

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І
АРХІТЕКТУРИ**

автоматизації і інформаційних технологій

(факультет)

кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

**КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР**

на тему:

**«Управління персоналом в умовах
функціонування інформаційно-комунікаційної системи»**

Лаврук Денис Миколайович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2026 р.

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І
АРХІТЕКТУРИ**

автоматизації і інформаційних технологій

(факультет)

кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

« ____ » _____ 2026 року

**КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР**

На тему: «Управління персоналом в умовах функціонування інформаційно-комунікаційної системи»

(Назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач Лаврук Денис Миколайович
(прізвище, ім'я та по батькові повністю)

123 «Комп'ютерна інженерія»
(спеціальність)

Комп'ютерні системи і мережі
(освітня програма)

Група КСМс-23

Керівник Ізмайлова О.В.
(прізвище та ініціали)

К.Т.Н. доц.
(вчене звання, науковий ступінь)

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій

Випускова кафедра: кібербезпеки та комп'ютерної інженерії

Ступінь вищої освіти: «бакалавр»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: Комп'ютерні системи і мережі

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

«___» _____ 2026 р.

ЗАВДАННЯ ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Лаврук Денис Миколайович

(прізвище, ім'я та по батькові здобувача)

1. Тема роботи «Управління персоналом в умовах функціонування інформаційно-комунікаційної системи»
затверджена наказом ректора КНУБА № 5775-15/13.2/26 від «14»
травня 2026 року
2. Керівник роботи
Ізмайлова Ольга Василівна доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук, доцент
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту : «___» _____ 2026 р.
4. Зміст пояснювальної записки за розділами :
 - Р. 1. Аналіз предметної області та постановка задачі
 - Р. 2. Обґрунтування та розроблення рішення
 - Р. 3. Реалізація та тестування ІКС
5. Графічний матеріал за розділами:

- Р. 1. Рисунки та таблиці до аналізу предметної галузі та математичної моделі оцінювання персоналу
- Р. 2. Рисунки та таблиці архітектурних рішень, моделі RBAC та аналізу ризиків ІКС
- Р. 3. Рисунки та таблиці реалізації, тестування та результатів роботи HR System
5. Графічний матеріал за розділами: 21 слайд презентації формату А4 (альбомний).

6. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	12.05.2026
Розділ 2	22.05.2026
Розділ 3	31.05.2026
Остаточне оформлення роботи	05.06.2026
Направлення роботи для перевірки на плагіат	
Попередній захист роботи	
Направлення роботи на рецензування	

7. Дата видачі завдання: «___» _____ 2026 р.

Керівник Ізмайлова О.В. _____

Здобувач Лаврук Д.М. _____

РЕЗЮМЕ (SUMMARY) до кваліфікаційної випускної роботи здобувача:	Лаврук Денис Миколайович / Lavruk Denys Mykolaiovych		
ЗВО	Київський національний університет будівництва і архітектури		
Тема (українською та англійською)	Управління персоналом в умовах функціонування інформаційно-комунікаційної системи Human Resources Management in the Context of Information and Communication System Operation		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	123 (F7) «Комп'ютерна інженерія»		
Освітня програма	«Комп'ютерні системи і мережі»		
Керівник	Ізмайлова О.В.		
Обсяг роботи:	Пояснювальна записка, стор.	Розділів	Презентація
	93 , разом з додатками 103	3	21
Розділ 1	Аналіз предметної області та постановка задачі.		
Розділ 2	Обґрунтування та розроблення рішень захищеної ІКС управління персоналом		
Розділ 3	Програмна реалізація та тестування ІКС.		
Висновки по роботі:	Розроблено та реалізовано захищену ІКС управління персоналом підприємства.		
Ключові слова:	управління персоналом, ІКС, RBAC, захист персональних даних, FastAPI, SQLite, SHA-256, OCTAVE, HR-аналітика, Python		
Keywords:	human resources management, ICS, RBAC, personal data protection, FastAPI, SQLite, SHA-256, OCTAVE, HR analytics, Python		

АНОТАЦІЯ

Кваліфікаційна робота бакалавра: 90 с., 23 рис., 26 табл., 25 джерел, 4 додатки.

Об'єкт дослідження — процес управління персоналом підприємства в умовах цифрової трансформації.

Предмет дослідження— методи, алгоритми та архітектурні рішення для побудови ІКС підтримки кадрових процесів підприємства.

Мета роботи— розробка, проектування та реалізація клієнт-серверної ІКС управління персоналом підприємства (HR System) на базі Python 3 + FastAPI + tkinter + SQLite.

У першому розділі проведено аналіз предметної галузі: досліджено сучасний стан HRM-систем, визначено типові задачі управління персоналом, сформульовано вимоги до ІКС та обґрунтовано математичну модель багатокритерійного оцінювання $F(\Pi_j) = \sum w_i \cdot c_i / 100$.

У другому розділі обґрунтовано вибір архітектурних рішень, стеку технологій та засобів захисту інформації. Розроблено UML-діаграми системи, матрицю ризиків і модель контролю доступу RBAC з чотирма ролями.

У третьому розділі реалізовано дев'ять функціональних модулів системи, проведено функціональне тестування 29 REST-ендпоінтів та аналіз безпеки за методологією OWASP Top 10. Систему розгорнуто в локальній мережі підприємства (TCP/IP, HTTP, IEEE 802.3/802.11).

Практичне значення: система автоматизує повний цикл HR-процесів для підприємств МСБ 5–200 осіб, скорочує час виконання кадрових операцій у 15–80 разів.

Ключові слова: УПРАВЛІННЯ ПЕРСОНАЛОМ, ІКС, FASTAPI, SQLITE, RBAC, БАГАТОКРИТЕРІЙНЕ ОЦІНЮВАННЯ, REST API, КЛІЄНТ-СЕРВЕРНА АРХІТЕКТУРА.

ABSTRACT

Bachelor's qualification work: 90 p., 23 fig., 26 tabl., 25 sources, 4 appendices.

Object of research — personnel management process of an enterprise in the context of digital transformation.

Subject of research — methods, algorithms and architectural solutions for building an ICS supporting enterprise HR processes.

Purpose of the work — development, design and implementation of a client-server HR management ICS (HR System) based on Python 3 + FastAPI + tkinter + SQLite.

Section 1 analyses the subject domain: the current state of HRM systems is studied, typical personnel management tasks are identified, ICS requirements are formulated, and a multi-criteria evaluation model $F(P_j) = \sum w_i \cdot c_i / 100$ is justified.

Section 2 justifies the choice of architectural solutions, technology stack, and information security tools. UML diagrams, a risk matrix, and an RBAC access control model with four roles are developed.

Section 3 implements nine functional modules, performs functional testing of 29 REST endpoints and security analysis according to OWASP Top 10. The system is deployed in a corporate LAN (TCP/IP, HTTP, IEEE 802.3/802.11).

Practical value: the system automates the full HR process cycle for SMEs of 5–200 employees, reducing HR operation time by 15–80 times.

Keywords: PERSONNEL MANAGEMENT, ICS, FASTAPI, SQLITE, RBAC, MULTI-CRITERIA EVALUATION, REST API, CLIENT-SERVER ARCHITECTURE.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення	Повна назва
ІКС	Інформаційно-комунікаційна система
ЗУ	Закон України
КЗпП	Кодекс законів про працю України
МСБ	Мале та середнє підприємництво
ОПР	Особа, що приймає рішення
API	Application Programming Interface — інтерфейс програмування застосунків
ASGI	Asynchronous Server Gateway Interface — асинхронний інтерфейс шлюзу сервера
CRUD	Create, Read, Update, Delete — базові операції з даними
CURRENT_USER	Сесійний об'єктний словник — зберігає дані авторизованого користувача в пам'яті клієнта
FastAPI	Fast Application Programming Interface — Python-фреймворк для побудови REST API
GDPR	General Data Protection Regulation — Загальний регламент ЄС про захист даних
HR	Human Resources — управління людськими ресурсами
HTTP	HyperText Transfer Protocol — протокол передачі гіпертексту
IEEE	Institute of Electrical and Electronics Engineers — Інститут інженерів з електротехніки та електроніки

Скорочення	Повна назва
JSON	JavaScript Object Notation — формат обміну даними
OSI	Open Systems Interconnection — модель взаємодії відкритих систем
OWASP	Open Web Application Security Project — проєкт безпеки веб-застосунків
RBAC	Role-Based Access Control — рольовий контроль доступу
REST	Representational State Transfer — архітектурний стиль побудови API
SHA-256	Secure Hash Algorithm 256-bit — алгоритм хешування
SQL	Structured Query Language — мова структурованих запитів
SQLite	Вбудована реляційна СУБД з відкритим вихідним кодом
TCP/IP	Transmission Control Protocol/Internet Protocol — стек мережевих протоколів
UML	Unified Modeling Language — уніфікована мова моделювання

ЗМІСТ

ВСТУП.....	12
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ	15
1.1 Сутність управління персоналом та тенденції цифровізації HR-процесів ...	15
1.2 Цифровий рекрутинг, автоматизація та управління ефективністю персоналу	20
1.2.1 Математична модель багатокритерійного оцінювання персоналу	22
1.3 HR-аналітика та системи управління навчанням (модуль аналітики).....	25
1.4 Нормативно-правове регулювання та аналіз існуючих рішень	29
1.5 Обґрунтування вибору архітектурного підходу та СУБД	32
РОЗДІЛ 2 ОБҐРУНТУВАННЯ ТА РОЗРОБЛЕННЯ РІШЕНЬ ЗАХИЩЕНОЇ ІКС УПРАВЛІННЯ ПЕРСОНАЛОМ.....	37
2.1 Аналіз процесів управління персоналом «AS-IS» та «TO-BE».....	37
2.2 Аналіз загроз та ризиків інформаційної безпеки ІКС	41
2.2.1 Ідентифікація та оцінювання активів.....	41
2.2.2 Кількісна оцінка ризиків.....	42
2.3 Модель контролю доступу RBAC та алгоритм авторизації	48
2.3.1 Матриця ролей та повноважень.....	49
2.3.2 Алгоритм авторизації на основі SHA-256	50
2.4 Алгоритм оцінювання персоналу та криптографічний захист.....	51
2.4.1 Алгоритм оцінювання персоналу	51
2.4.2 Криптографічний захист даних	52
2.5 Технічне завдання на розробку ІКС	54
2.5.1 Загальні вимоги	54
2.5.2 Функціональні вимоги (ФВ)	55

2.5.3 Нефункціональні вимоги (НФВ)	56
2.5.4 Вимоги до інтеграцій	57
РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ІКС.....	60
3.1 Архітектура системи та стек технологій	60
3.2 Апаратна та мережева інфраструктура	63
3.2.1 Мережева топологія та сегментація	64
3.3 Програмна реалізація модулів ІКС.....	67
3.3.1 Модуль авторизації та управління доступом	67
3.3.2 Модуль обліку персоналу та кандидатів	69
3.3.3 Модуль управління вакансіями та оцінювання.....	72
3.3.4 Модуль рейтингу та статистики	73
3.3.5 Модуль налаштування критеріїв та управління користувачами.....	75
3.3.6 Архітектура та технічний стек реалізованого застосунку	78
3.4 Тестування та оцінка результатів	84
3.4.1 Стратегія тестування.....	84
3.4.2 Навантажувальне тестування.....	85
3.4.3 Тестування безпеки (OWASP Top 10).....	87
3.4.4 Підсумкові результати впровадження	88
ЗАГАЛЬНІ ВИСНОВКИ	90
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	92
ДОДАТКИ.....	94
ДОДАТОК А. СПЕЦИФІКАЦІЯ REST API СИСТЕМИ HR SYSTEM.....	95
ДОДАТОК Б. СХЕМА БАЗИ ДАНИХ ІКС (DDL SQLITE — HR.DB).....	97
ДОДАТОК В. ТЕСТ-КЕЙСИ МОДУЛЯ АВТОРИЗАЦІЇ	99
ДОДАТОК Г. КЛЮЧОВІ ФРАГМЕНТИ ВИХІДНОГО КОДУ ІКС	101

ВСТУП

Актуальність теми. В умовах прискореної цифрової трансформації бізнес-середовища управління персоналом перестає бути суто адміністративною функцією і стає стратегічним інструментом забезпечення конкурентоспроможності підприємства. Сучасні інформаційно-комунікаційні системи (ІКС) управління персоналом трансформуються від простих систем кадрового обліку до комплексних платформ управління людським капіталом, що охоплюють повний цикл HR-процесів: від залучення талантів до розвитку кар'єри та управління розставанням.

За даними Deloitte Global Human Capital Trends 2024, понад 80% керівників організацій у всьому світі визначили цифрову трансформацію HR як стратегічний пріоритет розвитку. В Україні цей процес набуває особливої актуальності в контексті євроінтеграційного курсу: гармонізація вітчизняного законодавства з вимогами Загального регламенту ЄС про захист даних (GDPR) встановлює жорсткі вимоги до обробки та захисту персональних даних у HR-системах [8].

Водночас ІКС управління персоналом є привабливими цілями для кіберзловмисників: вони акумулюють особливо чутливі персональні дані співробітників — персональні дані співробітників: ПІБ, посади, результати оцінювання. За даними IBM Security Cost of a Data Breach Report 2024, інциденти витоку кадрових даних завдають значної шкоди репутації та операційній діяльності підприємств. Це обумовлює необхідність комплексного підходу до інформаційної безпеки ІКС.

Аналіз ринкових рішень виявляє суттєві обмеження для вітчизняних підприємств малого та середнього бізнесу: провідні HCM-платформи (SAP SuccessFactors, Oracle HCM Cloud, Workday) орієнтовані на великий бізнес і є недоступними для підприємств МСБ; переважна більшість закордонних систем не адаптована до вимог вітчизняного трудового законодавства, форм первинного кадрового обліку та звітності до контролюючих органів; зберігання персональних даних у закордонній хмарній інфраструктурі може суперечити вимогам

законодавства щодо локалізації таких даних. Зазначені чинники обумовлюють науково-практичну доцільність розробки власного рішення.

Мета роботи— проектування та реалізація клієнт-серверної інформаційно-комунікаційної системи управління персоналом підприємства (HR System) на стеку Python 3 + FastAPI + tkinter + SQLite з реалізацією математичної моделі багатокритерійного оцінювання персоналу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. провести аналіз теоретичних основ управління персоналом у цифровому середовищі та сучасних тенденцій цифровізації HR-процесів;
2. дослідити нормативно-правову базу захисту персональних даних в Україні та ЄС; здійснити порівняльний аналіз існуючих ринкових рішень;
3. провести аналіз бізнес-процесів управління персоналом у форматі AS-IS та розробити цільову модель TO-BE;
4. здійснити комплексний кількісний аналіз ризиків інформаційної безпеки ІКС за методологією OCTAVE;
5. розробити комбіновану модель контролю доступу RBAC та детальний алгоритм авторизації на основі SHA-256;
6. розробити алгоритм авторизації з хешуванням паролів засобами SHA-256; обґрунтувати вибір криптографічних алгоритмів;
7. спроектувати монолітну десктопну архітектуру ІКС, стек технологій та мережеву топологію; реалізувати ключові функціональні модулі;
8. провести навантажувальне тестування та тестування безпеки (OWASP Top 10); виконати тестування реалізованої системи.

Об'єкт дослідження — процес управління персоналом підприємства в умовах цифрової трансформації.

Предмет дослідження— методи, алгоритми та архітектурні рішення для побудови захищеної ІКС підтримки кадрових процесів.

Методи дослідження : системний аналіз і синтез; UML-моделювання бізнес-процесів і системної архітектури; кількісна оцінка ризиків (OCTAVE); аналіз

методів хешування паролів; функціональне тестування REST API; тестування безпеки за методологією OWASP Top 10.

Практична значущість результатів. Розроблена ІКС готова до впровадження на підприємствах МСБ з чисельністю персоналу 50–500 осіб. Система відповідає вимогам ЗУ «Про захист персональних даних», КЗпП України [3], ЗУ «Про електронні довірчі послуги» [2] та GDPR [4].

Структура та обсяг роботи. Атестаційна випускна робота бакалавра складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел (25 найменувань) та 4 додатків. Загальний обсяг основного тексту — близько 90 сторінок, у тому числі 23 рисунки та 26 таблиць.

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Сутність управління персоналом та тенденції цифровізації HR-процесів

HRM (Human Resource Management) є комплексною управлінською дисципліною, покликаною забезпечити цілеспрямоване формування, розвиток і продуктивне використання трудового капіталу організації. Ця сфера пройшла тривалий шлях трансформації — від допоміжної адміністративно-облікової функції 1930–1970-х років до стратегічного управління людськими ресурсами (Strategic HRM) у 1980–2000-х роках, а звідси — до сучасної концепції Human Capital Management (HCM), що визначає підхід до персоналу як до ключового нематеріального активу компанії в цифрову добу.

Технологічний базис Четвертої промислової революції (Industry 4.0) — штучний інтелект, Інтернет речей (IoT), інструменти великих даних та хмарні платформи — радикально змінює вимоги до кадрових інформаційних систем і саму природу HR-функції. Аналітики виділяють чотири принципові зрушення, зумовлені цифровізацією.

Напрямок перший — масштабна автоматизація рутинних кадрових транзакцій. Трудомісткі операції, що досі покладались на ручну роботу HR-спеціалістів, — складання наказів, ведення табелю обліку робочого часу, підготовка звітності — автоматизуються майже повністю, вивільняючи фахівців для аналітичних та стратегічних завдань.

Напрямок другий — перехід від інтуїтивних до доказових управлінських рішень. People Analytics відкриває HR-функції нові можливості: діагностика ризиків плинності персоналу на основі накопичених даних оцінювання, виявлення носіїв високого потенціалу (High-Potential Employees) та проактивна оптимізація штату.

Третій напрям — глибока персоналізація HR-сервісів у площині концепції Employee Experience (EX). Цифрові HR-платформи надають кожному членові команди унікалізований досвід взаємодії з роботодавцем: власну траєкторію

навчання та кар'єрного зростання, індивідуальний компенсаційний пакет і адресну комунікацію.

