УДК 37.014.5:004.056.5

Литвинчук А. О.
кандидат економічних наук, старший дослідник, директор ДНУ «Інститут освітньої аналітики», Київ, Україна, a.litvinchuk@iea.gov.ua
ORCID ID: https://orcid.org/0000-0002-7523-558X

Терещенко Г. М.
кандидат економічних наук, заступник директора з науково-організаційної роботи ДНУ «Інститут освітньої аналітики», Київ, Україна, tganna@ukr.net
ORCID ID: https://orcid.org/0000-0002-9458-2843

Кир'янов А. В.
заступник директора з науково-проєктної роботи та ІТ ДНУ «Інститут освітньої аналітики», Київ, Україна, a.kiryanov@iea.gov.ua
ORCID ID: https://orcid.org/0000-0003-0452-7689

Криворучко Ю. М.
молодший науковий співробітник ДНУ «Інститут освітньої аналітики», Київ, Україна, kryvoruchko2025@gmail.com
ORCID ID: https://orcid.org/0009-0007-0494-9749

Сологуб Я. Д.
студент САДМ-51 Державного університету інформаційно-комунікаційних технологій, Київ, Україна, jyariks@gmail.com
ORCID ID: https://orcid.org/0009-0008-5408-9246

ІНФОРМАЦІЙНА БЕЗПЕКА В ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМАХ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА ЄВРОІНТЕГРАЦІЇ: АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. *У статті розглянуто актуальні проблеми забезпечення інформаційної безпеки в освітніх інформаційних системах України в умовах цифрової трансформації та євроінтеграційного курсу держави. Зосереджено увагу на загрозах витоку, несанкціонованого доступу та зловживання персональними даними, які зберігаються й обробляються в освітніх цифрових середовищах, зокрема в такій масштабній системі, як ПАК «АІКОМ». Зазначено, що подальша цифровізація освітнього процесу зумовлює потребу в упровадженні комплексних механізмів кіберзахисту, які поєднують технічні, організаційні та правові інструменти. Стаття окреслює специфіку захисту персональних даних у сфері освіти, акцентуючи на підвищеній чутливості такої інформації. Окрему увагу приділено аналізу європейських підходів до кіберзахисту, що ґрунтуються на принципах «privacy by design and by default», системного управління ризиками й багаторівневої архітектури захисту (defence in depth). Розглянуто ключові регламенти ЄС, як-от GDPR, NIS2, ePrivacy Directive, а також міжнародні стандарти ISO/IEC 27001:2022 і NIST, що визначають вимоги до організації інформаційної безпеки. У межах порівняльного аналізу наведено відмінності між підходами ЄС та України в контексті правового регулювання, інституційної структури, технічних стандартів і прав суб'єктів персональних даних. Наголошено на потребі оновлення національного законодавства відповідно до європейських стандартів. На прикладі ПАК «АІКОМ» продемонстровано практичні аспекти захисту персональних даних в освітніх інформаційних системах, зокрема впровадження криптографічного захисту, багаторівневої авторизації, контролю доступу та систем аудиту. У підсумку наведено рекомендації щодо*

гармонізації української практики з нормами ЄС, які включають удосконалення законодавства, розвиток цифрової компетентності освітян, інституціоналізацію функцій кібербезпеки та посилення захисту прав суб'єктів даних.

Ключові слова: *цифрова трансформація, інформаційна безпека, освітні інформаційні системи, захист персональних даних, євроінтеграція.*

JEL classification: I21, I28, K24, L86.
DOI: 10.32987/2617-8532-2025-2-48-65.

На сучасному етапі розвитку ІКТ у світі питання кібербезпеки стають одними з ключових, зокрема 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 і вчителів до статистичних відомостей про заклади. Водночас недостатній рівень захисту таких систем створює потенційні ризики витоку, зловживання або неправомірного доступу до даних, що може мати 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 потребу в забезпеченні 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 адаптацію українських освітніх інформаційних систем до високих стандартів прозорості, надійності й відповідальності. Це вимагає не лише відповідних технічних рішень, а й розвитку культури цифрової грамотності та правової обізнаності у сфері захисту даних.

Тож, з огляду на зростання ролі цифрових технологій у сфері освіти, пропонована стаття «Інформаційна безпека в освітніх інформаційних системах в умовах цифрової трансформації та євроінтеграції: аспекти захисту персональних даних» є актуальною, а дослідження проблематики інформаційної безпеки в освітньому середовищі – надзвичайно важливим і своєчасним, адже сприятиме розумінню викликів і можливостей цифровізації освіти, а також формуванню комплексного підходу до захисту персональних даних відповідно до сучасних європейських стандартів.

