачі,

володільці інформації й власники систем, яким закон делегує конкретні обов'язки і права.

Ключове значення у правовому регулюванні має Стаття 4, що встановлює загальні засади доступу до інформації в системі. Закон делегує визначення порядку доступу безпосередньо володільцеві інформації, водночас визнаючи, що порядок доступу до державних інформаційних ресурсів або інших відомостей із законодавчо встановленими вимогами захисту визначається окремими законами. Закон також передбачає, що у випадках, прямо визначених законом, доступ до інформації може здійснюватися без дозволу володільця у порядку, встановленому законодавством.

У Статтях 5-7 Закон визначає відносини між володільцем інформації, власником системи, користувачем та іншими власниками систем. Ці норми закладають договірну основуправового регулювання, відповідно до якої власник системи зобов'язаний забезпечувати захист інформації на умовах, визначених договором із володільцем інформації, якщо інше не встановлено законом; він також має інформувати володільця про механізми захисту інформації. Взаємодія між власниками систем у випадках обміну чи спільної обробки інформації також регламентується договором, що гарантує правову визначеність і юридичну відповідальність за захист інформації.

Стаття 8 формує загальні умови обробки інформації в системі, орієнтуючи діяльність щодо захисту на комплексну систему заходів, поєднаних організаційно-технічними рішеннями і засобами, включно з криптографічними та технічними заходами, що мають підтвердження відповідності встановленим вимогам. Це положення підкреслює, що захист інформації – це не лише технічна функція, а й упорядкований набір заходів відповідно до визначених нормативних стандартів.

Стаття 9 визначає, що відповідальність за забезпечення захисту інформації в системі покладається на власника системи. У разі обробки державних інформаційних ресурсів або інформації з обмеженим доступом закон встановлює, що власник системи має створити службу захисту інформації або

призначити відповідальних осіб для контролю за його реалізацією; при цьому він зобов'язаний повідомляти спеціально уповноважений орган про спроби або факти несанкціонованих дій.

Стаття 10 розвиває питання повноважень державних органів. Вона зобов'язує Кабінет Міністрів України визначати вимоги до захисту державних інформаційних ресурсів та інформації з обмеженим доступом. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку і захисту інформації відповідає за формування пропозицій щодо державної політики з питань захисту інформації, організацію державної експертизи засобів захисту, здійснення контролю за їх застосуванням та реалізацію заходів щодо виявлення загроз. Це положення конституціоналізує державне управління безпекою інформаційних систем в межах компетенції визначених органів.

У Статтях 11-13 Закон передбачає відповідальність за порушення законодавства про захист інформації в системах, встановлює правові наслідки недотримання вимог, закріплює механізми участі України у міжнародних договорах у цій сфері і містить прикінцеві положення для транзиту до поточного правового режиму.

У своїй сукупності Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» створює усталену правову платформу для розвитку інформаційної безпеки в Україні. Він формує базові правові засади, які дозволяють розвивати подальші спеціалізовані стандарти, технічні регламенти та інтегрувати національні системи захисту із сучасними міжнародними моделями управління інформаційними ризиками. Його місце в національному правовому полі – це базис для всіх подальших нормативних актів у сфері кібербезпеки, захисту інформації, електронних комунікацій та персональних даних, що забезпечують цілісність та безперервність функціонування цифрової інфраструктури держави.

Закон України «Про захист персональних даних» [101] є основним нормативно-правовим актом, що визначає правові відносини, пов'язані з

обробкою персональних даних і спрямований на захист фундаментальних прав і свобод людини, зокрема права на повагу до приватного життя у зв'язку з обробкою персональних даних.

У загальному обсязі свого регулювання Закон покриває відносини, які виникають під час обробки персональних даних незалежно від того, чи використовується при цьому автоматизована обробка, чи обробка здійснюється у формі картотеки або іншої структурованої сукупності даних. Закон не розповсюджується на обробку персональних даних фізичною особою виключно для власних побутових потреб, а також на діяльність журналістів чи творчих працівників в межах їх професійних обов'язків.

У своїй структурі Закон вирізняє низку базових понять, що визначають предмет та обсяг правового регулювання. Персональні дані трактуються як відомості про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Обробка персональних даних охоплює будь-які дії щодо них – від збору й зберігання до використання, передачі, знеособлення чи знищення. База персональних даних – це упорядкована сукупність таких даних у електронній формі або у вигляді картотеки; володілець бази формує мету обробки, визначає її зміст і встановлює процедури обробки. Суб'єкт персональних даних – це фізична особа, щодо якої здійснюється обробка даних, а розпорядник персональних даних – особа, що отримує від володільця право безпосередньо обробляти дані. Третьою особою визнається будь-який отримувач, який не належить до попередніх категорій.

Закон встановлює принципи та вимоги до обробки персональних даних, які мають бути законними, прозорими і відповідати чітко сформульованій меті. Мета обробки має бути визначена в законодавстві, установчих документах або іншому нормативному акті, і будь-яка зміна цієї мети без згоди суб'єкта даних є правовим порушенням. Персональні дані повинні бути точними та, за потреби, актуалізовані, їх обсяг має відповідати реальній потребі обробки. Існують також вимоги щодо первинних джерел даних, якими виступають особисті документи чи відомості, надані самою особою.

Закон підкреслює, що персональні дані, за винятком знеособлених, є інформацією з обмеженим доступом, і лише у законодавчо встановлених випадках вони можуть бути вільно доступними. Окремі категорії даних не можуть автоматично відноситися до відкритої інформації, зокрема коли йдеться про фізичних осіб, що займають певні публічні посади, за винятком інформації, чітко визначеної законодавством.

Закон також визначає спеціальні вимоги до категорій даних, що стосуються расової чи етнічної приналежності, політичних поглядів, релігійних переконань, членства в профспілках, стану здоров'я чи інтимного життя, обробка яких заборонена без явно вираженої згоди суб'єкта даних, за винятком випадків, передбачених законом (наприклад, для медичної допомоги, захисту життєвих інтересів, виконання трудових обов'язків тощо).

Закон створює правову основу для здійснення контролю за додержанням вимог щодо захисту персональних даних, надаючи повноваження Уповноваженому Верховної Ради України з прав людини здійснювати нагляд і реагувати на порушення. Суб'єкти персональних даних мають право доступу до своїх даних, зміни неточних чи неповних даних, отримувати інформацію про дії, що здійснюються з їхніми даними, а також оскаржувати рішення або дії, що порушують їх права.

Аналіз цього Закону демонструє, що він закладає комплексну систему захисту прав і свобод людини у сфері особистих даних, базовану на принципах прозорості, поваги до приватності, визначеності мети обробки та відповідальності за порушення. Він поєднує правові механізми, що зобов'язують суб'єктів даних і володільців до обережної і правомірної обробки даних, із заходами державного контролю. Зі створенням проекту нової редакції Закону, що має гармонізувати українське законодавство з європейськими стандартами (такі як GDPR), чинний Закон залишається ключовою базою правового регулювання персональних даних в Україні.

У контексті євроінтеграційних процесів, доцільно розглянути вплив європейських стандартів на формування українського законодавства (табл.4.1).

Таблиця 4.1

Вплив європейських стандартів на формування українського законодавства

Європейський стандарт	Що регулює	Шляхи імплементації в Україні	Нормативні акти України
Конвенція 108 / 108+	Захист персональних даних, автоматизована обробка, контроль	Закон «Про захист персональних даних» побудований на основних принципах Конвенції; модернізація через законопроєкт 8153	ЗУ «Про захист персональних даних»
Будапештська конвенція	Кіберзлочини, цифрові докази, міжнародна співпраця	Гармонізація кримінального законодавства; створення інституцій протидії кіберзлочинності (кіберполіція, CERT-UA)	ККУ, КПК; ЗУ «Про основні засади забезпечення кібербезпеки»
GDPR	Повний комплекс норм з обробки та захисту ПД	Український законопроєкт 8153 адаптує суб'єктний склад, принципи, права суб'єктів, DPIA, breach notification, DPO	Закон України «Про захист персональних даних»

Складено авторами.

Конвенція Ради Європи № 108 [102] стала першим міжнародним документом, який встановив універсальні правила щодо захисту особи у зв'язку з обробкою персональних даних. Її фундаментальна ідея полягає в утвердженні права кожної людини на приватність у цифровому середовищі, яке набуває щораз більшого значення в умовах глобального обігу інформації. Центральним змістом Конвенції є система принципів, що визначають правомірність та етичність обробки даних. Обробка повинна здійснюватися чесно та законно, відповідно до наперед визначених і легітимних цілей, які не можуть змінюватися довільно. Дані мають бути адекватними, релевантними та не надмірними щодо поставленої мети, а також точними й такими, що за потреби підлягають оновленню. Передбачається, що дані не зберігатимуться довше, ніж цього вимагає мета обробки, після чого вони мають бути знищені або анонімізовані. У цих принципах втілено не лише технічну логіку інформаційної безпеки, а й гуманістичний підхід, що захищає людину від необмеженого та невиправданого втручання у приватне життя.

Однією з фундаментальних інновацій Конвенції є визнання права суб'єкта даних на знання про те, що щодо нього збираються та обробляються дані, а також на доступ до цих даних і можливість вимагати їх виправлення або видалення у разі неточності чи незаконності обробки. У цих положеннях закладено підхід, який сьогодні вважається класикою у сфері захисту даних: обробка не може бути одностороннім актом контролера, вона має враховувати автономію та інтереси особи, чиї дані обробляються. Таким чином, Конвенція вперше на міждержавному рівні встановила суб'єктивне право людини на контроль над інформацією про себе, що згодом стало підґрунтям для європейських і глобальних норм, включно із загальним регламентом ЄС про захист даних (GDPR).

Урядові та приватні структури, що здійснюють обробку даних, несуть обов'язок створювати належні технічні й організаційні заходи для запобігання випадковому чи незаконному доступу, зміні чи поширенню даних. Конвенція передбачає, що захист даних не є лише юридичною умовою, але й технологічною відповідальністю, яка потребує побудови комплексних систем безпеки. Цей обов'язок охоплює також ситуації транскордонного обміну даними: держави, що підписали Конвенцію, зобов'язані гарантувати, що передання даних до інших юрисдикцій можливе лише за умови наявності адекватного рівня захисту на стороні отримувача. Саме це положення стало основою для формування принципу «адекватності», який нині є одним із ключових механізмів міжнародного руху персональних даних.

Зростання потужності сучасних інформаційно-комунікаційних технологій вимагало модернізації Конвенції 108. Так з'явилася Конвенція 108+, яка суттєво розширила зміст оригінального документа. Модернізована версія передбачає посилення стандартів законності обробки, а також введення додаткових підстав, за яких обробка може вважатися правомірною. Особливу увагу приділено спеціальним категоріям даних – таким як дані про здоров'я, расову чи етнічну приналежність, політичні переконання чи біометричні характеристики. Їх обробка допускається лише у виняткових, чітко визначених законом випадках і

за умови високого рівня захисту. Тут чітко проявляється намір адаптувати міжнародні стандарти до реалій епохи великих даних та алгоритмічної обробки.

Конвенція 108+ також суттєво зміцнює права суб'єктів даних. Окрім традиційного доступу та виправлення, вводяться розширені права, що дозволяють людині впливати на процеси автоматизованої обробки, зокрема у контексті ухвалення рішень, які ґрунтуються виключно на алгоритмах. Прозорість таких рішень та можливість їх оскарження стають одними з ключових елементів демократичного контролю за використанням новітніх технологій. У цих нормах особливо чітко відчутна загальноєвропейська тенденція – не обмежуватися формальним захистом даних, а забезпечувати реальний контроль людини над тим, як саме технології впливають на її життя.

Конвенція 108+ передбачає посилений інституційний механізм контролю – кожна держава зобов'язана створити або підтримувати незалежний орган із захисту даних, який має повноваження проводити перевірки, втручатися у разі порушень та взаємодіяти з аналогічними органами інших країн. Ця мережа регуляторів перетворює Конвенцію на інструмент не лише правового, а й міжнародного практичного співробітництва.

У сучасному вигляді Конвенція 108 та її протокол 108+ становлять цілісний, гнучкий і адаптований до цифрової епохи міжнародний стандарт. Їхня нормативна модель не лише захищає права людини, але й формує спільний простір довіри між державами, бізнесом та суспільством – простір, у якому персональні дані розглядаються не лише як ресурс, а як елемент людської гідності, що потребує відповідального ставлення.

Конвенція Ради Європи про кіберзлочинність, відома як Будапештська [103], постає одним із найпослідовніших міжнародних актів, що трансформували уявлення держав про природу злочинності у цифрову епоху. Її структура вибудувана таким чином, щоб поступово окреслити коло діянь, які складають ядро протиправності у сфері інформаційних технологій, а також механізми, завдяки яким держави можуть ефективно протидіяти таким загрозам і співпрацювати між собою. Уже на рівні перших статей Конвенція формує

нормативну карту цифрового середовища, визначаючи незаконний доступ до комп'ютерних систем як діяння, що не потребує настання шкоди для визнання його кримінальним. Такий підхід демонструє перехід від реактивної моделі кримінального права до превентивної, де небезпека полягає не лише у факті порушення цілісності системи, а й у самому вторгненні в неї. Аналогічно Конвенція класифікує незаконне перехоплення даних як посягання на приватність, визнаючи, що в умовах сучасної технологічної реальності навіть метадані можуть нести чутливу інформацію про особу, а отже, потребують такого самого правового захисту, як і зміст комунікацій.