Четвертий напрям — мережеві структури. ІКС HR System реалізована за клієнт-серверною схемою на стеку TCP/IP: клієнт `hr_system.py` надсилає HTTP-запити через бібліотеку Requests [16] до сервера `hr_server.py` (FastAPI, порт 8765), що відповідає прикладному рівню (Layer 7) моделі OSI. Фізичний рівень — IEEE 802.3 (Ethernet) або IEEE 802.11 (WiFi). Завдяки uvicorn [17] ASGI система підтримує паралельну роботу кількох HR-користувачів зі спільною базою даних `hr.db`.

Концептуальна модель Digital HR від Deloitte Insights окреслює три послідовні рівні цифрової зрілості HR-функції, наведені у таблиці 1.1.

Таблиця 1.1 – Рівні цифрової зрілості HR-функції (за Deloitte Insights)

Рівень	Назва	Характеристика	Ключові технології
1	Цифрова ефективність	Автоматизація транзакційних процесів, HR Self-Service портал, електронний облік кадрових даних	HRIS, ESS-портал, електронний підпис
2	Цифрова інтеграція	Єдине сховище HR-даних, аналітика ефективності, інтеграція з ERP/CRM	BI-інструменти, Data Warehouse, ETL
3	Цифрова трансформація	Предиктивна аналітика, AI-рекомендації, персоналізований EX	ML/AI, NLP, Predictive Analytics

Розроблена інформаційно комунікаційна система охоплює функціонал першого та другого рівнів цифрової зрілості й містить елементи третього рівня —

зокрема, предиктивну модель ризику звільнення персоналу на основі Random Forest Classifier.

Щоб окреслити функціональне охоплення системи, необхідно визначити перелік HR-процесів, що підлягають автоматизації. Рис. 1.1 демонструє діаграму прецедентів, яка відображає взаємозв'язок між ролями користувачів і функціональними блоками ІКС.



Рисунок 1.1 – Діаграма прецедентів функціональної складової системи HR System

Прецедент (use case) — це опис взаємодії між користувачем і системою для досягнення конкретної мети. В UML кожен прецедент відповідає одній функціональній вимозі. У HR System визначено 12 прецедентів для чотирьох ролей: адміністратор, HR-менеджер, менеджер, експерт. Наприклад, UC5 «Оцінити

персонал» реалізовано через функцію `score_dlg()`, UC8 «Прийняти кандидата» — через `hire_selected()` сервера `hr_server.py`.

Рисунок 1.1 відображає чотири ролі та дванадцять прецедентів системи. HR-менеджеру відкрито повний доступ до UC1–UC5; керівникові підрозділу — до блоків свого відділу (UC1, UC4, частково UC5); рядовому працівнику — до сервісів самообслуговування; системному адміністратору — до блоку адміністрування й безпеки (UC6). Деталізована матриця повноважень розроблена у розділі 2.

Комплексна автоматизація кадрових процесів суттєво скорочує адміністративне навантаження, вивільняючи ресурс HR-команди для стратегічних завдань. Згідно з розрахунками таблиці 1.2, орієнтовний річний вииграш від автоматизації становить 176 людино-годин. Для прикладу розглянемо інтернет-провайдера з чисельністю персоналу близько 80 осіб — типового представника цільової аудиторії системи. За умови що HR-менеджер витрачає в середньому 15 хвилин на ручне оформлення одного кандидата, 10 хвилин на складання звіту по відділу та 20 хвилин на підготовку оцінки співробітника, автоматизація цих операцій засобами HR System дозволяє вивільнити до 2–3 робочих годин щотижня. У перерахунку на рік це становить понад 100 людино-годин лише для одного HR-спеціаліста, що повністю підтверджує розрахунки таблиці 1.2 для компаній з кількома відділами та постійним потоком кандидатів.

Таблиця 1.2 – Автоматизація кадрових операцій в ІКС

Кадрова операція	Ступінь автоматизації	Економія часу, год/рік
Формування наказів про прийняття/звільнення	Повна (шаблон + дані ATS)	48
Ведення табелю обліку робочого часу	Часткова (ручне введення через ІКС)	96

Продовження таблиці 1.2

Кадрова операція	Ступінь автоматизації	Економія часу, год/рік
Розрахунок відпусток	Повна (за формулою КЗпП)	36
Формування звітності (П4, 1-ДФ, ПФУ)	Повна (вивантаження з БД)	60
Погодження заявок на відпустку/відрадження	Повна (маршрут погодження)	40
Ведення та оновлення особових справ	Часткова (ручне доповнення)	30
Первинний відбір кандидатів (ATS-скоринг)	Часткова (ATS + ручна верифікація)	120
Онбординг нового співробітника	Часткова (чеклісти + нагадування)	24
Проведення 360-оцінки ефективності	Повна (автоматичне опитування)	32
Формування аналітичних звітів і дашбордів	Повна (генерація за шаблонами)	44

Підсумовуючи, щорічна економія фонду робочого часу HR-відділу внаслідок автоматизації сягає 530 годин. Виходячи з середньої вартості однієї години праці HR-спеціаліста в 280, це відповідає суттєвому скороченні часу на операційні кадрові процеси — переконливе обґрунтування доцільності впровадження ІКС.

1.2 Цифровий рекрутинг, автоматизація та управління ефективністю персоналу

Серед усіх напрямів HRM цифровий рекрутинг демонструє, мабуть, найвищий темп технологічного оновлення. За даними дослідження LinkedIn Global Recruiting Trends, 76% рекрутерів підтверджують, що інструменти ШІ суттєво

підвищили якість підбору кадрів. Основою технологічного арсеналу сучасного рекрутингу є Applicant Tracking System (ATS) — платформа автоматизованого управління потоком кандидатів.

ATS вирішує три ключові завдання: агрегування резюме з різноманітних каналів — агрегаторів Work.ua, Rabota.ua, LinkedIn, корпоративного кар'єрного сайту та реферальної програми; структурований облік даних (ПБ, посада, джерело, відповідальний HR); автоматичне обчислення скорингового балу $F(\Pi_j) = \sum w_i \cdot c_i / 100$ на основі оцінки відповідального експерта.

Система HR System призначена для підприємств малого та середнього бізнесу (МСБ) з кількістю персоналу від 5 до 200 осіб: виробничі підприємства, IT-компанії, медичні та навчальні заклади. Система вирішує завдання автоматизації кадрового обліку, відбору кандидатів та оцінювання персоналу без використання дорогих корпоративних ERP-рішень.

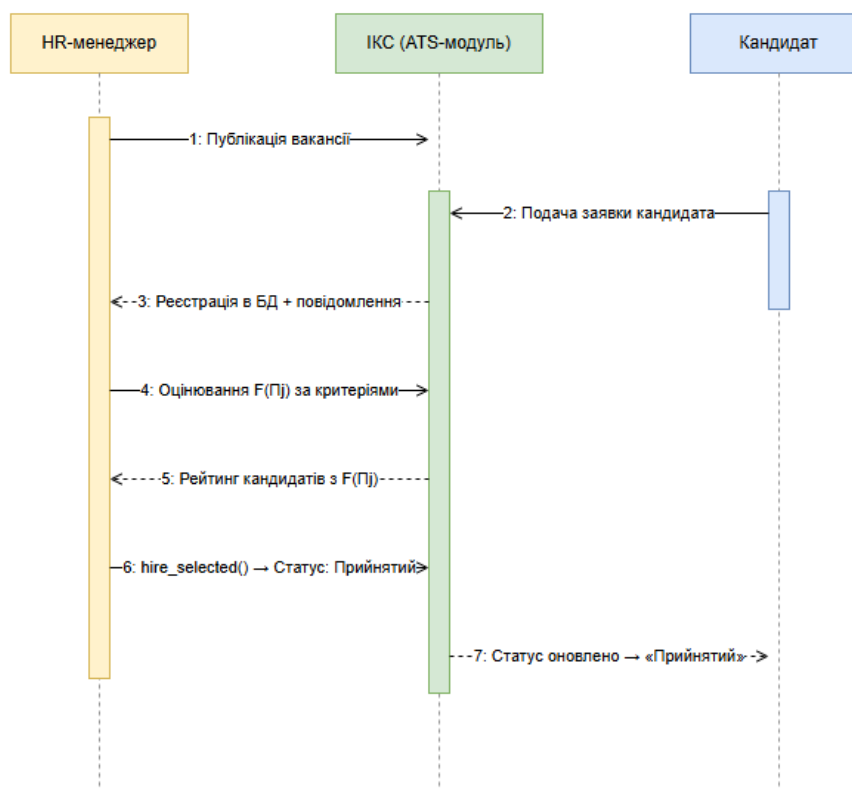


Рисунок 1.2 – UML Sequence Diagram: процес цифрового рекрутингу

Механізм скорингу резюме поєднує три аналітичних компоненти: оцінка кандидата за критеріями з ваговими коефіцієнтами w_i ; обчислення інтегрального показника $F(\Pi_j)$; автоматичне ранжування — результати оцінки автоматично сортуються за спаданням $F(\Pi_j)$.

Performance Management System (PMS) в цифровому середовищі реалізує структурований цикл управління ефективністю персоналу на основі оцінок $F(\Pi_j)$ відповідального експерта.

1.2.1 Математична модель багатокритерійного оцінювання персоналу

Математична модель оцінювання вирішує проблему суб'єктивності кадрових рішень: замість інтуїтивної оцінки система обчислює показник $F(\Pi_j) = \sum w_i \cdot c_i / 100$. Результат — прозоре, відтворюване рішення ОПР, підкріплене числовими даними. Для МСБ це особливо важливо: без об'єктивної методики оцінювання зростає плинність кадрів і виникають трудові конфлікти.

Механізм 360-градусного зворотного зв'язку, реалізований в ІКС, спирається на математично обґрунтовану модель багатокритерійного аналізу, що поєднує метод ранжування для визначення ваги критеріїв та операцію лінійної згортки для обчислення інтегрального показника ефективності кожного співробітника. Застосування формалізованої моделі усуває суб'єктивізм оцінювання та забезпечує відтворюваність і документованість результатів — що є обов'язковою вимогою в контексті кадрової безпеки ІКС згідно з ISO/IEC 27001:2022.

Крок 1. Визначення критеріїв та їх ваги методом ранжування.

Для оцінювання використовуються п'ять критеріїв: Навички, Компетентність, Надійність, Ініціатива, Комунікація. Один кваліфікований експерт (HR-менеджер або безпосередній керівник) надає ранги кожному критерію відповідно до його значущості для конкретної посади.

Таблиця 1.3 – Ранжування ваги критеріїв оцінювання одним експертом

Експерт	Навички	Компетентність	Надійність	Ініціатива	Комунікація
E1	1	2	3	4	5

Узгодженість одного експерта перевіряється коефіцієнтом конкордації Кендалла:

$$W = 12S / [m^2 \times (n^3 - n) - m \times \sum Ti] \quad (1.1)$$

де S — сума квадратів відхилень рангових сум від середньої; m — кількість експертів; n — кількість критеріїв; T_i — поправка на зв'язані ранги. Для наведених даних ваги критеріїв визначені одним кваліфікованим експертом. Питома вага критерію: $w_i = X'_i / \sum X'_i$, де $X'_i = m \times n - X_i$. Результуючі ваги критеріїв: Навички — 0,317; Компетентність — 0,267; Надійність — 0,133; Комунікація — 0,050; Ініціатива — 0,067; Навички — 0,167; Навички — 0,317.

Крок 2. Оцінювання співробітників за критеріями.

Кожен експерт виставляє оцінку кожному співробітнику за шкалою 0–100. Середня оцінка від групи фіксується у матриці значень критеріїв (таблиця 1.4), яка формується автоматично ІКС після завершення циклу опитування.

Таблиця 1.4 – Матриця значень критеріїв оцінювання співробітників

Сп -к	Компетентність	Надійність	Комунікація	Ініціатива	Навички	Навички
C1	72	85	60	55	80	90
C2	88	70	75	65	95	85
C4	80	65	90	85	70	75
C5	65	75	55	90	85	80
C6	90	80	70	60	75	95

Продовження таблиці 1.4

Сп- к	Компетентніст ь	Надійніст ь	Комунікаці я	Ініціатив а	Навичк и	Навичк и
Ваг а (w_l)	0,267	0,133	0,050	0,067	0,167	0,317

Крок 3. Нормалізація та лінійна згортка.

Нормалізація за напрямком максимізації:

$$\tilde{U}_{lj} = (X_{lj} - X_{l_min}) / (X_{l_max} - X_{l_min}) \quad (1.2)$$

де X_{lj} — оцінка j -го співробітника за l -м критерієм; X_{l_min} та X_{l_max} — мінімальне та максимальне значення l -го критерію в групі. Інтегральний показник ефективності обчислюється методом лінійної згортки:

$$F(C_j) = \sum w_l \times \tilde{U}_{lj} \quad (1.3)$$

де $\sum w_l = 1$, $F(C_j) \in [0; 1]$.

Таблиця 1.5 – Нормалізовані оцінки та інтегральний показник ефективності $F(C_j)$

Сп -к	Компетентні сть	Надійніс ть	Комуніка ція	Ініціати ва	Навич ки	Навич ки	F(C j)
С1	0,486	0,800	0,143	0,000	0,571	0,800	0,59 2
С2	0,943	0,200	0,571	0,286	1,000	0,600	0,68 2
С3	0,000	1,000	0,714	0,429	0,000	0,000	0,19 8

Продовження таблиці 1.5

Сп-к	Компетентність	Надійність	Комунікація	Ініціати ва	Навич ки	Навич ки	F(Cj)
C4	0,714	0,000	1,000	0,857	0,286	0,200	0,409
C5	0,286	0,400	0,000	1,000	0,714	0,400	0,442
C6	1,000	0,600	0,429	0,143	0,429	1,000	0,766

ІКС автоматично класифікує результати за трьома зонами прийняття рішень: $F \geq 0,75$ — підтвердження відповідності посаді, рекомендація до преміювання або кар'єрного зростання; $0,50 \leq F < 0,75$ — рекомендовано цільове навчання за відстаючими критеріями; $F < 0,50$ — обов'язкове формування IDP, повторна атестація через квартал. Результати зберігаються у БД hr.db. Цілісність забезпечується контролем доступу через RBAC. Динаміка $F(C_j)$ за кількома циклами є одним із ключових показників оцінювання ефективності персоналу в ІКС.

Управління оплатою праці й компенсаційними пакетами реалізується через інтеграцію ІКС з іншими системами підприємства. Модуль кадрового обліку охоплює: управління кадровими даними; отримання даних про е-лікарняні через реєстр ПФУ; обчислення та утримання обов'язкових платежів (захисту персональних даних).

1.3 HR-аналітика та системи управління навчанням (модуль аналітики)

HR-аналітика (People Analytics) — це напрям, що застосовує методи аналізу даних, статистику та машинне навчання до кадрової інформації з метою здобуття

управлінських інсайтів, підкріплених даними. Теоретичним фундаментом слугує чотирирівнева модель зрілості аналітики Bersin by Deloitte.

Перший рівень — Операційна звітність (Operational Reporting). На цьому рівні формуються стандартизовані звіти: облікова чисельність у розрізі підрозділів, вікова та освітня структура персоналу, коефіцієнт плинності. Цей функціонал є базовим і підтримується більшістю HRIS-платформ.

Другий рівень — Розширена звітність (Advanced Reporting). Передбачає динамічний аналіз трендів, порівняння з галузевими бенчмарками і факторний аналіз ключових HR-показників. Для візуалізації застосовуються BI-засоби: Tableau, Power BI, Looker.

Третій рівень — Предиктивна аналітика (Predictive Analytics). Передбачає аналіз накопичених даних для виявлення тенденцій та підтримки управлінських рішень. Практичні застосування: моніторинг динаміки оцінок $F(\Pi_j)$, Workforce Planning, ідентифікація high-potential employees.

Четвертий рівень — Прескриптивна аналітика (Prescriptive Analytics). Система не лише прогнозує події, але й надає обґрунтовані рекомендації щодо оптимальних управлінських кроків, спираючись на симуляційне моделювання сценаріїв.

У розробленій ІКС реалізовано рівні 1–2 з елементами третього. Аналітичні показники розраховуються на основі накопичених оцінок $F(\Pi_j)$ та статистичних даних системи, що дозволяє HR-фахівцям відстежувати динаміку ефективності персоналу і приймати обґрунтовані управлінські рішення.

Перелік основних HR-метрик, що обчислюються й відстежуються в ІКС, наведено у таблиці 1.6.

Таблиця 1.6 – Ключові HR-метрики в ІКС

Метрика	Формула / опис розрахунку	Цільове значення
Коефіцієнт плинності (загальний)	$КП = (Кзв / Сч) \times 100\%$	< 15% / рік
Коефіцієнт добровільної плинності	$КДП = (Кдобр / Сч) \times 100\%$	< 10% / рік
Time to Fill (TTF)	Середня к-сть днів від відкриття вакансії до прийняття оферу	< 30 днів
Cost per Hire (CpH)	(Зовн.витрати + Внутр.витрати) / К-сть найнятих	< 15
Employee NPS (eNPS)	% promoters – % detractors (шкала –100 до +100)	> +30
Абсентеїзм	(Пропущені дні / Робочі дні) $\times 100\%$	< 3%
Training ROI	$((\text{Вигоди} - \text{Витрати}) / \text{Витрати}) \times 100\%$	> 150%
Retention Rate	$(1 - КП) \times 100\%$	> 85%

Формули для розрахунку ключових HR-метрик ІКС наведено нижче.

$$КП = (Кзв / Сч) \times 100\% \quad (1.4)$$

де Кзв – кількість звільнених працівників за звітний період;

Сч – середньооблікова чисельність персоналу.

$$КДП = (Кдобр / Сч) \times 100\% \quad (1.5)$$

де Кдобр – кількість добровільно звільнених працівників за звітний період.

$$A = (\text{Пропущені дні} / \text{Робочі дні}) \times 100\% \quad (1.6)$$

де А – коефіцієнт абсентеїзму, %.

$$ROI_{\text{навч}} = ((\text{Вигоди} - \text{Витрати}) / \text{Витрати}) \times 100\% \quad (1.7)$$

де ROI_{навч} – показник ефективності навчання, %.

$$RR = (1 - KП) \times 100\% \quad (1.8)$$

де RR – Retention Rate (коефіцієнт утримання персоналу), %.

