УДК 342.72

Георгій ГОЛУБ
Олеся ВОЙТОВИЧ

ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ДОСТУПУ ДО ЛОКАЛЬНОЇ БАЗИ ДАНИХ СТУДЕНТІВ УНІВЕРСИТЕТУ

Вінницький національний технічний університет

Анотація

У дослідженні розглянуто організацію захищеного доступу до локальної бази персональних даних студентів університету. На основі правових вимог спроєктовано трирівневу архітектуру системи з розмежуванням доступу відповідальних осіб. Описано технічні рішення: парольна автентифікація на двох рівнях, розмежування прав користувачів за ролями та захист даних при зберіганні.

Ключові слова: чутливі персональні дані, захист персональних даних, кіберзахист, управління доступом, розмежування доступу, парольна автентифікація.

Abstract

The study examines the organization of secure access to a local database of university students' personal data. In accordance with legal requirements, a three-tier system architecture with access control for authorized personnel has been designed. Technical solutions are described: two-level password authentication, role-based MySQL user access control, and data protection at rest.

Keywords: sensitive personal data, personal data protection, cybersecurity, access control, role-based access control, password authentication.

Вступ

Бази даних студентів університетів містять чутливі персональні дані: відомості про ПІБ, дату народження, паспортні дані, ідентифікаційний код та фінансовий статус навчання і вимагають використання спеціальних захисних механізмів для забезпечення їх безпеки [1-3]. Стаття 24 Закону України «Про захист персональних даних» № 2297-VI [4] зобов'язує володільця вживати організаційних і технічних заходів для захисту таких даних від несанкціонованого доступу та незаконної обробки. Виконання цієї вимоги потребує не лише загальних принципів, а й конкретних технічних рішень, адаптованих до архітектури конкретної системи.

Актуальність проблеми полягає в тому, що університетські інформаційні системи часто будуються на зв'язці реляційної СУБД та настільного застосунку без належного розмежування доступу: часто, відповідальні особи працюють під одним обліковим записом, відсутня журналізація дій, а доступ до сервера бази даних не обмежений на мережному рівні. Мета роботи - розробити та описати технічні рішення для організації захищеного локального доступу до бази персональних даних студентів з дотриманням вимог [4] та Наказу Адміністрації Держспецзв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація» [5].

Результати та дослідження

Правові засади захисту чутливих персональних даних. Відсутність розмежування доступу в університетських інформаційних системах створює реальні загрози безпеці персональних даних студентів. Якщо всі відповідальні особи працюють під одним обліковим записом бази даних, будь-хто з них може виконати довільний запит, змінити або видалити записи - і встановити, хто саме це зробив, технічно неможливо. Відсутність журналізації дій та необмежений доступ до сервера на мережному рівні додатково посилюють цю проблему. Саме

такі умови і призводять до порушення вимог статті 24 [4], яка зобов'язує застосовувати організаційні та технічні заходи захисту персональних даних.

Закон [4] у статті 7 встановлює спеціальний режим для чутливих персональних даних, а стаття 6 закріплює принцип мінімізації: до бази вносяться лише поля, необхідні для адміністрування навчання. Стаття 24 прямо зобов'язує застосовувати організаційні та технічні заходи захисту від несанкціонованого доступу та незаконної обробки - саме ця норма є правовою підставою для впровадження описаних нижче рішень.

Для вирішення проблеми важливо побудувати систему за трирівневою архітектурою, де сервер розміщується на окремому комп'ютері університетської локальної мережі та виконує роль сховища даних, агенти користувачів з правами доступу встановлюються на робочих місцях відповідальних осіб і виконує роль фронтенду - форми, запити, генерація документів. Використання локальної мережі університету як середовища доступу відповідає вимогам статті 24 [4] та Базового профілю безпеки [5]: підключення дозволяється лише з авторизованих IP-адрес локальної мережі, а зовнішній доступ заблоковано на рівні сервера, що забезпечує контрольоване та захищене середовище обробки персональних даних. З'єднання між сервером та користувачем реалізується через ODBC-драйвер: у системі налаштовується DSN, який містить адресу сервера, ім'я бази та облікові дані користувача. Відповідальні особи працюють виключно через форми і не мають прямого доступу до сервера - це унеможливлює виконання довільних запитів та обмежує операції з даними лише дозволеними функціями інтерфейсу.