Положення, присвячені втручанню в дані та втручанню в системи, створюють нормативну симетрію між інформацією як ресурсом і технічними платформами як інфраструктурою. За своєю логікою Конвенція розглядає цифрові об'єкти як суспільно значущі блага, порушення цілісності яких може мати наслідки, співставні зі шкодою для матеріальних об'єктів. Завдяки цьому у правовій площині утверджується принцип еквівалентності цифрової і фізичної власності. Водночас стаття, присвячена неправомірним пристроям, доповнює цей підхід, фокусуючись не на результаті, а на інструменті. Створення, придбання або поширення засобів, призначених для обходу технічних бар'єрів, розглядається як автономна загроза. Конвенція тим самим окреслює технічний арсенал кіберзлочинності як сферу, що потребує особливої кримінально-правової уваги.

Подальші статті, спрямовані на комп'ютерне підроблення та комп'ютерне шахрайство, транслюють традиційні кримінально-правові категорії у цифровий вимір. Електронний документ постає рівнозначним паперовому, цифрова транзакція – еквівалентною фізичній, а отже, правопорядок має реагувати на їх фальсифікацію або маніпулювання з тією самою серйозністю. До цього блоку додається положення щодо захисту авторських прав, яке фіксує економічну вразливість цифрового середовища до масового і швидкого незаконного копіювання. У такий спосіб Конвенція окреслює цифрову економіку як простір, де інтелектуальна власність повинна мати дієвий кримінально-правовий щит.

Найбільш концептуально насичена частина Конвенції пов’язана з процедурними заходами, адже вона адаптує кримінальний процес до реалій електронних доказів. У дипломатичному тексті закріплено розуміння того, що електронні дані є нестійкими, змінними й такими, що можуть бути знищені навіть ненавмисними діями. Тому запроваджуються спеціальні механізми негайного збереження даних, доступу до них та їх вилучення з дотриманням вимог пропорційності та законності. У цьому простежується баланс між необхідністю забезпечити ефективність правоохоронної діяльності та зобов’язанням захищати права людини, які завжди мають залишатися в центрі кримінального провадження.

Завершальний розділ Конвенції присвячений міжнародній співпраці, що є її ключовим інституційним досягненням. Кіберзлочинність не знає кордонів, і Конвенція прямо реагує на цю реальність, проголошуючи обов’язок держав допомагати одна одній у розслідуванні злочинів, обмінюватися інформацією та використовувати механізми екстрадиції. Особливу роль відіграє створення мережі оперативних контактів «24/7», яка стає оперативною інфраструктурою для швидкого реагування, минаючи бюрократичні бар’єри. Цей інститут демонструє, що Конвенція не обмежується деклараціями, а формує практичні інструменти, які дозволяють державам діяти своєчасно й узгоджено.

У сукупності статті Будапештської конвенції відображають цілісну філософію регулювання цифрового простору, де безпека, права людини та міжнародна солідарність функціонують у неподільній єдності. Конвенція створює нормативну модель, у якій цифрове середовище розглядається як спільний простір відповідальності, а кіберзлочинність – як глобальний виклик, що потребує узгоджених правових рішень. Саме тому цей документ і надалі залишається основною архітектурною опорою сучасної політики протидії кіберзлочинності.

GDPR [104] – це Загальний регламент про захист даних Європейського Союзу, який був ухвалений Європейським парламентом і Радою ЄС 27 квітня 2016 року і набрав чинності 25 травня 2018 року як безпосередньо застосовний

нормативно-правовий акт у всіх країнах-членах ЄС і Європейської економічної зони (ЄЕЗ). Він замінив попередню Директиву про захист даних 95/46/ЕС та створив уніфіковану правову систему захисту персональних даних, яка поширюється на всі форми обробки інформації, що може прямо або опосередковано ідентифікувати фізичну особу. Регламент є частиною ширшої архітектури захисту прав людини в ЄС, пов'язаної з правом на приватність і захист особистої інформації, закріпленим у Хартії основних прав Європейського Союзу.

У центрі нормативної архітектури GDPR стоїть Стаття 5, яка формує ідейний фундамент усього регламенту. Саме тут закріплено принципи обробки персональних даних, що визначають її межі, цілі й етичні виміри. Стаття вимагає, щоб дані оброблялися законно й прозоро, відповідно до чітко визначених і легітимних цілей. Принцип цільової обмеженості не дозволяє перетворювати дані на універсальний ресурс для будь-яких експериментів чи бізнес-моделей, а вимагає дотримання тієї логіки, у межах якої вони були зібрані. Принципи точності, мінімізації й обмеженого зберігання запроваджують дисципліну поводження з даними: організація має не лише знати, що вона обробляє, а й чому саме, і чи не виходить її діяльність за межі необхідного. У Статті 5 закріплюється і принцип підзвітності, який перетворює контролера даних на відповідального суб'єкта, що мусить доводити правомірність своїх дій, а не лише формально її декларувати.

Стаття 6 поглиблює зміст юридичної законності обробки персональних даних. У ній визначено підстави, що надають контролеру право здійснювати обробку: від згоди суб'єкта даних до виконання контрактних чи законодавчих обов'язків, від захисту життєво важливих інтересів до виконання завдань, пов'язаних із публічною владою, або реалізації законних інтересів контролера. У статті фактично створено баланс між потребами суспільства, бізнесу та держави й фундаментальними правами особи. Концепція «законного інтересу» тут набуває особливого значення, адже вона відкриває простір для гнучкого

тлумачення, але одночасно вимагає ретельного зважування потенційної шкоди для суб'єкта даних.

Надзвичайно важливими є статті, що встановлюють права суб'єкта даних. Стаття 12 визначає загальну вимогу прозорості та зобов'язує контролера надавати інформацію зрозумілою і доступною мовою. Це положення стає ключем до реалізації всіх інших прав, адже без доступності інформації контроль над даними лишався б декларативним. У Статтях 13 і 14 конкретизуються обставини, коли контролер повинен повідомити суб'єкта про обробку: незалежно від того, чи були дані зібрані безпосередньо у людини, чи отримані з інших джерел. У цих положеннях простежується ідея, що суб'єкт даних не може бути пасивною стороною у процесі обробки; навпаки, він має виступати рівноправним учасником, здатним ухвалювати рішення щодо своєї інформації.

Стаття 15 закріплює право на доступ – право, яке в європейській правовій традиції розглядається як інструмент контролю над владою і над технологічними структурами. Людина має право знати, які дані про неї обробляються, з якою метою, кому вони передаються і яким є строк їх зберігання. Доступ стає тим механізмом, що дозволяє суб'єкту даних згодом реалізувати інші права, включно з правом на коригування даних, яке закріплено в Статті 16. У ній ідеться не лише про технічну можливість виправлення неточностей, а й про забезпечення того, що у цифрових системах не закріплюватимуться помилки, які можуть мати суттєві наслідки для особи.

Стаття 17 присвячена праву на видалення, яке у публічному дискурсі здобуло назву «право бути забутим». Це право є реакцією на феномен цифрової пам'яті, яка, на відміну від людської, не має природної схильності до забуття. Наявність механізму видалення даних стає засобом відновлення автономії, дозволяючи людині наново окреслювати межі своєї цифрової ідентичності. Стаття 18, яка вводить право на обмеження обробки, ще більше розширює цей інструментарій, дозволяючи тимчасово зупиняти діяльність контролера, якщо виникають підстави сумніватися в законності обробки або її точності.

Особливого значення набуває стаття 20, що закріплює право на перенесення даних. Це нова концепція, яка поєднує захист приватності з економічною конкуренцією. Вона дає змогу суб'єктові переносити свої дані між різними платформами або сервісами у структурованому та машиночитаному форматі, тим самим руйнуючи монополію великих технологічних компаній на дані користувачів. Стаття 21, що передбачає право на заперечення, дозволяє людині протидіяти обробці її даних у випадках, коли інтереси контролера не переважають над її правами та свободами.

У питаннях безпеки GDPR виявляє особливо високий стандарт. Стаття 32 визначає обов'язок контролера вживати відповідних технічних і організаційних заходів для забезпечення безпеки даних. Вона не обмежується переліком інструментів, а змушує контролера мислити категоріями ризику, контексту та пропорційності. Принцип безпеки за замовчуванням і за дизайном, який проходить через увесь зміст статті, має на меті не реактивний, а превентивний захист системи.

Статті 33 і 34 вводять механізм повідомлення про порушення безпеки даних. Контролер повинен у короткі строки інформувати наглядовий орган про інцидент, якщо існує ризик для прав і свобод фізичних осіб; а в окремих випадках повідомлення має бути адресовано й самим суб'єктам даних. Це перетворює кібербезпеку з технічної дисципліни на правове зобов'язання, а інцидент – на потенційне порушення прав людини.

Заключні положення GDPR щодо призначення Data Protection Officer, оцінки впливу на захист даних та взаємодії з наглядовими органами формують завершений контур відповідальності. Вони демонструють, що захист персональних даних є безперервним процесом, який охоплює і правові, і організаційні, і технологічні елементи.

У сукупності ключові статті GDPR вибудовують нову філософію обробки даних: дані – це не ресурс, яким розпоряджається організація, а елемент особистої свободи, що належить людині. GDPR переводить цю філософію у практичні механізми, які вимагають від контролерів дисципліни,

відповідальності й прозорості, а суб'єктам даних надають інструменти реального контролю. Саме тому регламент став першою універсальною моделлю, яка визначила глобальні стандарти у сфері цифрової приватності.

Інституційна система забезпечення кібербезпеки та захисту персональних даних в Україні.

Інституційна архітектура кібербезпеки та захисту персональних даних в Україні формується відповідно до положень Конституції України, стратегічних актів у сфері національної безпеки (Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» [105]) та профільних законів, що визначають повноваження суб'єктів у цій сфері. В умовах стрімкої цифровізації та гібридної агресії структурована система державних органів забезпечує стійкість інформаційного середовища держави та гарантує реалізацію прав громадян на захист персональних даних.

Центральною ланкою стратегічного рівня виступає Рада національної безпеки і оборони України, яка відповідно до Закону України «Про національну безпеку України» [106] визначає державну політику у сфері кібербезпеки та затверджує стратегічні документи, що встановлюють пріоритети функціонування цифрового простору. Її рішення, введені в дію указами Президента, мають зобов'язуючий характер і забезпечують координацію усіх органів виконавчої влади у реагуванні на загрози в кіберпросторі.

Оперативно-координаційну функцію виконує Національний координаційний центр кібербезпеки при РНБО, створений для моніторингу, прогнозування та аналізу кіберзагроз, а також організації міжвідомчої взаємодії. НКЦК забезпечує інтеграцію інформації, що надходить від Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, Національної поліції України, Міністерства оборони, Міністерства цифрової трансформації та недержавного сектора. Така координація створює єдиний ситуаційний простір для протидії загрозам національної кіберстійкості.

Державна служба спеціального зв'язку та захисту інформації України виконує ключові функції у сфері технічного та криптографічного захисту інформації. Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [100], Держспецзв'язку уповноважена здійснювати сертифікацію засобів криптографічного захисту, впровадження комплексних систем захисту інформації та державну експертизу таких систем. У її структурі діє CERT-UA – національний центр реагування на комп'ютерні інциденти, що забезпечує оперативний моніторинг загроз і реагування на кібератаки.

Служба безпеки України реалізує контррозвідувальні заходи у сфері кібербезпеки та виконує функції протидії кібертероризму, кібератакам та іншим діям, що можуть завдати шкоди національній безпеці. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [99] СБУ визначено одним із головних суб'єктів кібербезпеки, що здійснює виявлення, розслідування та запобігання загрозам, спрямованим на критичну інформаційну інфраструктуру.

МЦТ формує державну політику у сфері цифрової трансформації та відповідає за інтеграцію принципів кібербезпеки у системи електронного врядування. Мінцифри здійснює також нормотворчу діяльність у сфері цифрової безпеки та координує процес адаптації законодавства України до європейських стандартів, зокрема положень Регламенту ЄС 2016/679 (GDPR).

Нарешті, незалежним наглядовим органом у сфері захисту персональних даних є Уповноважений Верховної Ради України з прав людини, чия діяльність ґрунтується на Законі України «Про захист персональних даних» [101]. Уповноважений здійснює контроль за додержанням прав суб'єктів даних, проводить перевірки, розглядає скарги та має повноваження щодо застосування заходів впливу до порушників. Його інституційна роль наближається до моделі європейських органів захисту даних, що забезпечує відповідність України міжнародним стандартам.