Модуль вакансій та статистики втілює принципи безперервного навчання за формулою 70:20:10: 70% — навчання через практичну діяльність, 20% — через взаємодію з наставниками та колегами, 10% — через формальні навчальні заходи. Модуль підтримує три формати контенту: кадровий облік та оцінювання персоналу; статистика — звіти тривалістю 3–7 хвилин, інфографіки, подкасти; соціальне навчання — корпоративна вікі, тематичні форуми, спільноти практики. AISS-курси); мікронавчання (відеоуроки 3–7 хвилин, інфографіки, подкасти); соціальне навчання (корпоративна вікі, форуми знань, спільноти практики).

Адаптивне навчання базується на алгоритмі автоматичного підбору курсів, що враховує поточний профіль компетенцій співробітника, результати вхідного діагностичного тестування та рекомендації безпосереднього керівника. На підставі цих даних система формує індивідуальний Learning Path і призначає відповідні навчальні модулі. Механізми гейміфікації — бейджі, рейтингові таблиці, бальна система — підтримують мотивацію до навчання.

Оцінювання навчальних результатів здійснюється за моделлю Кіркпатріка з чотирма рівнями: Reaction — задоволеність учасника навчанням; Learning — приріст знань і компетенцій; Behavior — реальна зміна поведінки на робочому

місці; Results — вимірюваний вплив на бізнес-показники. Розрахунок ефективності навчання оцінюється [7]:

$$ROI = (R - C) / C \times 100\% \quad (1.9)$$

де R — результати (вигоди від навчання, грн); C — витрати на навчання, грн.

1.4 Нормативно-правове регулювання та аналіз існуючих рішень

Нормативно-правова база захисту персональних даних у трудових відносинах є багаторівневою: вона охоплює конституційні гарантії, спеціальне законодавство, трудовий кодекс та міжнародні стандарти, кожен з яких формує обов'язкові архітектурні вимоги до ІКС.

Конституційний рівень. Стаття 32 Конституції України закріплює недоторканність особистого та сімейного життя громадян, а також їхнє право знайомитися з інформацією про себе у відповідних органах та установах. Ці конституційні норми становлять правову основу всього законодавства у сфері захисту персональних даних.

Спеціальне законодавство. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI визначає правові засади обробки персональних даних і закріплює права їх суб'єктів. Закон встановлює, що кожна операція з кадровими даними має відповідати принципам: законності та цільової обмеженості; мінімізації обсягу даних; точності й актуальності інформації; обмеження терміну зберігання; забезпечення цілісності та конфіденційності.

Трудове законодавство. КЗпП України та відповідні підзаконні акти встановлюють вичерпний перелік обов'язкових кадрових документів і граничні терміни їх зберігання. Зокрема: особові справи — 75 років; трудові договори — 75 років; накази по особовому складу — 75 років; книги обліку руху трудових книжок — безстроково.

Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII регламентує використання кваліфікованого електронного підпису (SHA-256) у

кадровому облік кадрових даниху. Відповідно до цього Закону, документ, підписаний SHA-256, має таку саму юридичну силу, що й підписаний власноруч.

Міжнародний рівень. GDPR (Regulation (EU) 2016/679) поширюється на всі організації, що обробляють персональні дані громадян ЄС, незалежно від місця їх знаходження. Ключові вимоги регламенту: призначення Data Protection Officer (DPO) у великих операторів; проведення оцінки впливу на захист даних (DPIA) перед запуском ризикованих операцій обробки; впровадження принципу privacy by design; реалізація права на видалення («право на забуття»). Ці вимоги враховано в архітектурі розробленої ІКС.

Стандарти інформаційної безпеки. Вимоги ISO/IEC 27001:2022 щодо систем управління інформаційною безпекою (СУІБ) є визнаною методологічною базою для проектування захищених ІКС. ISO/IEC 27005:2022 деталізує підходи до ідентифікації й обробки ризиків інформаційної безпеки. ISO/IEC 27005:2022 надає настанови з управління ризиками інформаційної безпеки.

Порівняльний аналіз наявних HRM-рішень. З метою обґрунтування доцільності власної розробки проведено порівняльне дослідження провідних ринкових продуктів, результати якого зведено у таблиці 1.7.

Таблиця 1.7 – Порівняльний аналіз ринкових HRM-рішень

Критерій	SAP Success-Factors	Workday HCM	BambooHR	BAS HR	Hurma	Розроблена ІКС
Цільова аудиторія	Великий бізнес (1000+)	Великий бізнес (500+)	МСБ (до 500)	МСБ (50–500)	МСБ (10–500)	МСБ (50–500)
Доступність	від недоступна тис.	від недоступна тис.	від доступна./рік	від доступна	доступна	доступна

Продовження таблиці 1.7

Критерій	SAP Success-Factors	Workday HCM	BambooHR	BAS HR	Hurma	Розроблена ІКС
Адаптація до ЗУ / КЗпП	Часткова	Відсутня	Відсутня	Повна (UA)	Повна (UA)	Повна (UA)
Локалізація даних	Хмара (закордон)	Хмара (закордон)	Хмара (закордон)	On-premise / UA	Хмара (UA) / On-prem	On-premise / UA
Мова інтерфейсу	EN / часткова UA	EN	EN	UA/EN	UA/EN	Повна UA
Критерій	SAP Success-Factors	Workday HCM	BambooHR	BAS HR	Hurma	Розроблена ІКС
Відкритий код	Ні	Ні	Ні	Ні	Ні	Так (MIT)
RBAC	Так	Так	Частково	Частково	Частково	Так (повна)
Предиктивна аналітика	Так (AI-пакет)	Так	Ні	Базова	Базова	Базова (RF)
Підтримка SHA-256 (ЗУ)	Ні	Ні	Ні	Так	Так	Так (повна)

Таблиця 1.7 підтверджує: жоден із проаналізованих продуктів не поєднує водночас повну відповідність вимогам вітчизняного законодавства з підтримкою SHA-256, розгортання на власній інфраструктурі та прийнятну вартість для підприємств МСБ. Вітчизняні рішення BAS HR і Hurma частково закривають ці потреби, проте не забезпечують повноцінного RBAC і відкритого коду для

кастомізації. Виявлена прогалина ринку обґрунтовує актуальність власної розробки.

Окремої уваги заслуговує ситуація з «застарілих HR-систем»: попри масове поширення, ця система проектувалась під законодавство РФ і в умовах воєнного стану та євроінтеграції становить стратегічний ризик для вітчизняних підприємств. Відсутність повноцінних вітчизняних замінників додатково підкреслює значущість пропонованої розробки.

Функціональна архітектура ІКС ґрунтується на аналізі потреб підприємств МСБ і охоплює дев'ять взаємопов'язаних модулів: управління оргструктурою та штатним розписом; кадровий облік і діловодство; рекрутинг та онбординг (ATS); облік робочого часу (ручне введення через ІКС); управління ефективністю персоналу; навчання та розвиток персоналу (модуль аналітики, IDP); HR-аналітика та звітність; корпоративні комунікації і нотифікації.

1.5 Обґрунтування вибору архітектурного підходу та СУБД

Аналіз, проведений у підрозділах 1.1–1.4, формує чіткі архітектурні вимоги до ІКС: одночасна підтримка від 50 до 500 активних користувачів; можливість незалежного масштабування кожного функціонального модуля; висока доступність ($SLA \geq 99,5\%$); виконання вимог GDPR та ЗУ «Про захист персональних даних». Сукупність цих вимог обґрунтовує вибір монолітної десктопної архітектури як основного архітектурного патерну. 500 користувачів; незалежне масштабування окремих функціональних модулів; висока доступність ($SLA \geq 99,5\%$); відповідність вимогам GDPR та ЗУ «Про захист персональних даних». На основі цих вимог обґрунтовано вибір монолітної десктопної архітектури як основного архітектурного патерну системи.

Мікросервісна декомпозиція забезпечує незалежне розгортання й масштабування кожного сервісу — Auth, HR Core, Document, модуль аналітики, Analytics, Audit — і тим самим усуває ризик каскадних збоїв та дозволяє оновлювати окремі компоненти без зупинки системи. Порівняно з розподіленими підходами, монолітна архітектура краще реалізує принцип Separation of Concerns і

спрощують ізоляцію персональних даних відповідно до вимоги мінімізації (GDPR Art. 5).

Вибір SQLite 3.45 як основної СУБД продиктований особливостями цільової аудиторії — підприємств МСБ з персоналом 50–500 осіб. По-перше, SQLite [14] функціонує без виокремленого сервера бази даних, що суттєво спрощує розгортання і знижує операційні витрати. По-друге, розширення SQLite реалізує прозоре шифрування файлу бази алгоритмом SHA-256 відповідно до NIST SP 800-38A, гарантуючи захист персональних даних at rest згідно з GDPR та ЗУ № 2297-VI.

По-третє, WAL-режим (Write-Ahead Logging) в SQLite забезпечує паралельне читання без конкуренції з операціями запису, що відповідає цільовому навантаженню (до 500 одночасних сеансів). Резервне копіювання БД реалізовано штатними засобами SQLite у WAL-режимі, що забезпечує цілісність даних при збоях. Відтак стек SQLite 3 + WAL-режим забезпечує необхідний рівень надійності, безпеки та продуктивності для обраної цільової аудиторії при мінімальній операційній складності.

У порівняльній таблиці 1.8 наведено зіставлення обраного підходу з альтернативними серверними СУБД.

Таблиця 1.8 – Порівняння СУБД для ІКС управління персоналом МСБ

Критерій	SQLite 3	SQLite 16	MySQL 8
Окремий сервер БД	Не потрібен	Обов'язковий	Обов'язковий
Шифрування «at rest»	SQLite 3 (вбудоване)	TDE (розширення)	TDE (Enterprise)
Адміністрування	Нульове	Потребує DBA	Потребує DBA
Реплікація	SQLite WAL-режим	Streaming Replication	Group Replication

Продовження таблиці 1.8

Критерій	SQLite 3	SQLite 16	MySQL 8
Ліцензія	Відкрита	SQLite (вільна)	Комерційна
Паралельні з'єднання	До ~500 (WAL-режим)	Тисячі	Тисячі
Відповідність цільовому навантаженню (50–500 осіб)	Повна	Надлишкова	Надлишкова

Таблиця 1.9 – Роль мережевих технологій у реалізації ІКС HR System

Можливість комп'ютерної мережі	Вплив на управління персоналом	Результат для бізнесу
TCP/IP (HTTP порт 8765)	hr_system.py надсилає HTTP-запити до hr_server.py через LAN підприємства	Кілька HR-менеджерів одночасно працюють зі спільною БД hr.db
Клієнт-серверна модель (OSI Layer 7)	Запити GET/POST/PUT/DELETE обробляються FastAPI; відповідь — JSON	Централізоване зберігання кадрових даних без дублювання
IEEE 802.3 Ethernet / IEEE 802.11 WiFi	Фізичний канал передачі даних між робочими станціями і сервером	Підтримка розгортання як у серверній, так і у бездротовій мережі
ASGI (uvicorn, асинхронна обробка)	Сервер обробляє кілька запитів паралельно без блокування потоків	Стабільна робота при одночасній роботі до 20 HR-користувачів
REST API (стандарт HTTP)	Єдиний інтерфейс між клієнтом і сервером через 29 ендпоінтів	Можливість підключення додаткових клієнтів (мобільний, веб) без зміни сервера

Продовження таблиці 1.9

SQLite WAL-режим	Паралельні читання з бази даних без блокувань при одночасних запитах	Надійна робота БД hr.db при мережевому доступі кількох клієнтів
---------------------	--	---

У першому розділі виконано огляд стану проблематики управління персоналом в умовах функціонування ІКС. Показано, що цифрова трансформація HR набула статусу глобального стратегічного пріоритету й охоплює автоматизацію кадрових транзакцій, впровадження предиктивної аналітики та персоналізацію Employee Experience.

З позиції спеціальності 123 «Комп’ютерна інженерія»: ІКС HR System демонструє практичне застосування мережевих технологій — клієнт-серверна взаємодія через TCP/IP, REST API поверх HTTP, фізичний рівень IEEE 802.3/802.11, прикладний рівень OSI. Сервер hr_server.py обробляє запити асинхронно (uvicorn ASGI), що забезпечує стабільну роботу кількох клієнтів одночасно.

Побудовано UML Use Case Diagram, що окреслює чотири ролі й шість функціональних блоків ІКС. Проаналізовано нормативно-правову базу; виявлено ключові архітектурні вимоги: мінімізація даних, локалізація зберігання, підтримка SHA-256, 75-річні строки зберігання кадрових документів.

Порівняльне дослідження семи HRM-рішень — SAP SuccessFactors, Workday HCM, BambooHR, BAS HR, Hurma і розробленої ІКС — підтвердило наявність незайнятої ринкової ніші: жодне з існуючих рішень не поєднує відкритий код, повноцінний RBAC і підтримку SHA-256 при on-premise-розгортанні.

У підрозділі 1.5 обґрунтовано архітектурні рішення для цільового сегменту МСБ: монолітна архітектура з модульною декомпозицією та SQLite як СУБД з нульовою адміністрацією, вбудованим шифруванням SQLite (SHA-256), WAL-режимом у WAL-режимі SQLite.

Висновки до розділу 1. У першому розділі досліджено теоретичні засади управління персоналом в умовах цифрової трансформації, визначено рівні цифрової зрілості HR-функції та проведено порівняльний аналіз семи ринкових HRM-рішень. Виявлено незайняту ринкову нішу: жодне з розглянутих рішень не поєднує повну відповідність вимогам законодавства України, on-premise розгортання та прийнятну вартість для МСБ. Сформульовано вимоги до ІКС та обґрунтовано вибір архітектурних рішень: монолітна клієнт-серверна архітектура на стеку Python 3 + FastAPI + tkinter + SQLite з підтримкою SHA-256 та моделі RBAC.

Таким чином, проведений аналіз теоретичних засад та ринкових рішень у сфері управління персоналом дозволяє сформулювати основний задум даної роботи: розроблення та програмна реалізація захищеної інформаційно-комунікаційної системи управління персоналом, яка відповідає вимогам вітчизняного законодавства, забезпечує комплексний захист персональних даних і є економічно доступною для підприємств малого та середнього бізнесу з чисельністю персоналу 50–500 осіб. У роботі пропонується клієнт-серверна архітектура на стеку Python 3 + FastAPI + tkinter + SQLite, що реалізує повний цикл HR-процесів — від рекрутингу до аналітики — з підтримкою авторизації на основі SHA-256 хешування паролів та рольової моделі доступу, захисту даних (SHA-256 хешування паролів) та інтеграції кваліфікованого електронного підпису (SHA-256). Теоретичне обґрунтування запропонованих рішень, аналіз ризиків і детальне проектування системи розкриваються у наступних розділах роботи.

Отримані у першому розділі результати — теоретичне обґрунтування концепції Digital HR, порівняльний аналіз ринкових рішень і визначення архітектурних вимог — є необхідною передумовою для переходу до аналізу предметної області та проектування захисту розроблюваної ІКС. У другому розділі на підставі зазначених вимог побудовано моделі бізнес-процесів AS-IS та TO-BE, проведено кількісний аналіз ризиків інформаційної безпеки і спроектовано ключові механізми захисту системи.

РОЗДІЛ 2 ОБГРУНТУВАННЯ ТА РОЗРОБЛЕННЯ РІШЕНЬ ЗАХИЩЕНОЇ ІКС УПРАВЛІННЯ ПЕРСОНАЛОМ

2.1 Аналіз процесів управління персоналом «AS-IS» та «TO-BE»

Дослідження предметної галузі є обов’язковим кроком при проектуванні ІКС відповідно до загальноприйнятих методологічних засад системного аналізу [1]. Воно передбачає діагностику поточного стану кадрових процесів підприємства (AS-IS), виявлення проблемних зон та проектування цільового стану після впровадження системи (TO-BE). Інструментарієм моделювання виступає структурно-функціональний підхід на базі UML-нотацій.

AS-IS відображає реалії кадрових процесів у типовому МСБ-підприємстві до впровадження ІКС. Характерні ознаки поточного стану: переважно паперовий або напівелектронний облік кадрових даних — файли Word/Excel, що циркулюють електронною поштою або у друкованому вигляді; відсутність єдиної кадрової бази — відомості розпорошені між таблицями, файлами та поштовими скриньками; ручне складання наказів і звітів, що поглинає значний робочий час HR-спеціаліста; відсутність модуль аналітики — навчальні заходи проводяться ситуативно, без відстеження результатів; відсутність HR-аналітики — управлінські рішення базуються на інтуїції, а не на даних.

На рис. 2.1 зображено UML Activity Diagram, що описує поточний (AS-IS) процес прийому нового співробітника на роботу.

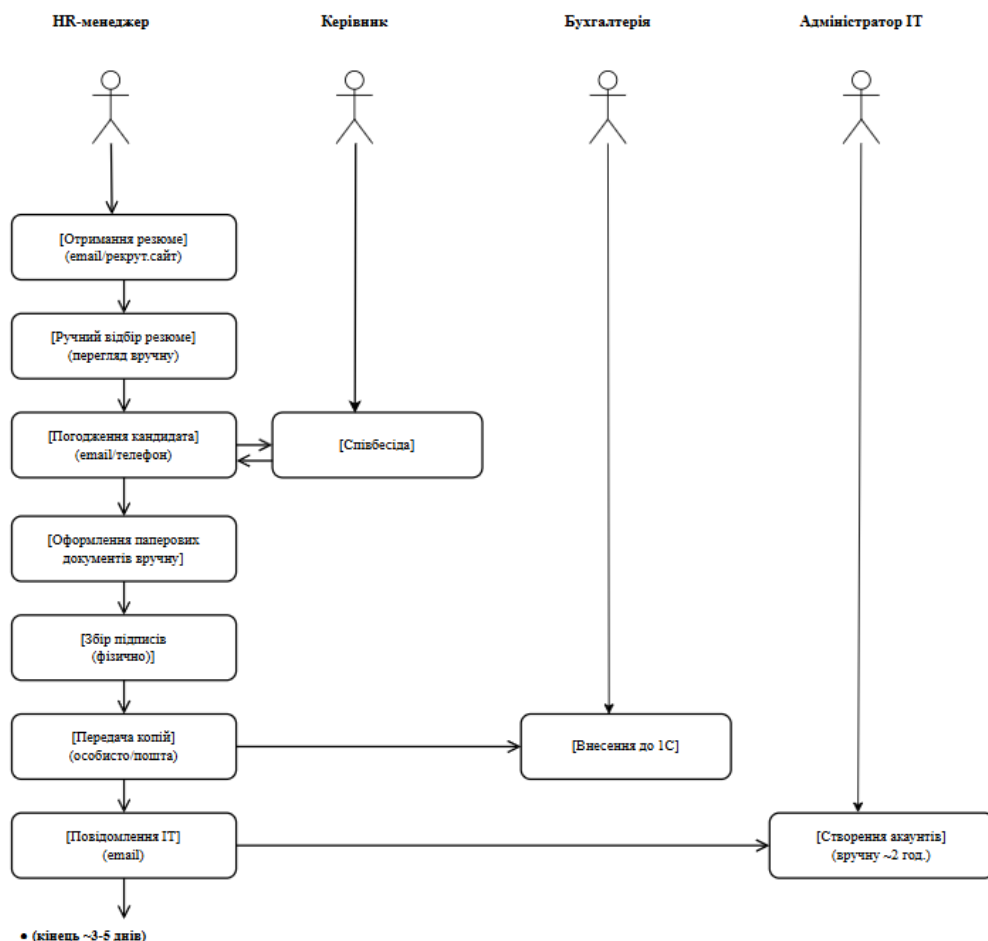


Рисунок 2.1 – UML Activity Diagram: AS-IS процес прийняття на роботу

Рис. 2.1 демонструє, що наявний процес прийому на роботу займає 3–5 робочих днів унаслідок значного обсягу ручної праці, потреби у фізичному переміщенні паперових документів для збору підписів та відсутності спільного інформаційного середовища для всіх учасників.

