Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

РАЙЧУК ІСУС ВАСИЛЬОВИЧ

УДК 004.9+005.4+008

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ УПРАВЛІННЯ ПОТОКАМИ ПЕРСОНАЛЬНИХ ДАНИХ СУБ'ЄКТІВ ОСВІТНЬОГО СЕРЕДОВИЩА В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

122 Комп'ютерні науки
12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ І.В. Райчук

Науковий керівник: Хлевна Юлія Леонідівна, доктор технічних наук, професор

Київ – 2025

АНОТАЦІЯ

Райчук І.В. Моделі та методи управління потоками персональних даних суб'єктів освітнього середовища в умовах діджиталізації. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії в галузі знань інформаційні технології за спеціальністю 122 Комп'ютерні науки. Київський національний університет імені Тараса Шевченка, Київ, 2025.

Актуальність теми дослідження управління потоками персональних даних суб'єктів освітнього середовища в умовах діджиталізації зумовлена стрімким розвитком цифрових технологій, які змінюють підходи до обробки та захисту персональних даних у сфері освіти. У сучасному світі освітні установи стикаються з дедалі більшою кількістю інформаційних потоків, що містять персональні дані студентів, викладачів і співробітників. Ефективне управління цими потоками є ключовим для підтримки стабільності та безпеки всього освітнього процесу.

Діджиталізація в галузі освіти відкриває нові можливості для оптимізації навчальних процесів, робить можливим персоналізоване навчання та сприяє глобалізації освіти. Проте, разом із цими перевагами з'являються й нові виклики, зокрема суттєвий ризик порушення конфіденційності та несанкціонованого використання персональних даних. Управління ризиками витоку персональних даних – один з елементів підтримки стабільної роботи освітніх середовищ та збереження довіри до них. Трансформація освітнього середовища у бік цифровізації вимагає не лише обробки даних, але й забезпечення їхнього захисту на всіх етапах. У зв'язку з цим, розробка надійних моделей і методів та інформаційної технології управління потоками персональних даних стає необхідністю.

Окрему увагу слід приділити невідповідності між зростаючим обсягом потоків даних та наявними технічними засобами зберігання. Відсутність принципів управління збереженням таких потоків може призвести до зниження ефективності управлінських рішень в освітньому середовищі, а також до ризиків безпеки та збереження інформації.

Тому своєчасним є питання моделювання управління зберіганням потоків даних в освітньому середовищі, в основі якого прогнозування апаратних вимог і оцінка показових переваг до зберігання потоків даних.

Дослідження та впровадження сучасних інформаційних технологій для управління потоками персональних даних є одним із визначених напрямків розвитку освітнього середовища в умовах цифрової трансформації. Розробка спеціалізованих моделей спрямована не лише на підвищення ефективності зберігання потоків даних, але й на забезпечення їхнього захисту на всіх етапах життєвого циклу. Інформаційна технологія, що базується на таких підходах дозволить досягти нового рівня автоматизації та надійності в управлінні персональними даними. Це сприятиме підвищенню якості освітнього процесу, збереженню конфіденційності учасників та забезпеченню безпеки інформаційних систем.

Важливість цієї теми полягає також у необхідності дотримання нормативних вимог щодо захисту персональних даних, таких як Загальний регламент захисту даних (GDPR) у Європейському Союзі та інші закони України. Інститути освіти, що не забезпечують належного рівня безпеки даних, ризикують не лише втратити довіру з боку спільноти, але й зазнати фінансових втрат через штрафи.

Теоретичні та прикладні аспекти розроблення методу, моделей та алгоритмів управління інформаційними потоками в умовах діджиталізації освітньої сфери з метою підвищення рівня захищеності навчального процесу представлені в роботах: P. Petrov, I. Kuyumdzhiev, Susanti, Ani Widyawati, Svitlana Bader, Alla Oleksiienko, Kochkareva I. V., Cramarenco R. E., Burcă-Voicu M. I., Martyniuk O.O., Martyniuk O.S, Zhen-Yu Wu, Gunawan D., Mambo M., Fengjun Li, Xukai Zou, J. Ma, Mygal V., Lovecek T., Ristvej J., Minzhu Zhang. Усе це свідчить про доцільність управління потоками персональних даних освітнього середовища в умовах діджиталізації у вигляді програмного рішення.

Таким чином, дослідження в цій галузі є не лише актуальним, але й має потенціал для започаткування нових практик і політик в управлінні даними, що мають критичне значення як для розвитку освітньої сфери, так і для суспільства в цілому. Це

дослідження пропонує рішення, які можуть бути застосовані у багатьох секторах, інтегруючись у ширші стратегії інформаційної безпеки та управління ризиками в умовах цифрової трансформації.

Виникає **актуальна** науково-прикладна проблема, пов’язана зі створенням та застосуванням моделей, методу управління потоками персональних даних освітнього середовища в умовах діджиталізації, що направлено на підвищення рівня захищеності персональної інформації учасників навчального процесу та забезпечення якісних та ефективних механізмів підвищення конфіденційності такого процесу, з урахуванням ризиків, а також викликів.

Зважаючи на це, проведено аналіз, за результатами якого встановлено, що з розвитком цифрових технологій, обсяг даних, які збираються про учасників навчального процесу, стрімко зростає. Це включає інформацію про академічні досягнення, поведінкові дані в навчальних системах, особисті дані студентів та викладачів, дані про взаємодію з навчальними платформами, а також адміністративні дані. Таке накопичення інформації вирізняється складністю та обсягами, ставлячи перед системами освіти задачу постійного вдосконалення управлінських практик і технологій збереження даних. Хоча ці дані є вкрай важливими для аналізу і покращення якості навчання, їх зберігання й обробка несе ризики, пов’язані з витоками даних та несанкціонованим доступом.

Збільшення обсягу даних створює необхідність їх ефективного менеджменту, оскільки несанкціоноване використання таких даних може мати серйозні наслідки як для окремих учасників навчального процесу, так і для установ загалом. Незважаючи на різноманітні підходи до захисту інформації, такі як шифрування, захист мережевих протоколів і автентифікація користувачів, вони здебільшого зосереджені на захисті вже зібраних даних та каналів їх передачі.

На противагу цьому, концепція анонімізації пропонує не лише захист, а й профілактику витоків, оскільки дані стають такими, які неможливо розпізнати з самого початку. Це означає, що дані, які можуть бути корисними для освітніх аналітиків,

дослідників та адміністраторів, не можуть бути пов'язаними з конкретними особами, що значно ускладнює можливості їх несанкціонованого використання. Зокрема, дослідивши цей напрямок детально, варто зазначити, що методи анонімізації можуть включати техніки заміни, генерації псевдонімів, агрегування, та інші способи зміни структури даних. Це дозволяє зберігати інформацію, що є важливою для навчального аналізу, при цьому забезпечуючи приватність осіб.

Однак, проведений аналіз показує, що анонімізація не є широко розповсюдженим підходом у сфері освіти. Значна частина навчальних закладів все ще не має чітких методик її впровадження, що є наслідком відсутності достатньої кількості досліджень і документальних прикладів успішного використання таких підходів. Як результат, заклади освіти часто обмежуються стандартними методами захисту, які не забезпечують достатнього рівня безпеки у сучасному діджиталізованому світі.

Крім того, впровадження методик анонімізації стикається з технічними та організаційними викликами через відсутність системного бачення та стандартів у цій сфері. Для навчальних установ критично важливо мати уніфіковані підходи та інструменти, які можна інтегрувати у вже наявні системи управління навчанням. Це дозволило б ефективно захищати дані, використовуючи новітні технології та методики.

Все це вказує на **необхідність розробки моделей та методів, які б дозволили освітнім установам впроваджувати управління потоками персональних даних суб’єктів освітнього середовища в умовах діджиталізації** на всіх етапах збереження та обробки даних. Зокрема, такі моделі та методи повинні враховувати різні рівні конфіденційності даних, типи освітніх систем, а також технологічні можливості конкретних навчальних закладів.

Метою цієї дослідницької роботи є підвищення ефективності управління потоками персональних даних освітнього середовища в умовах діджиталізації за рахунок розробки моделей, методу та інформаційної технології захисту персональних даних учасників освітнього процесу.

Дослідження у цьому напрямку також сприятиме довірі між учасниками навчального процесу, включаючи студентів, викладачів та адміністрацію, забезпечуючи при цьому відповідність сучасним стандартам інформаційної безпеки.

Для реалізації цих цілей необхідно вирішити ряд науково-прикладних завдань:

- аналіз існуючих підходів до управління інформаційними потоками освітнього середовища у контексті діджиталізації;
- розробка концепції управління потоками персональних даних у контексті діджиталізації освітньої сфери, в основі якої модель інформаційних потоків та інформаційних взаємодій у діджиталізованій освітній сфері;
- формування моделі управління зберіганням потоків даних освітнього середовища;
- запропонувати модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища;
- розробка методу управління потоками персональних даних в умовах діджиталізації освітньої сфери;
- розробка, застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації та визначення її ефективності.

Дослідження в рамках цієї роботи базуватимуться на існуючих актуальних напрацюваннях у сфері освіти, захисту інформації, зокрема й анонімізації даних персональної інформації. Планується детально проаналізувати сучасні методики та інструменти, які вже були застосовані в інших сферах, з метою адаптації їх до освітнього контексту. Крім того, розроблена методологія анонімізації даних буде впроваджена в межах однієї з великих існуючих навчальних платформ. Це дозволяє не лише перевірити ефективність запропонованих підходів, а й отримати цінний практичний досвід, який може бути використано для подальшого вдосконалення системи захисту даних в освітній сфері.

Отже, в роботі виконано аналіз існуючих підходів до управління інформаційними потоками освітнього середовища у контексті діджиталізації. Зокрема проаналізовано роботи у таких напрямках: вплив діджиталізації на інформаційні потоки в освітній сфері, існуючі підходів до управління інформаційними потоками у діджиталізованій освітній сфері, існуючі моделі та інформаційні рішення із захисту персональних даних у діджиталізованому освітньому середовищі, проблемні завдання управління інформаційними потоками діджиталізованого освітнього середовища та застосування анонімізації з метою захисту персональних даних в інформаційних потоках в освітній сфері.

Розроблено концепцію управління потоками персональних даних у контексті діджиталізації освітньої сфери. В контексті якої створено та детально описано схему інформаційних потоків діджиталізованого освітнього середовища в контексті поширення персональних даних його стейкхолдерів. Ідентифіковано головних стейкхолдерів інформаційної взаємодії діджиталізованої сфери освіти. Після цього на основі аналізу інформаційних взаємодій у діджиталізованому освітньому середовищі та формування категорій стейкхолдерів освітнього процесу розроблено модель інформаційної взаємодії у діджиталізованій освітній сфері. Отримавши достатній інформаційний базис, побудовано модель визначення витоку персональних даних діджиталізованої інформаційної взаємодії. Ця модель дозволяє зрозуміти основні точки контролю потоків персональних даних.

Створено модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища. Модель демонструє зону виникнення ризикових подій витоку персональних даних. Крім того, проведено експертну оцінку причин витоку персональної інформації та їх можливих наслідків. Після чого виділено головні ймовірні причини виникнення подій витоку персональних даних.

Зрозумівши основні ризики пов’язані з витоком персональних даних стейкхолдерів діджиталізованої освіти, створено принципи мінімізації поширення персональних даних учасників навчального процесу.

Наступним кроком стало формування моделі управління зберіганням потоків даних освітнього середовища. Модель дає можливість підготовлено підійти до прийняття рішення про місце розташування інформаційних потоків навчального закладу, що є важливим фактором з точки зору захисту персональної інформації стейкхолдерів освітнього процесу.

Створено моделі управління потоками персональних даних у контексті діджиталізації освітньої сфери. До яких входять модель анонімізації персональних даних стейкхолдерів в інформаційних потоках при інформаційній взаємодії у діджиталізованому освітньому середовищі, а також модель анонімізації персональних даних стейкхолдерів в інформаційних потоках при інформаційній взаємодії у діджиталізованому освітньому середовищі. Ці моделі демонструють які дані повинні покидати межі діджитал системи навчального закладу, а які ні. Також на моделі анонімізації видно яка інформація буде вертатись навчальному закладу. В свою чергу модель діджиталізації описує правила інформаційної взаємодії при запитах зовнішніх платформ на деанонімізацію даних.

Розроблено метод управління потоками персональних даних в умовах діджиталізації освітньої сфери. Метод детально описує імплементацію та застосування програмного забезпечення для анонімізації та деанонімізації персональної інформації головних інформаційних об’єктів навчального простору (Студент, Викладач, Адміністратор та інші). В межах створеного методу було:

- створено алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти, який покроково описує кожен етап створення та інтеграції сервісу анонімізації в діджитал систему менеджменту даних навчального закладу, починаючи плануванням і закінчуючи створенням фінальних звітів;

- створено алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти який у свою чергу описує кроки які необхідно пройти для розробки, а також впровадження сервісу деанонімізації у діджитал менеджмент систему навчального закладу;
- створено та описано загальну схему впровадження анонімізації та деанонімізації персональних даних в інформаційному просторі діджиталізованої освіти;
- розроблено та детально описано метод анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти; його можна застосовувати окремо від загального методу, але у більшості випадків анонімізація не має сенсу без деанонімізації;
- створено метод деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти, який дозволяє впровадити сервіс деанонімізації, але він має зміст тільки якщо попередньо впроваджено анонімізацію;
- об’єднано методи анонімізації та деанонімізації персональних даних та на їх основі отримано метод одночасного впровадження анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти.

Розроблено та застосовано інформаційну технологію управління потоками персональних даних освітнього середовища в умовах діджиталізації та визначено її ефективність. Зокрема було:

- створено архітектуру інформаційної технології анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти, яка включає у себе загальну схему архітектури інформаційної технології, вимоги до складових архітектурного рішення інформаційної технології та структуру бази даних;
- імплементовано програмне забезпечення для анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти;

- застосовано інформаційні технології анонімізації та деанонімізації персональних даних;
- проведено оцінку ефективності застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації.

Ключові слова: управління, персональні дані, потоки даних, ідентифікація ризиків, анонімізація, деанонімізація, захист персональних даних, рекомендації щодо захисту персональних даних, передача інформації, класифікація інформаційних потоків, інформаційні загрози, підтримка прийняття рішення, розташування інформаційних потоків, зменшення ризиків втрат, інформаційна технологія.

ABSTRACT

Raichuk I. Models and methods of managing personal data flows of subjects of the educational environment in the conditions of digitalization. Qualification of scientific work as a manuscript.

Thesis for the Doctor of Philosophy degree in Information Technology, specialty 122 Computer Science. Technology". Taras Shevchenko National University of Kyiv, Kyiv, 2025.

The relevance of research on the management of personal data flows of subjects of the educational environment in the context of digitalization is due to the rapid development of digital technologies, which are changing approaches to the processing and protection of personal data in education. In the modern world, educational institutions are faced with increasing information flows containing the personal data of students, teachers, and employees. Effective management of these flows is key to maintaining the stability and security of the entire educational process. Digitalization in the field of education opens up new opportunities for optimizing educational processes, makes personalized learning possible, and contributes to the globalization of education. However, along with these advantages, new challenges also arise, in particular, a significant risk of breach of confidentiality and unauthorized use of personal data. Managing the risks of leakage of personal data is one of the elements of supporting the stable operation of educational environments and maintaining trust in them. The transformation of the educational environment towards digitalization requires not only data processing but also ensuring their protection at all stages. In this regard, the development of reliable models and methods and information technology for managing personal data flows becomes a necessity.

Special attention should be paid to the discrepancy between the growing volume of data flows and the available technical means of storage. The lack of principles for managing the storage of such flows can lead to a decrease in the effectiveness of management decisions in the educational environment, as well as to security and information security risks. Therefore, the issue of modeling the storage management of data flows in the educational

environment, based on the prediction of hardware requirements and the assessment of the indicative advantages of storing data flows, is timely.

Research and implementation of modern information technologies for managing personal data flows is one of the identified areas of development of the educational environment in the context of digital transformation. The development of specialized models is aimed not only at increasing the efficiency of storing data flows but also at ensuring their protection at all stages of the life cycle. Information technology based on such approaches will allow achieving a new level of automation and reliability in personal data management. This will contribute to improving the quality of the educational process, preserving the confidentiality of participants, and ensuring the security of information systems.

This topic is also important because it requires compliance with regulatory requirements for the protection of personal data, such as the General Data Protection Regulation (GDPR) in the European Union and other Ukrainian laws. Educational institutions that do not provide an adequate level of data security risk losing the community's trust and incurring financial losses through fines.

Theoretical and applied aspects of developing a method, models and algorithms for managing information flows in the context of digitalization of the educational sphere in order to increase the level of security of the educational process are presented in the works: P. Petrov, I. Kuyumdzhiev, Susanti, Ani Widyawati, Svitlana Bader, Alla Oleksiienko, Kochkareva I. V., Cramarenco R. E., Burcă-Voicu M. I., Martyniuk O.O., Martyniuk O.S, Zhen-Yu Wu, Gunawan D., Mambo M., Fengjun Li, Xukai Zou, J. Ma, Mygal V., Lovecek T., Ristvej J., Minzhu Zhang. All this indicates the feasibility of managing personal data flows in the educational environment in the context of digitalization in the form of a software solution.

Thus, research in this area is not only relevant but also has the potential to introduce new practices and policies in data management that are critical to the development of the educational sphere and society as a whole. This research suggests solutions that can be applied across multiple sectors, integrating into broader information security and risk management strategies in the context of digital transformation.

There is a **pressing** scientific and applied problem related to the creation and application of models and methods for managing flows of personal data in the educational environment in the digitalized environment. This problem aims to increase the security of participants' personal information in the educational process and ensure high-quality and effective mechanisms for increasing the confidentiality of such a process, taking into account risks and challenges.

Because of this, an analysis was conducted, the results of which showed that with the development of digital technologies, the volume of data collected about participants in the educational process is rapidly growing. This includes information on academic achievements, behavioral data in educational systems, personal data of students and teachers, data on interaction with educational platforms, as well as administrative data. Such accumulation of information is distinguished by its complexity and volume, setting before education systems the task of constantly improving management practices and data storage technologies. Although this data is crucial for analyzing and improving the quality of education, its storage and processing carry risks associated with data leaks and unauthorized access.

The increase in the volume of data creates the need for its effective management, as unauthorized use of such data can have serious consequences for both individual participants in the educational process and institutions as a whole. Despite various approaches to information security, such as encryption, network protocol protection, and user authentication, they mostly focus on protecting the data already collected and its transmission channels.

In contrast, the concept of anonymization offers not only protection but also prevention of leaks, as the data becomes unrecognizable from the very beginning. This means that data that can be useful for educational analysts, researchers, and administrators cannot be associated with specific individuals, which greatly complicates the possibility of their unauthorized use. In particular, having studied this area in detail, it is worth noting that anonymization methods can include substitution techniques, pseudonym generation, aggregation, and other ways of changing the data structure. This allows you to preserve

information that is important for educational analysis while maintaining the privacy of individuals.

However, the analysis shows that anonymization is not a widespread approach in the field of education. A significant part of educational institutions still does not have clear methods for its implementation, which is a consequence of the lack of sufficient research and documented examples of the successful use of such approaches. As a result, educational institutions are often limited to standard protection methods that do not provide a sufficient level of security in the modern digital world.

In addition, the implementation of anonymization methods faces technical and organizational challenges due to the lack of a systemic vision and standards in this area. It is critically important for educational institutions to have unified approaches and tools that can be integrated into existing learning management systems. This would allow for effective data protection using the latest technologies and techniques.

All this indicates the **need to develop models and methods that would allow educational institutions to implement the management of personal data flows of subjects of the educational environment in the conditions of digitalization** at all stages of data storage and processing. In particular, such models and methods should take into account different levels of data confidentiality, types of educational systems, as well as technological capabilities of specific educational institutions.

The purpose of this research work is to increase the efficiency of managing personal data flows in the educational environment in the conditions of digitalization by developing models, methods, and information technology for the protection of the personal information of participants in the educational process.

Research in this direction will also contribute to trust between participants in the educational process, including students, teachers, and administration while ensuring compliance with modern information security standards.

To achieve these goals, it is necessary to solve several scientific and applied tasks:

- analysis of existing approaches to managing information flows in the educational environment in the context of digitalization;
- development of a concept for managing personal data flows in the context of digitalization of the educational sphere, based on a model of information flows and information interactions in the digitalized educational sphere;
- formation of a model for managing the storage of data flows in the educational environment;
- propose a model of personal data leakage risks during information interaction in the digitalized educational environment;
- development of a method for managing personal data flows in the context of digitalization of the educational sphere;
- development, application of information technology for managing personal data flows in the educational environment in the context of digitalization, and determination of its effectiveness.

Research within the framework of this work will be based on existing current developments in the field of education, and information protection, in particular, anonymization of personal information data. It is planned to analyze in detail modern methods and tools that have already been applied in other areas, to adapt them to the educational context. In addition, the developed methodology for data anonymization will be implemented within one of the large existing educational platforms. This allows not only to verify the effectiveness of the proposed approaches but also to gain valuable practical experience that can be used to further improve the data protection system in the educational sphere.

Thus, the paper analyzes existing approaches to managing information flows in the educational environment in the context of digitalization. In particular, the work in the following areas is analyzed: the impact of digitalization on information flows in the educational sphere, existing approaches to managing information flows in the digitalized educational sphere, existing models and information solutions for protecting personal data in

the digitalized educational sphere, problematic tasks of managing information flows in the digitalized educational sphere and the use of anonymization to protect personal data in information flows in the educational sphere.

A concept for managing personal data flows in the context of digitalization of the educational sphere has been developed. In the context of this, a scheme of information flows of the digitalized educational environment in the context of the distribution of personal data of its stakeholders has been created and described in detail. The main stakeholders of information interaction in the digitalized educational sphere have been identified. After that, based on the analysis of information interactions in the digitalized educational environment and the formation of categories of stakeholders in the educational process, a model of information interaction in the digitalized educational sphere was developed. Having received a sufficient information basis, a model for determining the leakage of personal data of digitalized information interaction was built. This model allows us to understand the main points of control of personal data flows.

A model of risks of personal data leakage in information interaction in the digitalized educational environment was created. The model demonstrates the zone of occurrence of risk events of personal data leakage. In addition, an expert assessment of the causes of personal information leakage and its possible consequences was carried out. After that, the main probable causes of personal data leakage events were identified.

Having understood the main risks associated with the leakage of personal data of stakeholders of digitalized education, principles were created to minimize the distribution of personal data of participants in the educational process.

The next step was the formation of a model for managing the storage of data flows in the educational environment. The model makes it possible to prepare for deciding on the location of an educational institution's information flows, which is an important factor from the point of view of protecting the personal information of stakeholders in the educational process.

Personal data flow management models have been created in the context of the digitalization of the educational sphere. These include a model of anonymization of stakeholders' personal data in information flows during information interaction in a digitalized educational environment, as well as a model of anonymization of stakeholders' personal data in information flows during information interaction in a digitalized educational environment. These models demonstrate which data should leave the boundaries of the digital system of the educational institution and which should not. The anonymization model also shows what information will be returned to the educational institution. In turn, the digitalization model describes the rules of information interaction when external platforms request data de-anonymization.

A method of managing personal data flows in the context of digitalization of the educational sphere has been developed. The method describes in detail the implementation and use of software for anonymization and de-anonymization of personal information of the main information objects of the educational space (Student, Teacher, Administrator, and others). Within the framework of the created method, the following was done:

- an algorithm for anonymizing the personal data of stakeholders of digitalized education was created, which step by step describes each stage of creating and integrating an anonymization service into the digital data management system of the educational institution, starting with planning and ending with creating final reports;
- an algorithm for deanonymizing the personal data of stakeholders of digitalized education was created, which in turn describes the steps that must be taken to develop and implement a deanonymization service into the digital management system of the educational institution;
- a general scheme for implementing anonymization and deanonymization of personal data in the information space of digitalized education was created and described;
- a method for anonymizing personal data in the interaction of elements of the information space of digitalized education was developed and described in detail; it can be

used separately from the general method, but in most cases, anonymization does not make sense without deanonymization;

- a method of deanonymization of personal data in the interaction of elements of the information space of digitalized education was created, which allows the implementation of a deanonymization service, but it has meaning only if anonymization has been previously implemented;
- the methods of anonymization and deanonymization of personal data were combined and based on them a method of simultaneous implementation of anonymization and deanonymization of personal data in the interaction of elements of the information space of digitalized education was obtained.

An information technology for managing flows of personal data of the educational environment in the conditions of digitalization was developed and applied and its effectiveness was determined. In particular, it was:

- created an information technology architecture for anonymization and de-anonymization of personal data of stakeholders of digitalized education, which includes a general scheme of the information technology architecture, requirements for the components of the information technology architectural solution, and the database structure;
- software for anonymization and deanonymization of personal data of stakeholders of digitalized education was implemented;
- information technology for anonymization and deanonymization of personal data was applied;
- an assessment of the effectiveness of the application of information technology for managing personal data flows in the educational environment in the context of digitalization was carried out.

Keywords: management, personal data, data flows, risk identification, anonymization, de-anonymization, personal data protection, recommendations for personal data protection, information transfer, classification of information flows, information threats, decision support, data flow placement, risk reduction of loss, information technology.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України:

Тімінський О. Г. & Райчук І. В. (2019). Метод ціннісно-орієнтованого управління зацікавленими сторонами проекту діджиталізації. Управління проектами та розвиток виробництва, 3(71), 114–120.

Тімінський О. Г., Войтенко О. С. & Райчук І. В. (2021). Аналіз моделей і методів діджиталізації бізнес-процесів. Управління розвитком складних систем, 46, 38–47.

Райчук І. В., Хлевна Ю. Л., Войтенко О. С. & Тімінський О. Г. (2022). Розробка моделі діджиталізації процесу закупівель Hardware для ІТ-компанії. Управління розвитком складних систем, 50, 44–51.

Бушуєв С., Івко А. & Райчук І. В. (2023). Вибір моделі організаційної структури проєкту діджиталізації бізнес процесів в контексті синкретичного управління. Вісник Львівського державного університету безпеки життєдіяльності, 28, 5–13.

Райчук І. В. (2024). Експертна оцінка ідентифікації ризиків втрати персональних даних при інформаційній взаємодії у діджиталізованому освітньому середовищі. Наука і техніка сьогодні, Серія «Техніка», 13(41), 1227–1238.

Райчук І. В. & Мірошниченко І. В. (2025). Модель управління зберіганням потоків даних освітнього середовища. Наука і техніка сьогодні, Серія «Техніка», 1(42), 1360–1379.

Статті включені до наукометричної бази даних Scopus:

Raichuk I., Khlevna I., Timinskyi O. & Voitenko O. (2022). Cognitive model of digitalization of business processes of a project-oriented IT company. CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3382/Paper12.pdf

Khlevna I., Raichuk I. & Timinskyi O. (2023). The development of the information technology architecture for the anonymisation of stakeholders personal data of digitalized education based on formulated criteria and requirements. In Workshop Proceedings of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023) (Kyiv, Ukraine, November 20-21, 2023, с. 139–148).

Raichuk I., Kolesnikova K., Khlevna I., Timinskyi O. & Kubiavka L. (2024). Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools. Procedia Computer Science, 231, 347–352. https://doi.org/10.1016/j.procs.2023.12.215

Тези конференцій за темою, в яких автор приймав участь:

Тімінський О. Г. & Райчук І. В. (2019). Передумови розробки моделей і методів для управління проектом створення генералізованого штучного інтелекту на базі ціннісного підходу. У Матеріали VI міжнародної науково-практичної конференції «Інформаційні технології та взаємодії» (с. 80–83). Київ.

Raichuk I. (2020). Models of digitalization of business processes of project-oriented organizations based on artificial neural networks. In Proceedings of the VII International Conference "Information Technology and Interactions" (Satellite) (pp. 217–220). Kyiv.

ЗМІСТ

ВСТУП

Актуальність теми дослідження управління потоками персональних даних суб’єктів освітнього середовища в умовах діджиталізації зумовлена стрімким розвитком цифрових технологій, які змінюють підходи до обробки та захисту персональних даних у сфері освіти. У сучасному світі освітні установи стикаються з дедалі більшою кількістю інформаційних потоків, що містять персональні дані студентів, викладачів і співробітників. Ефективне управління цими потоками є ключовим для підтримки стабільності та безпеки всього освітнього процесу.

Діджиталізація в галузі освіти відкриває нові можливості для оптимізації навчальних процесів, робить можливим персоналізоване навчання та сприяє глобалізації освіти. Проте, разом із цими перевагами з’являються й нові виклики, зокрема суттєвий ризик порушення конфіденційності та несанкціонованого використання персональних даних. Управління ризиками витоку персональних даних – один з елементів підтримки стабільної роботи освітніх середовищ та збереження довіри до них. Трансформація освітнього середовища у бік цифровізації вимагає не лише обробки даних, але й забезпечення їхнього захисту на всіх етапах. У зв'язку з цим, розробка надійних моделей і методів та інформаційної технології управління потоками персональних даних стає необхідністю.

Окрему увагу слід приділити невідповідності між зростаючим обсягом потоків даних та наявними технічними засобами зберігання. Відсутність принципів управління збереженням таких потоків може призвести до зниження ефективності управлінських рішень в освітньому середовищі, а також до ризиків безпеки та збереження інформації. Тому своєчасним є питання моделювання управління зберіганням потоків даних в освітньому середовищі, в основі якого прогнозування апаратних вимог і оцінка показових переваг до зберігання потоків даних.

Дослідження та впровадження сучасних інформаційних технологій для управління потоками персональних даних є одним із визначених напрямків розвитку освітнього середовища в умовах цифрової трансформації. Розробка спеціалізованих

моделей спрямована не лише на підвищення ефективності зберігання потоків даних, але й на забезпечення їхнього захисту на всіх етапах життєвого циклу. Інформаційна технологія, що базується на таких підходах дозволить досягти нового рівня автоматизації та надійності в управлінні персональними даними. Це сприятиме підвищенню якості освітнього процесу, збереженню конфіденційності учасників та забезпеченню безпеки інформаційних систем.

Важливість цієї теми полягає також у необхідності дотримання нормативних вимог щодо захисту персональних даних, таких як Загальний регламент захисту даних (GDPR) у Європейському Союзі та інші закони України. Інститути освіти, що не забезпечують належного рівня безпеки даних, ризикують не лише втратити довіру з боку спільноти, але й зазнати фінансових втрат через штрафи.

Теоретичні та прикладні аспекти розроблення методу, моделей та алгоритмів управління інформаційними потоками в умовах діджиталізації освітньої сфери з метою підвищення рівня захищеності навчального процесу представлені в роботах: P. Petrov, I. Kuyumdzhiev, Susanti, Ani Widyawati, Svitlana Bader, Alla Oleksiienko, Kochkareva I. V., Cramarenco R. E., Burcă-Voicu M. I., Martyniuk O.O., Martyniuk O.S, Zhen-Yu Wu, Gunawan D., Mambo M., Fengjun Li, Xukai Zou, J. Ma, Mygal V., Lovecek T., Ristvej J., Minzhu Zhang. Усе це свідчить про доцільність управління потоками персональних даних освітнього середовища в умовах діджиталізації у вигляді програмного рішення.

Таким чином, дослідження в цій галузі є не лише актуальним, але й має потенціал для започаткування нових практик і політик в управлінні даними, що мають критичне значення як для розвитку освітньої сфери, так і для суспільства в цілому. Це дослідження пропонує рішення, які можуть бути застосовані у багатьох секторах, інтегруючись у ширші стратегії інформаційної безпеки та управління ризиками в умовах цифрової трансформації.

Виникає **актуальна** науково-прикладна проблема, пов’язана зі створенням та застосуванням моделей, методу управління потоками персональних даних освітнього середовища в умовах діджиталізації, що направлено на підвищення рівня захищеності

персональної інформації учасників навчального процесу та забезпечення якісних та ефективних механізмів підвищення конфіденційності такого процесу, з урахуванням ризиків, а також викликів.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана в Київському національному університеті імені Тараса Шевченка і пов'язана з вирішенням завдань створення та впровадження методологій управління проєктами.

Дисертація відповідає тематичному спрямуванню наукових розробок у рамках виконуваної автором науково-дослідної роботи «Розробка інформаційно-аналітичних інструментів управління портфелями проєктів і програм в інтегрованих функціональних середовищах» (державний реєстраційний номер 0121U107799), а також «Розробка моделей, методів інтелектуального управління проєктами інноваційно орієнтованих підприємств» (державний реєстраційний номер 0121U107801).

Мета і завдання дослідження. Метою роботи є підвищення ефективності управління потоками персональних даних освітнього середовища в умовах діджиталізації за рахунок розробки моделей, методу та інформаційної технології захисту персональних даних учасників освітнього процесу.

Для досягнення поставленої мети в дисертації визначена необхідність виконання наступних завдань:

- аналіз існуючих підходів до управління інформаційними потоками освітнього середовища у контексті діджиталізації;
- розробка концепції управління потоками персональних даних у контексті діджиталізації освітньої сфери, в основі якої модель інформаційних потоків та інформаційних взаємодій у діджиталізованій освітній сфері;
- формування моделі управління зберіганням потоків даних освітнього середовища;
- запропонувати модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища;

- розробка методу управління потоками персональних даних в умовах діджиталізації освітньої сфери;
- розробка, застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації та визначення її ефективності.

Об'єктом дослідження є процеси управління потоками персональних даних суб'єктів освітнього середовища в умовах діджиталізації.

Предметом дослідження є моделі, методи управління потоками персональних даних суб'єктів освітнього середовища, які забезпечують їх ефективне зберігання, захист та конфіденційність.

Науково-прикладна проблема створення методу управління потоками персональних даних в умовах діджиталізації освітньої сфери вирішувалась у рамках сучасних концепцій комп'ютерних наук.

Методи досліджень ґрунтувались на застосуванні емпіричних підходів реальний експеримент для розуміння практичності розробленого рішення, опис, зокрема алгоритмів та кроків реалізації інформаційної технології, складання схем та побудова таблиць. Крім того, застосовувалися формалізація, наукове моделювання, аналіз та синтез. Для досягнення поставлених в дисертаційній роботі використано імітаційне моделювання (в контексті створення моделей інформаційної взаємодії та потоків даних у діджиталізованій освітній сфері, ризиків витоку персональних даних, управління зберіганням потоків даних, анонімізації та деанонімізації персональних даних), теорію алгоритмів (для побудови алгоритму впровадження анонімізації та деанонімізації персональних даних), теорію програмування (для створення програмного продукту за результатами дослідження).

Наукова новизна отриманих результатів.

Вперше. Створено модель інформаційної взаємодії та потоків даних у діджиталізованій освітній сфері. Унікальність побудованої моделі полягає у врахуванні особливостей взаємодії навчального закладу з різними типами зовнішніх споживачів,

включає глибокий аналіз потоків даних через розбиття на етапи обробки та має націленість на освітню сферу. Вона дозволяє оцінити загальну небезпеку інформаційної взаємодії, визначити потоки даних з найбільшою вразливістю та ідентифікувати найнебезпечніші етапи обробки даних у контексті витоків персональних даних.

Розроблено метод управління потоками персональних даних в умовах діджиталізації освітньої сфери, який поєднує алгоритми анонімізації та деанонімізації, що дозволяє розрахувати оцінку небезпеки потоків даних навчального закладу, ідентифікувати ризики та причини їх виникнення, а також обирати оптимальну стратегію зберігання даних. Застосування цього методу підвищує ефективність управління потоками персональних даних навчального закладу, забезпечує вищий рівень захищеності персональних даних у діджиталізованому освітньому середовищі, водночас зберігаючи переваги діджиталізації.

Вдосконалено. Модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища. Особливість цієї моделі полягає в її спеціалізації на галузі освіти, з головним фокусом на навчальному закладі. Застосування моделі дозволяє оцінити вагу кожної причини виникнення ризикової події витоку персональних даних та виділити ті причини, які потребують найбільшої уваги. Це сприяє ефективнішій роботі з ризиками витоку персональних даних під час управління потоками даних навчального закладу.

Практичне значення отриманих результатів. На основі наукових результатів, отриманих автором, розроблено та застосовано практичні інструменти:

- побудовано програмний шар анонімізації персональних даних стейкхолдерів діджиталізованої освіти та інтегровано в існуючу діджитал менеджмент систему даних стейкхолдерів освітнього процесу;
- програмний функціонал з деанонімізації персональної інформації учасників діджиталізованого навчального процесу та інтегровано в існуючу діджитал менеджмент систему даних стейкхолдерів освітнього процесу;

- результати дисертаційного дослідження впроваджено в компанію «Едютон Україна», яка надає одні з найпрогресивніших та найгнучкіших сервісів з управління інформаційними потоками у діджиталізованій освітній сфері. Компанія просуває ідею захищеності персональної інформації стейкхолдерів освітньої сфери та забезпечення конфіденційності навчального процесу (акт впровадження від 11.11.2024 – додаток А).

Особистий внесок автора у праці, які склали основу дисертації та виконані у співавторстві.

Основні результати дисертаційної роботи отримані здобувачем самостійно. Робота містить теоретичні та методичні положення, висновки, які сформульовані дисертантом особисто. У наукових працях, написаних у співавторстві, здобувачу належать: у [1] розроблено алгоритм (послідовність кроків) методу ціннісно-орієнтованого підходу в управлінні проєктом діджиталізації; у [2] проаналізовано основні підходи до управління проєктом створення діджитал продукту з контексті ШІ; у [3] частково розглянуто та проаналізовано роботи з автоматизації та діджиталізації бізнес-процесів у різних галузях в тому числі й освіті; у [4] розробка власної моделі діджиталізації бізнес-процесу в ІТ секторі, також створено схему архітектури інформаційної технології; у [5] проведено аналіз у напрямку діджиталізації бізнес-процесів проєктно-орієнтованих організацій, зумовленої різкими змінами у сучасному світі; у [6] розроблено архітектуру інформаційної технології анонімізації персональних даних стейкхолдерів навчального процесу; у [7] взято участь в аналізі існуючих підходів до діджиталізації бізнес-процесів, а також у створені моделі діджиталізації бізнес-процесу; у [8] розроблено модель захисту персональних даних в умовах діджиталізації освітньої сфери з використанням інформаційних технологій; у [9] створено модель управління зберіганням потоків даних освітнього середовища.

Апробація результатів дисертації. Основні результати досліджень доповідались на Міжнародних і Всеукраїнських наукових конференціях, зокрема:

VI міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (Київ 2019), VII international conference «Information Technology and

Interactions» (Satellite) (Kyiv 2020), 7th International Conference on Digital Technologies in Education, Science and Industry (DTESI 2022) (2022, Almaty, Kazakhstan), X International Scientific Conference “Information Technology and Implementation" (IT&I 2023) (Kyiv 2023), 14th International Conference on Emerging Ubiquitous Systems and Pervasive Networks / 13th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (EUSPN/ICTH 2023) (2023, Almaty, Kazakhstan).

Публікації. За результатами дослідження опубліковано 11 наукових праць, з них 9 статей опубліковані у рецензованих фахових виданнях України та іноземних виданнях, 3 англійською мовою, що не є перекладом з інших мов у періодичному виданні, включеному до наукометричної бази даних Scopus, 2 тези доповідей у матеріалах конференцій.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, 4 розділів, висновків, списку літератури зі 173 найменувань та 3 додатки. Загальний обсяг дисертації становить 250 сторінок, із них 191 сторінка основного тексту, який містить 19 таблиць, 53 рисунків на 14 повних сторінках.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ ОСВІТНЬОГО СЕРЕДОВИЩА У КОНТЕКСТІ ДІДЖИТАЛІЗАЦІЇ

1.1 Аналіз впливу діджиталізації на інформаційні потоки в освітній сфері

Останнім часом, як видно з багатьох досліджень [10 – 26] одним із найактуальніших напрямків досліджень в освітній сфері є вивчення впливу діджитал технологій та інформаційних сервісів на навчання. Багато досліджень зосереджені на розробці та впровадженні ефективних онлайн платформ, відеоуроків, інтерактивних засобів навчання тощо [15 – 16, 21, 24, 26 – 43]. Крім цього є й інші важливі напрямки досліджень в контексті стрімкого розвитку та поширення інформаційних технологій. Зокрема в [13, 18, 44, 45] приділяється велика увага вивченню інноваційних методик і підходів до організації навчального процесу. Автори робіт [46, 34, 25] зосередились на вивченні групової роботи, деяких проблемних методів навчання, розвитку креативності та критичного мислення учнів. Також варто виділити напрацювання [29, 32, 37, 47 – 52] напрямком яких є дослідження психологічних аспектів навчання, включаючи мотивацію студентів, їхній психологічний комфорт у навчальному середовищі та вивчення оптимальних стратегій мотивації для досягнення успіху. Підсумовуючи, можна з упевненістю сказати, що основні напрямки досліджень спрямовані на пошук інноваційних рішень для покращення якості освіти та розвитку більш ефективних підходів до навчання у сучасному світі та тісно переплітаються з діджитал технологіями [53 – 54].

Тому, розуміючи всепроникність та важливість інформаційних технологій сьогодні, вирішено зосередитись на дослідженні впливу діджиталізації на освітній процес. Для подальшої роботи у цьому напрямку необхідно сформувати чітке розуміння причин таких змін. Тож спираючись на існуючі роботи їх виділено:

1. Швидкі технологічні зміни – сучасний світ швидко розвивається в галузі інформаційних технологій, і впровадження діджитал рішень в освітній процес є необхідним для підготовки учнів до життя в діджитал епосі [40].

2. Широкі можливості для індивідуалізації – інформаційні технології дозволяють індивідуалізувати навчання, враховуючи потреби кожного учня. Цифрові адаптивні платформи можуть пристосовувати матеріали до рівня знань та інтересів конкретного учня. [25 – 26, 55]

3. Залучення студентів – використання інтерактивних технологій робить навчання цікавішим та привабливішим для учнів. Це допомагає зберегти їхню увагу та сприяє кращому засвоєнню матеріалу. [52, 56 – 58]

4. Підвищення доступності – діджиталізація допомагає зменшити бар'єри в доступі до освіти, зокрема для людей з обмеженими можливостями або тих, хто знаходиться в регіонах з обмеженим доступом до якісної освіти. [35, 59, 60]

Окрім цього, як зазначається у [32, 49, 61 – 62] дослідження впливу діджитал технологій на навчання дозволяють ефективніше аналізувати результати навчання, вдосконалювати засоби оцінювання та стимулювати розвиток нових педагогічних підходів у цифровій ері.

То які ж зміни у сфері освіти зв'язані з новими умовами вартують уваги і які конкретні чинники вплинули найбільше на пришвидшення діджиталізації? Автори робіт [10 – 11, 36] відзначають, що за останні роки кілька факторів сприяли різкому прискоренню діджиталізації у сфері освіти. Насамперед таким фактором стала пандемія COVID-19 [62 – 66]. Світова пандемія змусила школи та університети швидко переходити до дистанційного навчання. Це стало причиною використання діджитал інструментів для уможливлення продовження безпечного та ефективного навчального процесу. [47, 56, 67 – 68]

Очевидним наступним фактором є швидкий технологічний прогрес, який спостерігається за останні роки практично у всіх сферах життєдіяльності людей. У дослідженнях [42 – 43, 69 – 71] звертається увага на швидкий розвиток нових

технологій, таких як штучний інтелект, віртуальна реальність, блокчейн та інші. Це надає більше можливостей для інновацій в освіті та підвищує запит на цифрові рішення.

Крім того, у роботах [36, 50, 72 – 73] підкреслюється факт, що більш гостро стала відчуватись потреба у гнучкості навчальних платформ та закладів. Відзначається, що сучасні учні та студенти мають різноманітні потреби та вимоги до навчання. І саме цифрові технології можуть допомогти задовольняти ці потреби через індивідуалізований підхід та доступність навчальних матеріалів у будь-який час та в будь-якому місці.

І наостанок варто зауважити, що розвиток людства та прогрес в усіх сферах життєдіяльності людини призводить до збільшення потреб у професіоналах найрізноманітнішого напрямку [74 – 77]. А отже, неминучою була поява найрізноманітніших навчальних альтернатив вищим навчальним закладам та класичним навчальним платформам. Тобто, також одним з факторів прискорення діджиталізації в освітній сфері є зростання конкуренції в освіті. Умови сьогодення вимагають гнучкості від освіти, тому навчальні заклади та викладачі шукають шляхи покращення процесу навчання, залучаючи до цього діджитал технології [22, 42, 70, 78 – 79].

Саме ці фактори сприяли різкому пришвидшенню діджиталізації у сфері освіти, роблячи цифрові рішення все більш важливими для сучасного навчання та розвитку галузі [26].

Зважаючи на вище описані тенденції, діджиталізація та дослідження у сфері діджиталізації є надзвичайно популярним напрямом діяльності в усіх аспектах життєдіяльності людини [26, 80 – 81]. Доказами цьому слугує популярність напрямку цифрової трансформації й у бізнесі [82 – 83]. А саме дослідження, спрямовані на впровадження цифрових технологій та процесів в бізнес-середовищі для оптимізації роботи, покращення ефективності та зростання конкурентоспроможності [84].

Тому проведено аналіз у яких саме галузях інформаційних технологій спостерігається суттєвий розвиток. Почнемо з інтернету речей (IoT). Зустрічаються дослідження [51, 85 – 86] використання підключених пристроїв та систем у виробництві, медицині, транспорті та інших галузях для збору даних, моніторингу та автоматизації процесів. Обов'язково потрібно згадати штучний інтелект (AI). Доказом тому є безліч досліджень [87 – 90] спрямованих на застосування штучного інтелекту та алгоритмів машинного навчання для розв'язання різноманітних завдань, від аналітики даних до автоматизації процесів. Крім того, більш популярним став і напрямок кібербезпеки. Як видно з [18, 91 – 93] питання кібербезпеки, виявлення та запобігання кіберзлочинності, розробки захисту від кібератак та забезпечення конфіденційності даних у діджиталізованому середовищі є дуже важливим. Доволі перспективною та актуальною залишаються блокчейн технології. У роботах [21, 35, 71, 86] досліджуються можливості використання блокчейн технологій для підвищення безпеки та надійності транзакцій, збереження даних, підтримки децентралізованих систем та інші.

Проведений аналіз робіт показав, що ці напрямки досліджень у сфері діджиталізації допомагають розробляти інноваційні рішення для покращення різних секторів господарства та суспільства у цілому. Також можемо зробити висновок що дослідження у сфері діджиталізації різних сфер життя людини є надзвичайно актуальними.

Але що стосовно сфери освіти? Оскільки однією з основних галузей розвитку людства є освіта, то і не дивно що діджиталізація стосується цієї сфери значною мірою також. Більше того, провівши аналіз основних чинників, які призводять до росту діджиталізації освітнього середовища, можна з упевненістю стверджувати, що нові напрацювання з діджиталізації освіти є надзвичайно актуальним напрямком досліджень [56, 94, 95, 60, 96]. Тож окреслено найпопулярніші напрямки досліджень у сфері діджиталізації освіти:

1. Ефективність дистанційного навчання. Дослідження [60, 95], спрямовані на оцінку ефективності дистанційного навчання в порівнянні з традиційною очною освітою, включаючи вивчення результативності, залучення студентів та підвищення якості навчання.

2. Розробка та використання онлайн-платформ. Дослідження [97 – 99] з фокусом на розвиток та впровадження інноваційних онлайн-платформ для навчання, включаючи адаптивні системи, відеоуроки, віртуальні лабораторії тощо.

3. Цифрова компетентність вчителів. Вивчення рівня цифрової компетентності вчителів, їх готовності до використання цифрових технологій у навчальному процесі й проблем, які можуть виникнути у процесі діджиталізації. [18, 37, 100 – 102].

4. Використання штучного інтелекту та аналітики даних в освіті. Напрацювання [48, 63, 103 – 105], що досліджують використання інноваційних технологій, таких як штучний інтелект та аналітика даних, для підвищення ефективності навчального процесу та індивідуалізації навчання.

5. Кібербезпека в освіті. Безліч досліджень [11, 93, 97 – 98], спрямованих на розробку та впровадження механізмів кібербезпеки в освітніх інформаційних системах для захисту від кібератак та збереження конфіденційності даних.

Ці напрямки досліджень у сфері діджиталізації освіти вкрай важливі для подальшого розвитку сучасної освітньої системи та покращення якості навчання [106]. Хоч це і доводить, що з діджиталізацією освіта зазнала доволі суттєвих змін за останній час, потрібно означити що саме змінилось. У [107] зазначається, що діджиталізація вплинула на різні аспекти навчання та навчального процесу. Тому проведено аналіз робіт у цьому напрямку та виділено найзначущіші зміни в контексті діджиталізації в освіті є наступними:

- Відбувся перехід до дистанційного навчання. З появою діджитал технологій в освіті дистанційне навчання стало більш поширеним і доступним. Дослідження [28,

46, 108 – 109] доводять, що університети, школи та інші навчальні заклади активно використовують онлайн-платформи для забезпечення навчання відстані.

- Навчання стало більш індивідуалізоване. Як видно з [49, 87, 110 – 111] цифрові технології дозволяють адаптувати навчальні матеріали до потреб кожного учня, створюючи можливість для індивідуалізованого навчання та підтримки студентів на всіх рівнях навчання.
- Все частіше застосовуються інтерактивні засоби. Роботи [30, 100, 112 – 113] є прикладом того як вивчення нового матеріалу здійснюється через інтерактивні платформи, відеоуроки, віртуальні лабораторії та інші цифрові інструменти, що сприяють кращому засвоєнню матеріалу та залученню студентів.
- Частіше використовується аналітика даних. Завдяки інформаційним технологіям можливо збирати та аналізувати велику кількість даних про навчальний процес та успішність студентів, що дозволяє покращити методи навчання та забезпечити індивідуалізовані підходи [45, 56, 111, 113].
- Відбулось покращення у напрямку доступності освіти. Проаналізувавши дослідження [18, 72, 91, 109], зроблено висновки, що діджиталізація знизила бар’єри в доступі до освіти, забезпечуючи можливість навчання в будь-якому місці з доступом до інтернету та цифрових гаджетів.
- Спостерігається суттєва глобалізація навчання. Інтернет і цифрові технології дозволяють студентам отримувати доступ до глобальних ресурсів, викладачів та можливостей навчання з усього світу [49, 59, 88, 114].
- Колаборативне навчання. З аналізу [17, 83, 114, 116] випливає, що діджитал інструменти сприяють співпраці студентів та вчителів у режимі реального часу, використовуючи онлайн-платформи та спільні простори для спільної роботи.
- Розвиток навичок майбутнього. цифрова освіта допомагає студентам розвивати ключові навички для успішності у цифровому світі, такі як критичне мислення, комунікація, технологічна грамотність тощо. Прикладами цього є роботи [18, 45, 48, 109].

- Відбулась зміна ролі вчителів. Дослідження [24, 30, 40, 60, 88] показують, що вчителі стали не лише посередниками знань, але й фасилітаторами навчання, що стимулює самостійне навчання та взаємодію учнів.

Важливо, що зміни формують новий підхід до освіти, сприяють розвитку гнучких та інтерактивних методів навчання та допомагають готувати студентів до вимог сучасного цифрового світу.

Як результат аналізу бачимо, що діджиталізація має значний вплив на освіту, вносячи революційні зміни у спосіб навчання та навчальний процес. Але варто розуміти що зміни завжди мають як позитивні наслідки, так і негативні. Тому виконано аналіз позитивних та негативних впливів діджиталізації на освіту. Спочатку позитивний вплив. Про це уже ішлося раніше, але варто підкреслити це і тут, що найочевиднішою зміною є те, що діджиталізація однозначно призвела до збільшення доступності освіти [46, 109]. Цифрові технології роблять можливим навчання у будь-якому місці та у будь-який час, знижуючи географічні обмеження та роблячи освіту більш доступною для всіх. Також ще раз згадаємо, що стала можливою ґрунтовніша індивідуалізація та персоналізація [110]. Цифрові платформи дозволяють адаптувати навчання до потреб та рівня знань кожного учня, стимулюючи індивідуальний підхід та покращення успішності. Додатковим важливим аспектом змін є розвиток критичного мислення та технологічної грамотності [45]. Адже використання цифрових інструментів сприяє розвитку критичного мислення, аналітичних навичок та підвищенню технологічної грамотності студентів. Крім того, у [49] підкреслюється, що беззаперечним є розвиток креативності – використання цифрових інструментів сприяє розвитку креативності учнів та підтримує їхні інноваційні підходи до вирішення завдань. І наостанок, діджиталізація забезпечує гнучкість навчального процесу та стимулює появу інновацій. Цифрові інформаційні технології дозволяють впроваджувати нові методи навчання, сприяючи інноваціям та змінам у підходах до освіти [18, 109].

Проведений аналіз свідчить, що позитивний вплив є дуже серйозним. Але не варто забувати й про негативні наслідки. Тож розглянемо цю сторону діджиталізації. Незважаючи на високий рівень діджиталізації повсякденного життя людей, у [72, 117] вказується, що присутня певна нерівність доступу до технологій. Не всі учні мають рівний доступ до цифрових технологій, що може посилювати нерівність у доступі до якісної освіти. Також робота [118] висвітлює появу залежності від технологій. У деяких випадках поширена залежність від цифрових технологій може призвести до втрати здатності до критичного мислення та аналізу інформації [48]. Ну і найголовнішою зміною є віддаленість від соціальної взаємодії, тобто дистанційне навчання може обмежувати можливості для розвитку соціальних навичок та взаємодії між учнями та вчителями [30, 111, 119].

Підсумовуючи проведений аналіз впливу діджиталізації на життєдіяльність людей, а в особливості на освітню сферу, можна чітко окреслити напрями розвитку діджитал технологій, які чекають на нас у майбутньому. Тож у наступні роки можна очікувати подальший розвиток діджиталізованої освіти, з фокусом на наступні аспекти:

1. Інтеграцію штучного інтелекту та аналітики даних – штучний інтелект буде використовуватися для індивідуалізації навчання та підвищення ефективності навчального процесу [64, 109 – 110].

2. Експансію використання новітніх інформаційних технологій, зокрема віртуальної та розширеної реальності – VR та AR будуть ширше використовуватися для покращення імерсивності та ефективності навчання [45 – 46, 87].

3. Посилення кібербезпеки та приватності даних – для захисту від кіберзагроз та збереження конфіденційності велике значення матимуть кібербезпека та захист даних в освітній сфері [18, 49, 102].

Тож зміни у напрямку діджиталізації життєдіяльності людства мають суттєвий вплив на освітнє середовище. Що змінює інформаційні потоки в освітній сфері. Проаналізувавши вплив діджиталізації на інформаційні потоки в освітній сфері, визначено, що збільшується як кількість даних загалом, так і кількість персональних

даних учнів та викладачів, яка потрапляє в мережу. Все більше даних пов’язаних з навчальним процесом з’являється у вільному доступі, тож це було неминучим. Зважаючи на це, проведено аналіз існуючих напрацювань з метою визначення, що точно є основними причинами цього.

Отже, першою причиною є збільшення використання онлайн-платформ учасниками навчального процесу. З досліджень [72, 100, 109, 115] видно, що зі стрімкою діджиталізацією, учні та викладачі все більше використовують онлайн-платформи для навчання та комунікації. Це в свою чергу призводить до збільшення кількості персональних даних, які проходять через ці платформи.

Наступною причиною є використання хмарних сервісів. Як видно з досліджень [30, 110, 120] частіше використання хмарних сервісів для зберігання даних та документів також сприяє збільшенню кількості персональної інформації учасників освітнього процесу в мережі.

Також важливу роль відіграє інтеграція діджитал платформ навчання безпосередньо у навчальні заклади. Багато закладів використовують цифрові платформи для навчання та онлайн-тестувань, де зберігається інформація про успішність учнів, що може містити персональні дані [18, 109 – 110, 121].

Варто зазначити, що у зв’язку з цим, персональна інформація учасників освітнього процесу може стати більш доступною та менш захищеною. Загалом причин витоку та втрати персональних даних є очевидними. Низький рівень кібербезпеки, адже не всі освітні установи мають належні заходи кібербезпеки, що може призвести до витоку персональної інформації через кібератаки або порушення безпеки даних [45, 102, 110]. Можливі проблеми з управлінням даними. Автори робіт [49, 60, 72] зазначають, що велика кількість даних, яка збирається та зберігається в діджитал-середовищі, може призвести до проблем з управлінням та захистом цих даних. Також існують ризики порушення конфіденційності – адже збільшення кількості персональної інформації у мережі може збільшити ризики порушення конфіденційності цих даних через недостатній контроль доступу [18, 45, 72].

Отже, зростання діджиталізації в освіті призводить до змін інформаційних потоків в освітньому середовищі, а саме збільшенню кількості таких потоків та об'єму поширюваної інформації [45, 109 – 110]. Що в свою чергу є причиною збільшення кількості персональної інформації учасників освітнього процесу в мережі. Тож вимагає підвищеної уваги до впровадження ефективних заходів для захисту даних учасників навчального процесу.

1.2 Аналіз існуючих підходів до управління інформаційними потоками у діджиталізованій освітній сфері

Проведений аналіз вказує на серйозні зміни в освітній сфері пов'язані з діджиталізацією. Як наслідок збільшилась та продовжує зростати кількість даних які поширюються при інформаційній взаємодії діджиталізованого навчання. Велика частина таких даних є персональними даними учасників навчального процесу. Саме тому важливо ефективно управляти інформаційними потоками. Потрібно зосередитись на забезпеченні безпеки, доступності та ефективності навчального процесу [10, 11]. Тому, проведено аналіз існуючих підходів до управління інформаційними потоками в діджиталізованій освіті.

Визначено, що є кілька категорій на які можна поділити практики управління інформаційними потоками. Першою й однією з найбільш важливих є кібербезпека та захист даних. Тут найпоширенішим підходом є використання шифрування даних та механізмів автентифікації для захисту конфіденційності та інше. Одним з чудових прикладів робіт цього напрямку є стаття [123], у якій глибоко досліджується питання безпеки даних та пропонується математична структура направлена на зменшення ризиків несанкціонованого доступу до персональних даних. Також у цьому напрямку зустрічаються й інші дослідження [116, 124]. Наступним підходом є регулярна перевірка систем на наявність вразливостей та моніторинг підозрілих активностей. І

останнім підходом у цій категорії є використання інструментів для виявлення та запобігання кіберзагрозам.

Наступною категорією є підходи направлені на автоматизацію та оптимізацію процесів. Прикладом такого підходу є робота [125], у якій автор Z. Zhang використовує цифрову обробку для аналізу тривимірного простору освітніх методів і поєднує аналіз графіків та зображень для виконання інтелектуального розпізнавання тексту. Також зустрічаються роботи [126] пов'язані з впровадженням систем автоматизації оцінювання та аналізу даних для отримання швидкого та точного звіту про успішність студентів та ефективність навчання. Наступним підходом є використання автоматичних систем управління контентом для ефективного створення, редагування та поширення навчального матеріалу [20].