Таким чином, інституційна система забезпечення кібербезпеки і захисту персональних даних в Україні має комплексний і багаторівневий характер, що дозволяє забезпечувати стратегічне планування, оперативне реагування, технічний та наглядовий контроль у цифровому середовищі. Така структура є важливим інструментом захисту інформаційного суверенітету держави та гарантування прав людини в умовах сучасного кіберпростору.

4.3. Інституційно-правові підходи до кібербезпеки та захисту персональних даних в країнах-членах ЄС

Нормативно-правові підходи країн Європейського Союзу у сфері кібербезпеки та захисту персональних даних формуються на основі єдиного інтегрованого правового простору, що істотно вирізняє ЄС серед інших регіональних об'єднань. Право на захист персональних даних у Європейському Союзі має статус фундаментального і закріплене вже на рівні первинного права – у Статті 8 Хартії основних прав ЄС [107] та статті 16 Договору про функціонування ЄС. Така конституціоналізація інформаційної безпеки означає, що держави-члени ЄС формують своє національне законодавство насамперед через призму захисту прав людини, а обов'язок забезпечувати приватність і безпеку даних стає не просто інституційною функцією, а нормою правопорядку.

Ключовим елементом європейського підходу до регулювання персональних даних є Загальний регламент про захист даних (GDPR), який має пряму дію в державах-членах і встановлює уніфіковані правила для всіх сфер обробки даних. Його концепція ґрунтується на принциповій та технологічно нейтральній моделі: незалежно від того, які технології використовуються, обробка має відповідати основним принципам законності, прозорості, пропорційності, мінімізації та забезпечення цілісності даних. Водночас у регламенті закладено ризик-орієнтований підхід, який зобов'язує контролера визначати масштаб і характер технічних та організаційних заходів залежно від

можливих ризиків для прав і свобод суб'єктів даних. Суттєвою рисою європейської моделі є також принцип підзвітності, який вимагає не лише дотримуватися вимог, а й уміти довести це через відповідні політики, реєстри, процедури оцінки впливу, аудит безпеки та інші механізми доказового комплаєнсу.

Окремо врегульована сфера обробки персональних даних у діяльності правоохоронних органів, де застосовується Директива 2016/680 (LED). На відміну від GDPR, вона підлягає транспозиції в національне законодавство, однак відтворює ті самі фундаментальні принципи, доповнюючи їх специфічними режимами, необхідними для проведення кримінальних розслідувань. Цей документ зберігає баланс між ефективністю діяльності правоохоронних органів і гарантіями захисту приватності, зокрема шляхом встановлення чітких обмежень щодо цільової обробки, використання даних у різних стадіях розслідування та забезпечення незалежного нагляду з боку національних органів із захисту даних.

У сфері кібербезпеки система нормативного регулювання ЄС також демонструє системність та багаторівневість. Директива NIS, у модернізованій редакції NIS 2, формує спільний підхід до захисту критичної інфраструктури в усіх державах-членах. Вона зобов'язує держави розробляти національні стратегії кібербезпеки, створювати компетентні органи та національні команди реагування (CSIRT), а операторів критично важливих секторів – запроваджувати комплексні системи управління кіберризиками, повідомляти про кіберінциденти та проходити посилений нагляд з боку держави. Новий підхід у NIS 2 характеризується розширенням переліку секторів, посиленням відповідальності керівних органів компаній та встановленням суворіших санкцій, що підсилює режим безпеки на рівні ЄС.

Важливим нормативним елементом є Регламент «Cybersecurity Act», який не лише закріплює постійний мандат Європейського агентства з кібербезпеки (ENISA), а й створює єдину європейську рамку сертифікації кібербезпеки для продуктів, послуг і процесів. Це означає, що виробники цифрових технологій

можуть проходити сертифікацію за єдиними стандартами, які визнаються на всій території ЄС, а національні органи діють у межах гармонізованих процедур.

Ще один сучасний компонент нормативної архітектури – Регламент «Cyber Resilience Act», який поширює обов'язкові вимоги кібербезпеки на всі продукти з цифровими елементами. Він вводить вимоги до безпеки на всіх етапах життєвого циклу продукту, зобов'язує виробників забезпечувати оперативне усунення вразливостей, повідомляти про серйозні інциденти та гарантує, що лише продукти, які відповідають стандартам безпеки, можуть потрапляти на ринок ЄС. Таким чином, кібербезпека стає не лише умовою експлуатації, а характеристикою якості продукту з моменту його створення.

Характерною рисою європейського нормативного підходу є поєднання наднаціонального й національного регулювання. ЄС визначає базові вимоги через регламенти та директиви, тоді як держави-члени деталізують їх у своїх правопорядках; таким чином забезпечується високий, але уніфікований рівень захисту цифрового середовища. Усі країни ЄС зобов'язані мати незалежні органи захисту даних, національні агентства кібербезпеки, CSIRT-команди, а також ефективні механізми контролю та санкції. Загальною тенденцією є також упровадження risk-based та security-by-design підходів, які вимагають вбудовувати вимоги безпеки у проєктні рішення, продукти, сервіси та інфраструктуру.

Нормативно-правові підходи Європейського Союзу до кібербезпеки й захисту персональних даних формують спільне регуляторне поле, однак у межах цього поля кожна держава вибудовує власну модель, яка відображає її політичні пріоритети, технічний потенціал та історичний досвід. Німеччина демонструє тенденцію до правового формалізму і багаторівневого інституційного контролю. Її нормативна система ґрунтується на Федеральному законі про захист даних (BDSG), який адаптовано для гармонізації з GDPR, але доповнено суворішими правилами щодо обробки чутливих даних, зокрема у сфері працевлаштування. У сфері кібербезпеки Німеччина дотримується моделі, орієнтованої на інфраструктурну стійкість: Закон про безпеку інформаційних технологій (IT-

Sicherheitsgesetz 2.0) покладає на операторів критичної інфраструктури розширені обов'язки щодо забезпечення технічного та організаційного захисту, а також зобов'язує повідомляти про інциденти Федеральному відомству з безпеки інформаційних технологій (BSI). Така система відображає німецький інституційний підхід, що поєднує технологічну експертизу, правовий порядок і чітку відповідальність суб'єктів.

Франція, на відміну від Німеччини, розвиває свою модель навколо понять цифрового суверенітету та активного державного втручання. Національна комісія з інформатики і свобод (CNIL) відіграє роль авторитетного регулятора, який формує не лише юридичну, а й етичну рамку застосування технологій. Французьке законодавство про персональні дані тісно інтегроване з GDPR, однак робить акцент на розширених правах суб'єкта даних та суворих санкціях за порушення. У сфері кібербезпеки Франція акцентує на посиленні оборонного компоненту: Агентство з національної безпеки інформаційних систем (ANSSI) має повноваження, що виходять за межі технічного аудиту, включно з можливістю видавати обов'язкові до виконання інструкції для операторів стратегічних сервісів. Французький підхід поєднує регулятивну жорсткість із прагненням встановити державний контроль над цифровим простором.

Естонія у цьому контексті вирізняється тим, що стала одним із перших у світі «цифрових суспільств», і її нормативна система вибудувана на парадигмі цифрової довіри. Ретельно продуманий закон про інформаційну безпеку, законодавство про публічні послуги та електронну ідентифікацію утворюють нормативну основу, у якій кібербезпека є не оборонним інструментом, а технічною передумовою функціонування держави. Після масштабної кібератаки 2007 року Естонія стала ініціатором створення Центру кібероборони НАТО і запровадила модель розподіленої цифрової інфраструктури (X-Road), що забезпечує горизонтальний обмін даними між установами з одночасним дотриманням суворих правил конфіденційності. В межах застосування GDPR Естонія відзначається більш технологічною інтерпретацією регламенту,

інтегруючи його з системою е-ідентичностей, що робить її нормативне поле одним із найпрогресивніших у Європі.

Нідерланди репрезентують ліберально-інноваційну модель, що розглядає кібербезпеку як елемент національної економічної стратегії. Закон про захист персональних даних (Uitvoeringswet AVG) [108] адаптує GDPR до національних потреб без запровадження надмірних обмежень, роблячи акцент на прозорості, відповідальності та співпраці між державою і приватним сектором. У галузі кібербезпеки Нідерланди реалізують підхід, побудований на партнерстві: Національний центр кібербезпеки (NCSC) координує співпрацю між державними структурами, бізнесом і критичною інфраструктурою, а законодавство визначає обов'язки щодо обміну інформацією про інциденти та мінімізацію ризиків. У цій моделі держава виступає не стільки регулятором, скільки фасилітатором спільної цифрової безпеки.

Узагальнюючи підходи цих країн, можна виокремити кілька важливих тенденцій. По-перше, у всіх випадках законодавство щодо захисту персональних даних є результатом глибокої інтеграції з GDPR, однак національні системи демонструють різні акценти – від інституційної жорсткості у Німеччині до технологічної гнучкості в Естонії. По-друге, у сфері кібербезпеки спостерігається різний ступінь централізації: Франція і Німеччина орієнтовані на державне керівництво, Нідерланди та Естонія – на партнерські моделі. По-третє, відмінності між країнами демонструють, що нормативно-правові підходи до кібербезпеки визначаються не лише законодавчими рамками ЄС, а й політичними пріоритетами, культурою управління та рівнем цифрової зрілості суспільства.

Саме взаємодія наднаціонального регулювання з національними моделями створює багатовимірну правову картину кібербезпеки в Європі, де GDPR задає загальні стандарти приватності, а директиви NIS і національні стратегії кібербезпеки формують інфраструктурні й організаційні механізми захисту. Цей багаторівневий підхід перетворює ЄС на один із найпослідовніших і найвпливовіших гравців у сфері цифрового регулювання на глобальному рівні.

Італія демонструє модель, у якій захист персональних даних тісно інтегрований із концепцією етичного використання цифрових технологій. Центральним актором тут виступає Garante per la protezione dei dati personali – один із найвпливовіших і найавтономніших наглядових органів Європи. Італійське законодавство про персональні дані (Codice in materia di protezione dei dati personali), адаптоване під вимоги GDPR, зберегло історичну традицію підвищених гарантій для чутливих категорій даних і містить детальні приписи щодо обробки даних у медичній, трудовій та банківській сферах. У сфері кібербезпеки Італія обрала шлях стратегічної централізації: створення Agenzia per la Cybersicurezza Nazionale (ACN) стало відповіддю на потребу інтегрувати оборонні, розвідувальні та технічні механізми захисту в єдину систему. Італійська модель орієнтована на державний контроль, але водночас робить наголос на регламентуванні процедур реагування на інциденти й обов'язковому дотриманні технічних стандартів, що формуються на європейському рівні.

В Іспанії нормативно-правова модель відзначається гнучкістю й адаптивністю. Закон про захист персональних даних та гарантії цифрових прав (LOPDGDD) [109], який імплементує GDPR, став одним із перших прикладів законодавства, що не лише копіює європейські норми, а й доповнює їх принципово новими категоріями. Іспанія першою у світі ввела поняття «цифрових прав громадян» – цифрової спадщини, права на мережеву недоторканність, цифрової освіти. Регулятор AEPD відіграє значну роль у просуванні культури приватності, пропонуючи рекомендації, що впливають на практику організацій. У кібербезпеці Іспанія дотримується моделі розподіленої відповідальності: INCIBE та Національний криптологічний центр координують діяльність між державними установами, військовими структурами і приватним сектором, формуючи модель, у якій кібербезпека є спільним суспільним обов'язком.

Польща становить цікавий приклад нормативної еволюції у країні, що за останні роки значно посилила цифрові інститути. Закон RODO (національна версія GDPR) імплементований з акцентом на регуляторну суворість і чіткість

процедур. Польський регулятор UODO отримав широкі повноваження щодо накладання санкцій та контролю за обробкою даних. У той же час польський підхід до кібербезпеки зосереджений на побудові національної кібернетичної стійкості: Закон про кібербезпеку 2018 року створив структуру CSIRT-команд на державному, національному та військовому рівнях, а також запровадив обов'язки для операторів критичних систем щодо повідомлення інцидентів і дотримання стандартів. Польща приділяє окрему увагу загрозам, пов'язаним з іноземним втручанням та кіберрозвідкою, що відображає її геополітичну чутливість.

Швеція, хоча й має один із найстаріших у Європі законів про персональні дані (Personuppgiftslagen), після ухвалення GDPR повністю переформатувала свою нормативну модель. Шведський регулятор Datainspektionen, перейменований на Integritetsskyddsmyndigheten, став одним із найбільш «проактивних» наглядових органів у ЄС. Швеція традиційно підтримує відкрите цифрове середовище, але її законодавство встановлює особливо високі вимоги до обробки даних у державному секторі, включно з відкритими реєстрами та електронним урядуванням. Кібербезпека у Швеції має оборонний характер: Державне агентство цивільної оборони та Шведське агентство із захисту інформаційних систем співпрацюють у межах моделі «загальної оборони», що поєднує військові, цивільні й технологічні структури. Цей підхід виходить з того, що цифрова інфраструктура не відокремлена від національної безпеки.