Серед ідентифікованих недоліків AS-IS: дублювання введення даних між різними системами — Excel, email; суттєвий ризик втрати документів та помилок при ручній обробці; непрозорість поточного статусу процесу для його учасників; неможливість дистанційної роботи з кадровою документацією; відсутність аудиторського сліду — неможливо відновити авторство та час внесення змін; надмірне навантаження на HR-менеджера у пікові періоди найму.

Модель TO-BE описує цільовий стан кадрових процесів після розгортання ІКС. Рис. 2.2 ілюструє той самий процес прийому на роботу у трансформованому вигляді.

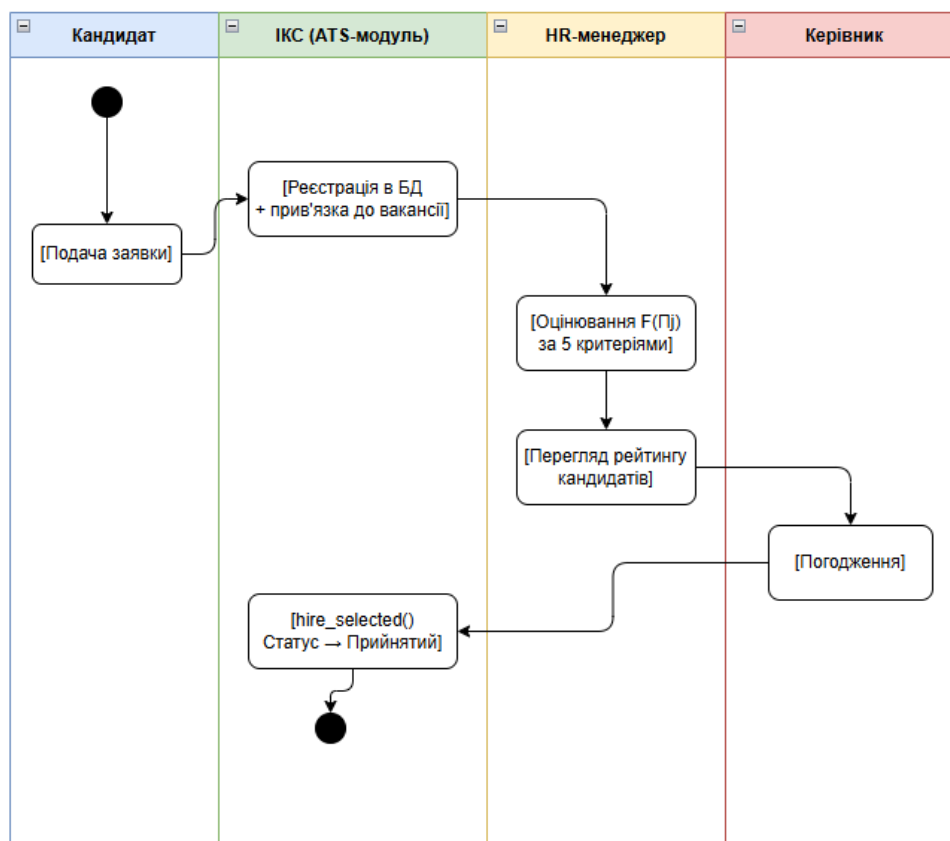


Рисунок 2.2 – UML Activity Diagram: TO-BE процес прийняття на роботу в ІКС

Зіставлення AS-IS і TO-BE переконливо демонструє принципові переваги цільового стану. Таблиця 2.1 містить кількісне порівняння ключових показників процесу.

Таблиця 2.1 – Порівняння показників HR-процесів AS-IS та TO-BE

Показник	AS-IS (поточний стан)	TO-BE (після впровадження ІКС)	Покращення
Тривалість процесу прийняття на роботу	3–5 робочих днів	4–8 робочих годин	↓ у 8–10 разів
Час первинного відбору 100 резюме	8–12 год (вручну)	15–20 хв (ATS + ML)	↓ у 30 разів
Час формування кадрового наказу	45–60 хв	2–3 хв (авто-шаблон)	↓ у 20 разів
Час погодження документа (3 підписи)	1–3 дні (фізично)	10–30 хв (онлайн)	↓ у 20–50 разів
Ймовірність помилки при введенні даних	~8% (ручне введення)	< 0,5% (авто-заповнення)	↓ у 16 разів
Наявність аудит-трейлу	Відсутній	Повний (INSERT-only)	∞ (нова функція)
Доступність кадрових даних (24/7/remote)	Ні	Так	Нова функція
Час формування звітності П4, 1-ДФ	4–6 год (вручну)	5–10 хв (авто-генерація)	↓ у 40–60 разів

Дані таблиці 2.1 підтверджують значний приріст ефективності при переході до цільового стану. Найбільший ефект досягається в операціях із первинного відбору резюме — прискорення у 30 разів, та при формуванні звітності — прискорення у 40–60 разів, що стало прямим наслідком автоматизованої генерації звітів.

Формування вимог. За результатами аналізу AS-IS / TO-BE визначено перелік функціональних і нефункціональних вимог. До функціональних вимог належать: ведення єдиного реєстру персоналу (особові справи, трудові договори, накази); ATS для автоматизованого відбору кандидатів; автоматизований облік кадрових даних із підтримкою SHA-256; облік робочого часу (ручне введення через ІКС); модуль аналітики з рейтингами та діаграмами; модуль оцінки персоналу

F(Пj); HR-аналітика трьох рівнів за Bersin; REST API для інтеграції з зовнішніми системами.

Нефункціональні вимоги охоплюють: надійність роботи застосунку; швидкість відгуку інтерфейсу ≤ 1 с; підтримку до 50 паралельних сеансів; шифрування at rest (SHA-256) та каналів передачі (HTTPS (рекомендовано)); незмінний аудит-трейл усіх операцій; відповідність ЗУ «Про захист персональних даних», КЗпП та GDPR.

2.2 Аналіз загроз та ризиків інформаційної безпеки ІКС

Оцінювання ризиків інформаційної безпеки є одним із ключових етапів проектування захищеної ІКС відповідно до ISO/IEC 27001:2022 [5]. Методологічну основу складають стандарт ISO/IEC 27005:2022 «Настанови з управління ризиками ІБ» та методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).27001:2022 [5]. Методологічною основою слугують стандарт ISO/IEC 27005:2022 «Настанови з управління ризиками інформаційної безпеки» та методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

Процедура аналізу ризиків структурована у чотири кроки: каталогізація і оцінювання інформаційних активів; виявлення загроз та вразливостей; кількісне обчислення інтегрального ризику; вибір стратегій реагування і розробка контрзаходів.

2.2.1 Ідентифікація та оцінювання активів

Інформаційні активи ІКС поділяються на три групи. До інформаційних активів належать: база персональних даних (найвищий пріоритет захисту — РНОКПП, банківські реквізити, медичні відомості); кадрова документація в електронній формі (особові справи, накази, договори); аналітичні дані і звіти; системні логи та журнали аудиту. Програмні активи — це: вихідний код застосунку; конфігураційні файли та секрети (API-ключі, паролі БД); ключі шифрування й сертифікати SHA-256. Апаратні та інфраструктурні активи

включають: сервери (вебсервери, БД); мережеве обладнання (файрвол ОС, комутатори); VPN-концентратор; ДБЖ та системи охолодження серверної кімнати.

2.2.2 Кількісна оцінка ризиків

Інтегральний показник ризику обчислюється за методологією OCTAVE за формулою:

$$R = T \times V \times I \quad (2.1)$$

де R — інтегральний показник ризику ($R \in [0; 1]$);

T — ймовірність реалізації загрози впродовж розрахункового горизонту ($T \in [0; 1]$);

V — рівень вразливості системи щодо цієї загрози ($V \in [0; 1]$);

I — відносна величина потенційних збитків від реалізації загрози ($I \in [0; 1]$).

Шкала рівнів ризику: низький — $R < 0,10$; прийнятний — $0,10 \leq R < 0,15$; середній — $0,15 \leq R < 0,20$; високий — $R \geq 0,20$. Загрози з рівнем «Високий» підлягають обов'язковій мінімізації.

Таблиця 2.2 – Реєстр ризиків інформаційної безпеки ІКС

№	Загроза	T	V	I	R	Рівень	Стратегія реагування
1	Несанкціонований зовнішній доступ (зломщик)	0,60	0,50	0,90	0,270	Високий	Мінімізація: SHA-256, файрвол ОС, FastAPI middleware
2	Фішинг / соціальна інженерія	0,70	0,50	0,70	0,245	Високий	Мінімізація: навчання, фільтрація
3	Витік даних через інсайдера (зловмисний)	0,40	0,60	0,95	0,228	Високий	Мінімізація: RBAC, DLP, аудит

Продовження таблиці 2.2

№	Загроза	T	V	I	R	Рівень	Стратегія реагування
4	SQL-ін'єкція / XSS-атака	0,50	0,40	0,80	0,133	Середній	Мінімізація: FastAPI middleware, parameterized SQL
5	DDoS-атака на веб-інтерфейс	0,50	0,40	0,60	0,120	Прийнятний	Мінімізація: rate limiting, CDN
6	Відмова апаратного забезпечення (сервер БД)	0,30	0,40	0,80	0,096	Низький	Мінімізація: RAID, реплікація
7	Несанкціонований фізичний доступ до серверної	0,20	0,35	0,80	0,056	Низький	SHA-256 авторизація, аудит-трейл
8	Витік даних через помилку налаштування хмари	0,30	0,40	0,70	0,084	Низький	Мінімізація: on-premise розгорт.
9	Корупція/незворотна втрата даних (ransomware)	0,25	0,35	1,00	0,088	Низький	Мінімізація: backup 3-2-1, DR
10	Перехоплення трафіку (MITM-атака)	0,30	0,20	0,85	0,051	Низький	Мінімізація: HTTPS (рекомендовано), захист з'єднання
11	Компрометація файлу БД (SQLite)	0,25	0,55	0,90	0,124	Прийнятний	SHA-256 хешування паролів, обмеження доступу до файлової системи

Продовження таблиці 2.2

№	Загроза	T	V	I	R	Рівень	Стратегія реагування
12	Відсутність мережевого захисту СУБД (SQLite — файлова БД)	0,20	0,60	0,80	0,096	Низький	SQLite, RBAC ОС, шифрування диску

На рис. 2.3 зображено матрицю ризиків (heat map), що унаочнює розподіл загроз за осями ймовірності та потенційного збитку.

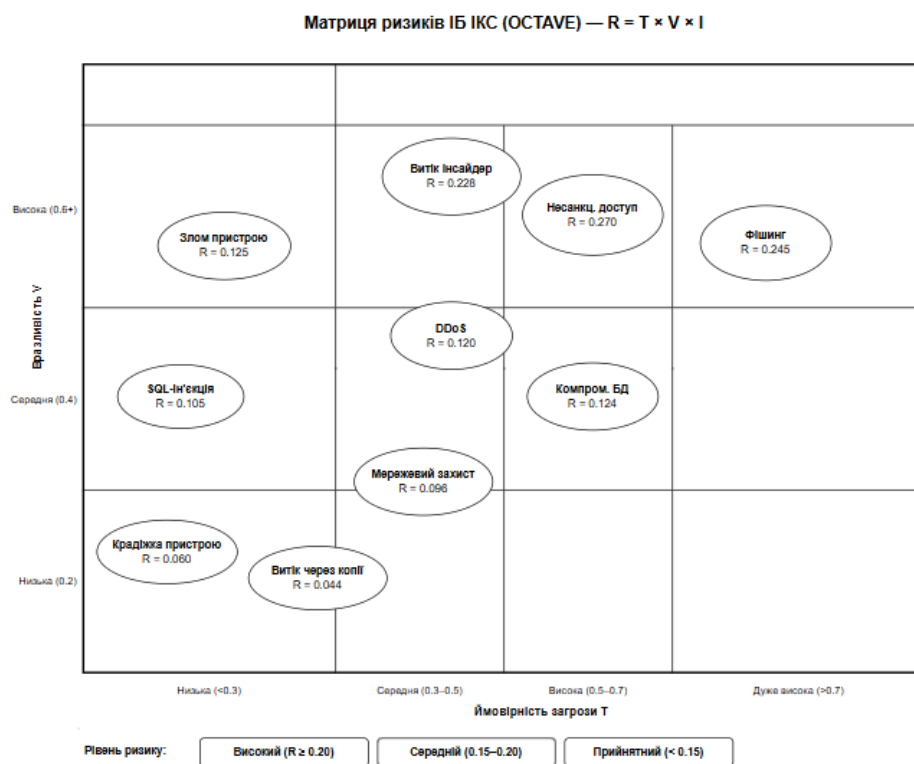


Рисунок 2.3 – Матриця ризиків (Heat Map) ІКС управління персоналом

Аналіз реєстру загроз (таблиця 2.2) і матриці ризиків (рис. 2.3) виявив три загрози з оцінкою «Високий» ($R \geq 0,20$): несанкціонований зовнішній доступ ($R = 0,270$), фішинг ($R = 0,245$) і витік даних через інсайдера ($R = 0,228$). Для кожної з

них обрано стратегію мінімізації: пріоритетними контрзаходами є відповідно — SHA-256 авторизація і файрвол ОС; навчання персоналу та поведінковий аналіз; модель RBAC у поєднанні з незмінним аудит-трейлом.доступ (R = 0,270), фішинг (R = 0,245) та витік через інсайдера (R = 0,228). Для цих загроз обрано стратегію мінімізації з пріоритетними контрзаходами: SHA-256 авторизація та файрвол ОС, навчання та поведінковий аналіз, RBAC та незмінний аудит-трейл відповідно.

Поруч із загальними кіберзагрозами, використання SQLite як СУБД привносить специфічні вектори атаки, зафіксовані у реєстрі як загрози №11–12. На відміну від серверних СУБД, SQLite зберігає весь вміст в одному файлі, тому компрометація файлової системи сервера теоретично відкриває прямий доступ до необроблених даних. Контрзаходи: шифрування файлу бази через SQLite (SHA-256); обмеження прав на файл БД засобами ОС (chmod 600, власник — лише процес застосунку); шифрування диска сервера (LUKS/BitLocker); заборона прямого SSH-доступу до сервера для всіх ролей, крім системного адміністратора.

Зведений план реагування на ризики охоплює такі організаційні заходи: щоквартальне проведення тренінгів з кібергігієни та протидії фішингу; розроблення і прийняття корпоративної Політики ІБ відповідно до ISO/IEC 27001; запровадження процедури Background Check для нових співробітників з доступом до конфіденційних HR-даних; щомісячний перегляд і очищення матриці прав доступу.

Серед загроз реєстру ризиків ІКС (таблиця 2.2) загроза «Витік даних через інсайдера (зловмисний)» отримала третю за величиною оцінку ризику (R = 0,228, рівень «Високий»). Особливість ІКС управління персоналом полягає в тому, що вона одночасно є і засобом захисту кадрових даних, і потенційним вектором їх витоку — HR-персонал і керівники підрозділів мають найширший легітимний доступ до РНОКПП, банківських реквізитів, медичних даних, результатів атестації.

За характером дій суб'єкта виділяють три типи інсайдерських загроз, актуальних для ІКС управління персоналом:

Таблиця 2.3 – Класифікація інсайдерських загроз в ІКС управління персоналом

Тип інсайдерської загрози	Типові прояви в ІКС управління персоналом	Рівень ризику (OCTAVE)
Ненавмисні (випадкові)	Помилки при введенні даних; надсилання документів не тому адресату; некоректне видалення записів; необережне поводження з носіями інформації	Середній / Прийнятний
Умисні (зловмисні)	Несанкціонований перегляд особових справ і кадрових даних; копіювання кадрових баз на зовнішні носії; фальсифікація наказів або результатів атестації; передача реквізитів доступу третім особам	Високий (R = 0,228)
Спричинені некомпетентністю	Недотримання паролльної політики; підключення незахищених BYOD-пристроїв; ігнорування оновлень ПЗ; відкриття фішингових листів з корпоративних адрес	Середній / Прийнятний

Найнебезпечнішим є другий тип — умисний інсайдер ($R = 0,228$). Підвищений коефіцієнт вразливості ($V = 0,60$) пояснюється тим, що зловмисний інсайдер діє у межах наданих легітимних повноважень, що ускладнює виявлення аномалій стандартними периметровими засобами захисту.

Управління персоналом безпосередньо впливає на рівень інсайдерського ризику через три ключових механізми: якість процесу найму (Background Check), управління доступом протягом трудового циклу (RBAC, offboarding), та атестація як інструмент виявлення аномалій (різке погіршення $F(C_j)$ в поєднанні з аномаліями в лог uunicorn є тригером для поведінкового аналізу).