Проблематика інформаційної безпеки в освіті в умовах цифрової трансформації та євроінтеграції є предметом активних наукових пошуків. Досліджуються різні аспекти цієї проблематики, зокрема особливості інформаційної безпеки в процесі цифрової трансформації та шляхи її забезпечення; наводиться визначення цифрової трансформації в телеологічному й діяльнісному аспектах; наголошується на необхідності вжиття дієвих заходів інформаційної

безпеки через зростання кількості та інтенсивності інформаційних загроз у сферах, де цифрова трансформація відбувається найшвидше [1]. Вартий уваги збірник матеріалів наукової конференції Інституту цифровізації освіти НАПН України, що містить доповіді, присвячені розвитку цифрових технологій у відкритій освіті й науці. Учасники конференції описують теоретичні та практичні аспекти проєктування й використання сучасних засобів навчання в комп'ютерно орієнтованому середовищі, зокрема застосування хмарних та імерсивних технологій. Окрему увагу приділено питанням інформаційної безпеки й захисту персональних даних в умовах цифрової трансформації освітнього процесу [2]. Деякі наукові праці присвячено розробленню ефективного підходу до протидії загрозам, пов'язаним із соціальною інженерією в цифровому середовищі [3]. Загалом питання інформаційної безпеки в умовах цифрової трансформації освіти набувають дедалі більшої актуальності. Дослідники наголошують на необхідності створення безпечного інформаційного середовища для реалізації цифрових прав громадян і розвитку сучасної освітньої інфраструктури з урахуванням новітніх технологій.

Якщо говорити про конкретні заходи захисту в інформаційних системах, то є чимало публікацій українських учених на цю тему. 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 [4]. Автори публікацій аналізують основні й додаткові заходи захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах [5], особливості захисту персональних даних в умовах стрімкого розвитку інформаційно-телекомунікаційних технологій [6]; розглядають актуальні загрози, пов'язані з обробкою персональної інформації, та пропонують технічні й організаційні заходи для її убезпечення [7]; наголошують на необхідності захисту персональних даних, які створюються та обробляються прикладним програмним забезпеченням в автоматизованих системах [8]; аналізують сучасні методи захисту персональних даних в інформаційних системах, зокрема в контексті мобільних платформ [9]; обґрунтовують ефективність знеособлення (анонімізації) як методу захисту персональних даних в умовах сучасного цифрового середовища [10].

Таким чином, у сучасних публікаціях українських учених велика увага приділяється заходам захисту персональних даних в інформаційних системах, зокрема в контексті цифровізації освітнього простору, розвитку телекомунікаційних технологій і посилення кіберзагроз. Дослідники аналізують як загальні принципи й моделі захисту, так і практичні методи. Окрему увагу вони приділяють упровадженню комплексних систем безпеки та адаптації підходів до умов роботи хмарних технологій.

У контексті євроінтеграції України огляд сучасних досліджень засвідчує зростання уваги до інформаційної безпеки в умовах цифрової

трансформації освіти, зокрема таких аспектів, як захист персональних даних, гармонізація з європейськими стандартами, зокрема GDPR, і розвиток цифрової компетентності.

Наприклад, стаття О. В. Легкої присвячена розгляду позитивного міжнародного досвіду щодо законотворчої діяльності з питань захисту персональних даних. Дослідницею проаналізовано основні норми міжнародних і вітчизняних нормативно-правових документів, які регулюють питання захисту персональних даних, ключові нововведення GDPR, положення про екстратериторіальність дії GDPR у контексті можливості його застосування щодо фізичних та юридичних осіб України; надано пропозиції стосовно основних шляхів адаптації національного законодавства про захист персональних даних до міжнародних стандартів [11].

Також окремі статті присвячуються аналізу й порівнянню нормативно-правових актів, що регулюють захист персональних даних в Україні, США та ЄС. Автори цих статей підкреслюють, що вітчизняне законодавство, зокрема Закон України «Про захист персональних даних», потребує оновлення й гармонізації з міжнародними стандартами, такими як GDPR і CCPA. Крім того, вони звертають увагу на прогалини в національному законодавстві, зокрема відсутність чітких вимог до кіберзахисту інформаційно-комунікаційних систем, в яких обробляються персональні дані. Автори наголошують на необхідності впровадження в нашій країні найкращих світових практик для підвищення рівня довіри громадян і бізнесу до державних інституцій, а також для стимулювання розвитку цифрової економіки України [12]. Порівняльну характеристику нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах також наводять В. Кальченко і В. Ободяк. Науковці аналізують відмінності між національним законодавством і GDPR щодо захисту персональних даних. У їхній статті наголошується на необхідності адаптації українських нормативних актів до стандартів ЄС для підвищення ефективності захисту персональних даних і розвитку цифрової інфраструктури країни [13]. У контексті євроінтеграційного курсу України сучасні дослідники роблять акцент на необхідності гармонізації національного законодавства у сфері захисту персональних даних з європейськими й міжнародними стандартами, насамперед GDPR. Вони звертають увагу на прогалини в українському правовому полі, зокрема у сфері кіберзахисту інформаційно-комунікаційних систем, що обробляють персональні дані, й підкреслюють потребу в упровадженні ефективних правових та організаційних механізмів.