Таким чином, нормативно-правові підходи країн ЄС вирізняються високим рівнем інтегрованості, пріоритетністю прав людини, стандартизованістю вимог і посиленим регуляторним наглядом. Європейський Союз створив комплексну модель, у якій захист даних і кібербезпека взаємодіють не як окремі сфери, а як елементи цілісної системи цифрової безпеки. Саме така архітектура забезпечує баланс між інноваціями, ринковим розвитком, технологічним прогресом і правами громадян, задаючи орієнтири для третіх країн, включно з Україною, яка сьогодні рухається шляхом гармонізації свого законодавства з європейськими стандартами.

4.4. Напрями удосконалення кіберзахисту персональних даних в умовах євроінтеграції

Удосконалення української системи кіберзахисту та охорони персональних даних потребує концептуального оновлення, що має спиратися і на загальноєвропейські стандарти, і на порівняльний аналіз національних відмінностей між Україною та державами ЄС. Розрив між нормативними режимами не є суто технічним – він відображає різні рівні інституційної зрілості, характер правової культури та історичну еволюцію регуляторних моделей. Тому стратегія вдосконалення українського законодавства має враховувати не лише вимоги євроінтеграції, а й динаміку розвитку європейського цифрового простору, який давно перетворився на систему обов'язкових стандартів, а не лише рекомендаційних рамок.

Передусім необхідна переорієнтація української моделі захисту персональних даних у бік тієї нормативної логіки, яку закріплює GDPR. У Європейському Союзі право на захист персональних даних є фундаментальним, з окремим конституційним статусом, а отже, будь-які відхилення в регуляторній практиці автоматично розглядаються як порушення прав людини. В Україні ж це право поки що опосередковане через загальні положення про приватність, що суттєво звужує його практичну дієвість. Реформа ЗУ «Про захист персональних даних» [101], повинна стати не лише технічною імплементацією GDPR-подібної термінології, а повноцінним інституційним реформуванням: необхідно надати наглядовому органу реальні повноваження, включно з можливістю застосовувати санкції, співмірні з європейськими. Така модернізація створить не тільки правові гарантії для громадян, а й економічну передбачуваність для бізнесу, що працює в умовах глобальної цифрової конкуренції.

Порівняльний аналіз також засвідчує, що українське секторне правоохоронне регулювання потребує реконфігурації. У ЄС директива LED створює скоординовану систему стандартів для обробки даних у кримінальних розслідуваннях, тоді як українські підходи залишаються фрагментарними,

розпорошеними між КПК, законами про оперативно-розшукову діяльність, СБУ, поліцію та іншими органами. Гармонізація з європейськими зразками не зводиться до імплементації окремих положень, а має включати запровадження єдиних процедурних принципів: обмеження доступу, незалежний нагляд, підзвітність і контрольний механізм оскарження. Лише сумісність із цими стандартами відкриє шлях до повноцінної участі в європейських механізмах обміну інформацією у сфері правопорядку (табл. 4.2).

Таблиця 4.2

Порівняльна таблиця нормативно-правових підходів України та ЄС у сфері захисту персональних даних і кібербезпеки

Критерій порівняння	Європейський Союз	Україна
Правовий статус права на захист персональних даних	Конституційний рівень: ст. 8 Хартії основних прав ЄС, ст. 16 ДФЄС. Право є фундаментальним.	Конституційно закріплене право на приватність (ст. 32 Конституції), але захист даних не виділений як окреме фундаментальне право.
Базовий акт у сфері персональних даних	GDPR – Регламент прямої дії, єдиний для всіх країн ЄС; обов'язкове застосування без імплементації.	ЗУ «Про захист персональних даних» (2010) – побудований на моделі Директиви 95/46/ЕС; триває реформа (законопроєкт № 8153 для гармонізації з GDPR).
Секторальне правоохоронне регулювання	Директива 2016/680 (LED), транспозиція в національні правопорядки; стандартизовані гарантії у кримінальних розслідуваннях.	Специфічної LED-подібної конструкції немає; регулювання фрагментоване між КПК, законами про оперативно-розшукову діяльність, СБУ та поліцію.
Наглядовий орган у сфері персональних даних	Незалежний Data Protection Authority (DPA) у кожній країні; координація через Європейську раду із захисту даних (EDPB).	Уповноважений ВРУ з прав людини виконує функції DPA; незалежний статус забезпечено, але повноваження та інституційна спроможність значно вужчі, ніж у DPA ЄС.
Максимальні санкції за порушення	До 20 млн євро або 4 % світового обороту компанії (GDPR).	Санкції значно нижчі; відсутня шкала, співмірна з GDPR; у проєкті № 8153 передбачено підсилення.
Головний акт у сфері кібербезпеки	Директива NIS 2 – спільні стандарти для критичних секторів; наднаціональна гармонізація; обов'язкові CSIRT, стратегії, нагляд.	Закон «Про основні засади забезпечення кібербезпеки України» – закладає основу системи, однак рівень деталізації та обов'язкових вимог нижчий, ніж у NIS 2.

Критерій порівняння	Європейський Союз	Україна
Інституційна модель кібербезпеки	Сильні національні агентства (ANSSI, BSI, CISA-IT тощо), CSIRT, європейська координація через ENISA.	НКЦК при РНБО як координаційний орган, Держспецзв'язку, CERT-UA, СБУ, кіберполіція; інституції створені, але потребують зміцнення ресурсів і технічної спроможності.
Сертифікація кібербезпеки продуктів	«Cybersecurity Act» – єдина європейська рамка сертифікації (ENISA), рівні basic/substantial/high.	Наявні національні механізми КСЗІ; відсутня гармонізована модель сертифікації на зразок європейської.
Безпека цифрових продуктів і послуг	«Cyber Resilience Act» (CRA) – обов'язкові вимоги безпеки до всіх продуктів із цифровими елементами у ЄС.	Порівнянного режиму поки немає; напрями адаптації лише декларуються в стратегічних документах та рамках євроінтеграції.
Підхід до ризиків	Ризик-орієнтований підхід у GDPR, NIS 2, CRA; обов'язкові DPIA, security-by-design та supply chain security.	Українське законодавство містить окремі елементи risk-based підходу, але вони не є системними; DPIA не обов'язкові (змінюється в законопроєкті № 8153).
Механізми міжнародної співпраці	Участь у колективних структурах: ENISA, EDPB, європейські CSIRT, кіберінформаційний обмін.	Міжнародне співробітництво переважно через НАТО, США, ЄС; інтеграція до європейських механізмів поки що часткова.
Рівень гармонізації	Повна уніфікація між країнами ЄС: регламенти та директиви створюють єдиний правовий простір.	Україна перебуває у фазі поступового зближення; нормативна база ще не відповідає повністю стандартам ЄС.

Складено авторами.

Окремим напрямом удосконалення є формування інституційної моделі кібербезпеки, здатної не формально, а по суті виконувати функції, аналогічні тим, що реалізують ANSSI у Франції, BSI у Німеччині чи естонські кіберструктури. Уже існуюча система, що включає НКЦК, Держспецзв'язку, CERT-UA, СБУ та кіберполіцію, потребує не стільки розширення, скільки оптимізації. ЄС давно перейшов до моделі, за якої національні агентства поєднують регулятивну, аналітичну та технічну функції, а політика кібербезпеки не розділяється на оборонну та цивільну частини, а є інтегрованою. Для України це означає необхідність інституційного зближення, зміцнення технічної спроможності, запровадження обов'язкових стандартів для критичної

інфраструктури та системного використання європейських механізмів – від NIS 2 до ENISA-подібних моделей сертифікації.

Сертифікаційна сфера – ще один елемент, у якому різниця між ЄС і Україною особливо помітна. Європейський «Cybersecurity Act» створив єдину рамку сертифікації цифрових продуктів, яка встановлює рівні довіри й дозволяє ринку функціонувати в межах уніфікованих стандартів. Українські механізми КСЗІ, хоч і відіграли важливу історичну роль, уже не відповідають складності сучасних технологічних ланцюгів. Створення гармонізованої моделі сертифікації не лише посилить внутрішню стійкість ринку, а й стане передумовою для взаємного визнання сертифікатів із ЄС, що критично важливо для інтеграції у спільний цифровий простір.

Україна також має переглянути свій підхід до ризик-орієнтованого регулювання. ЄС у GDPR, NIS 2 та CRA заклав системне бачення ризику як ключового параметра у прийнятті рішень, що стосується як компаній, так і державних органів. Українське законодавство лише наближається до цієї логіки, але без повноцінного впровадження DPIA, security-by-design чи вимог до безпеки ланцюгів постачання воно не зможе досягти рівня сумісності з європейськими стандартами. Перехід до ризик-орієнтованої моделі є не технічною, а концептуальною зміною: він потребує нової культури управління, в якій безпека не оцінюється як реакція на загрози, а як постійна превентивна діяльність.

Водночас, на відміну від ЄС, Україна не має розвиненої системи міжнародної інтеграції у сфері кібербезпеки та захисту даних. Хоч співпраця з НАТО, США і структурами ЄС є інтенсивною, вона не замінює повноцінної участі у таких механізмах, як ENISA, європейські CSIRT-мережі або EDPB. Поступовий доступ до таких платформ є не лише політичним кроком, а елементом фахового обміну, без якого неможливо забезпечити стійкість у середовищі, де загрози є транснаціональними й динамічними.

Удосконалення кіберзахисту та системи охорони персональних даних в Україні потребує комплексного підходу, який має враховувати досвід країн Європейського Союзу, водночас спираючись на власні інституційні реалії та

стратегічні виклики. Аналіз нормативних моделей Німеччини, Франції, Естонії, Нідерландів, Італії, Іспанії, Польщі та Швеції дозволяє сформувати бачення того, як Україна може розвивати свою національну систему безпеки у цифровому середовищі. Йдеться не про копіювання окремих елементів, а про вироблення узгодженої доктрини, де технічні стандарти, правові норми та інституційна структура функціонують у єдиній логіці державної цифрової стійкості.

Україні насамперед необхідно зміцнити нормативну основу кібербезпеки шляхом переходу від реактивних моделей до превентивної архітектури, подібної до тієї, яку успішно впровадили Німеччина та Франція. Йдеться про запровадження обов'язкових стандартів для операторів критичної інфраструктури, регулярних аудитів, механізмів повідомлення про інциденти та формування системи державного нагляду, здатного не лише фіксувати порушення, а й встановлювати стратегічні технічні вимоги. Для України це означає створення стійкої інституційної вертикалі, яка поєднуватиме компетенції кібероборони, цивільної безпеки та національного регулятора, а також матиме дієві інструменти впливу на приватний сектор.

Разом із тим українська система має рухатися у напрямі, що охоплює не тільки оборонні механізми, а й розвиток цифрової довіри. Естонський досвід демонструє, що по-справжньому ефективний кіберзахист можливий лише у поєднанні з сучасною інфраструктурою електронної ідентифікації, прозорими державними реєстрами та високим рівнем взаємодії між органами влади. Україна вже має передумови для такого розвитку, однак потребує подальшого вдосконалення міжвідомчих протоколів обміну даними, впровадження єдиних технічних правил для державних інформаційних систем і створення більш гнучких цифрових сервісів, де безпека не відокремлена від функціональності, а інтегрована у технологічний дизайн.

Окрема увага має бути приділена удосконаленню законодавства про персональні дані, яке, попри значний прогрес, все ще тяжіє до фрагментарності та не повністю узгоджене з нормами GDPR. Європейські підходи показують, що сучасна модель захисту даних не обмежується правовими деклараціями, а

вимагає чітких механізмів дії: права на доступ, виправлення, видалення та перенесення даних мають отримати дієві процедурні форми, а контролери – обов'язок впроваджувати принципи «захисту за дизайном» і «захисту за замовчуванням». Це також передбачає розбудову спроможного, незалежного наглядового органу з реальними повноваженнями, який зможе виконувати для України ту функцію, яку виконує CNIL у Франції чи Datainspektionen у Швеції.

Важливою складовою удосконалення є формування партнерської моделі, подібної до нідерландської, у якій держава не тільки встановлює вимоги, але й активно співпрацює з бізнесом і громадянським суспільством у питаннях кіберзахисту. Україна може суттєво підвищити стійкість цифрового середовища, створивши механізми систематичного обміну інформацією про загрози, одночасно дотримуючись високих стандартів конфіденційності. Така модель передбачає розвиток кіберволонтерства, галузевих центрів реагування та спільних платформ аналізу інцидентів.

Не менш важливим напрямом є розбудова оборонної складової кібербезпеки за прикладом Польщі та Франції, де кіберзахист розглядається не лише як технологічний інструмент, а як елемент національної стійкості. Для України, яка перебуває у стані військової агресії та постійних кібероперацій проти державних і приватних ресурсів, інтеграція кібероборони, стратегічної розвідки та цивільного захисту набуває першочергового значення. Це потребує як розвитку фахових кадрів, так і створення умов для координації на всіх рівнях – від локальних адміністрацій до центральних органів влади.

