МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “Методи забезпечення захисту персональних даних у компаніях на основі регламенту GDPR”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав ДАРІЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Владислав ДАРІЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій САВЧЕНКО
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дарію Владиславу Романовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення захисту персональних даних на основі регламенту GDPR”,
керівник кваліфікаційної роботи САВЧЕНКО Віталій, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *персональні дані, методи та засоби, конфіденційність, міжнародні стандарти, захист даних.*

4. Перелік питань, які мають бути розроблені:
4.1 Проаналізувати основні засади регламенту GDPR щодо визначення персональних даних та їх категоріювання
4.2. Дослідити основні вимоги регламенту GDPR до збору та обробки персональних даних у компаніях.
4.3. Дослідити вплив регламенту GDPR та визначити методи реалізації вимог для захисту персональних даних у компаніях

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	25.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз положень Загального регламенту про захист даних GDPR	13.04.2025	
4.	Дослідження основних принципів регламенту, розгляд доповнень і коментарів до документу	23.04.2025	
5.	Вивчення інструментів та методів впровадження змін у системи захисту для відповідності вимогам GDPR	03.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	07.04.2025	
7.	Оформлення роботи.	08.05.2025	
8.	Оформлення презентації.	11.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Владислав ДАРІЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Дарій В. Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи забезпечення захисту персональних даних у компаніях на основі регламенту GDPR"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Владислав ДАРІЙ у кваліфікаційній роботі проаналізував вимоги та принципи регламенту GDPR, дослідив основні засади забезпечення захисту персональних даних, вивчив інструменти та методи формування обізнаності й навчання персоналу з інформаційної безпеки, розробила практичні рекомендації за темою дослідження.

ДАРІЙ Владислав показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ДАРІЯ Владислава на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Дарій В.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ДАРІЯ Владислава
на тему “Методи забезпечення захисту персональних даних у компаніях на основі регламенту GDPR”

Актуальність. Створення Загального регламенту про захист даних (GDPR) мало дуже великий вплив на систему захисту персональних даних для компаній та організацій. З впровадженням GDPR, вимоги до обробки та зберігання особистої інформації значно посилилися, що потребує нових підходів до забезпечення інформаційної безпеки. Питання безпеки персональних даних та можливе зловживання даними клієнтів з боку компаній є одним з найважливіших питань світової інформаційної безпеки загалом, а з урахуванням стрімкого розвитку технологій, в тому числі і у сфері збору та обробки даних, дотримання вимог GDPR є необхідним та актуальним завданням для організацій.

З огляду на зазначене дослідження проблема відповідності захисту даних GDPR є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено вимог регламенту GDPR та основні положення
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків та таблиць.
3. Автор опрацював значну джерельну базу: близько 50 публікацій, багато іноземних.
4. За результатами дослідження запропоновано рекомендації щодо забезпечення захисту даних відповідно регламенту GDPR у системах електронного навчання

Недоліки.

Доцільно було б приділити більше уваги вивченню програмних інструментів для реалізації розроблених методів захисту персональних даних.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ДАРІЙ Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____

підпис

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 5 рисунків, висновків і списку використаних джерел із 53 найменувань. Загальний обсяг роботи становить 58 аркушів, з яких 7 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є визначення методів реалізації захисту персональних даних у організаціях на основі вимог GDPR.

Об'єктом дослідження є процеси захисту персональних даних у компаніях.

Предмет дослідження – методи забезпечення відповідності захисту персональних даних вимогам GDPR у компаніях.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, опрацювання документів, статистичних даних та існуючих моделей забезпечення належного рівня захисту даних.

Як результат у роботі проаналізовано засади регламенту, основні принципи, правила та вимоги щодо обробки персональних даних, розроблено практичні рекомендації для впровадження заходів, що підвищить відповідність систем обробки і захисту даних вимогам регламенту GDPR.

Галузь застосування. Можливість застосування результатів дослідження для підвищення рівня захисту персональних даних, зокрема у системах електронного навчання, та забезпечення відповідності вимогам GDPR для мінімізації ризиків порушень правил щодо обробки персональних даних.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, НОРМАТИВНО-ПРАВОВІ ДОКУМЕНТИ, ЗАХИСТ ДАНИХ, ІДЕНТИФІКАЦІЯ, КОНФІДЕНЦІЙНІСТЬ.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 8 figures, conclusions and the list of references containing 57 items. The total volume of the work is 58 pages, of which 7 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to investigate the methods of implementing personal data protection methods in organisations based on the GDPR requirements.

The object the study is the processes of personal data protection in companies.

The subject of the study is the methods of ensuring compliance of personal data protection with the GDPR requirements in companies.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, processing of documents, statistical data and existing models of ensuring an adequate level of data protection were used in the work.

As a result, the work analyzed the fundamentals of the regulation, basic principles, rules and requirements for personal data processing, and develops practical recommendations for implementing measures that will increase the compliance of data processing and protection systems with the requirements of the GDPR.

Field of application. The results of the study can be used to improve the level of personal data protection, in particular in e-learning systems, and to ensure compliance with the GDPR requirements to minimise the risks of violations of the rules for processing personal data.

Keywords: PERSONAL DATA, INFORMATION SECURITY MANAGEMENT, REGULATORY DOCUMENTS, DATA PROTECTION, IDENTIFICATION, CONFIDENTIALITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ .....…….…… 9

ВСТУП ……..... 10

РОЗДІЛ 1 ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗГІДНО З GDPR …….. 12

1.1 Сутність персональних даних в контексті GDPR …… 12

1.2 Історична еволюція регулювання захисту даних в ЄС ……..…… 18

1.3 Основні принципи та вимоги GDPR щодо обробки персональних даних ……..... 20

Висновки до розділу 1……. 25

РОЗДІЛ 2 СИСТЕМА ЗАХОДІВ ВІДПОВІДНОСТІ ВИМОГАМ GDPR …… 27

2.1 Організаційні механізми забезпечення відповідності GDPR ……..... 27

2.2 Оцінювання впливу на захист даних …… 34

2.3 Технологічні засоби забезпечення захисту персональних даних…….. 35

Висновки до розділу 2 …… 38

РОЗДІЛ 3 СПЕЦИФІКА РЕАЛІЗАЦІЇ ВИМОГ GDPR У СИСТЕМАХ ЕЛЕКТРОННОГО НАВЧАННЯ …….... 40

3.1 Особливості обробки даних в освітніх платформах…… 40

3.2 Визначення та документування правових підстав обробки …….. 42

3.3 Забезпечення реалізації прав користувачів у системах електронного навчання ……..... 45

Висновки до розділу 3…… 49

ВИСНОВКИ …… 51

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …… 53

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) …….. 59

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

GDPR	General Data Protection Regulation (Загальний регламент з захисту даних
DPO	Data Protection Officer (Співробітник з питань захисту даних)
DPIA	Data Protection Impact Assessment (Оцінювання впливу на захист даних)

ВСТУП

Актуальність теми. Створення Загального регламенту про захист даних (GDPR) мало дуже великий вплив на систему захисту персональних даних для компаній та організацій. З впровадженням GDPR, вимоги до обробки та зберігання особистої інформації значно посилилися, що потребує нових підходів до забезпечення інформаційної безпеки. Питання безпеки персональних даних та можливе зловживання даними клієнтів з боку компаній є одним з найважливіших питань світової інформаційної безпеки загалом, а з урахуванням стрімкого розвитку технологій, в тому числі і у сфері збору та обробки даних, дотримання вимог GDPR є необхідним та актуальним завданням для організацій.

Мета роботи полягає у визначенні методів реалізації захисту персональних даних у організаціях на основі вимог GDPR.

Об'єкт дослідження – процеси захисту персональних даних у компаніях.

Предмет дослідження – методи забезпечення відповідності захисту персональних даних вимогам GDPR у компаніях.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати основні засади регламенту GDPR щодо визначення персональних даних та їх категоріювання.
2. Проаналізувати вимоги регламенту GDPR до збору та обробки персональних даних у компаніях.
3. Дослідити вплив регламенту GDPR та сучасні підходи для реалізації принципів регламенту у компаніях.
4. Визначення методів реалізації захисту персональних даних згідно вимог GDPR у системах електронного навчання.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, опрацювання документів, статистичних даних та існуючих

моделей забезпечення належного рівня захисту даних.

Практичне значення одержаних результатів. Можливість застосування результатів дослідження для підвищення рівня захисту персональних даних, зокрема у системах електронного навчання, та забезпечення відповідності вимогам GDPR для мінімізації ризиків порушень правил щодо обробки персональних даних.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗГІДНО З GDPR

1.1 Сутність персональних даних в контексті GDPR

Персональні дані у сучасному світі є одним з найголовніших інформаційних активів, та їх захист є не менш важливим ніж захист інших прав та свобод людини. Стаття 4 регламенту GDPR визначає поняття персональних даних як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати (“суб’єкт даних”); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім’я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи [1]. Саме ці персональні дані і є основними активами громадян, з метою забезпечення захисту яких і існує GDPR. Однак, різні типи персональних даних мають різну важливість, а відповідно, пріоритети захисту також можуть відрізнятись. Відповідальним за це є контролер – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних. Серед інших понять, які часто фігурують у статтях GDPR, слід виділити «обробник» – фізична чи юридична особа або орган, який опрацьовує персональні дані від імені контролера, та «одержувач» – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою стороною. Органів публічної влади, що можуть отримувати персональні дані в рамках конкретного запиту згідно з законодавством Союзу чи держави-члена, не вважають одержувачами.

З точки зору ефективності ідентифікації, дані умовно поділяються на явні та опосередковані ідентифікатори [2]. Явні, або ж прямі ідентифікатори, такі як паспортні дані чи біометричні показники, дозволяють ідентифікувати особу без необхідності використання додаткових джерел інформації. Опосередковані дані дають можливість визначити особу лише за комбінацією цих даних, кожен з яких окремо не дозволяє ідентифікувати особу. До таких даних належать онлайн-ідентифікатори (IP-адреси, cookie-файли), дані про місцезнаходження, професійні характеристики та інші параметри, які тільки при комплексному аналізі можуть призвести до встановлення особистості.

Важливою характеристикою сучасного розуміння ідентифікованості є її динамічний характер. Згідно з Підставою 26 GDPR [3], при визначенні можливості ідентифікації необхідно враховувати не лише наявні на момент обробки технології, але й ті засоби, які можуть з'явитись у майбутньому. Це означає, що дані, які сьогодні вважаються анонімними і не дають можливості визначити особу, завдяки розвитку технологій (наприклад, вдосконаленим алгоритмам машинного навчання) можуть стати персональними в майбутньому. Європейська рада з захисту даних у своїх рекомендаціях [4] підкреслює, що контролери даних повинні оцінювати не лише поточні, а й потенційні майбутні ризики деанонімізації.

Динамічність ідентифікації проявляється також у зміні характеру самих ідентифікаторів. З розвитком цифрових технологій з'являються нові форми персональних даних, такі як цифрові відбитки пристроїв, метадані про поведінку в інтернеті або агреговані дані, які при певних умовах можуть дозволити ідентифікацію особи. Це створює значні виклики для забезпечення відповідності вимогам GDPR, оскільки вимагає від організацій постійного моніторингу технологічних змін та адаптації підходів до захисту даних.