Зарубіжні публікації присвячено 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) і потреба в нових підходах до цифрової ідентифікації [14]; прогалини в регулюванні штучного інтелекту в рамках ЄС і необхідність узгодження його з положеннями GDPR [15]; кримінально-правова відповідальність за кібершахрайство в епоху edge

computing та виклики, пов'язані із захистом персональної інформації [16].

Згадані та інші численні публікації змальовують цілісну картину міжнародного досвіду з питань забезпечення інформаційної безпеки, підкреслюючи необхідність міждисциплінарного підходу, нормативної адаптації та інтеграції захисту даних у всі сфери цифрової діяльності.

Метою статті є аналіз сучасного стану інформаційної безпеки в освітніх інформаційних системах України, виокремлення ключових ризиків порушення конфіденційності персональних даних і розроблення практичних рекомендацій щодо вдосконалення політики захисту даних відповідно до вимог цифрової трансформації та євроінтеграційних процесів.

Для убезпечення 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 й 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 із боку третіх осіб і втрати довіри до цифрових сервісів. Ефективний кіберзахист слугує гарантією конфіденційності, цілісності й доступності персональних даних відповідно до принципів законності та добросовісної обробки.

В ЄС системи кіберзахисту базуються на принципах системного управління ризиками, захисту даних за замовчуванням і на етапі проєктування (privacy&security by design and by default [17]), а також на концепції багаторівневого захисту (defence in depth [18]). Головна ідея полягає в тому, що кібербезпека не є окремим технічним інструментом, а невід'ємною частиною загальної цифрової екосистеми. Відповідно, захист даних має впроваджуватися 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 [19], NIST [20–22] та ін.) і безперервному вдосконаленню заходів захисту.

Також важливу роль відіграють правові документи ЄС, зокрема GDPR, який встановлює вимоги до безпеки персональних даних, та Директива (EU) 2016/1148 (NIS Directive), що визначає кіберзахист як обов'язковий елемент для операторів критично важливої інфраструктури [23]. Ці підходи ґрунтуються на принципі проактивності: держава й оператори повинні не чекати на інцидент, а постійно оцінювати ризики, розробляти політики безпеки та впроваджувати запобіжні заходи. Крім того, велике значення надається прозорості, підзвітності й координації на рівні держав-членів ЄС через спільні структури, зокрема ENISA (Агентство ЄС із кібербезпеки), що розробляє методичні підходи до безпеки в цифровому середовищі.

Зупинимося детальніше на аналізі GDPR. Загальний регламент Європейського парламенту і Ради (ЄС) 2016/679

про захист даних від 27 квітня 2016 р. набрав чинності 25 травня 2018 р. 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 [24].

Основними принципами GDPR є такі:

– Законність, справедливість і прозорість – персональні дані мають оброблятися на законних підставах та 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 та конфіденційність – захист даних від несанкціонованого доступу.

– Підзвітність – організації повинні доводити відповідність вимогам GDPR.

Основними правами фізичних осіб згідно з GDPR є:

• право на доступ до своїх даних;

• право на виправлення чи 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. Він встановлює високий рівень захисту особистої інформації та відповідальність організацій. За порушення передбачено штрафи до 20 млн євро, або 4 % річного світового обороту компанії (залежно від того, що більше).

У свою чергу, питання кіберзахисту персональних даних регулюється низкою інших правових актів, як-от:

• Директива про конфіденційність та електронні комунікації, або 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 один одну, але перший стосується загальних даних, а друга – електронного зв'язку [25].

• Директива про безпеку мережевих та інформаційних систем, або Директива (EU) 2016/1148 (NIS Directive). Це перша загальноєвропейська директива щодо кібербезпеки, яка встановлює вимоги для держав і операторів критичної інфраструктури (транспорт, енергетика, охорона здоров'я тощо). Також її положення зобов'язують повідомляти про кіберінциденти [23].

• Директива (EU) 2022/2555 (NIS2 Directive). Набрала чинності у 2023 р., розширює охоплення секторів і компаній (освіта, державні органи тощо); посилює нагляд, звітність і штрафи за порушення. Країни ЄС мали імплементувати її до жовтня 2024 р. [26].

• Регламент (EU) 2018/1725. Застосовується до інституцій та органів ЄС (Єврокомісії, Європарламенту), є так званим внутрішнім GDPR для інституцій Євросоюзу [27].

• Регламент (EU) 2022/868 (Data Governance Act). Створює механізми управління даними в ЄС, а також

спрямований на безпечний обмін публічними й приватними даними між організаціями [28].