Як окрему категорію можна виділити управління доступом до інформації [81, 127]. Тут важливим є створення гнучких та безпечних систем управління доступом до різних рівнів інформації для студентів, викладачів та адміністраторів [124]. Як ще один підхід можна виділити використання ідентифікації двофакторним або біометричним способом для забезпечення точнішої ідентифікації користувачів [128].

Наступна категорія – моніторинг та аналіз даних. Застосовується аналітика даних для виявлення тенденцій у навчанні, покращення якості навчального процесу та прогнозування успішності студентів [129]. Додатково може встановлюватися постійний моніторинг інформаційних потоків для виявлення аномальних активностей та негайного реагування на потенційні загрози. Прикладом роботи такого напрямку є стаття [130] у якій розроблено стратегію та модель виявлення вторгнень.

І остання категорія – навчання та свідомість користувачів. Очевидним підходом є проведення інструктажів та тренінгів щодо кібербезпеки для користувачів діджитал систем з метою підвищення свідомості щодо важливості захисту персональної інформації та правил безпеки в інтернеті [38].

Звісно найважливішим напрямком є захист даних, адже витоки персональних даних можуть не лише знизити якість навчального процесу та довіру до навчальних

закладів а й завдати шкоди учасникам навчального процесу. Тому важливим є комбіноване застосування підходів які дозволяють забезпечити ефективне та безпечне управління інформаційними потоками в діджиталізованій освіті.

1.3 Аналіз існуючих моделей та інформаційних технологій із захисту персональних даних у діджиталізованому освітньому середовищі

Як видно, є безліч підходів управління інформаційними потоками, але при стрімкій діджиталізації важливо забезпечити безпеку даних учасників інформаційного обміну. Отже, проведено дослідження та виділено на що варто звернути увагу в існуючих працях.

Перше що варте уваги у цьому напрямку є розробка політик безпеки [131]. Як зазначають автори дослідження [11] для захисту інформаційних активів освітньої організації від внутрішніх, зовнішніх, навмисних або ненавмисних загроз повинна бути розроблена «Політика інформаційної безпеки».

Наступне на що варто звернути увагу це зменшення людського фактору [132]. Адже можна розробити складні механізми захисту даних, але вони можуть не спрацювати в критичній ситуації якщо не працювати над зниженням людського фактору.

У багатьох роботах [116, 128, 133 – 136] зустрічається застосування анонімізації даних для убезпечення інформаційного обміну від несанкціонованого доступу до важливих даних. У цих роботах анонімізація визначається як один з найефективніших засобів захисту даних при інформаційному обміні в діджиталізованому середовищі.

У дослідженні [137] зазначається важливість підвищення компетентностей студентів і викладачів в контексті діджиталізації навчального процесу. У цьому напрямку існує також багато напрацювань [138]. Зокрема можна виділити роботи [43, 92, 97, 139 – 140]. Зокрема у [97] описується проєкт «Електронний портал техніки безпеки та безпеки на основі компетенції» метою якого є розвиток компетенцій

студентів, викладачів, дослідників та інших. У [140] проводилось дослідження під час якого застосовувались технології 2D та 3D візуалізації для підвищення обізнаності про кіберситуацію.

Автори роботи [141] звертають увагу на появу величезних обсягів даних (Big Data). Зазначається, що існує багато труднощів, пов’язаних зі збором даних, зберіганням, використанням, аналізом, конфіденційністю та довірою, які потрібно вирішити наразі, з убезпечення Big Data. Саме тому автори аналізують найпопулярніші підходи та роблять висновки щодо їх застосування.

Ще одним цікавим дослідження є робота [98], у якій аналізується застосування опенсорс програм. Автори цього дослідження підтверджують позитивний вплив інструментів з відкритим кодом на безпеку закладу. Адже більшість таких програм розробляються з огляду на актуальні стандарти захисту даних.

Додатково виявлено безліч робіт направлених на безпечне зберігання даних. Зокрема дослідження [142] вказує на проблеми централізованого сховища інформації та пропонує нову структуру протоколу зберігання даних, яка має на меті підвищити ефективність екосистеми децентралізованого зберігання даних в поєднанні з технологією блокчейн.

З проведеного аналізу стало очевидним що існує безліч підходів до підвищення безпеки даних і є потреба у більш ґрунтовному зануренню у сферу. Саме тому, додатково проведено дослідження існуючих напрацювань у сфері захисту інформації. В результаті аналізу структуризовано галузі пов’язані з інформаційною безпекою. Їх короткий опис:

- Криптографія – це важлива галузь інформаційної безпеки, що охоплює різні методи забезпечення конфіденційності, цілісності та автентичності даних. Основні напрямки включають симетричну криптографію з алгоритмами AES і DES, які використовують один ключ для шифрування та дешифрування; асиметричну криптографію з алгоритмами RSA та ECC, що застосовують пару ключів; і хешування для цілісності даних з алгоритмами як SHA-256.

- Контроль доступу та ідентифікація. Це ключові напрямки в безпеці інформації, тут застосовуються багатофакторна автентифікація (MFA), біометрична ідентифікація, управлінні доступом і запобігання компрометації даних та багато іншого [86, 130, 143].
- Захист мереж [98]. Основні напрямки включають виявлення та запобігання вторгнень (IDS/IPS), використання машинного навчання для покращення точності систем виявлення загроз, а також заходи протидії DoS/DDoS через розробку методів виявлення аномального трафіку тощо.
- Захист від шкідливих програм (malware). Тут зустрічаються як традиційні методи розробки різного роду антивірусного програмного забезпечення, так і нетрадиційні, такі як поведінковий аналіз та реверс-інжиніринг malware та інше.
- Безпека даних і конфіденційність [130, 142 – 144]. З головних підходів варто виділити застосування анонімізації та деперсоналізацію даних, інструменти запобігання втратам даних (DLP) та конфіденційне обчислення.
- Безпека інтернету речей (IoT) [93]. Дослідження включають розробку легких механізмів автентифікації для пристроїв з обмеженими ресурсами, застосування ефективних протоколів шифрування, систем IDS/IPS для виявлення загроз, а також безпечні механізми оновлення програмного забезпечення.
- Варто виділити, що, як зазначається у [124, 145] суттєвого розвитку та використання зазнали хмарні технології, а отже, і галузь кібербезпеки в хмарних середовищ що спрямована на забезпечення безпеки даних і сервісів, що використовуються в хмарах [127]. Існує безліч напрацювань спрямованих як на забезпечення конфіденційності, цілісності та доступності даних так і тих, які зосереджуються на розробці нормативних актів для відповідності вимогам та вдосконаленні стратегій реагування на інциденти [124, 127, 145 – 146].
- Безпека блокчейнів і розподілених реєстрів. Застосування блокчейнів зустрічається як в освіті [42, 71, 86] так і в інших галузях [81]. Основні напрямки включають забезпечення безпеки протоколів консенсусу, захист смарт-контрактів від вразливостей, конфіденційність транзакцій у публічних блокчейнах, стійкість

криптографічних алгоритмів, управління ідентичністю учасників, безпеку фізичної та мережевої інфраструктури та багато іншого.

Отже, як видно захист персональних даних у діджиталізованому освітньому середовищі є багатогранним завданням, що потребує комплексного підходу і використання різних технологій та методів. Існуючі моделі та технології, зокрема системи управління доступом, шифрування даних, анонімізація, нормативно-правові заходи, системи запобігання витоку даних, інформаційно-просвітницька робота, а також технології AI та ML, забезпечують певний рівень безпеки та конфіденційності персональних даних. Однак, для досягнення оптимальних результатів важливо постійно моніторити нові загрози та вдосконалювати існуючі підходи та рішення.

1.4 Аналіз проблемних завдань управління інформаційними потоками діджиталізованого освітнього середовища

Провівши аналіз існуючих моделей та інформаційних технологій із захисту персональних даних у діджиталізованому освітньому середовищі, стало зрозуміло, що управління інформаційними потоками у такому середовищі є складним і багатогранним завданням, яке стикається з різноманітними викликами та проблемами [71, 130]. Як зазначається у великій кількості робіт [10, 27, 45, 132, 146 – 150], ці виклики можуть мати як технічну чи людську природу, так і бути пов’язані з організаційними аспектами. Зважаючи на це, виникла потреба у виділенні та аналізі основних проблемних завдань управління інформаційними потоками в такому середовищі [43, 49, 123].

Першим таким завданням є забезпечення захисту персональних і конфіденційних даних студентів, викладачів і адміністративного персоналу які беруть участь у навчальному процесі. В працях [44, 103,116,] авторами зазначається, що серед можливих проблем є: використання незахищених чи невідповідних методів зберігання

даних, що збільшує ризик крадіжки їх крадіжки; недоліки в механізмах аутентифікації та авторизації які можуть призвести до несанкціонованого доступу до конфіденційної інформації.

Наступне проблемне завдання – інтеграція різноманітних систем та платформ. На це звертається увага у багатьох роботах [13, 47, 55, 60, 85, 112, 151 – 153]. Аналіз таких робіт дав змогу виділити можливі виклики. Перше це те, що різні платформи можуть використовувати різні стандарти та протоколи, що ускладнює їх інтеграцію. А друге – відсутність єдиного джерела істини. Це призводить до дублювання даних і можливих помилок при їхньому обміні.

Управління доступом та ідентифікацією. В контексті цього пункту можна виділити роботи [11, 103, 111, 147]. На основі аналізу таких робіт можна сказати, що основною проблемою є забезпечення належного рівня доступу для різних категорій користувачів (студенти, викладачі, адміністратори) без компрометації безпеки. Серед викликів з якими стикаються у даному напрямку виділяються наступні: різнорідність ролей і прав доступу, тобто необхідність підтримки та управління великою кількістю ролей і прав доступу, а також часті зміни прав доступу у сучасному світі відбуваються постійні зміни у вимогах до прав доступу через зміни в академічних та адміністративних структурах.

Наступним пунктом є проблемні завдання пов’язані з забезпеченням точності та актуальності даних, для уникнення помилок у процесі управління та прийняття рішень. На основі робіт [55, 59, 103] з проблем можна виділити те що різні системи можуть зберігати дані у різних форматах, що ускладнює їх об'єднання й аналіз. Крім того, дані можуть застарівати через несвоєчасне внесення змін або оновлення.

Як зазначалось раніше з’являється аспект управління великими обсягами даних (Big Data). У цьому напрямку проблематичним є зберігання, обробка та аналіз великих обсягів даних, що генеруються освітніми системами [103]. Обробка великих обсягів даних може перевантажувати системи та знижувати їх продуктивність, крім того, з'являється складність аналізу даних, адже дуже ймовірним є виникнення необхідності

використовувати спеціалізовані інструменти та методи для аналізу даних [103, 141, 154].

Слідуючим проблемним завданням є забезпечення захисту освітніх систем від кіберзагроз та атак, таких як фішинг, DDoS, зловмисне програмне забезпечення та інші. Адже необізнані користувачі можуть стати жертвами фішингових атак через брак знань про кібербезпеку. Ну і звісно прогрес не стоїть на місці тому є постійний розвиток нових типів атак і методів їх виконання [92, 103, 155].

Останньою виділеною проблемою є забезпечення безперервного моніторингу, аудиту та контролю інформаційної інфраструктури діджиталізованого освітнього середовища. В цьому контексті опрацьовано велику кількість робіт [48, 52, 93, 110, 121, 124, 130, 133, 136, 142 – 144, 156 – 157]. З цього аналізу видно, що головними викликами є необхідність відстеження активності у розподілених і децентралізованих системах, а також потреба інтеграції рішень для моніторингу з уже існуючими діджитал системами.

Отже, вкотре підтверджено, що управління інформаційними потоками у діджиталізованому освітньому середовищі об’єднує безліч аспектів, кожен з яких потребує ретельного планування та постійного вдосконалення [14, 130]. Впровадження сучасних технологій та методів, таких як багатофакторна автентифікація, шифрування даних, анонімізація інформації, рольовий контроль доступу, стандарти обміну даними, інструменти для аналізу великих даних, тренінги з кібербезпеки та системи моніторингу, покликані вирішити вищезгадані проблеми та підвищити загальний рівень безпеки та ефективності діджиталізованого освітнього середовища [42, 123, 124, 130]. Але головне, на що неодноразово зверталась увага раніше, це те, що зі зростанням діджиталізації освітнього середовища зростає і кількість персональних даних, що обробляються і зберігаються у різних інформаційних системах. Про це ідеться у багатьох роботах, як приклад варто згадати [78, 84, 123, 139, 149]. Як зазначається в статтях – забезпечення конфіденційності цих даних стає все більш критичним завданням [86, 127, 158]. І саме анонімізація даних перед їх поширенням навчальним

закладом зовнішнім платформам є одним з найефективніших методів захисту персональних даних. Крім того, отримані знання з проведеного аналізу та практичного досвіду роботи у сфері надання послуг навчальним закладам з управління потоками даних дозволяють стверджувати, що анонімізація набуває значної актуальності з багатьох причин.

Першою такою причиною є необхідність відповідності нормативно-правовим вимогам [115]. У багатьох країнах діють суворі закони та нормативні акти щодо захисту персональних даних. Прикладами є Генеральний регламент захисту даних (GDPR) у Європейському Союзі, Закон про захист прав споживачів Каліфорнії (CCPA) у США. І саме впровадження анонімізації дозволяє організаціям відповідати цим вимогам, знижуючи ризики, пов’язані з витоками даних і порушеннями конфіденційності.

Наступною причиною є те, що анонімізовані дані значно складніше ідентифікувати, що захищає людей від потенційних загроз, зокрема викрадення особистих даних. І навіть у разі витоку анонімізовані дані не несуть такої ж загрози, як повністю ідентифіковані, що значно пом’якшує наслідки кіберінцидентів.

Також захист персональних даних за допомогою анонімізації підвищує довіру студентів, викладачів і батьків до освітніх інститутів, адже демонструючи зобов’язання щодо захисту конфіденційності, освітні установи підкреслюють свою етику та відповідальність перед своєю аудиторією.

Забезпечується можливість безпечного застосування аналітики та досліджень. Освітні інститути часто здійснюють дослідження на основі зібраних даних. Анонімізація дозволяє проводити ці дослідження без ризику порушення конфіденційності. Крім того, використання анонімізованих даних дозволяє більш широко застосовувати аналітику і відкрити доступ до даних для наукових досліджень та розробок.

Наступна причина стосується зростання обсягів даних і їх організаційна складність. Як зазначалось раніше діджиталізація освітнього процесу призводить до збільшення обсягів даних, що обробляються, зокрема даних студентів, навчальних

матеріалів, результатів оцінювання тощо. Високий рівень складності управління такими обсягами даними призводить до появи додаткових ризиків виникнення помилок і витоків. І саме анонімізація допомагає зменшити ці ризики.

Також варто врахувати появу нових технологій і методів [125]. Новітні алгоритми та підходи до анонімізації дозволяють ефективніше захищати дані. Наприклад, диференційна приватність (differential privacy) надає додатковий рівень захисту, зберігаючи при цьому корисність даних [159]. Крім того, застосування штучного інтелекту для автоматизації процесу анонімізації може значно підвищити ефективність і точність захисту даних.

Останнє про що варто сказати – існує ризик, що навіть частково анонімізовані дані можуть бути поєднані з іншими наборами даних для ідентифікації особистостей, з огляду на ці ризики, необхідно і надалі вдосконалювати методи анонімізації для забезпечення стійкості до повторної ідентифікації [123].

Підсумовуючи аналіз актуальності та важливості подальших досліджень у сфері анонімізації даних в освітньому середовищі, виділено низку причин, які однозначно це доводять [52, 88, 149]. Адже анонімізація дозволяє забезпечити відповідність нормативним вимогам і зниження ризиків правових санкцій [127]. Підвищити рівень довіри до освітніх інститутів [145]. Забезпечити високий рівень безпеки та конфіденційності персональних даних. Надає можливість проведення безпечних досліджень і аналізу великих обсягів даних. А також впливає на вдосконалення технологій і підвищення організаційної ефективності.

Таким чином, подальші дослідження у сфері застосування анонімізації до захисту персональних даних є необхідними для створення безпечного і надійного освітнього середовища в умовах зростаючої діджиталізації [123, 160].

1.5 Аналіз застосування анонімізації з метою захисту персональних даних в інформаційних потоках в освітній сфері

Як визначено раніше, анонімізація даних є важливим інструментом для забезпечення конфіденційності в освітній сфері, особливо в умовах діджиталізації, коли великі обсяги даних обробляються та зберігаються в електронному вигляді [116, 123]. А застосування анонімізації дозволяє знизити ризики, пов'язані з несанкціонованим доступом до персональних даних [134]. Зважаючи на це, необхідним є аналіз можливого застосування анонімізації в освітній сфері.

Оскільки освітні установи збирають величезні обсяги даних про академічну успішність, відвідуваність, оцінки та інше, такі дані можуть бути анонімізовані для аналізу тенденцій, проведення досліджень або обміну з третіми сторонами без розкриття ідентичності студентів. Для цього можна застосовувати шифрування ідентифікаційних та персональних даних, використання псевдонімів замість реальних імен, агрегування даних.

Часто наукові дослідження в освітній сфері часто потребують доступу до великих обсягів студентських даних. Дослідники можуть використовувати анонімізовані набори даних для проведення аналізу, що дозволяє уникнути витоку конфіденційної інформації. Тут має сенс видалення ідентифікаційних полів, додавання шумів до даних (диференційна приватність) [159].

А головне освітні заклади постійно передають дані постачальникам освітніх послуг, дослідницьким організаціям або урядовим структурам. Передача анонімізованих даних зменшує ризики втрати конфіденційності під час обміну інформацією [128, 135]. Також може бути застосована псевдонімізація, агрегація даних, маскування даних.

На основі попереднього аналізу існуючих напрацювань, прикладами яких є [84, 123, 128, 133 – 136, 159], дефініційовано основні методи анонімізації даних:

1. Видалення ідентифікаційних полів. Видалення або маскування полів, які можуть безпосередньо ідентифікувати особу (ім'я, адреса, номер студентського квитка тощо). Характеризується простотою реалізації, але дані можуть все ще бути вразливими до повторної ідентифікації при поєднанні з іншими наборами даних.

2. Псевдонімізація. Замінювання реальних ідентифікаторів на штучно створені псевдоніми. З переваг – забезпечує певний рівень конфіденційності, зберігаючи корисність даних для подальшого аналізу. Недолік – псевдонімізація може бути недостатньо захищеною від розпізнавання з іншими наборами даних.

3. Агрегація даних. Комбінування даних у великі групи, що робить неможливим виокремлення окремих осіб. Цей спосіб забезпечує високий рівень захисту конфіденційності, підходить для аналізу загальних тенденцій. З недоліків можна виділити втрату деталей, що можуть бути корисними для глибокого аналізу.

4. Додавання шуму до даних (диференційна приватність) [159]. Додавання випадкових змін до даних з метою запобігання ідентифікації індивідуальних записів. Цей спосіб має високий рівень захисту, особливо під час статистичного аналізу великих обсягів даних, але може впливати на точність даних для окремих записів [133].

Після цього визначено головні переваги застосування анонімізації в освітній сфері які випливають з згаданого раніше в цьому розділі:

1. Основна перевага анонімізації — захист конфіденційності студентів, викладачів та іншого персоналу, зменшення ризику витоків і зловживань.

2. Виконання вимог щодо захисту персональних даних, встановлених різними актами, як GDPR, FERPA та інші.

3. Анонімізовані дані можуть бути використані для проведення освітніх та наукових досліджень без порушення конфіденційності.

4. Захист персональних даних підвищує довіру до освітніх установ з боку студентів, батьків і інших стейкхолдерів.

Але крім позитивного аспекту є і негативний, тому наведено перелік недоліків та викликів пов’язаних з застосуванням анонімізації:

1. Ризик повторної ідентифікації, оскільки низький рівень анонімізації та використання зовнішніх додаткових наборів даних може призвести до повторної ідентифікації анонімізованих даних.

2. Зниження корисності даних. На противагу попередньому пункту деякі кардинальні методи анонімізації можуть значно знизити точність і корисність даних для аналізу.

3. Високорівневі методи анонімізації можуть бути складними в реалізації й вимагати спеціалізованих знань і ресурсів.

4. Крім того, не всі системи та платформи можуть підтримувати складні методи анонімізації, і нормативно-правові акти можуть накладати додаткові обмеження.

Отже, анонімізація є потужним інструментом для захисту персональних даних в освітньому середовищі, забезпечуючи як захист конфіденційності, так і відповідність регулятивним вимогам. Попри наявні виклики та ризики, застосування анонімізації дозволяє значно підвищити рівень безпеки інформаційних потоків. Подальші дослідження в цій сфері допоможуть удосконалити існуючі методи та розробити нові підходи для більш ефективного і безпечного управління даними в галузі освіти. [84, 116, 123, 127 – 128, 133 – 136, 143, 147]

1.6 Постановка задачі дослідження

Як видно з проведеного аналізу з розвитком цифрових технологій, обсяг даних, які збираються про учасників навчального процесу, стрімко зростає. Це включає інформацію про академічні досягнення, поведінкові дані в навчальних системах, особисті дані студентів та викладачів, дані про взаємодію з навчальними платформами, а також адміністративні дані. Таке накопичення інформації вирізняється складністю та обсягами, ставлячи перед системами освіти задачу постійного вдосконалення управлінських практик і технологій збереження даних. Хоча ці дані є вкрай важливими

для аналізу і покращення якості навчання, їх зберігання й обробка несе ризики, пов’язані з витоками даних та несанкціонованим доступом.

Збільшення обсягу даних створює необхідність їх ефективного менеджменту, оскільки несанкціоноване використання таких даних може мати серйозні наслідки як для окремих учасників навчального процесу, так і для установ загалом. Незважаючи на різноманітні підходи до захисту інформації, такі як шифрування, захист мережевих протоколів і автентифікація користувачів, вони здебільшого зосереджені на захисті вже зібраних даних та каналів їх передачі.

На противагу цьому, концепція анонімізації пропонує не лише захист, а й профілактику витоків, оскільки дані стають такими, які неможливо розпізнати з самого початку. Це означає, що дані, які можуть бути корисними для освітніх аналітиків, дослідників та адміністраторів, не можуть бути пов'язаними з конкретними особами, що значно ускладнює можливості їх несанкціонованого використання. Зокрема, дослідивши цей напрямок детально, варто зазначити, що методи анонімізації можуть включати техніки заміни, генерації псевдонімів, агрегування, та інші способи зміни структури даних. Це дозволяє зберігати інформацію, що є важливою для навчального аналізу, при цьому зберігати приватність осіб.

Однак, проведений аналіз показує, що анонімізація не є широко розповсюдженим підходом у сфері освіти. Значна частина навчальних закладів все ще не має чітких методик її впровадження, що є наслідком відсутності достатньої кількості досліджень і документальних прикладів успішного використання таких підходів. Як результат, заклади освіти часто обмежуються стандартними методами захисту, які не забезпечують достатнього рівня безпеки у сучасному діджиталізованому світі.

Крім того, впровадження методик анонімізації стикається з технічними й організаційними викликами через відсутність системного бачення та стандартів у цій сфері. Для навчальних установ критично важливо мати уніфіковані підходи та інструменти, які можна інтегрувати у вже наявні системи управління навчанням. Це дозволило б ефективно захищати дані, використовуючи новітні технології та методики.

Все це вказує на **необхідність розробки моделей та методів, які б дозволили освітнім установам впроваджувати управління потоками персональних даних суб'єктів освітнього середовища в умовах діджиталізації** на всіх етапах збереження та обробки даних. Зокрема, такі моделі та методи повинні враховувати різні рівні конфіденційності даних, типи освітніх систем, а також технологічні можливості конкретних навчальних закладів.

Метою цієї дослідницької роботи є підвищення ефективності управління потоками персональних даних освітнього середовища в умовах діджиталізації за рахунок розробки моделей, методу та інформаційної технології захищеності персональної інформації учасників освітнього процесу.

Дослідження у цьому напрямку також сприятиме довірі між учасниками навчального процесу, включаючи студентів, викладачів та адміністрацію, забезпечуючи при цьому відповідність сучасним стандартам інформаційної безпеки.

Для реалізації цих цілей необхідно вирішити ряд науково-прикладних завдань:

1) аналіз існуючих підходів до управління інформаційними потоками освітнього середовища у контексті діджиталізації;

2) розробка концепції управління потоками персональних даних у контексті діджиталізації освітньої сфери, в основі якої модель інформаційних потоків та інформаційних взаємодій у діджиталізованій освітній сфері;

3) формування моделі управління зберіганням потоків даних освітнього середовища;

4) запропонувати модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища;

5) розробка методу управління потоками персональних даних в умовах діджиталізації освітньої сфери;

6) розробка, застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації та визначення її ефективності.

Дослідження в рамках цієї роботи базуватимуться на існуючих актуальних напрацюваннях у сфері освіти, захисту інформації, зокрема й анонімізації даних персональної інформації. Планується детально проаналізувати сучасні методики та інструменти, які вже були застосовані в інших сферах, з метою адаптації їх до освітнього контексту. Крім того, розроблена методологія анонімізації даних буде впроваджена в межах однієї з великих існуючих навчальних платформ. Це дозволяє не лише перевірити ефективність запропонованих підходів, а й отримати цінний практичний досвід, який може бути використано для подальшого вдосконалення системи захисту даних в освітній сфері.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. У цьому розділі всебічно проаналізовано вплив діджиталізації на інформаційні потоки в освітній сфері, що є ключовим фактором у формуванні сучасного навчального середовища. Дослідження у сфері освіти показали, що постійні зміни, викликані новими технологіями, значно трансформують як педагогічний процес, так і управління інформацією. Розглянуто конкретні зміни, пов'язані з розвитком технологій, і проаналізовано, як різноманітні інформаційні технології впливають на освітню діяльність.

2. Проведено глибокий аналіз існуючих підходів до управління інформаційними потоками в умовах діджиталізації, що дозволило зрозуміти, як ці процеси інтегруються у функціонування освітніх систем. Також досліджено акцент на необхідності підвищення безпеки у сфері захисту персональних даних та розглянуто актуальні моделі захисту, що застосовуються в цифрових освітніх середовищах.

3. Розглянуто проблемні питання, які супроводжують управління інформаційними потоками в умовах діджиталізації, приділено увагу проблемам в освіті та викликам, що виникають під час роботи з даними. Аналіз виявив недоліки та

загрози, що могли б погіршити процес діджиталізації, особливо в розрізі захисту інформації та особистих даних учасників освітнього процесу.

4. Особлива увага у розділі приділена аналізу застосування анонімізації як перспективного підходу для забезпечення безпеки персональних даних. З'ясовано, що анонімізація може значно знизити ризики, пов'язані з витоками інформації, роблячи дані менш вразливими до несанкціонованого доступу. Дослідження підтвердили, що правильно застосовані методології анонімізації мають суттєвий потенціал для покращення захисту інформаційних потоків у системах освіти.

5. Виконано постановку задач дослідження, які мають бути реалізовані для забезпечення ефективного управління потоками персональної інформації в діджиталізованій освітній сфері. Ці задачі включають: аналіз потоків персональних даних з акцентом на навчальні заклади як центральні елементи, класифікацію стейкхолдерів для роботи з їх персональними даними, ідентифікацію ключових точок контролю цих потоків. На основі цього необхідно розробити модель ризиків витоку даних і побудувати модель анонімізації та деанонімізації даних учасників навчального процесу. Також важливими є задачі з розробки принципів мінімізації поширення даних і створення методів управління потоками з анонімізацією та деанонімізацією, які повинні включати алгоритми для цих процесів. Практична частина передбачає розробку інформаційної технології, архітектури, програмного забезпечення та оцінку ефективності цих рішень. Розв’язання цих задач стане основою для подальших досліджень та впровадження в освітніх платформах.

РОЗДІЛ 2. МОДЕЛІ УПРАВЛІННЯ ПОТОКАМИ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ДІДЖИТАЛІЗАЦІЇ ОСВІТНЬОЇ СФЕРИ

2.1 Концепція управління потоками персональних даних у контексті діджиталізації освітньої сфери

2.1.1 Потоки персональних даних у діджиталізованій освітній сфері

Отримавши чітке розуміння існуючих напрацювань в галузі, а також визначивши завдання роботи, логічним першим кроком стала побудова схеми інформаційних потоків діджиталізованого освітнього середовища в контексті поширення персональних даних стейкхолдерів (рис. 2.1).

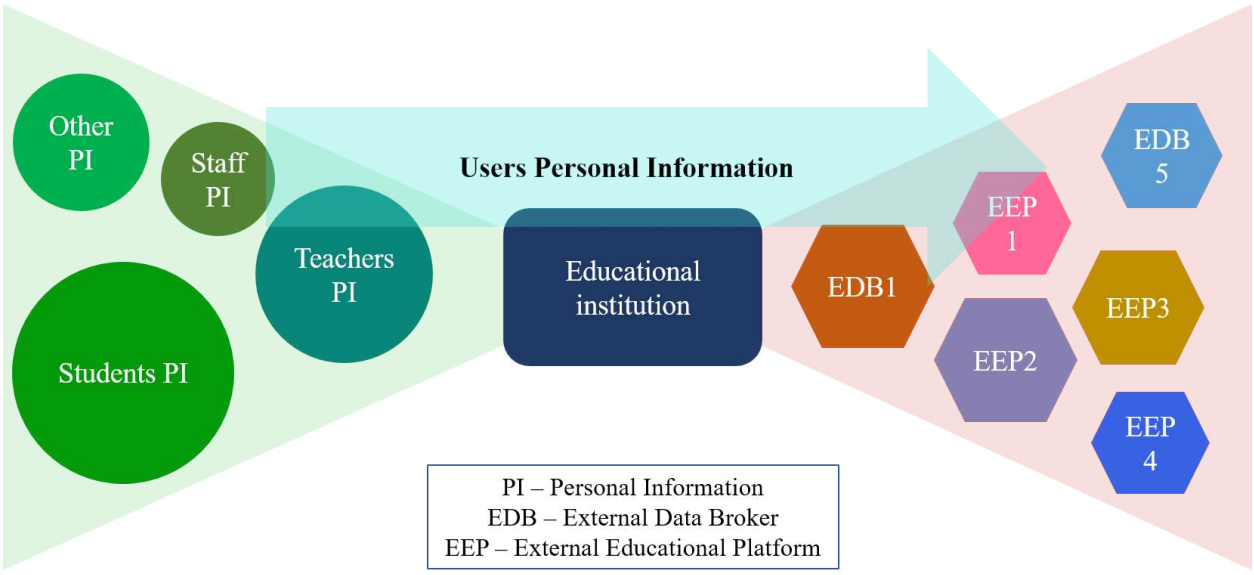

Рис. 2.1. Потоки персональної інформації діджиталізованого освітнього середовища

Побудована схема складається з трьох ключових частин. Кожна з цих частин має такі елементи:

1. Навчальний заклад – є центром інформаційної взаємодії діджиталізованого освітнього середовища. Є ініціатором інформаційного обміну. Також являється як споживачем персональної інформації від її власників, так і її джерелом для зовнішніх споживачів.

2. Вхідні потоки персональних даних стейкхолдерів навчального процесу – це можуть бути дані різного роду, починаючи з імені та фамілії користувача і закінчуючи адресою проживання та номерами телефонів батьків. Існує кілька основних джерел такої інформації:

2.1. Студенти – найбільш вразлива частина зацікавлених сторін освітнього середовища. Для вступу в навчальний заклад, а також успішного продовження навчання у ньому студенти поширюють неймовірну кількість персональних даних з навчальним закладом. Процес менеджменту такої кількості персональної даних вимагає застосування високих стандартів захисту даних.

2.2. Викладачі – оскільки викладачі не просто навчаються у навчальному закладі, а є основною частиною його персоналу, персональних даних їм доводиться надавати про себе навчальному закладу не менше. Крім стандартного набору персональних даних уже додаються платіжні реквізити, рекомендаційні листи та чимало іншої приватної інформації.

2.3. Інший персонал навчального закладу – перелік таких посад досить великий: охоронець, директор з обладнання, клінінг-адміністратор та багато інших. Тут ситуація дещо схожа з викладацьким персоналом, за винятком того що заклад зазвичай не збирає інформацію з наукової діяльності такого персоналу. Та все ж освітній заклад має доволі серйозний набір персональних даних кожного з таких працівників.

3. Вихідні потоки персональних даних стейкхолдерів навчального закладу – поширення інформації освітнім закладом з третіми сторонами присутнє у будь-якій його сфері діяльності. Починаючи з банківських послуг і закінчуючи закупівлею канцелярського обладнання. Та найбільш суттєвим інформаційний обмін є при забезпеченні закладом своєї основної функції – навчання студентів. Забезпечуючи

високий рівень знань та технологій студентам, навчальний заклад у діджиталізованому середовищі не може обійтись без обміну персональною інформацією користувачів з зовнішніми навчальними платформами та ресурсами. Тут розрізняється два основних типи зовнішніх сервісів:

3.1. Зовнішня навчальна платформа – усі діджиталізовані заклади інтегруються з безліччю таких платформ. Це можуть бути сервіси з розміщення навчальних матеріалів, онлайн щоденники, відео платформи тощо. Різноманіття таких ресурсів у сучасному цифровому світі справді вражає. Але крім безумовних переваг, які приносять в навчальний процес такі інформаційні технології, як невід'ємний побічний ефекти, маємо появу нових суттєвих ризиків витоку персональної інформації їх користувачів.

3.2. Зовнішній брокер даних – така система, як і звичайна зовнішня навчальна платформа може надавати певні інформаційно-технологічні рішення для полегшення та покращення навчального процесу інтегруючись з навчальним закладом. Такі як візуалізація даних користувачів, сортування, фільтрація і безліч іншого функціоналу. Але основною функцією такого сервісу є поширення стандартизованих даних наступним споживачам. Тобто суть полягає в наступному – брокер даних отримує інформацію у певному форматі від навчального закладу і забезпечує перетворення її у будь-який інший потрібний формат для забезпечення інтеграції з іншими зовнішніми навчальними платформами, поширюючи дані у потрібному споживачеві форматі. Звідси, брокер даних перетворюється зі споживача персональної інформації на її джерело подальшим споживачам. Тобто ризики витоку персональної інформації стейкхолдерів навчального процесу зростають в рази.

2.1.2 Стейкхолдери інформаційної взаємодії діджиталізованої сфери освіти

Обов'язковою вимогою при вдосконаленні існуючої сталої моделі взаємодії та поширення інформації у сфері освіти – є попереднє вивчення та аналіз середовища у

якому і виконується ця взаємодія. Також важливим є розуміння та опрацювання існуючих інформаційних потоків, адже саме це і є тією складовою, яка несе ризики витоку персональної інформації усіх осіб задіяних у цьому процесі.

Проведено аналіз інформаційної взаємодії, який дозволив сформувати перелік сторін залучених в обміні персональною інформацією у сфері освіти. Далі перелічено такі стейкхолдери з коротким описом їх ролі в освітньому процесу:

1. Здобувачі освіти. Основні суб’єкти освітнього процесу, які надають свої особисті дані, такі як ім'я, адреса, дата народження, контактна інформація, ідентифікаційні номери, академічні досягнення тощо.

2. Викладачі та інші працівники освітніх установ, включаючи викладачів, адміністраторів, керівників відділень та інших співробітників, які також надають свої персональні дані, а також можуть мати доступ до особистої інформації здобувачів освіти.

3. Освітні установи. Інформація про самі освітні установи, такі як назва, контактні дані, правовий статус, фінансові деталі, може бути залучена в обміні даними з іншими організаціями чи інституціями. Крім того, освітня установа, по суті, є рушієм усієї інформаційної взаємодії.

4. Батьки або опікуни здобувачів освіти. Якщо студенти є неповнолітніми, їхні батьки або опікуни можуть бути залучені у процесі обміну інформацією, особливо щодо навчальних питань та організації навчання.

5. Електронні платформи та інформаційні системи. Інформаційні технології, які використовуються в освітній сфері, такі як онлайн-платформи для навчання, системи управління навчальним процесом, електронні реєстри тощо, є також залучені в обміні персональною інформацією.

6. Зовнішні партнери та інші сторони, адже у деяких випадках, освітні заклади можуть співпрацювати з іншими організаціями або сторонами, такими як дослідницькі організації, виконавчі агентства, страхові компанії тощо, і обмінюватися даними з ними.

7. Державні органи та регулятори. У деяких випадках, зокрема з питань статистики або виконання законодавства про освіту, персональна інформація може передаватися державним органам або регуляторам.

Отже, встановлено, що глобально атомарною одиницею обміну інформації у цій галузі є навчальний заклад або їх об’єднана мережа. Глобальною та найменш регульованою стороною, яка споживає, опрацьовує та обмінюється персональною інформацією здобувачів освіти, викладачів і інших осіб залучених у навчальному процесі є зовнішні електронні платформи та інформаційні системи.

2.1.3 Модель інформаційної взаємодії та потоків даних у діджиталізованій освітній сфері

На основі аналізу інформаційних взаємодій та потоків даних у діджиталізованому освітньому середовищі та визначених стейкхолдерах освітнього процесу сформовано модель інформаційної взаємодії та потоків даних у діджиталізованій освітній сфері. Схематичне зображення такої моделі наведено на рис. 2.2.

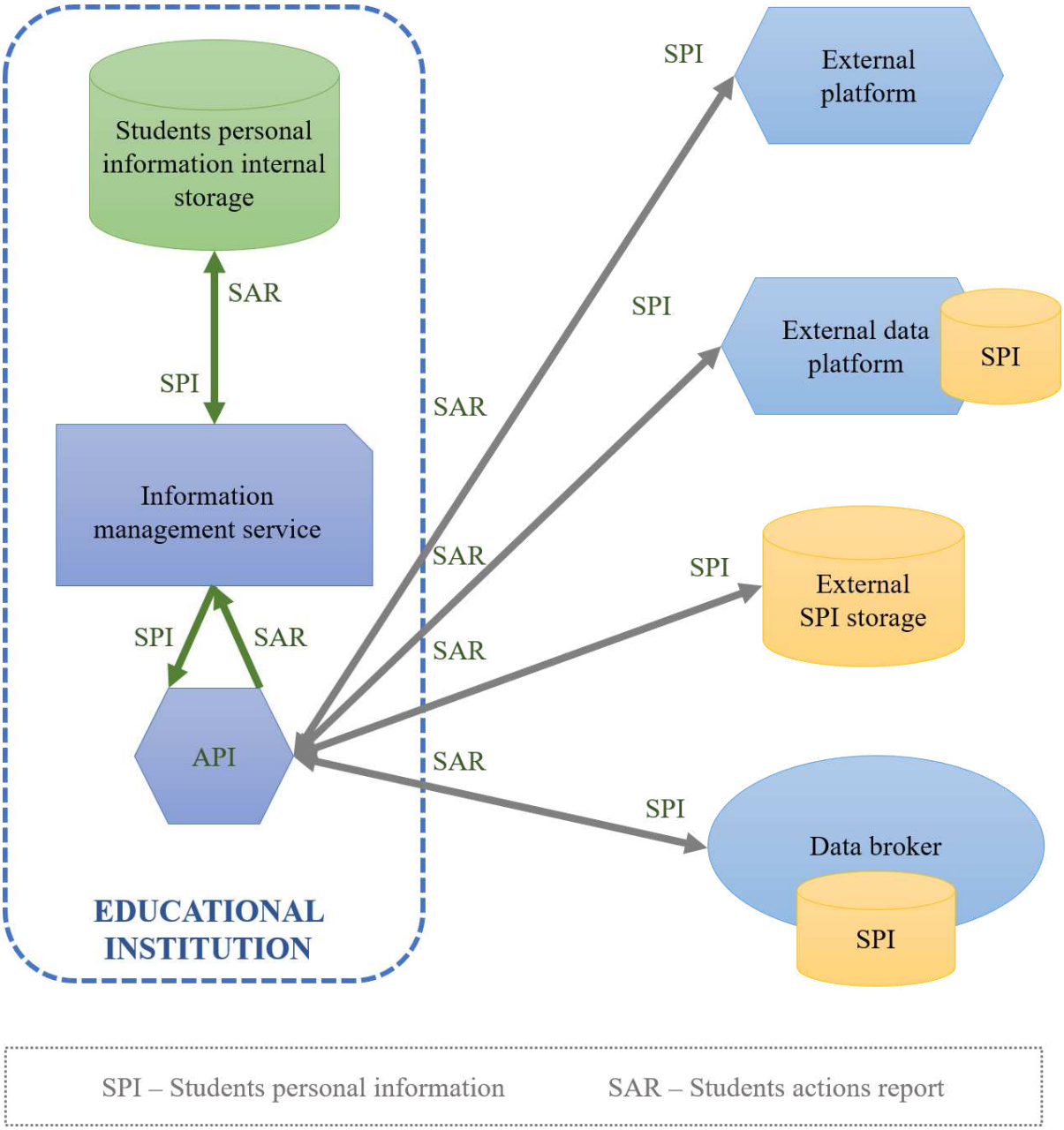

Рис. 2.2. Схематична модель інформаційної взаємодії та потоків даних в освітньому середовищі в умовах діджиталізації

Як видно на розробленій схемі потоки даних мають джерело даних і споживача. Джерелом даних при інформаційній взаємодії у діджиталізованому освітньому середовищі є навчальний заклад. Споживачами даних можуть бути різного роду зовнішні сервіси інтеграцію з якими встановлено навчальним закладом. Базуючись на цьому, визначено, що ***потік даних*** в діджиталізованому освітньому середовищі – це

сукупність дій, які застосовуються до цифрових даних з метою передачі даних від джерела до отримувача, кінцевою ціллю якої є забезпечення отримання від споживача певного сервісу. При такій інформаційній взаємодії потік даних може містити в собі різного типу етапи роботи з даними: передача, трансформація, збереження тощо.

Як видно зі схеми (рис. 2.2) існує кілька типів зовнішніх споживачів даних з якими може інтегруватись навчальний заклад. Тож, виділено ці типи та описано етапи через які можуть проходити дані у потоці даних при інформаційній взаємодії з такими типами зовнішніх сервісів (табл. 2.1).

Таблиця 2.1. Типи зовнішніх споживачів даних та етапи потоку даних

№	Зовнішній споживач даних	Етапи через які проходять дані
1	Проста зовнішня платформа	Передача даних, обробка даних
2	Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних
3	Сховище даних	Передача даних, збереження даних
4	Брокер даних	Передача даних, обробка даних, збереження даних, наступні передачі, обробки та збереження даних

Як видно з таблиці інформаційна взаємодія освітньої установи з різними типами зовнішніх сервісів характеризується різним набором етапів, які проходять дані. Загалом можна виділити три їх види:

1) Передача даних – тобто цифрове транспортування даних від джерела до отримувача. Як зазначалось раніше джерелом зазвичай є навчальний заклад. Але є і виняток, якщо інтеграція з зовнішнім сервісом вимагає додаткового перетворення даних чи іншої проміжної роботи з ними, то застосовуються брокери даних. У цьому випадку, звісно, головним джерелом даних є навчальний заклад, адже саме він

поширює дані з брокером, але для третьої сторони, тобто кінцевого навчального сервісу, який вимагає трансформованих даних джерелом буде саме брокер.

2) Обробка даних. Обробка може бути різних видів, як то перетворення в інший формат, формування з отриманих даних електронних листів та багато іншого.

3) Збереження даних. Збереження може відбуватись просто у файл, базу даних чи у сховище будь-якого іншого виду. Звісно, більшість сервісів не зберігають усю отриману інформацію, зазвичай зберігається лише важлива частина даних. Варто зазначити, що деякі сервіси, додатково зберігають статистику сформовану з використанням отриманих даних.

Оскільки, як визначено раніше, при управлінні потоками даних одним з найголовніших завдань є забезпечення високого рівня захищеності даних, тому зосереджено увагу саме на цьому аспекті. Розрахунок оцінки небезпечності етапу у потоці даних з точки зору витоку персональних даних запропоновано здійснювати за:

$$DE = V * U \qquad (2.1)$$

де *DE* – оцінка небезпеки витоку персональних даних на етапі потоку даних;

V – вразливість до витоку персональних даних на етапі потоку даних;

U – співвідношення кількості персональних до загальної кількості даних на етапі потоку даних;

Вразливість до витоку персональних даних *V* на етапі потоку персональних даних може бути оцінена різними шляхами. Таку оцінку може дати зібрана група експертів, звіт зовнішньої аудиторської компанії тощо.

Для визначення відносної оцінки небезпеки потоку даних в контексті витоку персональних даних введено формулу:

$$DP = D * I * \sum_{i=1}^{n} DE_i, i = 1...n, \qquad (2.2)$$

де *DP* – відносна оцінка небезпеки потоку даних в контексті витоку персональних даних;

D – співвідношення середньої кількості даних у потоці даних до середньої кількості даних усіх потоків даних навчального закладу;

I – співвідношення інтенсивності потоку даних до інтенсивності усіх потоків даних навчального закладу;

DE_i – оцінка небезпеки витоку персональних даних на *i*-му етапі потоку даних *(2.1)*;

n – кількість етапів через які проходять дані у потоці даних.

Інтенсивність потоку даних *I* розраховується як співвідношення кількості запусків цього потоку даних відносно кількості запусків усіх потоків даних освітньої установи за певний часовий відрізок. Часовий відрізок вибирається індивідуально для кожного закладу таким чином, щоб якомога точніше врахувати кількість запусків усі існуючих потоків.

Сумарну оцінку вразливості потоків даних до витоку персональних даних при інформаційних взаємодій навчального закладу у діджиталізованій освітній сфері можна виразити формулою:

$$SD = \sum_{j=1}^{m} DP_j, j = 1...m, \qquad (2.3)$$

де *SD* – оцінка вразливості потоків даних навчального закладу до витоку персональних даних;

DP_j – відносна оцінка небезпеки *j*-го потоку даних в контексті витоку персональних даних *(2.2)*;

m – кількість потоків даних навчального закладу.

Отже, для визначення чи є інформаційні взаємодії навчальної установи в контексті діджиталізованої освітньої сфери повністю безпечними застосовується формула *(2.3)*. Якщо розраховане значення за *2.3* більше нуля, це означає що потоки даних, які забезпечують інтеграцію навчального закладу з зовнішніми сервісами не є безпечними. Чим значення є більшим, тим більш серйозні заходи з посилення безпеки потрібно застосувати до потоків даних.

Для визначення які з потоків даних є найбільш незахищеними застосовується формула *(2.2)*. Отримавши відносні оцінки небезпеки виникнення подій витоку персональних даних у кожному потоці даних, потрібно розставити пріоритети відповідно до отриманих значень. Якщо ймовірність виникнення витоку персональних даних є більшою від нуля, то такий потік підлягає підвищенню рівня захищеності. Чим більша розрахована оцінка, тим пріоритетнішою є робота з посилення захищеності даних на цьому потоці даних.

Запропоновано приклад застосування розробленої моделі з використанням даних наближених до реальної ситуації одного з навчальних закладів. Через вимогу джерела інформації до конфіденційності та анонімності дані згенеровано штучно. Тому дані не є реальними, але вони являються наближеними до таких. В таблиці 2.2 зображено перелік потоків даних навчального закладу та усі необхідні дані по кожному з них. Також за формулою *(2.1)* розраховано рівень небезпеки кожного етапу цих потоків.

Таблиця 2.2. Дані потоку “навчальний заклад – проста зовнішня платформа 1”

Навчальний заклад – проста зовнішня платформа 1			
Етап	V	U	DE
Передача даних	0,1	0,4	0,04
Обробка даних	0,2	0,4	0,08
		Сумарна небезпека усіх етапів:	0,12

Таблиця 2.3. Дані потоку “навчальний заклад – проста зовнішня платформа 2”

Навчальний заклад – проста зовнішня платформа 2			
Етап	V	U	DE
Передача даних	0,1	0,5	0,05

Обробка даних	0,2	0,5	0,1
		Сумарна небезпека усіх етапів:	0,15

Таблиця 2.4. Дані потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 1”

Навчальний заклад – зовнішня платформа зі зберіганням даних 1			
Етап	V	U	DE
Передача даних	0,1	0,6	0,06
Обробка даних	0,2	0,5	0,1
Збереження даних	0,4	0,5	0,2
		Сумарна небезпека усіх етапів:	0,36

Таблиця 2.5. Дані потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 2”

Навчальний заклад – зовнішня платформа зі зберіганням даних 2			
Етап	V	U	DE
Передача даних	0,1	0,6	0,06
Обробка даних	0,3	0,5	0,15
Збереження даних	0,5	0,5	0,25
		Сумарна небезпека усіх етапів:	0,46

Таблиця 2.6. Дані потоку “навчальний заклад – брокер даних – зовнішня платформа зі зберіганням даних 3”

Навчальний заклад – брокер даних – зовнішня платформа зі зберіганням даних 3			
Етап	V	U	DE
Передача даних	0,1	0,5	0,05
Обробка даних	0,2	0,5	0,1
Збереження даних	0,2	0,5	0,1
Передача даних	0,1	0,6	0,06
Обробка даних	0,3	0,6	0,18
Збереження даних	0,4	0,6	0,24
Сумарна небезпека усіх етапів:			0,73

Як видно з даних, є два потоки типу “навчальний заклад – проста зовнішня платформа”, два типу “навчальний заклад – зовнішня платформа зі зберіганням даних” та один за участі брокера “навчальний заклад – брокер даних – зовнішня платформа зі зберіганням даних”. В таблиці 2.7 вказано відносні оцінки інтенсивності потоків та кількості даних у них. Також розраховано оцінку небезпеки кожного потоку даних за формулою *(2.2)*.

Таблиця 2.7. Оцінки інтенсивності потоків, кількості даних у них та сумарна оцінка їх небезпеки

Потік даних	D	I	DP
Навчальний заклад – проста зовнішня платформа 1	0,1	0,2	0,0024
Навчальний заклад – проста зовнішня	0,1	0,1	0,0015

платформа 2			
Навчальний заклад – зовнішня платформа зі зберіганням даних 1	0,3	0,2	0,0216
Навчальний заклад – зовнішня платформа зі зберіганням даних 2	0,2	0,2	0,0184
Навчальний заклад – брокер даних – зовнішня платформа зі зберіганням даних 3	0,3	0,3	0,0657

Застосувавши отримані оцінки, підраховано оцінку вразливості потоків даних навчального закладу до витоку персональних даних за формулою *(2.3)* – SD = 0,1096. Отримане значення є більшим за нуль, відповідно інформаційні взаємодії навчального закладу не є повністю безпечними та вимагають застосування певних заходів з підвищення рівня їх безпеки.

З таблиці 2.7 видно, що в першу чергу увагу варто звернути на потік даних “навчальний заклад – брокер даних – зовнішня платформа зі зберіганням даних 3”, адже оцінка його небезпеки є найвищою та суттєво переважає оцінки інших потоків. Що означає, що потоки даних за участю брокера даних вимагають більш уважного та обережного застосування.

Крім того, помітно, що потоки даних які передбачають етап збереження даних у базі даних зовнішнього споживача даних “навчальний заклад – зовнішня платформа зі зберіганням даних” 1 та “навчальний заклад – зовнішня платформа зі зберіганням даних 2” є суттєво небезпечними відносно таких же, але без збереження даних “навчальний заклад – проста зовнішня платформа 1” та “навчальний заклад – проста зовнішня платформа 2”. Що показує важливість відсутності збереження персональних даних користувачів у сховищах сторонніх сервісів в контексті підвищення рівня захищеності навчального процесу.

Також варто зауважити, що сумарна оцінка небезпеки етапів потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 1” дорівнює 0,12 (табл. 2.2) та є меншою за “навчальний заклад – зовнішня платформа зі зберіганням даних 2” яка рівна 0,15 (табл. 2.3). Важливо також, що кількість етапів цих потоків співпадає, адже вони одного типу. Але оцінка небезпеки самого потоку даних “навчальний заклад – зовнішня платформа зі зберіганням даних 1” дорівнює 0,0024 та є більшою за “навчальний заклад – зовнішня платформа зі зберіганням даних 2” яка рівна 0,0015 (табл. 2.6). Причиною цього є те, що хоч і кількість даних у цих потоках співпадає, але інтенсивність потоків відрізняється. Якщо інтенсивність потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 1” дорівнює 0,2, то інтенсивність потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 2” є меншою і дорівнює 0,1. Що вказує на важливість параметра інтенсивності потоку даних. Адже навіть якщо сумарна небезпека витоку персональних даних на етапах певного потоку даних є вищою відносно інших потоків, це може не мати суттєвого значення та знизити його пріоритет з точки зору застосування заходів по підвищенню рівня безпеки інформаційної взаємодії за умови низької частоти його використання.

Схожа ситуація спостерігається з потоками даних “навчальний заклад – зовнішня платформа зі зберіганням даних 1” та “навчальний заклад – зовнішня платформа зі зберіганням даних 2”. Ці два потоки є одного типу і мають однакову кількість етапів. Також інтенсивність цих потоків однакова. І хоч сумарна оцінка небезпеки усіх етапів потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 1” дорівнює 0,36 (табл. 2.4) та є меншою за оцінку “навчальний заклад – зовнішня платформа зі зберіганням даних 2” яка рівна 0,46 (табл. 2.5), загальна оцінка небезпеки цих потоків показує протилежний результат. Адже оцінка небезпеки потоку даних “навчальний заклад – зовнішня платформа зі зберіганням даних 1” рівна 0,0216 і є більшою за оцінку небезпеки потоку “навчальний заклад – зовнішня платформа зі зберіганням даних 2” яка рівна 0,0184. У цьому випадку зіграла роль відносна оцінка середньої кількості даних які проходять через потік даних (табл. 2.6). Для потоку “навчальний

заклад – зовнішня платформа зі зберіганням даних 1” вона рівна 0,3, а для “навчальний заклад – зовнішня платформа зі зберіганням даних 2” – 0,2. Що демонструє важливість не лише інтенсивності потоків даних, але і кількості даних, які проходять через ці потоки.

Розрахунки у прикладі вище демонструють, що розроблена модель не лише достовірно описує та поділяє на типи інформаційні взаємодії навчального закладу у діджиталізованій освітній сфері, а також враховує більшість важливих факторів, які впливають на рівень безпеки інформаційної взаємодії такі як: інтенсивність потоків даних, кількість даних у цих потоках та інші. Застосування моделі на практиці показало що вона працює і є корисною з точки зору управління потоками даних у діджиталізованій освітній сфері.

2.1.4 Точки контролю потоків персональних даних діджиталізованої освітньої сфери

Відповідно до розробленої моделі інформаційних потоків та інформаційних взаємодій у діджиталізованій освітній сфері виокремлено наступні об’єкти:

1. Освітній заклад – основне джерело, сховище та процесор персональної інформації осіб залучених у навчальному процесі. Складається з наступних частин:

1.1. Внутрішнє сховище персональних даних – місце де зберігається вся наявна інформація пов’язана з навчальним процесом кожного залученого у ній. Таке сховище є внутрішнім і доступ до нього напряму не повинен здійснюватися жодним зовнішнім споживачем інформації.

1.2. Внутрішня інформаційна менеджмент система – головний інструмент роботи з інформацією у навчальному закладі, рівні доступу до даних повинні бути чітко регламентовані, а дії виконувані за допомогою інструменту повинні моніторитись для внутрішнього регулярного аудиту.

1.3. Інтерфейс взаємодії з зовнішніми учасниками обміну даними – сервіс, який забезпечує авторизоване поширення та отримання даних з зовнішніми системами. Саме цей сервіс є найвразливішим місцем і повинен мати на своєму озброєнні найсучасніші інформаційні технології захисту даних.

2. Зовнішні інформаційні платформи – платформи, які надають послуги у сфері освіти, певним чином опрацьовуючи чи трансформуючи отриману інформацію не зберігаючи її у себе. Таких платформ є досить мало, але саме вони є найбільш безпечними в інформаційній взаємодії, адже не зберігають копії отриманих персональних даних у себе.

3. Зовнішні інформаційні платформи зі збереженням даних – платформи які не лише надають незначні послуги у сфері освіти як попередній варіант, а й пропонують певний навчальний продукт, який тим чи іншим чином покращує ефективність навчання або взагалі частково або повністю забезпечує його. Такі платформи зазвичай зберігають персональні дані у своїх базах даних, адже це є необхідним для збереження проміжних результатів здобувачів освіти або надання послуг пов’язаних з навчальним процесом. Такий варіант зовнішніх інформаційних платформ є переважаючим.

4. Зовнішні сховища даних – іноді певну інформацію є сенс і необхідність зберігати у фізично віддаленому місці як то хмарні сховища, такі сховища забезпечують високу ефективність, комфорт та варіативність доступу до даних, але можуть мати менш строгі політики захисту даних ніж внутрішні локальні сховища даних.

5. Брокер даних – це системи, які забезпечують можливість обміну інформацією з найрізноманітнішими зовнішніми діджитал платформами. У сучасному світі майже неможливо обійтись без їх послуг, адже кожна платформа має свій формат даних та інтерфейс роботи з ними й саме брокери даних забезпечують можливість інтеграції навчального закладу з більшістю зовнішніх навчальних платформ. Оскільки брокер даних не лише споживає і зберігає персональну інформацію здобувачів освіти та

інших учасників даних, а й поширює її третім сторонам, то варіантів для витоку персональних даних з’являється набагато більше.

Для визначення найбільш вразливих точок до витоку персональних даних розраховано оцінку небезпеки витоку таких даних для кожного типу потоків даних за участю вище описаних об’єктів. Розрахунки зроблено базуючись на розробленій моделі потоків даних та інформаційних взаємодій у діджиталізованій освітній сфері. Оскільки потрібно отримати загальне розуміння ситуації, а не зробити розрахунки для конкретної організації, то значення параметрів формули *(2.2)* замінено умовними позначеннями та введено умови рівності. Вважається що:

- вразливість до витоку персональних даних на усіх етапах усіх потоків даних рівна і дорівнює *a*;
- співвідношення кількості персональних даних до кількості усіх даних на кожному етапі кожного потоку даних рівна і дорівнює *b*;
- кількість даних на кожному етапі кожного потоку даних є рівною і дорівнює *c*;
- інтенсивність усіх потоків даних рівна і дорівнює *d*;

Результати розрахунків показано в таблиці 2.8.