Окрім звичайних персональних даних, у регламенті вказано деякі інші категорії до яких застосовуються інші правила захисту і обробки. Так, у статті 9 GDPR надано перелік даних, що належать до спеціальної категорії. Туди входять персональні дані що розкривають расову чи етнічну приналежність,

політичні переконання, релігійні чи філософські вірування, членство в професійних спілках, генетичні і біометричні дані для цілі єдиної ідентифікації фізичної особи, дані стосовно статевого життя та стану здоров’я. На відміну від звичайних персональних даних, на дані що входять до спеціальної категорії діє загальна заборона на обробку, яка може бути знята лише за конкретних виняткових обставин.

Основною підставою для обробки спеціальних категорій даних є явна згода суб'єкта даних. Ця згода повинна бути добровільною, конкретною, інформованою та однозначною. Важливо відзначити, що навіть за наявності згоди, обробка спеціальних категорій даних може бути обмежена, якщо національне законодавство держави-члена ЄС встановлює додаткові вимоги. Окрім згоди, GDPR передбачає низку інших винятків. Зокрема, обробка спеціальних категорій даних дозволяється, коли вона необхідна для виконання зобов'язань у сфері трудового права та соціального захисту. Це включає, наприклад, обробку медичних даних для оцінки працездатності працівника або надання соціальних пільг. Однак такі дії повинні бути прямо передбачені національним законодавством і включати відповідні гарантії захисту прав суб'єктів даних.

Ще однією важливою підставою є захист життєво важливих інтересів, коли суб'єкт даних фізично або юридично неспроможний дати згоду. Це стосується, зокрема, екстрених медичних випадків, коли обробка даних про здоров'я необхідна для надання невідкладної допомоги. Для неурядових організацій, таких як релігійні або політичні об'єднання, GDPR дозволяє обробку спеціальних категорій даних у межах їхньої законної діяльності, за умови що ця обробка стосується лише членів організації і дані не розголошуються третім особам без додаткової згоди.

Окремо варто відзначити обробку даних, які суб'єкт явно оприлюднив. Наприклад, якщо особа публікує свої політичні погляди у соціальних мережах або блозі, це може слугувати підставою для їх подальшої обробки, проте таке тлумачення вимагає обережного підходу. У сфері охорони здоров'я обробка

спеціальних категорій даних дозволяється для превентивної медицини та гігієни праці, оцінки працездатності працівника, медичної діагностики, надання медичної допомоги або лікування, а також управління системами охорони здоров'я. При цьому такі дії повинні здійснюватися під наглядом професійного медичного персоналу або інших осіб, які зобов'язані дотримуватися професійної таємниці. Для наукових, історичних чи статистичних досліджень також передбачені спеціальні умови обробки, які вимагають вжиття відповідних технічних і організаційних заходів для захисту прав і свобод суб'єкта даних, зокрема принципу мінімізації даних. Важливо підкреслити, що незалежно від підстави обробки, контролери даних зобов'язані вживати додаткові заходи захисту коли йдеться про спеціальні категорії даних.

Третя і остання категорія персональних даних, виокремлена у регламенті GDPR, це дані про судимості та кримінальні злочини. Ця категорія включає широкий спектр інформації - від офіційних записів про кримінальні засудження до даних про підозрюваних у скоєнні злочинів, свідків та постраждалих. Їхня чутливість обумовлена серйозними ризиками дискримінації, загрозами репутації та довгостроковими наслідками для життя людей. Обробка таких даних дозволена лише у виняткових випадках і суворо регламентована. Основне навантаження регулювання лягає на національне законодавство країн-членів ЄС, яке має чітко визначати умови та межі такої обробки. GDPR встановлює загальні рамки, вимагаючи, щоб будь-яка робота з цими даними здійснювалася під офіційним контролем і лише уповноваженими органами - правоохоронними структурами, судам, іншими визначеними у законодавстві органами. Ключовим принципом є мінімізація обробки - збір і використання таких даних має бути обмеженим лише необхідним мінімумом для досягнення конкретної законної мети. Наприклад, перевірка судимості при працевлаштуванні дозволена лише для окремих видів діяльності, де це безпосередньо пов'язано з характером роботи. GDPR накладає особливо суворі вимоги до захисту цих даних. Терміни зберігання таких даних мають бути чітко визначеними і обґрунтованими. Важливо, що навіть для цієї надзвичайно

чутливої категорії GDPR зберігає певні права суб'єктів даних. Особи мають право знати про факт обробки своїх даних (за винятком випадків, коли це може завадити розслідуванню), отримувати доступ до інформації про себе, вимагати виправлення неточностей. Водночас, ці права можуть обмежуватись у інтересах правосуддя або національної безпеки, а міжнародна передача таких даних регулюється особливо суворо.

Типи даних, питання обробки яких порушуються у регламенті GDPR, представлені на рис. 1.1. Підстави, за якими ці дані можуть оброблюватись наведені у табл. 1.1. Подібні категорії даних визначені і в українському законодавстві. За Законом України «Про захист персональних даних» обмежується обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних [5].

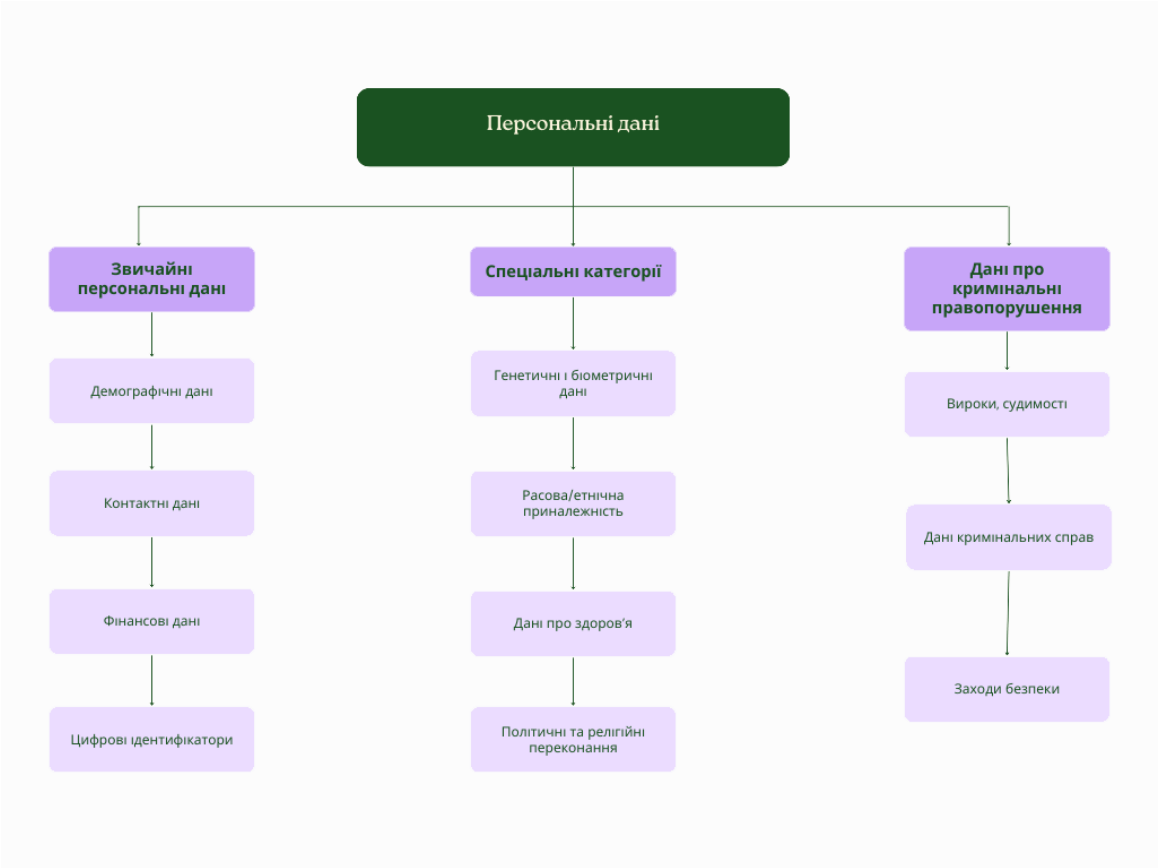

Рис. 1.1. Категорії персональних даних згідно GDPR

Таблиця 1.1

Підстави для обробки персональних даних за GDPR

Категорії даних	**Підстави для обробки**
Звичайні персональні дані (ім'я, контакти, історія покупок)	• Згода суб’єкта • Виконання договору • Виконання обов’язку згідно закону • Захист життєво важливих інтересів • Виконання завдань суспільного інтересу • Законний інтерес
Спеціальні категорії даних (здоров'я, біометрія, ідеологічні переконання)	• Явна згода суб’єкта • Обробка для трудового права • Захист життєвих інтересів • Діяльність фондів/організацій • Дані, оприлюднені суб’єктом • Судова допомога або медична діагностика • Суспільний інтерес у галузі охорони здоров’я • Архівні цілі або наукові дослідження
Кримінальні дані	• Офіційний контроль (національне законодавство) • Виконання обов’язків контролера даних у сфері правоохоронної діяльності
Дані дітей	• Згода батьків (для дітей до 13-16 років) • Інші підстави для звичайних персональних даних

1.2 Історична еволюція регулювання захисту даних в ЄС

Європейська Директива 95/46/ЄС, яка була попередником GDPR, стала першою спробою ЄС створити комплексну систему захисту персональних даних [6]. Директива була ключовим нормативним актом, що регулює захист фізичних осіб під час обробки персональних даних і забезпечує вільне переміщення таких даних у межах Європейського Союзу. Ця директива встановила основні принципи та вимоги до обробки персональних даних, які стали фундаментом для сучасних стандартів захисту даних. Прийнята у 1995 році, вона встановила базові принципи, які згодом лягли в основу GDPR та інших сучасних стандартів захисту даних. Основні положення:

- Принципи обробки даних: законність, справедливість, прозорість, цілеспрямованість, мінімізація даних, точність та обмеження терміну зберігання.
- Права суб'єктів даних: право на доступ, виправлення, заперечення проти обробки.
- Вимоги до передачі даних за межі ЄС (обмеження на експорт даних до країн із недостатнім рівнем захисту).
- Вимоги до створення державами-членами ЄС незалежних органів контролю для моніторингу дотримання вимог щодо захисту даних.

Положення Директиви 95/46/ЄС стали основою для Закону України «Про захист персональних даних», прийнятого у 2010 році. Цей закон запровадив ключові принципи обробки персональних даних, аналогічні до тих, що містилися в Директиві, включаючи законність, прозорість, обмеження мети та мінімізацію даних. Крім того, він передбачав створення незалежного органу контролю – Державної служби України з питань захисту персональних даних, що відповідало вимогам Директиви. З часом цей орган було ліквідовано, а повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини.