Проведений аналіз інституційно-правового підґрунтя кіберзахисту в ЄС показав, що методичні підходи до захисту персональних даних базуються на інтегрованій моделі, яка поєднує технічні, організаційні та управлінські компоненти. У центрі уваги – концепція системного управління ризиками, що передбачає ідентифікацію, оцінювання й постійний моніторинг загроз для інформаційних систем. У межах цього підходу великого значення набуває впровадження захисту на всіх етапах життєвого циклу цифрових продуктів – від проєктування 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.

Основним 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. Чимала увага приділяється стандартизації процедур захисту, упровадженню систем управління інформаційною безпекою, розвитку в користувачів культури кібергігієни, а також посиленню внутрішнього контролю й 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, актуалізується питання, яким чином подібні принципи впроваджуються в українській практиці. З огляду на посилення цифровізації державного управління й освіти, особливо в умовах воєнного стану, формування національної системи кібербезпеки, зокрема в частині захисту персональних даних, набуває стратегічного значення. Тож далі зосередимося 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 є Закон України «Про національну безпеку України» [29], який окреслює та розмежовує повноваження державних органів у сферах національної безпеки і оборони, створює підґрунтя для інтеграції політики й процедур органів державної влади, інших державних органів, чиї функції стосуються національної безпеки та оборони, сил безпеки і сил оборони, визначає систему командування, контролю й координації операцій сил безпеки і сил оборони, запроваджує всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектора безпеки і оборони.

Важливим документом є також Указ Президента України «Про Стра-

тегію кібербезпеки України» [30]. Ця стратегія 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. Вона передбачає формування ефективної системи реагування на кіберзагрози, удосконалення нормативно-правового поля та розвиток кадрового потенціалу у сфері кіберзахисту, є основою для планування й реалізації державних програм, нормативних актів і механізмів взаємодії суб'єктів сектора безпеки в умовах зростання кіберризиків.

Інституційним підґрунтям забезпечення кібербезпеки є відповідні органи державної влади, зокрема Державна служба спеціального зв'язку та захисту інформації України [31]. Серед її основних функцій – здійснення ліцензування та контроль за дотриманням законодавства у сфері кібербезпеки. Зокрема, на сайті установи наведено список законодавчих і нормативно-правових актів, що визначають провадження ліцензованої діяльності в галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) і технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. Також до її функцій належить формування вимог до комплексних систем захисту інформації (КСЗІ), що забезпечують захист від несанкціонованого доступу, витоку або знищення персональних даних [32].

Загалом в Україні сформовано інституційно-правове підґрунтя для гарантування кібербезпеки, що забезпечує комплексний підхід до управління у сфері безпеки, зокрема інформаційної й кібербезпеки, з 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, включаючи криптографічний захист, контроль доступу, аудит систем та застосування політик безпеки. Це особливо важливо для систем, які обробляють великі обсяги чутливих даних громадян, зокрема в галузях освіти, охорони здоров'я й державного управління.

У свою чергу, нормативно-правове забезпечення у сфері захисту персональних даних у нашій країні охоплює, зокрема, закони України «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 включає правові, організаційні й технічні аспекти зберігання, обробки та передачі персональних даних.

Поряд із цим в умовах війни та широкомасштабної цифровізації, що спричиняє збільшення загроз у кіберпросторі, важливо забезпечити практичну реалізацію положень національного законодавства з урахуванням найкращих європейських

практик. Це передбачає, зокрема, адаптацію української системи захисту персональних даних до норм і стандартів ЄС.

Зазначене дає підстави для висновку, 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, у т. ч. у межах національної безпеки, створює умови для координації між органами влади, що відповідають за інформаційну безпеку, та запроваджує контроль за їхньою діяльністю. Особливої актуальності набуває впровадження принципів безпеки в управлінські, адміністративні й 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 захисту інформації для програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту» (ПАК «АІКОМ»). Адже на сьогодні він є централізованим інструментом управління освітніми процесами, що акумулює чутливу інформацію про учасників освітнього процесу. Виняткова важливість ПАК «АІКОМ» для вітчизняної системи освіти вимагає впровадження надійних організаційно-технічних рішень для захисту даних відповідно до національних стандартів безпеки та європейських підходів до персоналізованої цифрової освіти.

До речі, у ПАК «АІКОМ» реалізовано системний підхід до захисту інформації, що відповідає вимогам національного законодавства України та враховує найкращі міжнародні практики. Головна мета – забезпечити цілісність, конфіденційність і доступність персональних та службових даних у межах освітнього середовища. ПАК «АІКОМ» містить великий обсяг персональної інформації про здобувачів освіти, педагогічних працівників та управлінський персонал, що зумовлює високі вимоги до безпеки платформи. Основними елементами 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, який забезпечує досить високу стійкість 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 і протоколювання дій. Завдяки цьому унеможливлюється несанкціонований доступ до інформації, кожна дія в системі реєструється, що дає змогу проводити моніторинг та аудит активності. Застосовується багаторівнева система авторизації, яка забезпечує доступ до даних виключно в межах наданих повноважень.