Узагальнюючи, можна сказати, що стратегія вдосконалення української системи кіберзахисту та захисту персональних даних має рухатися у напрямі глибокої євроінтеграційної трансформації. Вона передбачає підсилення інституцій, модернізацію законодавства, гармонізацію стандартів, розвиток сертифікаційних механізмів та інтеграцію в європейські мережі. Важливо, щоб ці зміни відбувалися не як вимушена адаптація під зовнішні вимоги, а як внутрішньо вмотивований проект побудови цифрової держави, для якої приватність, безпека та довіра є не деклараціями, а функціональною основою

розвитку. Україна, спираючись на досвід ЄС та власні потреби, може вибудувати модель, у якій кібербезпека стає одним із ключових елементів національної стійкості, а захист персональних даних – справжнім інструментом захисту людської гідності в цифрову епоху.

Таким чином, для України оптимальною є модель, що поєднує превентивну нормативну базу, інституційну централізацію без надмірної бюрократизації, технологічну інтеграцію державних сервісів, незалежний і впливовий наглядовий орган, партнерство держави та бізнесу, а також стратегічний компонент кібероборони. Усі ці елементи разом формують не просто політику кібербезпеки, а цілісну цифрову екосистему, в якій захист даних і безпека інформаційних систем стають не реакцією на загрозу, а основою цифрового розвитку держави та суспільства.

4.5. Забезпечення інформаційної безпека в освітніх інформаційних системах в умовах євроінтеграції: аспекти захисту персональних даних

Для забезпечення безпеки персональних даних критично важливим інструментом є кіберзахист. Насамперед, це пов’язано з тим, що в умовах цифрової трансформації значна частина особистої інформації громадян зберігається, обробляється та передається в електронному вигляді через інформаційні системи, які можуть стати об’єктом кібератак. Без належного технічного та організаційного захисту персональні дані стають вразливими до несанкціонованого доступу, викрадення, маніпуляцій чи витоку, що може призвести до порушення прав людини, зловживань з боку третіх осіб і втрати довіри до цифрових сервісів. Ефективний кіберзахист дозволяє гарантувати конфіденційність, цілісність і доступність персональних даних відповідно до принципів законності та добросовісної обробки.

У ЄС підходи система кіберзахисту базуються на принципах системного управління ризиками, захисту даних за замовчуванням і на етапі проєктування

(privacy&security by design and by default [110]), а також на концепції багаторівневого захисту (defence in depth [111]). Основна ідея полягає в тому, що кібербезпека не є окремим технічним інструментом, а невід'ємною частиною загальної цифрової екосистеми. Відповідно, захист даних має впроваджуватись не лише технічними засобами, а й через нормативне регулювання, інституційні рамки, стандартизацію процесів та освіту користувачів. Велика увага приділяється моделюванню загроз, оцінці вразливостей, відповідності систем вимогам стандартів (ISO/IEC 27001 [112], NIST [113–115] тощо) та безперервному вдосконаленню заходів захисту.

Окрему роль відіграють правові документи ЄС, зокрема GDPR, що встановлює вимоги до безпеки персональних даних, та Директива (EU) 2016/1148 (NIS Directive), яка визначає кіберзахист як обов'язковий елемент для операторів критично важливої інфраструктури [116]. Ці підходи ґрунтуються на принципі проактивності – держава та оператори повинні не чекати на інцидент, а постійно оцінювати ризики, розробляти політики безпеки та впроваджувати запобіжні заходи. Крім того, велике значення надається прозорості, підзвітності та координації на рівні держав – членів ЄС через спільні структури, зокрема ENISA (Агентство ЄС з кібербезпеки), яка формує методичні підходи до безпеки в цифровому середовищі.

Зупинимося більш детально на аналізі GDPR. Загальний регламент захисту даних ЄС 2016/679 Європейського парламенту і Ради від 27.04.2016 щодо захисту фізичних осіб у зв'язку з обробкою персональних даних і щодо вільного переміщення таких даних набув чинності 25.05.2018. Він є обов'язковим правовим актом, що регламентує збір, обробку, зберігання та використання персональних даних фізичних осіб на території ЄС, а також для компаній і організацій за межами ЄС, які обробляють дані громадян Євросоюзу [117].

Основні принципи GDPR:

– Законність, справедливість і прозорість – персональні дані мають оброблятися на законних підставах і прозоро для суб'єкта даних.

– Цільове обмеження – дані збираються лише для чітко визначених і легітимних цілей.

– Мінімізація даних – збір лише необхідного мінімуму інформації.

– Точність – забезпечення актуальності даних.

– Обмеження зберігання – зберігання даних не довше, ніж це потрібно.

– Цілісність і конфіденційність – захист даних від несанкціонованого доступу.

– Підзвітність – організації повинні доводити відповідність вимогам GDPR.

Основні права фізичних осіб згідно з GDPR:

- Право на доступ до своїх даних.
- Право на виправлення або видалення («право на забуття»).
- Право на обмеження обробки.
- Право на перенесення даних.
- Право на заперечення проти обробки.
- Право не бути підданим автоматизованому прийняттю рішень.

GDPR є базовим стандартом цифрових прав у ЄС. GDPR встановлює високий рівень захисту особистої інформації та відповідальність організацій. За порушення передбачені штрафи до 20 млн євро або 4 % від річного світового обороту компанії – залежно від того, що більше.

У свою чергу питання кіберзахисту персональних даних регулюється низкою інших правових актів.

Директива про конфіденційність та електронні комунікації (Директива 2002/58/ЕС (ePrivacy Directive) регулює обробку даних у сфері електронного зв’язку, включаючи cookies, електронну пошту, телефонію. Забезпечує конфіденційність комунікацій та забороняє несанкціонований доступ до них. GDPR і ePrivacy доповнюють одне одного, але перша стосується загальних даних, а друга – електронного зв’язку [118].

Директива про безпеку мережевих і інформаційних систем (Директива (EU) 2016/1148 (NIS Directive) є першою загальноєвропейською директивою

щодо кібербезпеки, що встановлює вимоги для держав і операторів критичної інфраструктури (транспорт, енергетика, охорона здоров'я тощо). Також положення Директиви зобов'язують повідомляти про кіберінциденти [116].

Директива (EU) 2022/2555 (NIS2 Directive), яка набрала чинності у 2023 році, розширює охоплення секторів і компаній (освіта, державні органи тощо); посилює нагляд, звітність та штрафи за порушення. Також країни ЄС мали імплементувати NIS2 до жовтня 2024 року [119].

Регламент (EU) 2018/1725 застосовується до інституцій та органів ЄС (Єврокомісія, Європарламент). Можна сказати, що це «внутрішній GDPR» для інституцій Євросоюзу [120].

Data Governance Act (Регламент (EU) 2022/868) створює механізми управління даними в ЄС, а також спрямований на безпечний обмін публічними та приватними даними між організаціями [121].

Підсумовуючи здійснений аналіз інституційно-правової основи кіберзахисту в ЄС можна стверджувати, що методичні підходи до захисту персональних даних ґрунтуються на інтегрованій моделі, яка поєднує технічні, організаційні та управлінські компоненти. У центрі уваги є концепція системного управління ризиками, що передбачає ідентифікацію, оцінювання та постійний моніторинг загроз для інформаційних систем. В межах цього підходу великого значення набуває впровадження захисту на всіх етапах життєвого циклу цифрових продуктів: від проектування до експлуатації. Принципи «захисту за задумом» і «захисту за замовчуванням» реалізуються через вбудовані механізми контролю доступу, шифрування, а також мінімізацію обробки даних і багаторівневу архітектуру безпеки.

Ключовим методологічним напрямом є забезпечення багаторівневого захисту (defence in depth), що передбачає розміщення взаємодоповнюючих засобів безпеки на кількох рівнях: фізичному, мережевому, прикладному тощо. Така модель гарантує стійкість до проникнень, забезпечуючи безперервне виявлення, ізоляцію та реагування на інциденти. Значна увага приділяється стандартизації процедур захисту, впровадженню систем управління

інформаційною безпекою, розвитку культури кібергігієни серед користувачів, а також посиленню внутрішнього контролю і підзвітності. У сукупності ці підходи спрямовані на забезпечення цілісності, конфіденційності та доступності даних у цифровому середовищі.

На тлі усталених європейських підходів до забезпечення кіберзахисту, що базуються на системному управлінні ризиками, стандартизованих процедурах безпеки та багаторівневій архітектурі захисту, актуальним постає аналіз того, яким чином подібні принципи впроваджуються в українській практиці. З огляду на посилення цифровізації державного управління та освіти, особливо в умовах воєнного стану, питання формування національної системи кібербезпеки, зокрема в частині захисту персональних даних набуває стратегічного значення. Тож далі зосередимся на особливостях нормативно-інституційного забезпечення кіберзахисту в Україні, а також на практичних механізмах захисту персональних даних у національних інформаційних системах управління освітою.

В Україні концептуальні засади кібербезпеки визначаються низкою нормативно правих актів. Базовим законодавчим актом є Закон України «Про національну безпеку України» [106], яким визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.

Важливим документом також є Указ Президента України від 26 березня 2021 року № 96/2021 «Про Стратегію кібербезпеки України» [122]. Стратегія була спрямована на зміцнення національного кіберпростору, захист критичної інфраструктури, підвищення кіберстійкості державних органів, підприємств та громадян, а також розвиток партнерства з приватним сектором і міжнародними

організаціями. Документ передбачає формування ефективної системи реагування на кіберзагрози, удосконалення нормативно-правового поля та розвиток кадрового потенціалу у сфері кіберзахисту. Стратегія є основою для планування та реалізації державних програм, нормативних актів і механізмів взаємодії суб'єктів сектору безпеки в умовах зростаючих кіберризиків.

Інституційною основою забезпечення кібербезпеки є відповідні органи державної влади, серед яких Державна служба спеціального зв'язку та захисту інформації України [123].

Серед основних функцій Державної служби спеціального зв'язку та захисту інформації України є здійснення ліцензування та контроль за дотриманням законодавства у сфері кібербезпеки. Зокрема, на сайті установи наведено перелік законодавчих та нормативно-правових актів, що визначають провадження ліцензованої діяльності у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. Також до її функцій належить також формування вимог до комплексних систем захисту інформації (КСЗІ), що забезпечують захист від несанкціонованого доступу, витоку або знищення персональних даних.

Загалом в Україні сформовано інституційно-правову основу для забезпечення кібербезпеки, що забезпечує комплексний підхід до управління у сфері безпеки, зокрема інформаційної та кібербезпеки, із розмежуванням повноважень між державними органами, встановленням системи координації та контролю, а також демократичного нагляду над безпековими структурами.

Особливу увагу в системі кіберзахисту приділено захисту персональних даних, що є одним із ключових елементів інформаційної безпеки. Забезпечення конфіденційності, цілісності та доступності персоналізованої інформації потребує впровадження як організаційних, так і технічних механізмів безпеки, включно з криптографічним захистом, контролем доступу, аудитом систем і застосуванням політик безпеки. Це особливо важливо для систем, які

обробляють великі обсяги чутливих даних громадян, зокрема в галузях освіти, охорони здоров'я та державного управління.

У свою чергу, доцільно наголосити, що нормативно-правове забезпечення у сфері захисту персональних даних в Україні охоплює низку актів, серед яких закони «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про захист персональних даних», а також положення щодо електронного документообігу та електронних довірчих послуг. Це свідчить про системне регулювання, що охоплює правові, організаційні та технічні аспекти зберігання, обробки та передачі персональних даних.

Поряд з цим, у нинішніх умовах війни та широкомасштабної цифровізації, що спричиняє зростання загроз у кіберпросторі важливо забезпечити практичну реалізацію положень національного законодавства з урахуванням кращих європейських практик. Це передбачає зокрема адаптацію української системи захисту персональних даних до норм та стандартів ЄС.

Вищезазначене дає змогу говорити, що загалом в Україні сформовано нормативно-інституційну базу, яка забезпечує комплексний підхід до кібербезпеки та захисту персональних даних, зокрема в освітніх інформаційних системах. Законодавче регулювання, зокрема в межах національної безпеки, створює умови для координації між органами влади, які відповідають за інформаційну безпеку, та запроваджує контроль за їхньою діяльністю. Особливої актуальності набуває впровадження принципів безпеки в управлінські, адміністративні та аналітичні цифрові платформи освіти, які акумулюють великі обсяги персоналізованих даних учнів, студентів, педагогічного персоналу та батьків.

З огляду на стрімке зростання обсягів персональних даних, що обробляються в освітніх інформаційних системах, варто окремо зупинитися на питаннях створення комплексної системи захисту інформації (КСЗІ) для ПАК «АІКОМ». Адже на сьогодні ПАК «АІКОМ» є централізованим інструментом управління освітніми процесами, що акумулює чутливу інформацію про учасників освітнього процесу. Виключна важливість ПАК «АІКОМ» для

системи освіти України вимагає впровадження надійних організаційно-технічних рішень для захисту даних відповідно до національних стандартів безпеки та європейських підходів до персоналізованої цифрової освіти.