Директива 95/46/ЄС, попри велику значущість для глобального розвитку захисту, не була достатньо ефективною та мала досить значні недоліки, які розглядались багатьма науковцями [7,8,9]. Це зумовило необхідність комплексної реформи, результатом якої стало ухвалення Загального регламенту про захист даних (GDPR).

Одним з ключових недоліків Директиви 95/46/ЄС була її фрагментарна імплементація на національному рівні держав-членів ЄС. Хоча директива була обов'язковою для виконання, вона дозволяла значну свободу трактування положень, що призвело до нерівномірного застосування норм у різних країнах ЄС. Така розбіжність перешкоджала створенню єдиного цифрового ринку та ускладнювала транскордонну передачу даних.

Іншим важливим недоліком директиви була нечіткість формулювань ключових понять, таких як "згода суб'єкта даних" або "законність обробки". Це призводило до правової невизначеності та ускладнювало забезпечення ефективного контролю над персональними даними. Крім того, у Директиві 95/46/ЕС були відсутні чіткі зобов'язання щодо повідомлень про порушення безпеки персональних даних, що дозволяло компаніям приховувати інциденти. Суттєвим зауваженням є те, що директива не враховувала реалії цифрової доби, такі як хмарні технології, автоматизовану обробку, алгоритми прийняття рішень або масову аналітику. Норми, що існували, не передбачали регулювання таких явищ, що створювало нормативні прогалини [10]. Натомість, GDPR запропонував комплексні положення, які прямо регламентують обробку даних із використанням новітніх технологій.

Ще одним обмеженням директиви була її територіальна сфера дії. Вона застосовувалася лише в межах ЄС і не охоплювала компанії з інших країн, які обробляли персональні дані громадян ЄС. Це дозволяло уникати регулювання деяким компаніям, які отримували прибутки взаємодіючи з даними громадян Євросоюзу, але при цьому не були зобов’язані виконувати вимоги директиви. GDPR же має екстратериторіальний характер і застосовується до будь-якого суб’єкта, що працює з даними резидентів ЄС, незалежно від локації [12].

Окремо слід відзначити відсутність у директиві чітко закріпленого права на забуття — фундаментального для цифрового середовища. Це право було лише опосередковано згадане в деяких інтерпретаціях, але не мало нормативного закріплення. GDPR, навпаки, прямо гарантує це право та визначає процедури його реалізації.

У деяких дослідженнях також акцентується увага на проблемах реалізації нагляду та відповідальності [13]. Директива не містила уніфікованих вимог щодо санкцій, залишаючи це на розсуд держав-членів. Як наслідок, штрафи й контрольна практика суттєво відрізнялися, що послаблювало превентивний ефект. GDPR впровадив систему масштабних штрафів, деталізовані вимоги до ведення документації обробки даних і визначив обов'язкову роль у процесі захисту даних Data Protection Officer (Співробітника з питань захисту даних), що посилило механізми підзвітності. Дослідники звертають увагу на те, що директива була продуктом 1990-х років і не відповідала сучасним викликам інформаційної безпеки [14]. Її заміна стала логічною відповіддю на нові технологічні та соціальні обставини. GDPR не лише уніфікував підходи до захисту даних у ЄС, а й створив нову етико-правову парадигму персональної автономії в цифрову епоху.

Аналіз наукових джерел показує що основні причини заміни Директиви 95/46/ЕС на GDPR полягають у фрагментарності застосування директиви, відсутності адаптації до сучасних цифрових технологій, нечіткості понять, слабких наглядових механізмах, обмеженій юрисдикції та відсутності важливої частини прав суб'єкта даних.

1.3 Основні принципи та вимоги GDPR щодо обробки персональних даних

У статті 5 Загального Регламенту про Захист Даних (GDPR) встановлено систему принципів щодо обробки персональних даних на всій території Європейського Союзу.

- Законність, справедливість і прозорість – обробка даних повинна здійснюватися на законній підставі, яка ґрунтується на одній з 6 законних підстав, які зазначені у Статті 6. Суб'єкти даних мають отримувати чітку інформацію про обробку їхніх даних.
- Цільове обмеження – дані збираються лише для чітко визначених, явних і легітимних цілей. Подальша обробка для інших цілей можлива лише у випадках, передбачених GDPR.
- Мінімізація даних – обробка має обмежуватись лише тими даними, що необхідні для досягнення визначених цілей.
- Точність – дані мають бути точними та за потреби оновлюватись. Неправдиві дані мають бути вилучені або виправлені. Контролер повинен установити часові рамки для стирання або періодичного перегляду даних.
- Обмеження зберігання – дані зберігаються не довше, ніж це необхідно для мети обробки.
- Цілісність і конфіденційність – дані мають оброблятись з гарантіями безпеки, зокрема щодо захисту від несанкціонованого доступу, втрати чи пошкодження.
- Підзвітність – контролер даних несе відповідальність за дотримання цих принципів і повинен бути готовий продемонструвати їх виконання.

GDPR передбачає широкий спектр прав для суб’єктів персональних даних — фізичних осіб, персональна інформація яких обробляється. Ці права закріплено в статтях 12–23 Регламенту і вони є фундаментальними для забезпечення контролю особи над власними даними. До основних прав належать:

1. Право на доступ до даних (Article 15 GDPR) — особа має право знати, які саме її персональні дані обробляються, з якою метою, кому передаються, протягом якого строку зберігаються тощо. Це право дозволяє забезпечити прозорість та контроль обробки. Також особа може запитувати та отримувати копію своїх персональних даних, які обробляються, а також

інформацію про джерело їх отримання.

2. Право на виправлення (Article 16 GDPR) — суб’єкт даних може вимагати від контролера виправлення неточних або застарілих даних без зайвого зволікання.

3. Право на забуття (Article 17 GDPR) — дозволяє особі вимагати видалення персональних даних у випадках, коли вони більше не потрібні, обробка є незаконною або згода була відкликана.

4. Право на обмеження обробки (Article 18 GDPR) — передбачає тимчасове призупинення обробки у разі, якщо точність даних оскаржується або суб’єкт заперечує проти обробки.

5. Право на перенесення даних (Article 20 GDPR) — забезпечує можливість отримати власні персональні дані у структурованому, машиночитаному форматі та передати їх іншому контролеру.

6. Право на заперечення проти обробки (Article 21 GDPR) — особа має право заперечити проти обробки з обробки своїх даних, зокрема для прямих маркетингових цілей..

7. Право не підлягати виключно автоматизованому прийняттю рішень (Article 22 GDPR) — захищає від рішень, що приймаються лише автоматизованими засобами, без втручання людини.

GDPR встановлює чіткі механізми для реалізації цих прав. Контролер зобов’язаний надати інформацію щодо обробки даних протягом одного місяця, а у разі відмови в задоволенні запиту – суб’єкт даних має право звернутися до наглядового органу або до суду. Держави-члени зобов’язані забезпечити ефективні адміністративні та судові механізми захисту прав. Слід розуміти що наявність цих прав не гарантує їх виконання, оскільки контролери можуть уникати активного виконання цих обов’язків. У цьому контексті роль державних наглядових органів та судової системи стає критичною важливою, оскільки саме вони мають здійснювати моніторинг стосовно того, наскільки ефективно контролери здійснюють реалізацію прав суб’єктів даних через впровадження технічних і організаційних заходів [15, 16, 17]. Загальні вимоги

організацій з обробки даних представлені на табл. 1.2.

Таблиця 1.2

Обов’язки контролерів даних згідно з GDPR

Критерії	**Вимоги GDPR**
Законність та прозорість	Обробка лише на підставі згоди, договору або законного інтересу (ст. 6). Надання інформації суб’єктам даних(ст. 13-14).
Захист даних	Впровадження технічних і організаційних заходів (ст. 32). Обов’язкове повідомлення про порушення даних (ст. 33-34).
Права суб’єктів даних	Забезпечення прав на доступ, виправлення, видалення, забуття, перенесення даних (ст. 15-21).
Ведення обліку	Документування процесів обробки (ст. 30). Оцінка впливу на захист даних DPIA (ст. 35).
Співпраця з регуляторами	Призначення DPO (якщо потрібно, ст. 37-39). Дотримання міжнародних передач даних (ст. 44-50).

Незважаючи на позитивний вплив регламенту GDPR на захищеність персональних даних громадян ЄС, для компаній відповідність всім вимогам регламенту потребує значних зусилль. Особливо це стосується малих та середніх бізнесів, для яких це може стати серйозним фінансовим навантаженням. У одному з досліджень [18] було обраховано що витрати на забезпечення відповідності GDPR для малих та середніх підприємств у Хорватії можуть сягати понад 50 000 євро для кожного підприємства, включаючи витрати на зовнішнє консультування, впровадження внутрішніх політик, підвищення кваліфікації персоналу та впровадження технічних заходів захисту

даних. Ще однією проблемою є нерівномірна практика застосування санкцій. Попри те, що GDPR встановлює значні штрафи, фактична реалізація покарань залежить від національних регуляторів. Як вказує Європейська рада із захисту даних, у деяких країнах тривалість розгляду скарг може перевищувати один рік, що знижує ефективність механізмів захисту прав [19]. У щорічному звіті DLA Piper зазначається, що обсяг накладених штрафів значно відрізняється між державами-членами ЄС. Наприклад, у 2022 році Ірландія та Люксембург відповідали за найбільші суми штрафів, зокрема Ірландія — за понад 1,3 млрд євро загалом, тоді як у країнах Центральної та Східної Європи штрафи були в десятки або навіть сотні разів менші [20]. Це створює нерівномірність правозастосування та знижує загальну довіру до ефективності регулювання.

На таблиці 1.3. представлено розподіл штрафів за типами порушень GDPR з підрахунком частки від загальної суми штрафів [21].

Таблиця 1.3.

Статистика штрафів за підставами GDPR

Тип порушення	**Кількість штрафів**	**Частка від загальної суми штрафів (%)**
Недостатня правова підстава для обробки даних	612	36,9
Недотримання загальних принципів обробки даних	561	46,5
Недостатні технічні та організаційні заходи для забезпечення безпеки	357	8,7
Неналежне виконання інформаційних обов’язків	187	5,5
Неналежне виконання прав суб’єктів даних	193	2,2
Недостатня співпраця з наглядовими органами	107	0,14
Неналежне виконання обов’язків щодо повідомлення про витік даних	35	0,04
Недостатня участь уповноваженого з питань захисту даних	20	0,02
Неналежне укладення угоди про обробку даних	11	0,02

Проблеми реалізації захисту даних згідно GDPR існують і у технічній сфері, такі як відсутність чітко визначених практичних механізмів реалізації багатьох вимог GDPR. Регламент надає загальні принципи, однак не містить конкретних технічних чи процедурних рішень, які можна було б безпосередньо впровадити. Це змушує компанії створювати свої підходи, що призводить до нерівномірної практики реалізації навіть серед організацій одного сектору. Багато підприємств, особливо у фінансовому секторі та державному управлінні, досі використовують застарілі програмні рішення, розроблені задовго до появи GDPR. Як свідчать дані [22], близько 68% таких систем не відповідають концепції "privacy by design", що вимагає їх повної модернізації або заміни.