• Сучасні криптографічні засоби захисту, наприклад протоколи SSL/TLS для безпечної передачі даних у

мережі, а також алгоритми шифрування AES та RSA для зберігання конфіденційної інформації. Такий підхід дає змогу гарантувати захист даних на фізичному, мережевому, прикладному рівнях передачі та під час зберігання. Додатково впроваджено механізми резервного копіювання, що забезпечують відновлення критичної інформації в разі технічних збоїв чи кібератак.

• Забезпечення антивірусного захисту та моніторингу загроз. ПАК «АІКОМ» використовує сертифіковані засоби виявлення й блокування шкідливих програм, системи захисту від DdoS-атак і SQL-ін'єкцій. В умовах зростання кіберзагроз особлива увага приділяється постійній актуалізації безпекових політик, оновленню захисного програмного забезпечення та навчанню адміністраторів системи принципів кібергігієни.

Під час дії режиму 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 вкрай важливо забезпечити практичну реалізацію положень національного законодавства щодо захисту персональних даних з урахуванням найкращих 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 чи 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 і пріоритетів у сфері захисту персональних даних в освітніх інформаційних системах доцільно виконати порівняльний аналіз інституційно-правових підходів до кібербезпеки в Україні та ЄС. Такий підхід допомагає ідентифікувати як спільні засади політики безпеки в обох юрисдикціях, так і структурні відмінності, що впливають на ефективність реалізації політик захисту даних (таблиця).

Наведена порівняльна таблиця демонструє, що підходи ЄС і України до забезпечення кібербезпеки та захисту персональних даних мають спільні засадничі елементи, однак відрізняються за ступенем інституційної зрілості, рівнем інтеграції стандартів та силою механізмів контролю. Якщо в ЄС акцент робиться на системному управлінні ризиками, підзвітності й прозорості при обробці даних, то в Україні домінує модель із переважанням державного контролю та акцентом на впровадженні КСЗІ як ключового інструмента захисту.

Слід зауважити, що ще 1 липня 2020 р. Президент України підписав документ, який, по суті, скасовує виконання вимог КСЗІ для держорганів. А точніше, пропонує використовувати замість «застарілого» національного стандарту захисту інформації прийняті в Європі стандарти СУІБ (системи управління інформаційною безпекою, англ. ISMS – Information Security Management System). СУІБ – це сукупність політик, процедур, проце-

Таблиця

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 інституційній координації та державному регулюванні
Правова база	GDPR, ePrivacy Directive, NIS Directive, NIS2, Data Governance Act	Закон України «Про національну безпеку України», Указ «Про Стратегію кібербезпеки України», закони України «Про захист персональних даних» та інші
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'язки 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 стандартів ISO
Права суб'єктів даних	Право на доступ, виправлення, забуття, заперечення, перенесення даних	Закріплено в законодавстві, але потребує оновлення та гармонізації зі стандартами ЄС
Механізми нагляду та санкцій	Адміністративні штрафи, аудит, контроль відповідності	Державний нагляд, ліцензування, обмежені санкційні механізми

Складено авторами.

сів і засобів контролю, що використовуються для системного управління інформаційною безпекою в організації з метою захисту конфіденційності, цілісності та доступності інформації. Зазвичай упроваджується відповідно до міжнародного стандарту ISO/IEC 27001:2022 [19].

Водночас, у відповідь на зростання кіберзагроз, особливо в умовах війни й масової цифровізації, держава переглядає усталені підходи, замінюючи формалізовані механізми більш динамічними системами управління ризиками. Яскравим свідченням цього стало розроблення нового закону у квітні 2025 р., що суттєво змінює регуляторну архітектуру у сфері захисту персональних даних і кіберінфраструктури [33]. Закон України від 17.04.2025 № 4336-IX 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[1] та галузеві регіональні структури, що формуються державними й муніципальними органами. Особливо важливим є запровадження системного обміну інформацією про кіберзагрози, що дасть можливість не лише швидше

[1] CERT-UA – це урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України.

реагувати на інциденти, а й формувати превентивні стратегії. Відмова від жорстко регламентованих КСЗІ на користь гнучкого управління ризиками – це ключова трансформація, яка наближає українську практику до підходів ЄС і NIST. Окрім того, новий закон посилює кадрову спроможність державних установ, передбачаючи введення посад фахівців із кібербезпеки, та змінює акценти в контролі: замість формального звітування передбачено аудит із фокусом на ефективність, а не на формальне дотримання вимог.