Таблиця 2.8. Оцінки небезпеки витоку персональних даних кожного типу потоків даних

№	Потік даних	Етапи які проходять дані	Оцінка небезпеки потоку (*DP*)
1	Навчальний заклад – Проста зовнішня платформа	Передача даних, обробка даних. (2)	*cd*2ab*
2	Навчальний заклад – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних. (3)	*cd*3ab*

3	Навчальний заклад – Сховище даних	Передача даних, збереження даних. (2)	*cd*2ab*
4	Навчальний заклад – Брокер даних – Проста зовнішня платформа	Передача даних, обробка даних, збереження даних, передача даних, обробка даних. (5)	*cd*5ab*
5	Навчальний заклад – Брокер даних – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних, передача даних, обробка даних, збереження даних. (6)	*cd*6ab*
6	Навчальний заклад – Брокер даних – Сховище даних	Передача даних, обробка даних, збереження даних, передача даних, збереження даних. (5)	*cd*5ab*

З розрахунків видно, що найвищі оцінки мають потоки даних у яких застосовується брокер даних. Відповідно найвищий пріоритет в контексті визначення точок контролю має об’єкт брокер даних.

Також на основі отриманих даних і моделі потоків даних та інформаційних взаємодій у діджиталізованій освітній сфері визначено точки контролю витоків персональних даних в інформаційних потоках та взаємодіях (рис. 2.3) [8]. Крім того, особлива увага була приділена саме брокеру даних.

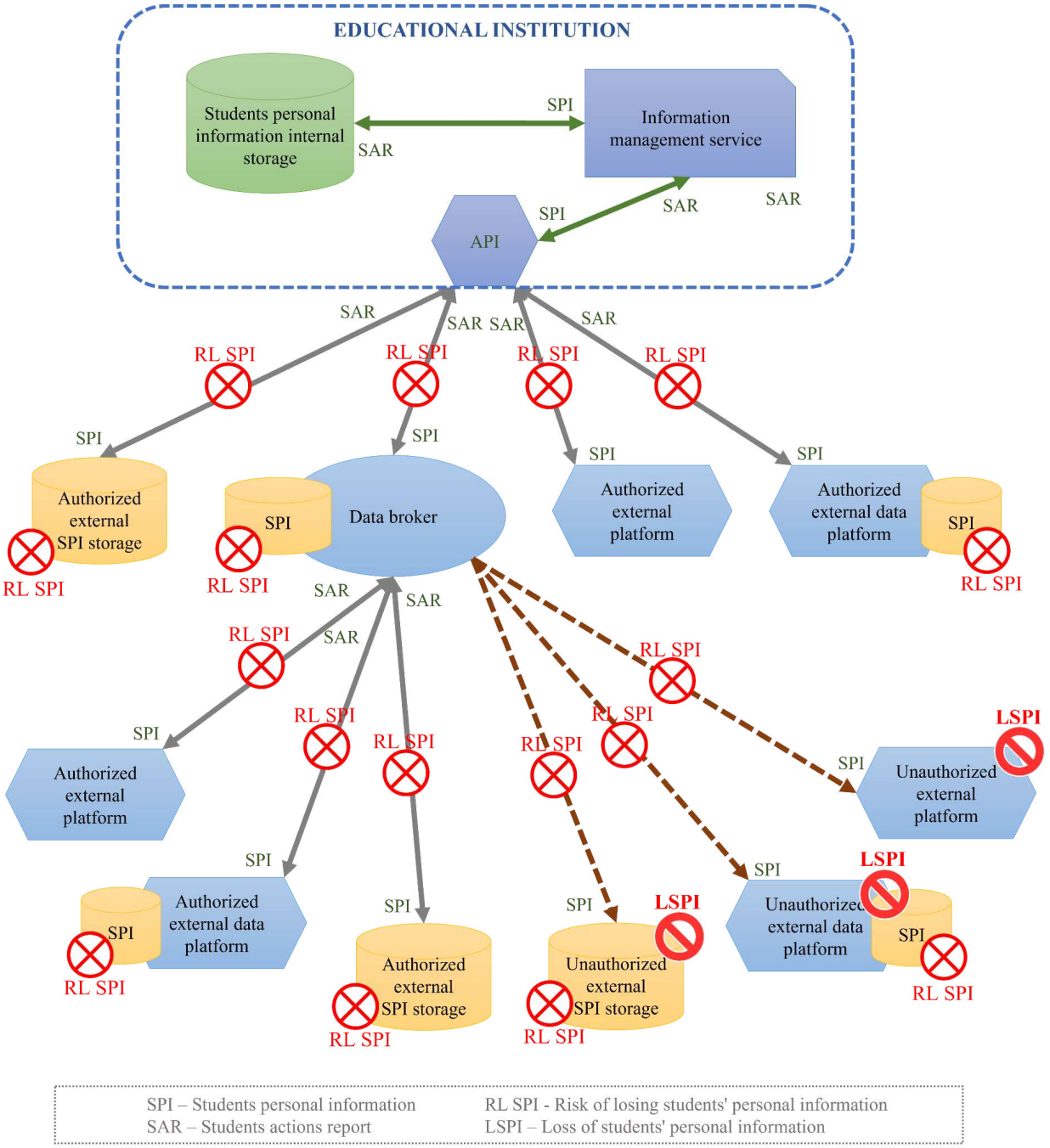

Рис. 2.3. Схематична модель визначення можливих точок витоку персональних даних при інформаційній взаємодії у сфері освіти

У цій моделі основна увага сфокусована на обміні даними освітнього середовища з використанням брокера даних. Адже його було виділено раніше як головний об’єкт з точки зору підвищення небезпеки витоку персональних даних при інформаційній взаємодії. Крім того, брокер даних є найбільш значущим об’єктом при інформаційній

інтеграції навчального закладу та більшості зовнішніх діджитал сервісів у навчальному середовищі. Як видно на моделі крім раніше визначених типів потоків даних присутні додаткові. А саме потоки даних до неавторизованих зовнішніх споживачів, це стає можливим, саме завдяки застосуванню брокера даних.

Розглянуто кожен з об’єктів моделі, зазначаючи чи присутні ризики витоку персональних даних при взаємодії з кожним з них.

1. Освітній заклад – власник прав на збереження та розповсюдження персональних даних. Містить в собі:

1.1. Внутрішнє сховище персональних даних – оскільки таке сховище є внутрішнім і доступ до нього напряму не повинен здійснюватися жодним зовнішнім споживачем інформації, то і ризики витоку персональних даних студентів тут мінімальні або взагалі відсутні у порівнянні з іншими складовими глобального процесу обміну персональними даними в освітньому середовищі.

1.2. Внутрішня інформаційна менеджмент система – також внутрішня складова навчальної цифрової системи. Стосовно неї повинні виконуватись наступні умови: рівні доступу до нього є чітко регламентовані; дії виконувані за його допомогою зберігаються для внутрішнього регулярного аудиту; аудит відповідно проводиться по певному графіку з дотриманням необхідних процедур. У такому випадку ризики витоку персональних даних учасників навчального процесу так як і для попереднього пункту є незначними.

1.3. Інтерфейс взаємодії з зовнішніми учасниками обміну інформацією – оскільки це сервіс, який забезпечує поширення та прийняття персональної інформації з зовнішніми системами. Саме тут починається зона підвищеної ймовірності витоку персональної інформації.

2. Зовнішні інформаційні платформи – хоча такі платформи є найбільш безпечними в інформаційній взаємодії, адже не зберігають копії отриманих персональних даних у себе. Існує ризик витоку персональних даних при передачі їх від навчального закладу до зовнішньої навчальної платформи.

3. Зовнішні інформаційні платформи зі збереженням даних – оскільки такі платформи зазвичай зберігають персональні дані у своїх базах даних, то тут є два джерела ризиків витоку персональних даних. Як і для звичайних навчальних платформ присутній ризик витоку даних при передачі. Також ризик витоку персональних даних безпосередньо з локальної бази даних зовнішньої навчальної платформи. Адже такі платформи не звітують перед навчальними закладами про дотримання необхідних рівнів захисту інформації та не зобов'язані забезпечувати такий максимальний захист своїх баз даних. Тут усе залежить від професіоналізму команди, яка підтримує даний проєкт та відповідальності людей які мають безпосередній доступ до персональних даних користувачів навчальних закладів.

4. Зовнішні сховища даних – тут, як і у попередньому випадку, є два джерела ризиків витоку персональних даних. Витік даних може статись як під час передачі, так і сховища можуть мати менш строгі політики захисту даних ніж внутрішні локальні сховища даних, що може призвести до витоку інформації безпосередньо з самої віддаленої бази даних.

5. Брокер даних – оскільки у сучасному світі майже неможливо обійтись без послуг таких інформаційних технологій, цей випадок потрібно розглянути більш детально. Як зазначалось, брокер даних не лише споживає, а часто і зберігає персональну інформацію студентів та інших учасників даних для її подальшої трансформації та поширення, то тут варіантів для витоку персональних даних з'являється набагато більше.

Виокремлено такі ризики:

- ризики на етапі передачі даних від навчального закладу і збереження їх у локальній базі даних брокера. Тобто є ризик витоку персональних даних на етапі їх транспортування до сховищ брокера даних.
- ризик витоку інформації з локальної бази даних брокера.
- ризики витоку даних, які з'являються на другому етапі взаємодії навчального закладу та брокера даних – на етапі поширення персональних даних

учасників навчального процесу брокером даних з третіми сторонами. Тобто з такими ж системами як ми уже розглядали раніше, а також особливі випадки притаманні такій взаємодії:

5.1. Зовнішні інформаційні платформи – тут існує ризик витоку персональних даних при передачі їх від брокера даних до самої зовнішньої навчальної платформи.

5.2. Зовнішні інформаційні платформи зі збереженням даних – випадок майже не відрізняється від прямої передачі даних від навчального закладу, відмінність лише у тому, що тут джерелом даних виступає брокер даних. Тобто як і для звичайних навчальних платформ присутній ризик витоку даних при передачі. Але також додається ризик витоку персональних даних безпосередньо з локальної бази даних зовнішньої навчальної платформи.

5.3. Зовнішні сховища даних – знову ж таки, витік персональних даних користувачів може статись під час передачі даних. Також і самі зовнішні сховища можуть мати менш строгі політики захисту даних, що може призвести до витоку інформації безпосередньо з самої віддаленої бази даних.

5.4. Оскільки джерелом даних виступає не освітній заклад напряму, а саме брокер даних, то з’являється ризик поширення інформації зі споживачами які не є авторизовані отримувати доступ до таких даних самим навчальним закладом. Тут причиною таких неавторизованих потоків даних може стати як звичайний людський фактор, на кшталт непорозуміння у комунікації між представниками освітніх закладів і командою брокера даних, так і технічні виняткові ситуації.

Варто підкреслити ще раз той факт що розповсюджувачем персональної інформації у даному випадку є не сам освітній заклад, а брокер даних. Звідси похідним ризиком є те, що представники освітнього закладу не завжди можуть мати прямий контроль над списком третіх сторін, яким надається доступ до персональної інформації студентів навчального закладу.

Також зазначимо, що такі сервіси є більш цікавою ціллю для зловмисників, які полюють на персональні дані студентів, ніж поодинокі зовнішні навчальні платформи.

Адже вони можуть агрегувати у своїх сховищах дані мільйонів студентів, сотень і навіть тисяч навчальних закладів з різних куточків світу.

2.2 Модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища

Провівши аналіз потоків даних при інформаційній взаємодії у діджиталізованій освітній сфері, а також визначивши головні точки контролю в управлінні потоками даних, необхідно виявити можливі безпекові ризики, які з'являються при такій інформаційній взаємодії. Як видно з рисунку 2.4 поширення персональних даних третім сторонам, таким як зовнішні навчальні платформи, брокери даних те інші, і є причиною виникнення більшості ризиків витоку персональних даних стейкхолдерів діджиталізованого освітнього середовища [161].

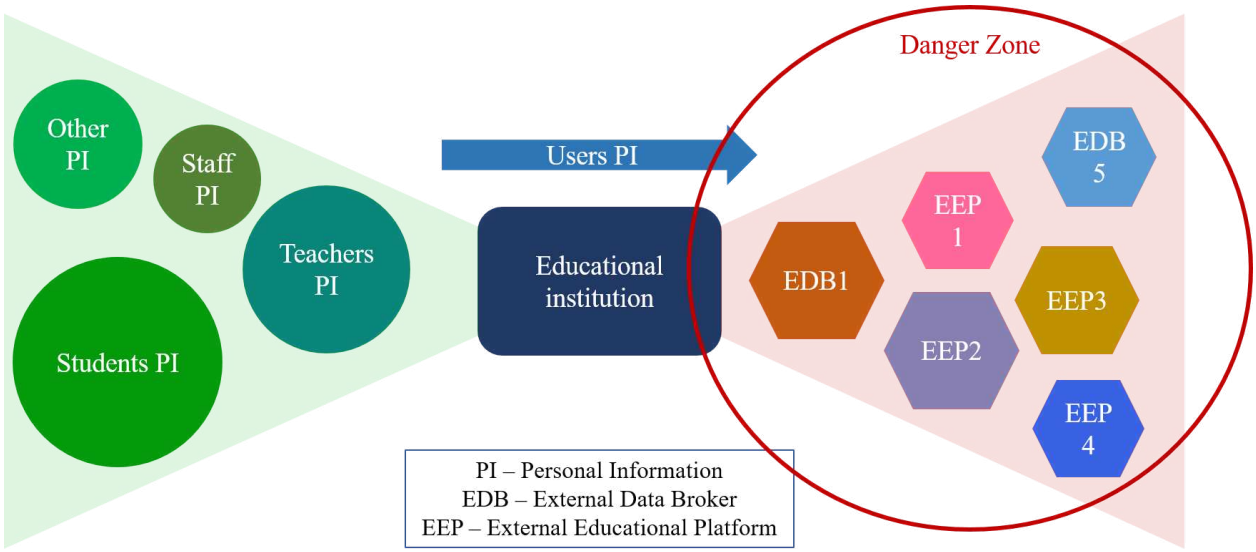

Рис. 2.4. Зона виникнення ризиків витоку персональних даних при інформаційній взаємодії у діджиталізованому освітньому середовищі

Отримавши розуміння найбільш вагомих зон виникнення ризикових ситуацій, які можуть призвести до витоку персональних даних стейкхолдерів діджиталізованого освітнього середовища, потрібно провести ідентифікацію ризиків витоку персональних даних.

Після проведення аналізу існуючих напрацювань у цьому напрямку виділено роботу Корченко О. Г., Дрейс Ю. О. та Лозова І. Л. “Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах” [162]. Автори оперують наступними характеристиками: характеристика персональних даних (ідентифікація їх складу та змісту), характеристика середовища обробки баз персональних даних в автоматизованій системі, мета обробки персональних даних, аудит застосованих механізмів безпеки, характеристика існуючих функціональних послуг безпеки, ідентифікація загроз безпеці таких даних при обробці баз, величина можливих збитків від втрати персональних даних, оцінка ризику захисту персональних даних, а також керування ризиком та досягнення необхідного рівня гарантій захисту. Загалом метод дає чіткий опис персональних даних та дозволяє врахувати багато аспектів для оцінки ризиків. Але є кілька особливостей які не дають змоги його напряму застосувати у поточній ситуації. По-перше, метод є доволі загальним, тобто є потреба розробки чогось більш спеціалізованого під освітню сферу. По-друге, носієм персональних даних виступає документ, тоді як при інформаційній взаємодії інформація поширюється та зберігається в потоках даних. І останнє, розглянутий метод описує ситуації пов’язані з такими середовищами обробки даних як: «MS Word», «MS Excel», «MS Access» та інші, тоді як дані у потоках даних діджиталізованої освіти обробляються зовнішніми навчальними платформами такими як: LMS, SIS тощо.

Зважаючи на це, розроблено власну модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища беручи до уваги згадані раніше напрацювання.

У розробленій моделі застосовано підхід, що базується на формуванні групою експертів критеріїв оцінювання та їх вагових коефіцієнтів. Зокрема можна використати метод Дельфі [163]. Основні етапи проведення експертної оцінки можна визначити так:

1. Формування експертних груп – вибір фахівців у конкретній галузі, які володіють необхідними знаннями та досвідом.

2. Перший раунд опитування – експертам висилають запитання, які вони повинні оцінити/відповісти, надаючи свою думку або прогнози.

3. Аналіз відповідей – збір і узагальнення отриманих відповідей. Всі результати анонімні, що дозволяє уникнути домінування окремих думок.

4. Другий та наступні раунди – узагальнені результати й додаткова інформація з першого раунду використовується для повторного опитування експертів. Вони можуть змінити свої оцінки з урахуванням думок групи аби інших груп.

5. Досягнення консенсусу – процес триває кілька раундів до досягнення певного ступеня згоди або стабільності в думках експертів.

6. Фінальний аналіз – оцінка остаточних результатів, їх узагальнення та підготовка висновків.

Для оцінки узгодженості експертів використано коефіцієнт узгодженості Кенделла (W) [164], адже він особливо корисний, коли оцінки мають рангову природу (наприклад, 1-10 для якості, де 1 – погано, а 10 – дуже добре). Коефіцієнт рахується після кожного раунду індивідуального оцінювання і якщо він не задовольняє порогове значення відбувається групове обговорення після чого призначається наступний раунд. Варто зазначити що кількість раундів обмежена. Тобто наступний раунд не призначається якщо коефіцієнт Кенделла (W) більший або рівний 0.7 або кількість раундів вичерпано.

Дуже важливою частиною методу експертної оцінки є формування експертних груп. Сформовано п’ять груп експертів: експерти у галузі освіти, експерти у сфері розробки програмного забезпечення, експерти у сфері захисту даних, менеджери та юристи.

Група експертів в галузі освіти:

- Вища освіта.
- Досвід роботи у закладах освіти різних рівнів або на освітніх платформах не менше 5 років.

- Знання базових методів і технологій управління даними в освітньому процесі та їх захисту.

Група експертів у сфері розробки програмного забезпечення:

- Вища освіта в галузі інформаційних технологій.
- Досвід розробки програмного забезпечення не менше 5 років.
- Володіння сучасними технологіями розробки програмного забезпечення для підтримки та управління базами даних.

Група експертів у сфері захисту даних:

- Вища освіта у сфері захисту інформації та кібербезпеки.
- Досвід роботи у сфері захисту даних не менше 5 років.
- Володіння сучасними технологіями захисту інформації, стандартами безпеки та практичний досвід впровадження захисних протоколів.

Група менеджерів:

- Вища освіта у сферах управління, бізнес-адміністрування або суміжних галузях.
- Досвід управлінської діяльності не менше 5 років.
- Навички проєктного менеджменту, управління ризиками та вміння приймати стратегічні рішення.

Група юристів:

- Вища юридична освіта.
- Досвід роботи у сферах захисту даних, корпоративного права або права в IT-сфері не менше 5 років.

У результаті формування груп експертів отримано наступні усереднені їх характеристики:

Група експертів в галузі освіти:

- Середній вік – 40 років.
- Освіта – магістри та спеціалісти.
- Досвід роботи – 7 років у сфері освіти.

- Додаткові знання та сертифікації – сертифікації у сфері управління даними.

Група експертів у сфері розробки програмного забезпечення:

- Середній вік – 35 років.
- Освіта – бакалаври або магістри.
- Досвід роботи – 6 років, включаючи участь у розробці великих програмних проєктів.
- Додаткові знання та сертифікації – сертифікації з конкретних мов програмування чи технологій.

Група експертів у сфері захисту даних:

- Середній вік – 38 років.
- Досвід роботи – 8 років у розробці та впровадженні стратегій захисту даних.
- Освіта – бакалавр та магістри.
- Додаткові знання та сертифікації – сертифікації на зразок CISSP чи CISM.

Група менеджерів:

- Середній вік – 42 роки.
- Освіта – магістри.
- Досвід роботи – 6-8 років в управлінні проєктами та командами.
- Додаткові знання та сертифікації – сертифікації у сфері управління проєктами.

Група юристів:

- Середній вік – 36 років.
- Освіта – магістри.
- Досвід роботи – 5-7 років у сфері правового захисту інформації, консультування з питань дотримання законодавства.

Після формування груп перше завданням експертів – визначити головні ризикові події витоку персональної інформації стейкхолдерів діджиталізованої освіти. Були визначені наступні критичні ризикові події витоку даних:

- Витік персональних даних при зчитуванні зовнішніми споживачами.
- Витік персональних даних з бази даних сервісів зовнішніх споживачів.
- Несанкціоноване поширення даних зовнішнім споживачем на інші платформи.
- Витік персональних даних через дії персоналу зовнішньої компанії-споживача даних.

На наступному етапі експерти визначили найбільш ймовірні причини виникнення таких ризикових подій:

- Поширення персональних даних третім сторонам.
- Збирання персональної інформації третіми сторонами.
- Низький рівень захисту бази даних.
- Низький рівень підготовки персоналу.
- Відсутність культури роботи з приватними даними персоналу зовнішніх компаній.
- Низький рівень захисту каналів комунікації.
- Зовнішні атаки зловмисників.
- Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту.
- Використання застарілих інформаційних технологій.
- Оренда апаратних потужностей у сумнівних постачальників.
- Використання персональної інформації в цілях зовнішньої платформи (реклама, тестування тощо).

На основі експертного аналізу сформовано відповідність ризикових подій витоку персональних даних та їх ймовірних причин (табл. 2.9).

Таблиця 2.9. Ризикові події витоку персональних даних та їх ймовірні причини

№	Ризикова подія	Ймовірні причини
E1	Витік персональних даних при вичитці	1. Поширення персональних даних третім сторонам (*p1*)

	зовнішніми споживачами	2. Низький рівень захисту каналів комунікації (*p6*) 3. Зовнішні атаки зловмисників (*p7*) 4. Використання застарілих інформаційних технологій (*p9*)
E2	Витік персональних даних з бази даних навчальних систем зовнішніх споживачів	1. Поширення персональних даних третім сторонам (*p1*) 2. Збирання персональної інформації третіми сторонами (*p2*) 3. Низький рівень захисту бази даних (*p3*) 4. Низький рівень підготовки персоналу (*p4*) 5. Відсутність культури роботи з приватними даними персоналу зовнішніх компаній (*p5*) 6. Зовнішні атаки зловмисників (*p7*) 7. Використання застарілих інформаційних технологій (*p9*) 8. Оренда апаратних потужностей у сумнівних постачальників (*p10*)
E3	Несанкціоноване поширення даних зовнішнім споживачем з іншим платформами	1. Поширення персональних даних третім сторонам (*p1*) 2. Збирання персональної інформації третіми сторонами (*p2*) 3. Низький рівень підготовки персоналу (*p4*) 4. Відсутність культури роботи з приватними даними персоналу зовнішніх компаній (*p5*) 5. Використання персональної інформації в цілях зовнішньої платформи (реклама, тестування тощо) (*p11*)

		6. Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту (*p8*)
E4	Витік персональних даних через дії персоналу зовнішньої компанії-споживача даних	1. Поширення персональних даних третім сторонам(*p1*) 2. Збирання персональної інформації третіми сторонами (*p2*) 3. Низький рівень підготовки персоналу (*p4*) 4. Зовнішні атаки зловмисників (*p7*) 5. Відсутність культури роботи з приватними даними персоналу зовнішніх компаній (*p5*) 6. Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту (*p8*)

Експерти встановили ймовірність виникнення кожної з подій в системі оцінок від 0 до 10, де 0 – неможлива подія, 10 – гарантована подія. Також експертами була встановлена оцінка серйозності наслідків кожної з ризикових подій витоку персональних даних (від 0 до 10, де 0 – наслідків немає, 10 – наслідки максимально критичні). Ці оцінки зведені у табл. 2.10.

Таблиця 2.10. Експертна оцінка ризикових подій витоку персональних даних та їх наслідків

№	Ризикова подія	Можливі наслідки	*Ve* - ймовірність виникнення ризикової події (1-10)	*Re* - серйозність наслідків виникнення ризикової події (1-10)

E1	Витік персональних даних при вичитці зовнішніми споживачами	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – низька ймовірність. Витік усіх персональних даних усіх клієнтів – низька ймовірність.	2	4
E2	Витік персональних даних з бази даних навчальних систем зовнішніх споживачів	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних усіх клієнтів – висока ймовірність.	3	10
E3	Несанкціоноване поширення даних зовнішнім	Витік частини персональних даних	1	6

	споживачем з іншим платформами	деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – середня ймовірність. Витік усіх персональних даних усіх клієнтів – низька ймовірність.		
E4	Витік персональних даних через дії персоналу зовнішньої компанії-споживача даних	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – низька ймовірність. Витік усіх персональних даних усіх клієнтів – висока низька.	7	5

Наступне завдання експертів полягало у визначенні загальної оцінки кожної з причин настання ризикових подій на основі ціннісного підходу [1]. Цей підхід дозволяє експертам на основі власного професійного досвіду врахувати не лише ймовірність виникнення конкретних ризикових ситуацій та їх наслідків, а й інші додаткові фактори (табл. 2.11).

Таблиця 2.11. Ціннісні оцінки причин настання ризикових подій

№	Причина ризикових подій	*Ce* - Оцінка (1-10)
p1	Поширення персональних даних третім сторонам	10
p2	Збирання персональної інформації третіми сторонами	9
p3	Низький рівень захисту бази даних	8
p4	Низький рівень підготовки персоналу	8
p5	Відсутність культури роботи з приватними даними персоналу зовнішніх компаній	7
p6	Низький рівень захисту каналів комунікації	8
p7	Зовнішні атаки зловмисників	7
p8	Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту	5
p9	Використання застарілих інформаційних технологій	6
p10	Оренда апаратних потужностей у сумнівних постачальників	1
p11	Використання персональної інформації в цілях зовнішньої платформи (реклама, тестування тощо)	2

На основі введених оцінок ризикових подій та їх причин вводиться в розгляд числова характеристика ваги причини виникнення ризикової події витоку персональних даних MP_j (*2.4*):

$$MP_j = \sum_{i=1}^{4} (Ve_i * Re_i) + ACe_j, j = 1, 2, \ldots, 11, \quad (2.4)$$

де Ve_i – імовірність настанні ризикової події;

Re_i – серйозність наслідків настання ризикової причини;

Ce_j – ціннісна оцінка причини виникнення ризикової події визначена експертами.

A – коефіцієнт приведення величини ціннісної оцінки причини виникнення ризикової події Ce_j до загального впливу ризикової події та серйозності її наслідків, який визначається наступним чином:

$$A = \frac{\sum_{j=1}^{11}(\sum_{i=1}^{4}(Ve_i * Re_i))}{\sum_{j=1}^{11} Ce_j} \qquad (2.5)$$

Такий вибір коефіцієнта приведення A дозволяє зменшити переважаючий вплив ціннісних оцінок причин Ce_j у порівнянні із загальним впливом ризикових подій та серйозності її наслідків $Ve_i * Re_i$.

При цьому всі величини Ve_i, Re_i, Ce_j використовуються нормалізованими.

Застосувавши формулу *2.5,* обчислено значення коефіцієнта $A = 0.72$.

Таким чином для даних згідно з таблицями 2.3, 2.4, 2.5 та матрицею *MX*, матриця ваг причин ризикових подій *MP* матиме наступний вигляд:

$$MP = (1.51\ \ 1.36\ \ 0.88\ \ 1.29\ \ 1.21\ \ 0.66\ \ 1.23\ \ 0.71\ \ 0.81\ \ 0.37\ \ 0.2)$$

Результати виконання усіх необхідних підрахунків за описаними вище формулами виражено у таблиці (табл. 2.12).

Таблиця 2.12. Причини ризикових подій та їх вагова оцінка

№	Назва причини	Вага
1	Поширення персональних даних третім сторонам	1.51
2	Збирання та зберігання персональної інформації третіми сторонами	1.36
3	Низький рівень захисту бази даних	0.88

4	Низький рівень підготовки персоналу	1.29
5	Відсутність культури роботи з приватними даними персоналу зовнішніх компаній	1.21
6	Низький рівень захисту каналів комунікації	0.66
7	Зовнішні атаки зловмисників	1.23
8	Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту	0.71
9	Використання застарілих інформаційних технологій	0.81
10	Оренда апаратних потужностей у сумнівних постачальників	0.37
11	Використання персональної інформації в цілях зовнішньої платформи (реклама, тестування тощо)	0.2

З таблиці 2.12 видно, що є кілька причин ризикових ситуацій які мають велику вагу відносно інших. Тож найсуттєвішими причинами є такі:

1. Поширення персональних даних третім сторонам.
2. Збирання та зберігання персональної інформації третіми сторонами.
3. Відсутність культури роботи з приватними даними персоналу зовнішніх компаній.
4. Низький рівень підготовки персоналу.
5. Зовнішні атаки зловмисників.

Також видно, що очевидною першопричиною виникнення ризикових ситуацій витоку персональної інформації стейкхолдерів діджиталізованого навчального простору є те, що такі дані поширюються з третіми сторонами, тобто зовнішніми навчальними платформами та брокерами даних.

Крім того, експертами окремо виділено застосування хмарних технологій. Підкреслено, що особливу увагу також варто звернути на те, що багато сервісів

розміщується в хмарах. При зберіганні даних не в локальній мережі, а в хмарі можуть бути присутні додаткові фактори.

2.3 Принципи мінімізації поширення персональних даних в умовах діджиталізації освітньої сфери

Провівши аналіз ризиків, встановлено, що головною причиною виникнення ризику витоку персональних даних стейкхолдерів навчального процесу є поширення таких даних. Отже, для підвищення рівня захищеності освітнього процесу потрібно знизити вплив цього фактору. Звідси виникає правило, що для ефективного обміну інформацією повинна задовольнятись умова поширення лише мінімально необхідної інформації. Що за собою тягне і мінімізацію поширення персональних даних.

Розробка і впровадження принципів мінімізації поширення персональних даних є важливим кроком до безпечної та відповідальної діджиталізації освітньої сфери, що забезпечує збереження конфіденційності та довіри у цифровому середовищі. Тож сформуємо принципи мінімізації поширення персональних даних в умовах діджиталізації освітньої сфери:

1) Принцип необхідності:

a. Збір даних для конкретних цілей – установи повинні збирати тільки ті персональні дані, які необхідні для досягнення конкретно визначених освітніх чи адміністративних цілей. Наприклад, для ведення навчального процесу можна збирати інформацію про академічні результати, але не обов'язково інформацію про особисте життя студента.

b. Регулярний перегляд даних: потрібно постійно переглядати й аналізувати дані, що зберігаються, щоб визначити, які з них більше не є необхідними й можуть бути безпечно видалені.

2) Принцип обмеження мети:

a. Чітке формулювання мети збору – доцільно чітко визначити та довести до відома всіх учасників, навіщо збираються дані. Для кожного типу даних має бути визначена конкретна мета.

b. Використання тільки за призначенням – заборонено використовувати дані для цілей, відмінних від тих, для яких вони були зібрані, без згоди суб'єктів даних.

3) Принцип обмеженого доступу:

a. Контроль доступу – доступ до даних повинен бути обмежений лише тими особами, хто безпосередньо потребує їх для виконання своїх обов’язків, наприклад, адміністраторами системи чи безпосередніми викладачами.

b. Системи управління доступом – впроваджувати системи контролю і звітності доступу, щоб стежити за тим, хто і коли отримує доступ до певних даних.

4) Принцип анонімізації та псевдонімізації:

a. Анонімізація даних – це процес трансформації даних таким чином, щоб ідентифікувати окремих осіб в них було неможливо. Це знижує ризик розкриття ідентичності при обробці великих масивів даних.

b. Псевдонімізація – замість справжніх даних використовуйте псевдоніми, тобто замінники реальних даних, щоб тільки авторизовані особи могли реконструювати початкові дані.

5) Принцип обмеження зберігання:

a. Визначення терміну зберігання – дані повинні зберігатися тільки так довго, як це необхідно для досягнення визначених цілей. Після цього вони повинні бути видалені відповідно до політики знищення даних.

b. Своєчасне видалення – автоматизуйте процеси видалення даних, які більше не використовуються, щоб запобігти зберіганню застарілої або непотрібної інформації.

6) Прозорість і підзвітність:

a. Документування процесів – усі процедури збору, зберігання й обробки даних повинні бути чітко задокументовані, щоб показати, як і чому дані використовуються.

b. Інформування суб'єктів – регулярно інформувати суб’єктів даних (студентів, співробітників) про їхні права і про те, як їхні дані будуть використовуватися.

7) Освіта та підвищення обізнаності:

a. Навчання персоналу – потрібно забезпечити регулярне навчання для співробітників освітньої установи щодо безпечного та відповідального використання й обробки персональних даних.

b. Формування культури обережності – необхідно сприяти створенню культури, де всі учасники усвідомлюють важливість захисту даних і активно беруть участь у підтримці політики безпеки.

Впровадження цих принципів дозволить значно знизити ризики, пов’язані з поширенням персональних даних, і сприятиме підвищенню рівня довіри до освітніх установ в цифрову епоху. Надійне управління персональними даними не лише забезпечує дотримання регуляторних вимог, але й зміцнює імідж установи, підвищуючи довіру студентів, батьків і співробітників.

2.4 Модель управління зберіганням потоків даних освітнього середовища

У попередніх розділах роботи розглянуто основні причини витоку інформації в освітньому середовищі. Виділено що деякі з них пов’язані з використанням хмарних технологій у сфері збереження та управління даними [127]. Одним з головних занепокоєнь є безпека даних, оскільки перенесення інформації на хмарні платформи може збільшити ризик несанкціонованого доступу і втрати конфіденційності. Однак, незважаючи на ці побоювання, сьогодні більшість сервісів обирають розміщення у хмарному середовищі.

Ця тенденція спостерігається і в секторі освіти, де діджитал системи управління даними навчальних закладів активно використовують хмарні платформи. Популярність цього підходу зумовлена декількома вагомими причинами. По-перше, використання

хмарних сервісів звільняє заклади від необхідності підтримки власних, часто дорогих, локальних обчислювальних ресурсів. Це значно скорочує витрати на апаратне забезпечення та технічну підтримку. По-друге, хмарні системи забезпечують можливість гнучкого масштабування, дозволяючи збільшувати або зменшувати обчислювальні можливості відповідно до змін потреб або завантаженості системи.

Враховуючи ці фактори, виникає питання оптимального визначення моменту, коли перехід на хмарні технології стає не лише бажаним, але й економічно й операційно обґрунтованим. Для цього розроблено спеціальну модель (рис. 2.5), призначену для оцінки необхідності переходу діджитал менеджмент системи навчального закладу на хмарні потужності [9]. Ця модель базується на використанні алгоритмів прогнозування, які дозволяють передбачити майбутні потреби в апаратному забезпеченні. Таким чином, навчальні заклади можуть більш усвідомлено підходити до рішення про перехід на хмарні технології, зважуючи всі можливі вигоди та ризики.

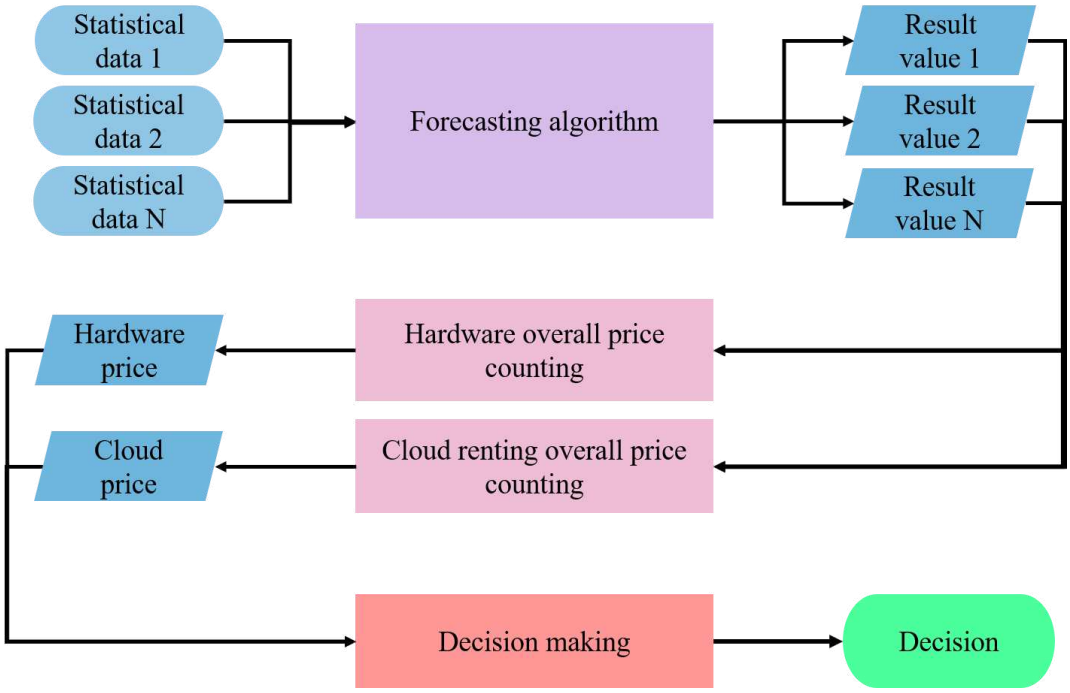

Рис. 2.5. Модель управління зберіганням потоків даних освітнього середовища [9]

Розроблена модель передбачає наявність певних вхідних даних та кількох рівнів отримання проміжних результатів та їх повторної обробки. Елементи розробленої моделі включають:

- Статистичні дані використання потужностей існуючою діджитал системою менеджменту даних навчального закладу. Тут важливими є наступні показники: відсоток використання процесора; відсоток використання оперативної пам’яті; чи були сповіщення про підвищене навантаження на систему, якщо були, то їх кількість; відсоток використаної постійної пам’яті, завантаженість мережі тощо.
- Алгоритм прогнозування необхідних потужностей у майбутньому. Тут використовуються саме дані про відсоток завантаженості процесора, оперативної пам’яті та постійної пам’яті.
- Результати прогнозування по введених статистичних показниках.
- Обчислення вартості забезпечення локального апаратного забезпечення. Базуватись потрібно на середній ціні сервера за визначеними параметрами. Крім того, варто врахувати інформацію про попередження системи про високий рівень завантаженості.
- Обчислення вартості оренди хмарних потужностей. До уваги, як і в попередньому пункті беруться результуючі показники та на їх основі підбираються наближені до оптимальних варіанти на ринку. Важливо хмарні потужності орендувати у постачальника з хорошою репутацією, але потрібно тримати баланс і не переплачувати за розрекламовані рішення.
- Ціна необхідного апаратного забезпечення.
- Ціна оренди хмарних потужностей.
- Прийняття рішення про перехід на хмарні потужності. Застосування отриманих даних щодо цін, а також додаткових параметрів для прийняття рішення.
- Рекомендація щодо рішення про перехід на хмарні потужності.

Для застосування моделі розроблено алгоритм, який пояснює послідовність кроків, вхідні та вихідні дані на кожному етапі:

1) Статистичні дані. Потрібно зібрати статистичні дані про використання потужностей необхідних для функціонування діджитал системою менеджменту даних навчального закладу. Має сенс робити поділ по місяцях. Тобто визначити узагальнене значення за місяць. Період охоплення статистичних даних повинен бути як мінімум за останні кілька років. Це мають бути такі показники: розмір використаної оперативної пам'яті, відсоток завантаженості процесора, трафік (вхідний та вихідний), кількість інтеграцій, кількість активних користувачів, розмір бази даних або кількість використаної постійної пам'яті та кількість нотифікацій про високе завантаження системи.

2) Зібравши потрібні статистичні дані, потрібно застосувати комбінований алгоритм прогнозування. Кроки такого алгоритму:

- Моделювання – додавання предикторів, потрібно використати попередні значення самого ряду рік і місяць.
- Вибір моделей прогнозування. Потрібно застосувати кілька різних підходів до прогнозування, для цього запропоновано вибрати декілька моделей з перерахованих нижче:

❖ ARIMA (AutoRegressive Integrated Moving Average) – популярна модель для аналізу та прогнозування часових рядів. Вона використовується для виявлення та моделювання залежностей у даних, які мають тенденції або сезонні коливання. Модель ARIMA визначається трьома основними параметрами [165]:

p — порядок авторегресії (AR);

d — порядок інтеграції (I);

q — порядок ковзного середнього (MA).

Формально, ARIMA модель можна представити так [166]:

$$Y_t = c + \phi_1 Y_{t-1} + \phi_2 Y_{t-2} + \ldots$$
$$\ldots + \phi_p Y_{t-p} + \theta_1 \epsilon_{t-1} + \theta_2 \epsilon_{t-2} + \ldots + \theta_q \epsilon_{t-p} + \epsilon_t \qquad (2.6)$$

де Y_t – значення часового ряду в момент часу *t*;

c – константа;

ϕ – коефіцієнти авторегресії;

θ – коефіцієнти ковзного середнього;

ϵ_t – похибка (залишок) в момент часу t.

❖ Експоненційне зважування (Exponential Weighting) – метод, що використовується для надання різним спостереженням в часових рядах змінних ваг, зосереджуючи увагу на більше недавніх даних. Цей підхід дозволяє отримувати більш обґрунтовані прогнози, оскільки свіжі дані зазвичай є більш релевантними.

Основні принципи експоненційного зважування наступні: в експоненційному зважуванні найближчі спостереження отримують більшу вагу, а старіші — меншу; вага кожного спостереження зменшується експоненціально з плином часу; параметр α (діапазон від 0 до 1) визначає, наскільки швидко зменшуються ваги; чим ближче α до 1, тим більше значення зосереджуються на останніх спостереженнях; якщо α = 0.5, то надається однакова вага кожному другому спостереженню в історії.

Вагове середнє за методом експоненційного зважування можна записати як [167]:

$$S_t = \alpha Y_t + (1 - \alpha) S_{t-1}, \qquad (2.7)$$

де S_t – згладжене значення для часу t;

Y_t – спостережене значення в момент часу t;

S_{t-1} – попереднє згладжене значення;

α – параметр згладжування.

❖ ETS (Exponential Smoothing State Space Model) — це модель для прогнозування часових рядів, яка ґрунтується на методі експоненціального згладжування. Вона використовується для аналізу даних, які мають тенденції та/або сезонні коливання. Модель ETS включає три основні компоненти. Level (середнє значення) – це постійна частина моделі, яка представляє середній рівень часового ряду. Trend (тенденція) – відображає направлення, в якому змінюється середнє значення

даних (зростання, спадання). Модель може включати як адитивну, так і мультиплікативну тенденцію. Seasonality (сезонність) – враховує повторювані коливання даних у конкретні періоди (тижні, місяці тощо). Це також може бути адитивний або мультиплікативний компонент.

Прогнозування за моделлю ETS виконується за допомогою двох рівнянь. Перше – пряме (наступне) прогнозування [166]:

$$Y_{t+h} = l_t + h * b_t + s_{t+h-m*\lfloor (h-1)/m \rfloor}, \quad (2.8)$$

де l_t – рівень на момент часу *t*;

b_t – значення тренду на момент часу *t*;

$s_{t+h-m*\lfloor (h-1)/m \rfloor}$ – сезонний компонент.

Друга частина це оновлення рівнянь. Для рівня, тренду та сезонності використовуються набори рівнянь зі згладжувальними параметрами [166]:

$$l_t = \alpha Y_t + (1 - \alpha)(l_{t-1} + b_{t-1}), \quad (2.9)$$

$$b_t = \beta(l_t - l_{t-1}) + (1 - \beta)b_{t-1}, \quad (2.10)$$

$$s_t = \gamma(Y_t - l_t) + (1 - \gamma)s_{t-m}, \quad (2.11)$$

де α, β та γ – параметри згладжування для рівня, тренду та сезонності відповідно.

❖ XGBoost (Extreme Gradient Boosting) – потужний алгоритм машинного навчання, який базується на методі градієнтного підсилення. Він оптимізує функцію втрат, використовуючи метод градієнтного підсилення. Основна мета полягає в мінімізації такої функції [168]:

$$L(y, x) + \sum_{k=1}^{K} \Omega(f_k), \quad (2.12)$$

де $L(y, x)$ – функція втрат, яка визначає відхилення між справжніми значеннями *y* і прогнозованими *x*;

$\Omega(f_k)$ – регуляризаційний вираз, що контролює складність кожного дерева f_k.

Регуляційний вираз може бути представлений так [168]:

$$\Omega(f_k) = \gamma T + \frac{1}{2}\lambda||\omega||^2, \quad (2.13)$$

де T – кількість листів (вузлів) у дереві;

γ – параметр, що штрафує за кількість листів у дереві;

ω – вектор ваг (коефіцієнтів) дерев;

λ – параметр, що контролює L2-регуляризацію.

❖ Elastic Net – це метод регуляризації, що об'єднує переваги Lasso (L1-регуляризація) і Ridge (L2-регуляризація) для покращення моделей лінійної регресії, особливо при обробці даних з високою розмірністю. Математична формула [169]:

$$ElasticNetLoss = \frac{1}{2n}\sum_{i=1}^{n}(y_i - x_i)^2 + \lambda\left(\sum_{j=1}^{p}\left|\beta_i\right| + (1 + \alpha)\sum_{j=1}^{p}\beta_j^2\right), \quad (2.14)$$

де $\frac{1}{2n}\sum_{i=1}^{n}(y_i - x_i)^2$ – середньоквадратична помилка (MSE), регресійний термін втрати, що вимірює різницю між прогнозованими та фактичними значеннями;

λ – параметр регуляризації, що контролює загальну силу регуляризації;

α – параметр змішування, визначає баланс між регуляризаціями L1 (Lasso) і L2 (Ridge);

$\sum_{j=1}^{p}\left|\beta_i\right|$ – регуляризація L1, яка сприяє зменшенню деяких коефіцієнтів до нуля;

$\sum_{j=1}^{p}\beta_j^2$ – регуляризація L2, компенсує малі коефіцієнти.

- Далі виконується формування тестової та навчальної вибірки даних по кожному ряду даних.
- До кожного часового ряду потрібно виконати побудову кожної вибраної з переліку вище математичної моделі.
- Застосовуємо побудовані моделі до тестових вибірок.

- Оцінюється та обирається краща математична модель до кожного часового ряду за метрикою RMSE [170]:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(Y_i - X_i)^2}, \quad (2.15)$$

де n — кількість спостережень;

Y_i – фактичне значення для i-го спостереження;

X_i – прогнозоване значення для i-го спостереження;

$Y_i - X_i$ – помилка (залишок) для i-го спостереження.

Обравши кращу модель по кожному ряду даних, використовується обрана модель до всього часового ряду і будуємо прогноз по рядах на майбутнє.

Після виконання прогнозування буде отримано значення показників необхідних для функціонування системи через в майбутньому.

3) Важливо врахувати додаткові фактори, такі як кількість попереджень про високий рівень завантаженості системи тощо. Тому для розрахунку необхідних потужностей (*FP*) вводиться формула:

$$FP = P * k, \quad (2.16)$$

де P – значення необхідного розміру потужностей отримане при прогнозуванні;

k – коефіцієнт необхідної зміни потужностей (*2.17*).

$$k = (M + U) / 2, \quad (2.17)$$

де M – відношення середньої місячної кількості повідомлень про високий рівень завантаженості системи за минулий рік до року перед ним (*2.18*). Для нівелювання виняткових випадків введено верхню межу значення V_{max}, ця межа задається індивідуально і повинна бути рівна максимально очікуваному навчальним закладом росту використовуваності сервісу в наступному році відносно попереднього*:* M не може бути більше $maxV$ тобто якщо $M > V_{max}$, то $M = V_{max}$;

U – відношення середнього значення кількості активних користувачів за місяць минулого року до середнього значення активних користувачів за місяць року перед ним

(*2.19*), для нівелювання впливу певних виняткових ситуацій введено використання правила про верхню межу значення описаного вище: U не може бути більше $maxV$, тобто якщо $U > V_{max}$, то $U = V_{max}$.

$$M = M_{new} / M_{old}, \qquad (2.18)$$

де M_{new} – місячна середня кількість повідомлень про високий рівень завантаженості системи за минулий рік;

M_{old} – місячна середня кількість повідомлень про високий рівень завантаженості системи за позаминулий рік.

$$U = U_{new} / U_{old}, \qquad (2.19)$$

де U_{new} – середнє значення кількості активних користувачів за місяць минулого року;

U_{old} – середнє значення кількості активних користувачів за місяць позаминулого року.

4) Далі застосовується наступний підхід для розрахунку вартості необхідного в майбутньому локального апаратного забезпечення: на платформах які є доступними для певного територіального положення вибирається кілька різних серверів (оптимально буде до 10) які б повністю задовольняють усі раніше отримані вимоги до апаратного забезпечення. Після чого вираховується середня ціна такого сервера.

5) Також ці значення (отримані за формулою *2.16*) застосовуються як вхідні дані для обрахунку вартості оренди хмарних потужностей. Використовуючи такий підхід: потрібно взяти до уваги лише провайдерів, що здатні надати хмарні потужності які територіально задовольняють певну установу а також мають позитивну перевірену репутацію; після цього, використовуючи отримані вимоги до апаратних потужностей, потрібно проаналізувати ціни на оренду хмарного рішення на рік. Варто звернути увагу на специфіку різних типів хмарних середовищ, адже деякі є рекомендованими для графічних навантажень, деякі для процесорних, а є й універсальні. Не потрібно зупинятись на 2 чи 3 варіантах, а як і у попередньому пункті оглянути до 10 різних.

6) Отримавши вартості локальних та хмарних апаратних потужностей, приймається рішення про перехід на хмарні потужності. Для прийняття такого рішення важливо мати певну основу. Для цього далі вводиться формула розрахунку доцільності переходу в хмару на основі фінансової складової:

$$SMF = (CP + CM) / (LP + LM), \quad (2.20)$$

де *CP* – розрахована раніше вартість оренди хмарного середовища;

CM – вартість обслуговування хмарного середовища на рік;

LP – розрахована раніше вартість закупівлі локального апаратного забезпечення;

LM – поточні витрати на утримання існуючого локального середовища на рік.

Також далі вводиться формула розрахунку доцільності переходу в хмару на основі очікуваного зростання навантаження протягом наступного року:

$$SML = SLY / SLX, \quad (2.21)$$

де SLY – місячне середнє значення показників навантаженості за прогнозований рік;

SLX – місячне середнє значення показників навантаженості системи за минулий рік.

Крім ціни потрібно врахувати і деякі додаткові фактори, тому далі у таблиці 2.13 перелічено головні чинники які потрібно взяти до уваги.

Таблиця 2.13. Правила прийняття рішення про перехід в хмару

Аспект	**Фактори**	**Порогове значення**
Вартість і бюджет	Поточні витрати на підтримку локальних сервісів. Приблизно оцініть загальні витрати на обслуговування, включаючи купівлю обладнання, електроенергію, ліцензії, зарплати працівників. (B1)	За результатами експертної оцінки перехід до хмари доцільний, якщо прогнозовані хмарні витрати не перевищують

	Орієнтовні витрати на купівлю необхідного локального апаратного забезпечення. Врахуйте прогнозовані витрати на покупку апаратного забезпечення за отриманим результатом як описано вище.	70-80% від витрат на апгрейд та підтримку локального апаратного забезпечення (розрахунок проводиться за формулою *2.20*).
	Орієнтовні витрати на хмарні сервіси. Візьміть до уваги вартість оренди хмарних потужностей за спрогнозованими показниками як описано вище.	
Безпека і відповідність	Стандарти безпеки. Якщо локальна інфраструктура не відповідає стандартам безпеки, перехід у хмару може бути вигідним. Хмарні провайдери зазвичай пропонують високий рівень безпеки й регулярні оновлення.	Перехід потрібно робити лише якщо повністю задовольняється 2 пункт і лише після цього, якщо може мати сенс пункт 1.
	Відповідність нормативним вимогам. Переконайтеся, що хмарний провайдер відповідає всім регулятивним вимогам, які застосовуються до вашого закладу.	
Гнучкість і масштабованість	Якщо є потреба у швидкому розширенні потужностей, хмарні рішення дозволяють легко збільшувати або зменшувати ресурси.	За результатами експертної оцінки перехід до хмари варто розглядати, якщо

		очікується зростання навантаження більше ніж на 20% протягом року (розрахунок проводиться за формулою *2.21*).
Експертність та технічна підтримка	Технічні знання команди. Якщо у закладу немає достатньо кваліфікованих IT-спеціалістів для обслуговування сервера, хмарний провайдер може надати необхідну підтримку.	Якщо на якийсь з факторів відповідь так тоді перехід може мати сенс.
	Доступність підтримки. Хмарні провайдери зазвичай пропонують цілодобову підтримку, що важливо при обмежених ресурсах всередині закладу.	
Надійність і безперебійність	Хмарні рішення часто мають високу доступність і резервування.	Якщо існують проблеми з надійністю локальної інфраструктури, то хмара може стати кращим варіантом.
Доступність та мобільність	Якщо для користувачів важливо мати доступ до ресурсів з різних місць, хмарні сервіси зазвичай забезпечують кращу мобільність.	Якщо це вагомий фактор тоді перехід є більш обґрунтованим.

Порогові значення можуть відрізнятися в залежності від специфіки закладу, але, загалом, рішення про перехід до хмари слід приймати на основі детального аналізу, враховуючи вищеописані фактори. Рекомендується також провести тестові міграції та консультації з хмарними провайдерами для точної оцінки.

7) Визначення фінального рішення важливості переходу на хмарне середовище. Тут до уваги беруться усі розроблені вище правила (табл. 2.13) і якщо на більшість пунктів відповідь що перехід на хмарні потужності потрібен, тоді фінальне рішення повинне бути на користь хмари.

Маючи розроблену модель визначення необхідності перенесення діджитал системи менеджменту даних навчального закладу на хмарні потужності з використанням алгоритмів прогнозування необхідного апаратного забезпечення, а також описаний алгоритм її застосування, зроблено приклад застосування створеного теоретичного підходу на практиці. Дані для прикладу згенеровано штучно через вимогу джерела інформації до конфіденційності та анонімності. Але хоч дані не є реальними вони являються наближеними до таких. Тож в додатку Б наведено згенеровані статистичні дані. Використовуючи їх, далі наведено приклад застосування розробленого підходу.

1. Прогнозування. Варто зазначити що у прогнозуванні беруть участь саме такі дані: відсоток завантаженості процесора, використана оперативна та постійна пам’ять. Решта показників можна упустити при прогнозуванні, адже вони не є критичними чи достатньо інформативними у нашому випадку. Першим кроком додано предиктори (рік, місяць). Далі обрано кілька варіантів моделей для часових рядів: два варіанти XGBoost (з learn_rate 0.35 та 0.5) і Elastic net (GLMNet). Формування тестової та навчальної вибірки. Оскільки є дані за 36 місяців, то вирішено взяти 3 для тестової вибірки, а решту для навчальної. На рис. 2.6, 2.7 та 2.8 зображено результати тестової побудови до кожного часового ряду по кожній математичній моделі.

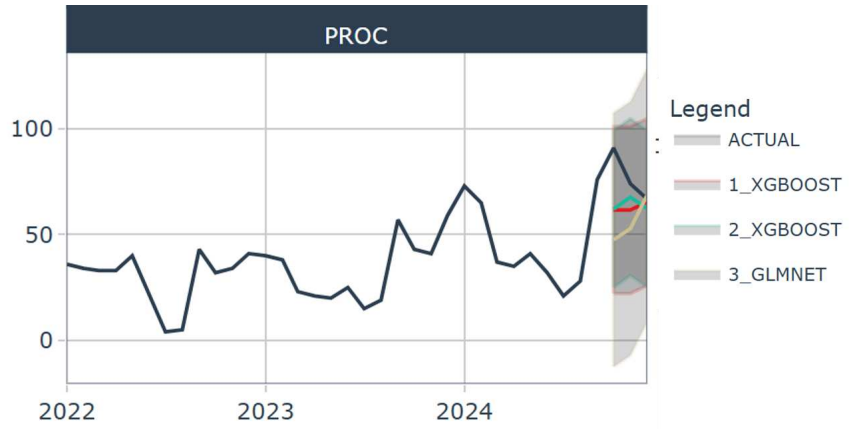

Рис. 2.6. Тестове прогнозування відсотка завантаженості процесора

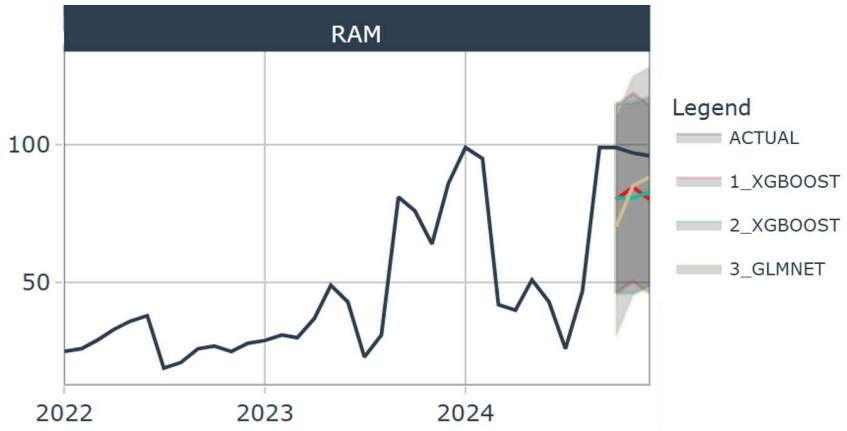

Рис. 2.7. Тестове прогнозування відсотка зайнятої оперативної пам’яті

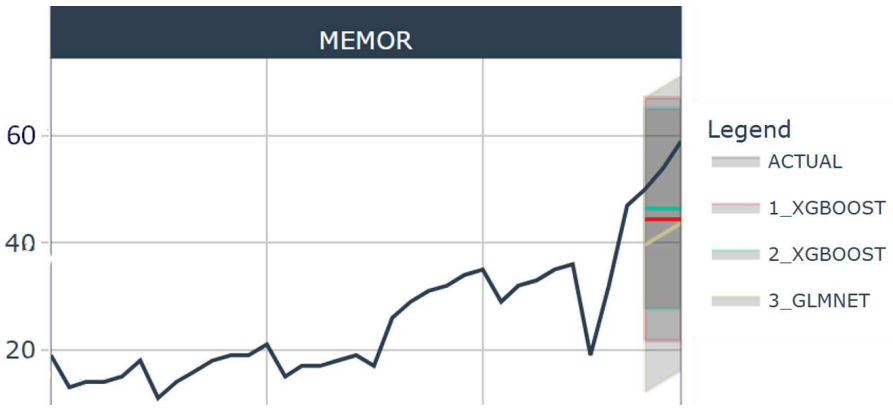

Рис. 2.8. Тестове прогнозування кількості зайнятої постійної пам’яті

Після цього оцінено кожну з математичних моделей на тестовій вибірці та обрано кращу математичну модель до кожного часового ряду за метрикою RMSE. Результати оцінки та вибору наступні: відсоток завантаженості процесора – XGBoost_2 (з learn_rate 0.5), відсоток зайнятої оперативної пам’яті – XGBoost_1 (з learn_rate 0.35) та кількість зайнятої постійної пам’яті – XGBoost_2 (з learn_rate 0.5). Вибрані варіанти показано на графіках нижче (рис. 2.9, 2.10, 2.11).