Окремої уваги заслуговує питання управління згодами користувачів. Вимоги GDPR щодо отримання, зберігання та обліку згоди (ст. 7) вимагають від організацій створення складних технічних рішень. Компанії повинні розробити механізми для прозорого збору згоди на кожен вид обробки даних, легкого відкликання згоди користувачами та надійного архівування історії змін згоди. Однак, як показують дослідження PwC [23], більшість організацій (54%) не мають єдиної системи управління згодами, що призводить до численних порушень при обробці персональних даних.

Висновки до розділу 1

У першому розділі було розглянуто основні засади захисту персональних даних відповідно до вимог GDPR, проаналізовано поняття персональних даних, їхні категорії та підстави для обробки. GDPR запроваджує сучасний підхід до захисту персональних даних, визначаючи їх як будь-яку інформацію, що стосується ідентифікованої або ідентифікованої фізичної особи. Особливу увагу приділено спеціальним категоріям даних включаючи медичні, біометричні та інші чутливі дані, обробка яких дозволена лише за виняткових обставин. Також окремо регулюються дані про кримінальні засудження, що вимагають додаткових гарантій конфіденційності. Розглянуто також підстави,

за якими перелічені категорії персональних даних можуть збиратись та оброблятись.

Проаналізовано недоліки Директиви 95/46/ЕС які спричинили появу регламенту GDPR – серед них проблеми реалізації нагляду та відповідальності, обмеженість територіальної дії документа та відсутність адаптації до сучасних цифроих технологій. Досліджено основні вимоги GDPR щодо захисту даних, основні принципи які повинні забезпечуватись – законність, мінімізація даних, обмеження зберігання та підзвітність. Визначено ключові права суб'єктів даних, такі як право на забуття та перенесення даних, покликані забезпечити контроль особи над своєю інформацією.

Виявлені проблеми, такі як нерівномірність застосування санкцій у різних країнах, складність реалізації для невеликих організацій, високі витрати на впровадження вимог GDPR та необхідність створення власних чи вибору існуючих підходів до створення системи захисту персональних даних, підкреслюють необхідність подальшого дослідження ефективних підходів до забезпечення відповідності регламенту. Саме ці виклики обумовлюють актуальність подальшого аналізу сучасних технологічних рішень, організаційних методів та практичних інструментів, які дозволяють підвищити рівень захисту персональних даних та мінімізувати ризики щоб відповідати вимогам регламенту.

Розділ 2 СИСТЕМА ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ GDPR

2.1 Організаційні механізми забезпечення відповідності GDPR

Одним із ключових елементів організаційної структури, необхідної для відповідності GDPR є призначення співробітника з питань захисту даних (DPO). Згідно зі статтями 37–39 GDPR, призначення DPO є обов’язковим у таких випадках:

1) Коли обробка здійснюється публічним органом або установою (за винятком судових органів у межах їх судових повноважень)

2) Якщо основні види діяльності контролера або обробника полягає в обробці персональних даних, що вимагає регулярного та систематичного моніторингу суб'єктів даних у великому масштабі.

3) Якщо основна діяльність контролера або обробника полягає в обробці в великому масштабі спеціальних категорій даних відповідно до статті 9 або персональних даних, що стосуються кримінальних вироків та правопорушень відповідно до статті 10.

Основні обов’язки DPO включають:

1. Інформування та надання порад контролеру або обробнику та працівникам, які здійснюють обробку, щодо їхніх зобов’язань відповідно до GDPR та інших положень законодавства про захист даних.

2. Моніторинг дотримання GDPR, інших положень законодавства про захист даних та політик контролера або обробника щодо захисту персональних даних, включаючи розподіл обов’язків, підвищення обізнаності та навчання персоналу, що бере участь в операціях з обробки, та пов’язані з цим аудити.

3. Надавати поради щодо того, чи потрібно проводити оцінку впливу на захист даних (DPIA), як її правильно проводити, і чи достатньо заходів для зменшення ризиків, які виявлені в ході цієї оцінки. Після цього DPO також слідкує, чи дійсно всі заплановані заходи були виконані.

4. Співпраця з наглядовим органом.

5. Виконання функції контактної особи для наглядового органу з питань, пов’язаних з обробкою, включаючи попередні консультації, та, при необхідності, консультації з будь-яких інших питань. DPO повинен мати можливість виконувати свої обов’язки незалежно, без отримання інструкцій щодо виконання цих завдань. Він повинен безпосередньо підпорядковуватися найвищому керівництву контролера або обробника.

DPO повинен мати професійні якості та експертні знання законодавства і практики захисту даних, а також здатність виконувати завдання, передбачені статтею 39 GDPR. Дефіцит кваліфікованих кадрів для цієї посади досить значна проблема. Як наслідок, DPO часто призначаються формально, без належного рівня незалежності чи реального впливу на внутрішні процеси, що суперечить вимогам GDPR [24].

Номінальна роль DPO у багатьох організаціях призводить до неефективного функціонування системи захисту даних. Згідно з дослідженнями, понад 30% DPO у ЄС повідомили про відсутність достатніх повноважень для виконання своїх обов’язків. Це призводить до того що в багатьох компаніях DPO фактично виконують роль «консультантів», а не активних учасників процесу прийняття рішень [25, 26, 27]. Особливо часто це відбувається у випадках, коли обов’язки DPO делегуються співробітникам юридичного або IT-відділів, що створює конфлікт інтересів. Практика передачі обов’язків DPO іншим відділам без належного механізму контролю є серйозним ризиком. Наприклад, коли функції DPO покладаються на працівників відділу кібербезпеки, це може призвести до перекосу у бік технічних заходів захисту даних за рахунок правових та організаційних аспектів. Водночас GDPR вимагає, щоб співробітники з питань захисту даних були безпосередньо залучені до оцінки впливу на захист даних DPIA та консультували керівництво.

Враховуючи усе вище перераховане, для забезпечення ефективності роботи співробітника з питань безпеки даних запропоновано такі рекомендації:

1. Чітко формалізувати роль DPO в організаційній структурі з визначенням повноважень і обов’язків.

2. Забезпечити незалежність DPO, уникаючи конфлікту інтересів, наприклад, не поєднувати цю посаду з функціями інших працівників.

3. Регулярно проводити навчання та підвищення кваліфікації DPO.

4. Впроваджувати механізми підтримки DPO, включно з наданням необхідних ресурсів , прямого зв’язку з керівництвом та доступом до необхідних даних.

5. Уникати формального призначення DPO без реальних повноважень і можливостей для виконання функцій.

Ефективне впровадження вимог GDPR вимагає системного підходу до розробки внутрішніх політик і процедур, які формалізують та структурують процеси обробки персональних даних в організації. Організаційні механізми впровадження GDPR слід розглядати як "комплекс взаємопов'язаних управлінських заходів, спрямованих на забезпечення відповідності діяльності організації нормативним вимогам захисту персональних даних".

Ключовими компонентами ефективної політики захисту персональних даних є:

1. Політика конфіденційності – документ, що встановлює загальні принципи та цілі обробки персональних даних, визначає категорії даних, що обробляються, та встановлює правові підстави для такої обробки. Політика конфіденційності є основоположним документом, який встановлює рамки для всіх інших процедур захисту персональних даних лв організації.

2. Процедура реагування на запити суб'єктів даних – встановлює порядок розгляду та виконання запитів щодо доступу, виправлення, видалення персональних даних та інших прав суб'єктів відповідно до статей 15-22 GDPR.

3. Процедура управління згодами – визначає механізми отримання, зберігання та відкликання згод на обробку персональних даних, що відповідають вимогам статті 7 GDPR щодо умов згоди.

4. Процедура оцінки впливу на захист даних (DPIA) – встановлює методологію проведення оцінки ризиків для прав і свобод фізичних осіб при впровадженні нових процесів обробки даних, відповідно до статті 35 GDPR.

5. Політика реагування на інциденти безпеки даних - визначає алгоритми дій у разі виявлення порушень безпеки персональних даних, включаючи процедури повідомлення наглядових органів та суб'єктів даних відповідно до статей 33-34 GDPR.

Важливим аспектом впровадження внутрішніх політик є їх інтеграція в загальну систему управління організацією. Як зазначається в керівних принципах Європейського комітету із захисту даних, "для забезпечення ефективності політик захисту персональних даних необхідно інтегрувати їх на рівні бізнес-процесів, щоб вимоги до захисту даних були органічно вбудовані в щоденну діяльність організації». На основі цього, представлено наступний підхід до розробки внутрішніх політик на рис. 2.1.

Рис. 2.1. Розробка внутрішніх політик для захисту персональних даних у компанії

Принцип підзвітності є одним із ключових положень GDPR, який зобов’язує компанії не лише дотримуватися вимог щодо захисту персональних даних, а й мати можливість підтвердити свою відповідність цим вимогам перед контролюючими органами. Це означає впровадження системних організаційних заходів, які забезпечують прозорість та контроль за процесами обробки даних.

Зокрема, компанія повинна вести детальну документацію, що включає реєстр операцій обробки персональних даних із зазначенням цілей обробки, категорій даних, строків зберігання та правових підстав. Така документація є основою для демонстрації відповідності вимогам GDPR і формує системний підхід до управління даними.

Для формування культури відповідальності в організації необхідно розробити внутрішні політики та процедури, які регламентують порядок обробки даних, а також регулярно проводити навчання працівників щодо вимог GDPR і їх ролі у захисті даних. Компанія має забезпечувати прозорість для суб'єктів даних, інформуючи їх про те, які дані збираються, з якою метою, на яких підставах і як довго зберігатимуться ці дані, що сприяє підвищенню довіри та дотриманню принципу законності і справедливості. Для практичної реалізації принципу підзвітності компаніям рекомендується проводити регулярні аудити, впроваджувати системи моніторингу та контролю, а також підтримувати в актуальному стані внутрішні політики і процедури. Такий системний підхід дозволяє не лише відповідати законодавству, але й підвищувати рівень захисту персональних даних, зменшуючи ризики виникнення порушень і негативних наслідків для бізнесу [28]. Оскільки GDPR не пропонує конкретного підходу до побудови таких систем контролю, організації можуть використовувати міжнародні фреймворки. Деякі з них будуть узагальнено розглянути далі.

ISO 27001 [29] – це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (ISMS). Він включає процедури оцінки ризиків, впровадження контролів безпеки, моніторинг і постійне вдосконалення системи. Він допомагає організаціям формалізувати політики, процеси та технічні заходи, що відповідають принципам GDPR, зокрема впровадженню концепції Privacy by Design і Privacy by Default. Вони закладені у статті 25 GDPR. і покликані забезпечити системний захист персональних даних на всіх етапах їх обробки.

Privacy by Design означає, що захист персональних даних та дотримання

принципів конфіденційності мають бути інтегровані безпосередньо у проєктування та розробку систем, продуктів і послуг - від початкової ідеї до повного життєвого циклу. Це передбачає врахування ризиків для приватності вже на стадії планування, застосування технічних і організаційних заходів для мінімізації цих ризиків, а також постійне підтримання захисту даних у процесі функціонування системи.