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 № 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 ЄС. Зокрема, європейський досвід упровадження GDPR та NIS-директив доводить ефективність таких підходів, як «privacy & security by design», багаторівневий захист (defence in depth), підзвітність і 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);

– упроваджувати ризик-орієнтовані моделі управління кібербезпекою в освітніх платформах;

– посилити вимоги до технічної захищеності освітніх IT-систем на базі міжнародних стандартів ISO/IEC 27001 та NIST;

– забезпечити постійне навчання персоналу освіти основ кібергігієни і правових аспектів 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. Передусім воно вимагає 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.

Список використаних джерел

1. *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.

2. Цифрова трансформація науково-освітніх середовищ в умовах воєнного стану / упоряд.: О. П. Пінчук, Н. В. Яськова. Київ : ІЦО НАПН України, 2024. 168 с. URL: https://tinyurl.com/yc23j2ss.

3. *Лаптєв С. О.* Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Кібербезпека: освіта, наука, техніка.* 2022. Т. 4. № 16. С. 45–62. DOI: https://doi.org/10.28925/2663-4023.2022.16.4562.

4. Освіта під час війни: розвиток інформаційно-аналітичного забезпечення, цифрова трансформація, євроінтеграція : зб. тез доп. V Міжнар. наук.-практ. конф., м. Київ, 26 жовт. 2023 р. Київ : ДНУ «Інститут освітньої аналітики», 2023. 216 с. URL: https://iea.gov.ua/wp-content/uploads/2023/11/book-of-abstracts_ssi-iea_2023.pdf?utm_source=chatgpt.com.

5. *Дрейс Ю. О.* Заходи захисту персональних даних в інформаційних (автоматизованих) системах. *Перспективні напрями захисту інформації* : зб. матеріалів І Всеукр. наук.-практ. конф., м. Одеса, 7–9 верес. 2015 р. Одеса : ОНАЗ 2015. С. 29–32. URL: https://www.researchgate.net/publication/389562867_ZAHODI_ZAHISTU_PERSONALNIH_DANIH_V_INFORMACIJNIH_AVTOMATIZOVANIH_SISTEMAH.

6. 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.

7. *Носулич М. В.* Захист персональних даних в інформаційних системах методом знеособлення. *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. С. 31–33. URL: http://www.konferenciaonline.org.ua/data/downloads/file_1633503018.pdf#page=31.

8. *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. DOI: https://doi.org/10.18372/2410-7840.18.10111.

9. *Краснощок В. М., Шестак Я. І.* Захист інформації в прикладних інформаційних системах. *Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану* / за заг. ред. В. А. Кудінова, К. В. Ярового. Київ : Нац. акад. внутр. справ, 2024. С. 81–83. URL: https://www.researchgate.net/publication/392895306_Zahist_informacii_v_prikladnih_informacijnih_sistemah.

10. *Бакаєв О. О., Суський Г. В.* Методи захисту персональної інформації в інформаційних системах. *Телекомунікаційні та інформаційні технології*. 2024. № 2 (83). С. 68–77. DOI: https://doi.org/10.31673/2412-4338.2024.028190.

11. *Легка О. В.* Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2 (31). С. 74–79. DOI: https://doi.org/10.32836/2521-6473.2021-2.15.

12. *Кальченко В. В., Ободяк В. К., Пугач І. О.* 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.

13. *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.

14. *Romansky R. P.* Internet of Things and User Privacy Protection. *2023 International Conference on Information Technologies (InfoTech).* 2023. DOI: https://doi.org/10.1109/InfoTech58664.2023.10266883.

15. *Brown R., Truby J., Ibrahim I. A.* Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies*. 2022. Vol. 9, Iss. 1. P. 61–90. DOI: https://doi.org/10.2478/eustu-2022-0003.

16. *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. DOI: https://doi.org/10.1186/s13677-023-00437-3.

17. What you need to know about privacy by design. *Cookiebot by Usercentrics*. 2024. URL: https://www.cookiebot.com/en/privacy-by-design/.

18. *Treharne J.* Defence in Depth: Why a Multi-Layered Approach is Essential for Cybersecurity in 2024. URL: https://assureddigitaltech.com/news/defence-in-depth/.

19. ISO/IEC 27001:2022. *ISO*. 2022. URL: https://www.iso.org/standard/27001.

20. *Pascoe C., Quinn S., Scarfone K.* The NIST Cybersecurity Framework (CSF) 2.0 / National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

21. Understanding the NIST cybersecurity framework. *Federal Trade Commission.* URL: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework.

22. What is the NIST Cybersecurity Framework? *IBM*. URL: https://www.ibm.com/think/topics/nist.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

30. 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.

31. Державна служба спеціального зв'язку та захисту інформації України : офіц. вебсайт. URL: https://cip.gov.ua/ua.

32. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

33. 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.