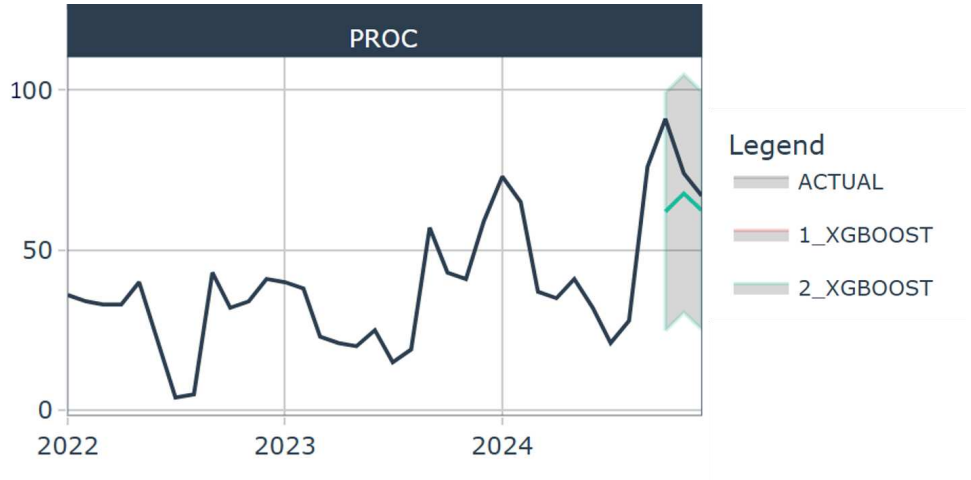

Рис. 2.9. Результат вибору кращої моделі по прогнозуванню завантаженості процесора

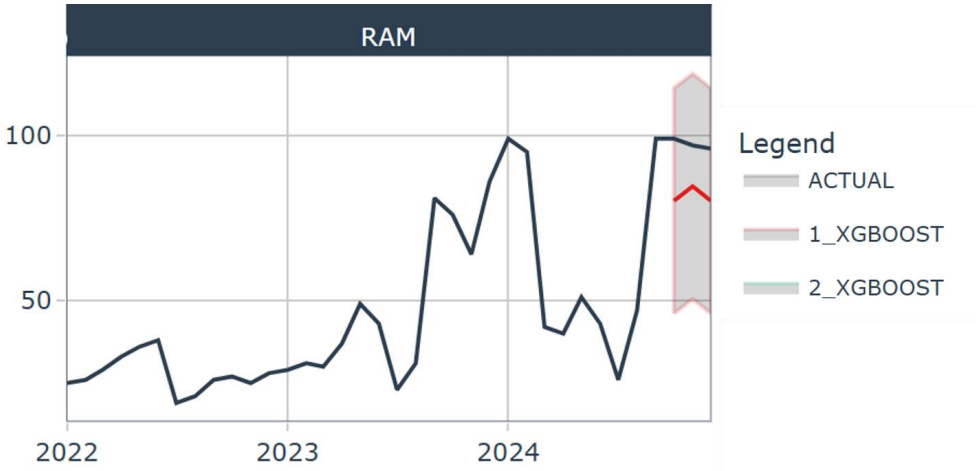

Рис. 2.10. Результат вибору кращої моделі по прогнозуванню зайнятої оперативної пам’яті

Рис. 2.11. Результат вибору кращої моделі по прогнозуванню зайнятої постійної пам’яті

Далі використано обрану модель до всього часового ряду (у кожного ряду може бути різна модель) і побудовано прогноз по рядах на майбутнє. На рис. 2.12, 2.13 та 2.14 результати прогнозування на рік.

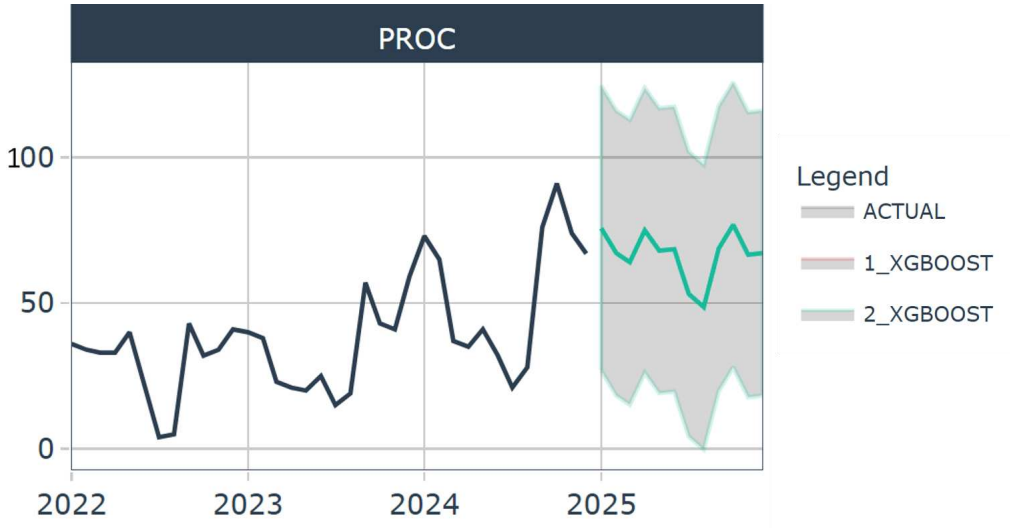

Рис. 2.12. Прогноз відсотків завантаженості процесора

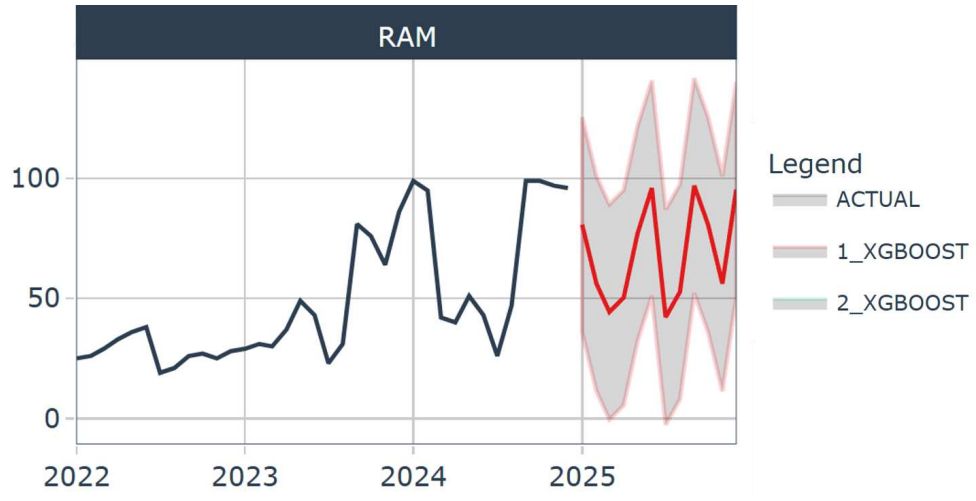

Рис. 2.13. Прогноз відсотків зайнятої оративної пам’яті

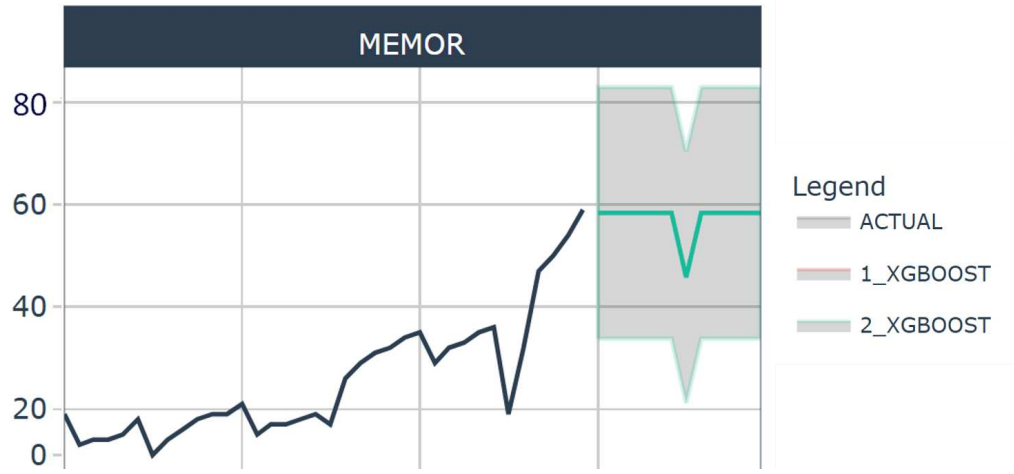

Рис. 2.14. Прогноз кількості зайнятої постійної пам’яті в гігабайтах

2. Визначення необхідних потужностей за результатами прогнозування та статистичними даними. Спершу фіналізуються необхідні апаратні потужності. Як видно у статистичних даних (додаток Б) за останній час різко зросла кількість повідомлень про високий рівень завантаженості системи. Також вважатиметься що навчальний заклад не бачить тенденцій до зменшення кількості активних користувачів діджитал сервісів.

Визначення необхідної кількості ядер процесора. На графіку прогнозованої завантаженості процесора (рис. 2.12) видно, що на наступний рік завантаженість ядер імовірно залишатиметься на високому рівні з можливими піками до 100 відсотків. Це

означає, що для забезпечення стабільної та швидкої роботи сервісу потужності потрібно збільшити. Оскільки зараз використовується 8 ядерний процесор, то ріст має бути до 12, а краще 16 ядер. Тож для розуміння необхідних потужностей застосовано раніше розроблену формулу *2.16*. За розрахунками отримано k = 1.8, FP = 14.5, тут результат не є цілим числом тому заокруглено до найближчого можливого значення кількості ядер – 16.

Визначення розміру необхідної оперативної пам’яті. Графік (рис. 2.12) показує, що оперативна пам’ять теж буде використовуватись близько до 100 відсотків. Отже, оперативну пам’ять теж потрібно збільшувати. В прикладі використовується 32 гігабайти оперативної пам’яті. Провівши розрахунки за (*2.16*), маємо FP = 58. Зважаючи на те, що серверів з такою кількістю оперативної пам’яті знайти неможливо, потрібно заокруглити отримане число до найближчого можливого – до 64 гігабайт.

Визначення необхідного розміру постійної пам’яті. На графіку прогнозування використання постійної пам’яті (рис. 2.14) максимальним прогнозованим значенням може бути до 85 гігабайтів. Далі виконано розрахунок потрібного значення (за формулою *2.16*) – FP = 153. Округливши до найближчого можливого значення, отримано 128 гігабайтів постійної пам’яті.

Отже, отримано наступні показники, на які варто орієнтуватись у подальших кроках. Кількість ядер процесора – 16, кількість гігабайт оперативної пам’яті – 64 та кількість гігабайт постійної пам’яті – 128.

Використовуючи локальні маркетплейси, виписано ціни у доларах США різних 10 варіантів які задовольняють наші умови. Ось перелік цін по зростанню: 2610, 2675, 2755, 3041, 3399, 3478, 3589, 3850, 3923, 4125. Вирахувавши середнє значення, отримано ціну 3347 доларів США.

Далі переглянувши кілька популярних сервісів з надання хмарних потужностей, виписано до 10 цін річної оренди різних варіантів які задовольняють зазначені вище вимоги. Ось перелік цін: 2470, 3127, 3440, 3489, 3513, 3562, 3686, 4206, 4889, 5238. Середня ціна виходить 3762 доларів США.

3. Побудова таблиці прийняття рішення. Отримавши приблизні значення цін, виконано побудову таблиці прийняття рішення про перехід у хмару (табл. 2.14).

Таблиця 2.14. Приклад прийняття рішення про перехід в хмару

Аспект	**Фактори**	**Рекомендація**
Вартість і бюджет	Зазначено що установа яку взято до прикладу витрачає приблизно на обслуговування локального сервера та інші пов’язані витрати 6100 доларів США.	Перехід у хмару та оренда потужностей на рік вартуватиме приблизно 7262 доларів США тоді як локальні потужності 9447. Застосувавши формулу *2.20,* отримуємо, що співвідношення ціни хмари до локальних потужностей 77% відсотків. Перехід має сенс.
	Витрати на новий локальний сервер 3347 доларів США.	
	Оренда хмари на рік 3762 доларів США. Витрати на підтримку та інше можна буде скоротити приблизно до 3500 доларів США на рік.	
Безпека і відповідність	Оскільки більшість хмарних провайдерів задовольняють усі вимоги до безпеки та постійно оновлюються до останніх версій складових програмного забезпечення, то перехід не суперечить вимогам до безпеки.	Можливо задовольнити обидва пункти, отже, перехід можливий.
	Вибрані провайдери не мають суперечностей з відповідністю	

	нормативним вимогам.	
Гнучкість і масштабованість	На початку можна орендувати середовище трохи меншої потужності адже, майже усі хмарні рішення дозволяють легко збільшувати або зменшувати ресурси. Що дозволить ще трохи скоротити витрати.	Застосувавши формулу *2.21,* виявлено, що зростання навантаження може бути суттєво більшим за 20% протягом року. Отже, перехід може бути корисним.
Експертність та технічна підтримка	З'являється можливість зменшити технічну команду зменшити, адже часто хмарний провайдер може надати необхідну підтримку. Що також дозволяє скоротити витрати.	Перехід дозволить скоротити витрати на обслуговування.
	Хмарні провайдери зазвичай пропонують цілодобову підтримку, що важливо при обмежених ресурсах всередині закладу.	
Надійність і безперебійність	Хмарні рішення часто мають високу доступність і резервування. Але як зазначив користувач на даному етапі це не має великого значення для установи, адже більшість користувачів є локальними й з існуючим середовищем не виникало проблем.	Проблем не спостерігалось, отже, перехід у хмару не дасть суттєвих переваг.
Доступність та	Більшість користувачів є локальними.	Перехід у хмару не має

мобільність		глобального сенсу.

4. Рекомендації щодо рішення про перехід на хмарні потужності. Як видно з таблиці прийняття рішення про перехід у хмару (табл. 2.14) по більшості пунктах перехід має сенс. Звісно використані дані є штучно згенеровані, але вони є наближеними до реального випадку. Результат у прикладі показує, що перехід на хмарні потужності є доволі вигідним навіть з цих грубих розрахунків. Крім того, як зазначалось раніше, так і це демонструє результуюча таблиця (табл. 2.14) крім ціни є й інші переваги застосування хмарних технологій: масштабованість, економічна ефективність, доступність, зниження витрат на обслуговування, інноваційність.

Звідси витікає висока популярність використання хмарних рішень. Також очевидним є те що не навіть, якщо певні навчальні заклади та платформи досі не перейшли на таку модель роботи вони ймовірно це зроблять у майбутньому. Але крім великих переваг які надають хмарні технології є і певні мінуси: безпека даних, обмежений контроль, правові та регуляторні проблеми.

Отже, враховуючи те, що з проведених досліджень раніше видно, що велика частина даних, які поширюються в діджиталізованому навчальному середовищі є персональна інформація стейкхолдерів навчального процесу таких як студенти, викладачі, адміністрація та інші. Саме тому конче необхідно звернути увагу на ризики витоку персональних даних при діджитал взаємодії в освітньому середовищі та способи їх зниження.

2.5 Модель анонімізації персональних даних в потоках даних при інформаційній взаємодії у діджиталізованому освітньому середовищі

Визначивши основні ризики витоку персональних даних учасників навчального процесу при застосуванні зовнішніх інформаційних технологій в освітній сфері,

виокремлено фактори ризику витоку персональної інформації стейкхолдерів навчального процесу. Розглянемо більш детально:

1. У будь-якій цифровій взаємодії є ризики витоку персональних даних на етапі її транспортування від джерела (як то освітній заклад чи брокер даних) до цільової платформи чи сховища.

2. Збереження копій персональної інформації зовнішньою системою чи зовнішнім сховищем даних є причиною виникнення ризику витоку персональних даних користувачів. Тобто з’являється ризик витоку такої інформації з зовнішньої (напряму не контрольованого представниками освітнього закладу) бази даних.

3. Коли джерелом даних виступає брокер, а не освітній заклад напряму, контрольованість поширення даних третім сторонам знижується. А відповідно ймовірність витоку персональних даних виростає в рази.

4. Зниження ризиків витоку персональної інформації студентів можливе лише за умови що така інформація не покидає межі локальної цифрової мережі навчального закладу.

Проаналізувавши отримані результати, прийнято рішення застосування анонімізації для зниження ризиків витоку персональних даних. Джерелом даних може виступати як навчальний заклад, так і брокер даних. Розраховано оцінку небезпеки попередньо визначених типів потоків даних при застосуванні анонімізації для обох випадків. Як і раніше вважається що:

- вразливість до витоку персональних даних на усіх етапах усіх потоків даних рівна і дорівнює a;
- співвідношення кількості персональних даних до кількості усіх даних на кожному етапі кожного потоку даних рівна і дорівнює b;
- кількість даних на кожному етапі кожного потоку даних є рівною і дорівнює c;
- інтенсивність усіх потоків даних рівна і дорівнює d;

Також вважається що анонімізація застосовується до усіх персональних даних які віддаються від джерела даних де впроваджено сервіс анонімізації персональних даних.

Результати розрахунків для випадку коли анонімізація застосовується лише на брокері даних показано в таблиці 2.15.

Таблиця 2.15. Оцінки небезпеки витоку персональних даних кожного типу потоків даних за умови застосування анонімізації на стороні брокера даних

№	Потік даних	Етапи які проходять дані	Оцінка небезпеки потоку (*DP*)
1	Навчальний заклад – Проста зовнішня платформа	Передача даних, обробка даних. (2)	*cd*2ab*
2	Навчальний заклад – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних. (3)	*cd*3ab*
3	Навчальний заклад – Сховище даних	Передача даних, збереження даних. (2)	*cd*2ab*
4	Навчальний заклад – Брокер даних – Проста зовнішня платформа	Передача даних, обробка даних, збереження даних, передача даних, обробка даних. (3+2)	*cd*3ab*
5	Навчальний заклад – Брокер даних – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних, передача даних, обробка даних, збереження даних. (3+3)	*cd*3ab*

6	Навчальний заклад – Брокер даних – Сховище даних	Передача даних, обробка даних, збереження даних, передача даних, збереження даних. (3+2)	*cd*3ab*

Результати розрахунків для випадку коли анонімізація застосовується на стороні навчального закладу показано в таблиці 2.16.

Таблиця 2.16. Оцінки небезпеки витоку персональних даних кожного типу потоків даних за умови застосування анонімізації на стороні навчального закладу

№	Потік даних	Етапи які проходять дані	Оцінка небезпеки потоку (*DP*)
1	Навчальний заклад – Проста зовнішня платформа	Передача даних, обробка даних. (2)	*0*
2	Навчальний заклад – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних. (3)	*0*
3	Навчальний заклад – Сховище даних	Передача даних, збереження даних. (2)	*0*
4	Навчальний заклад – Брокер даних – Проста зовнішня платформа	Передача даних, обробка даних, збереження даних, передача даних, обробка даних. (5)	*0*
5	Навчальний заклад	Передача даних, обробка даних,	*0*

	– Брокер даних – Зовнішня платформа зі сховищем даних	збереження даних, передача даних, обробка даних, збереження даних. (6)	
6	Навчальний заклад – Брокер даних – Сховище даних	Передача даних, обробка даних, збереження даних, передача даних, збереження даних. (5)	*0*

Аналіз зроблених розрахунків дає змогу стверджувати, що застосування анонімізації суттєво знижує оцінку небезпеки потоків даних при інформаційних взаємодіях навчального закладу. Але, оскільки в першому випадку (табл. 2.15) застосування відбувається лише на етапі віддачі даних брокером даних третім сторонам, то рівень небезпеки попередніх етапів потоків даних за участю брокера даних не змінився. Крім того, цей підхід не дозволяє впливати на потоки даних у яких не присутній брокер даних. Також варто зауважити що реальні персональні дані усе ще зберігаються у внутрішньому сховищі брокера даних. Відповідно лишається ризик несанкціонованого поширення цих даних неавторизованим споживачем.

У випадку застосування анонімізації на стороні навчального закладу за визначеними умовами ризик витоку персональних даних вдалось знизити до нуля. Звісно, у реальному житті не завжди є можливість застосувати токенізацію до усіх персональних даних які споживають зовнішні сервіси, але токенізація навіть частини з них дає можливість суттєво знизити ризики. Для підтвердження цього зробимо повторні розрахунки оцінок небезпеки потоків даних при інформаційних взаємодіях навчального закладу, змінивши кількість персональних даних, які токенізуються. Тож далі зберігаються ті ж самі умови стосовно кількості поширюваних даних, інтенсивності потоків, вразливості кожного етапу усіх потоків та співвідношенню кількості персональних даних на цих етапах. Але, далі вважатимемо що токенізуються

не усі персональні дані які віддає навчальний заклад, а лише половина. Результати розрахунку оцінок зображено у таблиці 2.17.

Таблиця 2.17. Оцінки небезпеки витоку персональних даних кожного типу потоків даних за умови часткового застосування анонімізації на стороні навчального закладу

№	Потік даних	Етапи які проходять дані	Оцінка небезпеки потоку (*DP*)
1	Навчальний заклад – Проста зовнішня платформа	Передача даних, обробка даних. (2)	*cd*ab*
2	Навчальний заклад – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних. (3)	*cd*1,5ab*
3	Навчальний заклад – Сховище даних	Передача даних, збереження даних. (2)	*cd*ab*
4	Навчальний заклад – Брокер даних – Проста зовнішня платформа	Передача даних, обробка даних, збереження даних, передача даних, обробка даних. (5)	*cd*2,5ab*
5	Навчальний заклад – Брокер даних – Зовнішня платформа зі сховищем даних	Передача даних, обробка даних, збереження даних, передача даних, обробка даних, збереження даних. (6)	*cd*3ab*
6	Навчальний заклад –	Передача даних, обробка даних,	*cd*2,5ab*

	Брокер даних – Сховище даних	збереження даних, передача даних, збереження даних. (5)	

Отримані результати демонструють що навіть за умови часткової токенізації персональних даних на стороні навчального закладу перед їх віддачею зовнішнім споживачам суттєво знижується рівень небезпеки усіх потоків. Але, оскільки частина персональних даних у відкритому вигляді усе ж поширюється зовнішнім платформам і відповідно брокеру даних, то лишаються ризики пов’язані з несанкціонованою передачею персональних даних брокером даних третім неавторизованим споживачам.

Отже, далі створено рекомендації до застосування сервісу анонімізації персональних даних до інформаційних взаємодій навчального закладу в діджиталізованій освітній сфері:

1. Анонімізація даних має відбуватись на стороні навчального закладу перед передачею зовнішнім споживачам даних.

2. Застосуванню анонімізації підлягають усі персональні дані перед віддачею, за умови збереження можливості надання зовнішньою платформою сервісів необхідних навчальному закладу.

3. Особлива увага має бути приділена токенізації даних які поширюються з брокером даних. При поширенні даних з брокером потрібно токенізувати якомога більшу кількість персональних даних.

4. Спосіб токенізації даних повинен бути надійним та водночас задовольняти вимоги зовнішніх споживачів даних до формату даних які поширюються.

Якщо слідувати цим рекомендаціям, то анонімізація буде ефективною, і відповідно ризики витоку персональних даних зменшуються. А в ідеальній ситуації вони наближуватимуться до нуля. Зважаючи на проведений аналіз, побудовано схематичну модель захисту персональних даних студентів з використанням сервісу анонімізації таких даних у локальній цифровій мережі навчального закладу (рис. 2.15) [8].

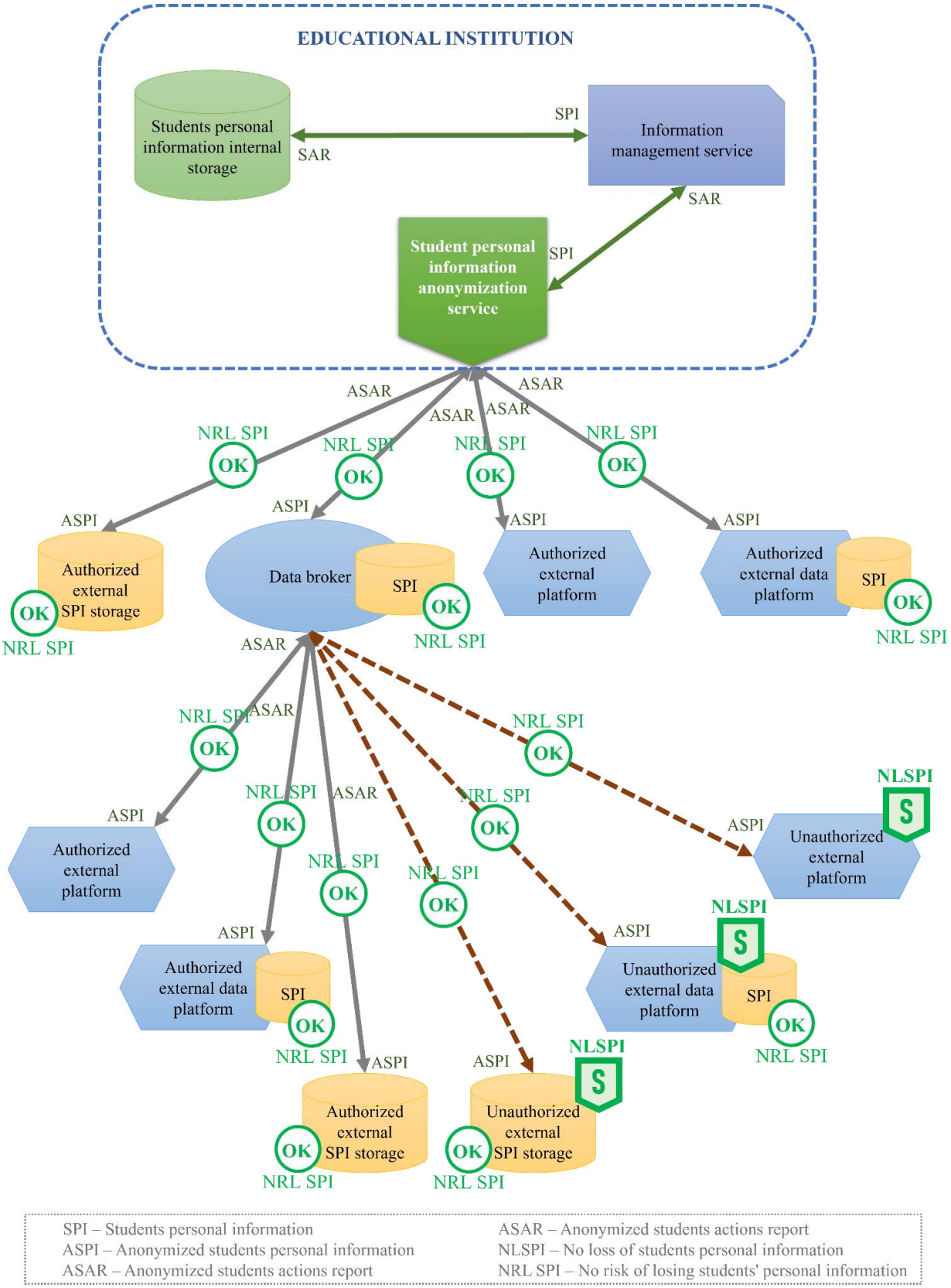

Рис. 2.15. Схематична модель застосування анонімізації персональних даних здобувачів освіти [8].

Обмеженням створеної моделі є те, що вона не впливає на виокремлені у роботі об’єкти, з якими співпрацює освітній заклад. Суть моделі – зосередження на джерелі даних. Адже зазвичай зовнішнім споживачам персональних даних не потрібно знати з яким конкретно стейкхолдером, здобувачем освіти чи групою здобувачів система комунікує. Важливим є лише забезпечення унікальності та консистентності даних, тобто можливість ідентифікувати кожен окремий елемент взаємодії. Звідси й випливає той факт, що зовнішнім системам не обов’язково надавати доступ до реальних даних, можна їх замінити унікальними анонімізованими одиницями. Лиш важливо, щоб сам заклад зміг у майбутньому співставити якому з реальних користувачів належать отримані від зовнішніх навчальних систем ті чи інші нові дані (звіти активності).

Особливістю запропонованої моделі є те, що це інформаційний інструмент (сервіс) в основі якого відбувається анонімізація персональної інформації стейкхолдерів освітнього середовища. Виокремлено основні вимоги до інформаційного інструменту:

1. Унікальному стейкхолдеру освітнього середовища для кожного окремого споживача повинен генеруватися окремий набір анонімних даних (токенів), який і повинен поширюватись з цією конкретною зовнішньою системою.

2. Сервіс анонімізації повинен підтримувати зворотний механізм, тобто деанонімізацію даних у межах локальної інформаційної мережі навчального закладу. Це потрібно у випадку, коли зовнішні системи повертатимуть нові (звітні) дані пов’язані з навчальним процесом кожного з користувачів.

3. Даний сервіс повинен забезпечувати всі необхідні інструменти для застосування адміністраторами навчального закладу різних алгоритмів та шаблонів анонімізації персональних даних студентів. Це потрібно для того, щоб згенеровані токени відповідали індивідуальним вимогам кожного зовнішнього споживача у інтеграції з яким має необхідність навчальний заклад.

4. Здатність поширювати відповідні анонімізовані дані лише з авторизованими зовнішніми споживачами персональних даних, список яких повинен конфігурувати адміністраторами навчального закладу.

З проведеного моделювання, встановлено, що не потрібно змінювати способи взаємодії з зовнішніми навчальними системами. Також не потрібно впроваджувати нові більш строгі правила обробки та зберігання даних до таких систем. І що найголовніше навчальний заклад більше не повинен перейматись які треті сторони можуть отримати доступ до поширених даних, адже, зовнішнім споживачам даних не надаються реальні дані витік яких є проблемою. Тобто, змінивши лише частину інформаційної мережі навчального закладу, вирішується більшість викликів, пов’язаних з ризиками витоку персональних даних стейкхолдерів освітнього середовища в умовах діджиталізації.

2.6 Модель деанонімізації персональних даних стейкхолдерів в інформаційних потоках при інформаційній взаємодії у діджиталізованому освітньому середовищі

Як визначено, у сучасному освітньому середовищі, яке постійно зазнає трансформацій під впливом технологічного прогресу, анонімізація даних стейкхолдерів є критично важливою складовою захисту конфіденційності. Адже вона забезпечує захист особистої інформації, зменшує ризики неправомірного використання даних і сприяє дотриманню законодавчих норм. Проте, існують ситуації, коли необхідність підтримувати зворотний зв’язок та забезпечувати якісний сервіс вимагають можливості деанонімізувати дані. Це може включати випадки, коли необхідно швидко реагувати на загрози безпеці, надавати персоналізовану підтримку студентам або здійснювати важливу комунікацію через прямі канали, такі як SMS або електронна пошта. Тому, хоча анонімізація залишається ключовим інструментом захисту даних, важливо також розуміти, що в деяких ситуаціях деанонімізація є виправданою та необхідною для ефективного управління освітнім процесом.

Далі визначено головні причини чому механізм деанонімізації анонімних даних в освітньому середовищі може бути необхідним:

1. безпека та реагування на надзвичайні ситуації – у разі загрози безпеці, наприклад, при виявленні потенційно небезпечної поведінки або загрози для студента чи співробітника, можливість ідентифікації може бути необхідною для швидкого реагування і запобігання небезпеці;

2. виправлення помилок або несправностей – інколи дані можуть бути анонімізовані помилково, що призвело до втрати важливої інформації для певних процесів і саме механізм деанонімізації дає змогу відновити доступ до вихідних даних, щоб виправити помилки чи несправності;

3. юридичні зобов'язання – у випадках, коли існують юридичні зобов'язання або рішення судів, що вимагають розкриття особи для розслідування інцидентів, деанонімізація може бути необхідною складовою відповідності законодавству;

4. індивідуальна підтримка – деякі освітні програми можуть вимагати персоналізованої підтримки студентів на основі персональних даних, таких як покращення академічної успішності чи психосоціальної підтримки, коли є в цьому обґрунтована потреба;

5. узгодження з учасниками – учасники навчального процесу (студенти, викладачі тощо) можуть добровільно надавати згоду на деанонімізацію своїх даних для участі в конкретних програмах або дослідженнях, які вимагають особистої ідентифікації;

6. пряма взаємодія з учасниками навчального процесу – у деяких випадках може виникнути необхідність у прямій комунікації зі стейкхолдерами через канали зв'язку, такі як SMS або електронна пошта. Наприклад, для надсилання важливих нагадувань про дедлайни, події, зміни в розкладі чи інші критичні оновлення. Деанонімізація може дозволити освітнім платформам забезпечити своєчасну та ефективну комунікацію з відповідними учасниками.

Варто зазначити, що така практика повинна здійснюватися з дотриманням політик конфіденційності та за згодою учасників, щоб забезпечити належний баланс між зручністю комунікації та захистом особистої інформації.

Як визначено раніше освітні заклади взаємодіють з різного типу зовнішніми навчальними платформами, які споживають персональну інформацію учасників навчального процесу. Тому далі на схематичних моделях (рис. 2.16, 2.17 та 2.18) показано процес взаємодії зовнішньої платформи з навчальним закладом з метою отримання дозволів для отримання та використання деанонімізованих даних.

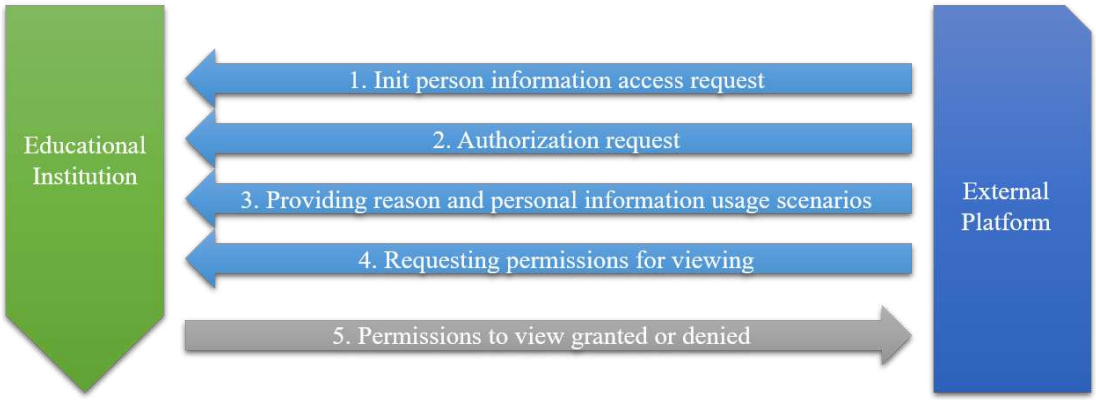

Рис. 2.16. Надання доступу до деанонімізованих даних зовнішній навчальній платформі, яка не зберігає і не поширює дані користувачів

Рис. 2.17. Надання доступу до деанонімізованих даних зовнішній навчальній платформі, яка зберігає, але не поширює дані користувачів

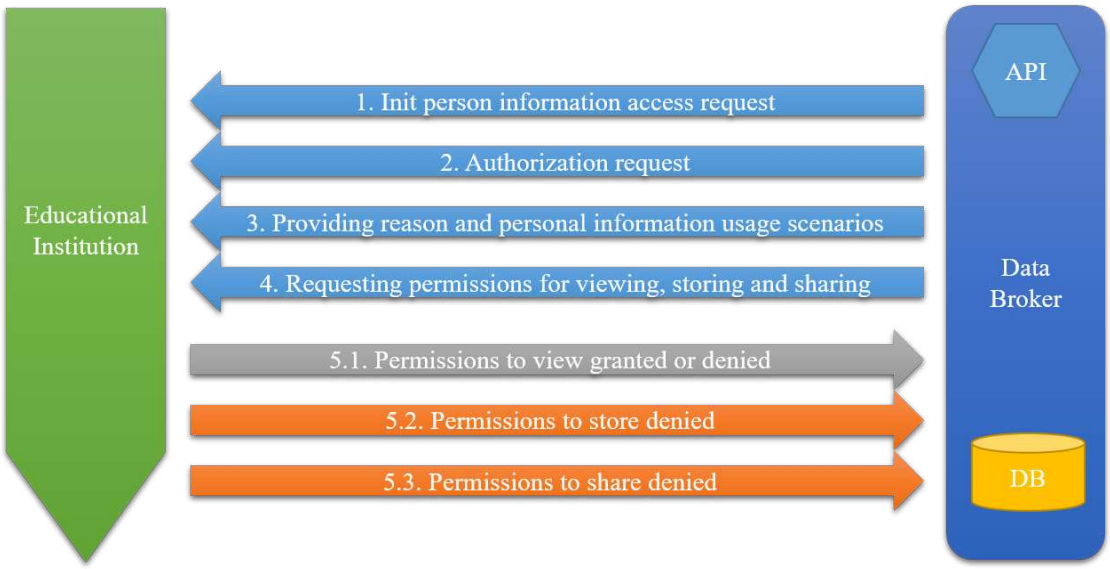

Рис. 2.18. Надання доступу до деанонімізованої інформації брокеру даних який зберігає і поширює дані користувачів

Як видно зі схематичних моделей є кілька типів зовнішніх освітніх платформ з якими може взаємодіяти навчальний заклад і кожен з типів може виконувати різні дії з персональними даними. Прості навчальні платформи іноді просто надають певний короткочасний сервіс учасникам навчального процесу, не зберігаючи їх персональну інформацію, для подальшого використання і відповідно не поширюють ці дані іншим платформам, як то генерація зображень, відправка електронного листа чи SMS тощо. Але іноді для надання своїх послуг такі платформи в певний момент можуть потребувати деякої персональної інформації користувача, як то електронна пошта, ім’я чи номер телефону. Тоді така платформа може зробити запит до навчального закладу на отримання деанонімізованих персональних даних певного користувача за його згоди та виконання певних дій на такій зовнішній платформі.

Підсумовуючи розроблені схеми (рис. 2.16, 2.17 та 2.18), описано загальні кроки взаємодії навчального закладу саме з навчальною платформою:

1. Зовнішня навчальна платформа ініціює процедуру отримання доступу до деанонімізованих даних користувача/користувачів.

2. Для подальшої взаємодії така платформа має пройти авторизацію у навчальному закладі. Тобто навчальний заклад має підтвердити що він готовий обробити запит такої платформи.

3. Далі зовнішня платформа надає підстави необхідності отримання деанонімізованих даних користувачів та надає сценарії використання такої інформації.

4. Після підтвердження навчальним закладом опрацювання інформації щодо необхідності навчальною платформою деанонімізованих даних певного типу така платформа робить запит на отримання прав на виконання певних дій з деанонімізованими даними.

5. Навчальний заклад переглядає запитані права аналізує їх необхідність та забезпечення захищеності таких даних зі сторони платформи й надає певні доступи. Варто зазначити що права на отримання певних деанонімізованих даних користувачів можуть надаватись лише для їх використання зовнішньою платформою за певними сценаріями й без подальшого зберігання таких даних цією платформою або поширення їх третім сторонам.

Далі на основі моделей взаємодії зовнішніх навчальних платформ з освітнім закладом для отримання деанонімізованих даних учасників освітнього процесу побудовано модель поширення деанонімізованих даних від навчального закладу до сторонніх навчальних сервісів (рис. 2.19).

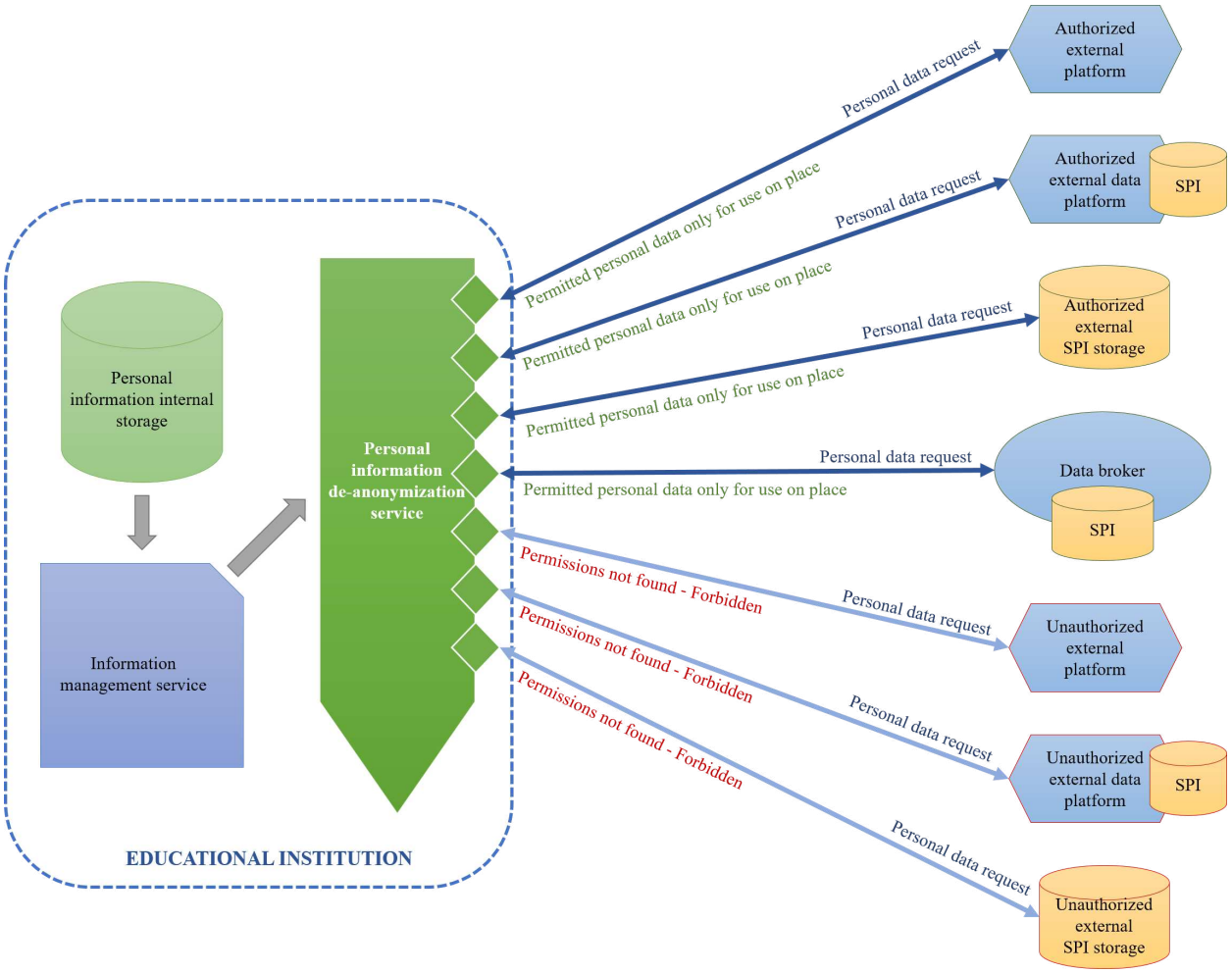

Рис. 2.19. Модель деанонімізації персональних даних стейкхолдерів навчального процесу

Як видно зі створеної моделі запити на отримання деанонімізованих даних можуть іти від різного типу зовнішніх споживачів. Тому далі описано їх типи та характер взаємодії з ними:

7) Навчальна платформа яка надає певний сервіс та не зберігає і не поширює дані користувачів. Тут взаємодія зі сторони навчального закладу і зі сторони навчальної платформи є максимально простою. Навчальний заклад поширює персональні дані лише для використання на місці без прав на збереження таких даних чи їх поширення, а платформі більших прав і не потрібно.

8) Більш складні навчальні платформи, які виконують зберігання даних користувачів у своїй локальній базі даних. Тут ситуація трішки складніше, адже для

безпеки учасників освітнього процесу дозволяється зберігати зовнішніми сервісами лише анонімізовані дані користувачів. Тож тут зовнішня платформа має гарантувати що деанонімізовані персональні дані користувачів не будуть збережені в локальне сховище і будуть використані лише на місці необхідності для надання певних додаткових послуг за згодою користувача. Тоді сервіс деанонімізації навчального закладу надасть доступ до певного роду персональної інформації та поширить її за запитом зовнішньої навчальної платформи.

9) Зовнішні сховища та бази даних. Оскільки збереження персональної інформації заборонено, то доступ до персональних даних користувачів може бути надано за такими ж правилами як і для зовнішніх навчальних платформ що зберігають користувацьку інформацію у локальному сховищі. Тобто дані можуть бути надані лише за згоди користувача і без права збереження таких даних у зовнішньому сховищі.

10) Брокери даних. Тут ситуація трішки складніша, адже суть брокера даних це збереження, перетворення та подальше поширення даних користувачів. Тобто виконання його прямих функцій з деанонімізованими даними неможливе. Але іноді брокери даних мають можливість надавати додаткові послуги крім роботи з даними та їх поширенням. І якщо буде забезпечено використання персональних даних лише у таких місцях без їх подальшого збереження і поширення, то тоді брокерам даних може надаватись такий обмежений доступ до персональної інформації користувачів, звісно за їх згоди.

11) Неавтентифіковані зовнішні платформи різного типу (прості, ті які зберігають користувацькі дані, зовнішні бази даних і навіть брокери). Тут все зрозуміло – таким сервісам доступ до деанонімізованих даних учасників навчального процесу не надається.

Також варто зазначити, що поширення персональних даних учасників навчального процесу є чутливим питанням, яке вимагає ретельного контролю та зваженого підходу. У сучасному цифровому світі обмін даними у навчальних

середовищах є невіддільною частиною освітньої діяльності, однак разом із цим зростають і ризики порушення конфіденційності та безпеки інформації.

Контроль над поширенням особистих даних повинен здійснюватися на всіх етапах збору, обробки, зберігання та передачі інформації. Це гарантує, що дані учасників освітнього процесу (студенти, викладачі, адміністративний персонал та інші) є захищеними й доступ до них можливий лише в обґрунтованих випадках. Для цього освітні установи повинні розробляти та впроваджувати чіткі політики конфіденційності та протоколи обробки інформації, що відповідають сучасним стандартам та законодавчим вимогам.

Поширення персональних даних має відбуватися виключно за наявності реальної потреби, наприклад, для покращення навчального процесу, надання адресної підтримки, виконання адміністративних чи навчальних обов’язків. Крім того, усі подібні дії мають бути прозорими для користувачів, із забезпеченням їх інформованої згоди на обробку даних.

Отже, описано підхід до застосування деанонімізації персональних даних користувачів. На основі цього створено модель захищеності персональних даних під час застосування сервісу деанонімізації персональних даних учасників навчального процесу.

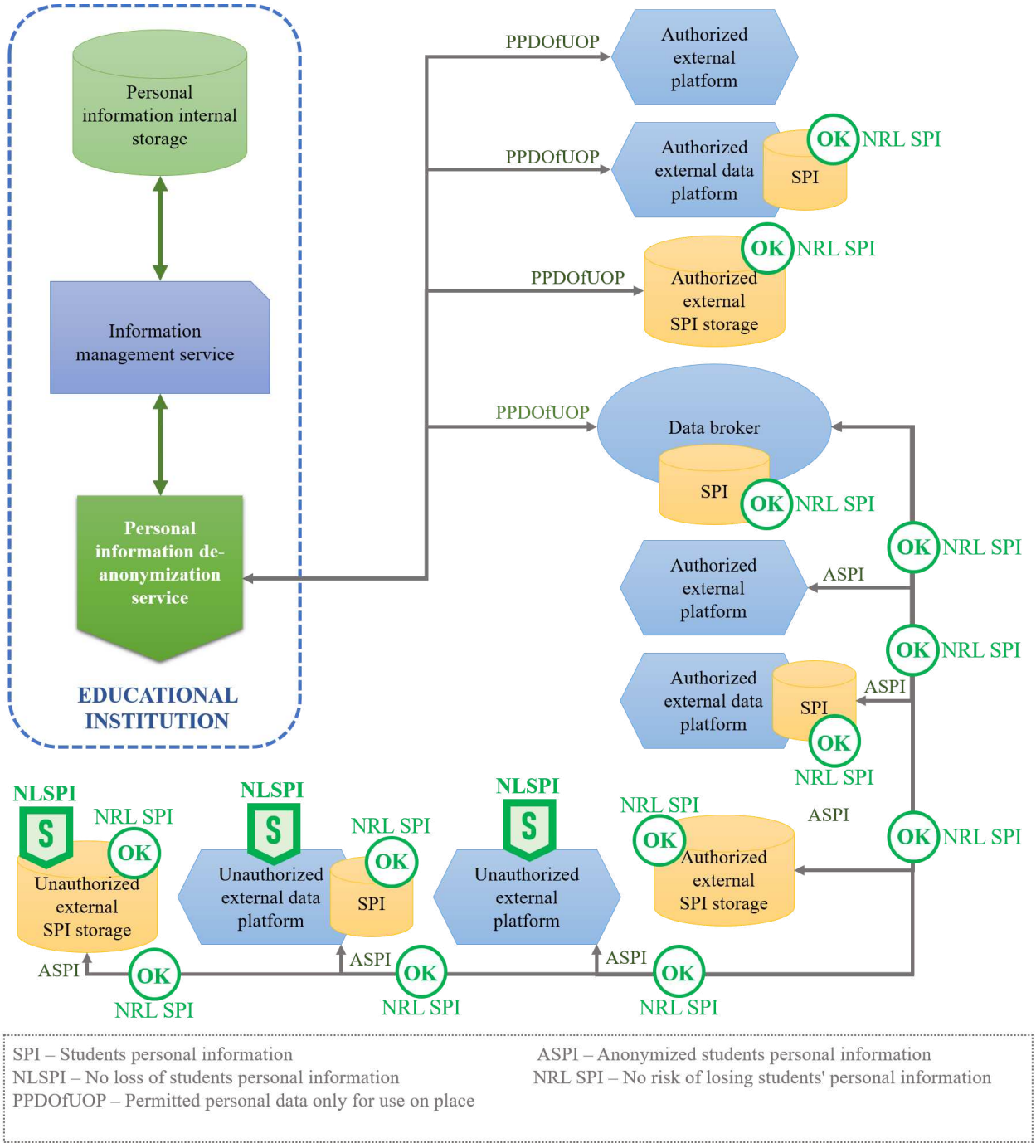

Рис. 2.20. Модель захищеності персональних даних під час використання сервісу деанонімізації

Дана модель (рис. 2.20) показує поширення деанонімізованих даних. Як видно з малюнку розроблений підхід передбачає опрацювання ризикових місць витоку персональної інформації учасників освітнього процесу. Перелік таких місць:

1) локальні бази даних зовнішніх навчальних платформ;

2) зовнішні сховища даних;

3) бази даних брокерів даних;

4) неавторизовані сторонні платформи;

5) неавторизовані сторонні сховища даних.

Варто пояснити чому саме на моделі ці місця позначені як опрацьовані місця ризику витоку персональних даних користувачів. Насправді ці фактори уже згадувались вище. Але все ж варто дати роз'яснення ще раз.

Першим фактором є встановлення та застосування процесу надання доступу до деанонімізованих даних стороннім сервісам самим навчальним закладом.

Другий – застосування описаних вище політик щодо цілей з якими можуть поширюватись персональні дані учасників навчального процесу. А саме лише за чіткого розуміння сценарію застосування цих даних стороннім сервісом освітній заклад поширює такі дані. І лише у випадку якщо цей сценарій є виправданим і необхідним для надання певного виду навчальних послуг. Крім того, такі дані можуть бути застосовані лише у місці потреби й не можуть бути збережені в локальних базах даних зовнішніх навчальних платформ чи брокерів даних. Також заборонене поширення цих даних в інші модулі зовнішніх платформ і тим більше іншим стороннім сервісам.

Ну й останній пункт – якщо задовольняються усі описані вище вимоги, користувач повинен підтвердити що він потребує цього особливого сервісу зовнішньої навчальної платформи (яка вимагає отримання певного роду персональної інформації користувача) і згідний з наданням описаних вище прав на його персональні дані.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. У цьому розділі наукової роботи була проведена глибока та систематична оцінка управління потоками персональних даних у контексті діджиталізації освітньої

сфери. Це дослідження є важливим внеском у розвиток безпечного та ефективного управління інформацією в освітніх установах.

2. Здійснено детальний аналіз потоків персональних даних у діджиталізованій освітній сфері. Визначено, як дані циркулюють між різними учасниками, такими як студенти, викладачі, адміністрація та зовнішні сервіси. Аналіз виявив ключові точки, де відбувається обробка даних, що дозволило розробити стратегії для підвищення безпеки та конфіденційності.

3. Також виділено та описано основні стейкхолдери інформаційної взаємодії у діджиталізованій освітній сфері. Проведено аналіз їхніх інформаційних потреб і пов’язаних ризиків, що допомогло створити модель потоків персональних даних. Ця модель стала основою для розробки рекомендацій щодо оптимізації збору, зберігання та обміну інформацією, мінімізуючи при цьому ризики порушення конфіденційності.

4. Важливим зазначити, що досліджено та визначено основні точки контролю потоків персональних даних. У розділі були виконані конкретні кроки з ідентифікації цих точок, що забезпечує можливість більш ефективного моніторингу та реагування на загрози.

5. У процесі дослідження була розроблена модель ризиків витоку персональних даних, що дозволяє не лише ідентифікувати потенційні загрози, але й оцінювати їх вплив. Це включало аналіз сценаріїв ризику та визначення методів їхнього зниження, що є необхідним для захисту даних у сучасному освітньому середовищі.

6. Після чого розроблено принципи мінімізації поширення персональних даних, які базуються на аналізі зібраної інформації та її релевантності. У рамках цього дослідження були сформульовані практичні рекомендації для освітніх закладів щодо зменшення обсягів даних, що обробляються, що допоможе знизити ризики неправомірного використання інформації.

7. Також опрацьовано аспект управління зберіганням даних навчального закладу в умовах стрімкої діджиталізації освітньої сфери. Створено модель призначену для оцінки необхідності переходу діджитал менеджмент системи навчального закладу

на хмарні потужності яка базується на використанні алгоритмів прогнозування. Після розробки моделі проведено її застосування на згенерованих даних наближених до реальної ситуації.

8. Базуючись на отриманих знаннях побудовано модель анонімізації персональних даних стейкхолдерів освітнього процесу. Продемонстровано різко позитивний вплив застосування анонімізації на ідентифіковані раніше ризикові точки витоку персональних даних.

9. Крім того, у роботі запропоновано модель деанонімізації даних. Описано підходи до взаємодії навчального закладу та кожного типу зовнішніх споживачів даних в контексті запиту на деанонімізацію токенізованих персональних даних учасників навчального процесу. Після чого продемонстровано ефективність розробленої моделі та вплив її застосування на захищеність та цілісність даних.

10. Таким чином, виконана робота являє собою комплексний підхід до управління персональними даними в освітній сфері, пропонуючи як теоретичні, так і практичні рішення для актуальних викликів діджиталізації.

РОЗДІЛ 3. РОЗРОБКА МЕТОДУ УПРАВЛІННЯ ПОТОКАМИ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ ОСВІТНЬОЇ СФЕРИ

3.1 Алгоритм впровадження анонімізації персональних даних стейкхолдерів діджиталізованої освіти

Як визначено в цій роботі раніше, навчальні заклади активно впроваджують технології для оптимізації навчальних процесів. Тому забезпечення конфіденційності та захисту персональних даних стейкхолдерів стає першочерговим завданням. Зроблено підготовчу роботу, яка дозволила б створити повноцінний метод інтеграції анонімізації даних у навчальному закладі. Ключовим елементом є саме розробка моделі анонімізації персональних даних учасників навчального процесу (рис 2.4). Беручи за основу цю модель, розроблено алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти. Алгоритм являє собою комплексний підхід до мінімізації ризиків, пов’язаних із витоком інформації, через структуровані процеси обробки та захисту даних. Алгоритм визначає кроки для ідентифікації, класифікації та анонімізації персональних даних учасників освітнього процесу, забезпечуючи безпеку даних незалежно від того, чи це студенти, викладачі або адміністрація закладу.

Робота з розробки такого алгоритму проводилась ітеративно. Насамперед розроблено загальний план впровадження анонімізації персональних даних стейкхолдерів діджиталізованої освіти:

1. Планування впровадження анонімізації персональної інформації учасників навчального процесу у діджитал систему менеджменту даних навчального закладу.
2. Визначення даних які навчальний заклад поширює або планує поширювати для кожного типу учасників навчального процесу (студенти, викладачі, адміністрація тощо).

3. Визначення які з поширюваних даних вважаються персональними та повинні бути захищені анонімізацією для усіх стейкхолдерів навчального процесу (телефон, прізвище, банківські дані тощо).

4. Ідентифікація зовнішніх платформ з якими взаємодіє або планує взаємодіяти навчальний заклад (адже з ними й будуть поширюватись певні дані).

5. Визначення алгоритму анонімізації для кожного поля об’єктів залучених в навчальному процесі (зазвичай найзручнішим варіантом буде токенізація зі збереженням формату).

6. Розробка стратегічної род мапи застосування анонімізації персональних даних до інтеграцій з зовнішніми навчальними платформами.

7. Розробка модуля анонімізації персональних даних стейкхолдерів навчального процесу.

8. Застосування анонімізації до інтеграцій навчального закладу з зовнішніми сервісами.

9. Завершення та створення звіту про виконані роботи й вплив змін на життєдіяльність навчального закладу як в контексті захисту інформації, так і в інших аспектах.

Оскільки тепер є високорівневий план анонімізації персональних даних стейкхолдерів діджиталізованої освіти можна рухатись далі. А найдетальніше описати кожен з пунктів. Отже, далі перший пункт. Планування впровадження анонімізації персональної інформації учасників навчального процесу у діджитал систему менеджменту даних навчального закладу:

1. Оцінка поточних процесів та потреб з поширення даних навчальним закладом. Найперше варто застосувати модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища в контексті поточного навчального закладу, щоб зрозуміти які ризики є найпріоритетнішими. Після цього, з метою визначення потреби та пріоритету підвищення рівня захищеності потоків даних необхідно застосувати модель інформаційної взаємодії та потоків даних

розроблену в цій роботі раніше. Якщо навчальний заклад планує перехід в хмарне середовище може бути застосована модель управління зберіганням даних для більш прийняття більш обґрунтованого рішення.

2. Розробка політик безпеки та конфіденційності персональних даних учасників навчального процесу. Тут потрібно керуватися раніше розробленими в цій роботі принципами мінімізації поширення персональних даних.

3. Створення загального плану впровадження анонімізації на основі розробленої моделі анонімізації персональної інформації.

Далі подано деталі стосовно визначення даних які навчальний заклад поширює або планує поширювати для кожного типу учасників навчального процесу:

1. Ідентифікація інформаційних об’єктів які поширює навчальний заклад (інформаційні об’єкти – діджитал сутності які представляють цифровий варіант стейкхолдера навчального процесу, як то викладач, студент тощо).

2. Дефініція полів кожного з інформаційних об’єктів (інформація яку несуть в собі інформаційні об’єкти, як то ім’я, прізвище, адреса).