Privacy by Default означає, що налаштування системи за замовчуванням мають гарантувати максимальний рівень захисту персональних даних без необхідності додаткових дій з боку користувача. Іншими словами, користувач, взаємодіючи з продуктом чи сервісом, автоматично отримує найвищий рівень приватності, і персональні дані не збираються або не обробляються понад мінімально необхідний обсяг без його свідомої згоди. Це забезпечує автоматичний захист права на недоторканність приватного життя, який реалізується за замовчуванням у будь-якій системі.

Разом з ISO 27001 існує стандарт ISO 27701 [30], що надає вказівки щодо впровадження, управління та постійного вдосконалення системи управління приватністю як частини системи управління інформаційною безпекою. Він визначає вимоги до обробки даних згідно з GDPR та ролі контролера та обробника. Схема комбінації цих стандартів для забезпечення відповідності GDPR представлена на рис. 2.2.

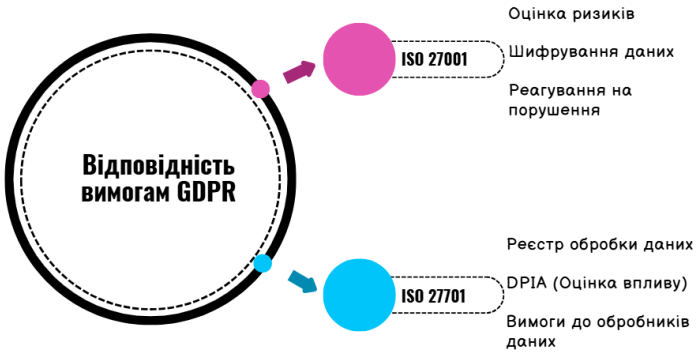

Рис. 2.2. Стандарти ISO для забезпечення відповідності вимогам GDPR

NIST Privacy Framework [31], розроблений Національним інститутом стандартів США (NIST), допомагає організаціям системно керувати захистом персональних даних. Завдяки цьому фреймворку компанії можуть ефективно виконувати статті GDPR, що стосуються безпеки обробки та повідомлення про порушення. Визначає 5 ключових функцій, які охоплюють весь життєвий цикл управління кібербезпекою в організації (рис. 2.3)

1. Identify (Ідентифікація)
   a) Визначення, які персональні дані обробляються.
   b) Мапування потоків даних (наприклад, від клієнта до хмарного сховища).
2. Govern (Управління)
   a) Створення політик приватності (хто відповідає, які цілі обробки).
   b) Відповідність до Article 5 GDPR (принципи обробки даних).
3. Control (Контроль)
   a) Технічні заходи: шифрування, обмеження доступу (Article 32).
   b) Договори з обробниками даних (Article 28).
4. Communicate (Комунікація)
   a) Інформування користувачів про їхні права (Articles 12–14).
   b) Прозорість (наприклад, оновлення Політики конфіденційності).
5. Protect (Захист)
   a) Запобігання витокам даних (Data Loss Prevention).
   b) Моніторинг інцидентів (обов'язок повідомляти про порушення за Article 3)

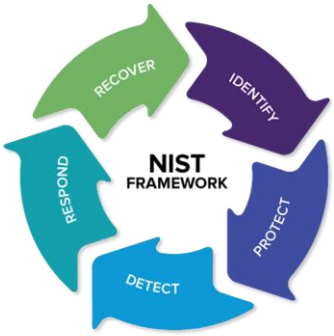

Рис. 2.3. Цикл керування даними згідно NIST Privacy Framework

2.2 Оцінювання впливу на захист даних

Оцінювання впливу на захист даних – процедура яка передбачена статтею 35 GDPR. Регламент вимагає її здійснення за трьох умов:

1. Систематичного та масштабного оцінювання персональних аспектів, що стосуються фізичних осіб, яке ґрунтується на автоматизованому опрацюванні, в тому числі, профайлінгу, та на якому ґрунтуються рішення, що мають юридичні наслідки щодо фізичної особи чи подібним чином істотно впливають на фізичну особу.

2. Широкомасштабного опрацювання спеціальних категорій даних, вказаних у Статті 9, та персональних даних про судимості і кримінальні злочини, вказані в Статті 10.

3. Систематичного та широкомасштабного моніторингу зони, що знаходиться у відкритому доступі.

DPIA допомагає організаціям виявляти та мінімізувати ризики для конфіденційності, і зазвичай проводиться перед впровадженням нових процесів, проектів або політик. DPIA має на меті виявити потенційні проблеми, щоб їх можна було вирішити заздалегідь, зменшивши таким чином ймовірність їх виникнення та пов'язані з ними витрати. Крім того, DPIA має приносити безпосередню користь організації, покращуючи політику, процеси та системи, а також зміцнюючи відносини з клієнтами та зацікавленими сторонами. Оцінювання повинне містити принаймні систематичний опис передбачених операцій опрацювання та цілі опрацювання, в тому числі, за необхідності, законний інтерес контролера, оцінювання необхідності та пропорційності операцій опрацювання щодо цілей, оцінювання ризиків для прав і свобод суб'єктів даних, вказаних в умовах опрацювання. Також DPIA повинна містити заходи, передбачені для боротьби з ризиками, в тому числі, гарантії, заходи безпеки та механізми забезпечення захисту персональних даних та доведення відповідності Регламенту GDPR, з урахуванням прав і законних інтересів суб'єктів даних та інших залучених осіб [32,33].

2.3 Технологічні засоби забезпечення захисту персональних даних

Принципи Privacy by Design та Privacy by Default повинні реалізовуватись у системі і при використанні технологічних засобів для захисту персональних даних [34]. Регламент GDPR висуває 4 вимоги, які стосуються забезпечення належного рівня безпеки інформації.

1. Використання псевдонімів і шифрування персональних даних.
2. Наявність та стійкість систем та послуг опрацювання.
3. Здатність вчасно відновити наявність і доступ до персональних даних у випадку технічної аварії.
4. Створення процесу для регулярного тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки опрацювання даних.

Використання псевдонімів або псевдонімізація – процес відокремлення особи суб'єкта даних від персональних даних, які обробляються для цього суб'єкта даних. Як правило, такий процес може здійснюватися шляхом заміни одного або декількох персональних ідентифікаторів, що стосуються суб'єкта даних, так званими псевдонімами, наприклад, випадково згенерованими значеннями. Стандарт ISO 25237 [35] називає цей процес особливим тип знеособлення, який одночасно усуває зв’язок із суб’єктом даних і встановлює зв’язок між певним набором характеристик, що стосуються суб’єкта даних, та одним або кількома псевдонімами. GDPR визначає поняття псевдонімізації як обробку персональних даних таким чином, що персональні дані більше не можуть бути пов'язані з конкретним суб'єктом даних без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо і до неї застосовуються технічні та організаційні заходи, що унеможливлюють зв'язок персональних даних з конкретною фізичною особою, яка може бути ідентифікована або визначена [36]. Важливо уточнити що псевдонімізована інформація відрізняється від анонімізованої тим, що при певних обставинах та маючи додаткову інформацію, з її допомогою все ще

можна ідентифікувати особу [37]. Це означає що псевдонімізовані дані все ще залишаються персональними даними суб'єкта і вимоги Регламенту GDPR стосовно їх захисту та обробки залишаються актуальними. Анонімізована інформація, яка вже ніяк не може бути використана для ідентифікації особи виходить за межі дії регламенту, оскільки не вважається персональними даними. Додаткова інформація яка може використовуватись для обернення процесу псевдонімізації повинна розділятись з псевдонімізованою інформацією щоб при витоку даних, зловмисник не отримав доступ до обох видів даних і таким чином не міг ідентифікувати особу, яка є суб'єктом цих даних. Загалом же, використання псевдонімізації підвищує безпеку обробки інформації, зменшує ризики для суб'єктів даних та дозволяє використовувати інформацію у дослідженнях та іншій аналітичній діяльності, при цьому не збільшуючи шанс ідентифікації осіб, дані яких оброблюються [38, 39].

Існує багато методів здійснення псевдонімізації [40, 41]. Серед них:

1. Хешування без ключа: класичне хешування з використанням стандартної хеш-функції (наприклад, SHA-256), без додаткових значень.

2. Хешування з ключем: криптографічне хешування з використанням секретного ключа (наприклад, HMAC-SHA-256), яке забезпечує кращий захист.

3. Шифрування: перетворення даних у зашифрований вигляд з дешифруванням за наявності ключа. Це дає можливість тимчасово приховати ідентифікатор і, за потреби, повернути його назад.

4. Токенізація: лзаміна даних на токен – унікальний символ чи рядок, який не має математичного зв'язку з початковими даними, які в свою чергу зберігаються на безпечному токен-сервері.

Шифрування є одним з найголовніших технічних заходів захисту персональних даних. GDPR прямо зазначає шифрування як відповідний технічний захід для забезпечення рівня безпеки, який відповідає рівню ризику обробки персональних даних. Стаття 34 регламенту звільняє контролера даних від обов'язку повідомляти суб'єкта даних про порушення безпеки, якщо до даних було застосовано шифрування. Конкретні види та правила шифрування

регламент не вказує, тому організації самі можуть вибирати, який рівень шифрування відповідає її потребам [42, 43, 44, 45]. Шифрування даних можна виконувати коли вони знаходяться в стані спокою, під час передачі, та під час обробки.

Дані в стані спокою зберігаються у базах даних, файлових системах, хмарних сховищах або на фізичних носіях. Для даних у стані спокою зазвичай застовують симетричне шифрування, наприклад AES-256. Шифрування даних під час передачі забезпечуються протоколами, такими як Transport Layer Security (TLS) та Secure Sockets Layer (SSL). Для шифрування даних під час обробки існує перспективне рішення – гомоморфне шифрування яке дозволить виконувати обчислення над зашифрованими даними без їх дешифрування. Загалом, вибір конкретних алгоритмів шифрування повинен здійснюватися з урахуванням контексту обробки даних, включаючи чутливість інформації, вимоги до продуктивності та специфіку операційного середовища. Також слід приділити увагу управлінню криптографічними ключами – фізичними або хмарними засобами.

Слід розуміти що зашифровані дані все ще вважаються персональними даними, бо можуть бути повернені до звичайного стану за допомогою криптографічного ключа [46]. Тому, окрім шифрування слід застосовувати додаткові засоби захисту – контроль доступу, системи виявлення та запобігання вторгненням (IDS/IPS), рішення для моніторингу безпеки, управління подіями та інформацією безпеки (SIEM) та інструменти аналізу поведінки користувачів і об'єктів (UEBA). Ці системи повинні бути налаштовані для швидкого виявлення потенційних порушень, щоб забезпечити дотримання 72-годинного терміну повідомлення суб’єкту даних про факт порушення встановленого GDPR.