Andrii Lytvynchuk
Ph. D. (Economics), Senior Researcher, SSI "Institute of Educational Analytics", Kyiv, Ukraine, a.litvinchuk@iea.gov.ua
ORCID ID: https://orcid.org/0000-0002-7523-558X

Hanna Tereshchenko
Ph. D. (Economics), Senior Researcher, SSI "Institute of Educational Analytics", Kyiv, Ukraine, tganna@ukr.net
ORCID ID: https://orcid.org/0000-0002-9458-2843

Andrii Kyrianov
SSI "Institute of Educational Analytics", Kyiv, Ukraine, a.kiryanov@iea.gov.ua
ORCID ID: https://orcid.org/0000-0003-0452-7689

Yurii Kryvoruchko
SSI "Institute of Educational Analytics", Kyiv, Ukraine, kryvoruchko2025@gmail.com
ORCID ID: https://orcid.org/0009-0007-0494-9749

Yaroslav Solohub
State University of Information and Communication Technologies, Kyiv, Ukraine, jyariks@gmail.com
ORCID ID: https://orcid.org/0009-0008-5408-9246

INFORMATION SECURITY IN EDUCATIONAL INFORMATION SYSTEMS UNDER THE CONDITIONS OF DIGITAL TRANSFORMATION AND EUROPEAN INTEGRATION: ASPECTS OF PERSONAL DATA PROTECTION

Abstract. *This article explores the topical issues of ensuring information security in Ukraine's educational information systems amid digital transformation and the country's path towards European integration. It focuses on threats of data breaches, unauthorised access, and misuse of personal data stored and processed in digital educational environments, particularly in large-scale systems such as the software and hardware complex "Automated Information Complex of Educational Management" (SHC "AICEM"). It is noted that further digitalisation of the educational process necessitates the introduction of comprehensive cybersecurity mechanisms that combine technical, organisational, and legal instruments. The paper outlines the specifics of personal data protection in the field of education, emphasising the increased sensitivity of such data. Particular attention is given to European cybersecurity approaches, based on the principles of "privacy by design and by default", systematic risk management, and defence-in-depth architecture. Key EU regulations are reviewed, such as the GDPR, NIS2, and the ePrivacy Directive, along with international standards like ISO/IEC 27001:2022 and NIST, which define the requirements for organising information security. Within the framework of the comparative analysis, the differences between the EU and Ukrainian approaches are outlined in terms of legal regulation, institutional structure, technical standards, and the rights of personal data subjects. The need to align national legislation in line with European standards is emphasised. Using the SHC "AICEM" as an example, practical aspects of personal data protection in educational information systems are demonstrated, including the implementation of cryptographic protection, multi-level authorisation, access control, and audit systems. The article concludes with recommendations for harmonising Ukrainian practices with EU norms, including the enhancement of legislation, development of educators' digital competencies, institutionalisation of cybersecurity functions and strengthening the protection of data subjects' rights.*

Keywords: *digital transformation, information security, educational information systems, personal data protection, European integration.*

References

1. Shopina, I. (2023). Information security of digital transformation. *Scientific Journal of Lviv State University of Internal Affairs*, *1*, 28-35. DOI: https://doi.org/10.32782/2311-8040/2023-1-4 [in Ukrainian].

2. Pinchuk, O. P., & Yaskova, N. V. (Eds.). (2024). *Digital transformation of scientific and educational environments under martial law*. Kyiv: ITsO NAPN Ukrainy. Retrieved from https://tinyurl.com/yc23j2ss [in Ukrainian].

3. Laptiev, S. (2022). The advanced method of protection of personal data from attacks using social engineering algorithms. *Cybersecurity: Education, Science, Technique*, *4*(16), 45-62. DOI: https://doi.org/10.28925/2663-4023.2022.16.4562 [in Ukrainian].

4. SSI "Institute of Educational Analytics". (2023). *Education during the war: development of information and analytical support, digital transformation, European integration*. Kyiv. 216 p. Retrieved from https://iea.gov.ua/wp-content/uploads/2023/11/book-of-abstracts_ssi-iea_2023.pdf?utm_source=chatgpt.com [in Ukrainian].

5. Dreis, Yu. (2015). Measures to protect personal data in information (automated) systems. *Promising areas of information protection,* Proceedings of the 1st All-Ukrainian Scientific and Practical Conference. Odesa. Retrieved from https://www.researchgate.net/publication/389562867_ZAHODI_ZAHISTU_PERSONALNIH_DANIH_V_INFORMACIJNIH_AVTOMATIZOVANIH_SISTEMAH [in Ukrainian].

6. Hulak, H., Kozachok, V., Skladannyi, P., Bondarenko, M., & Vovkotrub, B. (2017). Personal data protection systems in modern information and telecommunication systems. *Modern Information Security, 2(30)*, 65-71. Retrieved from https://journals.dut.edu.ua/index.php/dataprotect/article/view/1491 [in Ukrainian].