Наступним є процес визначення які з поширюваних даних вважаються персональними та повинні бути захищені анонімізацією для усіх стейкхолдерів навчального процесу:

1. Формування переліку полів які вважаються персональною інформацією учасника навчального процесу і повинні бути захищені анонімізацією (для студентів це може бути ім’я, прізвище, телефон та інші, тоді як для викладачів до цього переліку додаються ще банківська інформація, адреса проживання, і так далі).

2. Поділ персональних даних на такі які мають бути анонімізовані в обов’язковому порядку та такі що є бажаними до анонімізації.

Далі ідентифікація зовнішніх платформ з якими взаємодіє або планує взаємодіяти навчальний заклад:

1. Формування списку типів платформ з якими взаємодіє чи планує взаємодіяти навчальний заклад (брокер даних, зовнішні сховища даних та інші).

2. Визначення найбільш критичних зовнішніх сервісів які використовує навчальний заклад для забезпечення ефективного навчального процесу.

Після цього має слідувати визначення алгоритму анонімізації для кожного поля об'єктів залучених в навчальному процесі:

1. Вивчення вимог до даних зовнішніх споживачів (вимоги щодо унікальності, формату тощо).

2. Визначення мінімального ступеня захищеності даних (чи допустимо певне поле токенізувати тим чи іншим способом).

3. Вибір оптимального алгоритму токенізації кожного з полів базуючись на вище отриманій інформації (вимоги споживачів, вимоги до захисту даних тощо)

Тепер деталі стосовно розробки стратегії застосування анонімізації персональних даних до інтеграцій з зовнішніми навчальними платформами:

1. Формування та відправка інформуючих листів представникам зовнішніх платформ, якщо такі потрібні. Або комунікація у більш відповідній формі, залежно від ситуації.

2. Узгодження потрібних деталей з представниками зовнішніх платформ, якщо виникають певні непорозуміння чи складнощі.

3. Розробка род мапи переходу до використання анонімізації персональних даних при їх поширенні з зовнішніми платформами (план переходу може бути загальним для всіх зовнішніх платформ за можливості, але за потреби може застосовуватись індивідуальний підхід у випадку виникнення певних складнощів у переході на анонімізовану взаємодію у контексті певної зовнішньої платформи).

Ну і тепер найголовніше, опис пункту розробки модуля анонімізації персональних даних стейкхолдерів навчального процесу:

1. Вивчення існуючої цифрової системи менеджменту інформації навчального закладу.

2. Розробка плану імплементації модуля анонімізації персональних даних.

3. Розробка плану інтеграції модуля анонімізації персональних даних в існуючу систему менеджменту інформації навчального закладу.

4. Імплементація модуля анонімізації персональних даних учасників навчального процесу.

5. Інтеграція розробленого модуля анонімізації з існуючою платформою менеджменту інформації навчального закладу.

5.1. Інтеграція з модулем внутрішнього менеджменту інформації навчального закладу (адмін-сторінка системи менеджменту інформації, яку зазвичай використовує адміністративний та викладацький персонал навчального закладу).

5.2. Інтеграція з API існуючої системи менеджменту інформації.

6. Тестування інтеграції новоствореного модуля анонімізації в існуючу інформаційну менеджмент систему навчального закладу.

7. Тестування існуючих інтеграцій навчального закладу з зовнішніми навчальними платформами з використанням анонімізації персональних даних учасників освітнього процесу.

Щодо застосування анонімізації для інтеграції навчального закладу з зовнішніми сервісами необхідними є такі підпункти:

1. Навчання персоналу користуватись новостворенim функціоналом.

2. Моніторинг та вдосконалення.

2.1. Створення процесу постійного моніторингу та регулярних перевірок для виявлення можливих вразливостей.

2.2. Внесення покращення на основі зворотного зв’язку і зміни регуляторних вимог.

І на завершення, обов’язково створюється звіт про виконані роботи та вплив змін на життєдіяльність навчального закладу як в контексті захисту інформації, так і в інших аспектах.

Далі, маючи доволі детально описані кроки по анонімізації персональних даних стейкхолдерів діджиталізованої освіти, виконано найголовніше завдання поставлене в

цьому підрозділі. Тобто створено детальний алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти:

1. Планування впровадження моделі анонімізації персональних даних:

1.1. Оцінка поточних процесів та потреб:

1.1.1. Збір відгуків викладачів, студентів та адміністрації щодо того, як дані використовуються та які проблеми можуть виникати з їх анонімізацією.

1.1.2. Визначення типів даних, що збираються, і способи їх зберігання, щоб зрозуміти обсяги роботи по інтеграції анонімізації.

1.1.3. Розробка матриці відповідальності для участі співробітників у процесі анонімізації даних.

1.2. Розробка політик безпеки та конфіденційності:

1.2.1. Розробка нових чи адаптація існуючих внутрішніх політик відповідно до норм GDPR чи інших актуальних актів законодавства.

1.2.2. Впровадження регулярних навчальних програм із захисту даних для співробітників.

1.2.3. Створення процедури з реагування на витоки даних та порушення політик безпеки.

1.3. Створення загального плану впровадження:

1.3.1. Планування проєктних етапів, ресурсів та вимірювальних показників успіху для кожного етапу впровадження.

1.3.2. Визначення ролей та обов’язків команд, залучених у процесі впровадження анонімізації.

1.3.3. Розробка комунікаційного плану, щоб забезпечити постійний обмін інформацією між зацікавленими сторонами.

2. Визначення даних, які поширює навчальний заклад:

2.1. Ідентифікація інформаційних об'єктів:

2.1.1. Проведення ревізії всіх існуючих систем, щоб виділити, які цифрові записи стосуються стейкхолдерів закладу.

2.1.2. Залучення відповідальних за дані осіб для ідентифікації та класифікації всіх релевантних інформаційних об’єктів.

2.2. Дефініція полів:

2.2.1. Створення детальної документації всіх полів, що містяться в інформаційних об’єктах, включаючи описові метадані для кожного поля.

2.2.2. Впровадження класифікаційної системи для легкого визначення, які поля є чутливими чи критичними з погляду безпеки.

3. Визначення персональних даних для захисту:

3.1. Формування переліку полів:

3.1.1. Сегментування учасників (студенти, викладачі та інші) для точної диференціації видів даних, що для них критичні.

3.1.2. Співпраця з юридичним та технічним відділами, щоб уточнювати, які поля підлягають захисту.

3.2. Поділ персональних даних:

3.2.1. Визначення даних які можуть бути менш чутливими та встановлення критеріїв бажаної анонімізації.

3.2.2. Встановлення формалізованих критеріїв, на базі яких визначається, які дані мають бути анонімізовані за будь-яких умов.

4. Ідентифікація зовнішніх платформ:

4.1. Формування списку типів платформ:

4.1.1. Складання детального списку всіх зовнішніх платформ, взаємодія з якими може включати передачу даних.

4.1.2. Оцінка IT-відділом поточних технологічних інтеграцій з зовнішніми платформами.

4.2. Визначення критичних сервісів:

4.2.1. Аналіз впливу кожної зовнішньої платформи на загальний процес навчання для визначення критичності.

4.2.2. Створення план управління ризиками на випадок, якщо критичні платформи зазнають збоїв або витоків.

5. Визначення алгоритму анонімізації:

5.1. Вивчення вимог до даних зовнішніх споживачів:

5.1.1. Аналіз вимоги та специфікації різних платформ, щоб зрозуміти які саме дані повинні передаватися в якому форматі.

5.1.2. Збір інформації щодо стандартів безпеки та протоколів обміну даними зовнішніх постачальників послуг.

5.1.3. Перегляд існуючих угод про рівень обслуговування (SLA) та оновлення їх відповідно до нових вимог до анонімізації.

5.2. Визначення мінімального ступеня захищеності даних:

5.2.1. Оцінка впливу різних методів анонімізації на якість і точність даних.

5.2.2. Розробка критеріїв для прийнятності токенізації чи інших методів анонімізації даних для кожного поля в контексті збереження якості даних.

5.2.3. Впровадження пілотного проєкту для оцінки ефективності різних підходів до анонімізації.

5.3. Вибір оптимального алгоритму токенізації:

5.3.1. Виконання порівняльного аналізу існуючих технологій токенізації, враховуючи ефективність, швидкість обробки та безпеку.

5.3.2. Перевірка що обраний алгоритм дозволяє зберігати функціональність системи без шкідливого впливу на робочі процеси.

5.3.3. Підготовка звітів про тестування різних алгоритмів і вибір найефективнішого для кожного виду даних.

6. Розробка стратегії застосування анонімізації:

6.1. Формування та відправка інформуючих листів:

6.1.1. Підготовка шаблонів листів, що чітко описують нові політики даних та наслідки анонімізації для зовнішніх платформ.

6.1.2. Планування зустрічей з ключовими зовнішніми партнерами для особистого представлення змін якщо такі потрібні.

6.1.3. Перевірка чи усі документи надіслано всім зацікавленим сторонам до початку впровадження.

6.2. Узгодження потрібних деталей:

6.2.1. Проведення консультації з представниками зовнішніх платформ, щоб вирішити будь-які непорозуміння чи складнощі за потреби.

6.2.2. Аналіз зворотного зв'язку від партнерів і уточнення технічних чи адміністративних нюансів.

6.3. Розробка род мапи переходу до анонімізації:

6.3.1. Створення детального плану переходу, який включатиме всі кроки й етапи впровадження анонімізації.

6.3.2. Врахування специфічних вимог та можливостей кожної платформи, з якою ведеться співпраця, для адаптації плану.

6.3.3. Увімкнення механізму зворотного зв'язку для внесення коригувань у процес переходу в разі виявлення перешкод.

7. Розробка модуля анонімізації даних:

7.1. Вивчення існуючої цифрової системи:

7.1.1. Проведення глибокого технічного аудиту існуючої системи менеджменту даних для ідентифікації змін, які потрібно внести для інтеграції анонімізації.

7.1.2. Визначення точок доступу до даних у системі для виявлення можливих вразливостей.

7.2. Розробка плану імплементації модуля:

7.2.1. Розробка покрокового плану дій з урахуванням ресурсів, часу та необхідних технічних засобів для успішної імплементації модуля.

7.2.2. Визначення ключових етапів реалізації проєкту, встановлення дедлайнів та відповідальних осіб для кожного завдання.

7.3. Розробка плану інтеграції:

7.3.1. Створення технічної специфікації для інтеграції модуля з існуючою системою менеджменту інформації навчального закладу, враховуючи всі необхідні зміни в архітектурі програмного забезпечення.

7.3.2. Проведення аналізу з технічними командами для узгодження деталей інтеграції та виявлення потенційних викликів.

7.4. Імплементація модуля анонімізації:

7.4.1. Використання методології Agile для виконання завдань поетапно, забезпечуючи гнучкість та швидке реагування на зміни.

7.4.2. Співпраця з розробниками та тестувальниками для впровадження і перевірки всіх компонентів модуля.

7.5. Інтеграція з існуючою системою:

7.5.1. Інтеграція з модулем внутрішнього менеджменту інформації:

7.5.1.1. Забезпечення збереження усіх існуючих функції управління даними, адаптувавши їх під новий стандарт анонімізації.

7.5.1.2. Тестування нового модуля у реальних сценаріях використання, щоб оцінити його вплив на навчальний і адміністративний процеси.

7.5.2. Інтеграція з API існуючої системи:

7.5.2.1. Розробка додаткової API версії для забезпечення сумісності зі сторонніми сервісами, які можуть читати дані системи.

7.5.2.2. Перевірка працездатності API після інтеграції для підтвердження стабільності та продуктивності.

7.6. Тестування інтеграції:

7.6.1. Застосування комплексних тестових сценаріїв, які симулюють різні види взаємодій з системою для перевірки коректності анонімізації.

7.6.2. Застосування стрес-тестів для оцінки як система справляється з підвищенням обсягів даних.

7.7. Тестування інтеграцій із зовнішніми платформами:

7.7.1. Здійснення тестових передач даних до всіх зовнішніх платформ, з якими підтримується взаємодія, для перевірки анонімізації.

7.7.2. Залучення представників зовнішніх платформ для незалежної перевірки та підтвердження правильності процесу анонімізації за потреби.

8. Застосування анонімізації:

8.1. Навчання персоналу:

8.1.1. Розробка комплексного навчального плану для всіх співробітників з детальним поясненням нових процесів та інструментів.

8.1.2. Застосування інтерактивних навчальних методів, включаючи симуляції та реальні кейси для підвищення ефективності навчання.

8.2. Моніторинг та вдосконалення:

8.2.1. Створення процесу моніторингу:

8.2.1.1. Впровадження системи аналітики для постійного відстеження ефективності анонімізації та виявлення потенційних вразливостей.

8.2.1.2. Регулярні оновлення і перевірки звітів про безпеку, для швидкого реагування на будь-які збої або загрози.

8.2.2. Внесення покращень:

8.2.2.1. Збір зворотного зв'язку від персоналу та залучених стейкхолдерів для постійного вдосконалення процесів.

8.2.2.2. Врахування змін в законодавстві для своєчасного оновлення політик та процедур анонімізації.

9. Завершення впровадження анонімізації:

9.1. Створення детального звіту про всі етапи впровадження анонімізації.

9.2. Аналіз впливу нових процесів на ефективність і безпеку роботи учасників освітнього процесу.

9.3. Підготовка рекомендацій для майбутніх вдосконалень та потенційних розширень системи анонімізації.

Підсумовуючи, розроблено алгоритм анонімізації персональних даних стейкхолдерів у діджиталізованій освіті, який ґрунтується на моделі анонімізації персональних даних при інформаційній взаємодії в освітньому середовищі. Цей алгоритм деталізує кожен етап процесу, від початкового планування до кінцевої реалізації та моніторингу, що дозволяє закладам освіти ефективно захищати персональні дані своїх учасників. Впровадження цього алгоритму гарантує дотримання сучасних стандартів безпеки та конфіденційності, зберігаючи при цьому високу якість та цілісність навчального процесу. Завдяки чітко визначеним крокам, заклади можуть не лише убезпечити дані, а й зміцнити довіру своїх студентів та співробітників до цифрових технологій в освіті.

3.2 Алгоритм впровадження деанонімізації персональних даних стейкхолдерів діджиталізованої освіти

Як зазначалось раніше захист інформації та конфіденційності даних учнів і викладачів набуває особливого значення. Розроблений алгоритм анонімізація даних є важливим та корисним інструментом для забезпечення безпеки особистої інформації, проте існують ситуації, коли може виникнути потреба в деанонімізації. Це може бути пов’язано з необхідністю проведення наукових досліджень, моніторингом якості освіти, а також відповідністю законодавчим вимогам щодо збереження та обробки даних.

Забезпечення можливості деанонімізації даних може бути критично важливим для навчальних закладів та зовнішніх освітніх сервісів, які використовують ці дані для вдосконалення своїх програм, аналізу успішності студентів чи виявлення тенденцій у навчальному процесі. Наприклад, для розробки індивідуальних маршрутів навчання або психологічної підтримки важливо мати доступ до первинних даних, які дозволяють краще розуміти потреби та особливості учнів.

Саме тому навчальні заклади прагнуть забезпечити як конфіденційність, так і, у певних випадках, доступність персональної інформації для підтримки якісного освітнього процесу. Для цього необхідно забезпечити відповідний механізм деанонімізації персональних даних в освітньому середовищі.

З цією метою розроблено алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти націлений на створення інструменту для безпечного відновлення доступу до даних, враховуючи правові, етичні та технічні аспекти. Він дозволяє ідентифікувати, які дані необхідно знову зробити доступними, розробити відповідні технологічні рішення і забезпечити інтеграцію цих рішень в існуючу інфраструктуру даних навчального закладу. Цей алгоритм служить дорожньою картою для навчальних закладів, які прагнуть підтримувати баланс між автономністю даних і забезпеченням їх доступності для навчальних і організаційних цілей.

Отже, нижче дано перелік кроків алгоритму деанонімізації персональних даних стейкхолдерів діджиталізованої освіти:

1. Планування впровадження сервісу деанонімізації персональної інформації учасників навчального процесу у діджитал систему менеджменту даних навчального закладу. Розробка плану механізму деанонімізації має базуватись на раніше створеній моделі деанонімізації персональних даних стейкхолдерів освітнього процесу.

2. Визначення типів персональних даних стейкхолдерів освітнього процесу які потребують деанонімізації.

3. Створення сервісу деанонімізації персональних даних.

4. Інтеграція сервісу деанонімізації персональної інформації учасників навчального процесу у діджитал систему менеджменту даних навчального закладу

5. Завершення впровадження сервісу деанонімізації персональної інформації.

Далі деталізовано кожен з кроків цього плану. Нижче описано крок планування впровадження сервісу деанонімізації:

1) Оцінка поточних потреб та вимог:

а) визначення цілей деанонімізації та її ролі у навчальному процесі;

b) залучення стейкхолдерів, щоб визначити їхні очікування та вимоги.

2) Аналіз правових та етичних аспектів:

a) оцінка законодавчих обмежень щодо відновлення доступу до персональних даних;

b) розгляд етичних питань, пов’язаних із деанонімізацією, і їх впливу на конфіденційність.

3) Розробка плану проєкту:

a) вибір часових рамок, ресурсів та ключових етапів для реалізації сервісу;

b) визначення відповідальності команди проєкту та створення графіка зустрічей.

Наступним кроком є визначення типів персональних даних для деанонімізації:

1) Ідентифікація необхідних даних для деанонімізації:

a. виявлення категорій даних, які потребують відновлення доступу для навчальних або адміністративних цілей;

2) Аналіз ризиків і переваг деанонімізації:

a. оцінка ризиків, пов’язаних із відновленням доступу до персональних даних;

b. аналіз потенційних переваг для навчального процесу або адміністрації.

3) Класифікація даних за пріоритетністю:

a. встановлення пріоритету деанонімізації для різних типів даних залежно від їхньої важливості та використання.

Третій крок – це створення сервісу деанонімізації персональних даних, тож далі описано пункти які містять цей етап:

1) Розробка архітектури сервісу:

a) визначення технічної архітектури сервісу, включаючи вибір платформи та технологій.

2) Розробка програмного забезпечення:

а) створення алгоритмів і програмних модулів для відновлення персональних даних.

3) Перевірка функціональності:

а) проведення тестів для перевірки коректності та безпеки роботи сервісу.

4) Розробка заходів безпеки:

а) впровадження механізмів контролю доступу для запобігання несанкціонованому використанню сервісу.

Передостаннім кроком алгоритму є інтеграція сервісу з діджитал системою менеджменту даних. Ось перелік дій які входять у цей пункт:

1) Аналіз існуючої системи:

а) оцінка поточної IT-інфраструктури для визначення необхідних змін для інтеграції.

2) Впровадження технічних змін:

а) модифікація існуючих систем для інтеграції з новим сервісом.

3) Тестування інтеграції:

а) перевірка роботи сервісу в умовах реальних дій для виявлення потенційних проблем.

4) Навчання користувачів:

а) проведення тренінгів для співробітників щодо використання нового сервісу.

Останній крок – завершення впровадження сервісу деанонімізації:

1) Оцінка впровадження:

а) аналіз результатів впровадження та збір відгуків від користувачів.

2) Документування процесів:

а) розробка інструкцій та керівництво для подальшого використання та технічної підтримки.

3) Оцінка впливу на процеси закладу:

а) визначення, як деанонімізація впливає на навчальний процес та адміністративні процеси.

Підсумовуючи, у цьому підрозділі представлено алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти, який спрямований на безпечне та санкціоноване відновлення доступу до персональних даних в освітньому середовищі. Алгоритм включає п’ять важливих кроків. Застосування яких дозволяє врахувати правові, етичні та технічні аспекти, забезпечуючи баланс між збереженням конфіденційності та доступністю даних. Завдяки впровадженню таких інструментів навчальні заклади зможуть ефективніше управляти даними для покращення як навчального процесу, так і адміністративних процедур.

3.3 Метод анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти

3.3.1 Схема впровадження анонімізації та деанонімізації персональних даних в інформаційному просторі діджиталізованої освіти

Не одноразово зазначалось що питання захисту персональних даних стає все більш актуальним. Але як видно з проведених досліджень важливо не втрачати баланс між закритістю системи та її функціональністю. У цьому контексті, метод анонімізації та деанонімізації персональних даних відіграє ключову роль у забезпеченні конфіденційності та доступності інформації. Для ефективної взаємодії елементів інформаційного простору діджиталізованої освіти розроблено кілька важливих моделей та алгоритмів. На першому етапі створено модель захисту персональних даних здобувачів освіти через їхню анонімізацію, що дозволяє знизити ризики несанкціонованого використання даних. Додатково, модель деанонімізації персональних даних стейкхолдерів навчального процесу надає можливість безпечного відновлення доступу до потрібної інформації, зберігаючи баланс між конфіденційністю та вимогами до доступності. Крім цих моделей, розроблено алгоритм анонімізації, що

націлений на методичне та безпечне перетворення даних, і алгоритм деанонімізації, який забезпечує безпроблемну інтеграцію в існуючу інформаційну інфраструктуру закладів освіти. Всі ці елементи спільно формують основу для ефективного управління інформаційним простором, де дані використовуються з дотриманням найвищих стандартів безпеки та етики.

Отже, маючи твердий фундамент, почато розробку методу анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти. Першим кроком стало створення плану впровадження підтримки анонімізації та деанонімізації навчальним закладом. На схемі (рис. 3.1) зображено послідовність таких кроків.

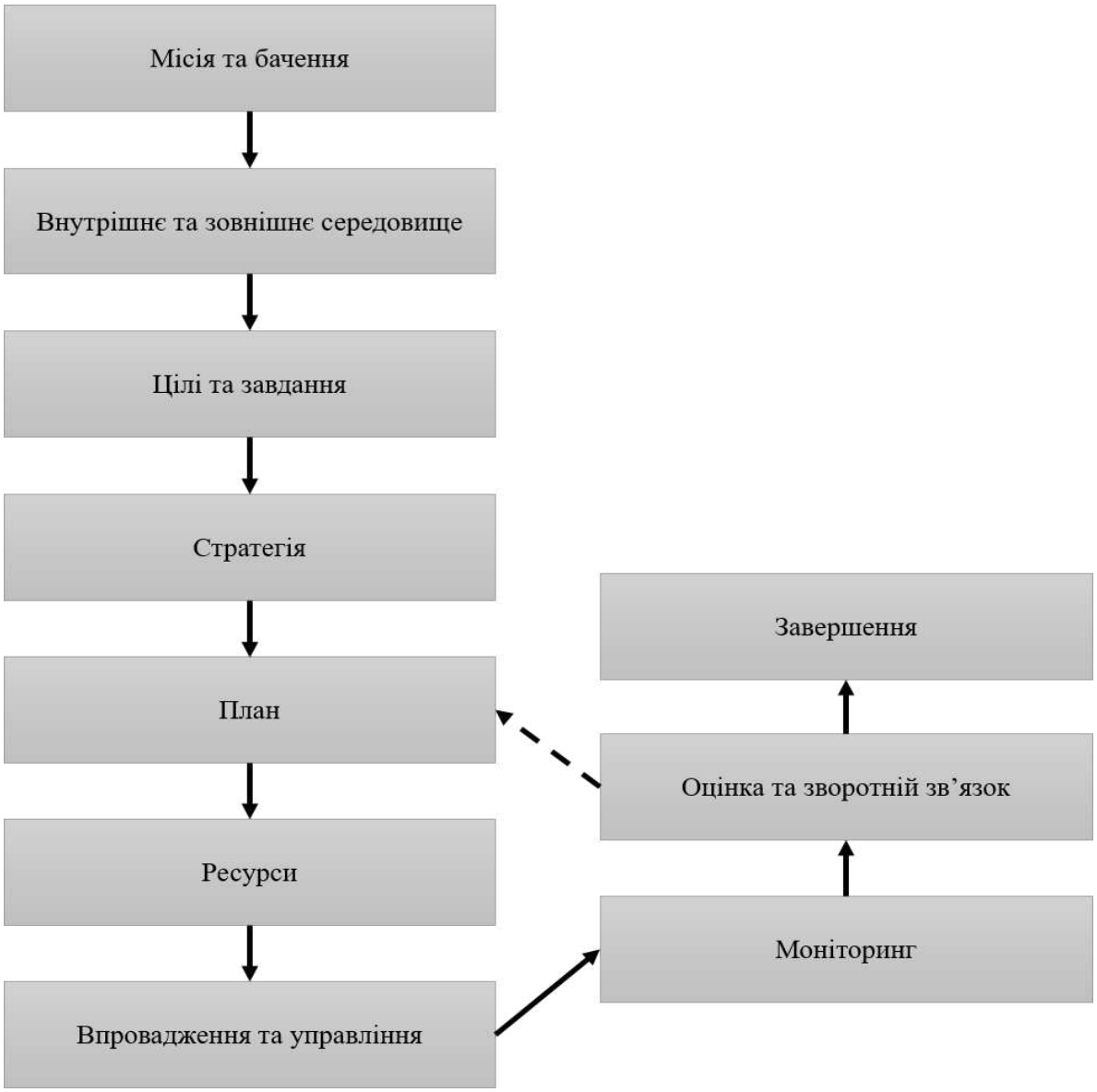

Рис. 3.1. Схема впровадження анонімізації та деанонімізації персональних даних в інформаційному простору діджиталізованої освіти

Для кращого розуміння схеми далі детально описано кроки зображені на ній. Також дано деталізацію по кожному з них.

Отже, першим кроком є визначення місії та бачення. Місія – це фундаментальне твердження про те, чим займається освітня організація, яка її основна мета і кого вона прагне обслуговувати. Місія повинна бути зрозумілою і надихаючою, задаючи напрямок для всіх дій. Місія повинна пояснювати для чого навчальному закладу потрібно впроваджувати анонімізацію персональних даних. Адже іноді виявляється, що

як малі, так і великі організації витрачають неймовірні ресурси на речі які їм не потрібні й не збігаються зі шляхом та принципами які були закладені в бізнес чи їх основу під час його створення. Розуміючи місію, потрібно сформувати бачення. Тобто уявлення про те, якою організація хоче бачити себе в майбутньому. Це додасть ясності стосовно того, яке місце впровадження анонімізації має в майбутньому навчального закладу. А також допоможе надихнути та мотивувати працівників досягати амбітних цілей.

Далі проводиться аналіз внутрішнього та зовнішнього середовища (SWOT-аналіз) [171]. Тут все очевидно та просто. Внутрішній аналіз – ідентифікація сильних (Strengths) та слабких (Weaknesses) сторін організації, таких як ресурси, процеси, компетенції. Зовнішній аналіз – вивчення можливостей (Opportunities) та загроз (Threats), що випливають з ринку, конкурентного середовища, економічних умов. Це допоможе зрозуміти як краще можна імплементувати та застосувати анонімізацію у діджитал взаємодії освітньої організації з іншими зовнішніми платформами.

Після цього потрібно встановити цілі та завдання. Цілі – це довгострокові кінцеві результати, яких організація прагне досягти в контексті анонімізації даних. Вони повинні відповідати критеріям SMART: бути конкретними (Specific), вимірюваними (Measurable), досяжними (Achievable), релевантними (Relevant) та обмеженими в часі (Time-bound) [172]. Деталізовані кроки чи підцілі, необхідні для досягнення основних цілей це і будуть самі завдання.

Далі слідує розробка стратегії. Формулювання стратегічних ініціатив і напрямків які повинні сприяти впровадженню нових технологій і вдосконалення існуючого функціоналу в контексті анонімізації та деанонімізації персональної інформації стейкхолдерів навчального процесу.

Наступний пункт – розробка плану дій. Маючи стратегію, цілі та завдання, потрібно створити конкретний план заходів із зазначенням відповідальних осіб, необхідних ресурсів та часових рамок для кожного напрямку роботи.

Маючи план, потрібно виконати розподіл ресурсів. Необхідно виконати оцінку наявних ресурсів і визначити потреби у додаткових ресурсах (людських, матеріальних, фінансових).

Тепер найголовніша частина, а саме впровадження та управління. Оскільки уже є готовий план дій та розподілені ресурси, потрібно, слідуючи розробленому плану, виконувати поставлені завдання. Необхідно визначити відповідальних за реалізацію, налагодити чіткий контроль виконання і коригування курсу при виникненні відхилень.

Але як зрозуміти чи робота іде по плану, та й взагалі що відбувається з реалізацією проєкту. Моніторинг та оцінка, саме це і є контролюючим інструментом виконання наміченого плану. Важливим є встановлення інструментів та критеріїв оцінки прогресу (ключових показників ефективності, KPI) для постійного відстеження виконання плану. Відповідно повинна проводитись оцінка відповідності фактичного виконання плану запланованим показникам.

Наступний пункт – оцінка та зворотний зв’язок. Мається на увазі регулярний перегляд результатів і виконаних дій з метою отримання зворотного зв’язку. Цей процес дозволяє вносити необхідні зміни, вдосконалювати стратегію та забезпечувати постійний розвиток організації.

І останній крок – завершення. Підсумкова оцінка всього процесу стратегічного планування, що включає перегляд досягнутих цілей і цілісного виконання стратегії. Це етап, на якому узагальнюються уроки, які організація вивчила в ході реалізації плану, і забезпечується передача знань всередині команди. Завершення передбачає формалізацію набутих знань та підготування організації до наступного циклу стратегічного планування, включаючи підзвітність і документацію для майбутньої діяльності.

3.3.2 Метод анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти

Розробивши усі необхідні моделі та алгоритми, створено блок-схему анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти (рис. 3.2).

Рис. 3.2. Блок-схема алгоритму анонімізації персональних даних учасників навчального процесу

Короткий опис блок-схеми. Спершу відбувається введення даних про інтенсивність потоків даних навчального закладу та кількість даних, які проходять через них. На основі цих даних виконується аналіз потоків даних освітньої установи та будується модель інформаційної взаємодії та потоків даних у діджиталізованій освітній сфері як це показано в другому розділі цієї роботи. Наступним кроком є визначення необхідності переходу у хмарне середовище, для цього застосовується розроблена раніше модель управління зберіганням потоків даних освітнього середовища. На основі проведеного аналізу визначається чи потрібно застосовувати дії направлені на підвищення рівня безпеки потоків даних *(2.3)*. Якщо отримане значення рівне нулю, то такі дії виконувати не потрібно. В іншому випадку такі дії є необхідними, а отже, виконується ідентифікація ризиків витоку персональних даних як показано в другому розділі (модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища). На основі отриманих даних виконується впровадження анонімізації. Після впровадження анонімізації перевіряється чи усі потоки даних є безпечними. Якщо так, то робота завершена. Якщо ні – проводиться наступна ідентифікація ризиків і застосовується анонімізація до потоків даних які лишились небезпечними.

Створено блок-схему алгоритму анонімізації персональних даних учасників навчального процесу. Також, розроблено загальний план імплементації та впровадження анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти. Тож далі потрібно зробити опису бізнес-процесів пов’язаних з впровадженням анонімізації та деанонімізації персональних даних. Спершу описано бізнес-процеси пов’язані з анонімізацією. За основу взято розроблений раніше алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти (3.2).

Тож першим кроком в цьому алгоритмі є планування впровадження моделі анонімізації персональних даних. На рис. 3.3 побудована схема бізнес-процесу

планування впровадження анонімізації персональних даних учасників з входами та виходами.

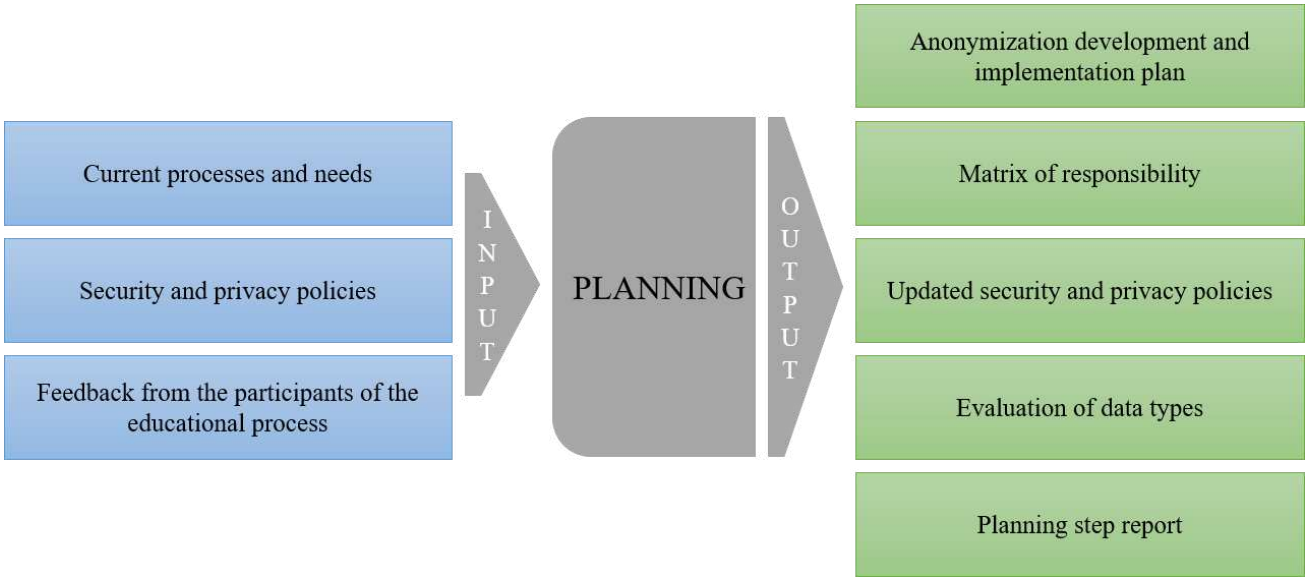

Рис. 3.3. Входи та виходи бізнес-процесу планування впровадження анонімізації персональних даних учасників

На цій схемі зображено наступні елементи які є ключовими для виконання бізнес-процесу планування і являються його входами:

1) Поточні процеси організації та її потреби. Тут мається на увазі, які є уже налагоджені або не налагоджені процеси в навчальному закладі. Такі як процес інтеграції з зовнішніми навчальними платформами, навчальні процеси, процеси пов’язані з моніторингом та якістю тощо. Стосовно потреб, важливою є інформація пов’язана з тим що саме вимагається для забезпечення якісного навчання, які є прогалини з точки зору безпеки даних які потрібно заповнити та інше.

2) Захист інформації та політики конфіденційності. Важливо отримати повне розуміння які вже є встановлені політики у сфері захисту інформації та конфіденційності навчального процесу в освітній установі.

3) Зворотний зв’язок від учасників навчального процесу. Звісно в першу чергу ідеться про адміністрацію та викладацький склад навчального закладу.

Маючи опис вхідних даних бізнес-процесу планування для повної картини, потрібно описати, що очікується на виході цього бізнес-процесу. Тож далі перераховано головні складові переліку вихідних елементів:

1) План розробки та впровадження анонімізації в існуючу діджитал менеджмент систему навчального закладу. Це найважливіший пункт. Складаючи план робіт, важливо детально пропрацювати кожен з етапів як розробки, так і впровадження нового функціоналу в уже існуючий інструмент.

2) Матриця відповідальності. Потрібно чітко визначити яка команда, а також її учасники за що відповідають. Також важливо зазначити яку роль повинен відігравати кожен з учасників у той чи інший момент, виконуючи свою частину роботи у проєкті.

3) Оновлені політики з конфіденційності та захисту інформації. Оскільки суть роботи це саме покращення рівня захищеності даних учасників навчального процесу, то у першу чергу потрібно розуміти цілі. Тобто розробити чіткі вимоги до безпеки, яким далі потрібно слідувати.

4) Оцінки типів даних які використовуються навчальним закладом в контексті інтеграції з зовнішніми навчальними платформами. Зазвичай таких типів не багато. Ось кілька типів інформаційних об’єктів які тут мають місце: Студент, Викладач, Курс, Предмет та інші.

5) Звіти по виконаній роботі. Звісно після виконання всіх робіт потрібно сформувати звіти. Адже досвід та напрацьовані знання можна буде використати для аналізу проведеної роботи та покращення наступних кроків чи оптимізації та полегшення виконання схожих проєктів.

Переходячи за розробленим алгоритмом анонімізації персональних даних учасників навчального процесу до наступного кроку потрібно зробити аналіз даних які навчальний заклад поширює з зовнішніми споживачами в контексті взаємодії з ними для отримання послуг які забезпечать покращення якості навчання. Тож на рис. 3.4 зображено входи та виходу бізнес-процесу аналізу таких даних.

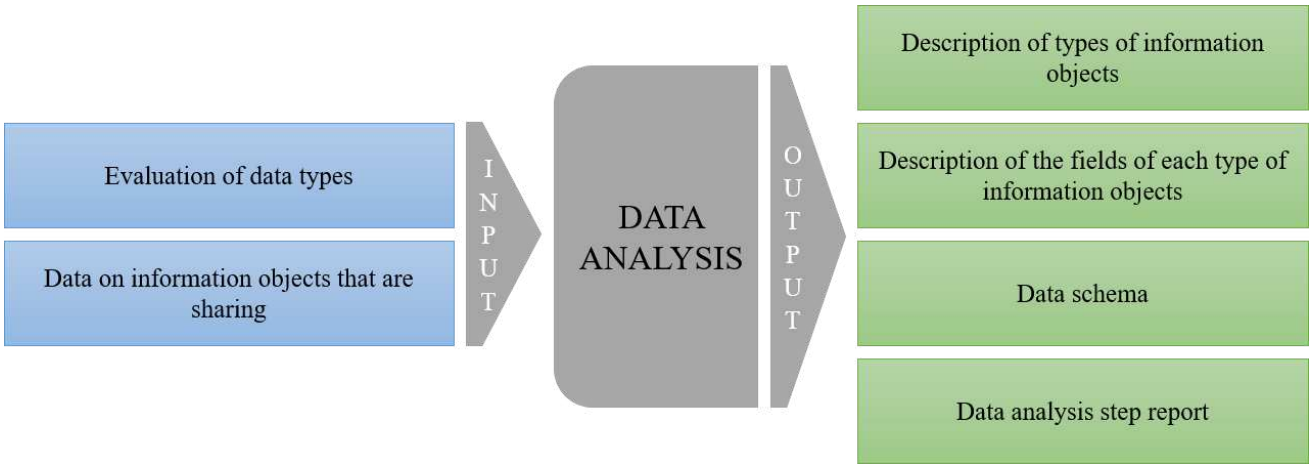

Рис. 3.4. Входи та виходи бізнес-процесу визначення даних які навчальний заклад поширює

Входи цього бізнес-процесу:

1) Раніше зроблена оцінка типів даних навчального закладу. Якщо заклад є доволі діджиталізованим, то таких типів може бути трохи більше. Ось кілька прикладів: дані про студентів, викладачів, оцінки, відвідування і багато іншого.

2) Дані про те які інформаційні об’єкти навчальний заклад поширює з зовнішніми сервісами. Зазвичай цей перелік є дуже схожий у кожного навчального закладу, ось кілька з них: Студент, Курс, Викладач тощо.

Маючи усі потрібні дані, визначено, що очікується на виході як результат виконання даного бізнес-процесу:

1) Повний опис інформаційних об’єктів навчального закладу. Маються на увазі, звісно, цифрові інформаційні об’єкти. Саме по таких даних потрібно скласти чітку та вичерпну документацію.

2) Повний опис атрибутів кожного з раніше визначених інформаційних об’єктів. Важливо крім розробки документації з переліку типів інформаційних об’єктів детально та зрозуміло описати кожен атрибут усіх інформаційних об’єктів.

3) Схема даних навчального закладу. Не всі навчальні заклади мають централізовану базу даних і іноді скласти таку схему це не зовсім проста робота. Але

якщо є одна або кілька цифрових баз даних які використовує навчальний заклад, то скласти таку схему не можна.

4) Звіти про виконання робіт. Оскільки виконано серйозний аналіз та опис типів інформаційних об’єктів навчального закладу, то й отримано чимало нового досвіду, який потрібно зафіксувати та в майбутньому детально вивчити.

Маючи готовий опис різних типів інформаційних об’єктів та їх полів з якими потрібно буде мати справу, можна перейти до наступного кроку. А саме до аналізу цих об’єктів в розрізі персональності та приватності. Тобто потрібно встановити які з цих об’єктів належать до таких, які несуть в собі персональну інформацію, а також які з їх атрибутів потребують захисту. Тож на рис. 3.5 зображено схему саме такого бізнес-процесу.

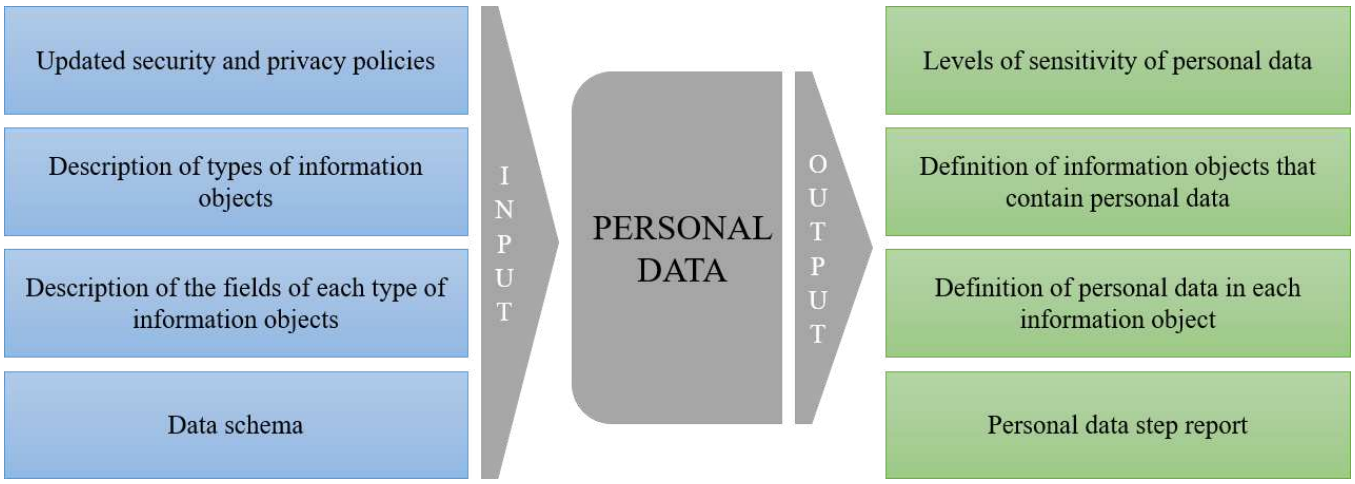

Рис. 3.5. Входи та виходи бізнес-процесу визначення які з поширюваних даних вважаються персональними та повинні бути захищені анонімізацією

Виокремлено входи та виходи бізнес-процесу визначення які з поширюваних даних вважаються персональними та повинні бути захищені анонімізацією:

1) Оновлені політики безпеки. Як уже зазначалось вище на етапі планування оновлено та доповнено вимоги до інформаційної безпеки. На поточному кроці вони є

надзвичайно важливими. Адже саме вони будуть вказівниками у процесі визначення які дані повинні бути захищені анонімізацією, а які ні.

2) Опис інформаційних об’єктів навчального закладу. На попередньому етапі була складена вичерпна документація таких об’єктів тож вона стане основою для поточного кроку.

3) Опис атрибутів інформаційних об’єктів. Ці дані сильно зв’язані з попереднім пунктом і доповнюють його.

4) Схема даних. Для правильної оцінки та визначення вимог до даних потрібне загальне бачення усієї картини. Саме для цього і потрібна така інформація.

Результатом виконання цього бізнес-процесу, тобто виходами процесу є:

1) Рівні чутливості персональних даних. Потрібно визначити які існують рівні чутливості персональних даних і зробити чітку документацію з вичерпними вимогами до об’єктів кожного з рівнів та їх атрибутів.

2) Визначення які інформаційні об’єкти несуть в собі чутливі персональні дані. Потрібно провести аналіз описаних раніше типів інформаційних об’єктів та визначити чи є такий об’єкт носієм персональних даних.

3) Визначення які саме атрибути інформаційних об’єктів несуть в собі чутливі персональні дані. Результатом роботи має бути документування які з атрибутів кожного з таких інформаційних об’єктів є персональною інформацією.

4) Підсумки та звіти про виконану роботу. Провівши усі необхідні роботи передбачені даним бізнес-процесом, потрібно зберегти отриманий досвід та знання.

Слідуючи в розробленому попередньо алгоритмі анонімізації персональних даних, потрібно зробити аналіз зовнішніх платформ з якими взаємодіє заклад. На рис. 3.6 зображено схему саме цього бізнес-процесу.

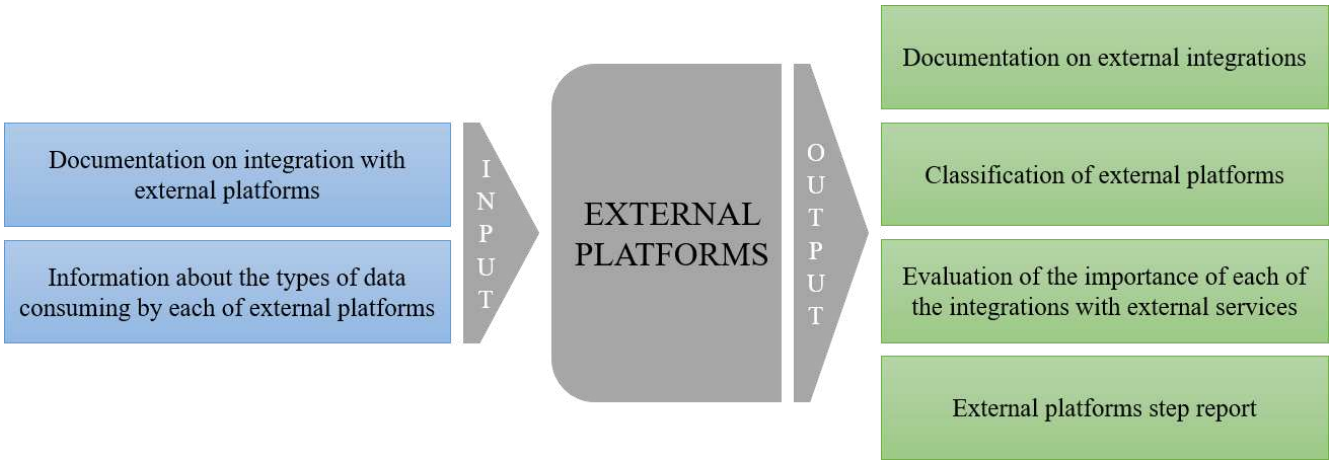

Рис. 3.6. Входи та виходи бізнес-процесу ідентифікації зовнішніх платформ

Входи бізнес-процесу ідентифікації зовнішніх платформ:

1) Документація по інтеграції навчальної установи з зовнішніми сервісами. Не завжди є достатньо такої документації у навчальних закладах. Але все ж потрібно зібрати усю можливу інформацію пов’язану з цим.

2) Інформація про типи даних які споживає кожна з платформ. Якщо у самому закладі нема такої документації, доведеться аналізувати усі існуючі інтеграції та складати перелік на старті цього етапу.

3) Дано визначення того що очікується як результат бізнес-процесу ідентифікації зовнішніх платформ:

1) Документація на зовнішні платформи з якими взаємодіє навчальний заклад. Точніше не зовсім на платформи, а більше на інтеграції. Потрібно проаналізувати кожну з таких взаємодій та розгорнуто описати. Адже далі потрібно буде зрозуміти чи дійсно установі потрібно така інтеграція і наскільки вона є критичною для забезпечення високого рівня освіти та ефективності навчання.

2) Класифікація та короткий опис зовнішніх платформ з точки зору використання їх сервісів навчальним закладом. Потрібно зробити чітку градацію платформ за різними типами та цілями застосування їх сервісів навчальним закладом до освітнього процесу.

3) Оцінка важливості кожної інтеграції з зовнішніми навчальними платформами. Тепер про найважливіше на поточному етапі. Потрібно, використовуючи отриману раніше інформацію, оцінити важливість кожної інтеграції, враховуючи усі виявлені раніше аспекти.

4) Звіти про виконані дії та їх результат. Потрібно задокументувати отримані знання як і стосовно результатів виконаної роботи, так і знання та досвід напрацьовані саме під час виконання цієї роботи.

Розроблені способи анонімізації повинні враховувати усі види інформаційних об’єктів які були визначені як такі що несуть в собі персональну інформацію. А також забезпечувати надійний захист усіх вразливих атрибутів цих об’єктів. На рис. 3.7 продемонстровано входи та виходи цього бізнес-процесу.

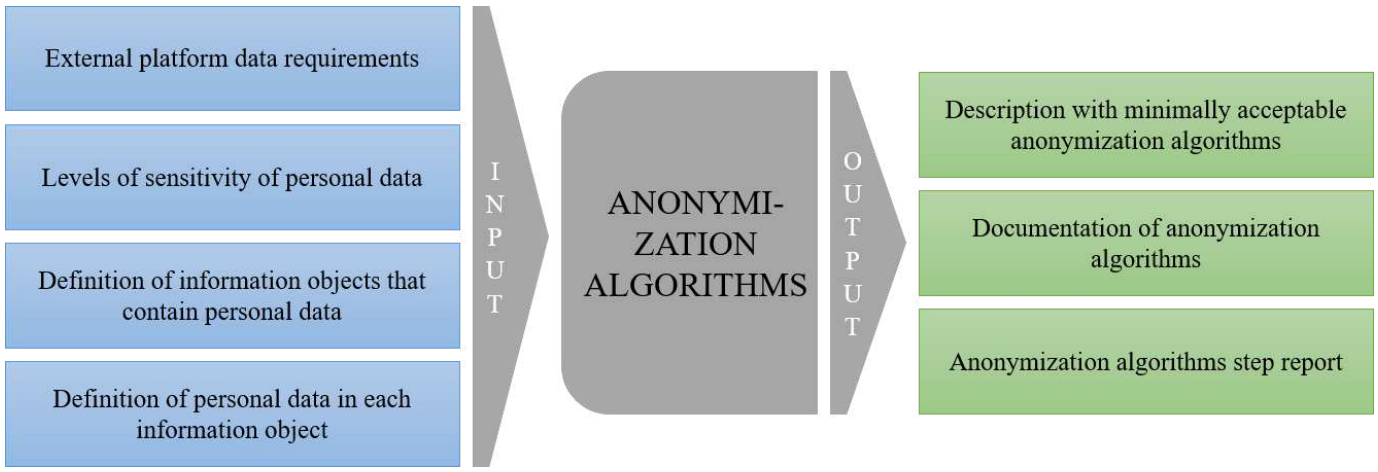

Рис. 3.7. Входи та виходи бізнес-процесу визначення алгоритму анонімізації

Входи бізнес-процесу визначення алгоритму анонімізації зображеного на цій схемі:

1) Вимоги зовнішніх навчальних платформ до даних. Такі дані можна отримати з бази знань навчального закладу. Але все одно потрібно також пошукати такі вимоги у документації самих зовнішніх навчальних платформ. Якщо така інформація є

лише в закритому доступі, то потрібно звернутись за нею до представників клієнтської підтримки таких сервісів.

2) Рівні чутливості персональних даних. Раніше розроблено таку документацію. Тож саме тут її й потрібно застосувати.

3) Документація з визначенням які інформаційні об’єкти несуть в собі персональну інформацію. На основі цих даних і буде проводитись робота з визначення які дані потрібно анонімізувати.

4) Визначення які з атрибутів інформаційних об’єктів є персональними даними й потребують певного рівня захищеності. Ця інформація дасть чіткіше розуміння що саме в інформаційних об’єктах потрібно анонімізувати і яким чином.

Маючи перелік вхідних даних, описано виходи бізнес-процесу визначення алгоритму анонімізації:

1) Опис мінімально прийнятних алгоритмів анонімізації. Оскільки не всі дані є однаково чутливими, то й захищати їх можна різними способами. Тому саме мінімальні вимоги до кожного виду даних потрібно розробити на даному етапі.

2) Документація з алгоритмів анонімізації. Необхідно зробити чіткий та логічний вибір алгоритмів анонімізації кожного з атрибутів інформаційних об’єктів які підлягають анонімізації. Робити, звісно, це потрібно з урахуванням вимог зовнішніх платформ до даних (їх формату, розміру тощо).

3) Звітність. Закінчивши виконання усіх обов’язкових пунктів пов’язаних з цим процесом, потрібно зберегти отримані знання та досвід.

Застосовуючи алгоритм анонімізації та рухаючись за розробленими вище методичними вказівками, на цей час буде у наявності уся необхідна інформація для ініціалізації процесу імплементації анонімізації персональних даних в інформаційному просторі діджиталізованої освіти. Але насправді потрібно зробити ще одну підготовчу роботу. А саме потрібно розробити стратегію застосування анонімізації персональних даних. Адже, маючи розуміння, які дані навчальний заклад поширює і що з таких даних є персональною інформацією, а також знаючи потреби для інтеграції з зовнішніми

платформами, потрібно розробити род мапу застосування анонімізації до цих інтеграцій. На рис. 3.8 зображено саме цей бізнес-процес.

Рис. 3.8. Входи та виходи бізнес-процесу розробки стратегії застосування анонімізації персональних даних для інтеграцій з зовнішніми навчальними платформами

Входи бізнес-процесу розробки стратегії застосування анонімізації персональних даних для інтеграцій з зовнішніми навчальними платформами:

1) План розробки та впровадження модуля анонімізації. Оскільки, розробляючи план, уже передбачено й описано в ньому процес інтеграції нового функціоналу, то це стане основою для розробки повної стратегії впровадження анонімізації даних учасників навчального процесу у контексті інтеграції з зовнішніми сервісами.

2) Оновлені політики захисту інформації та конфіденційності. Ця інформація потрібна як фундамент майбутньої стратегії. Адже, плануючи впровадження нового сервісу анонімізації та задовольняючи потреби споживачів даних, обов’язково потрібно враховувати аспекти захисту інформації.

3) Документація за зовнішні платформи. Розробляючи род мапу впровадження нового функціоналу, який стосується багатьох зовнішніх стейкхолдерів, очевидно, що необхідно врахувати їхні вимоги до даних та і загалом до інтеграції з освітньою установою. Тому важливо мати повну та вичерпну документацію стосовно цього перед початком роботи.

Маючи опис входів бізнес-процесу розробки стратегії застосування анонімізації, окреслимо виходи бізнес-процесу:

1) Род мапа застосування анонімізації до інтеграцій з зовнішніми навчальними платформами. По суті, це карта яка в майбутньому вказуватиме куди потрібно рухатись і які робити кроки для досягнення повного впровадження анонімізації до інтеграції з зовнішніми споживачами даних. Саме це і є головною ціллю цього бізнес-процесу.

2) Звіти про виконану роботу. Потрібно зібрати та впорядкувати всю інформацію про виконання робіт. Вона може бути використана для аналізу та покращенню певних аспектів поточного проєкту або наступних проєктів.

І от, нарешті настав найважливіший етап. Тепер справді можна приступити до безпосередньо розробки сервісу анонімізації персональних даних стейкхолдерів навчального середовища. Цей процес є доволі трудомістким, але на виході буде створено уже сам інструмент захисту персональної інформації. Тож на рис. 3.9 зображено схему такого бізнес-процесу.

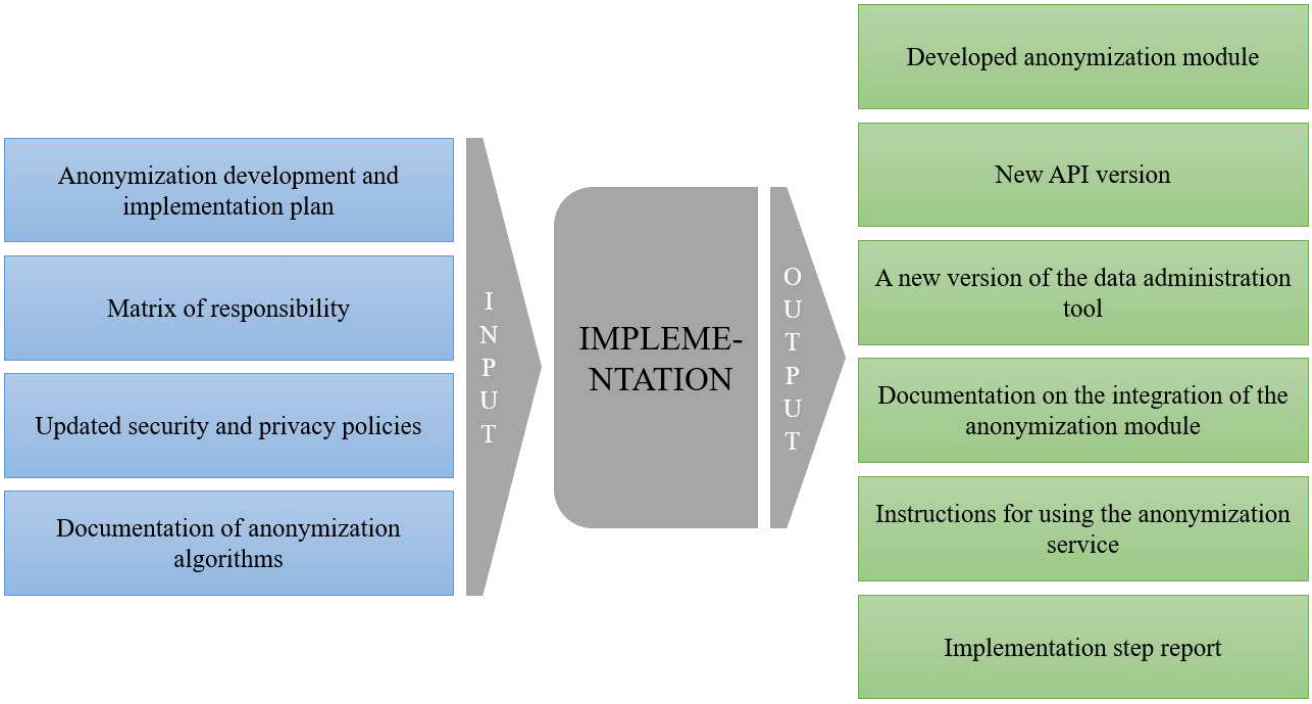

Рис. 3.9. Входи та виходи бізнес-процесу розробки модуля анонімізації персональних даних

Кроки які потрібно виконати на цьому етапі чітко описані в розробленому раніше алгоритмі анонімізації персональної інформації учасників навчального процесу. Але для розуміння цього бізнес-процесу краще, дано детальне визначення його входів:

1) План розробки та впровадження анонімізації. Розробка, моніторинг, контроль якості та багато іншого повинно відбуватись за визначеним алгоритмом та в контексті досягнення поставлених цілей. Саме ці аспекти і містяться у розробленому плані.

2) Матриця відповідальності.

3) Оновлені політики захисту інформації та конфіденційності. Як і впродовж усіх інших бізнес-процесів тут потрібно роблячи якісь рішення та імплементуючи їх постійно звірятись з вимогами до інформаційної безпеки.