Слід наголосити, що у ПАК «АІКОМ» реалізовано системний підхід до захисту інформації, що відповідає вимогам національного законодавства України та враховує найкращі міжнародні практики. Основною метою є забезпечення цілісності, конфіденційності та доступності персональних і службових даних у межах освітнього середовища. ПАК «АІКОМ» містить великий обсяг персональної інформації про здобувачів освіти, педагогічних працівників та управлінський персонал, що обумовлює високі вимоги до безпеки платформи.

По-перше, важливим елементом захисту є комплексна система інформаційної безпеки класу АС-3 (автоматизована система 3-го класу, яка обробляє персональні дані, інформацію з обмеженим доступом, що не становить державної таємниці, але потребує захисту від несанкціонованого доступу) та гарантований рівень захисту № 2, тобто такий, що забезпечує досить високий ступінь стійкості до більшості типових загроз: несанкціонованого доступу, витоку інформації через канали побічних випромінювань, зловмисних дій користувачів тощо, яка включає засоби розмежування доступу, ідентифікації користувачів, контролю повноважень та протоколювання дій. Завдяки цьому унеможливлюється несанкціонований доступ до інформації, кожна дія в системі реєструється, що дозволяє здійснювати моніторинг та аудит активності. Застосовується багаторівнева система авторизації, яка забезпечує доступ до даних виключно в межах наданих повноважень.

По-друге, використовується застосування сучасних криптографічних засобів захисту – зокрема, протоколів SSL/TLS для безпечної передачі даних у мережі, а також алгоритмів шифрування AES та RSA для зберігання конфіденційної інформації. Такий підхід дозволяє гарантувати захист даних як на фізичному, мережевому, прикладному рівнях передачі та під час зберігання.

Додатково впроваджено механізми резервного копіювання, що забезпечують відновлення критичної інформації у випадку технічних збоїв або кібератак.

По-третє, забезпечення антивірусного захисту та моніторингу загроз. ПАК «АІКОМ» використовує сертифіковані засоби виявлення та блокування шкідливих програм, системи захисту від атак типу DdoS та SQL-ін'єкцій. В умовах зростаючих кіберзагроз особливої уваги надається постійній актуалізації безпекових політик, оновленню захисного ПЗ та навчанню адміністраторів системи принципам кібергігієни.

В умовах воєнного стану ПАК «АІКОМ» демонструє високу адаптивність до нових кіберзагроз і підтримує стійку цифрову інфраструктуру освітнього менеджменту.

У свою чергу, в умовах воєнного часу та стрімкого впровадження цифрових рішень в освіті особливо важливо забезпечити практичну реалізацію положень національного законодавства щодо захисту персональних даних з урахуванням кращих європейських практик. Це включає адаптацію освітніх інформаційних систем до принципів конфіденційності за замовчуванням і на етапі проєктування, інтеграцію стандартів управління інформаційною безпекою та підвищення рівня цифрової компетентності персоналу. Такий підхід не лише мінімізує ризики витоку або зловживання чутливою інформацією, а й сприяє підвищенню довіри до державних освітніх сервісів та гарантує дотримання прав суб'єктів персональних даних у цифровому середовищі.

Для всебічного розуміння сучасних викликів та пріоритетів у сфері захисту персональних даних в освітніх інформаційних системах доцільно здійснити порівняльний аналіз інституційно-правових підходів до кібербезпеки в Україні та ЄС. Такий підхід дозволяє ідентифікувати як спільні засади, на яких ґрунтується політика безпеки в обох юрисдикціях, так і структурні відмінності, що впливають на ефективність реалізації політик захисту даних (табл. 4.3).

Представлена порівняльна табл. 4.3 демонструє, що підходи ЄС і України до забезпечення кібербезпеки та захисту персональних даних мають спільні засадничі елементи, однак відрізняються ступенем інституційної зрілості, рівнем

інтеграції стандартів та силою механізмів контролю. Якщо в ЄС акцент робиться на системне управління ризиками, підзвітність і прозорість в обробці даних, то в Україні домінує модель з переважанням державного контролю та акцентом на впровадження КСЗІ як ключового інструменту захисту.

Таблиця 4.3

Порівняння інституційно-правових підходів до кібербезпеки та захист даних в інформаційних системах

Критерії порівняння	Європейський Союз	Україна
Загальний підхід	Інтегрована модель управління ризиками; кіберзахист як частина цифрової екосистеми	Комбінована модель з акцентом на інституційну координацію та державне регулювання
Правова база	GDPR, ePrivacy Directive, NIS Directive, NIS2, Data Governance Act	Закон «Про національну безпеку України», Указ про Стратегію кібербезпеки, закони «Про захист персональних даних» тощо
Органи регулювання	ENISA, національні органи держав-членів	ДССЗЗІ, СБУ, Мінцифри
Принципи захисту даних	Privacy by design/default, мінімізація даних, багаторівневий захист	КСЗІ, контроль доступу, криптографія, політики конфіденційності
Обов’язкі операторів (технічних адміністраторів) систем	Регулярна оцінка ризиків, повідомлення про інциденти, підзвітність	Виконання вимог КСЗІ, аудит безпеки, дотримання технічних регламентів
Методи технічного захисту	Шифрування, контроль доступу, аудит, протоколювання, антивірусний захист	Захист каналів зв’язку (SSL/TLS), резервне копіювання, антивірусні системи
Стандарти безпеки	ISO/IEC 27001, NIST Cybersecurity Framework	Національні вимоги до КСЗІ, адаптація до ISO стандартів
Права суб’єктів даних	Право на доступ, виправлення, забуття, заперечення, перенесення даних	Закріплено в законодавстві, але потребує оновлення і гармонізації зі стандартами ЄС
Механізми нагляду та санкцій	Адміністративні штрафи, аудит, контроль відповідності	Державний нагляд, ліцензування, обмежені санкційні механізми

Складено авторами.

У свою чергу, у відповідь на зростання кіберзагроз, особливо в умовах війни та масової цифровізації, держава переглядає усталені підходи, замінюючи формалізовані механізми більш динамічними системами управління ризиками. Яскравим свідченням цього стала розробка нового закону у квітні 2025 року, що

суттєво змінює регуляторну архітектуру у сфері захисту персональних даних і кіберінфраструктури. Закон України № 4336-IX від 17 квітня 2025 року позначає якісний перехід у політиці кіберзахисту держави від формального підходу до ризик-орієнтованого управління. Уперше на законодавчому рівні закріплено створення цілісної національної системи реагування на кіберінциденти, зокрема через мережу CERT-UA (Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України) та галузеві регіональні структури, що формуються державними і муніципальними органами. Особливо важливим є запровадження системного обміну інформацією про кіберзагрози, що дозволить не лише швидше реагувати на інциденти, а й формувати превентивні стратегії. Відмова від жорстко регламентованих КСЗІ на користь гнучкого управління ризиками – ключова трансформація, що наближає українську практику до підходів ЄС і NIST. Новий закон також посилює кадрову спроможність державних установ, передбачаючи введення посад фахівців з кібербезпеки, і змінює акценти у контролі: замість формального звітування передбачено аудит із фокусом на ефективність, а не на формальне дотримання вимог [124].

Проведений аналіз засвідчує, що в Україні формується нова парадигма кіберзахисту, яка орієнтується на відхід від жорстких нормативно-технічних конструкцій на кшталт обов'язкових КСЗІ на користь динамічної, ризик-орієнтованої моделі. Особливої актуальності це набуває у сфері захисту персональних даних, де традиційна система забезпечення інформаційної безпеки не завжди адекватно реагує на сучасні кіберзагрози. Водночас, нова законодавча ініціатива (Закон України № 4336-IX) чітко окреслює вектор змін: від ізольованого технічного підходу до інтегрованої системи управління інформаційною безпекою на основі міжвідомчої координації, галузевої відповідальності, моніторингу кіберризиків і обміну інформацією.

У контексті освітніх інформаційних систем, таких як ПАК «АІКОМ», ці виклики стають критичними. Адже саме у сфері освіти здійснюється обробка

великих масивів персоналізованих даних дітей, педагогів і батьків, які мають підвищений рівень чутливості. На цьому тлі Україна потребує глибшої гармонізації з правовими, інституційними й технологічними стандартами Європейського Союзу. Зокрема, європейський досвід впровадження GDPR та NIS-директив доводить ефективність таких підходів як «privacy & security by design», багаторівневий (defence in depth) захист, підзвітність та проактивна політика управління кіберризиками.

У світлі викликів війни та масової цифровізації освіти, критично важливо забезпечити гармонізацію підходів до захисту персональних даних в освітніх інформаційних системах. Зокрема, пропонується:

– пришвидшити оновлення законодавства з урахуванням європейських директив (GDPR, NIS2);

– впроваджувати ризик-орієнтовані моделі управління кібербезпекою в освітніх платформах;

– посилити вимоги до технічної захищеності освітніх ІТ-систем на базі міжнародних стандартів ISO/IEC 27001 та NIST;

– забезпечити постійне навчання персоналу освіти основам кібергігієни та правовим аспектам обробки персональних даних;

– інституціоналізувати внутрішній аудит кібербезпеки в освітній сфері як частину загальної політики цифрової трансформації.

Загалом, забезпечення надійного захисту персональних даних в українській освіті вимагає не лише оновлення технічних засобів, а передусім системного реформування політик, процедур і підходів з урахуванням найкращих європейських практик та міжнародних стандартів. Гармонізація із законодавством ЄС є не лише вимогою євроінтеграції, а й нагальною потребою для забезпечення прав, свобод і безпеки громадян у цифрову епоху.

ВИСНОВКИ

1. За результатами оцінки стану розвитку цифровізації системи освіти України в умовах євроінтеграції встановлено, що цифровізація системи освіти України перебуває у фазі активного розвитку, однак характеризується нерівномірністю та фрагментарністю впровадження цифрових рішень. Євроінтеграційний вектор зумовлює необхідність переходу від локальних ІТ-рішень до системного підходу, орієнтованого на стандартизацію даних, інтероперабельність інформаційних систем та прозорість управлінських процесів. Визначенно ключові орієнтири цифрової трансформації освіти як складової інтеграції до Єдиного освітнього простору ЄС та формування передумов для даних-орієнтованої освітньої політики.

2. Аналіз стану розвитку освітніх інформаційних технологій в Україні показав, що освітні інформаційні технології в Україні розвиваються динамічно, охоплюючи електронне діловодство, освітні платформи, інформаційно-аналітичні системи та цифрові сервіси. Водночас їх розвиток стримується недостатньою узгодженістю архітектур, різним рівнем цифрової спроможності закладів освіти та обмеженою інтеграцією між системами. Окреслено пріоритети державної політики у сфері розвитку освітніх ІКТ, зокрема щодо підвищення ефективності управління та якості освітніх даних.

3. У процесі дослідження виявлено, що формування єдиного інформаційного освітнього простору ускладнюється фрагментацією цифрових ресурсів, відсутністю єдиних підходів до управління даними та нерівним доступом до цифрової інфраструктури. Науково-практичний висновок полягає у тому, що ефективний інформаційний освітній простір має базуватися на уніфікованих довідниках, стандартах обміну даними та інтегрованих інформаційних системах.

4. Грунтовний аналіз національних інформаційних систем управління освітою дав змогу встановити, що національні інформаційні системи управління освітою є базовим інструментом забезпечення прозорості, підзвітності та

ефективності управлінських рішень у сфері освіти. Їх роль полягає у централізованому зборі, обробці та аналізі освітніх даних. Також зроблено висновок щодо необхідності розгляду таких систем як елементів критичної державної інфраструктури, що потребують сталого розвитку, нормативного закріплення та інтеграції з іншими державними реєстрами.

5. Дослідження засвідчило наявність системних проблем у функціонуванні та інтеграції національних освітніх інформаційних систем, зокрема дублювання функцій, несумісність форматів даних та складність міжвідомчої взаємодії. Науково-практичний висновок полягає у тому, що ключовим стримуючим чинником є відсутність наскрізних механізмів інтероперабельності та управління життєвим циклом даних. Практичне значення результатів полягає у можливості використання їх для формування комплексних підходів до модернізації освітніх ІС.

6. Визначено критерії та показники ефективності освітніх інформаційних систем. Зокрема, у ході дослідження обґрунтовано необхідність застосування критеріїв і показників ефективності для оцінювання освітніх інформаційних систем. Встановлено, що ефективність таких систем має визначатися не лише технічними характеристиками, а й їх управлінською корисністю, якістю даних та здатністю підтримувати прийняття рішень. Розроблена система критеріїв можу бути використана як інструмент планування модернізації та оцінки результативності цифрових рішень у сфері освіти.

7. Визначено напрями модернізації програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту». Результати дослідження підтвердили, що модернізація ПАК «АІКОМ» є ключовою умовою підвищення ефективності управління освітою та розвитку електронного діловодства. Науково-практичний висновок полягає у доцільності трансформації ПАК «АІКОМ» у системоутворюючу платформу з розвиненими можливостями інтеграції, аналітики та автоматизованого збору освітньої статистики. Практичне значення результатів полягає у можливості їх

використання при формуванні технічних завдань та стратегій подальшої цифровізації.