7. Nosulych, M. (2014). Protection of personal data in information systems by depersonalization. *Information Society: Technological, Economic and Technical Aspects of Formation*, Abstracts of Papers of the All-Ukrainian Scientific Internet Conference. Ternopil: Taip. Retrieved from http://www.konferenciaonline.org.ua/data/downloads/file_1633503018.pdf#page=31 [in Ukrainian].

8. Korchenko, O., Dreis, Yu., & Lozova, I. (2016). Model and method of assessment risks protection of personal data during their processing at the automated system. *Ukrainian Information Security Research Journal, 18*(1), 39-47. DOI: https://doi.org/10.18372/2410-7840.18.10111 [in Ukrainian].

9. Krasnoshchok, V., & Shestak, Ya. (2024). Protection of information in applied information systems. In *Current cybersecurity issues in Ukraine under martial law* (pp. 81-83). Kyiv: National Academy of Internal Affairs. Retrieved from https://www.researchgate.net/publication/392895306_Zahist_informacii_v_prikladnih_informacijnih_sistemah [in Ukrainian].

10. Bakaiev, O., & Susskiy, G. (2024). Methods of protecting personal information in information systems. *Telecommunication and Informative Technologies, 2(83),* 68-77. DOI: https://doi.org/10.31673/2412-4338.2024.028190 [in Ukrainian].

11. Lehka, O. (2021). Current issues of personal data protection: domestic and international experience. *Legal Position, 2(31),* 74-79. DOI: https://doi.org/10.32836/2521-6473.2021-2.15 [in Ukrainian].

12. Kalchenko, V., Obodiak, V., & Puhach, I. (2024). Regulatory requirements of Ukraine in the field of cyber protection of personal data in information and communication systems in comparison with the requirements of the USA and the EU. *Visnyk of Kherson National Technical University, 2(89),* 162-169. DOI: https://doi.org/10.35546/kntu2078-4481.2024.2.23 [in Ukrainian].

13. Kalchenko, V., & Obodiak, V. (2024). Comparative characteristics of the regulatory requirements of Ukraine and the EU in the field of personal data cyber protection in information

and communication systems. *Information Technology and Society*, *5(11),* 14-20. DOI: https://doi.org/10.32689/maup.it.2023.5.2 [in Ukrainian].

14. Romansky, R. (2023). Internet of Things and User Privacy Protection. *2023 International Conference on Information Technologies (InfoTech).* DOI: https://doi.org/10.1109/InfoTech58664.2023.10266883.

15. Brown, R., Truby, J., & Ibrahim, I. A. (2022). Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies, 9*(1), 61-90. DOI: https://doi.org/10.2478/eustu-2022-0003.

16. Zhang, Y., & Dong, H. (2023). 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, 12*, 64. DOI: https://doi.org/10.1186/s13677-023-00437-3.

17. Cookiebot by Usercentrics. (2024). *What you need to know about privacy by design*. Retrieved from https://www.cookiebot.com/en/privacy-by-design/.

18. Treharne, J. (2024), *Defence in Depth: Why a Multi-Layered Approach is Essential for Cybersecurity in 2024*. Retrieved from https://assureddigitaltech.com/news/defence-in-depth/.

19. ISO. (2022). *ISO/IEC 27001:2022*. Retrieved from https://www.iso.org/standard/27001.

20. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.CSWP.29.

21. Federal Trade Commission. (n. d.). *Understanding the NIST cybersecurity framework*. Retrieved from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework.

22. IBM. (n. d.). *What is the NIST Cybersecurity Framework*? Retrieved from https://www.ibm.com/think/topics/nist.

23. The European Parliament and the Council of the European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council. *Official Journal of the European Union*, *L 194/1*. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

24. The European Parliament and the Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*, *L 119/1*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

25. The European Parliament and the Council of the European Union. (2002). Directive 2002/58/EC of the European Parliament and of the Council. *Official Journal of the European Union*, *L 201*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058.

26. The European Parliament and the Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council. *Official Journal of the European Union, L 333/80*. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

27. The European Parliament and the Council of the European Union. (2018). Regulation (EU) 2018/1725 of the European Parliament and of the Council. *Official Journal of the European Union, L 295/39*. Retrieved from https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

28. The European Parliament and the Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council. *Official Journal of the European Union, L 152/1*. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/868/oj.

29. Verkhovna Rada of Ukraine. (2018). *On the national security of Ukraine* (Act No. 2469-VIII, June 21). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

30. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"* (Decree No. 447/2021, August 26). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

31. State Service of Special Communications and Information Protection of Ukraine. (n. d.). Retrieved from https://cip.gov.ua/ua [in Ukrainian].

32. Verkhovna Rada of Ukraine. (2006). *On the State Service of Special Communications and Information Protection of Ukraine* (Act No. 3475-IV, February 23). Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text [in Ukrainian].

33. State Service of Special Communications and Information Protection of Ukraine. (2025). *President Zelenskyy Signs Law Enhancing Cybersecurity of State Information Resources*. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text [in Ukrainian].