4) Документація стосовно алгоритмів анонімізації інформаційних об’єктів та їх атрибутів. Маючи цю інформацію, слід приступити до її використання. Тобто до застосування вибраних та розроблених алгоритмів на практиці.

Визначено виходи бізнес-процесу розробки модуля анонімізації персональних даних:

1) Розроблений модуль анонімізації. Цей модуль може бути розроблений різними мовами програмування та з застосуванням найрізноманітніших фреймворків та бібліотек. Зазвичай рекомендується використовувати ту яку використовує ІТ відділ навчального закладу, але звісно потрібно зважати чи ці інструменти підійдуть для розробки функціоналу, який би повністю задовольнив поставлені цілі. Цей вибір потрібно робити зважено, адже після розробки нового сервісу потрібно буде його інтегрувати в діджитал менеджмент систему навчального закладу. Крім того, його потрібно буде підтримувати й дуже ймовірно, що робитиме це відділ технічної підтримки навчального закладу. Розроблений модуль повинен повністю покривати усі вимоги до анонімізації даних конкретного навчального закладу, не повинен бути занадто складним та глибоко інтегрованим в загальний функціонал менеджмент системи. Тобто в ідеалі це має бути просто ще один шар між менеджмент системою та

API яке використовується зовнішніми споживачами даних для отримання інформаційних об’єктів.

2) Нова версія API. Оскільки сервіс анонімізації може передбачати зміну форматів певних атрибутів інформаційних об’єктів, то потрібно модифікувати існуючий інтерфейс взаємодії з зовнішніми платформами. Також необхідно врахувати що може змінитись алгоритм підготовки даних до віддачі, адже до звичайної бізнес-логіки додається ще логіка анонімізації інформації.

3) Нова версія діджитал інструмента адміністрування даних навчального закладу. Оскільки іноді адміністраторам або іншому персоналу потрібно буде мати доступ як до реальних, так і до анонімних даних студентів, викладачів чи інших, то потрібно буде розробити й нову версію менеджмент інструменту. Ця версія повинна давати змогу управляти та моніторити як уже існуючий функціонал, так і новостворений сервіс анонімізації.

4) Документація з інтеграції модуля анонімізації. Лише розробити новий функціонал з анонімізації не достатньо. Адже насамперед комусь потрібно буде його інтегровувати та підтримувати. Тож обов’язково потрібно створити мануали з інтеграції нового функціоналу діджитал менеджмент системи навчального закладу.

5) Інструкції з використання сервісу анонімізації даних. Потрібно створити мануал з використання сервісу анонімізації – розгорнуту і зрозумілу кожному документацію з використання сервісу який інтегровано в існуючу систему.

6) Звітна документація. Які в усіх попередніх етапах важливим є збір, упорядкування та збереження отриманого досвіду та знань.

Завершивши імплементацію сервісу анонімізації персональної інформації учасників навчального процесу, як видно з розробленого алгоритму, маємо приступити до інтеграції цього нового інструменту. Рис. 3.10 описує бізнес-процес такої інтеграції.

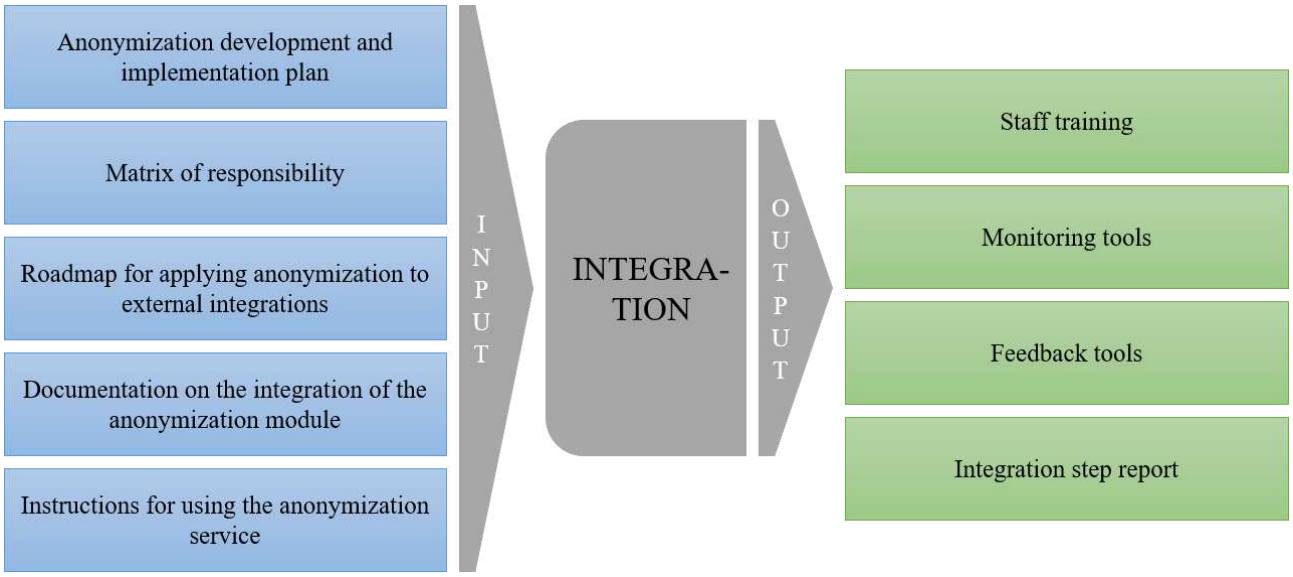

Рис. 3.10. Входи та виходи бізнес-процесу виконання розробленої стратегії впровадження анонімізації

Входи бізнес-процесу виконання розробленої стратегії впровадження анонімізації:

1) План розробки та впровадження сервісу анонімізації. В цьому плані розроблено кроки не лише по створенню нового сервісу, а і по його інтеграції. Тож потрібно дотримуватись створеного плану в усіх аспектах: моніторинг, ризики, зміст та інше.

2) Матриця відповідальності. Як і на етапі імплементації тут вказано яка команда та людина за що відповідає під час інтеграції нового функціоналу в існуючу менеджмент систему.

3) Род мапа застосування анонімізації до інтеграції з зовнішніми навчальними платформами. Саме це буде вказівником куди потрібно рухатись, взаємодіючи з зовнішніми платформами переводячи існуючі інтеграції з ними на нові рейки поширення анонімізованих даних.

4) Документація з інтеграції сервісу анонімізації. Під час розробки сервісу розробники описали та детально пропрацювали кроки інтеграції нового, ними

розробленого сервісу анонімізації. Тож саме його і потрібно використовувати для забезпечення гладкої та правильної інтеграції нового інструменту.

5) Мануали з використання сервісу анонімізації. Оскільки цей бізнес-процес передбачає і навчання персоналу використовувати модуль анонімізації, то необхідним джерелом інформації для цього процесу буде гайд з використання цього нового інструментарію.

Отже, перелічено усі входи поточного процесу. Необхідно звернути увагу на результати. Виходи бізнес-процесу виконання розробленої стратегії впровадження анонімізації:

1) Тренінги персоналу. Ці тренінги повинні містити не лише теоретичні відомості, а і достатню кількість практичних завдань та прикладі. І лише переконавшись що користувачі розуміють з чим мають справу і здатні використовувати новий інструментарій цей крок можна вважати завершеним.

2) Інструменти моніторингу. На етапі розробки девелопери турбуються про створення різного роду моніторинг систем в контексті нового функціоналу. Але потрібно ці інструменти інтегрувати та навчити відповідальних людей ними користуватись.

3) Інструменти та механізми зворотного зв’язку. Обов’язково має бути створений та налагоджений процес взаємодії користувачів системи, зовнішніх платформ та технічної підтримки діджитал менеджмент системи навчального закладу.

4) Звіти про виконану роботу. Має бути зібрана та збережена уся можлива інформація здобута під час виконання бізнес-процесу.

Зроблено багато роботи, планування, аналіз різного плану даних, врешті решт сама розробка та інтеграція сервісу анонімізації персональних даних в діджитал менеджмент систему навчального закладу. Але роботу не можна вважати завершеною доки не створено звіти, підсумки, зроблено певні висновки та інше. Тому наступним і останнім кроком є завершення впровадження анонімізації в систему управління даними

навчального закладу. На рис. 3.11 зображено схему такого бізнес-процесу з усіма входами та виходами.

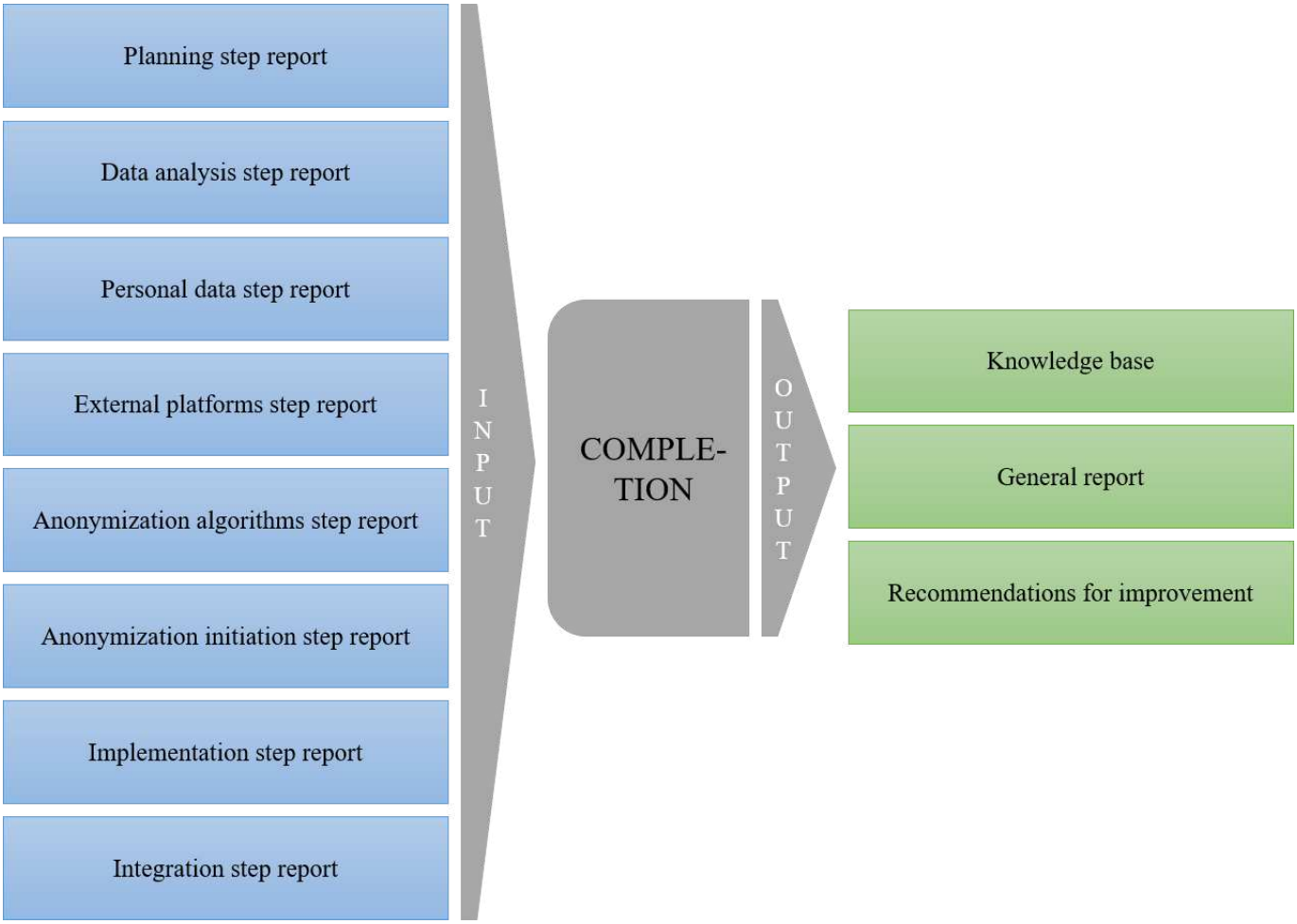

Рис. 3.11. Входи та виходи бізнес-процесу завершення впровадження анонімізації

Очевидно, що входами цього завершального бізнес-процесу будуть усі отримані знання та напрацьований досвід в процесі виконання проєкту. Тож, входи цього процесу:

1) Звіти про виконання бізнес-процесу планування впровадження моделі анонімізації персональної інформації учасників.

2) Звіти про виконання бізнес-процесу визначення даних які навчальний заклад поширює.

3) Звіти про виконання бізнес-процесу визначення які з поширюваних даних вважаються персональними та повинні бути захищені анонімізацією.

4) Звіти про виконання бізнес-процесу ідентифікації зовнішніх платформ.

5) Звіти про виконання бізнес-процесу визначення алгоритму анонімізації.

6) Звіти про виконання бізнес-процесу розробки стратегії застосування анонімізації персональних даних для інтеграцій з зовнішніми навчальними платформами.

7) Звіти про виконання бізнес-процесу розробки модуля анонімізації персональних даних.

8) Звіти про виконання бізнес-процесу виконання розробленої стратегії впровадження анонімізації.

Виходами будуть наступні пункти:

1) База знань. Тут можуть бути різного роду дані: інформація про терміни, вартість, якість та багато іншого що було під час виконання проєкту.

2) Загальний звіт. Потрібно підсумувати загалом що зроблено. Уже є звіти з кожного з етапів виконання проєкту впровадження сервісу анонімізації, але не вистачає більш стратегічного погляду. Необхідно зібрати усе до купи та створити загальний звіт, беручи до уваги не лише локальні звіти по кожному бізнес-процесу, а і розуміння проєкту загалом.

3) Висновки та рекомендації з покращення. Потрібно зробити чіткий аналіз того наскільки продукт задовольняє поставлені цілі і як можна його покращити.

Отже, розроблено метод впровадження анонімізації персональних даних стейкхолдерів навчального процесу у діджиталізованому освітньому середовищі. Цей метод базується на моделі анонімізації даних учасників навчального процесу. А також в його основі лежить алгоритм анонімізації персональної інформації.

3.3.3 Метод деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти

Як раніше зазначалось, анонімізація даних не лише забезпечує високий захист інформації, але іноді може створювати певні перешкоди для надання певних послуг зовнішніми сервісами навчальному закладу. Тому наступним кроком є розробка методики деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти.

Розроблено та описано бізнес-процеси, які у своїй сукупності забезпечують розробку та впровадження сервісу деанонімізації у діджитал систему менеджменту інформації навчального закладу. Застосувавши ці напрацювання у зв'язці з розробленими вище моделлю деанонімізації та алгоритмом деанонімізації, отримано підхід, який можна застосувати для конкретного освітнього закладу.

Тож першим кроком є планування. Про це також йдеться у розробленому нами раніше алгоритмі деанонімізації персональних даних стейкхолдерів діджиталізованої освіти. Тому розроблено схему такого бізнес-процесу (рис. 3.12).

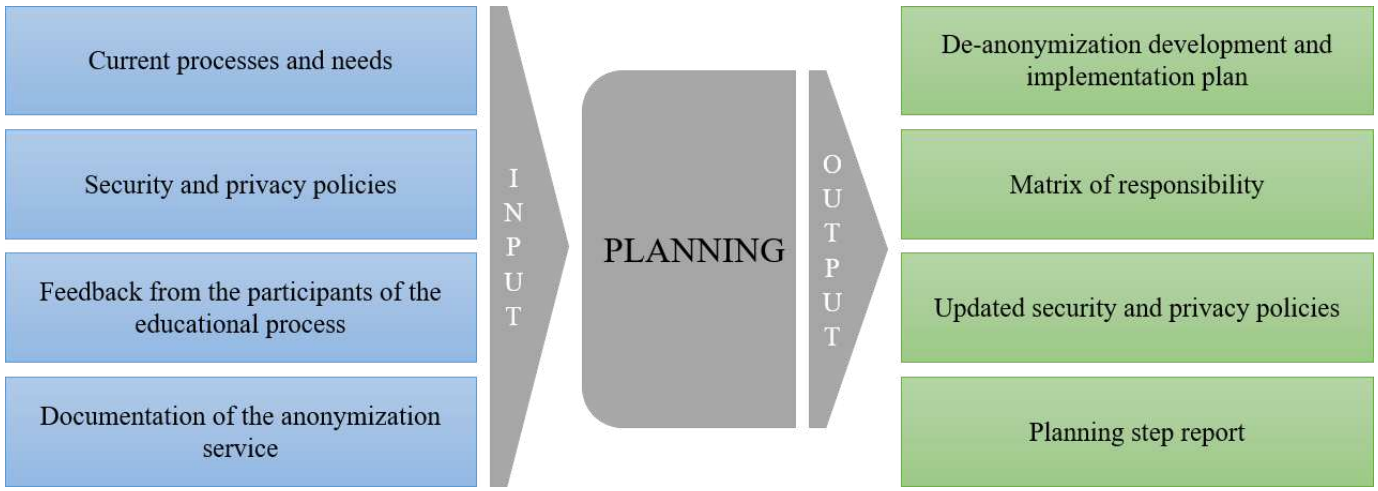

Рис. 3.12. Входи та виходи бізнес-процесу планування впровадження сервісу деанонімізації

Для повного розуміння цього бізнес-процесу описано його входи:

1) Поточні процеси та потреби. Необхідно визначити що уже наявно та як воно функціонує. Крім того, перед початком будь-яких робіт потрібно зробити дефініцію потреб які планується закрити.

2) Політики захисту інформації та конфіденційності. Потрібно розробити функціонал, який частково на вимогу уповноважених споживачів даних буде поширювати персональні дані. Тож до початку таких робіт потрібно узгодити усі кроки з розробленими вимогами до конфіденційності.

3) Відгук учасників навчального процесу. Система суттєво змінилась, адже впроваджено сервіс анонімізації персональних даних. Тож потрібно виконати процес збору відгуків, рекомендації тощо.

4) Документація розробленого сервісу анонімізації. Потрібно звернути увагу та достеменно опрацювати документацію по інструментарію анонімізації. Особливо якщо сервіси анонімізації та деанонімізації розробляють різні команди.

Чітко описавши входи бізнес-процесу планування впровадження сервісу деанонімізації, також описано виходи. Адже важливо розуміти, що саме має стати результуючими компонентами для початку роботи. Ось перелік основних виходів цього бізнес-процесу:

1) План розробки та впровадження сервісу деанонімізації персональних даних стейкхолдерів освітнього процесу. Важливо визначити чіткі завдання та метрики вимірювання відповідності результатів очікуванням, потрібно продумати та детально описати послідовність виконання цих завдань та багато іншого.

2) Матриця відповідальності. Обов’язково потрібно закріпити ролі за кожним учасником команди та розгорнуто і прозоро визначити рамки його відповідальності.

3) Оновлені політики захисту інформації та конфіденційності учасників навчального процесу. Якщо виявиться що деанонімізовувати потрібно досить не малий перелік атрибутів, можливо доведеться внести правки в політики конфіденційності.

4) Звіти щодо виконаних робіт. Після завершення усіх передбачених в алгоритмі впровадження деанонімізації робіт потрібно зібрати та зберегти отримані знання та досвід.

Оскільки уже є розроблені політики конфіденційності та захисту інформації з попереднього етапу (розробка сервісу анонімізації), а також повна документація усіх типів інформаційних об'єктів, які поширює навчальна установа, то ще раз цю роботу повністю виконувати не потрібно, а як зазначалось раніше лише допрацювати існуючі знання. Після цього потрібно перейти до аналізу даних які потребують деанонімізації. На рис. 3.13 зображено входи та виходи бізнес-процесу визначення типів персональних даних для деанонімізації.

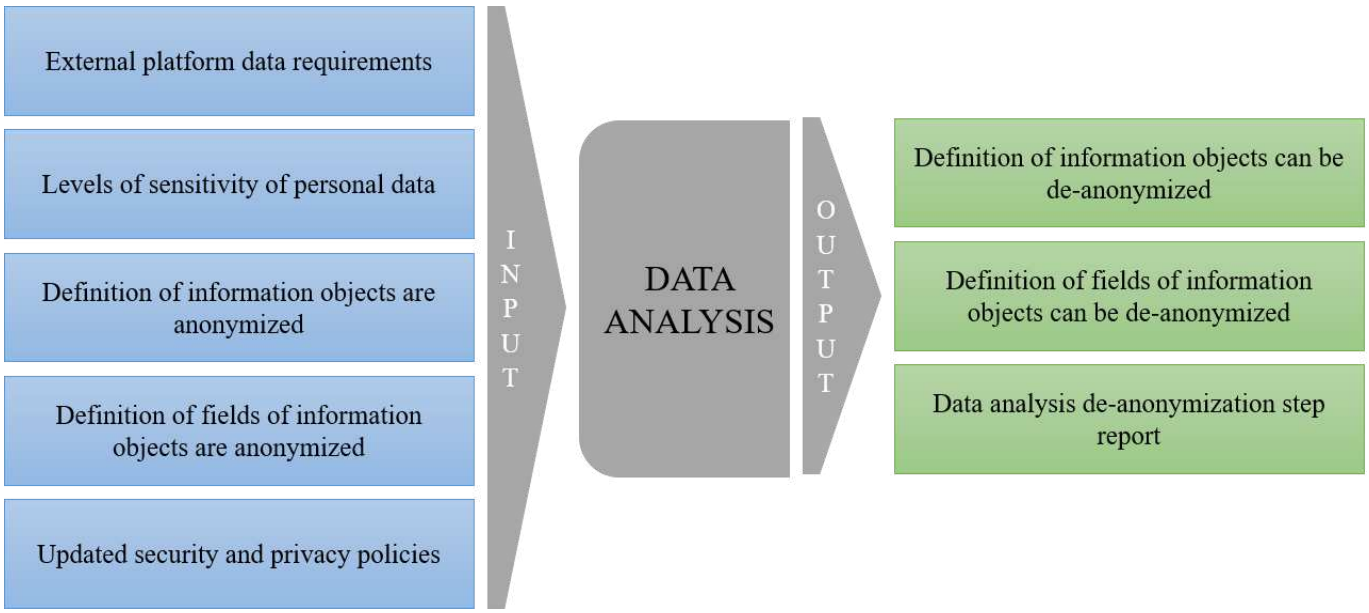

Рис. 3.13. Входи та виходи бізнес-процесу визначення типів персональних даних для деанонімізації

Детальний опис вході бізнес-процесу визначення типів персональних даних для деанонімізації:

1) Вимоги зовнішніх навчальних платформ до поширюваних даних. Ці дані вже збирались у процесі впровадження анонімізації, тож можна використати їх. Якщо

проєкт впровадження анонімізації виконувався доволі давно можна оновити цю інформацію.

2) Рівні чутливості персональних даних. Ці дані також уже в наявності з попереднього етапу – розробки анонімізації персональних даних.

3) Визначення інформаційних об’єктів які вже анонімізуються. Таку інформацію можна отримати зі звітів та документації яка була сформована при імплементації та інтеграції анонімізації.

4) Визначення атрибутів інформаційних об’єктів які анонімізуються. Це доповнення до попереднього пункту.

5) Оновлені політики захисту інформації та конфіденційності. Визначаючи які дані можна деанонімізовувати обов’язково потрібно спиратись на ці вимоги.

Тепер чітко зрозуміло що потрібно підготувати та використовувати під час виконання процесу визначення типів персональних даних для деанонімізації. Тому дано виходи цього бізнес-процесу:

1) Дефініція інформаційних об’єктів які підлягають деанонімізації. Потрібно вичерпно описати які саме об’єкті вимагають підтримки деанонімізації, це має бути переріз переліків даних які навчальний заклад може відкривати зовнішнім споживачам і даних які ці платформи вимагають для забезпечення потрібного навчальному закладу сервісу.

2) Дефініція полів інформаційних об’єктів які підлягають деанонімізації. Більшості зовнішніх навчальних платформ не потрібно мати усі реальні дані студента, а лише електронну адресу або номер телефону, щоб забезпечити ефективний навчальний процес. Тож у цей перелік мають входити лише реально потрібні дані.

3) Звіти про зроблені дії. Обов’язковим кроком закінчення бізнес-процесу є підсумки та звіти. Тому потрібно виконати це і тут.

Зробивши потрібний аналіз, отримано усю необхідну інформацію для початку робіт з впровадження сервісу деанонімізації в існуючу цифрову менеджмент систему

навчального закладу. Тому наступним процесом є імплементація цього інструменту. Рис. 3.14 демонструє саме цей бізнес-процес.

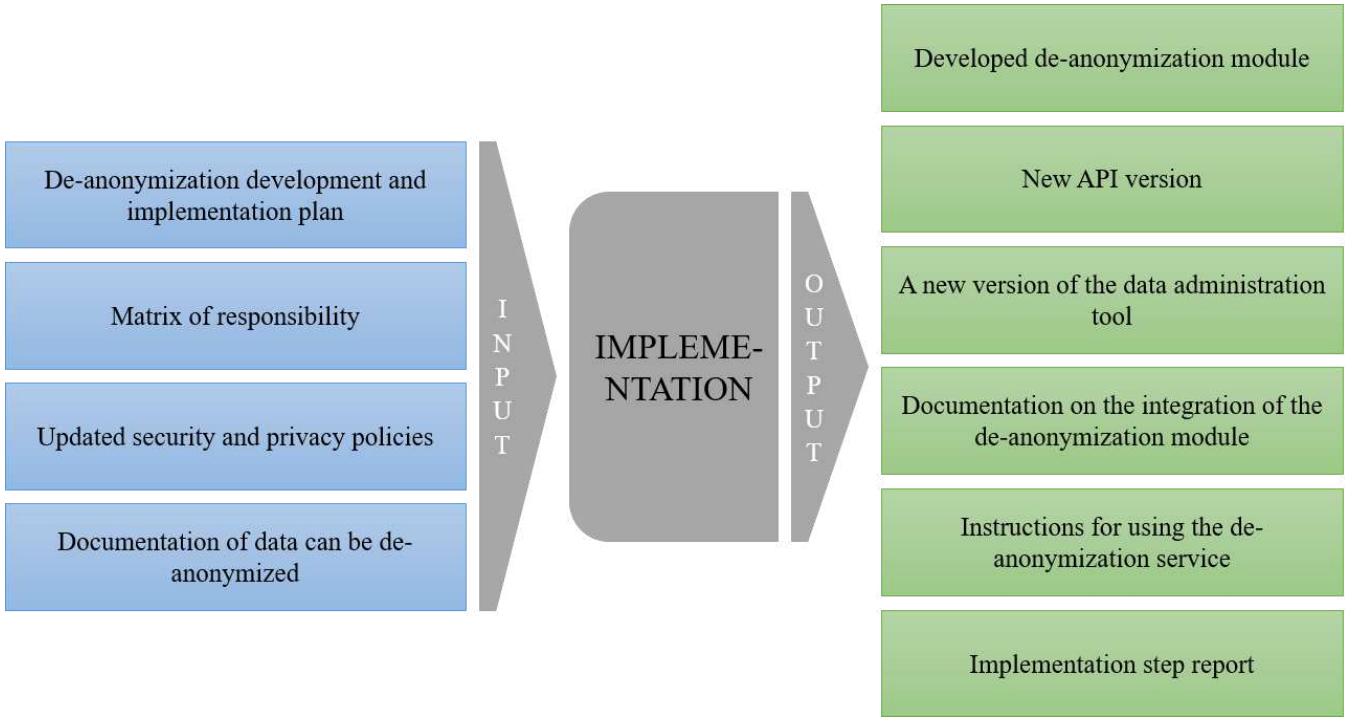

Рис. 3.14. Входи та виходи бізнес-процесу створення сервісу деанонімізації персональних даних

Виокремлено усі входи бізнес-процесу створення сервісу деанонімізації персональних даних:

1) План розробки та впровадження деанонімізації. Варто наголосити, що особлива увага має бути приділена моніторингу, контролю якості та управлінню ризиками.

2) Матриця відповідальності. Раніше визначено рамки відповідальності всіх залучених команд та кожного члена команди окремо. Це допоможе успішному виконанню робіт та полегшить координацію та контроль.

3) Оновлені політики безпеки. Потрібно постійно звірятися з цими вимогами. Тому тут вони теж мають застосовуватись.

4) Документація на дані які можуть бути деанонімізовані. Це і визначить точніший перелік даних, деанонімізацію для яких потрібно буде розробити.

Процес імплементації це доволі складний етап. Тут потрібно застосувати оптимальні підходи, практики та фреймворки, пишучи новий код. Адже це забезпечує як зручність, простоту та швидкість написання нового функціоналу так і найвищий рівень захисту інформації. Тому, на це потрібно звернути особливу увагу. Далі дано визначення виходів бізнес-процесу для розуміння що саме очікується як результат усієї роботи на даному етапі. Ось перелік таких виходів:

1) Розроблений модуль деанонімізації персональних даних. Функціонал потрібно розробляти таким чином, щоб його було просто увімкнути та вимкнути при потребі. Він має бути простим в інтеграції та підтримці. Потрібно також забезпечити легку майбутню підтримку та модернізацію.

2) Нова версія API який використовують зовнішні споживачі для інтеграції з освітньою установою. Оскільки модернізовано існуючий API впроваджуючи анонімізацію в інтеграції з зовнішніми навчальними платформами, то розроблюючи деанонімізацію потрібно знову це зробити. Потрібно, виконуючи всі вимоги до захисту даних, забезпечити безперебійне функціонування ендпоінтів пов’язаних з деанонімізацією даних.

3) Нова версія діджитал менеджмент інструменту навчального закладу. Вводячи новий функціонал в діджитал операційну систему навчального закладу не потрібно забувати про менеджмент інструменти. Потрібно дати можливість керувати новоствореними функціями.

4) Документація щодо інтеграції новоствореного інструментарію. Розробивши новий модуль, потрібно потурбуватись про те, щоб було зрозуміло що з ним робити. Тобто потрібно створити інструкції та рекомендації для людей які будуть інтегровувати новорозроблений сервіс.

5) Інструкції з використання сервісу деанонімізації персональної інформації. Варто закрити потреби користувачів. Тобто потрібно подбати про UX аспект та гайди з використання нового функціоналу.

6) Звіти щодо виконаних робіт. Оскільки створено багато нового функціоналу та документації до нього, потрібно зберегти для подальшого аналізу та перевикористання отриманий досвід.

Як і у випадку з методом впровадження анонімізації персональних даних стейкхолдерів навчального процесу, після виконання розробки сервісу настає етап його інтеграції. Тож далі описано бізнес-процес інтеграції розробленого на попередньому кроці сервісу деанонімізації персональної інформації для діджитал менеджмент системи освітньої установи. На рис. 3.15 зображено схему бізнес-процесу інтеграції цього сервісу з його входами та виходами.

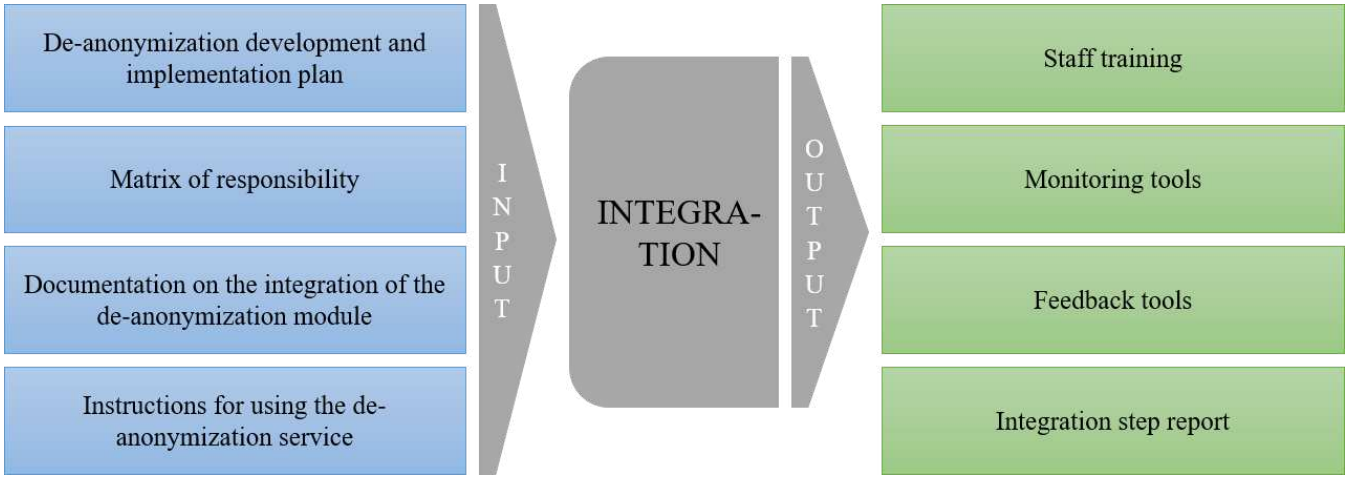

Рис. 3.15. Входи та виходи бізнес-процесу інтеграція сервісу деанонімізації з діджитал системою менеджменту даних

Входи цього бізнес-процесу:

1) План розробки та впровадження сервісу деанонімізації. Тут важлива частина стосовно впровадження. Адже план повинен описувати також перелік та послідовність дій для успішної інтеграції модуля деанонімізації.

2) Матриця відповідальності. Зазвичай у процесі інтеграції нового функціоналу не бере участь вся команда. Тому для розуміння які людські ресурси нам ще потрібні й за що відповідає кожен член команди використовується матриця.

3) Документація щодо інтеграції новоствореного сервісу деанонімізації. Це документація яка створювалася для даного етапу. Тут прописано, що і як потрібно робити, щоб успішно інтегрувати новий функціонал у існуючу конкретну систему.

4) Інструкції з використання модуля деанонімізації. Не потрібно забувати про людей які користуватимуться тим що створено. Тож для навчання персоналу потрібні такі інструкції.

Інтеграція нового функціоналу у вже існуючу систему доволі складний процес. Тому потрібно приділяти йому уваги не менше ніж самій розробці цього нового інструменту. Дано визначення виходів бізнес-процесу інтеграції сервісу деанонімізації з діджитал системою менеджменту даних:

1) Тренінги для персоналу. Потрібно забезпечити передачу знань до безпосереднього користувача. Тобто розробити та провести тренінги з навчання персоналу. Ці тренінги повинні включати теоретичну та практичну частини.

2) Інструменти моніторингу. Іноді трапляються ситуації що уже давно, а можливо і з самого свого старту роботи новостворений функціонал повною мірою не виконує покладені на нього обов’язки й команда підтримки дізнається про це лише коли клієнт звернувся до них напряму отримавши негативний досвід. Тому для превентивної роботи з такими випадками потрібно мати певні інструменти моніторингу та відповідно їх застосовувати.

3) Інструменти зворотного зв’язку. Буває, що моніторинг не може передбачити всі випадки й незважаючи на хороші інструменти моніторингу та професійну команду підтримки клієнти все одно стикаються з певними труднощами, непорозуміннями та проблемами. Саме тому і потрібно забезпечити можливість зворотного зв’язку.

4) Звітність по роботі. Закінчивши виконання усіх передбачених завдань, як завжди, потрібно виконати усі завершальні кроки та створити відповідні звіти.

Завершивши розробку нового функціоналу та виконавши його інтеграцію, потрібно завершити всі початі процеси. Також важливо зберегти та обробити отримані знання та досвід в процесі виконання всіх робіт. Тому останнім кроком є завершення впровадження деанонімізації персональних даних учасників навчального процесу у діджиталізованій освітній сфері. На рис. 3.16 зображено входи та виходи такого бізнес-процесу.

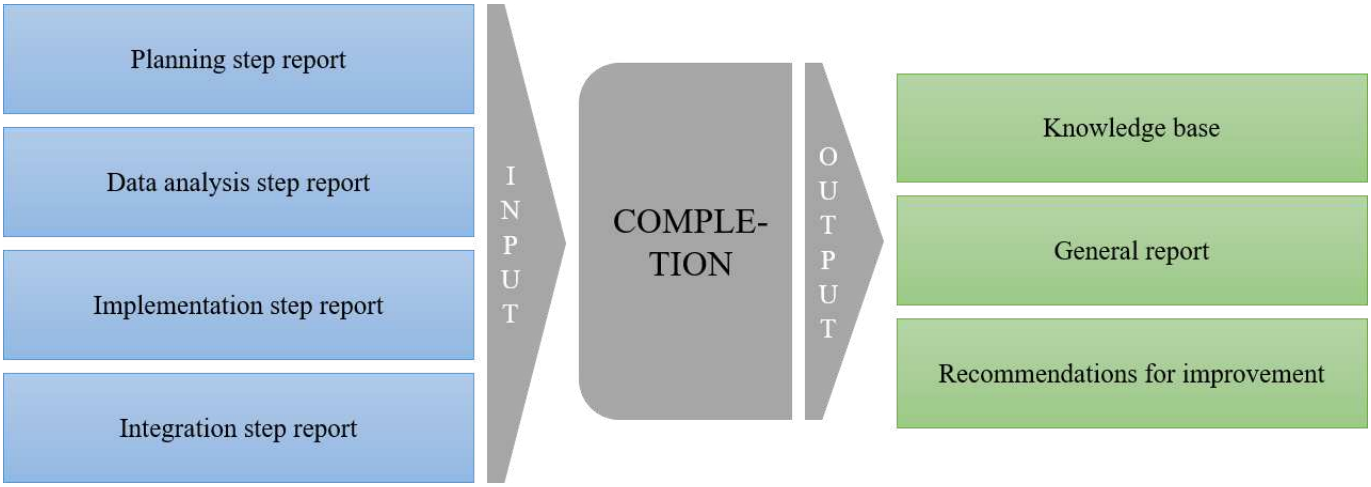

Рис. 3.16. Входи та виходи бізнес-процесу завершення впровадження сервісу деанонімізації

Запропоновано детальний опис входів та виходи бізнес-процесу завершення впровадження сервісу деанонімізації. Входи:

1) Звіти про виконані роботи бізнес-процесу планування впровадження сервісу деанонімізації.

2) Звіти про виконані роботи бізнес-процесу визначення типів персональних даних для деанонімізації.

3) Звіти про виконані роботи бізнес-процесу створення сервісу деанонімізації персональних даних.

4) Звіти про виконані роботи бізнес-процесу інтеграції сервісу деанонімізації з діджитал системою менеджменту даних.

Описано виходи цього бізнес-процесу:

1) База знань. Передусім важливо опрацювати напрацьовані дані та структурувати їх. Після чого буде можливо їх зберегти у базу даних певного типу. Такі бази можуть бути використані як для робіт з покращення та підтримки поточного проєкту, так і для інших подібних проєктів.

2) Генеральний звіт. Звісно уже сформовано звіти з кожного кроку виконання проєкту. Але потрібно зробити загальний підсумковий звіт дивлячись на усю роботу з точки зору вищого рівня. Тобто беручи до уваги не просто якийсь один бізнес-процес, а увесь проєкт загалом. Потрібно підсумувати витрати різного типу ресурсів, а також на основі цього коштів, також чітко визначити чи усім критеріям відповідає результату та багато іншого.

3) Рекомендації з покращення. Як відомо, зазвичай, розробка якогось нового сервісу не є останнім що повинно відбуватись з функціоналом. Потрібно постійно його покращувати, модифікувати з урахуванням нових вимог як до самого функціоналу, так і до інших аспектів основним з яких є безпека. Також варто забезпечити хороший рівень підтримки сервісу як технічної, так і користувацької. Тож це є одна з цілей виконання постаналізу та створення рекомендацій.

Отже, створено метод з впровадження деанонімізації персональних даних стейкхолдерів навчального процесу у діджитал середовищі. В контексті цього методу створено та детально описано кожен крок. При розробці використовувався попередньо розроблений алгоритм впровадження деанонімізації. Тобто кожен крок методу відсилається до конкретного кроку в алгоритму. Тому, застосовуючи його на практиці, потрібно дивитись також, що описано в цьому алгоритмі. Крім того, основою є модель деанонімізації персональних даних стейкхолдерів навчального процесу.

3.3.4 Об’єднаний метод впровадження анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти

Як зазначалось вище, в умовах сучасної діджиталізованої освіти, де інформаційні технології постійно вдосконалюються, важливим завданням стало управління персональними даними стейкхолдерів. Для цього розроблено два основоположні методи: метод впровадження анонімізації, який детально описує бізнес-процеси щодо захисту конфіденційності даних у взаємодії елементів інформаційного простору, та метод деанонімізації, який охоплює процеси відновлення доступності даних для підтримки освітніх і адміністративних цілей. Однак, з огляду на складність та взаємозалежність цих процесів, виникає необхідність у формуванні загального методу, що інтегрує обидва підходи. Це дозволить сформувати цілісну стратегію управління даними на вищому рівні, забезпечуючи як безпеку, так і функціональність в освітньому середовищі. Такий метод стане наріжним каменем для закладів освіти, що прагнуть оптимізувати управління даними, забезпечуючи при цьому всебічну підтримку освітніх та ділових процесів.

Зазвичай впровадження анонімізації відбувається у зв’язці з деанонімізацією, хоча звісно бувають винятки. Потрібно розробити метод який дозволяє об’єднати описані раніше методи впровадження анонімізації та деанонімізації персональних даних учасників навчального процесу. Адже часто має сенс запускати одночасно проєкти по анонімізації та деанонімізації. Розпочати потрібно зі створення порядку та залежностей виконання бізнес-процесів, які стосуються модулів анонімізації та деанонімізації. Тож розроблено схему, яка демонструє такі кроки (рис 3.16).

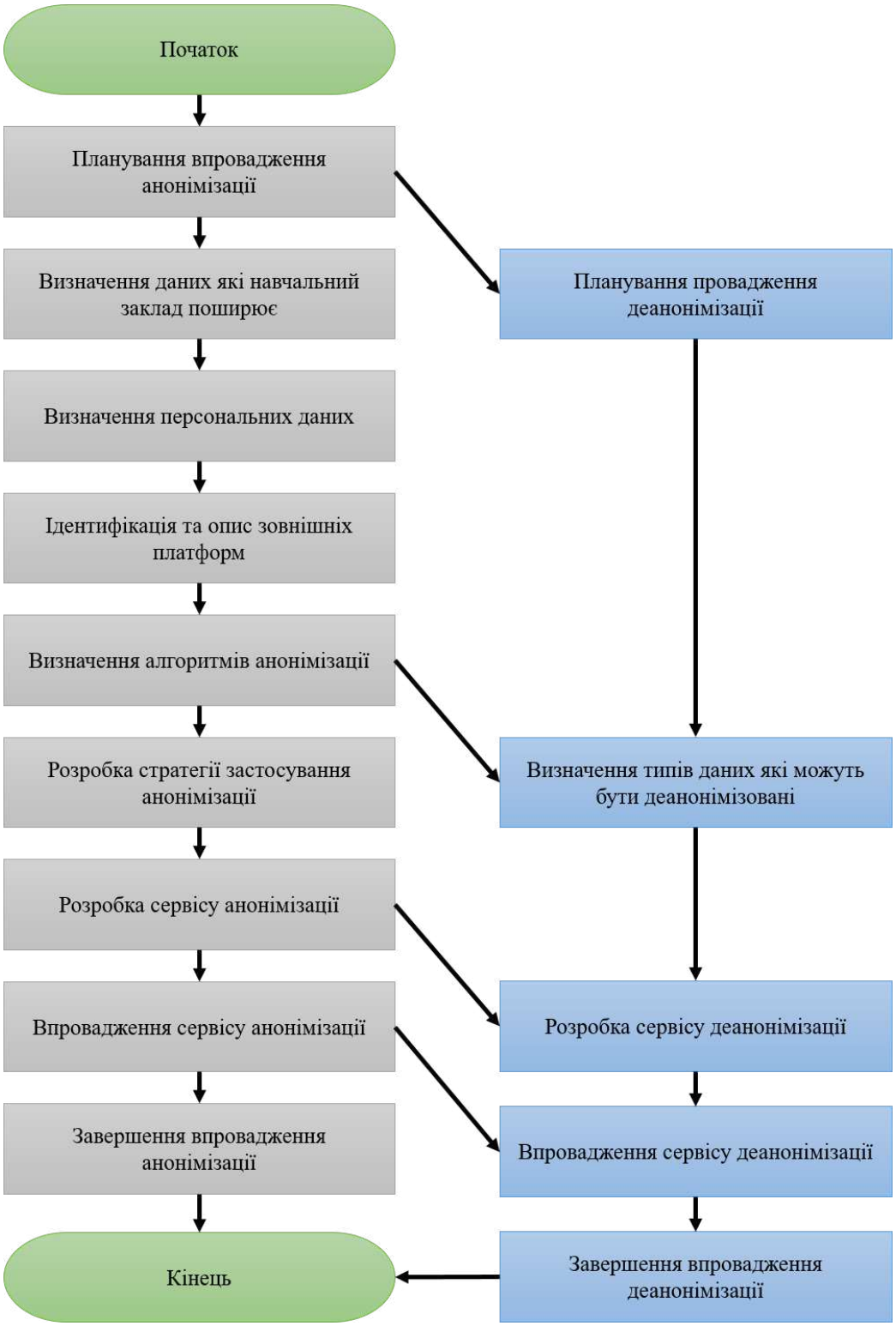

Рис. 3.17. Порядок виконання бізнес-процесів які стосуються впровадження анонімізації та деанонімізації в діджитал взаємодії навчального закладу

На схемі об’єднання бізнес-процесів анонімізації та деанонімізації (рис. 3.17) зображено усі раніше розроблені кроки, а також показані їх залежності. Для чіткого розуміння розробленої послідовності описано кожен крок окремо:

1) Початок робіт. Перед початком планування впровадження анонімізації та деанонімізації потрібно чітко сформувати загальне бачення фінального рішення та шляху яким ми до нього йтимемо. Виконати планування вищого рівня, тобто з точки зору анонімізації та деанонімізації як одного проєкту. Це важливо для розуміння робіт по деанонімізації і анонімізації командою, замовником та іншими не як окремих проєктів, а як частин одного. Лише отримавши чітке розуміння усіх майбутніх робіт як одного цілого, варто переходити до наступних етапів.

2) Планування впровадження анонімізації. Це перший крок з якого варто розпочинати усю роботу пов’язану з анонімізацією та деанонімізацією на нижчому рівні. Після його виконання буде зрозуміло що нам точно потрібно і як це зробити в контексті впровадження анонімізації в діджитал інтеграції навчального закладу та зовнішніх споживачів даних.

3) Планування впровадження деанонімізації. Роботу по деанонімізації потрібно починати лише коли готовий план з використання анонімізації навчальним закладом. Адже що можна деанонімізовувати, якщо робота по анонімізації ще навіть не починалась. Тож цей етап можна починати лише коли закінчене планування впровадження анонімізації. Тривати він може аж до початку ініціації розробки анонімізації. Тобто з його початком не потрібно поспішати. Іноді варто дати команді завершити кілька паралельних кроків які стосуються анонімізації. Тоді план можна буде зробити більш розгорнутим і врахувати більше деталей. Такі деталі можна отримати з наступних паралельно ідучих процесів по анонімізації: аналіз даних навчального закладу, визначення персональних даних, аналіз зовнішніх навчальних платформ.

4) Аналіз даних навчального закладу. Після закінчення планування анонімізації починається робота по збору інформації щодо діджитал типів даних навчального закладу та її аналізу.

5) Визначення персональних даних. Проаналізувавши дані, які поширюються освітньою установою в контексті взаємодії з зовнішніми сервісами, потрібно виділити що з цих даних можна вважати персональною інформацією. Тут потрібно діяти акуратно та виважено, адже безпека – це найголовніше.

6) Аналіз зовнішніх навчальних платформ. Для подальших робіт по розробці нового функціоналу потрібно розуміти в яких умовах він буде використовуватись та хто буде ним користуватись. Тому цей етап є дуже важливим. Треба зрозуміти з ким навчальний заклад співпрацює чи планує співпрацювати та врахувати вимоги цих стейкхолдерів.

7) Алгоритми анонімізації. Маючи опис інформаційних об’єктів та їх атрибутів, які беруть участь в діджитал взаємодії, розуміючи що з цього є персональною інформацією та враховуючи вимоги зовнішніх сервісів, слід перейти до наступного важливого кроку. Тобто до самої розробки алгоритмів анонімізації. На основі результатів виконання цього бізнес-процесу буде зрозуміло наскільки складною буде розробка та впровадження.

8) Аналіз даних для деанонімізації. На попередньому етапі визначено, що саме підлягатиме анонімізації. А отже, можна запускати роботу з визначення того, що саме необхідно деанонімізувати. Тут повинні бути враховані не лише розроблені алгоритми анонімізації, а й вимоги зовнішніх споживачів даних. Адже переважно саме для отримання від них певних унікальних сервісів і розробляється модуль деанонімізації.

9) Ініціація розробки та впровадження анонімізації. Цей етап повинен стартувати лише коли закінчені усі аналітичні роботи які стосуються анонімізації та створено алгоритми анонімізації персональних даних учасників навчального процесу.

Він є обов’язковим перед початком розробки модуля анонімізації, а також його інтеграції в існуючу діджитал менеджмент систему навчального закладу.

10) Розробка анонімізації. Уже виконано усі підготовчі роботи: аналіз типів, даних, розробка алгоритмів анонімізації та інше. Тому далі слідує імплементація сервісу анонімізації. Оскільки робота відбувається паралельно і над деанонімізацією, то потрібно це врахувати та зробити певні кроки для полегшення майбутньої розробки модуля деанонімізації персональної інформації.

11) Інтеграція анонімізації. Підготовка зроблена, сервіс імплементовано та створено всі необхідні документи та гайди для старту інтеграції новоствореного функціоналу з анонімізації персональних даних. Тож далі потрібно приступати до виконання наміченого плану цього бізнес-процесу.

12) Розробка деанонімізації. Цей процес можна починати зразу після завершення розробки сервісу анонімізації й старту його інтеграції. Це дасть змогу залучити ту ж команду розробників. А також уже буде розуміння архітектури шару анонімізації. Без цього розробка деанонімізації може вимагати більших ресурсів та модифікації після завершення розробки сервісу анонімізації. Також на даному етапі уже має бути готова уся необхідна документація та зарезервовані потрібні ресурси.

13) Інтеграція деанонімізації. Після закінчення розробки модуля деанонімізації та успішної інтеграції модуля анонімізації починається інтеграція модуля деанонімізації. Адже його функціонал має залежність на функціонал модуля анонімізації.

14) Завершення впровадження анонімізації. Виконано усі кроки пов’язані з розробкою та впровадженням сервісу анонімізації у навчальний заклад. Тож потрібно завершити усі розпочаті процеси, підготувати звіти та висновки та створити рекомендації для подальшої підтримки та модернізації сервісу.

15) Завершення впровадження деанонімізації. Як і у випадку з завершенням робіт по анонімізації, на цьому кроці уже закінчена розробка й інтеграції сервісу

деанонімізації. Тож потрібно завершити проєкт, внести дані у базу знань та підбити підсумки.

16) Завершення робіт. Вже закінчено усі роботи пов’язані як з впровадження в анонімізації, так і деанонімізації. Тож залишилось зробити висновки та підбити підсумки дивлячись на пророблену усю роботу загалом.

На завершення слід зазначити, що створення інтегрованого підходу до управління даними є ключовим моментом у забезпеченні ефективності та безпеки у навчальному процесі. Розроблений метод який об’єднує анонімізацію та деанонімізацію, детально описаний в цьому розділі, не тільки дозволить захистити конфіденційну інформацію, але й підтримувати доступ до неї у випадках, коли це необхідно для навчальних та адміністративних цілей. Поєднання цих двох підходів дає змогу забезпечити цілісний контроль над даними, зберігаючи баланс між конфіденційністю та функціональністю. Такий інтегрований метод є важливим кроком до побудови надійного та адаптивного інформаційного середовища в освіті, яке відповідає сучасним вимогам безпеки і регуляторним нормам.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. У третьому розділі детально описано механізми та способи їх застосування які забезпечують безпеку та ефективну взаємодію з зовнішніми споживачами персональних даних в сучасній освіті.

2. Насамперед створено алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти. В якому детально розписано кожен крок який необхідно виконати для впровадження анонімізації. Цей алгоритм є основою подальших розробок з анонімізації, застосування яких надає можливість захистити особисту інформацію від несанкціонованого доступу, зберігаючи цілісність навчальних і адміністративних процесів.

3. Далі створено алгоритм деанонімізації, застосування якого дозволяє відновити доступ до персональних даних у випадках, коли це виправдано адміністративними чи освітніми потребами. Це допомагає зберегти рівновагу між необхідністю захисту інформації та функціональними вимогами навчального закладу.

4. Як початковий крок створення методу анонімізації та деанонімізації персональних даних розроблено загальну схему впровадження анонімізації та деанонімізації. Схема на загальному рівні описує інтеграцію процесів у єдиний цикл, що забезпечує успішне виконання усіх кроків пов’язаних з розробкою та впровадженням анонімізації та деанонімізації.

5. Після цього створено метод анонімізації у взаємодії елементів інформаційного простору. Даний метод розгорнуто описує усі бізнес-процеси, які необхідно виконати для впровадження анонімізації в діджитал менеджмент систему навчальної установи. При застосуванні методу потрібно використовувати також розроблений у цьому ж розділі алгоритм анонімізації персональних даних. Адже вони є одним цілим.

6. Також розроблено метод деанонімізації, який визначає бізнес-процеси, що необхідно імплементувати для отримання функціоналу, який дозволить безпечно та ефективно відновлювати доступ до даних, коли це необхідно, забезпечуючи операційні потреби освіти без компромісів з безпекою. Цей метод щільно переплітається з алгоритмом деанонімізації й у своїй основі містить його структуру.

7. Об’єднавши ці напрацювання, розроблено метод управління потоками персональних даних в умовах діджиталізації освітньої сфери. Цей метод описує як потрібно застосовувати створені підходи до впровадження анонімізації та деанонімізації разом для отримання максимально ефективного інструментарію з захисту даних та їх зручного менеджменту. Застосування цього методу є ключем до трансформації інтеграцій з зовнішніми навчальними платформами для досягнення максимальної безпеки та конфіденційності навчального процесу.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ УПРАВЛІННЯ ПОТОКАМИ ПЕРСОНАЛЬНИХ ДАНИХ ОСВІТНЬОГО СЕРЕДОВИЩА В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

4.1 Архітектура інформаційної технології анонімізації/деанонімізації персональних даних стейкхолдерів діджиталізованої освіти

4.1.1. Загальна схема архітектури інформаційної системи з використанням анонімізації персональних даних

Виконавши аналіз існуючих підходів до управління персональною інформацією, та визначивши основні фактори які є ключовими при роботі з такими даними, сформовано загальні вимоги до архітектури інформаційного рішення анонімізації персональної інформації у діджиталізованій освітній сфері:

1. Повна анонімізація – система повинна гарантувати, що жодна особиста ідентифікаційна інформація не може бути відновлена з анонімізованих даних.
2. Збереження корисності даних – при анонімізації важливо зберігати цінність даних для подальшого аналізу і досліджень.
3. Спеціалізовані алгоритми анонімізації – використання відповідних алгоритмів анонімізації є ключовим для забезпечення високого рівня конфіденційності.
4. Контроль доступу – система повинна мати ретельний механізм керування доступом.
5. Шифрування даних – для запобігання можливому несанкціонованому доступу до анонімізованих даних важливо використовувати сильне шифрування на рівні зберігання і передачі даних.

6. Збереження контексту – система має зберігати деякий рівень контексту для забезпечення валідності та корисності даних.

7. Моніторинг та аудит – важливо вести постійний моніторинг та аудит системи анонімізації для виявлення можливих порушень конфіденційності та своєчасного їх усунення.

8. Простота інтеграції з існуючою екосистемою – система анонімізації персональних даних повинна бути розроблена з урахуванням простоти її інтеграції в існуючу інформаційну та технологічну інфраструктуру навчального закладу.

Забезпечення цих вимог допоможе створити ефективну систему анонімізації персональних даних, яка забезпечує високий рівень конфіденційності та захисту приватності учасників діджиталізованої освітньої сфери.

Враховуючи вищезазначену інформацію, розроблено модульну архітектуру інформаційної системи анонімізації персональних даних (Рис. 4.1) [6].

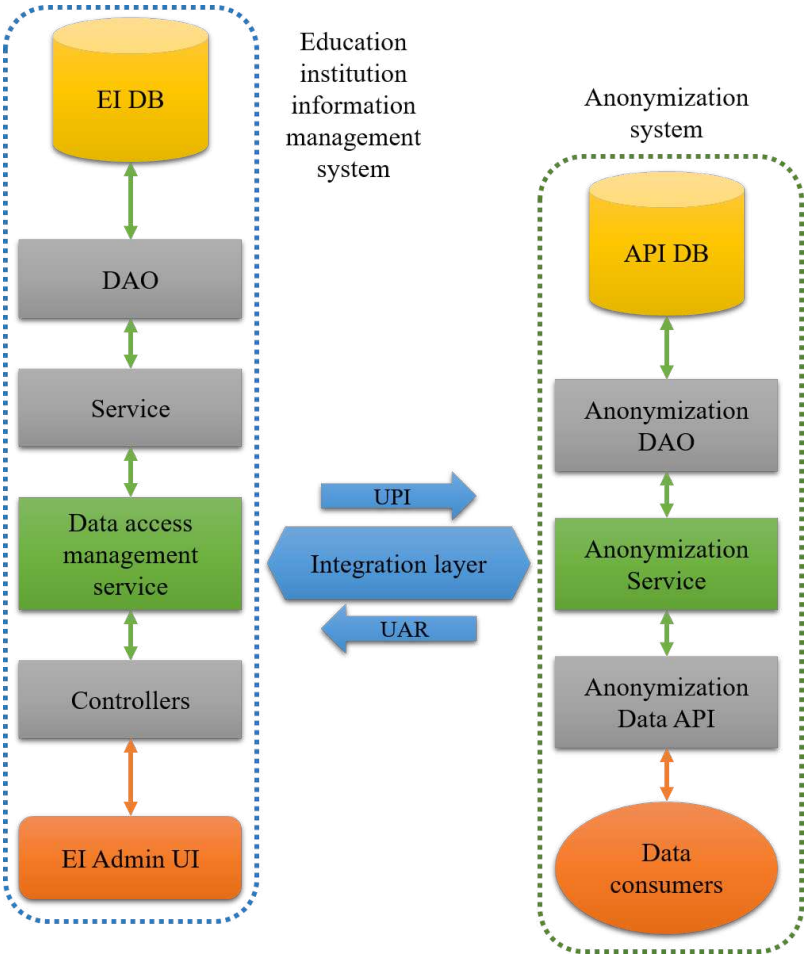

Рис. 4.1. Загальна архітектура інформаційної технології анонімізації персональних даних [6].