Важливим аспектом відповідності регламенту GDPR залишається реалізація прав суб’єктів даних. Організації повинна впроваджувати технологічні рішення для ефективного управління згодою та забезпечення реалізації цих прав [47]. Технології управління згодою повинні дозволяти

надавати суб’єктам даних згоди для обробки своїх даних для різних цілей, а також зберігати час, спосіб надання згоди та її конкретний зміст. Крім того, технологічні рішення повинні дозволяти суб’єктам легко здійснювати і інші свої права – такі як права на доступ, виправлення, видалення, забуття та перенесення даних. Це вимагає створення автоматизованих систем, здатних ідентифікувати всі персональні дані, пов’язані з конкретним суб’єктом та виконувати відповідні дії на запити.

Крім того, рекомендовано автоматизувати і процес оцінки впливу на захист даних. Автоматизовані інструменти для DPIA можуть значно полегшити цей процес забезпечивши систематичний аналіз ризиків та документування рішень. Ці інструменти можуть включати шаблони для документування процесів обробки, каталоги ризиків та заходів контролю, а також функції для автоматизованого аналізу ризиків на основі встановлених критеріїв. До того ж, автоматизований процес документації може допомогти продемонструвати відповідність вимогам GDPR, генеруючи звіти та документацію яка може бути надана наглядовим органам.

Висновки до розділу 2

Забезпечення відповідності вимогам регламенту GDPR потребує комплексного та системного підходу, який повинен реалізувати дотримання організацією принципів GDPR та прав суб’єкта даних. Внутрішні політики і процедури, такі як політики конфіденційності і реагування на інциденти процедури реагування на запити суб’єктів і управління згодами та DPIA повинні бути інтегрованими у діяльність організації та її бізнес-процеси щоб бути достатньо ефективними. Для цього є доцільним використання міжнародних стандартів, зокрема ISO 27001 та ISO 27701, які забезпечують методологічну базу для управління інформаційною безпекою та персональними даними, а також сприяють реалізації концепцій Privacy by Design та Privacy by

Default, які згідно регламенту вимагають вбудованого захисту персональних даних у саму архітектуру систем і процесів.

Важливим елементом організаційної структури є посада співробітника з питань захисту даних, який виконує функції контролю, консультування та взаємодії з наглядовими органами. На основі проаналізованих досліджень, можна зробити висновок що проблеми потрібної кількості фахівців на ринку, недостатніх повноваженнь DPO та розподілу обов'язків цієї посади між іншими співробітниками, є актуальними в багатьох організаціях. Приділено увагу необхідності забезпечення незалежності цієї посади, надання потрібних ресурсів та підтримки з боку керівництва.

Технологічні рішення відіграють ключову роль у забезпеченні відповідності GDPR, надаючи організаціям інструменти для реалізації принципів і вимог регламенту. Однак, технологічні рішеня не можуть забезпечити цю відповідність, якщо вони не доповнені відповідними політиками та організаційними заходами. Як технологічні, так і організаційні заходи повинні охоплювати весь життєвий цикл даних – від збору інформації, до обробки, зберігання та видалення, і взаємодіяти між собою для успішної діяльності, пов'язаної з процесами обробки персональних даних.

Розділ 3 СПЕЦИФІКА РЕАЛІЗАЦІЇ ВИМОГ GDPR У СИСТЕМАХ ЕЛЕКТРОННОГО НАВЧАННЯ

3.1. Особливості обробки даних в освітніх платформах

Цифровізація освітнього середовища стає все більш актуальною темою в останні роки, як в Україні, так і у світі. Системи електронного навчання дозволяють створювати віртуальне освітнє середовище, де учні та студенти можуть взаємодіяти з навчальними матеріалами та з викладачами у будь-який час та з будь-якого місця. Такі освітні платформи оброблюють значні обсяги інформації, в тому числі таку інформацію, яка підпадає під дію Регламенту GDPR. Цей розділ буде присвячено дослідженню методів реалізації вимог GDPR у системах електронного навчання.

Перед тим як визначитись з методами захисту, необхідно визначити які саме дані оброблюються у системах електронного навчання, та потребують захисту [48, 49]. Класифікація даних про користувачів системи представлена у табл. 3.1.

Таблиця 3.1

Види персональних даних що оброблюються у e-learning системах

Ідентифікаційні дані	Ім’я, прізвище, контактні дані, логіни, паролі унікальний ідентифікатор користувача
Навчальні дані	Виконані завдання, результати тестів, оцінки, прогрес у курсах, коментарі викладачів
Поведінкові дані	Час входу-виходу, статистика відвідуваності та активності, взаємодії з іншими користувачами
Технічні та метадані	IP-адреси, дані геолокації, файли cookie, інформація про пристрої та браузери
Спеціальні категорії даних	Дані про здоров’я (у випадку адаптації навчання для людей з особливим потребами), біометричні дані

Тепер розглянемо типові сценарії роботи з даними, які існують в системах електронного навчання. [50].

1. Адміністрація навчального процесу: реєстрація та автентифікація користувачів, управління доступом до курсів. Потребує збору та зберігання персональних даних для створення облікових записів.

2. Навчальна активність: зберігання та оцінювання робіт, відстеження прогресу студента, взаємодія студентів з викладачами.

3. Аналітика та персоналізація: аналіз активності та успішності студента, персоналізовані рекомендації щодо курсів чи адаптація контенту під потреби користувача на основі зібраних даних.

4. Дослідницька діяльність: оцінка ефективності навчальних програм, формування звітів, передача зібраних даних поза межі освітньої платформи (наприклад у Міністерство Освіти).

На основі перелічених процесів можна зробити висновок що будь-яка взаємодія з системами електроного навчання пов’язана зі збором та обробкою інформації та генерацією метаданих, що викликає певні ризики, які стосуються безпеки цих даних. Такі ризики можна поділити на три види – технологічні, управлінські та операційні ризики користувачів [51].

До технологічних ризиків відносяться помилки в конфігурації серверів або протоколах, вразливості у мережі, операційній системі та системах управління базами даних. Використання вразливостей апаратного та програмного забезпечення може призвести до вторгнення у систему, несанкціонованого доступу до даних чи витоку інформації, що ставить під загрозу конфіденційність користувачів.

Управлінські ризики стосуються насамперед адміністративного та IT-персоналу, який керує навчальною платформою та відстежує дії користувачів [52]. Сюди входить збір інформації без отримання попереднього дозволу, відсутність забезпечення конфіденційності на якомусь із етапів життєвого циклу даних, зміна конфігурацій платформи, помилки при наданні прав доступу деяким користувачам. Також в цю категорію можна включити

відсутність заходів з періодичного обслуговування, відновлення після аварій або резервного копіювання.

Ризики пов’язані з операціями користувачів зазвичай стосуються автентифікації користувача. Встановлення легких паролів або його розповсюдження, наявність шкідливого програмного забезпечення яке збирає їх дані та незаконно отримує доступ до системи, використання незахищених публічних мереж. Також користувачі через недбалість чи байдужість можуть не звернути увагу на умови конфіденційності та надати дозвіл збирати персональні дані без їх згоди, які не потрібні для цілей навчання.

Окрему увагу слід звернути на підстави, за якими персональні дані учнів можуть оброблюватись згідно регламенту GDPR. Якщо мова йде про платформи з онлайн-курсами, то тоді для обробки персональних даних вимагається згода суб’єкта даних або батьків чи опікунів, якщо суб’єкту даних менше 13-16 років (рік відрізняється у різних країнах ЄС). Якщо це стосується онлайн-навчання у державних освітніх закладах, зазвичай обробка персональних даних у них здійснюється на підставі суспільного інтересу або виконання договору про надання освітніх послуг, тому надання згоди суб’єкта даних не потрібно. Однак для деяких видів персональних даних які виходять за рамки необхідних для навчання, буде необхідно окремо отримувати згоду суб’єкта даних, що створює необхідність реалізації системи отримання та управління згодами.

3.2. Визначення та документування правових підстав обробки

Основним елементом відповідності GDPR є правильне визначення та документування правових підстав для кожної операції з обробки персональних даних. Освітні установи повинні чітко визначити правові підстави для кожного типу даних, що обробляються в системах електронного навчання, і прозоро інформувати про мету використання цих даних здобувачів освіти [53, 54].

- Виконання договору

Виконання договору є найбільш актуальною правовою підставою для основних функцій систем е-навчання, оскільки обробка даних є невід'ємною частиною надання освітніх послуг за договором між закладом та здобувачем освіти. Приклади застосування: реєстрація облікових записів студентів та викладачів, відстеження прогресу навчання, оцінювання та сертифікація, технічна підтримка навчальної платформи. Необхідні заходи:

1. Чітке визначення обсягу необхідних даних для виконання договору.
2. Регулярний аудит даних для забезпечення відповідності принципу мінімізації.
3. Документування зв'язку між обробкою даних та договірними зобов'язаннями.

Важливо розмежовувати дані, необхідні для виконання основного договору про надання освітніх послуг, та додаткові дані, що вимагають іншої правової підстави.

- Законні інтереси

Приклади застосування: аналітика використання навчальної платформи для її вдосконалення, моніторинг якості навчального процесу, заходи забезпечення безпеки. Необхідні заходи:

1. Проведення та документування тесту балансування інтересів.
2. Забезпечення можливості заперечення проти обробки.
3. Регулярний перегляд та актуалізація оцінки законних інтересів.

Законні інтереси можуть бути відповідною підставою для використання персональних даних для аналітики навчальних процесів, якщо навчальний заклад може продемонструвати, що переваги для якості освіти переважають потенційні ризики для конфіденційності [54]. Тест балансування інтересів – це

процес, який дозволяє визначити, чи може обробка персональних даних на основі законного інтересу контролера бути правомірною, і чи інтереси або основні права та свободи суб'єкта даних не переважають цей інтерес.

Згідно з останніми рекомендаціями Європейського комітету з захисту даних (EDPB), для застосування правової підстави законного інтересу необхідно виконати три умови які представлені на табл. 3.2.

Таблиця 3.2.

Тест балансування інтересів

Ідентифікація законного інтересу	Чіткий опис цілі обробки Законність мети Реальна практична потреба
Перевірка необхідності	Необхідність обробки Відсутність альтернативних шляхів
Балансування інтересів	Вплив на суб’єкт даних Характер даних Очікування суб’єктів

- Законний обов'язок

Застосовується коли обробка необхідна для виконання законного обов’язку. Приклади застосування: зберігання даних про академічні досягнення відповідно до вимог освітнього законодавства, надання інформації контролюючим органам, виконання податкових зобов'язань. Необхідні заходи:

1. Документування конкретних юридичних вимог, що обґрунтовують обробку.
2. Обмеження обробки лише необхідними для виконання обов'язку даними.
3. Встановлення відповідних термінів зберігання даних.

- Виконання завдання в суспільних інтересах.

Особливо актуально для державних освітніх закладів та офіційно визнаних освітніх програм. Приклади застосування: збір та аналіз статистичних

даних для забезпечення якості освіти. Організація освітнього процесу в умовах дистанційного навчання. Забезпечення інклюзивності та доступності освіти. Необхідні заходи:

1. Чітке визначення суспільного інтересу, що виправдовує обробку.
2. Забезпечення пропорційності обробки меті.
3. Документування юридичної основи для виконання завдання в суспільних інтересах.

