УДК 342.72

Анастасія ЄФІМЧЕНКО
Олеся ВОЙТОВИЧ

УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ ПЕРСОНАЛЬНИХ ДАНИХ СТУДЕНТІВ У БАЗІ УНІВЕРСИТЕТУ

Вінницький національний технічний університет

Анотація

У дослідженні розглянуто управління життєвим циклом персональних даних студентів у локальній базі університету. Правову основу складають Закон України № 2297-VI та Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409. На основі правових вимог спроєктовано архітектуру системи з розмежуванням доступу. Описано технічні рішення для кожної стадії циклу: імпорт даних з валідацією та контролем доступу, архівне зберігання без фізичного видалення, генерацію документів та два сценарії завершення циклу.

Ключові слова: життєвий цикл персональних даних, чутливі персональні дані, захист персональних даних, кіберзахист, управління доступом.

Abstract

The study examines the management of the personal data lifecycle of the students in a local database. The legal basis consists of Law of Ukraine No. 2297-VI and the Order of the State Service of Special Communications dated 30.06.2025 No. 409. Based on the legal requirements, a system architecture with access control has been designed. Technical solutions are described for each lifecycle stage: data import with validation and access control, archival storage without physical deletion, document generation, and two end-of-lifecycle scenarios.

Keywords: personal data lifecycle, sensitive personal data, personal data protection, cybersecurity, access control.

Вступ

Чутливі персональні дані в цифрових базах не є статичними об'єктами - вони проходять повний життєвий цикл: збір, зберігання, використання, передача та знищення. На кожному з цих етапів виникають специфічні ризики, і відсутність захисту хоча б на одній стадії робить весь цикл вразливим [1-2]. Університетські бази даних студентів належать до систем, що обробляють чутливі персональні дані: відомості про ПІБ, дату народження, паспортні дані, ідентифікаційний код та фінансовий статус навчання. Некоректне управління такими даними, зокрема, їх несанкціоноване розкриття або неконтрольоване видалення, може завдати прямої шкоди суб'єктам і порушити вимоги Закону України «Про захист персональних даних» № 2297-VI [3], Регламенту Ради Європи [4] НД ТЗІ 3.6-006-24 [5] та Наказу Адміністрації Держспецзв'язку від 30 червня 2025 року № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація» [6]. Актуальність проблеми обумовлена тим, що дані студентів постійно змінюються протягом усього строку навчання та зберігають юридичну значущість десятиліттями після його завершення. У зв’язку з цим важливо розробити технічні рішення для управління повним життєвим циклом персональних даних студентів з дотриманням вимог [3–6].

Результати дослідження

Правові засади обробки персональних даних студентів. Стаття 7 Закону [3] встановлює заборону на обробку чутливих персональних даних без правової підстави. Для університетської бази підставою є договір між університетом та студентом. Стаття 6 закріплює принцип мінімізації: до бази вносяться лише поля, необхідні для адміністрування навчання та формування документів - зайві відомості не збираються.

Життєвий цикл персональних даних студента охоплює кілька послідовних стадій: збір при вступі, зберігання та використання протягом навчання, оновлення при зміні статусу (переведення, поновлення, відрахування) та завершення після закінчення нормативного строку зберігання. Стаття 6 Закону [3] вимагає зберігати дані лише протягом строку, необхідного для мети обробки. При цьому стаття 15 надає суб'єкту право вимагати видалення або знищення своїх персональних даних, і університет зобов'язаний це виконати.

Для університету мета обробки не завершується з відрахуванням або випуском студента: обов'язок видачі офіційних документів зберігається відповідно до архівного законодавства протягом десятиліть. Студент може звернутися за випискою через 10-20 років, і документ має містити точну назву факультету та код освітньої програми, які були актуальні саме під час навчання - навіть якщо згодом вони змінилися або факультет реорганізовано. Це означає, що фізичне видалення активних записів і редагування довідникових таблиць є неприпустимим за замовчуванням: система зберігає всі версії даних в архівному статусі, і лише явна письмова вимога суб'єкта є підставою для їх повного видалення.

Вимоги щодо захисту персональних даних під час управління життєвим циклом. Першим кроком є збір даних через імпорт з таблиць, який реалізовано як основний механізм первинного наповнення бази та щорічного оновлення. Імпорт виконується лише уповноваженими відповідальними особами з відповідними правами доступу - працівники без права на внесення даних до імпорту не допускаються. Перед виконанням імпорту система перевіряє автентифікацію користувача та його належність до ролі з правом внесення даних - лише така особа може ініціювати запис до бази. Перед записом виконується валідація обов'язкових полів: відомості про ПІБ, дату народження, паспортні дані, ідентифікаційний код та фінансовий статус навчання. Записи з незаповненими або некоректними полями відхиляються з формуванням звіту про помилки. Поновлені студенти додаються окремим записом із відповідним статусом та посиланням на попередній запис - це зберігає повну історію без дублювання.