Складові такої системи:

1) Інформаційна система управління інформацією навчального закладу (Education institution information management system) – існуюча централізована цифрова система управління усією інформацією навчального закладу з якою і відбуватиметься майбутня інтеграція системи анонімізації персональних даних. Зазвичай такі системи мають наступну структуру:

a. База даних навчального закладу (EI DB) – цифрове сховище усі необхідної для повноцінного функціонування навчального закладу інформації.

b. Шар доступу до даних (DAO) – певна імплементація механізму забезпечення операцій читання та запису в базу даних.

c. Шар бізнес-логіки (Service) – менеджмент шар який забезпечує всі необхідні функції маніпуляції структурами даних навчального закладу.

d. Сервіс управління доступом до даних навчального закладу (Data access management service) – один з найважливіших елементів системи, шар який забезпечує санкціонований доступ до даних навчального закладу.

e. Шар контролерів (Controllers) – шар який забезпечує та декларує шляхи отримання та маніпуляції інформації.

f. Адмін-панель навчального закладу (EI Admin UI) – інструмент менеджменту цифрової інформації навчального закладу відповідно навченим персоналом.

2) Інтеграційний шар (Integration layer) – шар який забезпечує внутрішню комунікацію різних інформаційних систем навчального закладу. В контексті інтеграції з системою анонімізації персональних даних цей шар забезпечуватиме поширення персональних даних системі анонімізації, відповідно для подальшої їх анонімізації цією системою. В протилежну сторону буде йти потік нових даних (звітів, оцінок тощо) отриманих з зовнішніх джерел.

3) Інформаційна система анонімізації персональних даних стейкхолдерів діджиталізованої освітньої сфери (Anonymization system) – система, ціллю інтеграції якої в існуючі інструменти управління цифровими даними навчального закладу є забезпечення високого рівня захисту персональних даних стейкхолдерів освітнього процесу. Архітектурні складові системи анонімізації персональних даних наступні:

a. База даних системи анонімізації (API DB) – сховище для зберігання згенерованих анонімних даних та усіх необхідних для їх внутрішньої ідентифікації та опрацювання метаданих.

b. Шар доступу до бази даних системи анонімізації (Anonymization DAO) – шар що забезпечує доступ до інформації бази даних системи анонімізації, та надає інструментарій для роботи з нею.

c. Шар бізнес-логіки системи анонімізації (Anonymization Service) – шар у якому відбувається опрацювання реальних даних, генерація їх анонімних копій-замінників, деанонімізація ідентифікаторів та інша бізнес-логіка пов’язана з анонімізацією та деанонімізацією персональної інформації.

d. Інтерфейс доступу до даних зовнішніми споживачами (Anonymization Data API) – інтерфейс який забезпечує санкціонований обмін інформацією між навчальним закладом та зовнішніми навчальними платформами, які використовуються стейкхолдерами навчальної екосистеми для забезпечення ефективності навчального процесу.

Описавши усі основні архітектурні складники системи анонімізації персональних даних діджиталізованого освітнього закладу, потрібно вказати основні характеристики такої архітектури. Робити огляд таких характеристик необхідно з точки зору простоти застосування та ефективності виконання покладених на систему функцій, адже такі показники часто є визначальними при інтеграції нових функціональних одиниць в існуючу інформаційну технологію. Тож основні особливості такої архітектури системи анонімізації є наступними:

1) Масштабованість. Така архітектура здатна ефективно масштабуватися відносно зростаючого обсягу даних, що накопичується в освітньому процесі. Адже використання окремого шару доступу до бази даних дозволяє модифікувавши лише його перейти на різні моделі зберігання даних, як то розподілені бази даних. Це дозволить забезпечити надійну роботу системи навіть при збільшенні обсягу інформації.

2) Гнучкість. Таку архітектуру можна адаптувати до різних типів даних, які обробляються в освітньому контексті. Адже типи даних анонімізованої бази даних по суті повторюють уже існуючі типи даних (таблиці) в базі даних навчального закладу.

3) Різноманітні методи анонімізації. Маючи логіку анонімізації в окремому шарі (Anonymization Service), модифікація лише цієї частинки дозволить підтримувати різні методи анонімізації, включаючи заміщення, загальне шифрування, хешування та

інші. Це дозволяє вибрати найкращий підхід для конкретного типу даних та конкретних вимог до конфіденційності.

4) Інтеграція з існуючими системами. Модульна відділена архітектура системи анонімізації може бути сумісною з різноманітними існуючими інформаційними системами та платформами навчального закладу. Адже вона не вимагає зміни існуючої системи управління цифровими даними навчального закладу, а є окремим доповненням. Тобто достатньо просто налаштувати інтеграційний шар обміну повідомленнями між існуючою системою управління даними та системою анонімізації персональної інформації користувачів. Такий підхід забезпечує зручне і безперешкодне впровадження майбутньої системи анонімізації даних.

5) Швидкість обробки. Підхід відділеної системи є ефективним з точки зору швидкості обробки даних. Адже система здатна забезпечити вчасну анонімізацію при мінімальному впливі на продуктивність усієї цифрової менеджмент системи навчального закладу.

Саме такі характеристики спільно створюють просту, надійну та ефективну архітектуру системи анонімізації персональних даних стейкхолдерів в діджиталізованій освітній сфері, забезпечуючи надійний захист конфіденційності та приватності учасників навчального процесу.

4.1.2. Структура бази даних інформаційної технології анонімізації персональних даних

Базуючись на всьому вищезгаданому, більш прискіпливо варто зупинитись на структурі бази даних системи анонімізації персональної інформації стейкхолдерів діджиталізованої навчального закладу. Тож далі розглянуто узагальнену реляційну схему такої бази даних (рис. 4.2) [6].

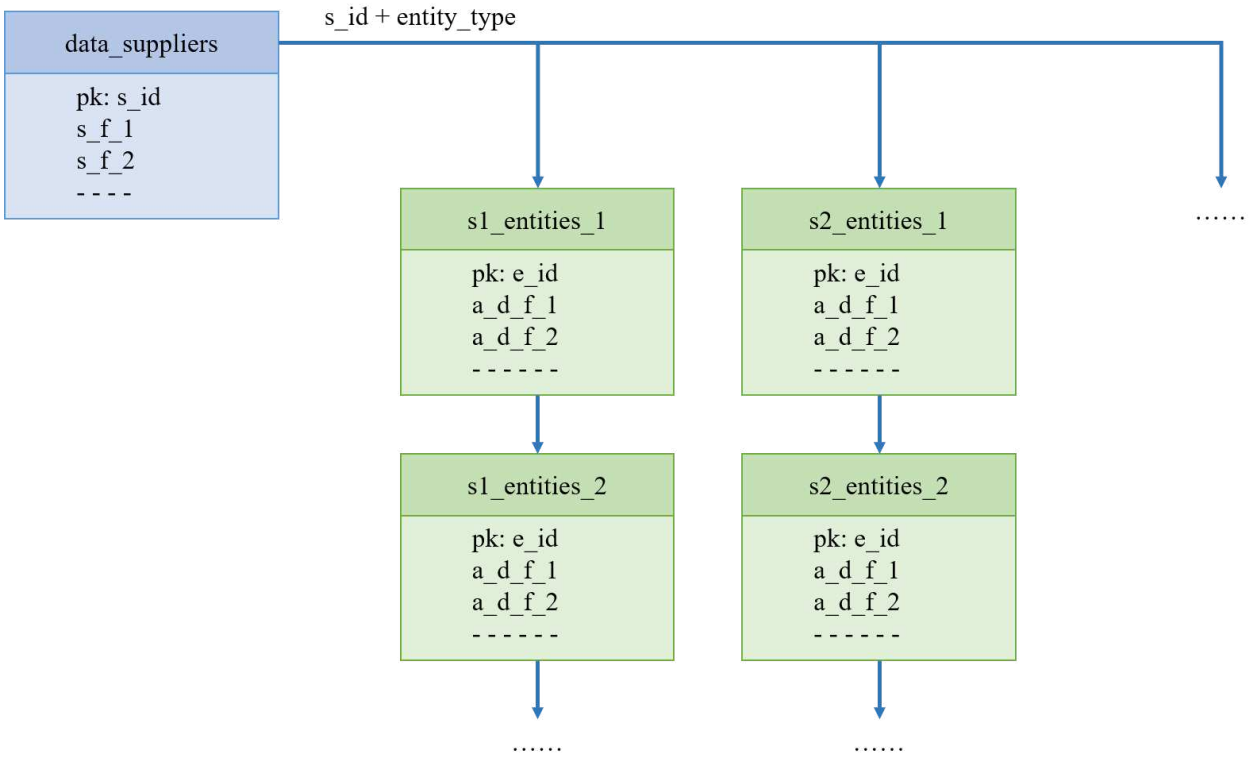

Рис. 4.2. Схема бази даних системи анонімізації персональних даних

Далі детально описано саму схему та принцип її імплементації при створенні бази даних анонімізованої персональної інформації. По суті така схема складається з двох частин:

1) Таблиця-реєстр споживачів персональної інформації (data_suppliers) – список існуючих споживачів персональних даних навчального закладу зі своїм унікальним ідентифікатором (s_id). Набір полів такої таблиці залежить від необхідної інформації навчальному закладу про певного споживача даних.

2) Сет таблиць по кожному типу даних для кожного споживача (s_id + entity_type) – являє собою набір таблиць для збереження анонімізованих екземплярів кожного типу даних навчального закладу для кожного споживача таких даних окремо. Набір полів таких таблиць буде містити усі ті ж поля, що містять реальні таблиці кожного з типів, а також додатково ідентифікатор (e_id).

На рис. 4.3 показано як може виглядати набір таблиць такої бази даних, якщо існує два споживачі даних та два типи інформаційних об’єктів: “Студент” та “Викладач” з полями “Ім’я” та “Телефон”.

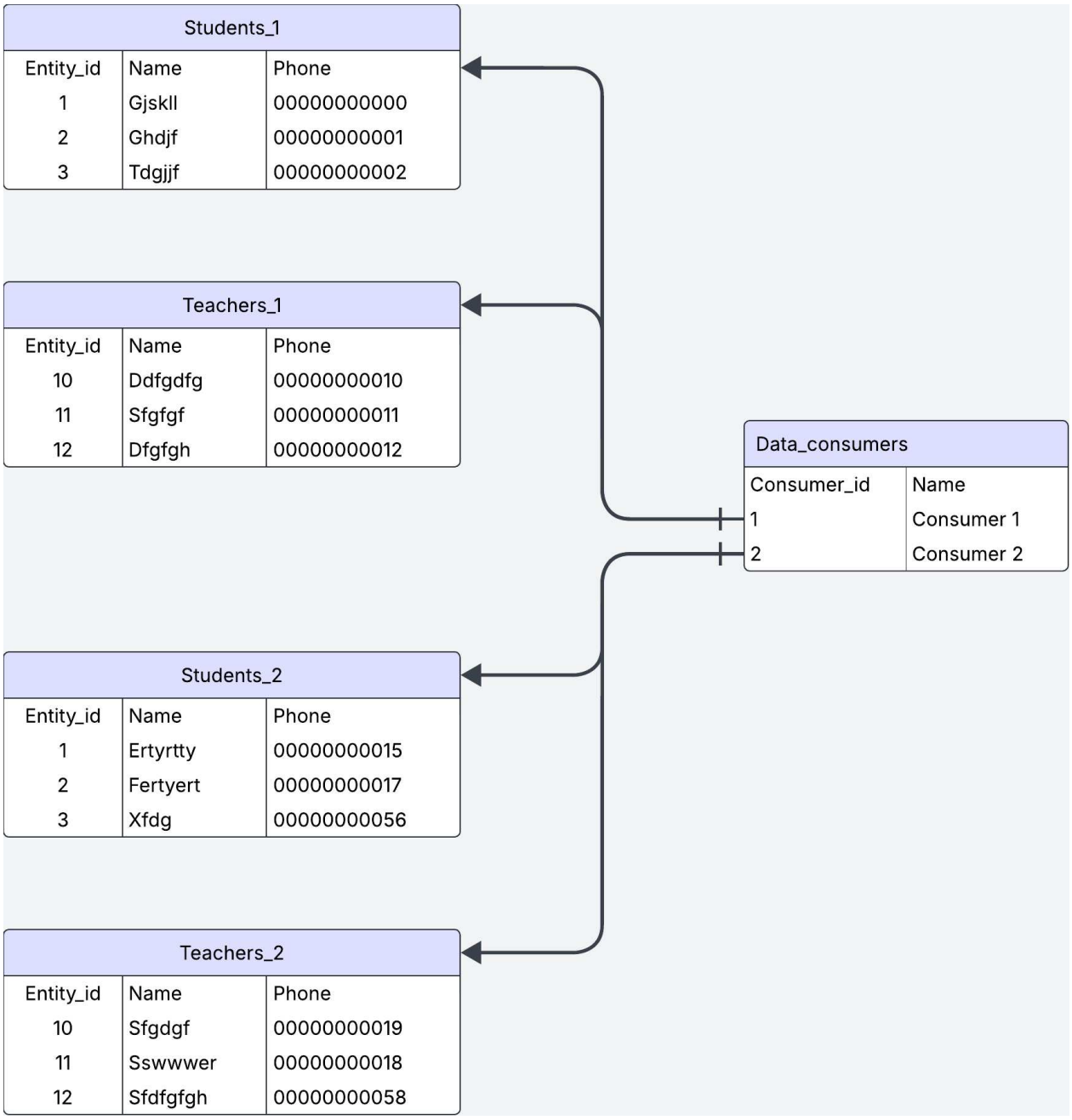

Рис. 4.3. Приклад таблиць з даними бази даних сервісу анонімізації

Виділено наступні особливості такої схеми таблиць бази анонімних даних. По-перше, чим з більшою кількістю споживачів анонімних даних інтегрований

навчальний заклад, тим більшу кількість таблиць матимемо у схемі бази даних. По-друге, чим більше різних типів персональних даних зберігає навчальний заклад тим більше таблиць анонімних їх версій матиме схема бази анонімних даних. Звідси отримано такі наслідки:

- Можливе зростання кількості таблиць у схемі бази анонімних даних навчального закладу. Але для сучасних СУБД тисячі навіть сотні тисяч таблиць не приносять ніяких проблем.
- Для кожного зовнішнього споживача є окремий сет таблиць, тобто окрема таблиця під кожен тип даних. Звідси паралельна робота з даними по кожному окремому типу даних кожного окремого споживача ніяким чином не впливає на консистентність даних інших користувачів, а також транзакції запитів інших споживачів даних. Що, як зазначалось раніше, є ключовою вимогою до системи анонімізації персональної інформації стейкхолдерів діджиталізованого освітнього закладу.

4.2 Програмне забезпечення інформаційної технології анонімізації/деанонімізації персональних даних стейкхолдерів діджиталізованої освіти

У цьому підрозділі продемонстровано практичне застосування розроблених теоретичних методів і алгоритмів, що стосуються анонімізації та деанонімізації персональних даних. Основою проведених досліджень стали наступні теоретичні напрацювання: метод анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти, метод деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти, алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти, алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти, схема впровадження анонімізації та деанонімізації персональних даних в інформаційному простору діджиталізованої освіти, вимоги до складових

архітектурного рішення інформаційної технології анонімізації персональних даних, структура бази даних інформаційної технології анонімізації персональних даних та їх складові. Крім того, при виконанні проєкту розробки програмного забезпечення використовувались напрацювання по [1–7, 173].

Далі опис створеного програмного забезпечення. Додано можливість навчальним закладам вибирати та встановлювати які саме дані по кожному типу користувачів вважаються чутливими й можуть потребувати додаткового захисту. На рис. 4.4 та 4.5 показано вкладку яка відповідає за такі налаштування.

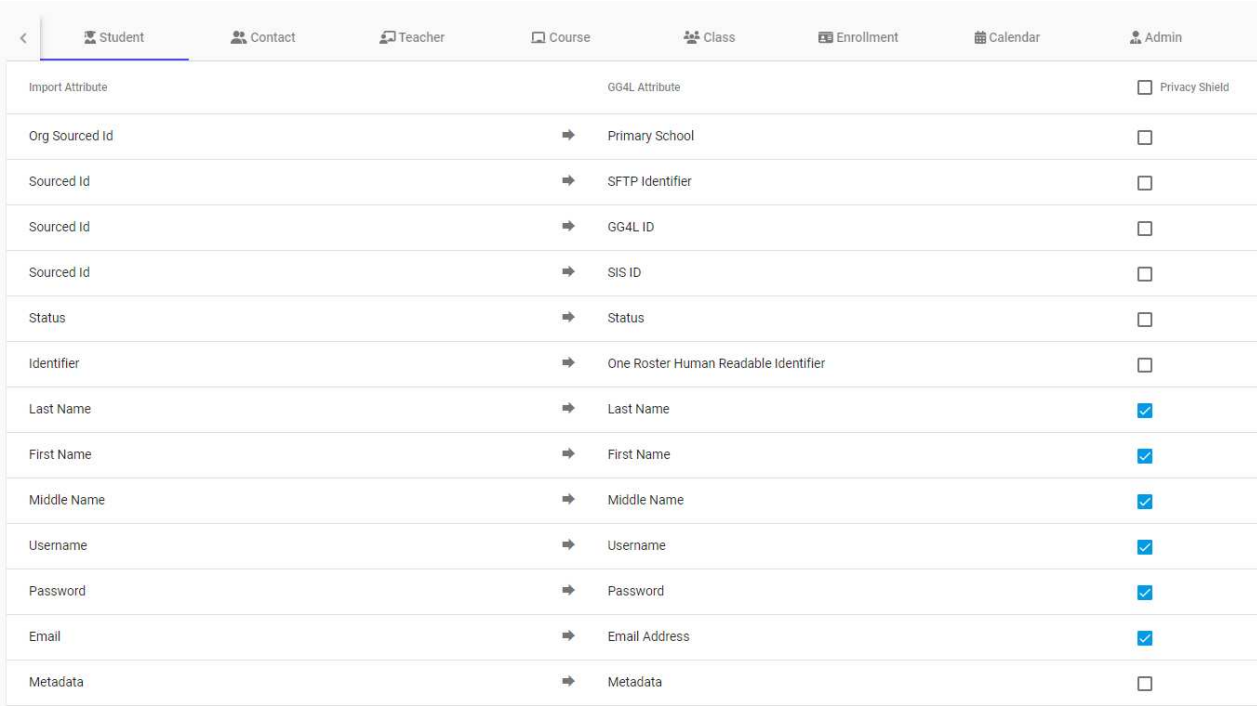

Рис. 4.4. Вкладка налаштування персональних даних інформаційних об’єктів навчального закладу в контексті “Студента”

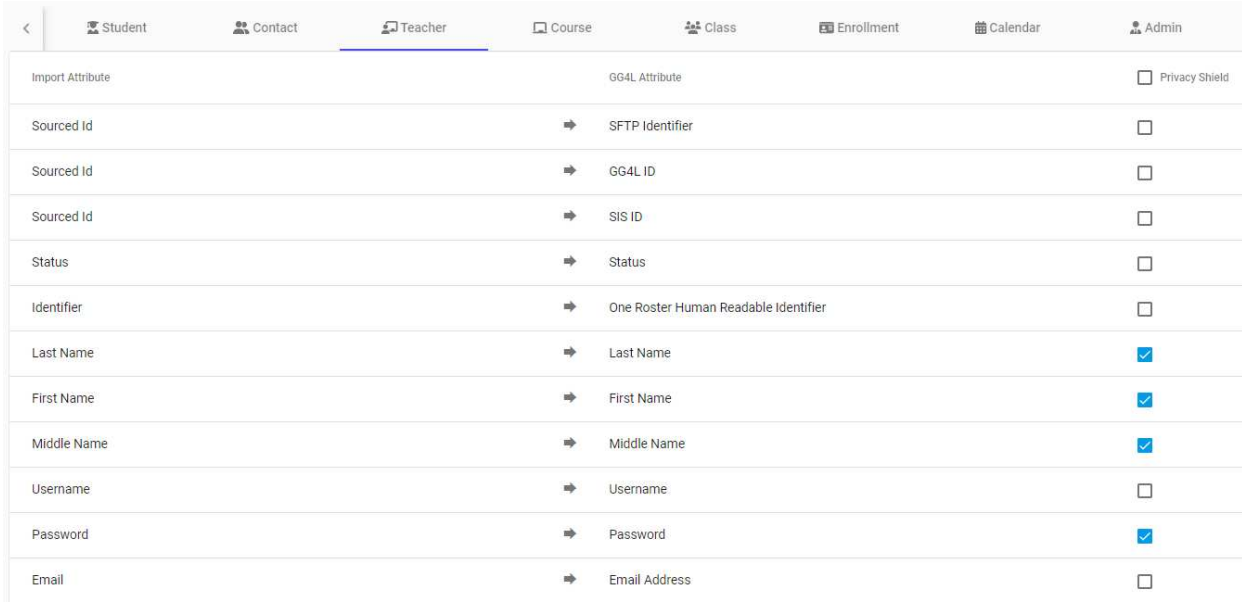

Рис. 4.5. Вкладка налаштування персональних даних інформаційних об’єктів навчального закладу в контексті “Викладача”

Як видно існує кілька типів інформаційних об’єктів, які можуть нести в собі персональну інформацію: “Студент”, “Контакт” (наприклад, батьки студента), “Викладач” та “Адміністратор”. Для кожного з цих типів можна налаштувати які атрибути вважатимуться системою як такі що потребують додаткової уваги та у деяких випадках посиленого захисту. На рис. 4.4 продемонстровано такі налаштування для об’єкта “Студент”, а на рис 4.5 для об’єкта “Викладач”. Оскільки налаштування виконуються однаковим чином для усіх об’єктів, але найпоширенішим є саме “Студент”, то більшість прикладів будуть розглядатись саме для цього типу інформаційного об'єкта. Ці налаштування може робити лише адміністратор навчального закладу і саме він вирішує які атрибути є особливими, а які ні. Загалом як тестовий приклад обрано такі атрибути як чутливі в інформаційному об’єкті “Студент”: ім’я, прізвище, по батькові, юзернейм, пароль та електронна адреса. А також ось такі для “Викладач”: ім’я, прізвище, по батькові та пароль. Це означає що у майбутньому при встановленні інтеграції з певною зовнішньою навчальною платформою ці атрибути будуть вважатись системою як чутлива персональна інформація.

Хоч навчальний заклад і є в центрі уваги, та саме він є джерелом даних, інтеграція неможлива за участі лише одного учасника. Адже навчальний заклад інтегрується з певними навчальними платформами. Як зазначалось раніше, навчальні платформи також можуть мати певні потреби в інформації, вимоги до її формату та особливості обробки персональної інформації користувачів для надання своїх сервісів. Тому також додано можливість споживачам даних визначати які саме дані вони можуть споживати в анонімізованому вигляді, а які мають все ж таки бути у відкритому стані. На рис. 4.6 та 4.7 показано вкладку таких налаштувань зі сторони зовнішньої навчальної платформи.

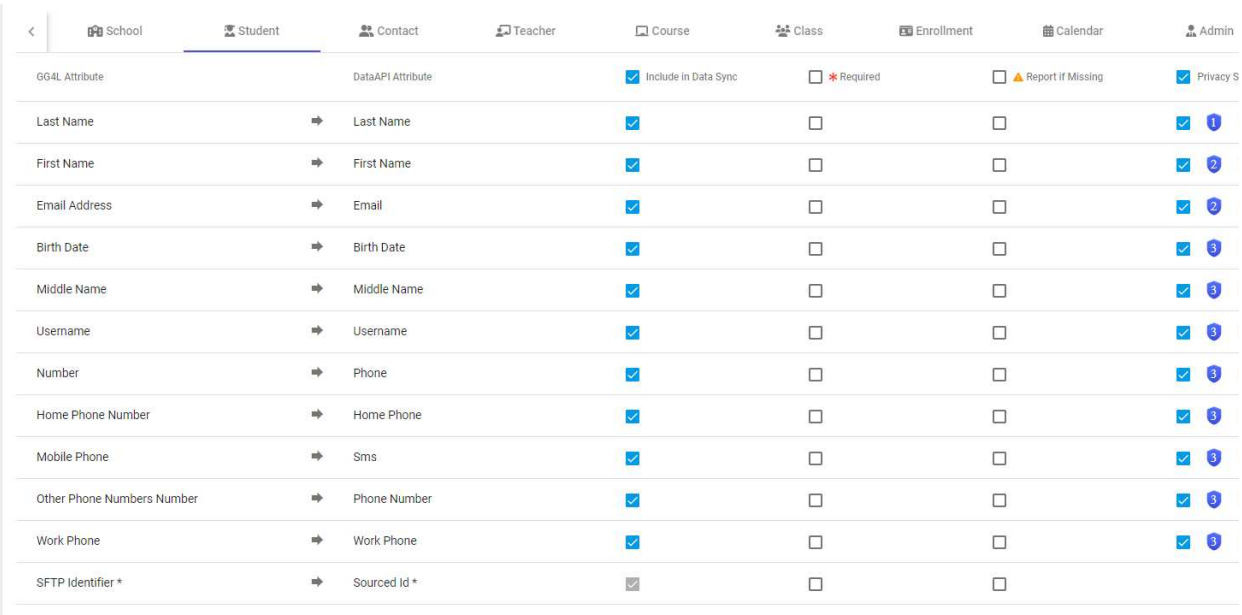

Рис. 4.6. Вкладка налаштування персональних даних інформаційних об’єктів споживача даних (контекст “Студента”)

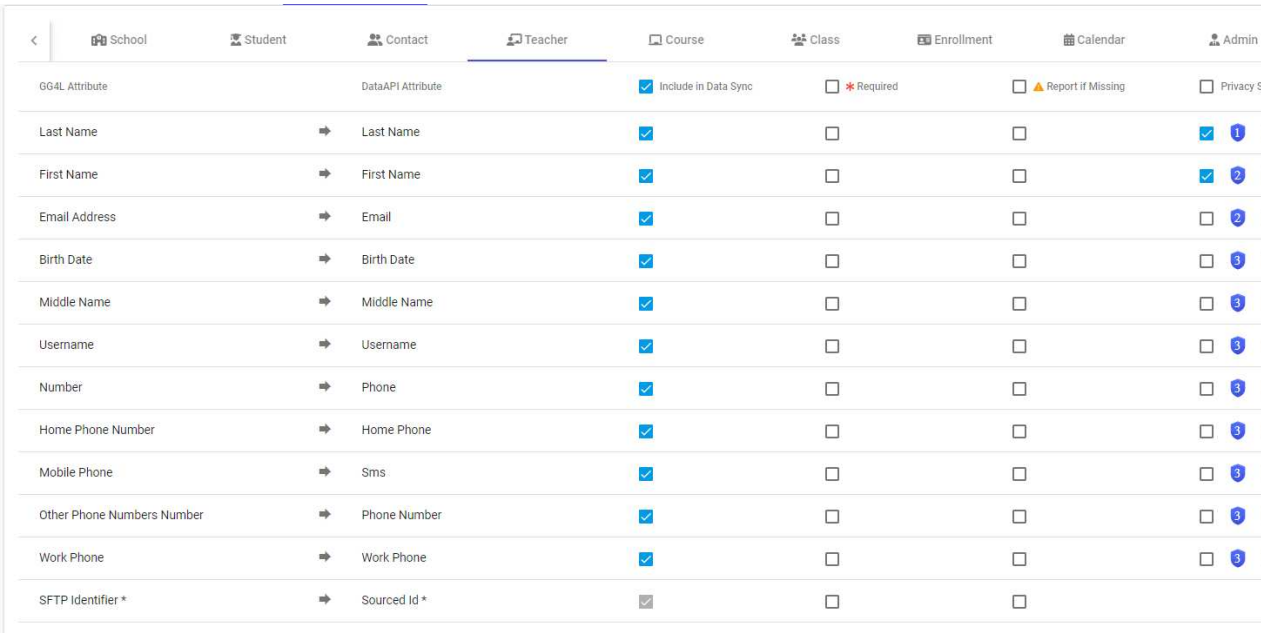

Рис. 4.7. Вкладка налаштування персональних даних інформаційних об’єктів споживача даних (контекст “Викладача”)

Ця вкладка дуже схожа на попередньо описану вкладку налаштувань персональних даних навчального закладу. Тут теж присутні усі ті ж самі об’єкті та їх атрибути. Єдина відмінність в сенсі цієї конфігурації. Якщо в випадку навчального закладу який є джерелом даних це були налаштування які дані вважаються персональними та є чутливими до втрати та витоку, то в даній ситуації ця конфігурація вказує які персональні атрибути інформаційних об’єктів зовнішня навчальна платформа може споживати в анонімізованому вигляді. Забігаючи наперед зазначається, що, поєднуючи налаштування персональних даних навчального закладу та споживача таких даних, можна створити інтеграцію оптимальним чином. Адже встановлюючи таку інтеграцію та вибираючи які дані будуть анонімізуватись, а які ні, є можливість взяти до уваги налаштування (які відображають побажання та вимоги) обох сторін, як постачальника інформації так і споживача.

Вертаючись до того що видно на цій вкладці, хоч тут і присутні усі ті ж самі інформаційні об’єкти та їх атрибути, що й у випадку конфігурації персональних даних для навчального закладу, адміністратор аккаунту зовнішньої навчальної платформи

вибрав інший перелік полів які така платформа може спожити в анонімізованому вигляді. А саме тут вибрано такі атрибути об’єкта “Студент”: ім’я, прізвище, по батькові, юзернейм, пароль, електронна адреса, дата народження та номери телефонів різного типу. Якщо для “Студента” цей перелік навіть більший ніж потрібно навчальному закладу продемонстровано раніше, то для “Викладача” він менший: ім’я та прізвище. Тобто якщо попередньо розглянутий навчальний заклад буде встановлювати інтеграцію з цим зовнішнім постачальником послуг з навчання, то у них буде неспівпадіння по атрибутах “Викладача”. Знову ж таки, забігаючи наперед, інтеграції налаштовуються вручну і сторони можуть домовитись про те які дані будуть анонімізуватись, а які ні.

Нижче розглянуто як же саме описані налаштування впливають на етап створення інтеграції. На рис 4.8 показано як виглядає вкладка налаштування атрибутів при запиті зовнішньою навчальною платформою на створення інтеграції з навчальним закладом.

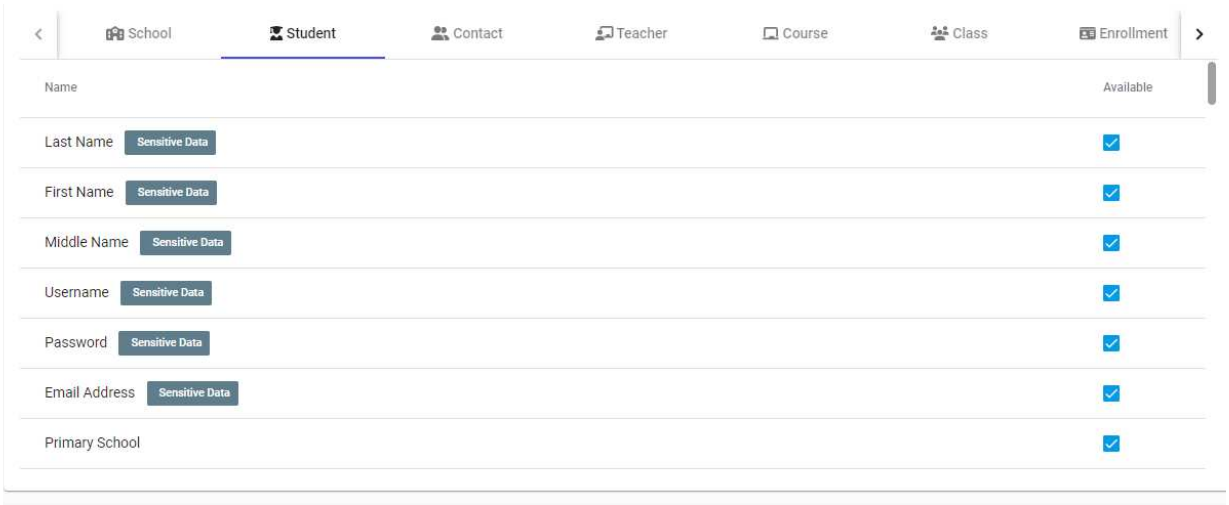

Рис. 4.8. Вкладка налаштування інтеграції з навчальним закладом на запит споживача даних без підтримки анонімізації

Якщо споживач даних хоче встановити інтеграцію з навчальним закладом, то йому показується які атрибути визначено навчальним закладом як чутливі. Але оскільки адміністратор цієї зовнішньої платформи (JesusTestDataConsumer1) не вказав

жодного атрибута, споживання якого підтримується в анонімізованому вигляді, то немає можливості вибрати хоча б один атрибут для споживання анонімізованим. Тобто, можна або відмовитись від споживання атрибутів які навчальний заклад вважає чутливими, або зробити запит і домовлятись, щоб адміністратор навчального закладу підтвердив інтеграцію з зовнішньою платформою надаючи доступ до справжніх, а не анонімізованих даних.

На рис. 4.9 показано налаштування запиту від зовнішньої навчальної платформи на інтеграцію з навчальним закладом з підтримкою анонімізації певних атрибутів (JesusTestDataConsumer2).

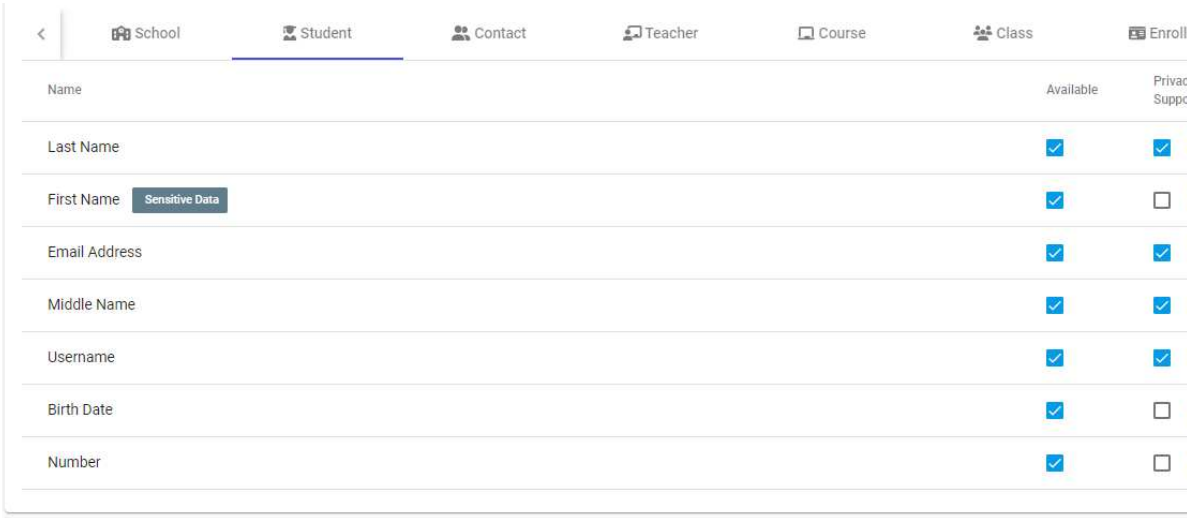

Рис. 4.9. Вкладка налаштування інтеграції з навчальним закладом на запит споживача даних з підтримкою анонімізації

Оскільки адміністратор цієї зовнішньої платформи вказав що платформа може споживати певні атрибути в анонімізованому вигляді, то з’являється можливість вмикати анонімізацію для цих атрибутів. Якщо у налаштуваннях навчального закладу певний атрибут позначено як чутливий, але споживач даних не включає анонімізацію цього атрибуту при запиті даних, то це поле буде підсвічуватись, на малюнку це атрибут “ім’я” інформаційного об’єкта “Студент”.

Розглянуто зміни які стосуються запиту інтеграції зі сторони споживача даних, але часто інтеграцію ініціює навчальний заклад. Зазвичай представники навчального

закладу домовляються про надання зовнішньою навчальною платформою певних навчальних сервісів, а тоді уже відбувається створення інтеграції в менеджмент інструмент і відповідно поширення даних. Тому зроблено зміни й для цього функціоналу. На рис. 4.10 та 4.11 показано як виглядає вкладка конфігурації запиту на інтеграцію навчального закладу з зовнішньою навчальною платформою.

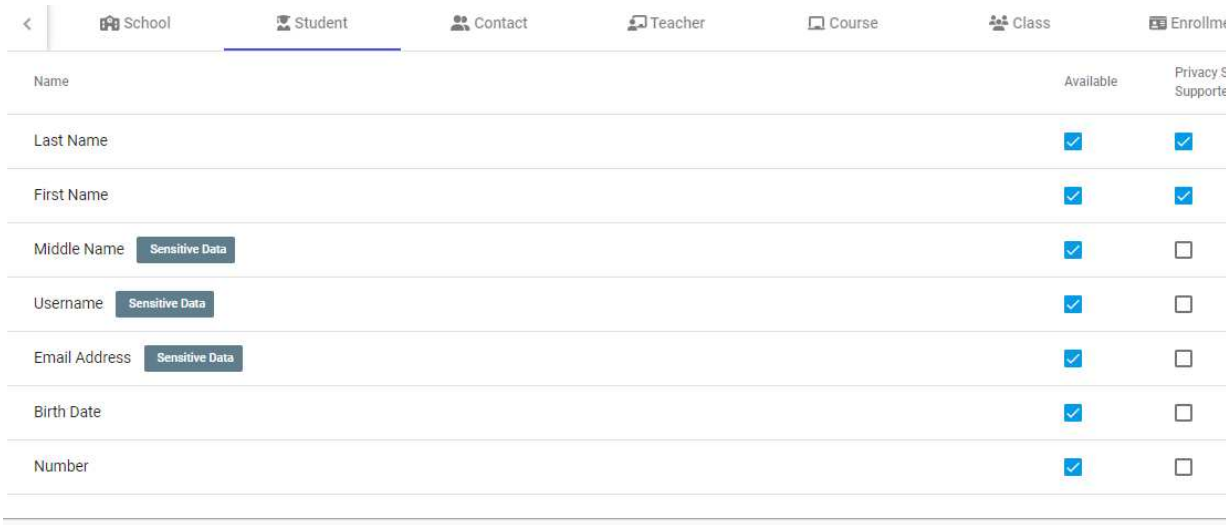

Рис. 4.10. Налаштування поширення атрибутів інформаційного об’єкта “Студент” у запиті на інтеграцію з зовнішньою навчальною платформою з частковим увімкненням анонімізації персональних даних

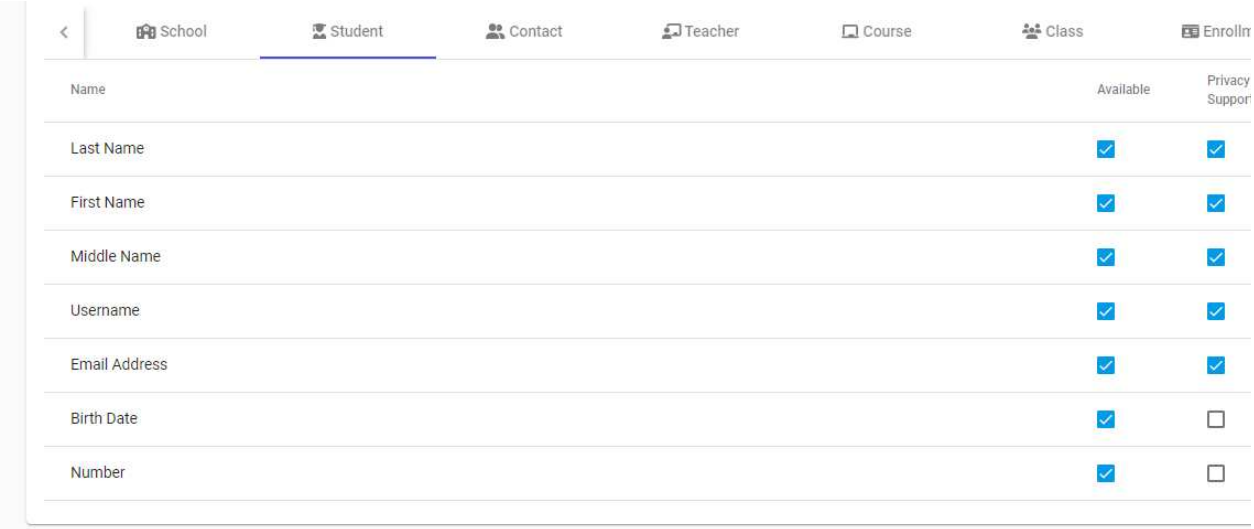

Рис. 4.11. Налаштування поширення атрибутів інформаційного об’єкта “Студент” у запиті на інтеграцію з зовнішньою навчальною платформою з увімкненням анонімізації персональних даних

При запиті на створення інтеграції зі споживачем даних навчальний заклад може вказати які атрибути потрібно анонімізувати. На прикладі (рис. 4.10 та 4.11) показано як це виглядає для об’єкта “Студент”, але і для інших інформаційних об’єктів можна задавати такі ж налаштування. На першому малюнку видно, що адміністратор при налаштуванні анонімізації вибрав увімкнув анонімізацію не для усіх чутливих атрибутів. Ті атрибути, які були не вибрані, але вважаються чутливими підсвічуються. У такому випадку це атрибути “Студента”: по батькові, юзернейм та електронна пошта. У другому прикладі (рис. 4.8) адміністратор увімкнув анонімізацію для усіх атрибутів визначених навчальним закладом як такі що є персональними і потребують додаткового захисту. Якщо обидві сторони погодять налаштування і затвердять інтеграцію, дані навчального закладу будуть поширюватися з зовнішньою навчальною платформою саме за цими правилами. Тобто, анонімізація працюватиме для усіх атрибутів, які в підсумку в цій інтеграції будуть вказані як ті, що мають анонімізуватись.

Важливо зазначити, що хоч кожен з учасників таких інтеграцій і має свої налаштування в контексті анонімізації, кожна окрема інтеграція може мати свій погоджений набір параметрів які будуть анонімізуватись. Тобто навчальний заклад може поширювати певні атрибути для деяких зовнішніх споживачів у відкритому вигляді, а для решти в закритому. Це потрібно у випадках коли певна зовнішня платформа не може забезпечити потрібні сервіси навчальному закладу якщо є анонімізованими певні атрибути. Тобто створений функціонал не лише забезпечує додатковий захист персональних даних стейкхолдерів навчального процесу, а й дає гнучкість у налаштуваннях, якщо це потрібно у виняткових ситуаціях.

Отже, описано основний доданий функціонал з анонімізації персональної інформації, а це означає що потрібно розповісти й про зміни в контексті деанонімізації. Ще до виконання впровадження анонімізації у менеджмент систему визначено, що

необхідно також забезпечити можливість деанонімізації даних. Це потрібно як для вирішення проблем, що виникатимуть у користувачів у майбутньому. Крім того, деанонімізація необхідна у деяких виняткових ситуаціях для моніторингу і підвищення якості продукту. Приклад застосування деанонімізації буде показано в наступному підрозділі. Але варто вказати, що для того щоб отримати доступ до функціоналу деанонімізації, потрібно мати особливий набір ключів, який поширюється лише у виняткових випадках адміністрацією і для якого працює постійна ротація. Крім того, доступ до даних регламентується роллю користувача. Якщо це “Адміністратор”, то можливий доступ до більшості даних навчального закладу, якщо “Викладач”, то лише до особистих даних, а також даних студентів які є у складі курсів які веде цей викладач. У випадку “Студента” можна отримати лише власні дані.

Функціонал з анонімізації забезпечує додатковий шар захисту персональної інформації. Також інструменти по деанонімізації розроблялись відповідно до суворих вимог захисту інформації, що мінімізує ймовірність несанкціонованого доступу до реальних персональних даних учасників навчального процесу.

4.3 Застосування інформаційної технології анонімізації/деанонімізації персональних даних стейкхолдерів діджиталізованої освіти

Створено додатковий шар анонімізації персональних даних стейкхолдерів освітнього процесу. Також реалізовано функціонал з деанонімізації таких даних. Тому застосовано розроблені покращення та показано як саме це виглядає на практиці. На рис. 4.12 показано як виглядають дані тестового студента “Nina Muraha” для споживача даних “JesusTestDataConsumer1”, який споживає усі атрибути у відкритому вигляді. А на рис 4.13 дані того ж тестового студента які споживає зовнішня навчальна платформа “JesusTestDataConsumer2”, тобто певні атрибути будуть анонімізовані.

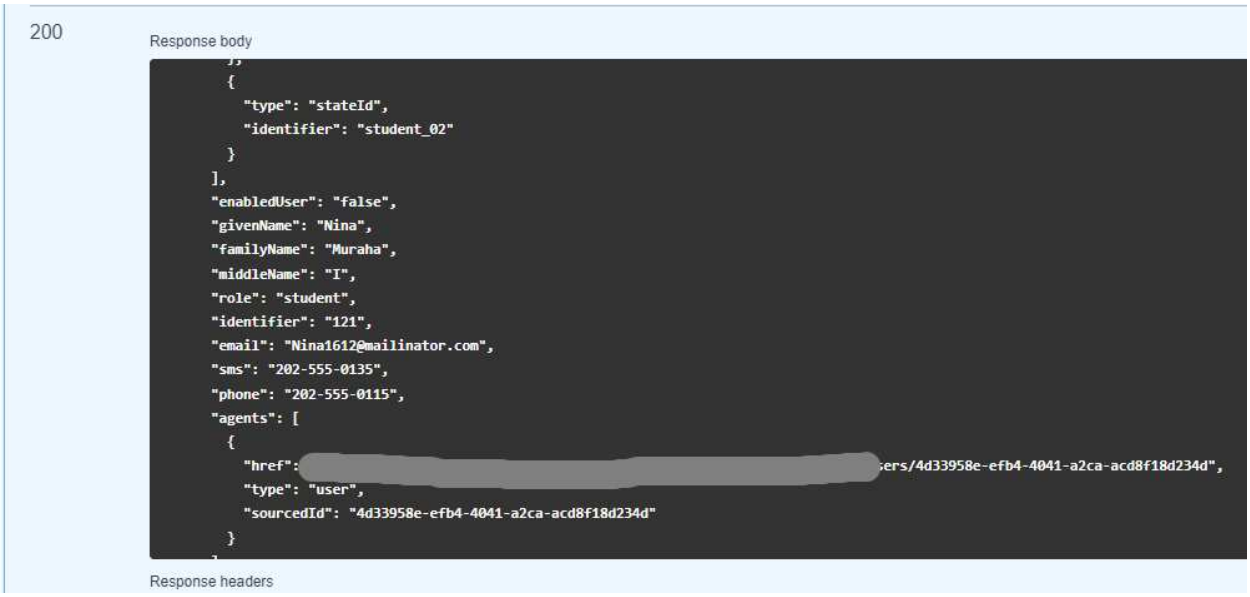

Рис. 4.12. Приклад читання даних студента” Nina Muraha” споживачем даних без застосування анонімізації (JesusTestDataConsumer1)

Рис. 4.13. Приклад читання даних студента “Nina Muraha” споживачем даних із застосуванням анонімізації (JesusTestDataConsumer2)

На рис. 4.8 видно, що при інтеграції навчального закладу зі споживачем даних не було ввімкнено анонімізацію для жодного атрибута й усі персональні дані поширюються в відкритому вигляді. Звісно іноді бувають ситуації коли потрібно мати

доступ до даних учасників навчального процесу, але в більшості випадків частину атрибутів можна анонімізувати. Саме для такого випадку є приклад продемонстрований на рис. 4.11. Створюючи інтеграцію зі споживачем даних “JesusTestDataConsumer2”, адміністратор увімкнув анонімізацію для наступних атрибутів: ім’я, прізвище, по батькові, юзернейм та електронна адреса. Відповідно замість реальних даних показано токени згенеровані системою для їх заміни. Тобто цей споживач замість реальних даних отримав наступні токени:

- Ім’я: реальне значення – Nina, отриманий токен – N-ggf’xjtdryr.
- По батькові: реальне значення – I, отриманий токен – I-ggm’xjtdryr.
- Прізвище: реальне значення – Muraha, отриманий токен – M-ggl’xjtdryr.
- Юзернейм: реальне значення – Nina1612112, отриманий токен – N-ggu’xjtdryr.
- Електронна адреса: реальне значення – Nina1612@mailinator.com, отриманий токен – QEXOzEyuqbUftUHz@581ab6aa-d3e0-4bbe-8717-4d5a53bca181.piixyz.com.

Унікальні токени генеруються для кожного користувача та для кожної зовнішньої навчальної платформи. Це означає, що колізії неможливі й навіть маючи набори даних різних зовнішніх платформ не вийде зіставити дані та детокенізувати персональну інформацію того чи іншого учасника навчального процесу.

Ще одним важливим нюансом є те, що як видно з прикладу шаблон анонімізації усіх полів був обраний зі збереженням формату даних. Це дуже важливо, адже більшість споживачів даних мають валідацію атрибутів які вони вичитують в контексті інтеграції з навчальними закладами. Тобто навіть при підтримці споживання анонімізованих значень певних атрибутів інформаційних об’єктів зовнішньою навчальною платформою могли б виникнути проблеми за умови не врахування цього фактору.

Вище продемонстровано застосування анонімізації в інтеграції навчального закладу та зовнішньої навчальної платформи. Як зазначалось раніше, іноді потрібно

мати можливість дані деанонімізовувати на рис 4.14 показано приклад виконання запиту по деанонімізації даних.

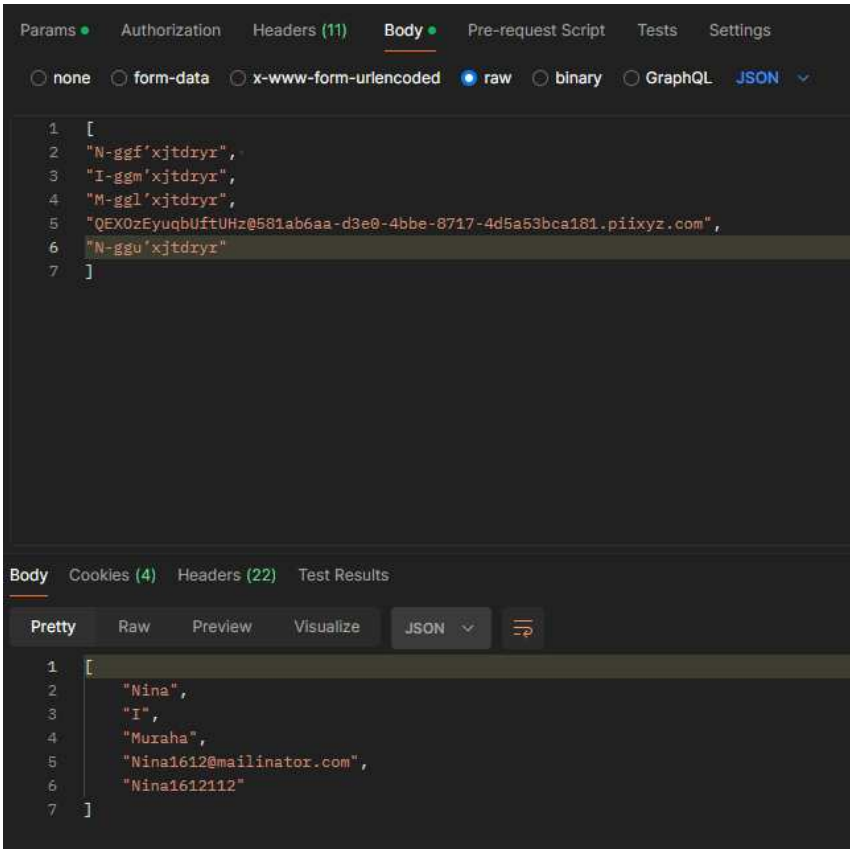

Рис. 4.14. Запит на деанонімізацію токенів які були згенеровані системою раніше споживачу даних “JesusTestDataConsumer2”

Нижче описано процес деанонімізації попередньо анонімізованих атрибутів тестового студента “Nina”. Насамперед потрібно пройти аутентифікацію. Для цього потрібно мати доступ до персонального особливого набору ключів. Виконавши аутентифікацію та отримавши “аксес токен”, формується запит на деанонімізацію потрібних токенів. Під час виконання цього запиту система авторизує користувача та автоматично визначить його роль. У такому випадку використовувалась роль “Адміністратор”, тож доступ до даних було надано. Відправивши перелік токенів, які потрібно деанонімізувати отримано справжні дані, які ховаються за цими токенами:

- Відправлено токен – N-ggf’xjtdryr, отримано значення – Nina.

- Відправлено токен – I-ggm’xjtdryr, отримано значення – I.
- Відправлено токен – M-ggl’xjtdryr, отримано значення – Muraha.
- Відправлено токен – -ggu’xjtdryr, отримано значення – Nina1612112.
- Відправлено токен – QEXOzEyuqbUftUHz@581ab6aa-d3e0-4bbe-8717-4d5a53bca181.piixyz.com, отримано значення – Nina1612@mailinator.com.

Як видно деанонімізація працює коректно й усі запитані токени деанонімізовано правильно. Відповідно використання анонімізації має не лише сенс, а тепер і є зручною для усіх користувачів. Адже за потреби та, маючи необхідні права, можна безпечно отримати доступ до потрібних реальних даних учасників навчального процесу.

4.4 Ефективність застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації

Щоб переконатись в дієвості та користі розробленої інформаційної технології потрібно виконати оцінку його ефективності. Для цього потрібно визначити чи застосування створеного програмного забезпечення знижує ймовірність виникнення ризикових подій витоку персональних даних учасників навчального процесу. Тобто потрібно провести повторні оцінювання та розрахунки які були виконані в другому розділі при постановці задачі з урахуванням нового фактора. Тим же самим групам експертів, які формували дані, що відображено в табл. 2.9, 2.10 та 2.11 другого розділу роботи потрібно дати завдання виконати повторне оцінювання ймовірності виникнення ризикових подій, серйозності їх наслідків та ціннісну оцінку ймовірних причин виникнення цих подій з урахування застосування розробленої інформаційної технології анонімізації персональних даних стейкхолдерів навчального процесу.

Після проведення повторного оцінювання експертами отримано результати зображені в табл. 4.1 та 4.2.

Таблиця 4.1. Експертна оцінка ризикових подій витоку персональної інформації та їх наслідків з урахуванням застосування інформаційної технології

№	Ризикова подія	Можливі наслідки	*Ve* - ймовірність виникнення ризикової події (1-10)	*Re* - серйозність наслідків виникнення ризикової події (1-10)
E1	Витік персональних даних при вичитці зовнішніми споживачами	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – низька ймовірність. Витік усіх персональних даних усіх клієнтів – низька ймовірність.	1	4
E2	Витік персональних даних з бази даних навчальних систем зовнішніх споживачів	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних	1	10

		деяких клієнтів – висока ймовірність. Витік усіх персональних даних усіх клієнтів – висока ймовірність.		
E3	Несанкціоноване поширення даних зовнішнім споживачем з іншим платформами	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – середня ймовірність. Витік усіх персональних даних усіх клієнтів – низька ймовірність.	1	6
E4	Витік персональних даних через дії персоналу зовнішньої компанії-споживача даних	Витік частини персональних даних деяких клієнтів – висока ймовірність. Витік усіх персональних даних деяких клієнтів – низька ймовірність.	1	5

		Витік усіх персональних даних усіх клієнтів – висока низька.		

Таблиця 4.2. Ціннісні оцінки причин настання ризикових подій з врахуванням застосування інформаційної технології

№	Ризикова подія	*Ce* - Оцінка (1-10)
p1	Поширення персональних даних третім сторонам	1
p2	Збирання персональної інформації третіми сторонами	1
p3	Низький рівень захисту бази даних	8
p4	Низький рівень підготовки персоналу	5
p5	Відсутність культури роботи з приватними даними персоналу зовнішніх компаній	4
p6	Низький рівень захисту каналів комунікації	3
p7	Зовнішні атаки зловмисників	6
p8	Непроходження зовнішніми споживачами сертифікацій зовнішнього аудиту	2
p9	Використання застарілих інформаційних технологій	5
p10	Оренда апаратних потужностей у сумнівних постачальників	1
p11	Використання персональної інформації в цілях зовнішньої платформи (реклама, тестування тощо)	1

На рис. 4.15 зображено зміни оцінок експертів ймовірності виникнення ризикових подій витоку персональних даних до і після застосування напрацювань з анонімізації. Як видно, ймовірність виникнення по всіх подіях (*E1, E2, E3, E4*) скоротилась до 1 балу з 10 можливих що є надзвичайно низьким значенням. Та все ж, за розробленим методом, персональні дані не повинні поширюватись взагалі, а отже, логічно припустити, що оцінки мають бути взагалі 0. Але експертами зазначено, що навіть з застосуванням розробленого методу анонімізації та деанонімізації персональних даних все ж існує певна невелика ймовірність що витік можливий через людський фактор, особливості імплементації конкретним навчальним закладом чи інше.

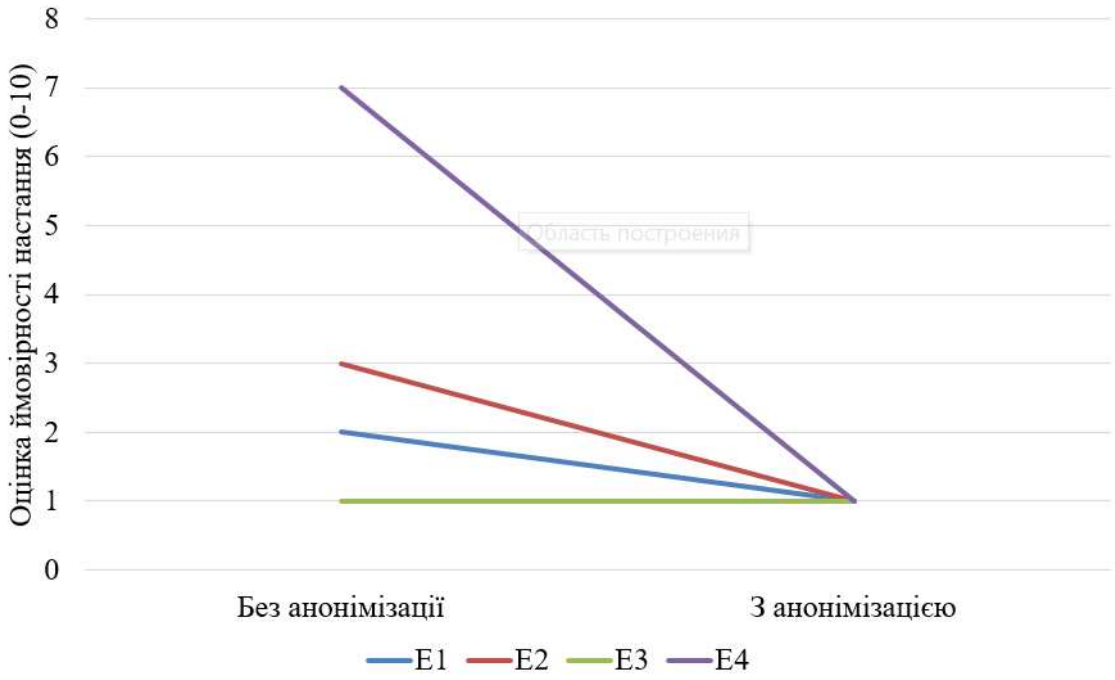

Рис. 4.15. Оцінки експертів ймовірності виникнення ризикової події витоку персональних даних до та після розробленого методу

Крім оцінки ймовірності маємо оцінки ваги кожної з причин (*p1, p2, p3, p4, p5, p6, p, p8, p9, p10, p11*) виникнення ризикових подій витоку персональних даних (рис. 4.15).