8. Дослідження показало, що інформаційна платформа «Освіта для ветеранів» виконує важливу соціально-управлінську функцію, забезпечуючи доступ ветеранів до освітніх можливостей в умовах воєнного стану. Практичний висновок полягає у тому, що ефективність платформи залежить від актуальності даних, зручності користування та інтеграції з іншими державними сервісами, що дозволяє використовувати її як інструмент реалізації цільової державної політики.

9. Встановлено, що платформа «Позашкілля» сприяє підвищенню доступності інформації про позашкільну освіту та систематизації даних у цій сфері. Науково-практичний висновок полягає у необхідності подальшого розвитку платформи як інструменту моніторингу та аналітики, що дозволить органам управління оцінювати охоплення та ефективність позашкільних освітніх послуг.

10. Дослідження засвідчило, що платформа «ЗнаЇмо» є важливим інструментом інформаційної підтримки реформи шкільного харчування та формування здорових харчових практик. Практичний висновок полягає у доцільності поєднання просвітницьких функцій платформи з елементами збору та аналізу даних для підвищення ефективності управління відповідною державною політикою.

11. За результатами аналізу встановлено, що платформа «Всеукраїнська школа онлайн» відіграє ключову роль у забезпеченні безперервності навчального процесу в умовах воєнного стану. Практичний висновок полягає у необхідності подальшого розвитку аналітичних інструментів платформи, інтеграції з інформаційними системами управління освітою та посилення її технологічної стійкості.

12. У ході дослідження узагальнено сучасні наукові підходи до забезпечення інформаційної безпеки в освітньому середовищі, які акцентують увагу на комплексності заходів та управлінні ризиками. Практичний висновок

полягає у необхідності поєднання технічних, організаційних і правових механізмів захисту інформації в освітніх системах.

13. Здійснено оцінку інституційно-правових засад кібербезпеки та захисту персональних даних в Україні. Встановлено, що національна система кібербезпеки та захисту персональних даних потребує подальшого вдосконалення з урахуванням специфіки освітньої сфери. Практичний висновок полягає у доцільності посилення нормативного регулювання, визначення відповідальності суб'єктів та впровадження стандартних процедур обробки персональних даних.

14. Проаналізовано інституційно-правові підходи до кібербезпеки та захисту персональних даних в країнах-членах ЄС. Аналіз європейського досвіду засвідчив, що країни ЄС застосовують системний та ризик-орієнтований підхід до кібербезпеки і захисту персональних даних. Практичний висновок полягає у можливості використання цього досвіду для гармонізації українського законодавства та практик з європейськими стандартами.

15. У межах дослідження визначено напрями удосконалення кіберзахисту персональних даних, що включають оновлення законодавства, впровадження ризик-орієнтованих моделей та підвищення цифрової компетентності персоналу. Практичне значення результатів полягає у можливості їх використання при розробленні державних і відомчих програм кібербезпеки в освіті. Встановлено, що забезпечення інформаційної безпеки в освітніх інформаційних системах має здійснюватися на засадах комплексності, відповідності європейським стандартам та системного управління ризиками. Практичний висновок полягає у необхідності інтеграції вимог захисту персональних даних у всі етапи проєктування та функціонування освітніх інформаційних систем як передумови сталого розвитку цифрової освіти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital Education Action Plan 2021–2027. *European Commission*. URL: https://education.ec.europa.eu/focus-topics/digital-education/actions.

2. Цифрова трансформація освіти і науки / М-во освіти і науки України. URL: https://mon.gov.ua/tag/tsifrova-transformatsiya-osviti-i-nauki?&tag=tsifrova-transformatsiya-osviti-i-nauki.

3. Digital Education Outlook 2023 / OECD. URL: https://www.oecd.org/education/digital-education-outlook-2023-c74f03de-en.htm.

4. Data for the SDG4 / UNESCO Institute for Statistics. URL: https://uis.unesco.org/en/topic/sdg4-sustainable-development-goal-4.

5. Про освіту : Закон України від 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text.

6. Council recommendation of 22 May 2018 on key competences for lifelong learning (2018/C 189/01) / European Commission. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01).

7. Про деякі питання державних стандартів повної загальної середньої освіти : постанова Кабінету Міністрів України від 30.09.2020 № 898. URL: https://zakon.rada.gov.ua/laws/show/898-2020-%D0%BF#Text.

8. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 03.03.2021 № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text.

9. Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки : постанова Кабінету Міністрів України від 05.08.2020 № 695. URL: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#n11.

10. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text.

11. Про функціонування Реєстру публічних електронних реєстрів : постанова Кабінету Міністрів України від 01.09.2023 № 969. URL: https://zakon.rada.gov.ua/laws/show/969-2023-%D0%BF#Text.

12. Реєстри та сервіси ЄДЕБО / М-во освіти і науки України. URL: https://mon.gov.ua/reestri-ta-servisi-edebo.

13. Матеріально-технічне забезпечення ЗЗСО в умовах воєнного стану в Україні (2022/2023 н. р.) / ДНУ «Інститут освітньої аналітики». URL: https://iea.gov.ua/wp-content/uploads/2023/11/az_materialno-tehnichne-zabezpechennya-zzso.pdf#:~:text=9,%D0%AF%D0%BA.

14. Школи отримають WI-FI-роутери та веб-камери. *Урядовий кур'єр*. URL: https://ukurier.gov.ua/uk/news/shkoli-otrimayut-wi-fi-routeri-ta-vebkameri/.

15. Дослідження якості організації освітнього процесу в умовах війни у 2022/2023 навчальному році / Державна служба якості освіти. URL: https://sqe.gov.ua/wp-content/uploads/2023/04/yakist-osvity-v-umovah-viyny-web-3.pdf.

16. МОН запровадило новий формат навчання для дітей на окупованих територіях. URL: https://nus.org.ua/2025/06/03/mon-zaprovadylo-novyj-format-navchannya-dlya-ditej-na-okupovanyh-terytoriyah/.

17. Україна: цифрова трансформація освіти як стратегічний шлях до стійкості та інновацій / ДНУ «Інститут освітньої аналітики». URL: https://eurydice.iea.gov.ua/.

18. UNESCO supports 50,000 Ukrainian teachers to safeguard learning amid war / UNESCO. URL: https://www.unesco.org/en/articles/unesco-supports-50000-ukrainian-teachers-safeguard-learning-amid-war.

19. Ukraine's Digital Learning Centres help children catch up on classes / UNICEF. URL: https://www.unicef.org/ukraine/en/stories/digital-learning-centres-help-children-catch-up-on-classes.

20. Learning and School Reforms Continue in Ukraine Despite War Challenges / World Bank. URL: https://www.worldbank.org/en/news/feature/2025/03/25/learning-and-school-reforms-continue-in-ukraine-despite-war-challenges.

21. Digital Competence Framework for Educators (DigCompEdu) / European Commission. URL: https://joint-research-centre.ec.europa.eu/digcompedu_en.

22. Концептуально-референтна Рамка цифрової компетентності педагогічних й науковопедагогічних працівників. URL: https://osvita.diia.gov.ua/uploads/0/2622-ramka_cifrovoi_kompetentnosti_ pedagogicnih_j_naukovo_pedagogicnih.pdf.

23. *Овчарук О. В.* Роль інструментів моніторингу самооцінювання цифрової компетентності вчителів у подоланні викликів в Україні та зарубіжжі. *Освітня аналітика України.* 2025. № 1 (33). С. 17–27. DOI: https://doi.org/ 10.32987/2617-8532-2025-1-17-27.

24. Про створення робочої групи з розроблення опису цифрової компетентності педагогічного працівника: наказ Міністерства освіти і науки України від 15.01.2019 № 38. URL: https://mon.gov.ua/npa/pro-stvorennya-robochoyi-grupi-z-rozroblennya-opisu-cifrovoyi-kompetentnosti-pedagogichnogo-pracivnika.

25. Концепція цифрової трансформації освіти і науки: МОН запрошує до громадського обговорення / М-во освіти і науки України. URL: https://mon.gov.ua/news/kontseptsiya-tsifrovoi-transformatsii-osviti-i-nauki-mon-zaproshue-do-gromadskogo-obgovorennya.

26. Вебпортал ПАК «АІКОМ». URL: https://aikom.iea.gov.ua/.

27. Автоматичне заповнення звітів та формування замовлень на виготовлення документів. *АС «Школа»*. URL: https://school.osvita.net/.

28. Ще більше цифрових можливостей: система «Єдина школа» приєдналася до АІКОМ. *Нова Українська школа*. URL: https://nus.org.ua/2023/08/16/shhe-bilshe-tsyfrovyh-mozhlyvostej-systema-yedyna-shkola-pryyednalasya-do-aikom/.

29. Інтегрована система електронної ідентифікації ID.GOV.UA. URL: https://id.gov.ua/.

30. Вебпортал «Мрія». URL: https://web.mriia.gov.ua/Welcome?ReturnUrl=%2F.

31. Дія.Підпис. URL: https://ca.diia.gov.ua/.

32. ПАК «АІКОМ» поповнила нова освітня інформаційна система «Всеосвіта» / ДНУ «Інститут освітньої аналітики». URL: https://iea.gov.ua/aikom-popovnyla-nova-osvitnya-informaczijna-systema-vseosvita/.

33. Єдина державна електронна база з питань освіти (ЄДЕБО). URL: https://info.edbo.gov.ua/.

34. Інформаційна система управління освітою (ІСУО). URL: https://isuo.org/.

35. EDdy : освітня платформа. URL: https://eddy.org.ua/.

36. HUMAN : каталог шкіл. URL: https://www.human.ua/schools.

37. Моя Школа : освітня платформа. URL: https://moiashkola.ua/.

38. Всеосвіта : освітній портал. URL: https://vseosvita.ua.

39. Просвіта : освітня платформа. URL: https://prosvita.net.

40. Smart School : електронна освітня система. URL: https://smart-school.com.ua/.

41. NIT School : електронна освітня система. URL: https://nit.school/.

42. E-Schools : освітня платформа. URL: https://e-schools.info/.

43. *Литвинчук О., Терещенко Г., Кир'янов А., Криворучко Ю., Сологуб Я.* Інформаційна безпека в освітніх інформаційних системах в умовах цифрової трансформації та євроінтеграції: аспекти захисту персональних даних. *Освітня аналітика України.* 2025. № 2 (34). С. 48–65. DOI: https://doi.org/10.32987/2617-8532-2025-2-48-65.

44. *Abramov E.* Adaptation of the military personnel transferred to the reserve as the instrument of ensuring their competitiveness in labor market. *Economics and organization of management.* 2016. № 2 (22). P. 259–265. URL: https://jeou.donnu.edu.ua/article/view/4818.

45. *Kirilova Yu., Znovyak V., Kazanska A.* Needs and Obstacles of Veterans in Employment. June–July 2023. Sociological Study. *Ukrainian Veterans Foundation of the Ministry of Veterans Affairs of Ukraine*. 2023. 87 p. URL: https://veteranfund.com.ua/wp-content/uploads/2023/07/Zvit_pereshkodi_precevlashtuvanii.pdf.

46. *Lavreniuk L. V.* Analysis of the Social Protection System for Veterans and Military Personnel. Ukraine : National Endowment for Democracy. 2022. 141 p. URL: https://legal100.org.ua/wp-content/uploads/2022/08/2022-Bila-kniga.pdf.

47. EU4Recovery – Empowering communities in Ukraine (EU4RECOVERY). *UNPD Ukraine*. URL: https://www.undp.org/uk/ukraine/projects/eu4recovery-rozshyrennya-mozhlyvostey-hromad-v-ukrayini-eu4recovery.

48. 10 million euro invested in vocational education – the Skills4Recovery project kicks off / Ministry of Education and Science of Ukraine. URL: https://mon.gov.ua/news/10-mln-evro-dlya-sferi-profesiynoi-osviti-startuvav-proekt-skills4recovery.

49. Навчання та перепідготовка кваліфікованої робочої сили для відбудови України. *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH*. URL: https://www.giz.de/en/worldwide/141163.html.

49. Вебпортал «Освіта для ветеранів». URL: https://osvitaveteraniv.gov.ua/.

50. Позашкільна освіта / М-во освіти і науки України. URL: https://mon.gov.ua/tag/pozashkilna-osvita?&type=all&tag=pozashkilna-osvita.

51. Про позашкільну освіту : Закон України від 22.06.2000 № 1841-III. URL: https://zakon.rada.gov.ua/laws/show/1841-14#Text.

52. Науково-аналітична діяльність : аналітика / ДНУ «Інститут освітньої аналітики». URL: https://iea.gov.ua/diyalnist/naukovo-analitichna-diyalnist/analitika/.

53. Досягнення і виклики дошкільної, загальної середньої, позашкільної та інклюзивної освіти у 2020–2022 роках / М-во освіти і науки України. URL: https://mon.gov.ua/news/dosyagnennya-i-vikliki-doshkilnoi-zagalnoi-serednoi-pozashkilnoi-ta-inklyuzivnoi-osviti-u-2020-2022-rokakh.