Технічні рішення для організації захищеного доступу. Розмежування доступу реалізовано через створення окремих користувачів для кожної ролі відповідальної особи. Наприклад, для працівників деканату створюється обліковий запис із правами SELECT, INSERT, UPDATE на таблиці студентів - але без права DELETE та без доступу до архівних таблиць. Для осіб, що відповідальні за забезпечення життєвого циклу обробки даних, в системі створюється окремі облікові записи із розширеними правами, включно з доступом до архіву та таблиці журналу подій. Підключення до сервера дозволяється лише з IP-адрес локальної мережі університету - підключення ззовні блокується на рівні налаштувань мережі. Це відповідає вимозі мінімізації повноважень (AC-6) відповідно до НД ТЗІ 3.6-006 -24 [6].

Парольна автентифікація реалізується на двох рівнях. На рівні користувача кожна відповідальна особа входить у застосунок через форму входу із перевіркою логіна та пароля - це дозволяє ідентифікувати конкретного користувача та зафіксувати його дії в журналі, що відповідає вимогам статті 24 [4] щодо захисту від несанкціонованого доступу. На рівні сервера паролі зберігаються у хешованому вигляді, мають містити не менше 12 символів різних категорій та змінюватися не рідше ніж раз на 180 днів відповідно до вимоги управління автентифікатором IA-5(1). Після 30 хвилин бездіяльності форма автоматично блокується і вимагає повторного входу відповідно до заходу блокування пристрою (AC-11).

Захист даних при зберіганні забезпечується кількома заходами. Файли сервера зберігаються у каталозі з обмеженими правами доступу операційної системи - лише системний процес має до них доступ відповідно до заходу захисту носіїв (MP-2). Резервне копіювання реалізується з автоматичним розкладом не рідше ніж щотижня (CP-9): резервні копії зберігаються в окремому захищеному каталозі, доступному лише адміністратору. Усі дії відповідальних осіб із даними студентів фіксуються в таблиці журналу подій із зазначенням користувача, типу операції, часу та ідентифікатора запису (AU-3). Журнал переглядається адміністратором не рідше ніж щотижня відповідно до вимоги аудитування та підзвітності (AU-6) Наказу Адміністрації Держспецзв'язку [5].

Оскільки система є виключно локальною і не передбачає віддаленого доступу, підключення до сервера ззовні університетської мережі технічно заблоковано. Це суттєво звужує поверхню атаки: єдиним можливим вектором несанкціонованого доступу є фізичний доступ до комп'ютерів у локальній мережі, що регулюється організаційними заходами університету.

Висновок

Запропоновані технічні рішення забезпечують захищений доступ до локальної бази персональних даних студентів: трирівнева архітектура обмежує пряму взаємодію з сервером, розмежування користувачів за ролями реалізує принцип мінімізації повноважень, парольна

автентифікація на двох рівнях ідентифікує кожну відповідальну особу, а журналювання дій забезпечує підзвітність. Блокування зовнішніх підключень на рівні мережевих налаштувань унеможливлює віддалений несанкціонований доступ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Щавінський Ю., Будзинський О. Аналіз актуальних проблем безпеки корпоративних баз даних в умовах сучасної інфраструктури та шляхи їх вирішення. Державний університет інформаційно-комунікаційних технологій. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/726 (дата звернення: 18.03.2026).
2. Петльовий Б. С. Способи та засоби захисту баз даних. Тернопільський національний технічний університет імені Івана Пулюя, 2024. 72 с. URL: https://elartu.tntu.edu.ua/handle/lib/48321 (дата звернення: 18.03.2026).
3. Задерейко О., Трофименко О., Єленич С., Логінова Н., Гура В. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. Національний університет «Одеська юридична академія». 2025. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/735 (дата звернення: 18.03.2026).
4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297 - 17 (дата звернення: 26.02.2026).
5. 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).
6. 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).

ГОЛУБ Георгій – студент групи 1БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,e-mail: holub.ge@gmail.com

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

HOLUB Heorhii – student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: holub.ge@gmail.com

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