Другим кроком є зберігання, організоване так, що жоден запис не видаляється фізично з основної таблиці. Кожен студентський запис має відповідний статус (активний, відрахований, випущений або поновлений). Відрахування та випуск змінюють лише статус із фіксацією дати події. Довідникові таблиці факультетів та освітніх програм також не редагуються - при зміні назви додається новий запис, а старий зберігається з міткою архівування. Студентський запис завжди посилається на ту версію факультету та КП, яка була актуальна під час вступу, що гарантує коректність виписок через роки. Доступ до даних на цьому етапі розмежовано за ролями: відповідальні особи мають право лише на перегляд та редагування записів у межах своїх повноважень без права видалення. Конфіденційність даних при зберіганні забезпечується обмеженням доступу до файлів бази на рівні операційної системи. Резервне копіювання повинно здійснюватися не рідше ніж щотижня (CP-9), копії зберігаються у захищеному каталозі з обмеженим доступом (MP-4).

Третім кроком є використання даних через набір запитів: наприклад, загальні списки за факультетами за роком вступу, фільтрація за формою навчання, списки відрахованих. Доступ до запитів надається лише автентифікованим користувачам відповідно до їх ролі — перегляд загальних списків доступний широкому колу відповідальних осіб, тоді як формування звітів із персональними даними обмежено лише уповноваженими особами. На цьому етапі передбачається генерація документів, як то: навчальна картка, додаткова угода тощо, необхідних при обробці даних студентів. Важливо, щоб перед формуванням документа система перевіряла наповненість усіх обов'язкових полів запису.

Останнім важливим етапом є завершення циклу, для якого передбачено два сценарії. За першим сценарієм - після закінчення нормативного строку зберігання - запис переміщується з основної таблиці до архівної таблиці зі збереженням усіх полів у повному обсязі. Доступ до архіву мають лише уповноважені відповідальні особи, автентифікація яких перевіряється при кожному зверненні до архівних даних. За другим сценарієм, якщо студент подає письмову вимогу про видалення своїх даних (у випадках, коли це не суперечить іншим законам), відповідно до статті 15 [3] - запис видаляється як з основної таблиці, так і з архівної. Після цього видати виписку на підставі цієї бази неможливо. Факт і дата видалення фіксуються в

журналі подій як підтвердження виконання правових зобов'язань відповідно до вимоги журналювання подій (AU-3).

Висновок

Запропоновані технічні рішення забезпечують захист персональних даних студентів на кожному етапі життєвого циклу: розмежування доступу за ролями унеможливлює несанкціоноване внесення або перегляд даних, валідація полів при імпорті гарантує цілісність інформації, обмежений доступ до файлів бази та регулярне резервне копіювання забезпечують конфіденційність при зберіганні, а журналювання всіх операцій підтримує підзвітність. Архівування записів після завершення навчання зберігає можливість видачі виписок через десятиліття, збереження старих версій факультетів і конкурсних пропозицій гарантує коректність документів, а повне видалення за письмовою вимогою суб'єкта забезпечує дотримання прав особи щодо власних даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Берездецький Ю. М., Шкрібляк К. П., Пальчик М. Л. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки України в умовах війни. URL: https://journal-app.uzhnu.edu.ua/article/view/346536 (дата звернення: 05.03.2026).

2. Бурчак В. Л. Кібербезпека: освіта, наука, техніка. Спеціальний випуск. URL: https://csecurity.kubg.edu.ua/index.php/journal/issue/view/34 (дата звернення: 05.03.2026).

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (чинна редакція станом на 12.02.2025). URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 26.02.2026).

4. Регламент Європейського Парламенту та Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, GDPR). Офіційний вісник Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 27.02.2026).

5. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. НД ТЗІ 3.6-006-24. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення: 08.03.2026).

6. Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація».URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-zatverdila-bazovi-profili-bezpeki-modernizuyuchi-pidkhodi-do-kiberzakhistu-derzhavnikh-sistem (дата звернення: 05.03.2026).

ЄФІМЧЕНКО Анастасія – студентка групи 1БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 14estasyf09@gmail.com

ВОЙТОВИЧ Олеся – доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: voytovych.olesya@vntu.edu.ua

YEFIMCHENKO Anastasiia – student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 14estasyf09@gmail.com

VOYTOVYCH Olesia – Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.olesya@vntu.edu.ua