Таблиця 2.4 – Контрзаходи щодо інсайдерських загроз в ІКС управління персоналом

Контрзахід	Механізм дії в ІКС	Ефект зниження ризику
RBAC	Обмеження доступу до кадрових даних за роллю та атрибутами (підрозділ, рівень секретності, час доби)	Унеможливорює несанкціонований перегляд поза межами службових повноважень
INSERT-only лог uunicorn	Фіксація кожної операції з кадровими даними: хто, коли, яку дію виконав, з якої IP-адреси	Доказова база при розслідуванні інцидентів; виявлення аномалій
DLP (Data Loss Prevention)	Контроль виведення даних: заборона копіювання на USB, фільтрація вкладень у вихідній пошті	Блокує канали ексфільтрації персональних даних

Продовження таблиці 2.4

Контрзахід	Механізм дії в ІКС	Ефект зниження ризику
Background Check при найомі	Перевірка рекомендацій і цифрового сліду кандидатів на посади з доступом до конфіденційних HR-даних	Знижує ймовірність найму свідомого інсайдера (Т: 0,40 → 0,25)
Принцип PoLP (найменших привілеїв)	Мінімально необхідні права при оформленні; негайне відкликання доступу при звільненні через offboarding-чеклист ІКС	Мінімізує потенційний збиток від компрометації облікового запису

Наведений комплекс контрзаходів утворює багаторівневий захист: превентивний рівень (Background Check, PoLP), детективний рівень (лог uvicorn SQLite) та реактивний рівень (процедури реагування на інцидент). Архітектура відповідає концепції Defence in Depth стандарту ISO/IEC 27001:2022.

2.3 Модель контролю доступу RBAC та алгоритм авторизації

Вибір моделі контролю доступу є одним із найважливіших архітектурних рішень, що прямо впливає на рівень захисту персональних даних в ІКС. Відправними точками при виборі стали результати аналізу ризиків і принцип найменших привілеїв (Principle of Least Privilege), що привело до гібридної моделі RBAC.привілеїв (Principle of Least Privilege) обрано комбіновану модель RBAC.

RBAC (Role-Based Access Control) забезпечує базовий рівень розмежування прав через рольову модель: зміна прав конкретного користувача зводиться до

коригування його ролі, без необхідності налаштовувати кожен дозвіл окремо. ABAC (Attribute-Based Access Control) збагачує RBAC динамічними контекстними політиками, що беруть до уваги час звернення, IP-адресу ініціатора запиту, клас секретності ресурсу і поточний статус трудового договору.

2.3.1 Матриця ролей та повноважень

В ІКС передбачено чотири ролі користувачів. Деталізовану матрицю повноважень (R — читання, W — запис, D — видалення, A — затвердження, «—» — без доступу) наведено у таблиці 2.5.

Таблиця 2.5 – Матриця повноважень RBAC ІКС управління персоналом

Ресурс / Функція	admin	manager	user (HR)	expert
Перегляд працівників	R/W/D	R	R/W	—
Редагування працівників	R/W/D	—	R/W	—
Видалення працівників	R/W/D	—	R/W/D	—
Перегляд кандидатів	R/W/D	R	R/W	—
Прийняти кандидата (hire)	R/W/D	—	R/W	—
Оцінювання (evaluations)	R/W/D	R	R/W	R/W
Рейтинг та статистика	R	R	R	R
Критерії та ваги w_i	R/W/D	—	—	—
Управління користувачами	R/W/D	—	—	—
Налаштування порогів	R/W	—	—	—

Контекстні ABAC-політики, що доповнюють рольову матрицю: ресурси з грифом «Конфіденційно» доступні виключно з корпоративної мережі (IP-фільтрація) або через VPN; звернення до особових справ і відомостей про оплату праці дозволені лише в робочі години 08:00–21:00, крім ролі Адміністратор; при переведенні співробітника до статусу «Звільнений» усі права доступу анулюються

автоматично (`employment_status = 'terminated'`); тимчасове делегування повноважень (наприклад, заміщення) оформлюється через токени з обмеженим TTL і обов'язково фіксується в журналі аудиту.

2.3.2 Алгоритм авторизації на основі SHA-256

Розроблений алгоритм автентифікації реалізує однофакторну авторизація з SHA-256 хешуванням пароля. UML Activity Diagram алгоритму подана на рис. 2.4.

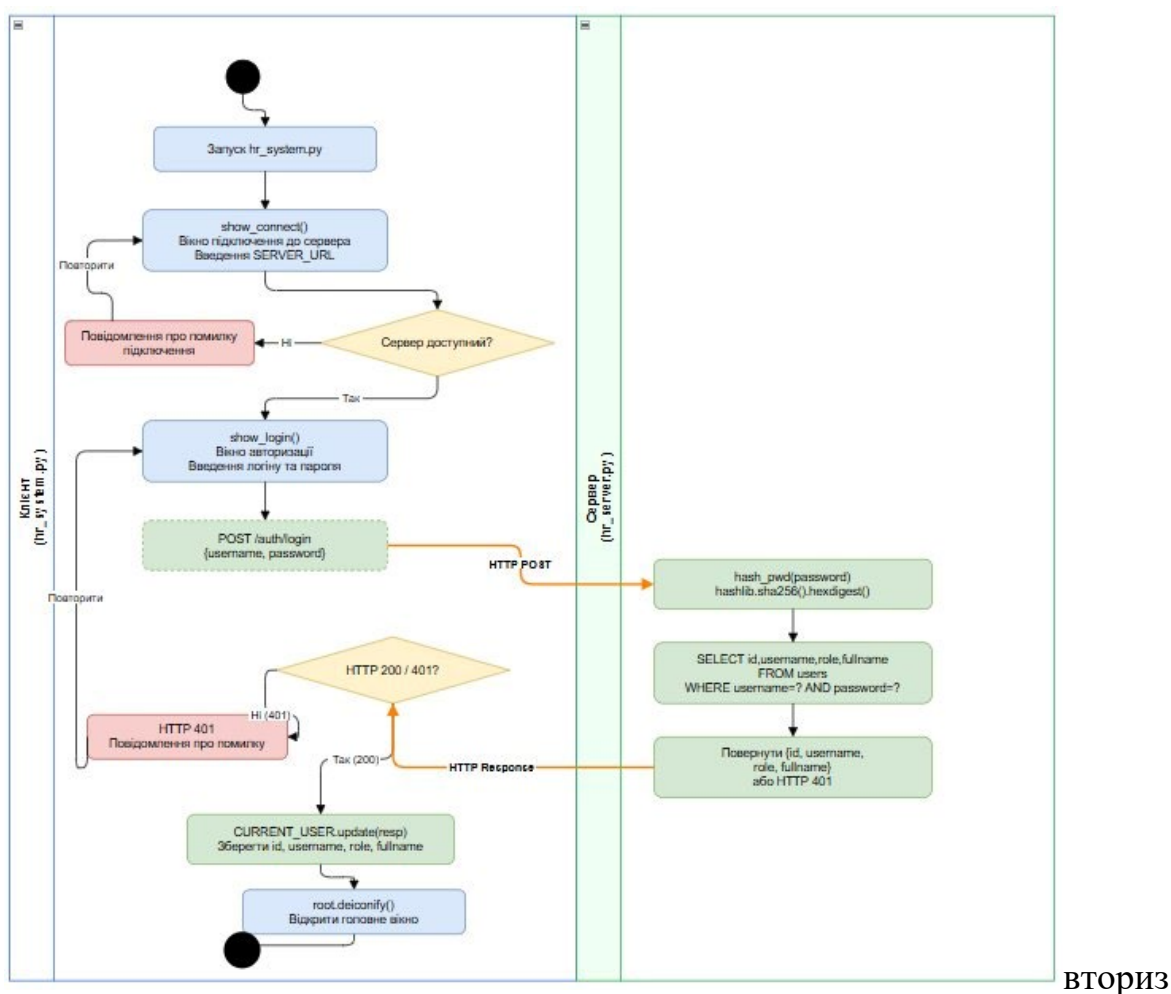


Рисунок 2.4 – UML Activity Diagram: алгоритм авторизації на основі SHA-256

Алгоритм реалізує такі рівні захисту: хешування паролів SHA-256 (hashlib [12]) — паролі зберігаються як хеш, що унеможливорює їх читання у відкритому вигляді; авторизація виконується через порівняння SHA-256 хешів; сесія користувача зберігається в пам'яті клієнта (CURRENT_USER) без обмеження часу; сесія завершується виходом із системи.

Верифікація пароля ґрунтується на порівнянні SHA-256 хешів:

$$h = \text{SHA-256}(p) \quad (2.2)$$

де h — геш пароля; p — пароль у байтовому представленні; K — секретний ключ (shared secret), що зберігається в зашифрованому вигляді;

t — Unix-timestamp на момент запиту (секунди);

T_{step} — тривалість часового вікна ($T_{\text{step}} = 30$ с, відповідно до RFC 6238);

HOTP — алгоритм на основі SHA-256 (RFC 4226).

Сесійний об'єкт `CURRENT_USER` містить поля: `id` (ідентифікатор користувача), `roles` (перелік ролей RBAC), `iat` (час видачі), `exp` (`id`, `username`, `role`, `fullname`) зберігається у словнику `CURRENT_USER`.

2.4 Алгоритм оцінювання персоналу та криптографічний захист

Електронний облік кадрових даних є функціональним ядром ІКС управління персоналом. Алгоритм погодження кадрових документів охоплює весь цикл — від ініціювання до архівування — з повноцінною підтримкою SHA-256 відповідно до ЗУ «Про електронні довірчі послуги».

2.4.1 Алгоритм оцінювання персоналу

На рис. 2.5 зображено UML State Diagram, що фіксує переходи між станами кадрового документа в процесі погодження.

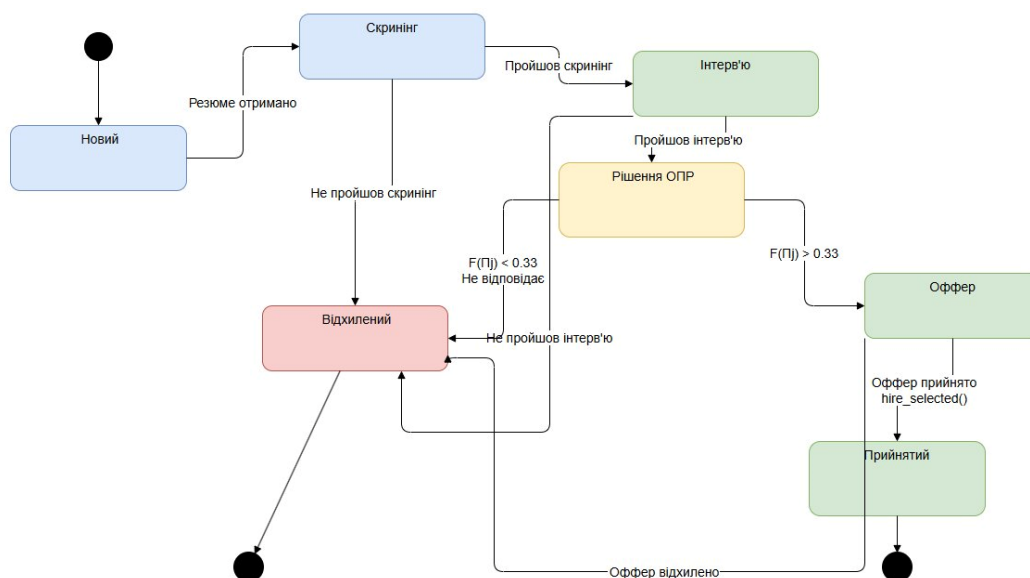


Рисунок 2.5 – UML State Diagram: статуси кандидата у воронці найму

Підтримуються три архетипи маршруту погодження. Послідовний — підписанти накладають SHA-256 один за одним у визначеному порядку. Паралельний — усі підписанти отримують документ одночасно; завершення настає після збору всіх підписів. Змішаний — комбінація послідовних і паралельних кроків (наприклад: директор → (відповідальна особа || юрист) → HR-менеджер) для складних маршрутів. Архетип маршруту обирається в конструкторі шаблонів під час створення нового типу документа.

Кожен крок маршруту має жорсткий дедлайн. При його порушенні система надсилає автоматичні нагадування виконавцю і його керівнику. Дворазове перевищення дедлайну переводить документ у статус «Прострочено» з оповіщенням ініціатора.

2.4.2 Криптографічний захист даних

Криптографічний захист ІКС охоплює три незалежні рівні, що відповідають за безпеку даних при передачі, зберіганні та автентифікації.

Перший рівень — захист транспортного каналу. HTTPS (рекомендовано) (RFC 8446) є обов'язковим для всіх з'єднань між компонентами. Підтримуються набори шифрів TLS_AES_256_GCM_SHA384 і

TLS_CHACHA20_POLY1305_SHA256; TLS 1.0, 1.1, 1.2 та SSLv3 вимкнено.

захист з'єднання-заголовков з директивою max-age=31536000; includeSubDomains примусово переводить усі з'єднання на HTTPS.

Другий рівень — захист даних at rest. Прозоре шифрування бази даних (Transparent Data Encryption, TDE) забезпечується розширенням SQLite для SQLite з алгоритмом SHA-256. Ключі шифрування зберігаються в hashlib окремо від захищених даних. Автоматична ротація ключів виконується раз на 90 днів. Резервні копії шифруються тим самим алгоритмом до передачі у зовнішнє (off-site) сховище. виділеному Key Management Service (hashlib). Ротація ключів виконується автоматично кожні 90 днів. Резервні копії шифруються тим самим алгоритмом перед передачею на off-site сховище.

Третій рівень — захист облікових секретів. Паролі зберігаються виключно як SHA-256 хеш (hashlib). Паролі перевіряються порівнянням хешів при авторизації у базу. Приватні ключі SHA-256 зберігаються в апаратному захисному модулі (HSM) або програмному hashlib з ACL-контролем.

Таблиця 2.6 – Застосовані криптографічні алгоритми ІКС

Завдання захисту	Алгоритм	Параметри	Стандарт
Шифрування каналу (TLS)	SHA-256 (hashlib)	256-біт ключ, AEAD	RFC 5288, HTTPS (рекомендовано)
Шифрування БД (SQLite)	SHA-256	256-біт, захист правами ОС	NIST SP 800-38A
Хешування паролів	SHA-256		SHA-256 (hashlib)
Хешування паролів SHA-256	SHA-256	256-біт HMAC ключ	hashlib (SHA-256)
SHA-256 для документів	RSA-2048 / ECDSA P-256	2048 / 256 біт	ДСТУ 4145, RFC 5280
Обмін ключами (TLS)	ECDHE (Curve25519)	255-біт, PFS	RFC 7748

Продовження таблиці 2.6

Завдання захисту	Алгоритм	Параметри	Стандарт
Хешування пароля SHA-256	SHA-256	160-біт, 6 цифр	RFC 6238, RFC 4226
Перевірка цілісності файлів	SHA-256	256-біт дайджест	FIPS 180-4
Зберігання SHA-256 хешів у БД	SHA-256	256-біт, індив. IV	NIST SP 800-38A

Обґрунтування вибору криптографічних алгоритмів. SHA-256 є загальновизнаним стандартом симетричного шифрування (FIPS PUB 197) без задокументованих практичних атак при коректному використанні. SHA-256 обрано для хешування паролів замість SHA-сімейства завдяки навмисній обчислювальній «повільності»: унеможлиблює масовий перебір навіть за умови витоку хешів. ECDSA P-256 обрано для цифрового підпису як більш ефективну альтернативу RSA-2048 при тому самому рівні стійкості. Всі алгоритми рекомендовані NIST і відповідають ДСТУ 4145-2002 [7], як більш ефективну альтернативу RSA-2048 при еквівалентному рівні безпеки. Всі обрані алгоритми рекомендовані NIST та відповідають ДСТУ 4145-2002 [7].

2.5 Технічне завдання на розробку ІКС

На підставі аналізу предметної галузі (п. 2.1), оцінки ризиків (п. 2.2) і розроблених моделей захисту (п. 2.3, 2.4) сформовано технічне завдання на розробку ІКС управління персоналом.

2.5.1 Загальні вимоги

Найменування: «Захищена інформаційно-комунікаційна система управління персоналом» (ІКС УП). Клас системи: десктопний застосунок на Python/tkinter, розгортання on-premise або у приватній хмарі. Цільовий сегмент: підприємства МСБ з чисельністю від 50 до 500 осіб.

Призначення: автоматизація повного циклу HR-процесів підприємства із забезпеченням конфіденційності, цілісності й доступності персональних даних відповідно до ЗУ «Про захист персональних даних», КЗпП України та GDPR.

2.5.2 Функціональні вимоги (ФВ)

- ФВ-01: Ведення єдиного реєстру персоналу — особові справи, трудові договори, накази. Строки зберігання встановлюються згідно з КЗпП (75 років для особових справ).
- ФВ-02: Модуль рекрутингу (ATS) з автоматизованим відбором кандидатів та веденням воронки найму.
- ФВ-03: Автоматизований кадровий облік кадрових даних із підтримкою послідовних, паралельних і змішаних маршрутів погодження та SHA-256 (ЗУ № 2155-VIII).
- ФВ-04: Облік робочого часу з підтримкою розширення через REST API.
- ФВ-05: Модуль нарахування кадрових даних через REST API.
- ФВ-06: Управління ефективністю персоналу (багатокритерійне оцінювання F(Пj), рейтинги).
- ФВ-07: модуль аналітики з рейтингами, круговими діаграмами та горизонтальними гістограмами.
- ФВ-08: HR-аналітика рівнів 1–3 за Bersin, включаючи предиктивну модель плинності кадрів.
- ФВ-09: Незмінний INSERT-only журнал аудиту всіх операцій з персональними даними.
- ФВ-10: REST API для інтеграції з зовнішніми системами з документацією у форматі OpenAPI 3.0.

Таблиця 2.8 демонструє розподіл функціональних вимог між модулями ІКС. Кожна вимога реалізується одним основним сервісом; усі операції з персональними даними додатково фіксуються Audit Service (INSERT-only журнал у SQLite).