54. Про організацію освітнього процесу в закладах позашкільної освіти у 2021/2022 навчальному році : лист Міністерства освіти і науки України від 17.08.2021 № 1/9-414. URL: https://rada.info/upload/users_files/44037815/552b0bcb583785e079f4a5c54b7d93be.pdf.

55. Дистанційне навчання / М-во освіти і науки України. URL: https://mon.gov.ua/osvita-2/pozashkilna-osvita/distantsiyne-navchannya?utm.

56. *Захарова А., Ніколайко Н., Румянцева Ю.* Довідка за результатами моніторингового дослідження (вивчення питання) щодо забезпечення доступу до якісної позашкільної освіти / Державна служба якості освіти України. Київ, 2023. URL: https://sqe.gov.ua/wp-content/uploads/2023/07/Monitoringove_doslidzhennya_pozashkilna_osvita_SQE-2023.pdf.

57. Пропозиції щодо вирішення проблем учасників освітнього процесу в умовах воєнного стану. *Освітній омбудсмен України*. URL: https://eo.gov.ua/propozytsii-sluzhby-osvitnoho-ombudsmena-shchodo-vyrishennia-problem-uchasnykiv-osvitnoho-protsesu-v-umovakh-voiennoho-stanu/2022/08/18/.

58. Про підготовку закладів освіти до нового навчального року та опалювального сезону в умовах воєнного стану : лист Міністерства освіти і науки України від 11.07.2022 № 1/7707-22. URL: https://zakon.rada.gov.ua/rada/show/v7707729-22#Text.

59. Підлітки та їхнє життя під час війни. Клуб добродіїв. Plan international. 2023. URL: https://auyc.org.ua/wp-content/uploads/2023/08/doslidzhennya-pidlitky-ta-yihnye-zhyttya-pid-chas-vijny-nastroyi-czinnosti-majbutnye.pdf.

60. Позашкільна освіта – проблеми, пропозиції та нові формати роботи. *Освітній омбудсмен України*. URL: https://eo.gov.ua/pozashkilna-osvita-problemy-propozytsii-ta-novi-formaty-roboty/2023/09/19/.

61. *Барладим В. М.* ІКТ в позашкільній освіті: огляд ресурсів для підлітків. *Збірник тез звітної наукової конференції ІІТЗН*. 2013. № 3. С. 124–128. URL: https://lib.iitta.gov.ua/id/eprint/10352/1/%D0%A2%D0%B5%D0%B7%D0%B8_03_2013_%D0%B7%D0%B2%D0%B8%D1%82%D0%BD%D0%B0_%D0%98%D0%98%D0%A2%D0%97%D0%9D.pdf.

62. Позашкільні заклади та освітні центри. *Офіційний портал Києва*. URL: https://kyivcity.gov.ua/dity_dytiachi_sadky_ta_shkoly/pozashkilni_zaklady_ta_osvitni_tsentry/.

63. Освіта. *Відкриті дані Львова*. URL: https://opendata.city-adm.lviv.ua/group/education.

64. У МОН відбулася всеукраїнська нарада з питань позашкільної освіти / М-во освіти і науки України. URL: https://mon.gov.ua/news/u-mon-vidbulasya-vseukrainska-narada-z-pitan-pozashkilnoi-osviti.

65. За цифровізацією – майбутнє освіти. І не лише через пандемію, – заступник Міністра освіти. *Децентралізація*. URL: https://decentralization.ua/news/14251.

66. Про збір відомчої адміністративної звітності дошкільної, загальної середньої та позашкільної освіти у 2022/2023 н. р. : наказ Міністерства освіти і науки України від 06.09.2022 № 795. URL: https://osvita.ua/legislation/Ser_osv/87400/.

67. Міністерствоосвіти і науки України та SoftServe оголосили про стратегічне партнерство. *European Business Association*. URL: https://eba.com.ua/ministerstvo-osvity-i-nauky-ukrayiny-ta-softserve-ogolosyly-pro-strategichne-partnerstvo/.

68. Вебпортал «Позашкілля». URL: https://pozashkillia-test.iea.gov.ua/#/.

69. Офіційний сайт платформи «Знаїмо». URL: https://znaimo.gov.ua.

70. Розпочала роботу платформа про здорове харчування у школах «Знаїмо» / М-во освіти і науки України. URL: https://mon.gov.ua/ua/news/rozpochala-robotu-platforma-pro-zdorove-harchuvannya-u-shkolah-znayimo.

71. Оперативні дані за результатами моніторингу впровадження реформи шкільного харчування : на нове меню перейшли понад 96 % закладів освіти України / М-во освіти і науки України. URL: https://mon.gov.ua/news/operativni-dani-za-rezultatami-monitoringu-vprovadzhennya-reformi-shkilnogo-kharchuvannya-na-nove-menyu-pereyshli-ponad-96-zakladiv-osviti-ukraini.

72. Деякі питання реалізації Стратегії реформування системи шкільного харчування на період до 2027 року : розпорядження Кабінету Міністрів України від 07.11.2025 № 1216-р. URL: https://zakon.rada.gov.ua/laws/show/1216-2025-%D1%80#Text.

73. Про схвалення Стратегії реформування системи шкільного харчування на період до 2027 року та затвердження операційного плану заходів з її реалізації у 2023-2024 роках : розпорядження Кабінету Міністрів України від 27.10.2023 № 990-р. URL: https://zakon.rada.gov.ua/laws/show/990-2023-%D1%80#Text.

74. Дайджест реформи шкільного харчування за 2023-2024 рр. URL: https://znaimo.gov.ua/media/news/%D0%94%D0%B0%D0%B9%D0%B4%D0%B6%D0%B5%D1%81%D1%82%20%D1%80%D0%B5%D1%84%D0%BE%D1%80%D0%BC%D0%B8%20%D1%85%D0%B0%D1%80%D1%87%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_06-24.pdf.

75. Дайджест реформи шкільного харчування за травень-грудень 2024 р. URL: https://znaimo.gov.ua/media/pdf/%D0%94%D0%B0%D0%B9%D0%B4%D0%B6%D0%B5%D1%81%D1%82-2_12-24_RGB.pdf.

76. Деякі питання оплати праці працівників державних та комунальних закладів охорони здоров'я : постанова Кабінету Міністрів України від 13.01.2023 № 28. URL: https://zakon.rada.gov.ua/laws/show/28-2023-%D0%BF#Text.

77. Education in a post-COVID world: nine ideas for public action / UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000373717.

78. COVID-19 Response Toolkit. *Global Education Coalition*. URL: https://globaleducationcoalition.unesco.org/response-toolkit.

79. Всеукраїнська школа онлайн. URL: https://lms.e-school.net.ua/.

80. Про затвердження Положення про вебплатформу дистанційного навчання «Всеукраїнська школа онлайн» : наказ Міністерства освіти і науки України від 16.06.2023 № 746. URL: https://zakon.rada.gov.ua/laws/show/z1094-23#Text.

81. *Шопіна І. М.* Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ*. 2023. № 1. С. 28–35. DOI: https://doi.org/10.32782/2311-8040/2023-1-4.

82. Цифрова трансформація науково-освітніх середовищ в умовах воєнного стану : зб. матеріалів. Звітна наукова конференція Інституту цифровізації освіти НАПН України, 23 лютого 2024 р., м. Київ / упоряд. :

О. П. Пінчук, Н. В. Яськова. Київ : ІЦО НАПН України, 2024. 168 с. URL: https://lib.iitta.gov.ua/id/eprint/740554/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7_%D0%B7%D0%B2%D1%96%D1%82%D0%BD%D0%BE%D1%97_2024_v2.pdf?utm.

83. *Laptiev S.* Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Кібербезпека: освіта, наука, техніка.* 2022. № 4 (16). С. 45–62. DOI: https://doi.org/10.28925/2663-4023.2022.16.4562.

84. Освіта під час війни: розвиток інформаційно-аналітичного забезпечення, цифрова трансформація, євроінтеграція : зб. тез доп. V Міжнар. наук.-практич. конф. (наукове електронне видання), 26 жовт. 2023 р. Київ : ДНУ «Інститут освітньої аналітики», 2023. 216 с.

85. *Дрейс Ю.* Заходи захисту персональних даних в інформаційних (автоматизованих) системах : зб. тез І Всеукр. наук.-практич. конф., 7 вересня 2015, Одеса : ОНАЗ. 2015. С. 29–32. URL: https://er.nau.edu.ua/server/api/core/bitstreams/3cf7c187-93ea-4786-85f2-1be9c569a931/content.

86. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах / Г. М. Гулак та ін. *Сучасний захист інформації*. 2017. № 2 (30). С. 65–71. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/1491.

87. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : зб. тез доп. Всеукр. наук. інтернет-конф. (м. Тернопіль, 25–26 квіт. 2014 р.). Тернопіль : Тайп, 2014. 106 с. URL: http://www.konferenciaonline.org.ua/data/downloads/file_1633503018.pdf#page=31.

88. *Корченко О., Дрейс Ю., Лозова І.* Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т. 18. № 1. С. 39–47.

89. *Краснощок В. М., Шестак Я. І.* Захист інформації в прикладних інформаційних системах. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/73a54273-0b6e-432c-93a7-881a9ee0c186/content.

90. *Гнатюк С. Л.* Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти : аналіт. доп. Київ : НІСД, 2014. 92 с. URL: https://www.niss.gov.ua/sites/default/files/2015-01/Druk_Gnatuk1.indd-8b6f2.pdf.

91. *Легка О. В.* Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2 (31). С. 74–79.

92. *Кальченко В., Ободяк В.* Порівняльна характеристика нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах. *Інформаційні технології та суспільство*. 2024. № 5 (11). С. 14–20. DOI: https://doi.org/10.32689/maup.it.2023.5.2.

93. *Кальченко В., Ободяк В., Пугач І.* Нормативні вимоги України в сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах у порівнянні з вимогами сша та ЄС. *Вісник Херсонського національного технічного університету.* 2024. № 2 (89). С. 162–169. DOI: https://doi.org/10.35546/kntu2078-4481.2024.2.23.

94. *Romansky R.* Internet of Things and User Privacy Protection. *37th International Conference on Information Technologies*. 2023. URL: http://infotech-bg.com/proceedings.

95. *Brown R., Truby J., Imad A.* Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies*. 2022. Vol. 9, Iss. 1. URL: https://sciendo.com/issue/EUSTU/9/1/.

96. *Zhang Y., Dong H.* Criminal law regulation of cyber fraud crimes – from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*. 2023. Vol. 12, 64. URL: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00437-3#citeas.

97. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр.

98. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

99. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

100. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

101. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

102. Convention 108 and Protocols. URL: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

103. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

104. Complete guide to GDPR compliance. URL: https://gdpr.eu/.

105. Про Стратегію забезпечення державної безпеки : Указ Президента України від 16.02.2022 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text.

106. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

107. Charter of fundamental rights of the European Union (2000/C 364/01) / European Communities. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

108. Uitvoeringswet van de Algemene Verordening Gegevensbescherming (UAVG). URL: https://www.considerati.com/nl/kennisbank/uitvoeringswet-algemene-verordening-gegevensbescherming.html.

109. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. URL: https://www.boe.es/eli/es/lo/2018/12/05/3/con.

110. What you need to know about privacy by design. 2024. URL: https://www.cookiebot.com/en/privacy-by-design/.

111. *Treharne J.* Defence in Depth: Why a Multi-Layered Approach is Essential for Cybersecurity in 2024. 2024. URL: https://assureddigitaltech.com/news/defence-in-depth/.

112. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO/IEC 27001:2022. URL: https://www.iso.org/standard/27001.

113. *Pascoe C., Quinn S., Scarfone K.* The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP). *National Institute of Standards and Technology, Gaithersburg, MD*. DOI: https://doi.org/10.6028/NIST.CSWP.29, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957258.

114. How To Spot, Avoid, and Report Tech Support Scams. URL: https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

115. What is the NIST Cybersecurity Framework? URL: https://www.ibm.com/think/topics/nist.

116. Directive (EU) 2016/1148 of the European Parliament and of the Council. *Official Journal of the European Union*. 2016. L 194/1. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

117. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*. 2016. L 119/1. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

118. Directive 2002/58/EC of the European Parliament and of the Council. *Official Journal of the European Union*. 2002. L 201. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058.

119. Directive (EU) 2022/2555 of the European Parliament and of the Council. *Official Journal of the European Union.* 2022. L 333/80. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

120. Regulation (EU) 2018/1725 of the European Parliament and of the Council. *Official Journal of the European Union*. 2018. L 295/39. URL: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

121. Regulation (EU) 2022/868 of the European Parliament and of the Council. *Official Journal of the European Union*. 2022. L 152/1. URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj.

122. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

123. Державна служба спеціального зв'язку та захисту інформації України : офіц. вебсайт. URL: https://cip.gov.ua/ua.

124. Президент України Володимир Зеленський підписав Закон № 4336-IX про кіберзахист державних інформаційних ресурсів / Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: https://cip.gov.ua/ua/news/prezident-ukrayini-volodimir-zelenskii-pidpisav-zakon-4336-ix-pro-kiberzakhist-derzhavnikh-informaciinikh-resursiv.