• Згода - використовується для операцій з обробки, що виходять за межі основних освітніх функцій. Приклади застосування: публікація фотографій студентів на веб-сайті закладу, використання даних для маркетингових цілей, передача даних третім сторонам для необов'язкових інтеграцій, обробка особливих категорій даних (стан здоров'я, релігійні переконання тощо). Необхідні заходи:

1. Розробка чітких форм згоди з детальним описом цілей обробки.
2. Впровадження механізмів відкликання згоди.
3. Документування всіх наданих та відкликаних згод.

Неналежна документація правових підстав є одним з найпоширеніших недоліків відповідності регламенту [56, 57]. Для дотримання вимог GDPR необхідно створити реєстр операцій з обробки даних, що відповідає вимогам статті 30 та включає перелік усіх категорій даних, що обробляються, цілі обробки для кожної категорії та правову підставу для кожної операції, а також терміни зберігання даних і заходи безпеки, як технічні, так і організаційні.

3.3. Забезпечення реалізації прав користувачів у системах електронного навчання

Ключовим фактором відповідності компанії регламенту GDPR є забезпечення прав суб’єктів даних. Студенти повинні мати змогу звернутись до платформи та заявити про своє бажання реалізувати ці права, видаливши свої персональні дані з системи, що їх оброблює або виконати інші дії, передбачені

регламентом. Далі запропоновано методи реалізації прав користувачів та інших механізмів, які допоможуть організації своєчасно та правильно оброблювати запити суб’єктів щодо обробки їх персональних даних.

- Право на інформацію (ст. 13-14 GDPR).

1. Багаторівнева політика конфіденційності.
   a) Перший рівень: короткий огляд практик обробки даних.
   b) Другий рівень: детальна політика конфіденційності.
2. Контекстуальні повідомлення про обробку даних в ключових точках взаємодії.
3. Візуалізація процесів обробки даних за допомогою інфографіки
4. Адаптація інформації для різних вікових груп (особливо для неповнолітніх).

- Право на доступ (ст. 15 GDPR).

1. Панель управління персональними даними в особистому кабінеті.
2. Функціональність експорту даних у машиночитаному форматі.
3. Автоматизований процес обробки запитів на доступ до даних.
4. Механізми верифікації особи для безпечного надання доступу.

- Право на виправлення (ст. 16 GDPR).

1. Зручний і зрозумілий інтерфейс редагування профілю.
2. Процедура верифікації змін для чутливих даних.
3. Журналювання змін для забезпечення цілісності даних.
4. Автоматичне оновлення даних у всіх пов'язаних системах.

- Право на видалення, або ж право на забуття (ст. 17 GDPR).

1. Диференційований підхід до видалення.
   a) Повне видалення необов'язкових даних.
   b) Псевдонімізація обов'язкових даних, що мають зберігатися з законних причин.
2. Чітка процедура обробки запитів на видалення.
3. Каскадне видалення даних з усіх пов'язаних систем та резервних копій.

4. Документування підстав для відмови у видаленні, якщо застосовано.

• Право на обмеження обробки (ст. 18 GDPR).

1. Технічні засоби тимчасового блокування обробки.

2. Система маркування даних з обмеженою обробкою.

3. Автоматичне повідомлення всіх обробників про обмеження.

4. Процес періодичного перегляду обмежень обробки.

• Право на перенесення даних (ст. 20 GDPR).

1. Експорт даних у стандартних форматах (XML, JSON, CSV) API для прямого перенесення даних між платформами.

2. Інструменти для вибіркового експорту окремих категорій даних.

3. Детальна документація структури даних для полегшення їхньої інтерпретації.

• Право на заперечення (ст. 21 GDPR).

1. Простий механізм відмови від обробки на основі законних інтересів.

2. Гранульований контроль, над тим, від якого типу обробки відмовляється користувач.

3. Автоматичне припинення відповідної обробки після отримання заперечення.

4. Чітке пояснення наслідків заперечення для функціональності системи.

Хоча згода не є основною правовою підставою для більшості операцій з обробки в освітніх платформах, ефективна система управління згодами необхідна для специфічних сценаріїв. Те що в ній повинно бути реалізовано:

1. Гранульована система згод для різних необов'язкових видів обробки.

2. Центр керування згодами в особистому кабінеті користувача.

3. Прості та зрозумілі формулювання запитів на згоду.

4. Механізми батьківського контролю для неповнолітніх користувачів.

5. Журналювання історії згод для аудиту та доказів відповідності вимогам.

• Автоматизація обробки запитів суб'єктів даних.

Для ефективного забезпечення прав суб'єктів даних доцільно впровадити:

1. Портал самообслуговування для автоматизованої обробки типових запитів.
2. Систему управління запитами для відстеження та документування нетипових звернень.
3. Шаблони відповідей на різні типи запитів.
4. Систему повідомлень та нагадувань для своєчасної обробки запитів.
5. Регулярний аудит ефективності процесів обробки запитів.

Для забезпечення інших принципів захисту та обробки інформації, які висуваються регламентом GDPR, створено загальну схему технічних заходів захисту, яку зображено на рис. 3.1.

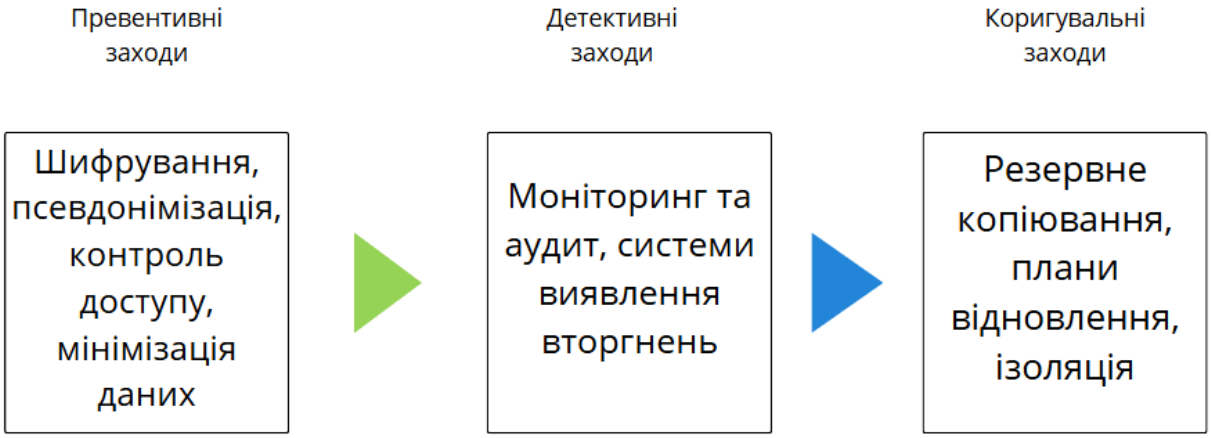

Рис. 3.1. Технічні заходи захисту інформації.

Превентивні заходи, такі як псевдонімізація та шифрування, покликані забезпечити безпеку даних шляхом ускладнення ідентифікації особи та захисту даних під час їх зберігання та передачі. Мінімізація відображає один з принципів GDPR про обробку мінімальної кількості даних для досягнення цілі. Не слід забувати і про DPIA. В контексті систем електронного навчання, проведення оцінювання впливу на захист даних обов'язково у випадках, коли у системі велика кількість користувачів, використовуються хмарні рішення з міжнародною передачею даних, проводиться збір даних про поведінку або використовується штучний інтелект та засоби машинного навчання для персоналізації навчання. Також DPIA проводиться повторно з плином часу або

при впровадженні нових технологій у існуючу систему. Схожі правила стосуються і створення посади DPO, як ключової ролі у контролі інформації. Якщо це державний або публічний навчальний заклад, фахівець повинен бути призначеним на цю посаду для контролю відповідності регламенту та співпраці з наглядовими органами.

Плани відновлення як коригувальний захід є важливими не тільки з точки зору безперервності роботи системи. Окрім технічних аспектів, ці плани повинні включати процедури повідомлення суб'єктів даних та наглядових органів у разі порушення обробки і безпеки персональних даних.

Висновки до розділу 3

Системи електронного навчання обробляють досить широкий спектр даних різних категорій та для різних цілей. У цьому розділі було визначено що крім звичайних ідентифікаторів, у них оброблюються поведінкові дані, академічні досягнення та деякі спеціальні категорії. Це вимагає комплексного підходу до захисту з урахуванням особливостей конкретної освітньої платформи. Реалізація вимог GDPR повинна будуватись на чіткому визначенні підстав для обробки даних, правильному збору згод щодо їх обробки та належному інформуванню суб'єктів даних щодо цілей обробки та можливих проблем.

Безумовно, головним показником відповідності GDPR є можливість реалізації прав суб'єктів даних. Для цього у роботі запропоновано декілька механізмів до кожного з прав суб'єктів. Їх реалізація, разом з системою збору та управлінням згодами, допоможе оброблювати дані студентів не тільки безпечно, але й ефективно, якщо для цього будуть залучені автоматизовані системи.

В залежності від виду навчальної платформи, типу і обсягів даних які там оброблюються, навчальним закладам потрібно визначитись з відповідальними за контроль персональних даних та відповідності нормам регламенту. Якщо

мова йде про державні або великі приватні заклади освіти, створення посади DPO є необхідним, як і надання йому повноважень для здійснення контролю та комунікації з регуляторними органами. В інших випадках більшість його повноважень можуть виконувати інші особи, а за потреби наймати консультанта від третьої сторони, який буде регулювати правовідносини з наглядовими органами.

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто Загальний регламент із захисту даних GDPR, область його дії та категорії даних якими він оперує. Визначено сутність персональних даних у контексті регламенту, поняття контролера та суб'єкта даних. Після аналізу документу було здійснено категоріювання персональних даних – звичайні персональні дані, спеціальної категорії (дані про етнічну приналежність, політичні переконання, релігійні чи філософські вірування, членство в професійних спілках, генетичні і біометричні дані) та дані про кримінальні правопорушення. Створено порівняльну таблицю, у якій продемонстровано різницю між підставами обробки для різних категорій даних, у якій також окремо виділено дані про дітей, за яких згоду оброблювати власні персональні дані можуть надати лише батьки та опікуни. Серед підстав для обробки звичайних персональних даних можна виділити виконання договору або законних зобов'язань, виконання завдань суспільного інтересу або законний інтерес. Спеціальні категорії даних, окрім явної згоди суб'єкта, також можна обробляти, якщо мова йде про захист життєвих інтересів, судову чи медичну допомогу, для трудового прафа а також у діяльності фондів та організацій. Опрацювання персональних даних про судимості і кримінальні злочини здійснюють лише під контролем офіційного органу.

Розглянуто основні принципи стосовно обробки даних, такі як законність, справедливість, прозорість, цільове обмеження, мінімізація даних і обмеження зберігання. Також було досліджено права суб'єктів даних – на видалення, перенесення, забуття, інформування, виправлення та інші. Завдяки аналізу наведеної статистики штрафів та дослідженням інших науковців було з'ясовано про такі недоліки GDPR як нерівномірність застосування санкцій в різних країнах, високі витрати на впровадження вимог і складність реалізації для невеликих організацій. Саме ця проблема і стала вектором наступних досліджень в цій роботі.