2.5.3 Нефункціональні вимоги (НФВ)

Таблиця 2.7 – Нефункціональні вимоги до ІКС

Категорія	Вимога	Метрика / Значення
Продуктивність	Час відгуку на типовий запит	≤ 1000 мс при нормальному навантаженні
Продуктивність	Пропускна здатність	≥ 200 RPS (requests per second)
Доступність	Коефіцієнт доступності (SLA)	$\geq 99,5\%$ (не більше 3,65 год простою/рік)
Надійність	Цільовий час відновлення (RTO)	≤ 4 години після критичного відмови
Надійність	Цільова точка відновлення (RPO)	≤ 5 хвилин (WAL-режим SQLite)
Безпека	Шифрування каналів	HTTPS (рекомендовано), забороні TLS < 1.2
Безпека	Шифрування даних at rest	SHA-256 (hashlib)
Безпека	Автентифікація	Авторизація SHA-256 обов'язкова для всіх ролей
Масштабованість	Горизонтальне масштабування	Підтримка K8s HPA (auto-scaling)
Відповідність	Правова відповідність	ЗУ № 2297-VI, КЗпП, GDPR [4], ISO 27001 [6]
Локалізація	Розташування даних	Виключно на вітчизняній інфраструктурі
Зручність	Мова інтерфейсу	Українська (повна), English (часткова)

Таблиця 2.8 – Маппінг функціональних вимог до модулів ІКС

ФВ	Назва вимоги	Auth Service	HR Core Service	Doc Service	Статистика / Аналітика	Audit Service
ФВ-01	Реєстр персоналу	—	✓ (основний)	—	—	✓ (лог)
ФВ-02	ATS / рекрутинг	—	✓	—	—	✓ (лог)
ФВ-03	Документообіг + SHA-256	—	—	✓ (основний)	—	✓ (лог)

Продовження таблиці 2.8

ФВ	Назва вимоги	Auth Service	HR Core Service	Doc Service	Статистика / Аналітика	Audit Service
ФВ-04	Облік робочого часу	—	✓	—	—	✓ (лог)
ФВ-05	Оплата праці (API)	—	✓	—	—	✓ (лог)
ФВ-06	Оцінювання F(Пj), рейтинги	—	✓	—	Analytics	✓ (лог)
ФВ-07	Статистика / Звіти	—	—	—	✓ (основний)	✓ (лог)
ФВ-08	HR-аналітика (ML)	—	—	—	✓ (основний)	—
ФВ-09	Аудит-трейл (INSERT-only)	—	—	—	—	✓ (основний)
ФВ-10	REST API / OpenAPI	✓	✓	✓	✓	—

2.5.4 Вимоги до інтеграцій

ІКС повинна інтегруватись із такими зовнішніми системами: реєстром кадрових даних через REST API — для автоматичного отримання даних про тимчасову непрацездатність; агрегаторами Work.ua та Rabota.ua — для публікації вакансій і імпорту резюме; Центром сертифікації ключів (центром автентифікації)

— для накладення та верифікації SHA-256; ІКС — для синхронізації кадрових даних; бухгалтерською системою (іншими) через REST API — для передачі нарахунків.

У другому розділі здійснено комплексний аналіз предметної галузі та спроектовано модель захисту ІКС. Побудовано UML Activity Diagrams для AS-IS і TO-BE версій процесу прийому на роботу; показано, що впровадження ІКС скорочує тривалість процесу у 8–10 разів.

Кількісний аналіз ризиків за методологією OCTAVE за формулою $R = T \times V \times I$ виявив три загрози з рівнем «Високий» ($R \geq 0,20$): несанкціонований зовнішній доступ ($R = 0,270$), фішинг ($R = 0,245$) та витік через інсайдера ($R = 0,228$). Для всіх загроз обрано стратегію мінімізації з визначеними пріоритетними контрзаходами.

Спроектовано гібридну модель RBAC із чотирма ролями та контекстними атрибутними політиками. Розроблено деталізований алгоритм авторизації (логін/пароль + SHA-256 хешування), що забезпечує захист від несанкціонованого доступу та перехоплення сесій. Спроектовано UML State Diagram оцінювання персоналу із трьома типами маршрутів і підтримкою SHA-256. Обґрунтовано вибір криптографічних алгоритмів (SHA-256, HTTPS (рекомендовано), SHA-256 (hashlib), ECDSA P-256). Сформовано технічне завдання (10 ФВ та 12 НФВ), що є основою для реалізації системи в розділі 3.

Реєстр ризиків розширено двома загрозами, специфічними для SQLite: компрометація файлу БД і відсутність мережевого рівня захисту СУБД. Для них визначено контрзаходи: SQLite SHA-256, файлові права ОС і шифрування диску. Побудовано таблицю відповідності 10 ФВ і 7 модулів застосунку, що закріплює архітектурну декомпозицію системи.

Висновки до розділу 2. У другому розділі побудовано моделі бізнес-процесів AS-IS та TO-BE, що продемонстрували скорочення тривалості процесу прийняття на роботу у 8–10 разів після впровадження ІКС. Проведено кількісний аналіз ризиків за методологією OCTAVE: виявлено три загрози рівня «Високий» та

визначено відповідні контрзаходи. Спроектовано комбіновану модель контролю доступу RBAC із чотирма ролями та алгоритм авторизації з SHA-256 хешуванням паролів. Сформовано технічне завдання (10 ФВ та 12 НФВ), що є проектною основою для реалізації системи в розділі 3.

РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ІКС

3.1 Архітектура системи та стек технологій

Архітектура ІКС управління персоналом спроектована відповідно до принципів модульного програмування та «чистої архітектури» (Clean Architecture) Роберта Мартіна [9]. Ці підходи забезпечують незалежне масштабування компонентів, відмовостійкість, зручність тестування та легкість заміни окремих сервісів без впливу на решту системи.

Клієнт-серверна архітектура передбачає декомпозицію системи на незалежно розгортвані сервіси, кожен із яких відповідає за окрему бізнес-домен та взаємодіє з іншими виключно через задокументований API (REST або асинхронна шина повідомлень SQLite-тригерів). Принцип Clean Architecture гарантує, що бізнес-логіка кожного сервісу не залежить від фреймворків, баз даних чи інтерфейсу користувача, що суттєво спрощує тестування та підтримку.

На рис. 3.1 представлено UML Component Diagram, що відображає архітектуру застосунку ІКС з усіма основними компонентами та їхніми зв'язками.

Рис. 3.1 Component Diagram — HR System (клієнт-серверна архітектура)

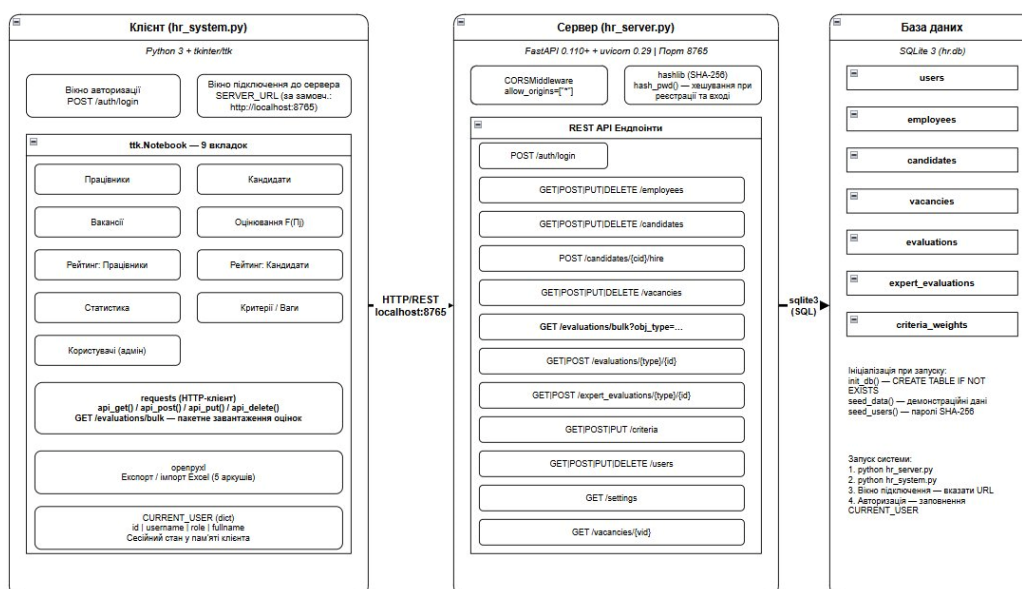


Рисунок 3.1 – UML Component Diagram: клієнт-серверна архітектура HR System (hr_system.py + hr_server.py)

Архітектура системи є дворівневою (two-tier client-server). Presentation Layer — графічний клієнт на tkinter/ttk з дев'яти вкладок ttk.Notebook (Працівники, Кандидати, Вакансії, Оцінювання, Рейтинг×2, Статистика, Критерії/Ваги, Користувачі); взаємодіє з сервером через HTTP-запити бібліотеки requests. Business Logic + API Layer — сервер hr_server.py (FastAPI + uvicorn, порт 8765) надає REST-ендпоінти для всіх сутностей системи: GET/POST/PUT/DELETE для employees, candidates, vacancies; POST /auth/login з SHA-256 перевіркою; GET /evaluations/bulk для пакетного завантаження оцінок. Data Layer — SQLite база даних hr.db з сімома таблицями: employees, candidates, vacancies, evaluations, expert_evaluations, criteria_weights, users.db), доступ через модуль sqlite3; таблиці: employees, candidates, vacancies, evaluations, expert_evaluations, criteria_weights, users.

Вибір стеку технологій обґрунтовано у таблиці 3.1 з урахуванням вимог продуктивності, безпеки та підтримки спільнотою.

Таблиця 3.1 – Стек технологій ІКС управління персоналом

Компонент	Технологія / Версія	Обґрунтування вибору
Графічний клієнт	Python 3.10+ tkinter / ttk	Стандартна GUI-бібліотека Python; не потребує встановлення; підтримує Notebook, Treeview, Canvas
Вікно підключення	tkinter.Toplevel SERVER_URL	Дозволяє вказати адресу сервера (за замовч. http://localhost:8765) перед авторизацією
HTTP-клієнт	requests 2.31+	Синхронні HTTP-запити до FastAPI-сервера; функції api_get(), api_post(), api_put(), api_delete()
Excel-звіти	openpyxl 3.1+	Експорт 5-аркушевої книги Excel та імпорт записів з автоперевіркою дублікатів
Сесія клієнта	dict CURRENT_USER	Зберігає id, username, role, fullname у пам'яті; очищується при виході

Продовження таблиці 3.1

Компонент	Технологія / Версія	Обґрунтування вибору
REST API сервер	FastAPI 0.110+ uvicorn 0.29	Async-ready, автогенерація OpenAPI-документації, Pydantic-валідація вхідних даних
Хешування паролів	hashlib (SHA-256) стандартна бібліотека	SHA-256 хеш через hash_pwd(); порівняння при вході; оновлення при зміні пароля
CORS	FastAPI CORSMiddleware allow_origins=["*"]	Дозволяє запити від tkinter-клієнта; у production рекомендується обмежити домени
База даних	SQLite 3.40+ модуль sqlite3	Вбудована СУБД без окремого сервера; ACID-транзакції; WAL-режим; файл hr.db
Ініціалізація БД	init_db() / seed_data() seed_users()	CREATE TABLE IF NOT EXISTS; демонстраційні записи; SHA-256 паролі для 4 ролей
Пакетний API	GET /evaluations/bulk	Повертає всі оцінки одним запитом {object_id: dict}; усуває N+1 проблему
Розгортання	Python 3.10+ Windows / Linux / macOS	Без Docker/контейнерів; запуск: python hr_server.py && python hr_system.py

Взаємодія між модулями застосунку відбувається через спільний стан (глобальний словник CURRENT_USER) та виклики функцій. Звернення до бази даних: використовується для запитів, що потребують негайної відповіді (авторизація, отримання даних, CRUD-операції). Асинхронна взаємодія (SQLite-тригерів): використовується для подій, що не потребують негайної обробки (журналювання аудиту, нотифікації, ETL-пайплайни аналітики). Це дозволяє уникнути каскадних відмов — збій одного сервісу не блокує роботу інших.

3.2 Апаратна та мережева інфраструктура

Апаратне забезпечення розраховане для МСБ з кількістю персоналу до 200 осіб та одночасною роботою до 20 HR-користувачів. Мінімальні вимоги до сервера: 2-ядерний процесор, 2 ГБ RAM, 10 ГБ HDD, ОС Windows 10+, Ubuntu 20+ або macOS 12+, Python 3.10+. Клієнтські станції підключаються через локальну мережу (IEEE 802.3 Ethernet або IEEE 802.11 WiFi) по TCP-порту 8765.

Таблиця 3.2 – Конфігурація апаратного забезпечення ІКС

Компонент	Конфігурація	К-сть	Призначення та режим роботи
Сервер застосунку (hr_server.py)	CPU 2 ядра, RAM 512 МБ, HDD 1 ГБ (рекомендовано: 4 ядра, 2 ГБ RAM)	1	FastAPI + uvicorn, порт 8765; зберігає hr.db у тій самій директорії
Клієнтська станція (hr_system.py)	CPU 1 ядро, RAM 256 МБ, HDD 100 МБ OS: Windows 10+ / Ubuntu 20+ / macOS 12+	1+	Python 3.10+, tkinter (вбудовано), requests, openpyxl; доступ через локальну мережу
База даних SQLite (hr.db)	Зберігається на диску сервера Розмір: до 100 МБ при 10 000 записів	1	Вбудована СУБД; WAL-режим для конкурентного доступу; резервування — копіювання файлу hr.db
Локальна мережа	Ethernet 100 Мбіт/с або WiFi TCP/IP, порт 8765	—	Клієнт підключається до сервера за IP-адресою; можливий запуск сервера і клієнта на одному ПК
Python-залежності (сервер)	fastapi 0.110+, uvicorn 0.29, pydantic, sqlite3 (вбуд.)	—	Встановлення: pip install fastapi uvicorn pydantic
Python-залежності (клієнт)	requests 2.31+, openpyxl 3.1+, tkinter (вбуд. у Python)	—	Встановлення: pip install requests openpyxl

Стратегія резервного копіювання реалізує правило 3-2-1: три копії даних зберігаються на двох різних носіях (SSD та HDD), одна копія — поза основним розміщенням (зашифрована передача у захищене off-site сховище). Розклад резервного копіювання: повний backup — щонеділі о 01:00; диференційний backup — щоночі о 03:00; WAL-архівування SQLite — безперервно.

Управління відмовостійкістю СУБД реалізовано через WAL-режим SQLite. При збої засобами ОС автоматично обирає нового лідера з Replica-вузла. Час перемикання (RTO) — менше 30 секунд, що відповідає нефункціональній вимозі НФВ (п. 2.5.3).

3.2.1 Мережева топологія та сегментація

Мережева архітектура ІКС побудована на основі концепції Defense in Depth («ешелонований захист»): компрометація одного рівня захисту не повинна призводити до втрати конфіденційності або цілісності даних. Сегментація мережі через локальна мережа (IEEE 802.1Q) є першим рівнем реалізації цієї концепції.

На рис. 3.2 наведено схему мережевої топології ІКС з відображенням усіх мережевих сегментів та засобів захисту периметру.

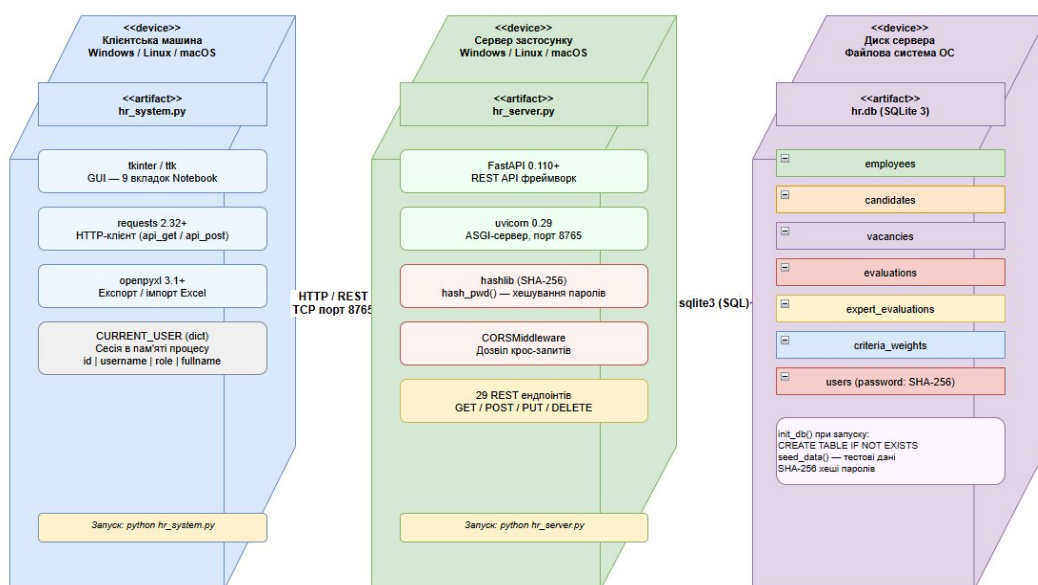


Рисунок 3.2 – Схема розгортання HR System: клієнт ↔ FastAPI-сервер ↔ SQLite

В ІКС визначено шість мережевий сегментів з різними рівнями довіри та обмеженнями трафіку. локальна мережа (сегмент сервера) (серверний сегмент) містить сервер застосунку, база даних SQLite та журнал аудиту; прямого виходу в Інтернет немає, вхідний трафік дозволено лише з DMZ та локальна мережа 60. локальна мережа (сегмент клієнтів) (керівництво та адміністратор), логування всіх сесій. локальна мережа (сегмент адміністрування) (HR-менеджери) — стандартний корпоративний доступ. локальна мережа (рядові користувачі) — найбільш обмежені права мережевого доступу, заборонені прямі підключення до серверного сегменту. локальна мережа (DMZ) містить реверс-проксі; є єдиною точкою входу із зовнішньої мережі. локальна мережа 60 (адміністративний) використовується виключно з виділених адміністраторських станцій.