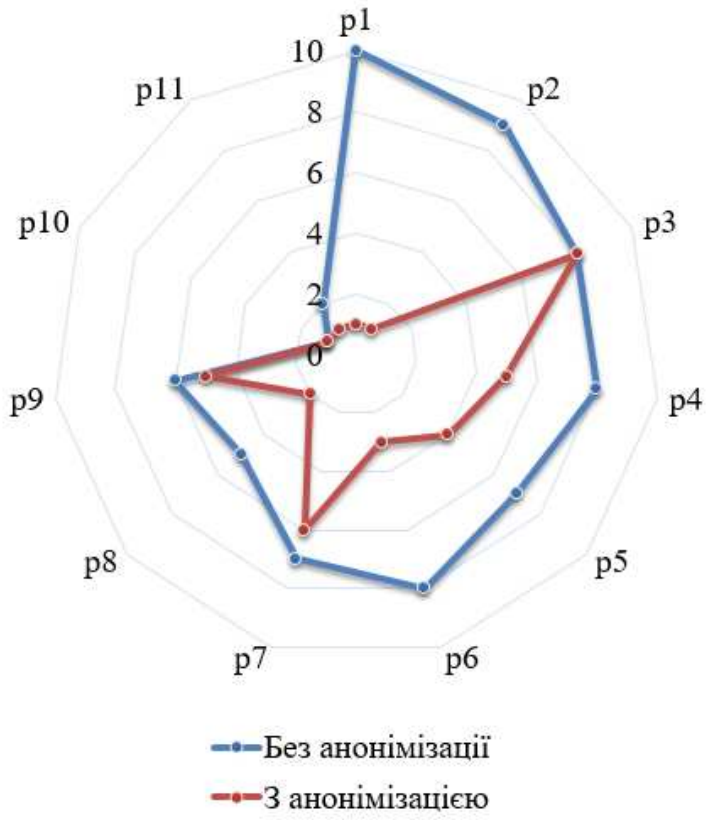

Рис. 4.16. Оцінки експертів ваг можливих причин виникнення ризикових подій витоку персональних даних

Як видно з діаграми на рис. 4.16 ваги усіх причин крім однієї вдалось суттєво знизити. Що говорить про ефективність розробленого методу та імплементованого за ним програмного забезпечення.

Для точної оцінки ефективності створеного програмного забезпечення E запропоновано таку оцінку виразити відношенням сумарної оцінки усіх причин ризикових подій до застосування інформаційної технології та після *(4.1)*:

$$E = MPA/MPB, \qquad (4.1)$$

де MPA – сумарна оцінка усіх причин ризикових подій до застосування інформаційної технології ($\sum_{j=1}^{11} MP_j$);

MPB – сумарна оцінка усіх причин ризикових подій після застосування інформаційної технології ($\sum_{j=1}^{11} MP_j$).

За таких умов інформаційну технологію можна вважати ефективною якщо результат обрахунку значення *E* є більшим одиниці. Тож виконавши обрахунки застосувавши формулу *2.4* та вище визначеною формулою *4.1*, отримано таке значення ефективності *E = 3.28.*

Як видно з розрахунків значення *E* є значно більшим одиниці. Це свідчить, що розроблена інформаційна технологія виконує свою функцію по підвищенню рівня захищеності персональних даних стейкхолдерів освітнього процесу і є ефективною.

Додатково після застосування розробленої інформаційної технології, крім мінімізації ризиків витоку персональних даних при інформаційній взаємодії в освітньому діджиталізованому середовищі на попередньо ідентифікованих точках можливих витоків таких даних виділено кілька додаткових плюсів. По-перше, підкреслено що створений інструментарій допомагає відповідати вимогам законодавства щодо захисту персональних даних. По-друге, нові можливості допомагають запобігти негативним наслідкам для репутації закладу у випадку, якщо дані будуть передані або оброблені невідповідним чином, адже забезпечення анонімності даних демонструє етичну відповідальність закладу та його турботу про приватність учасників навчального процесу. По-третє, студенти та співробітники більш впевнені в безпеці своїх даних, що підвищило довіру до закладу. І по-четверте, організації стало легше співпрацювати з різними платформами та компаніями, оскільки анонімізовані дані зазвичай не підпадають під суворе регулювання, яке застосовується до персональних даних.

ВИСНОВКИ ДО РОЗДІЛУ 4

1. У четвертому розділі більшу увагу приділено практичній частині дослідження, зокрема розроблено архітектуру інформаційної технології анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти.

2. В контексті розробки архітектури створено загальну схему архітектури такої інформаційної технології та детально описано кожен її компонент. На розробленій схемі показано як сервіс анонімізації інтегрується в менеджмент систему навчального закладу.

3. Після цього сформульовано вимоги до складових архітектурного рішення інформаційної технології. Вимоги розроблено до наступних компонентів: база даних системи анонімізації, шар доступу до бази даних, шар бізнес-логіки системи анонімізації та інтерфейс доступу до даних зовнішніми споживачами

4. Додатково описано структуру бази даних інформаційної технології анонімізації персональних даних. Варто зазначити, що розроблена структура дозволяє виконувати швидкий пошук анонімізованих даних, що є важливим при віддачі даних зовнішнім користувачам.

5. Розроблено програмне забезпечення інформаційної технології анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти. Також продемонстровано як виглядають налаштування анонімізації в контексті певних типів даних (Студент, Викладач).

6. Застосовано інформаційні технології анонімізації та деанонімізації персональних даних. На прикладі показано як користуватись новоствореним функціоналом.

7. Проведено оцінку ефективності застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації.

ВИСНОВКИ

1. На початку роботи виконано аналіз існуючих підходів до управління інформаційними потоками освітнього середовища у контексті діджиталізації. Зокрема проаналізовано роботи у таких напрямках: вплив діджиталізації на інформаційні потоки в освітній сфері, існуючі підходів до управління інформаційними потоками у діджиталізованій освітній сфері, існуючі моделі та інформаційні рішення із захисту персональних даних у діджиталізованому освітньому середовищі, проблемні завдання управління інформаційними потоками діджиталізованого освітнього середовища та застосування анонімізації з метою захисту персональних даних в інформаційних потоках в освітній сфері.

2. Розроблено концепцію управління потоками персональних даних у контексті діджиталізації освітньої сфери. В контексті якої створено та детально описано схему інформаційних потоків діджиталізованого освітнього середовища в контексті поширення персональних даних його стейкхолдерів. Ідентифіковано головних стейкхолдерів інформаційної взаємодії діджиталізованої сфери освіти. Після цього на основі аналізу інформаційних взаємодій у діджиталізованому освітньому середовищі та формування категорій стейкхолдерів освітнього процесу розроблено модель інформаційної взаємодії у діджиталізованій освітній сфері. Отримавши достатній інформаційний базис, побудовано модель визначення витоку персональних даних діджиталізованої інформаційної взаємодії. Ця модель дозволяє зрозуміти основні точки контролю потоків персональних даних.

3. Розроблено модель ризиків витоку персональних даних при інформаційній взаємодії діджиталізованого освітнього середовища. Модель демонструє зону виникнення ризикових подій витоку персональних даних. Крім того, проведено експертну оцінку причин витоку персональної інформації та їх можливих наслідків. Після чого виділено головні ймовірні причини виникнення подій витоку персональних даних.

4. Зрозумівши основні ризики пов’язані з витоком персональних даних стейкхолдерів діджиталізованої освіти, створено принципи мінімізації поширення персональних даних учасників навчального процесу.

5. Наступним кроком стало формування моделі управління зберіганням потоків даних освітнього середовища. Модель дає можливість підготовлено підійти до прийняття рішення про місце розташування інформаційних потоків навчального закладу, що є важливим фактором з точки зору захисту персональної інформації стейкхолдерів освітнього процесу.

6. Створено моделі управління потоками персональних даних у контексті діджиталізації освітньої сфери. До яких входять модель анонімізації персональних даних стейкхолдерів в потоках даних при інформаційній взаємодії у діджиталізованому освітньому середовищі, а також модель деанонімізації персональних даних стейкхолдерів в потоках даних при інформаційній взаємодії у діджиталізованому освітньому середовищі. Ці моделі демонструють які дані повинні покидати межі діджитал системи навчального закладу, а які ні. Також на моделі анонімізації видно яка інформація буде вертатись навчальному закладу. Так само модель діджиталізації описує правила інформаційної взаємодії при запитах зовнішніх платформ на деанонімізацію даних.

7. Розроблено метод управління потоками персональних даних в умовах діджиталізації освітньої сфери. Метод детально описує імплементацію та застосування програмного забезпечення для анонімізації та деанонімізації персональної інформації головних інформаційних об’єктів навчального простору (Студент, Викладач, Адміністратор та інші). В межах створеного методу було:

а. створено алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти, який покроково описує кожен етап створення та інтеграції сервісу анонімізації в діджитал систему менеджменту даних навчального закладу, починаючи плануванням і закінчуючи створенням фінальних звітів;

b. створено алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти який у свою чергу описує кроки які необхідно пройти для розробки, а також впровадження сервісу деанонімізації у діджитал менеджмент систему навчального закладу;

c. створено та описано загальну схему впровадження анонімізації та деанонімізації персональних даних в інформаційному просторі діджиталізованої освіти;

d. розроблено та детально описано метод анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти; його можна застосовувати окремо від загального методу, але у більшості випадків анонімізація не має сенсу без деанонімізації;

e. створено метод деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти, який дозволяє впровадити сервіс деанонімізації, але він має зміст тільки якщо попередньо впроваджено анонімізацію;

f. об’єднано методи анонімізації та деанонімізації персональних даних та на їх основі отримано метод одночасного впровадження анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти.

8. Розроблено та застосовано інформаційну технологію управління потоками персональних даних освітнього середовища в умовах діджиталізації та визначено її ефективність. Зокрема було:

a. створено архітектуру інформаційної технології анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти, яка містить у собі загальну схему архітектури інформаційної технології, вимоги до складових архітектурного рішення інформаційної технології та структуру бази даних;

b. імплементовано програмне забезпечення для анонімізації та деанонімізації персональних даних стейкхолдерів діджиталізованої освіти;

c. застосовано інформаційні технології анонімізації та деанонімізації персональних даних;

d. проведено оцінку ефективності застосування інформаційної технології управління потоками персональних даних освітнього середовища в умовах діджиталізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тімінський О. Г. & Райчук І. В. (2019). Метод ціннісно-орієнтованого управління зацікавленими сторонами проекту діджиталізації. Управління проектами та розвиток виробництва, 3(71), 114–120.

2. Тімінський О. Г. & Райчук І. В. (2019). Передумови розробки моделей і методів для управління проектом створення генералізованого штучного інтелекту на базі ціннісного підходу. У Матеріали VI міжнародної науково-практичної конференції «Інформаційні технології та взаємодії» (с. 80–83). Київ.

3. Тімінський О. Г., Войтенко О. С. & Райчук І. В. (2021). Аналіз моделей і методів діджиталізації бізнес-процесів. Управління розвитком складних систем, 46, 38–47.

4. Райчук І. В., Хлевна Ю. Л., Войтенко О. С. & Тімінський О. Г. (2022). Розробка моделі діджиталізації процесу закупівель Hardware для IT-компанії. Управління розвитком складних систем, 50, 44–51.

5. Raichuk I., Khlevna I., Timinskyi O. & Voitenko O. (2022). Cognitive model of digitalization of business processes of a project-oriented IT company. CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3382/Paper12.pdf

6. Khlevna I., Raichuk I. & Timinskyi O. (2023). The development of the information technology architecture for the anonymisation of stakeholders personal data of digitalized education based on formulated criteria and requirements. In Workshop Proceedings of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023) (Kyiv, Ukraine, November 20-21, 2023, с. 139–148).

7. Бушуєв С., Івко А. & Райчук І. В. (2023). Вибір моделі організаційної структури проєкту діджиталізації бізнес процесів в контексті синкретичного управління. Вісник Львівського державного університету безпеки життєдіяльності, 28, 5–13.

8. Raichuk I., Kolesnikova K., Khlevna I., Timinskyi O. & Kubiavka L. (2024). Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools. Procedia Computer Science, 231, 347–352. https://doi.org/10.1016/j.procs.2023.12.215

9. Райчук І. В. & Мірошниченко І. В. (2025). Модель управління зберіганням потоків даних освітнього середовища. Наука і техніка сьогодні, Серія «Техніка», 1(42), 1360–1379.

10. Santosa A. B., Sukirman S. & Subaidi S. (2022). Strategi manajemen perpustakaan digital untuk meningkatkan kualitas akademik. Kelola: Jurnal Manajemen Pendidikan, 9(2), 136–147. https://doi.org/10.24246/j.jk.2022.v9.i2.p136-147

11. Petrov P., Kuyumdzhiev I., Malkawi R. & Dimitrov G. (2022). Digitalization of educational services with regard to policy for information security. TEM Journal, 11(3), 1093–1102. https://doi.org/10.18421/TEM113-14

12. Bakhmat N. & Smorgun M. (2022). On the role of digitalization and globalization for the development of mobile video games in the education of the future: trends, models, cases. Futurity Education, 2(4), 63–74. https://doi.org/10.57125/FED.2022.25.12.07

13. Oleksiienko A., Kotendzhy L., Kyryllova Y., Kaminskyy V. & Viesova O. (2022). An analysis of the digital university phenomenon: dilemmas, new opportunities. Futurity Education, 2(4), 18–25. https://doi.org/10.57125/FED.2022.25.12.02

14. Tsekhmister Y. (2022). Education of the future: from post-war reconstruction to EU membership (Ukrainian case study). Futurity Education, 2(2), 42–52. https://doi.org/10.57125/FED/2022.10.11.28

15. Majid T. T., Sihite N. E. P., Farelluddien M., Purnama R. Y., Febriantina S. & Fidhyallah N. F. (2023). Heutagogy-based learning in the era of Society 5.0. JP (Jurnal Pendidikan): Teori Dan Praktik, 8(1), 77–85. https://doi.org/10.26740/jp.v8n1.p77-85

16. Wackenhut A. F. & Gillette M. B. (2022). «Covid-19 and (re)learning teaching: Never let a crisis go to waste». Högre utbildning, 12(1), 52–65. https://doi.org/10.23865/hu.v12.3562

17. Osabwa W. (2022). Coming to terms with COVID-19 reality in the context of Africa's higher education: Challenges, insights, and prospects. Frontiers in Education, 7, 643162. https://doi.org/10.3389/feduc.2022.643162

18. Chernenko A. (2021). Information and digital competence as a key demand of modern Ukrainian education. Educational Challenges, 26(2), 38–51. https://doi.org/10.34142/2709-7986.2021.26.2.04

19. Areskoug Josefsson K., Haarr K. H., Eriksen S. S. & Brossard Børhaug F. (2022). Using digital, universal, and intercultural didactics to improve higher education—A project protocol for a Norwegian interactive and collaborative improvement study concerning master's level courses in "Theory of science, research methods, and research ethics". Frontiers in Education, 7, 851783. https://doi.org/10.3389/feduc.2022.851783

20. Susanti A., Widyawati L. R. L., Arigiyati T. A. & Ernawati T. (2023). Digitalization of the laboratory management module for strengthening the laboratory skills of prospective science teachers. Jurnal Pijar Mipa, 18(1), 6–12. https://doi.org/10.29303/jpm.v18i1.4267

21. Gomes C. A. & Sousa C. Â. de M. (2023). Challenges and risks of remote education for children and adolescents. Ensaio: Avaliação e Políticas Públicas em Educação, 31(118), e0233752. https://doi.org/10.1590/S0104-40362022003003752

22. Mynaříková L. & Novotný L. (2020). Knowledge society failure? Barriers in the use of ICTs and further teacher education in the Czech Republic. Sustainability, 12(17), 6933. https://doi.org/10.3390/su12176933

23. Kropachev P., Imanov M., Borisevich Y. & Dhomane I. (2020). Information technologies and the future of education in the Republic of Kazakhstan. Scientific Journal of Astana IT University, 1, 30–38. https://doi.org/10.37943/AITU.2020.1.63639

24. Strutynska O. V., Torbin G. M., Umryk M. A. & Vernydub R. M. (2021). Digitalization of the educational process for the training of pre-service teachers. CTE Workshop Proceedings, 8, 179–199. https://doi.org/10.55056/cte.231

25. Bykova T. B., Ivashchenko M. V., Kassim D. A. & Kovalchuk V. I. (2021). Blended learning in the context of digitalization. CTE Workshop Proceedings, 8, 247–260. https://doi.org/10.55056/cte.236

26. Alenezi M., Wardat S. & Akour M. (2023). The need of integrating digital education in higher education: Challenges and opportunities. Sustainability, 15(6), 4782. https://doi.org/10.3390/su15064782

27. Mitescu-Manea M., Safta-Zecheria L., Neumann E., Bodrug-Lungu V. & Milenkova V. (2021). Teachers' digital competences in the first educational policy responses to the COVID-19 crisis in four countries. Journal of Educational Sciences, 43(1), 99–112. https://doi.org/10.35923/JES.2021.1.07

28. Hug T. (2021). Five theses on (dis)comfort in the educational cultures of digitality. International Journal of Research in E-Learning, 7(2), 1–22. https://doi.org/10.31261/IJREL.2021.7.2.02

29. Lindberg Y. & Öberg L.-M. (2023). The future scribe: Learning to write the world. Frontiers in Education, 8, 993268. https://doi.org/10.3389/feduc.2023.993268

30. Filipova M. & Usheva M. (2021). Social and labor relations of the digital age: To the question of future education development. Futurity Education, 1(2), 14–22. https://doi.org/10.57125/FED/2022.10.11.15

31. Aubakirova S., Kozhamzharova M., Zhumabekova G., Artykbayeva G., Iskakova Z. & Zhayabayeva R. (2023). Experience in forming entrepreneurial education in Kazakhstan universities in the conditions of information and digital development. Frontiers in Education, 8, 1199392. https://doi.org/10.3389/feduc.2023.1199392

32. Delcker J. & Ifenthaler D. (2022). Digital distance learning and the transformation of vocational schools from a qualitative perspective. Frontiers in Education, 7, 908046. https://doi.org/10.3389/feduc.2022.908046

33. H. N., Febriati F., Ervianti E. & Sujarwo S. (2021). The impact of computer-based test and students' ability in computer self-efficacy on mathematics learning outcomes. Journal of Education Technology, 5(4), 603–610. https://doi.org/10.23887/jet.v5i4.34942

34. Haugsbakk G. (2020). Special issue: 30 years of ICT and learning in education – major changes and challenges. Seminar.net, 16(2). https://doi.org/10.7577/seminar.4043

35. Pina Stranger A., Varas G. & Mobuchon G. (2023). Managing inter-university digital collaboration from a bottom-up approach: Lessons from organizational, pedagogical, and technological dimensions. Sustainability, 15(18), 13470. https://doi.org/10.3390/su151813470

36. Sun C., Liu J., Razmerita L., Xu Y. & Qi J. (2022). Higher education to support sustainable development: The influence of information literacy and online learning process on Chinese postgraduates' innovation performance. Sustainability, 14(13), 7789. https://doi.org/10.3390/su14137789

37. Bjelobaba G., Paunovic M., Savic A., Stefanovic H., Doganjic J. & Miladinovic Bogavac Z. (2022). Blockchain technologies and digitalization in function of student work evaluation. Sustainability, 14(9), 5333. https://doi.org/10.3390/su14095333

38. Benavides L. M. C., Tamayo Arias J. A., Arango Serna M. D., Branch Bedoya J. W. & Burgos D. (2020). Digital transformation in higher education institutions: A systematic literature review. Sensors, 20(11), 3291. https://doi.org/10.3390/s20113291

39. Ebinger F., Buttke L. & Kreimeier J. (2022). Augmented and virtual reality technologies in education for sustainable development: An expert-based technology assessment. TATuP, 31(1), 28–34. https://www.tatup.de/index.php/tatup/article/view/6955

40. Cramarenco R. E., Burcă-Voicu M. I. & Dabija D. C. (2023). Student perceptions of online education and digital technologies during the COVID-19 pandemic: A systematic review. Electronics, 12(2), 319. https://doi.org/10.3390/electronics12020319

41. Tănase F. D., Demyen S., Manciu V. C. & Tănase A. C. (2022). Online education in the COVID-19 pandemic—Premise for economic competitiveness growth? Sustainability, 14(6), 3503. https://doi.org/10.3390/su14063503

42. Alsayed Kassem J., Sayeed S., Marco-Gisbert H., Pervez Z. & Dahal K. (2019). DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. Applied Sciences, 9(15), 2953. https://doi.org/10.3390/app9152953

43. Javidi G. & Sheybani E. (2023). Transforming cybersecurity education through consulting. Journal of Systemics, Cybernetics and Informatics, 17(1), 157–168.

44. Jenita J., Ratna Nurdiana, I. Made Gede Ariestova Kurniawan, Darnilawati & Diana Triwardhani. (2022). Optimizing human resources management for higher education in the era of implementing an independent curriculum in Indonesia. Jurnal Iqra' : Kajian Ilmu Pendidikan, 7(2), 246–259. https://doi.org/10.25217/ji.v7i2.1803

45. Rodríguez Pérez N. & Heinsch B. (2021). The impact of digitalization on communicative competence in foreign languages in higher education. Latin American Journal of Educational Technology - RELATEC, 20(1), 71–85. https://doi.org/10.17398/1695-288X.20.1.71

46. Lund A. & Aagaard T. (2020). Digitalization of teacher education: Are we prepared for epistemic change? Nordic Journal of Comparative and International Education (NJCIE), 4(3-4), 56–71. https://doi.org/10.7577/njcie.3751

47. Almås A. G., Bueie A. A. & Aagaard T. (2021). From digital competence to professional digital competence: Student teachers' experiences of and reflections on how teacher education prepares them for working life. Nordic Journal of Comparative and International Education (NJCIE), 5(4), 70–85. https://doi.org/10.7577/njcie.4233

48. Muchacki M. (2022). Peculiarities of personality development of the future in the context of information and communication technologies and education system reform (Polish experience). Futurity Education, 2(1), 46–56. https://doi.org/10.57125/FED.2022.25.03.6

49. Sá M. J., Santos A. I., Serpa S. & Miguel Ferreira C. (2021). Digitainability—Digital competences post-COVID-19 for a sustainable society. Sustainability, 13(17), 9564. https://doi.org/10.3390/su13179564

50. Florea A. (2019). Digital design skills for factories of the future. In Proceedings of the 9th International Conference on Manufacturing Science and Education—MSE 2019 "Trends in New Industrial Revolution" (Sibiu, Romania, 5–7 June 2019; Volume 290, p. 14002). https://doi.org/10.1051/matecconf/201929014002

51. Afshar Jahanshahi A. & Polas M. R. H. (2023). Moving toward digital transformation by force: Students' preferences, happiness, and mental health. Electronics, 12(10), 2187. https://doi.org/10.3390/electronics12102187

52. Martyniuk O. O., Martyniuk O. S. & Muzyka I. O. (2021). Formation of informational and digital competence of secondary school students in laboratory work in physics. CTE Workshop Proceedings, 8, 366–383. https://doi.org/10.55056/cte.294

53. Devadze A., Gechbaia B. & Gvarishvili N. (2022). Education of the future: An analysis of definitions (literary review). Futurity Education, 2(1), 4–12. https://doi.org/10.57125/FED/2022.10.11.19

54. Trabelsi Z., Alnajjar F., Parambil M. M. A., Gochoo M. & Ali L. (2023). Real-time attention monitoring system for classroom: A deep learning approach for student's behavior recognition. Big Data and Cognitive Computing, 7(1), 48. https://doi.org/10.3390/bdcc7010048

55. Zinchenko V., Dorosheva A. & Mosiy I. (2023). Innovative and cultural transformations of educational environment of the future: Digitalization, barriers for traditional learning. Futurity Education, 3(1), 41–57. https://doi.org/10.57125/FED.2023.25.03.04

56. Harteis C., Goller M. & Caruso C. (2020). Conceptual change in the face of digitalization: Challenges for workplaces and workplace learning. Frontiers in Education, 5, 1. https://doi.org/10.3389/feduc.2020.00001

57. Ahn J. (2020). Unequal loneliness in the digitalized classroom: Two loneliness effects of school computers and lessons for sustainable education in the e-learning era. Sustainability, 12(19), 7889. https://doi.org/10.3390/su12197889

58. Nikolopoulou K. (2022). Students' mobile phone practices for academic purposes: Strengthening post-pandemic university digitalization. Sustainability, 14(22), 14958. https://doi.org/10.3390/su142214958

59. Vlachopoulos D., Thorkelsdóttir R. B., Schina D. & Jónsdóttir J. G. (2023). Teachers' experience and perceptions of sustainable digitalization in school education: An existential phenomenological study of teachers in Romania, Greece, Cyprus, Iceland, and the Netherlands. Sustainability, 15(18), 13353. https://doi.org/10.3390/su151813353

60. Rosak-Szyrocka J., Żywiołek J., Zaborski A., Chowdhury S. & Hu Y.-C. (2022). Digitalization of higher education around the globe during Covid-19. IEEE Access, 10, 59782–59791. https://doi.org/10.1109/ACCESS.2022.3178711

61. Łukasz T. (2021). Research trends in media pedagogy: Between the paradigm of risk and the paradigm of opportunity. International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 9(3), 399–406. https://doi.org/10.23947/2334-8496-2021-9-3-399-406

62. Erdmann A., Estrada Presedo A. & de Miguel Valdés M. (2021). Digital transformation of universities: The influence of COVID-19 and students' perception. Multidisciplinary Journal for Education, Social and Technological Sciences, 8(2), 19–41. https://doi.org/10.4995/muse.2021.16007

63. Saeed S. T. (2021). Higher education and quality assurance in Egypt: Pre and post COVID-19. International Journal of Social Sciences & Educational Studies, 8(2), 96–107.

64. Appolloni A., Colasanti N., Fantauzzi C., Fiorani G. & Frondizi R. (2021). Distance learning as a resilience strategy during COVID-19: An analysis of the Italian context. Sustainability, 13(3), 1388. https://doi.org/10.3390/su13031388

65. Berawi M. A. (2021). Innovative technology for post-pandemic economic recovery. International Journal of Technology, 12(1), 1–4.

66. Khoruzha L., Lokshyna O., Mazur N. & Proshkin V. (2022). Doctoral education in Ukraine: The application of digital tools and services by doctoral students under COVID-19 pandemic. Multidisciplinary Journal for Education, Social and Technological Sciences, 9(1), 87–112. https://doi.org/10.4995/muse.2022.16768

67. Makhachashvili R. & Semenist I. (2021). Interdisciplinary trends of digital education in the COVID-19 paradigm: Global event horizon. Journal of Systemics, Cybernetics and Informatics, 19(9), 57–64. https://doi.org/10.54808/JSCI.19.09.57

68. Villarica M. V. (2023). The effectiveness of flipped classrooms in distance education during the COVID-19 pandemic. International Journal of Computing Sciences Research, 7, 2296–2314. https://doi.org/10.25147/ijcsr.2017.001.1.160

69. Urbanek A., Losa A., Wieczorek-Kosmala M., Hlaváček K. & Lokaj A. (2023). Did the quality of digital communication skills in education improve after the pandemic? Evidence from HEIs. Sustainability, 15(15), 11878. https://doi.org/10.3390/su151511878

70. Yang C., Kaiser F., Tang H., Chen P. & Diao J. (2023). Sustaining the quality development of German vocational education and training in the age of digitalization: Challenges and strategies. Sustainability, 15(4), 3845. https://doi.org/10.3390/su15043845

71. Chen R., Wu X. & Liu X. (2023). RSETP: A reliable security education and training platform based on the alliance blockchain. Electronics, 12(6), 1427. https://doi.org/10.3390/electronics12061427

72. Beier F. & Czaja T. (2023). Digitalisierung, Inklusion und Gamification. Verschränkung von Querschnittsthemen in der Lehrkräftebildung im Lehr-Lern-Raum Inklusion. QfI - Qualifizierung für Inklusion, 5(2). https://doi.org/10.21248/QfI.124

73. Ari R., Altinay Z., Altinay F., Dagli G. & Ari E. (2022). Sustainable management and policies: The roles of stakeholders in the practice of inclusive education in digital transformation. Electronics, 11(4), 585. https://doi.org/10.3390/electronics11040585

74. Ljubojević S. D., Andrejić M. D. & Dragović N. K. (2013). Contribution to the improvement of management in defense logistics. Vojnotehnički glasnik, 61(4), 80–120. https://doi.org/10.5937/vojtehg61-2098

75. Illiger K., Hupka M., von Jan U., Wichelhaus D. & Albrecht U. (2014). Mobile technologies: Expectancy, usage, and acceptance of clinical staff and patients at a university medical center. JMIR mHealth and uHealth, 2(4), e42. https://doi.org/10.2196/mhealth.3799

76. Haque Md. S., Sharif S. (2021). The need for an effective environmental engineering education to meet the growing environmental pollution in Bangladesh. Cleaner Engineering and Technology, 4, 100114. https://doi.org/10.1016/j.clet.2021.100114

77. Ding D., Shen Y., Jiang J., Yuan Q., Xiu T., Ni K. & Liu C. (2023). Data collection and information security analysis in sports teaching system based on intelligent sensor. Measurement: Sensors, 28, 100854. https://doi.org/10.1016/j.measen.2023.100854

78. Engel O., Zimmer L. M., Lörz M., et al. (2023). Digital studying in times of COVID-19: Teacher- and student-related aspects of learning success in German higher education. International Journal of Educational Technology in Higher Education, 20, 12. https://doi.org/10.1186/s41239-023-00382-w

79. Kumar P. & Rai S. C. (2021). An overview of existing contours for promoting different strategies for livelihood security in Sikkim Himalaya. Current Research in Environmental Sustainability, 3, 100034. https://doi.org/10.1016/j.crsust.2021.100034

80. Shabani L., Behluli A., Qerimi F., Pula F. & Dalloshi P. (2022). The effect of digitalization on the quality of service and customer loyalty. Emerging Science Journal, 6(6), 1274–1289. https://doi.org/10.28991/ESJ-2022-06-06-04

81. Sifat M. M. H., Choudhury S. M., Das S. K., Ahamed M. H., Muyeen S. M., Hasan M. M., Ali M. F., Tasneem Z., Islam M. M., Islam M. R., Badal M. F. R., Abhi S. H., Sarker S. K. & Das P. (2023). Towards electric digital twin grid: Technology and framework review. Energy and AI, 11, 100213. https://doi.org/10.1016/j.egyai.2022.100213

82. Teplická K., Kádárová J. & Hurná S. (2022). The new model of the engineering education using digitalization and innovative methods. Management Systems in Production Engineering, 30(3), 207–213. https://doi.org/10.2478/mspe-2022-0026

83. Kucharcikova A. (2014). The importance of identification and analysis of educational needs for investment in human capital. Communications - Scientific Letters of the University of Zilina, 16(3), 86–92. https://doi.org/10.26552/com.C.2014.3.86-92

84. Li F., Zou X., Liu P. & Chen J. Y. (2011). New threats to health data privacy. BMC Bioinformatics, 12(12), S7. https://doi.org/10.1186/1471-2105-12-S12-S7

85. Veličković S. & Stošić L. (2016). Preparedness of educators to implement modern information technologies in their work with preschool children. International Journal of Cognitive Research in Science, Engineering and Education, 4(1), 23–30. https://doi.org/10.5937/IJCRSEE1601023V

86. Ryu J., Son S., Lee J., Park Y. & Park Y. (2022). Design of secure mutual authentication scheme for metaverse environments using blockchain. IEEE Access, 10, 98944–98958. https://doi.org/10.1109/ACCESS.2022.3206457

87. Nalyvaiko O. & Vakulenko A. (2021). CANVAS LMS: Opportunities and features. OD, 35(4), 154–172.

88. Stroe A. C. (2022). Digitalization of Romanian education system: Is Romania ready to embrace Education 4.0? Informatica Economica, 26(3), 16–25. https://ideas.repec.org/a/aes/infoec/v26y2022i3p16-25.html

89. Kochkareva I. V. (2020). Holding online student conferences: Typical mistakes. Development of Education, 74–78. https://doi.org/10.31483/r-75505

90. Yu H. & Guo Y. (2023). Generative artificial intelligence empowers educational reform: Current status, issues, and prospects. Frontiers in Education, 8, 1183162. https://doi.org/10.3389/feduc.2023.1183162

91. Bernsteiner A., Schubatzky T. & Haagen-Schützenhöfer C. (2023). Misinformation as a societal problem in times of crisis: A mixed-methods study with future

teachers to promote a critical attitude towards information. Sustainability, 15(10), 8161. https://doi.org/10.3390/su15108161

92. Ortiz-Garces I., Gutierrez R., Guerra D., Sanchez-Viteri S. & Villegas-Ch. W. (2023). Development of a platform for learning cybersecurity using capturing the flag competitions. Electronics, 12(7), 1753. https://doi.org/10.3390/electronics12071753

93. Idris M., Syarif I. & Winarno I. (2022). Web application security education platform based on OWASP API Security Project. EMITTER International Journal of Engineering Technology, 10(2), 246–261. https://doi.org/10.24003/emitter.v10i2.705

94. Prokopenko O. (2021). Technological challenges of our time in the digitalization of the education of the future. Futurity Education, 1(2), 4–13. https://doi.org/10.57125/FED/2022.10.11.14

95. Morze N. V. & Kucherovska V. O. (2021). Ways to design a digital educational environment for K-12 education. CTE Workshop Proceedings, 8, 200–211. https://doi.org/10.55056/cte.232

96. Veličković S. & Stošić L. (2016). Preparedness of educators to implement modern information technologies in their work with preschool children. International Journal of Cognitive Research in Science, Engineering and Education, 4(1), 23–30. https://doi.org/10.5937/IJCRSEE1601023V

97. Lovecek T., Ristvej J., Kampova K., Vaculík J., Gamboa R. & Zagorecki A. (2013). Portal of security and safety engineering as a tool to increase the sustainable development of higher education in security in the European Union and beyond. Communications - Scientific Letters of the University of Zilina, 15(2), 56–62. https://doi.org/10.26552/com.C.2013.2.56-62

98. León-Acurio J., Vite A., Sisa C., Bastidas Zambrano L. & Santamaría Philco A. (2018). Herramientas de código abierto: Incidencia en la seguridad inalámbrica de la Universidad Técnica de Babahoyo. Journal of Science and Research, 3(CITT2017), 56–60. https://doi.org/10.26910/issn.2528-8083vol3issCITT2017.2018pp56-60

99. Li F., Yu G., Mu C., Xue Q., Tseng S.-P. & Wang T. (2022). A personal growth system supporting the sustainable development of students based on intelligent graph element technology. Sustainability, 14(12), 7196. https://doi.org/10.3390/su14127196

100. Saputra P. S., Tjahyanti L. P. A. S., Pratama P. A. & Sutama G. R. (2023). Library apps to improve the digitization of Sekolah Penggerak Program. Matrix: Jurnal Manajemen Teknologi Dan Informatika, 13(2), 68–79. https://doi.org/10.31940/matrix.v13i2.68-79

101. Devi L. S., Rejekiningsih T. & Rusnaini R. (2022). Learning in digital era: Analysis of civic education learning materials for students in junior high school. Jurnal Civics: Media Kajian Kewarganegaraan, 19(1), 165–174. https://doi.org/10.21831/JC.V19I1.47908

102. Vladova G., Ullrich A., Sloane M., Renz A. & Tsui E. (2023). Editorial: New teaching and learning worlds - Potentials and limitations of digitalization for innovative and sustainable research and practice in education and training. Frontiers in Education, 8, 1175498. https://doi.org/10.3389/feduc.2023.1175498

103. Spanhel D. (2011). An approach for integrating media education into everyday school life and instruction at secondary school level. Enseñanza & Teaching: Interuniversity Journal of Didactic, 29(1), 181–190. Retrieved from https://revistas.usal.es/tres/index.php/0212-5374/article/view/8322

104. Shenkoya T. & Kim E. (2023). Sustainability in higher education: Digital transformation of the Fourth Industrial Revolution and its impact on open knowledge. Sustainability, 15(3), 2473. https://doi.org/10.3390/su15032473

105. Lesinskis K., Mavlutova I., Spilbergs A. & Hermanis J. (2023). Digital transformation in entrepreneurship education: The use of a digital tool KABADA and entrepreneurial intention of Generation Z. Sustainability, 15(13), 10135. https://doi.org/10.3390/su151310135

106. Yang D., Zhou J., Shi D., Pan Q., Wang D., Chen X. & Liu J. (2022). Research status, hotspots, and evolutionary trends of global digital education via knowledge graph analysis. Sustainability, 14(22), 15157. https://doi.org/10.3390/su142215157

107. Sissom J., Shih S. & Goro T. A. (2023). A low-cost remote lab for internet services distance education. Journal of Systemics, Cybernetics and Informatics, 4(4), 1–4.

108. Moskvina J. (trans.) (2021). Digital education: Lithuania among other European Union states. Acta Paedagogica Vilnensia, 47, 52–68. https://doi.org/10.15388/ActPaed.2021.47.4

109. Kostenko L., Ruda O., Sofilkanych M. & Bokshan A. (2023). Distance learning as an integrative response to contemporary challenges. Futurity Education, 3(1), 151–164. https://doi.org/10.57125/FED/2022.10.11.12

110. Wei S. (2023). Information technologies in the education of contemporary China: Reality and opportunities. Filosofiya Osvity. Philosophy of Education, 29(1), 92–110. https://doi.org/10.31874/2309-1606-2023-29-1-5

111. Ostanina A., Bazyl O., Tsviakh O. & Dovzhuk N. (2023). Formation of digital competence in higher education students as a basis for the transformation of education of the future. Futurity Education, 3(1), 126–135. https://doi.org/10.57125/FED.2023.25.03.10

112. Buck M. F. (2017). Gamification of learning and teaching in schools – A critical stance. Seminar.net, 13(1). https://doi.org/10.7577/seminar.2325

113. Denisov I., Petrenko Y., Koretskaya I. & Benčič S. (2021). The Gameover in universities education management during the pandemic COVID-19: Challenges to sustainable development in a digitalized environment. Sustainability, 13(13), 7398. https://doi.org/10.3390/su13137398

114. Sarah N. (2022). Social exclusive of education inequality in the Covid-19 pandemia by education digitalization activities. QALAMUNA: Jurnal Pendidikan, Sosial, Dan Agama, 14(2), 263–274. https://doi.org/10.37680/qalamuna.v14i2.1959

115. Mukhametshin L. M., Karamova K. K., Salekhova L. L. & Usmanov S. F. (2021). Barriers of teacher formation in the implementation of distance learning technologies

in modern education. Revista on line de Política e Gestão Educacional, 25(esp.1), 398–407. https://doi.org/10.22633/rpge.v25iesp.1.14976

116. Onesimu J. A., J. K., Eunice J., Pomplun M. & Dang H. (2022). Privacy preserving attribute-focused anonymization scheme for healthcare data publishing. IEEE Access, 10, 86979–86997. https://doi.org/10.1109/ACCESS.2022.3199433

117. Başol O., Sevgi H. & Yalçın E. C. (2023). The effect of digitalization on youth unemployment for EU countries: Treat or threat? Sustainability, 15(14), 11080. https://doi.org/10.3390/su151411080

118. Bond M., Marín V. I., Dolch C., et al. (2018). Digital transformation in German higher education: Student and teacher perceptions and usage of digital media. International Journal of Educational Technology in Higher Education, 15, 48. https://doi.org/10.1186/s41239-018-0130-1

119. Borrás-Gené O., Serrano-Luján L. & Díez R. M. (2022). Professional and academic digital identity workshop for higher education students. Information, 13(10), 490. https://doi.org/10.3390/info13100490

120. Area Moreira M. (2018). Towards the digital university: Where are we and where are we going? RIED. Revista Iberoamericana de Educación a Distancia, 21(2), 25–30. https://doi.org/10.5944/ried.21.2.21801

121. Bader S., Oleksiienko A. & Mereniuk K. (2022). Digitalization of future education: Analysis of risks on the way and selection of mechanisms to overcome barriers (Ukrainian experience). Futurity Education, 2(2), 21–33. https://doi.org/10.57125/FED/2022.10.11.26

122. Valdés K. N., Alpera S. Q. & Cerdá Suárez L. M. (2021). An institutional perspective for evaluating digital transformation in higher education: Insights from the Chilean case. Sustainability, 13(17), 9850. https://doi.org/10.3390/su13179850

123. Eldosouky A., Das T., Kotra A. & Sengupta S. (2022). Finding the sweet spot for data anonymization: A mechanism design perspective. IEEE Access, 10, 103718–103732. https://doi.org/10.1109/ACCESS.2022.3210521

124. Wu Z.-Y. (2019). A secure and efficient digital-data-sharing system for cloud environments. Sensors, 19(12), 2817. https://doi.org/10.3390/s19122817

125. Zhang Z. (2022). Application of digital intelligent communication technology in contemporary comparative education methodology. Alexandria Engineering Journal, 61(6), 4647–4657. https://doi.org/10.1016/j.aej.2021.10.019

126. Забуга А. Г. (2023). Автоматизація оцінювання успішності студентів за допомогою методів математичної статистики. Вчені записки, 32023146.

127. Vo T. H., Fuhrmann W., Fischer-Hellmann K.-P. & Furnell S. (2019). Identity-as-a-Service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. Інтернет майбутнього, 11(5), 116. https://doi.org/10.3390/fi11050116

128. Pejić Bach M., Pivar J. & Dumičić K. (2017). Data anonymization patent landscape. Croatian Operational Research Review, 8(1), 265–281. https://doi.org/10.17535/crorr.2017.0017

129. Lebedeva I., Norik L. & Lebedev S. (2022). Digital resources as a way to increase the motivation of economic specialties students in studies of mathematics. Educational Challenges, 27(2), 105–121. https://doi.org/10.34142/2709-7986.2022.27.2.08

130. Zhang M. & Dong X. (2017). Research on the network security strategy for digital distance education platform. MATEC Web of Conferences, 139, 00184. https://doi.org/10.1051/matecconf/201713900184

131. Sikman Lj., Latinovic T. & Sarajlic N. (2022). Modelling of fuzzy expert system for an assessment of security information management system UIS (University Information System). Tehnički vjesnik, 29(1), 60–65. https://doi.org/10.17559/TV-20200721154801

132. Mygal V., Mygal G. & Mygal S. (2021). Transdisciplinary convergent approach - human factor. Radioelectronic and Computer Systems, 0(4), 7–21. https://doi.org/10.32620/reks.2021.4.01

133. Gunawan D. & Mambo M. (2019). Data anonymization for hiding personal tendency in set-valued database publication. Future Internet, 11(6), 138. https://doi.org/10.3390/fi11060138

134. Su B., Huang J., Miao K., Wang Z., Zhang X. & Chen Y. (2023). K-anonymity privacy protection algorithm for multi-dimensional data against skewness and similarity attacks. Sensors, 23(3), 1554. https://doi.org/10.3390/s23031554

135. Majeed A. & Hwang S. O. (2023). A generic approach towards enhancing utility and privacy in person-specific data publishing based on attribute usefulness and uncertainty. Electronics, 12(9), 1978. https://doi.org/10.3390/electronics12091978

136. Ma J., Qiao Y., Hu G., Huang Y., Sangaiah A. K., Zhang C., Wang Y. & Zhang R. (2018). De-anonymizing social networks with random forest classifier. IEEE Access, 6, 10139–10150. https://doi.org/10.1109/ACCESS.2017.2756904

137. Forsling K. (2022). Cooperation for developing digital competence in preschool – Challenges for teacher education, students, and practicum preschools. Cogent Education, 9(1), 2141512. https://doi.org/10.1080/2331186X.2022.2141512

138. Bačlija Sušić B. & Mičija Palić M. (2022). Digital competencies in the context of preschool music education. International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 10(2), 77–87. https://doi.org/10.23947/2334-8496-2022-10-2-77-87

139. Muchacki M. (2022). Peculiarities of personality development of the future in the context of information and communication technologies and education system reform (Polish experience). Futurity Education, 2(1), 46–56. https://doi.org/10.57125/FED.2022.25.03.6

140. Ask T. F., Kullman K., Sütterlin S., Knox B. J., Engel D. & Lugo R. G. (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Frontiers in Big Data, 6, 1042783. https://doi.org/10.3389/fdata.2023.1042783

141. Al-Zahrani A. & Al-Hebbi M. (2022). Big data major security issues: Challenges and defense strategies. Tehnički glasnik, 16(2), 197–204. https://doi.org/10.31803/tg-20220124135330

142. Rahardja U., Ngadi M. A., Budiarto R., Aini Q., Hardini M. & Oganda F. P. (2021). Education exchange storage protocol: Transformation into decentralized learning platform. Frontiers in Education, 6, 782969. https://doi.org/10.3389/feduc.2021.782969

143. Liu Y., Tse W. K., Kwok P. Y. & Chiu Y. H. (2022). Impact of social media behavior on privacy information security based on analytic hierarchy process. Information, 13(6), 280. https://doi.org/10.3390/info13060280

144. Sienkiewicz P. & Gawliczek P. (2021). Theory and security systems engineering. Sučasnì Informacìjnì Tehnologìï u Sferì Bezpeki ta Oboroni, 0(1), 112–117.

145. Alqudhaibi A., Krishna A., Jagtap S., Afy-Shararah M. & Salonitis K. (2023). Safeguarding food industry: Understanding cyberthreats and ensuring cybersecurity. Engineering Proceedings, 40(1), 11. https://doi.org/10.3390/engproc2023040011

146. Ya'u B. I., Salleh N., Nordin A., Idris N. B., Abas H. & Alwan A. A. (2019). A systematic mapping study on cloud-based mobile application testing. Journal of Information and Communication Technology, 18(4), 485–527. https://doi.org/10.32890/jict2019.18.4.5

147. Nouskalis G. (2011). Biometrics, e-identity, and the balance between security and privacy: Case study of the Passenger Name Record (PNR) system. TheScientificWorldJOURNAL, 11, 474–477. https://doi.org/10.1100/tsw.2011.48

148. De-Waal E., & Grösser M. (2014). On safety and security in education: Pedagogical needs and fundamental rights of learners. Educar, 50(2), 339-361. https://doi.org/10.5565/rev/educar.44

149. Gryszczyńska A. (2021). The impact of the COVID-19 pandemic on cybercrime. Bulletin of the Polish Academy of Sciences. Technical Sciences, 69(4), e137933.

150. Lampoltshammer T. J., Albrecht V., & Raith C. (2021). Teaching Digital Sustainability in Higher Education from a Transdisciplinary Perspective. Sustainability, 13(21), 12039. https://doi.org/10.3390/su132112039

151. Łukasz T. (2021). Research Trends in Media Pedagogy: Between the Paradigm of Risk and the Paradigm of Opportunity. International Journal of Cognitive Research in Science, Engineering and Education 1 (IJCRSEE), 9(3), 399–406. 2 https://doi.org/10.23947/2334-8496-2021-9-3-399-406

152. Giesenbauer B., Müller-Christ G. (2020). University 4.0: Promoting the Transformation of Higher Education Institutions toward Sustainable Development. Sustainability, 12(8), 3371. 1 https://doi.org/10.3390/su12083371

153. Roy R., Al-Absy M.S.M. (2022). Impact of Critical Factors on the Effectiveness of Online Learning. Sustainability, 14(21), 14073. https://doi.org/10.3390/su142114073

154. Amalina F., et al. (2020). Blending big data analytics: Review on challenges and a recent study. IEEE Access, 8, 3629–3645. https://doi.org/10.1109/ACCESS.2019.2923270

155. Albalawi N., Alamrani N., Aloufi R., Albalawi M., Aljaedi A., & Alharbi A.R. (2023). The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities. Electronics, 12(12), 2664. https://doi.org/10.3390/electronics12122664

156. Bukliv R., Kuchak A., & Vasylyuk-Zaitseva S. (2023). Professional training of future academic staff and digitalization of education: analysis of mutual influences. Futurity Education, 3(1), 69–78. 1 https://doi.org/10.57125/FED.2023.25.03.06

157. Masters J. (2018). Trends in the Digitalization of K-12 Schools: The Australian Perspective. Seminar.net, 14(2), 120–131. https://doi.org/10.7577/seminar.2975

158. Huang, Y. (2021). Research on the design and application of online English education platforms based on the web. International Journal of Antenna and Propagation, 2021, 1–10. https://doi.org/10.1155/2021/7648856

159. Kalinin D., Severyn V., & Bezmenov M. (2024). Privacy models and anonymization techniques for tabular healthcare data. Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, (2(12)) 81–85. https://doi.org/10.20998/2079-0023.2024.02.12

160. Sarva E., Lāma G., Oļesika A., Daniela L., & Rubene Z. (2023). Development of Education Field Student Digital Competences—Student and Stakeholders' Perspective. Sustainability, 15(13), 9895. https://doi.org/10.3390/su15139895

161. Райчук І. В. (2024). Експертна оцінка ідентифікації ризиків втрати персональних даних при інформаційній взаємодії у діджиталізованому освітньому середовищі. Наука і техніка сьогодні, Серія «Техніка», 13(41), 1227–1238.

162. Корченко О. Г., Дрейс Ю. О., & Лозова І. Л. (2016). Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. Захист інформації, 18(1), 39–47. http://er.nau.edu.ua/handle/NAU/29200

163. Zosym M. (2023). Метод Дельфі (Delphi method). Available at: https://www.maxzosim.com/delphi-method (Accessed: February 2024).

164. Куц Ю. В., Лисенко Ю. Ю. (2022). Статистичні методи визначення залежностей між випадковими величинами. Київ: КПІ ім. Ігоря Сікорського. С. 56–60.

165. Hayes A. (2024). Autoregressive integrated moving average (ARIMA) prediction model. Available at: https://www.investopedia.com/terms/a/autoregressive-integrated-moving-average-arima.asp (Accessed: December 15, 2024).

166. Hyndman, R.J., & Athanasopoulos, G. (2021). Forecasting: principles and practice, 3rd edition, OTexts: Melbourne, Australia. OTexts.com/fpp3.

167. Kuzhda T. (2014). Exponential smoothing for financial time series data forecasting [Електронний ресурс]. Соціально-економічні проблеми і держава, 1(10), 177–184. Available at: http://sepd.tntu.edu.ua/images/stories/pdf/2014/14ktioez.pdf

168. Chen T. & Guestrin C. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16) (pp. 785–794). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/2939672.2939785

169. Dhumne S. (2023). Elastic net regression detailed guide! Available at: https://medium.com/@shruti.dhumne/elastic-net-regression-detailed-guide-99dce30b8e6e (Accessed: December 15, 2024).

170. Hemmati-Sarapardeh A., Larestani A., Nait Amar M. & Hajirezaie S. (2020). Chapter 1 - Introduction. In Applications of Artificial Intelligence Techniques in the Petroleum Industry (pp. 1–22). Gulf Professional Publishing. https://doi.org/10.1016/B978-0-12-818680-0.00001-1

171. Shewan D. (2024). How to do a SWOT analysis (with examples & free template!). Available at: https://www.wordstream.com/blog/ws/2017/12/20/swot-analysis (Accessed: September 2024).

172. Boogaard K. (2023). How to write SMART goals. Productivity. Available at: https://www.atlassian.com/blog/productivity/how-to-write-smart-goals (Accessed: September 2024).

173. Raichuk I. (2020). Models of digitalization of business processes of project-oriented organizations based on artificial neural networks. In Proceedings of the VII International Conference "Information Technology and Interactions" (Satellite) (pp. 217–220). Kyiv.

ДОДАТКИ

Додаток А

Акт про впровадження

«ЗАТВЕРДЖУЮ»
Директор ТОВ «Едютон Україна»
_____ К. В. Процун
«11» листопада 2024р.

АКТ

про впровадження у інформаційні технології та програмні продукти ТОВ «Едютон Україна» результатів дисертаційної роботи Райчука Ісуса Васильовича «Моделі та методи управління потоками персональних даних освітнього середовища в умовах діджиталізації»

Використовуються такі наукові результати, отримані дисертантом особисто:

- алгоритм анонімізації персональних даних стейкхолдерів діджиталізованої освіти;
- алгоритм деанонімізації персональних даних стейкхолдерів діджиталізованої освіти;
- метод анонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти;
- метод деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти;
- об'єднаний метод впровадженя анонімізації та деанонімізації персональних даних у взаємодії елементів інформаційного простору діджиталізованої освіти.

Впровадження результатів дисертаційної роботи Райчука І.В. у інформаційні технології та програмні продукти ТОВ «Едютон Україна» дозволило підвищити рівень захисту персональних даних стейкхолдерів освітнього середовища які використовують інформаційні технології та програмні продукти компанії, а також підвищило довіру користувачів до сервісів підприємства загалом.

Директор ТОВ «Едютон Україна» Процун К.В.

Додаток Б

Статистичні дані використання сервісу навчального закладу

A	B	C	D	E
№	Місяць	Кількість ядер	Відсоток використання процесора	Кількість оперативної пам'яті Gb
1	січень	8	36	32
2	лютий	8	34	32
3	березень	8	33	32
4	квітень	8	33	32
5	травень	8	40	32
6	червень	8	21	32
7	липень	8	4	32
8	серпень	8	5	32
9	вересень	8	43	32
10	жовтень	8	32	32
11	листопад	8	34	32
12	грудень	8	41	32
13	січень	8	40	32
14	лютий	8	38	32
15	березень	8	23	32
16	квітень	8	21	32
17	травень	8	20	32
18	червень	8	25	32
19	липень	8	15	32
20	серпень	8	19	32
21	вересень	8	57	32
22	жовтень	8	43	32
23	листопад	8	41	32
24	грудень	8	59	32
25	січень	8	73	32
26	лютий	8	65	32
27	березень	8	37	32
28	квітень	8	35	32
29	травень	8	41	32
30	червень	8	32	32
31	липень	8	21	32
32	серпень	8	28	32
33	вересень	8	76	32
34	жовтень	8	91	32
35	листопад	8	74	32
36	грудень	8	67	32

Продовження додатка Б

F	G	H
Відсоток використання пам'яті	Мережеве навантаження GbS	Кількість активних користувачів MAU
25	0.3	172
26	0.3	151
29	0.2	147
33	0.2	153
36	0.3	244
38	0.1	47
19	0.1	6
21	0.1	9
26	0.5	302
27	0.5	231
25	0.4	219
28	0.5	276
29	0.5	253
31	0.4	192
30	0.4	174
37	0.4	189
49	0.6	273
43	0.2	51
23	0.1	14
31	0.2	23
81	0.5	612
76	0.5	457
64	0.4	452
86	0.5	591
99	0.7	572
95	0.7	416
42	0.4	384
40	0.4	359
51	0.4	532
43	0.2	113
26	0.1	12
47	0.2	22
99	1	704
99	1.1	642
97	1	537
96	1	684

Продовження додатка Б

I	J	K
Використано постійної пам'яті Gb	Кількість інтеграцій	Кількість попереджень
19	1	0
13	1	0
14	1	0
14	1	0
15	1	0
18	1	0
11	1	0
14	1	0
16	1	0
18	1	0
19	1	0
19	1	0
21	1	0
15	1	0
17	1	0
17	1	0
18	1	0
19	1	0
17	1	0
26	1	0
29	1	3
31	1	0
32	1	0
34	1	2
35	1	7
29	1	4
32	1	0
33	1	0
35	1	1
36	1	0
19	1	0
32	2	0
47	2	32
50	2	36
54	2	28
59	2	25

Додаток В

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України:

Тімінський О. Г. & Райчук І. В. (2019). Метод ціннісно-орієнтованого управління зацікавленими сторонами проекту діджиталізації. Управління проектами та розвиток виробництва, 3(71), 114–120.

Тімінський О. Г., Войтенко О. С. & Райчук І. В. (2021). Аналіз моделей і методів діджиталізації бізнес-процесів. Управління розвитком складних систем, 46, 38–47.

Райчук І. В., Хлевна Ю. Л., Войтенко О. С. & Тімінський О. Г. (2022). Розробка моделі діджиталізації процесу закупівель Hardware для IT-компанії. Управління розвитком складних систем, 50, 44–51.

Бушуєв С., Івко А. & Райчук І. В. (2023). Вибір моделі організаційної структури проєкту діджиталізації бізнес процесів в контексті синкретичного управління. Вісник Львівського державного університету безпеки життєдіяльності, 28, 5–13.

Райчук І. В. (2024). Експертна оцінка ідентифікації ризиків втрати персональних даних при інформаційній взаємодії у діджиталізованому освітньому середовищі. Наука і техніка сьогодні, Серія «Техніка», 13(41), 1227–1238.

Райчук І. В. & Мірошниченко І. В. (2025). Модель управління зберіганням потоків даних освітнього середовища. Наука і техніка сьогодні, Серія «Техніка», 1(42), 1360–1379.

Статті включені до наукометричної бази даних Scopus:

Raichuk I., Khlevna I., Timinskyi O. & Voitenko O. (2022). Cognitive model of digitalization of business processes of a project-oriented IT company. CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3382/Paper12.pdf

Khlevna I., Raichuk I. & Timinskyi O. (2023). The development of the information technology architecture for the anonymisation of stakeholders personal data of digitalized

education based on formulated criteria and requirements. In Workshop Proceedings of the X International Scientific Conference “Information Technology and Implementation" (IT&I 2023) (Kyiv, Ukraine, November 20-21, 2023, c. 139–148).

Raichuk I., Kolesnikova K., Khlevna I., Timinskyi O. & Kubiavka L. (2024). Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools. Procedia Computer Science, 231, 347–352. https://doi.org/10.1016/j.procs.2023.12.215

Тези конференцій за темою, в яких автор приймав участь:

Тімінський О. Г. & Райчук І. В. (2019). Передумови розробки моделей і методів для управління проектом створення генералізованого штучного інтелекту на базі ціннісного підходу. У Матеріали VI міжнародної науково-практичної конференції «Інформаційні технології та взаємодії» (с. 80–83). Київ.

Raichuk I. (2020). Models of digitalization of business processes of project-oriented organizations based on artificial neural networks. In Proceedings of the VII International Conference "Information Technology and Interactions" (Satellite) (pp. 217–220). Kyiv.