Розглянуто організаційні заходи забезпечення відповідності вимогам

GDPR. Запропоновано використання стандартів серії ISO та NIST, а також список політик які необхідно створити для забезпечення надійного рівня безпеки даних. Особливу увагу приділено DPIA, яке є обов'язковим для компаній що займаються систематичними та масштабними опрацюваннями персональних даних. DPIA виявляє ризики заздалегідь, щоб мати можливість їх мінімізувати. Багато уваги в дослідженні приділено DPO – співробітнику з питань захисту даних. Він співпрацює з наглядовим органом, проводить DPIA та стежить за дотриманням GDPR та виконанням заходів з безпеки. Проблеми його діяльності також були проаналізовано, оскільки в багатьох організаціях вони не наділені достатньою кількістю повноважень, або його обов'язки перекладаються на інші відділи, що впливає на загальний процес забезпечення безпеки. Тому підтримка DPO ресурсами та прямим зв'язком з вищим керівництвом щоб забезпечити його незалежність, може стати вирішальною для відповідності організації всім вимогам GDPR.

Дослідивши специфіку персональних даних та процесів, які відбуваються у системах електронного навчання, було створено декілька заходів для кожного типу процесів, який підпадає під певну підставу для обробки даних. Крім того, були запропоновані методи забезпечення усіх прав для суб'єктів, чиї персональні дані оброблюються у системі, включаючи систему управління згодами та автоматизовану обробку запитів суб'єктів даних.

Загалом, як методи для захисту персональних даних у компанії згідно вимог GDPR були представлені реєстри обробки даних, документування, псевдонімізація, системи управління доступом, шифрування та вище перераховані технічні і організаційні заходи. Для подальших досліджень рекомендується звернути увагу на оптимізацію цих заходів для інтегрування їх у повсякденну діяльність компанії чи закладу, впровадження автоматизованих систем видалення даних, після завершення навчання та розробки інтерактивних інструментів для інформування студентів про політики безпеки та їх права, як суб'єктів даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).
URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

2. Kuner, C. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020. P. 89-95.

3. European Parliament and Council of the European Union. Regulation (EU) 2016/679, Recital 26. Official Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

4. European Data Protection Board. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 1.0. 2019. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en

5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р.
URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

6. Директива 95/46/ЄС Європейського парламенту та Ради від 24 жовтня 1995 року про захист осіб у зв’язку з обробкою персональних даних і про вільний рух таких даних, №281/31, 23.11.1995. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

7. Kuner C. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013. 368 p.

8. Bygrave L. A. Data Privacy Law in Context. Data Privacy Law. 2014. P. 1–30. DOI: https://doi.org/10.1093/acprof:oso/9780199675555.003.0001

9. Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Cham: Springer, 2014. 274 p.

10. Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015. 352 p.

11. Romansky, R.P., & Noninska, I.S. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288–5303p.

12. European Data Protection Supervisor. Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package, 2012.

13. Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Cham: Springer, 2014. 274 p.

14. Вишневський В.О. Ретроспектива розвитку європейського законодавства у сфері захисту персональних даних. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Вип. 68. С. 58–62.

15. Bygrave L. A. Data Protection Law: Approaching its Rationale, Logic and Limits. Dordrecht: Kluwer Law International, 2002. 329 p.

16. Tikkinen-Piri C., Rohunen A., Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. 2018. Vol. 34, Issue 1. P. 134–15. DOI: https://doi.org/10.1016/j.clsr.2017.05.015

17. Бочкова І. І., Врублевська-Місюна К. М. Права суб'єктів персональних даних як складова інформаційних прав людини. Серія: Право. Випуск 80. Том 1. 2023. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/58352

18. Mladinić A., Vukić Z., Rončević A. GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises. Journal of Law and Social Sciences of the Law Faculty of University J.J. Strossmayer in Osijek. 2023. Vol. 39, No. 3–4. C. 53–75. DOI: https://doi.org/10.25234/pv/23972

19. European Data Protection Board. Annual report 2022. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2022_en

20. DLA Piper. GDPR fines and data breach survey: January 2023. [Online]. URL: https://www.dlapiper.com/en/insights/publications/2023/01/gdpr-fines-and-data-breach-survey-2023/

21. CMS. GDPR Enforcement Tracker Report. Numbers and Figures. 2024. [Online]. URL: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures

22. McKinsey & Company. Tackling GDPR compliance before time runs out. McKinsey & Company. 2017. URL:https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/tackling-gdpr-compliance-before-time-runs-out

23. PwC India. Readiness of India Inc. for the Digital Personal Data Protection Act. PwC Analysis 2023.

24. Mantelero, A. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review. 2018. Vol. 34, Issue 4. p. 754–772.

25. Wolford, B. What Does a Data Protection Officer Do?. GDPR.eu. – 2021. [Online]. URL: https://gdpr.eu/data-protection-officer/

26. Fazzini K. Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but So Far It's Mostly Created Frustration for Users, Companies, and Regulators. CNBC. 2019 URL: https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html

27. The Effectiveness of the GDPR: A Study of Enforcement and Compliance. Institute for Information Law (IViR). Amsterdam : University of Amsterdam, 2021. – 112 p.

28. Voigt P., von dem Bussche A. Practical Implementation of the Requirements Under the GDPR. The EU General Data Protection Regulation (GDPR). Cham, 2017. DOI: https://doi.org/10.1007/978-3-319-57959-7_10

29. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Вид. офіц.. К. : ДП «УкрНДНЦ», 2023.

30. ДСТУ ISO/IEC 27701:2022 Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови (ISO/IEC 27701:2019, IDT).

31. National Institute of Standards and Technology (NIST). Privacy Framework Version 1.0 [Online]. URL: https://www.nist.gov/privacy-framework

32. Barezzani S. Data Protection Impact Assessment (DPIA). Encyclopedia of Cryptography, Security and Privacy. Berlin, Heidelberg, 2023. P. 1–3. DOI: https://doi.org/10.1007/978-3-642-27739-9_1813-1

33. I. T. Governance IT Governance Privacy Team, Alice White (Female Synthesized Voice). EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide, Fourth Edition. de Gruyter GmbH, Walter, 2020.

34. Bincoletto, G. Data protection by design: from privacy by design to Article 25 of the GDPR. Data Protection by Design in the E-Health Care Sector. — Baden-Baden: Nomos Verlagsgesellschaft, 2021.

35. ISO. 25237:2017. Health informatics - Pseudonymization. - Geneva: International Organization for Standardization, 2017.

36. European Data Protection Board. Guidelines 01/2025 on Pseudonymisation. Brussels: EDPB, 2025.

37. Hintze, M., & El Emam, K. Comparing the benefits of pseudonymisation and anonymisation under the GDPR. Journal of Data Protection & Privacy. 2018. Vol. 2, No. 2. P. 145–158.

38. Abu Attieh, H., Müller, A., Wirth, F., Prasser, F. Pseudonymization tools for medical research: a systematic review. BMC Medical Informatics and Decision Making. — 2025. — Vol. 25, Article 128.

39. Галінкіна В.С. Основні принципи обробки та захисту персональних даних.Науковий вісник Ужгородського Національного Університету. 2024. Вип. 111–115. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/19.pdf

40. European Union Agency for Network and Information Security (ENISA). Recommendations on shaping technology according to GDPR provisions:

An overview on data pseudonymisation. Athens: ENISA, 2018. URL: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

41. ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. Geneva: International Organization for Standardization, 2018. 46 p.

42. Hoofnagle C. J., van der Sloot B., Zuiderveen Borgesius F. The European Union General Data Protection Regulation: What It Is And What It Means. SSRN Electronic Journal. 2018. URL: https://doi.org/10.2139/ssrn.3254511

43. Quinn B. Data Protection Implementation Guide: A Legal, Risk and Technology Framework for the GDPR. Kluwer Law International, 2021.

44. Mansfield-Devine S. Meeting the needs of GDPR with encryption. Computer Fraud & Security. 2017. Vol. 2017, no. 9. P. 16–20. URL: https://doi.org/10.1016/s1361-3723(17)30100-8

45. Коробейнікова Т. І., Копач А. І. Сучасні алгоритми шифрування: детальний аналіз та перспективи розвитку. SWorldJournal. 2024. № 25-01. С. 89–95.

46. Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Human Genetics. 2018. Vol. 137, no. 8. P. 575–582. DOI: https://doi.org/10.1007/s00439-018-1919-7

47. Garber J. GDPR – compliance nightmare or business opportunity?. Computer Fraud & Security. 2018. Vol. 2018, no. 6. P. 14–15. DOI: https://doi.org/10.1016/s1361-3723(18)30055-1

48. International Conference of Data Protection and Privacy Commissioners. Resolution on E-Learning Platforms [Online]. – Brussels, 2018. – Режим доступу: https://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf

49. Trifonova I., Ivanova M. Following the GDPR to Preserve Data Privacy in an eLearning Environment. Lecture Notes in Networks and Systems. Cham, 2025. P. 324–334. DOI: https://doi.org/10.1007/978-3-031-83520-9_31

50. The SHEILA Framework: Informing Institutional Strategies and Policy Processes of Learning Analytics / Y.-S. Tsai et al. Journal of Learning Analytics. 2018. Vol. 5, no. 3. URL: https://doi.org/10.18608/jla.2018.53.2

51. Data protection in digital learning space: An overview. E. Djeki et al. INTERNATIONAL CONFERENCE ON ENGINEERING AND COMPUTER SCIENCE (ICECS) 2022: The Use of Innovative Technology in Accelerating Problems Sustainable Development, Bandar Lampung City, Indonesia. 2024. DOI: https://doi.org/10.1063/5.0204895

52. Security Issues in Digital Learning Spaces. E. DJEKI et al. 2021 IEEE International Conference on Computing (ICOCO), Kuala Lumpur, Malaysia, 17–19 November 2021. 2021. DOI: https://doi.org/10.1109/icoco53166.2021.9673575

53. Cormack A. N. A Data Protection Framework for Learning Analytics. Journal of Learning Analytics. 2016. Vol. 3, no. 1.
DOI: https://doi.org/10.18608/jla.2016.31.6

54. Hoel T., Chen W. Privacy and data protection in learning analytics should be motivated by an educational maxim–towards a proposal. Research and Practice in Technology Enhanced Learning. 2018. Vol. 13, no. 1. DOI: https://doi.org/10.1186/s41039-018-0086-8

55. Kamara I., De Hert P. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. SSRN Electronic Journal. 2018. DOI: https://doi.org/10.2139/ssrn.3228369

56. Purtova N. The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law. SSRN Electronic Journal. 2017. URL: https://doi.org/10.2139/ssrn.3036355

57. Breitbarth P. The impact of GDPR one year on. Network Security. 2019. Vol. 2019, no. 7. P. 11–13. URL: https://doi.org/10.1016/s1353-4858(19)30084-4