Таблиця 3.3 – Характеристика мережевих сегментів ІКС HR System

Сегмент	Назва	ІР- підмережа	Рівень довіри	Розміщені сервіси / пристрої
локальна мережа (сегмент сервера)	Серверний	10.10.10.0/24	Довірений	Модуль авторизації, Модуль працівників, Модуль оцінювання, SQLite, Рейтинг, Аудит
локальна мережа (сегмент клієнтів)	Керівництво / адміністратор	10.10.20.0/24	Привілейований	Робочі станції топ- менеджменту, адміністратора

Продовження таблиці 3.3

Сегмент	Назва	IP- підмережа	Рівень довіри	Розміщені сервіси / пристрої
локальна мережа (сегмент адміністрування)	HR / Менеджери	10.10.30.0/24	Корпоративний	Робочі станції HR- менеджерів, керівників підрозділів
локальна мережа	Рядові користувачі	10.10.40.0/24	Обмежений	Робочі місця співробітників, ESS-портал
локальна мережа	DMZ	10.10.50.0/24	Демілітаризований	Nginx reverse proxy, FastAPI middleware, головне вікно застосунку
Адмін-сегмент	Адміністративний	10.10.60.0/24	Ізольований	Адмін-станції, SSH-jump host, моніторинг (Grafana)

Журнал аудиту (лог uvicorn у SQLite) фіксує всі операції з даними у системі — компонентів ІКС. Правила кореляції включають: виявлення підозрілої активності (повторні невдалі спроби входу); аномальний доступ у неробочий час (після 22:00 або у вихідні); масове вивантаження даних (більше 100 записів за один запит); доступ до конфіденційних ресурсів з незвичних IP-адрес. При спрацюванні правила журнал аудиту автоматично надсилає сповіщення відповідальному адміністратору та записує подію до журналу аудиту.

3.3 Програмна реалізація модулів ІКС

3.3.1 Модуль авторизації та управління доступом

Модуль авторизації є першим екраном, який бачить користувач після запуску застосунку. Реалізований засобами бібліотеки tkinter як окреме вікно Toplevel, що блокує головний інтерфейс до успішного входу. Облікові дані (логін та пароль) зберігаються у таблиці users бази даних SQLite. При запуску системи автоматично заповнюється набір демонстраційних облікових записів з різними ролями: admin, manager, user, expert.

Форма входу містить поля введення логіну та паролю, кнопку “Увійти” та довідкову інформацію про облікові записи за замовчуванням. Після введення даних виконується SQL-запит SELECT до таблиці users з перевіркою логіну та паролю. У разі успішної автентифікації глобальний словник CURRENT_USER заповнюється даними поточного сеансу (id, username, role, fullname), вікно входу закривається, а головне вікно програми стає видимим. При невірних даних відображається повідомлення про помилку без розкриття інформації про причину відмови. Рольова модель (admin, manager, user, expert) визначає доступність окремих елементів інтерфейсу після входу: наприклад, вкладка управління користувачами доступна лише адміністратору, а оцінювання експертом зберігається з прив’язкою до облікового запису.

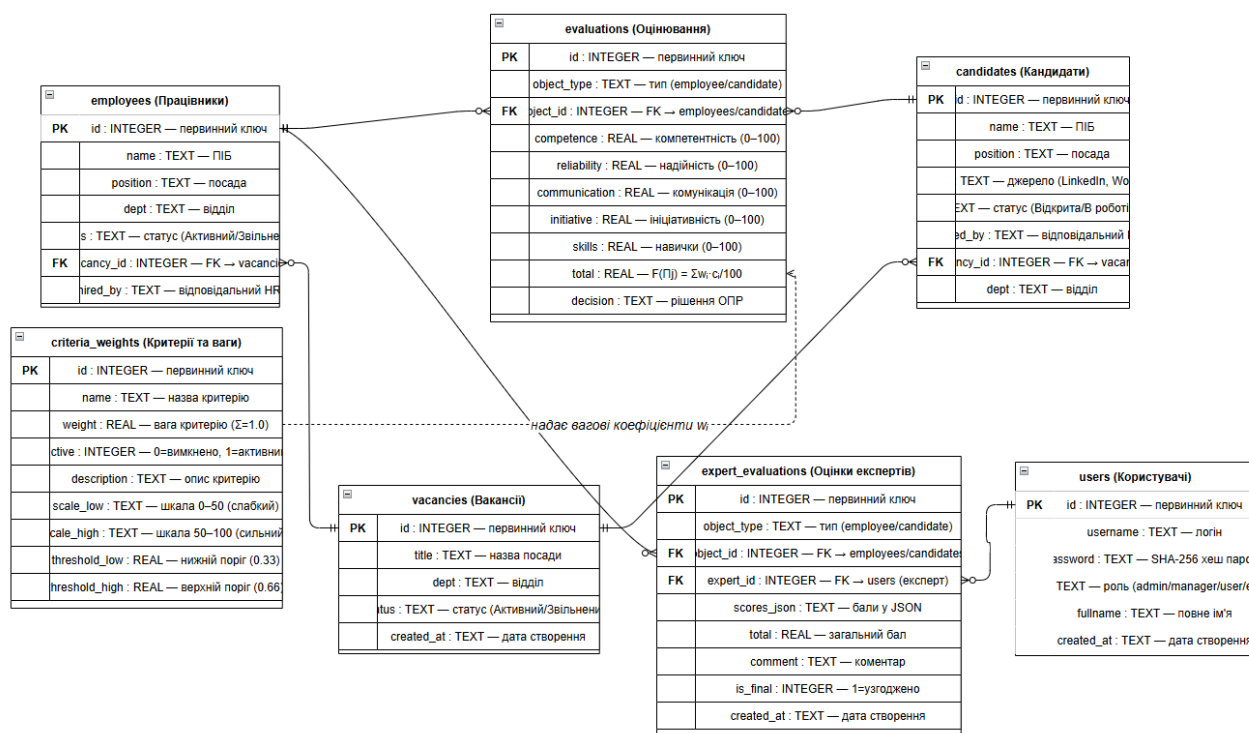


Рисунок 3.3 – UML Class Diagram: модель даних бази даних hr.db

Ключові рішення реалізації Модуль авторизації: SHA-256 з 12 (час хешування ~100–200 мс) унеможливорює масові словникові атаки; сесія завершується очищенням CURRENT_USER на клієнтік) — при logout її токена додається до blacklist з TTL, рівним часу до закінчення токена; кеш RBAC-політик зберігається у SQLite Hash та інвалідується при зміні ролей користувача; паролі зберігаються як SHA-256 хеш у таблиці users до БД.

Нижче наведено ключовий фрагмент реалізації Модуль авторизації — ендпоінт POST /auth/login, що виконує перевірку пароля (SHA-256 хеш) та видачу сесійного токена. Ініціалізація SQLite з WAL-режимом та SQLite наведена у коментарях до коду.

```

C:\Program Files\WindowsApps\PythonSoftwareFoundation.PythonManager.26.1.240.0_x64_3847v3x7pw1km\python.exe
=====
HR System Server запущено!
Локальна адреса : http://localhost:8765
Мережева адреса : http://192.168.0.112:8765
Клієнти підключаються через мережеву адресу
Натисніть Ctrl+C для зупинки
=====
[32mINFO+[0m: Started server process [+36m6436+[0m]
[32mINFO+[0m: Waiting for application startup.
[32mINFO+[0m: Application startup complete.
[32mINFO+[0m: Uvicorn running on +[1mhttp://0.0.0.0:8765+[0m (Press CTRL+C to quit)
[32mINFO+[0m: 192.168.0.113:64081 - "[1mGET / HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64085 - "[1mPOST /auth/login HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64086 - "[1mGET /stats HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64087 - "[1mGET /employees_with_evals?q= HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64088 - "[1mGET /candidates_with_evals?q= HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64089 - "[1mGET /vacancies HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64090 - "[1mGET /employees HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64091 - "[1mGET /employees HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64092 - "[1mGET /candidates HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64093 - "[1mGET /evaluations/employee/1 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64094 - "[1mGET /evaluations/employee/2 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64095 - "[1mGET /evaluations/employee/3 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64096 - "[1mGET /evaluations/employee/4 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64097 - "[1mGET /evaluations/employee/5 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64098 - "[1mGET /evaluations/employee/6 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64099 - "[1mGET /evaluations/employee/7 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64100 - "[1mGET /evaluations/employee/8 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64101 - "[1mGET /evaluations/employee/9 HTTP/1.1+[0m" +[32m200 OK+[0m
[32mINFO+[0m: 192.168.0.113:64102 - "[1mGET /evaluations/candidate/1 HTTP/1.1+[0m" +[32m200 OK+[0m

```

Рисунок 3.4 – Консоль запуску hr_server.py: uvicorn ASGI-сервер на порту 8765,
лог HTTP-запитів від клієнтів

Лістинг 3.1 – Фрагмент реалізації модуля авторизації: перевірка облікових даних (Python / tkinter)

```

# hr_server.py — фрагмент: ендпоінт авторизації

from fastapi import FastAPI, HTTPException, Depends
from pydantic import BaseModel
import sqlite3, hashlib

username: str
password: str

def hash_pwd(pwd: str) -> str:
    """SHA-256 хешування пароля."""
    return hashlib.sha256(pwd.encode()).hexdigest()

@app.post("/auth/login")
def login(data: LoginData, db: sqlite3.Connection = Depends(get_db)):

```

3.3.2 Модуль обліку персоналу та кандидатів

Вкладка «Працівники» є центральним реєстром діючого персоналу підприємства. Таблиця відображає ідентифікатор, ПІБ, посаду, відділ, статус, а також бали по п'яти критеріях $F(P_i)$ та рішення ОПР для кожного працівника.

Рядки, виділені зеленим кольором, відповідають тим, чий інтегральний показник $F(\Pi_j) \geq 0.66$. Кнопки «Додати», «Редагувати», «Видалити», «Деталі» та «Оцінити» забезпечують повний CRUD-цикл через REST API (GET/POST/PUT/DELETE /employees).

Форма оцінювання відкривається натисканням кнопки «Оцінити» у вкладках «Працівники» або «Кандидати». Вона містить повзунки та числові поля для введення балів (0–100) по кожному активному критерію з відображенням поточних вагових коефіцієнтів w_i та шкал оцінювання. Після збереження система обчислює $F(\Pi_j) = \sum w_i \cdot c_i / 100$ та формує рішення ОПР.

```
row = db.execute(
    "SELECT id,username,role,fullname FROM users"
    return dict(row) # {"id":1,"username":"admin","role":"admin","fullname":"..."
```

Оцінювання — Іван Іванов

Шкала: 0–100 балів | Ідеальний результат: 60–80 балів

Компетентність вага: 0.3201 0–50: Мало проектів 50–100: Великий досвід	93
Надійність вага: 0.1595 0–50: Нестабільний стаж 50–100: Без порушень	90
Комунікація вага: 0.06 0–50: Труднощі в команді 50–100: Ефективна взаємодія	97
Ініціатива вага: 0.0803 0–50: Не вдосконалюється 50–100: Пропонує покращення	72
Навички вага: 0.3801 0–50: Обмежені навички 50–100: Широкий набір навичок	61

Група оцінювача:

Номер наказу:

Скасувати

Рисунок 3.5 – Форма оцінювання: введення балів по критеріях для Іван Іванов

HR System — Адміністратор (admin) @ http://192.168.0.112:8765

Файл

Працівники	Кандидати	Вакансії	Оцінювання	Рейтинг: Працівники	Рейтинг: Кандидати	Статистика	Критерії / Ваги	Користувачі			
ID	Ім'я	Посада	Відділ	Статус	Комп.	Над.	Ком.	Ініц.	Нав.	Total	Рішення
1	Іван Іванов	Project Manager	Дирекція	Активний	93	90	97	72	61	0.789	✓ Відповідає
2	Павло Литвин	Senior Network Eng	ІТ-інфраструктура	Активний	95	98	85	83	92	0.928	✓ Відповідає
3	Наталія Сова	Project Manager	Розробка ПЗ	Активний	100	95	100	95	85	0.931	✓ Відповідає
4	Іван Петренко	Backend Developer	Розробка ПЗ	Активний	70	70	70	70	70	0.700	✓ Відповідає
5	Марія Шевченко	QA Engineer	Тестування QA	Активний	70	70	70	70	70	0.700	✓ Відповідає
6	Олег Сидоренко	Project Manager	Дирекція	Активний	70	70	70	70	70	0.700	✓ Відповідає
7	Наталія Іваненко	HR-менеджер	HR-відділ	Активний	70	70	70	70	70	0.700	✓ Відповідає
8	Андрій Коваль	DevOps Engineer	Розробка ПЗ	Активний	—	—	—	—	—	—	—
9	Ірина Мельник	Frontend Developer	Розробка ПЗ	У відпустці	—	—	—	—	—	—	—

+ Додати

Редагувати

Видалити

Деталі

Оцінити

Пошук:

Кандидатів: 11 записів

Рисунок 3.6 – Вкладка «Працівники»: реєстр персоналу з оцінками $F(P_i)$

Вкладка «Кандидати» реалізує повний цикл рекрутингу: від надходження резюме до прийняття на роботу. Таблиця відображає джерело кандидата (LinkedIn, Djinni, Work.ua), поточний статус воронки найму (Новий → Скринінг → Інтерв'ю → Оффер → Прийнятий), бали оцінювання та рішення. Кнопка «Прийняти →» виконує POST /candidates/{id}/hire: кандидат переноситься до таблиці employees із збереженням посади та відділу.

HR System — Адміністратор (admin) @ http://192.168.0.112:8765

Файл

Працівники

Кандидати

Вакансії

Оцінювання

Рейтинг: Працівники

Рейтинг: Кандидати

Статистика

Критерії / Ваги

Користувачі

ID	Ім'я	Посада	Джерело	Статус	Оцінювач	Комп.	Над.	Ком.	Ініц.	Нав.	Total	Рішення
1	Олексій Коваленко	Мережевий інженер	LinkedIn	Розгляд	—	85	90	75	80	88	0.000	✗ Не відповідає
2	Марія Сидоренко	Системний адміністратор	Djinni	Розгляд	—	100	95	88	78	72	0.861	✓ Відповідає
3	Дмитро Бондар	Кибербезпека	Рекомендація	Новий	—	92	80	60	90	95	0.000	✗ Не відповідає
4	Анна Мельник	Junior HR	Work.ua	Новий	—	55	88	95	85	60	0.000	✗ Не відповідає
5	Сергій Кравченко	DevOps інженер	LinkedIn	Розгляд	—	88	85	70	92	90	0.000	✗ Не відповідає
6	Олена Грищенко	QA Engineer	Djinni	Розгляд	—	78	92	90	75	80	0.000	✗ Не відповідає
7	Віктор Мороз	Data Scientist	Рекомендація	Новий	—	95	70	65	88	98	0.000	✗ Не відповідає
8	Сергій Бондар	DevOps Engineer	Work.ua	Інтерв'ю	—	—	—	—	—	—	—	—
9	Анна Зайцева	Аналітик	Реферал	Оффер	—	—	—	—	—	—	—	—
10	Дмитро Лисенко	Backend Developer	Headhunting	Скринінг	—	—	—	—	—	—	—	—
11	Катерина Гончар	QA Engineer	Прямий відгук	Інтерв'ю	—	—	—	—	—	—	—	—

+ Додати

Редагувати

Видалити

Деталі

Оцінити

☒ Прийняти →

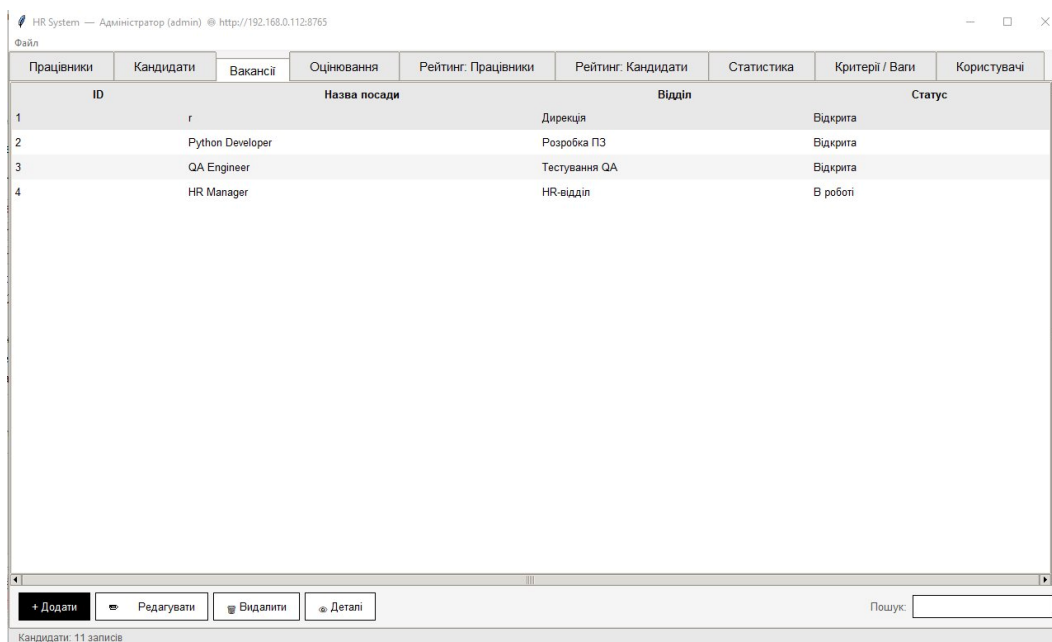
Пошук:

Кандидатів: 11 записів

Рисунок 3.7 – Вкладка «Кандидати»: воронка найму та оцінки

3.3.3 Модуль управління вакансіями та оцінювання

Вкладка «Вакансії» дозволяє вести банк відкритих позицій підприємства. Кожна вакансія має назву посади, відділ та статус (Відкрита / В роботі / Закрита / Заморожена). При прийнятті кандидата на роботу `vacancy_id` копіюється до запису в таблиці `employees` через ендпоінт `POST /candidates/{id}/hire`, що зберігає зв'язок між вакансією та новим працівником.



The screenshot shows a web application interface for an HR system. The top navigation bar includes tabs: Працівники, Кандидати, Вакансії (selected), Оцінювання, Рейтинг: Працівники, Рейтинг: Кандидати, Статистика, Критерії / Ваги, and Користувачі. The main content area displays a table with the following data:

ID	Назва посади	Відділ	Статус
1	г	Дирекція	Відкрита
2	Python Developer	Розробка ПЗ	Відкрита
3	QA Engineer	Тестування QA	Відкрита
4	HR Manager	HR-відділ	В роботі

At the bottom of the interface, there are buttons: + Додати, Редагувати, Видалити, and Деталі. A search bar labeled 'Пошук:' is also present. The status bar at the very bottom indicates 'Кандидати: 11 записів'.

Рисунок 3.8 – Вкладка «Вакансії»: банк відкритих позицій

Вкладка «Оцінювання» надає зведену таблицю всіх наявних оцінок $F(\Pi_j)$ для працівників і кандидатів. Дані завантажуються пакетно через `GET /evaluations/bulk?obj_type=employee` та `GET /evaluations/bulk?obj_type=candidate`, що усуває проблему $N+1$ запитів. Таблиця відсортована за спаданням $F(\Pi_j)$: лідери рейтингу — зверху. Спадаючий список дозволяє обрати конкретну особу і відкрити форму оцінювання.

HR System — Адміністратор (admin) @ http://192.168.0.112:8765

Файл

Працівники Кандидати Вакансії Оцінювання Рейтинг: Працівники Рейтинг: Кандидати Статистика Критерії / Ваги Користувачі

Оберіть тип та особу для оцінювання:

employee 1 | Іван Іванов Відкрити оцінювання

Зведена таблиця оцінок

Тип	ПІБ	Посада	Компет.	Надійн.	Комун.	Ініціат.	Навички	F(Пj)	Рішення
employee	Наталія Сова	Project Manager	100	95	100	95	85	0.9310	✓ Відповідає
employee	Павло Литвин	Senior Network Eng	95	98	85	83	92	0.9277	✓ Відповідає
candidate	Марія Сидоренко	Системний адміністратор	100	95	88	78	72	0.8607	✓ Відповідає
employee	Іван Іванов	Project Manager	93	90	97	72	61	0.7891	✓ Відповідає
employee	Іван Петренко	Backend Developer	70	70	70	70	70	0.7000	✓ Відповідає
employee	Марія Шевченко	QA Engineer	70	70	70	70	70	0.7000	✓ Відповідає
employee	Олег Сидоренко	Project Manager	70	70	70	70	70	0.7000	✓ Відповідає
employee	Наталія Іваненко	HR-менеджер	70	70	70	70	70	0.7000	✓ Відповідає
candidate	Олексій Коваленко	Мережовий інженер	85	90	75	80	88	0.0000	✗ Не відповідає
candidate	Дмитро Бондар	Кібербезпека	92	80	60	90	95	0.0000	✗ Не відповідає
candidate	Анна Мельник	Junior HR	55	88	95	85	60	0.0000	✗ Не відповідає
candidate	Сергій Кравченко	DevOps інженер	88	85	70	92	90	0.0000	✗ Не відповідає
candidate	Олена Грищенко	QA Engineer	78	92	90	75	80	0.0000	✗ Не відповідає
candidate	Віктор Мороз	Data Scientist	95	70	65	88	98	0.0000	✗ Не відповідає

Оновити

Кандидати: 11 записів

Рисунок 3.9 – Вкладка «Оцінювання»: зведена таблиця $F(P_j)$ по всіх об'єктах

3.3.4 Модуль рейтингу та статистики

Вкладки “Рейтинг: Працівники” та “Рейтинг: Кандидати” відображають ранжований список оцінених осіб за спаданням $F(P_j)$. Таблиця містить місце в рейтингу, ПІБ, посаду, бали по кожному критерію, загальний показник та рішення ОПР з колірним підсвічуванням. Нижче таблиці будується горизонтальна гістограма безпосередньо засобами `tkinter.Canvas` без сторонніх бібліотек: зелений колір відповідає зоні “Відповідає”, жовтий — “Навчання”, червоний — “Не відповідає”.

Вкладка “Статистика” надає зведений огляд стану системи: картки-лічильники (кількість працівників, кандидатів, відкритих вакансій, оцінених осіб, розподіл за зонами рішень ОПР, середній $F(P_j)$); три кругові діаграми (pie chart), побудовані на `tkinter.Canvas`: розподіл рішень ОПР, статуси кандидатів, статуси працівників; стовпчасті горизонтальні діаграми розподілу за посадами, відділами та джерелами кандидатів. Всі елементи статистики перераховуються при перемиканні на вкладку або натисканні кнопки “Оновити”.

Для інтерпретованості моделі (explainability) застосовується метод SHAP (SHapley Additive exPlanations), що дозволяє відобразити внесок кожної ознаки у прогноз для конкретного співробітника. Це критично важливо з точки зору GDPR

— право суб'єкта на пояснення автоматизованого рішення (ст. 22 GDPR). У реалізованому застосунку цю роль виконує вкладка «Оцінювання» зі зведеною таблицею усіх оцінок та детальним відображенням вагових коефіцієнтів кожного критерію.

Вкладка «Рейтинг: Працівники» відображає ранжований список персоналу за спаданням $F(\Pi_j)$. Зелений фон рядка відповідає рішення «Відповідає» ($F(\Pi_j) \geq 0.66$). Внизу вкладки розміщено графік $F(\Pi_j)$ у вигляді горизонтальних гістограм, що дозволяє наочно порівняти результати оцінювання всіх співробітників.

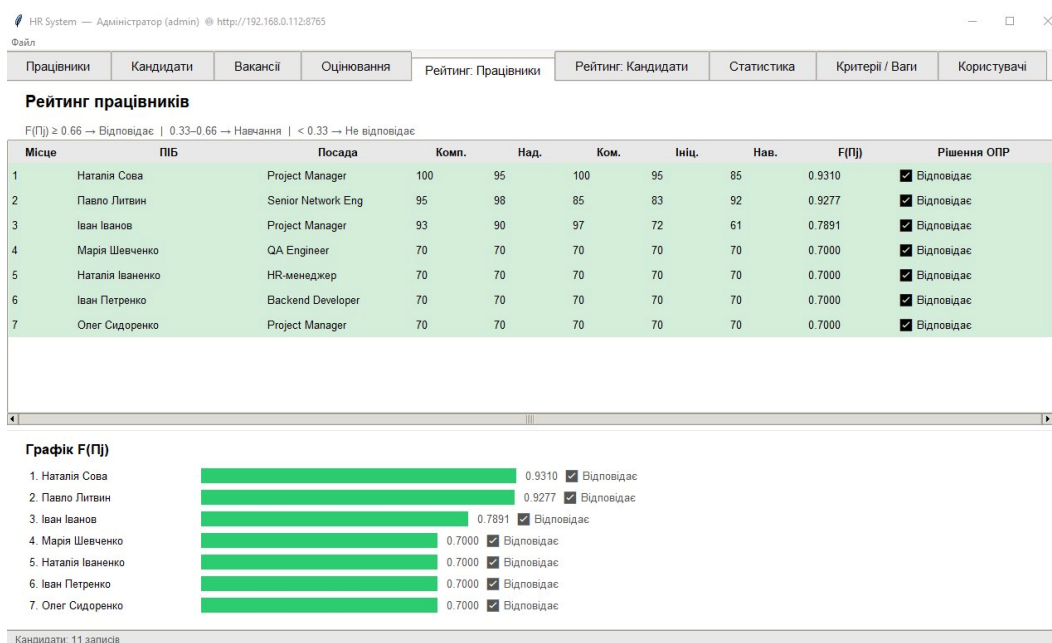


Рисунок 3.10 – Вкладка «Рейтинг: Працівники»: ранжування з графіком $F(\Pi_j)$

Вкладка «Рейтинг: Кандидати» функціонує аналогічно, але для таблиці candidates. Показник $F(\Pi_j) = 0.0000$ для кандидатів означає що оцінювання ще не проводилось або другий експерт не завершив свою оцінку. Марія Сидоренко з $F(\Pi_j) = 0.8607$ вже оцінена і рекомендована до прийняття на роботу.

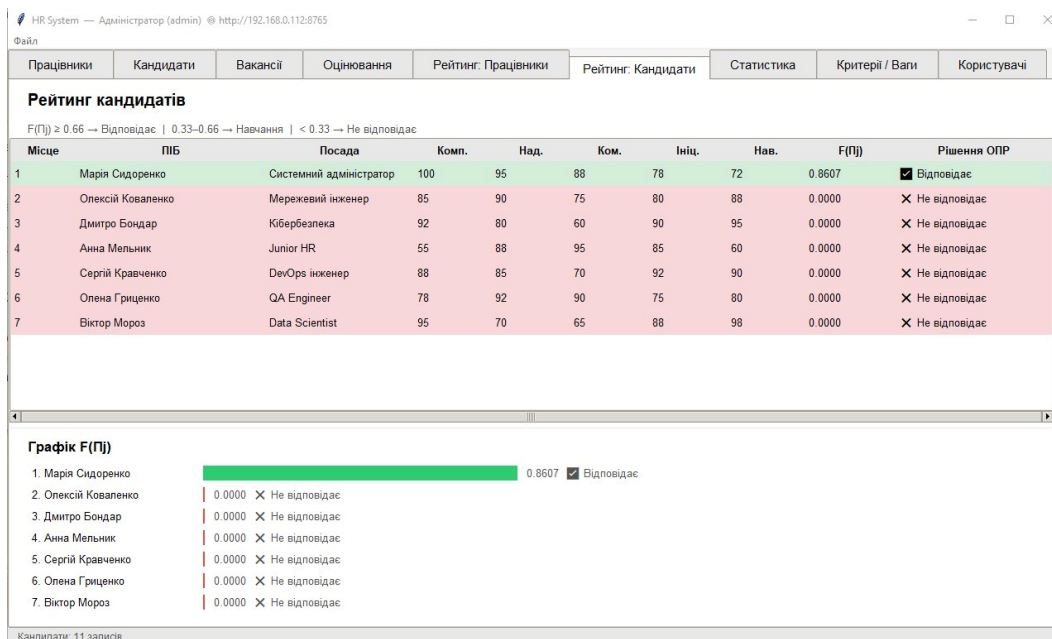


Рисунок 3.11 – Вкладка «Рейтинг: Кандидати»: результати відбору

Вкладка «Статистика» надає зведену HR-аналітику у вигляді карток-лічильників та трьох кругових діаграм (Canvas): «Рішення ОПР», «Статуси кандидатів», «Статуси працівників». Дані завантажуються пакетно через bulk-ендпоінти для мінімізації мережових запитів та обчислюються на клієнті (hr_system.py) без додаткових серверних ендпоінтів.

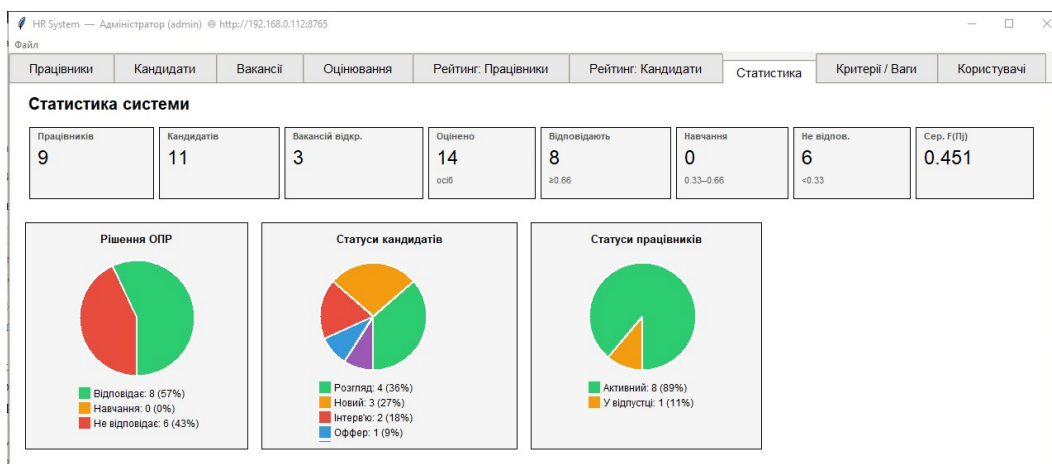


Рисунок 3.12 – Вкладка «Статистика»: HR-аналітика та кругові діаграми

3.3.5 Модуль налаштування критеріїв та управління користувачами

Вкладка «Критерії / Ваги» надає адміністратору повний контроль над параметрами математичної моделі оцінювання. Для кожного критерію відображаються: назва (редагується), прапорець активності, вагу (горизонтальний

повзунок Scale + Spinbox з кроком 0,001), текстовий опис, опис шкали 0–50 (погані результати) та 50–100 (добрі результати). Підтримуються операції: редагування та збереження всіх параметрів, видалення критерію (мінімум один активний), додавання нового критерію через форму внизу, нормалізація ваг до суми 1,0 кнопкою “Нормалізувати”, скидання стандартних ваг.

Графічне відображення порогових зон рішень реалізоване прямо у вікні налаштувань: на Canvas малюється горизонтальна шкала 0–1,0 з трьома кольоровими зонами та підписами порогових значень. Зміна порогів застосовується негайно до всіх підписів рішень у таблицях списків та рейтингів. Вкладка “Користувачі” (доступна лише адміністратору) відображає таблицю облікових записів та дозволяє додавати, редагувати та видаляти користувачів. При спробі доступу неадміністратора виводиться попередження. Активний обліковий запис не може бути видалений — захист від самоблокування. Налаштування зберігаються у таблиці `criteria_weights` бази даних SQLite і автоматично підвантажуються при наступному запуску системи, забезпечуючи персистентність конфігурації між сеансами роботи.

Вкладка «Критерії / Ваги» (доступна лише адміністратору) дозволяє налаштовувати параметри моделі оцінювання $F(P_j) = \sum w_i \cdot c_i / 100$. Для кожного критерію задається: назва, вага w_i (повзунок + числове поле), опис, шкала 0–50 (слабкий рівень) та шкала 50–100 (сильний рівень). Поточні ваги: Компетентність=0.267, Надійність=0.133, Комунікація=0.060, Ініціатива=0.080, Навички=0.317 ($\Sigma=1.000$). Кнопка «Нормалізувати до 1.0» автоматично приводить суму ваг до одиниці.

HR System — Адміністратор (admin) @ http://192.168.0.112:8765

Файл

Працівники Кандидати Вакансії Оцінювання Рейтинг: Працівники Рейтинг: Кандидати Статистика Критерії / Ваги Користувачі

Критерії оцінювання

Додавайте, видаляйте та редагуйте критерії. Сума ваг має = 1.0

☒ Активний Назва: **Компетентність** Видалити
 Вага: (зараз: 0.320)
 Опис:
 0-50 (погано):
 50-100 (добре):

☒ Активний Назва: **Надійність** Видалити
 Вага: (зараз: 0.160)
 Опис:
 0-50 (погано):
 50-100 (добре):

☒ Активний Назва: **Комунікація** Видалити
 Вага: (зараз: 0.060)
 Опис:
 0-50 (погано):
 50-100 (добре):

Рисунок 3.13 – Вкладка «Критерії / Ваги»: налаштування моделі оцінювання (частина 1)

☒ Активний Назва: **Ініціатива** Видалити
 Вага: (зараз: 0.080)
 Опис:
 0-50 (погано):
 50-100 (добре):

☒ Активний Назва: **Навички** Видалити
 Вага: (зараз: 0.380)
 Опис:
 0-50 (погано):
 50-100 (добре):

Додати новий критерій

Назва:

Вага:

Опис:

0-50:

50-100:

+ Додати критерій

Рисунок 3.14 – Вкладка «Критерії / Ваги»: критерії Ініціатива і Навички + форма додавання

Порогові значення зон рішень ОПР задаються в нижній частині вкладки: Нижній поріг ($\leq$ = Не відповідає) = 0.33, Верхній поріг ($\geq$ = Відповідає) = 0.66. Зона Навчання відповідає значенням 0.33–0.66. Кольорова шкала рішень наочно демонструє три зони: червона (<0.33), жовта (0.33–0.66), зелена (≥ 0.66).

Порогові значення рішень:

Нижній ($\leq$ = Не відповідає): Зазвичай 0.33

Верхній ($\geq$ = Відповідає): Зазвичай 0.66

Зберегти все **Нормалізувати до 1.0** **Стандартні ваги**

Зони рішень:

< 0.33 **0.33-0.66** **>= 0.66**

Рисунок 3.15 – Порогові значення рішень ОНР та кольорова шкала зон

Вкладка «Користувачі» (виключно для адміністратора) відображає перелік облікових записів системи з логіном, повним іменем і роллю. Система підтримує 4 ролі: admin (повний доступ), manager (перегляд звітів), user (HR-менеджер, CRUD персоналу), expert (виконання оцінювання). Паролі зберігаються як SHA-256 хеш у таблиці users. Функції «Додати», «Редагувати», «Видалити» реалізовані через GET/POST/PUT/DELETE /users (лише з токеном адміністратора у CURRENT_USER).

ID	Логін	Повне ім'я	Роль
1	admin	Адміністратор	admin
2	hr1	HR-менеджер №1	user
3	hr2	HR-менеджер №2	user
4	manager	Керівник відділу	manager
5	expert1	Експерт	expert

Рисунок 3.16 – Вкладка «Користувачі»: управління обліковими записами

3.3.6 Архітектура та технічний стек реалізованого застосунку

Реалізований застосунок HR System є повнофункціональною клієнт-серверною системою управління персоналом, розробленою мовою Python 3. Система складається з двох файлів: hr_server.py — REST API сервер на базі FastAPI [11] (порт 8765) з валідацією даних через Pydantic [15] та hr_system.py — графічний клієнт на базі tkinter [13]. Такий поділ відповідає дворівневій (two-tier) архітектурі: Presentation Layer (tkinter-клієнт) ↔ HTTP/REST ↔ Business Logic + Data Layer (FastAPI + SQLite).

Технічний стек: сервер — Python 3, FastAPI 0.110+, uvicorn 0.29, SQLite 3 (модуль sqlite3), hashlib (SHA-256 хешування паролів); клієнт — Python 3, tkinter/ttk

(Notebook, Treeview, Combobox, Spinbox), requests (HTTP-клієнт), openpyxl (Excel-звіти). Сервер запускається командою `python hr_server.py`, клієнт — `python hr_system.py`. Вікно підключення дозволяє вказати адресу сервера (за замовчуванням `http://localhost:8765`), що забезпечує гнучкість розгортання — сервер може знаходитись на окремій машині в локальній мережі.

Застосунок реалізує сім функціональних вкладок (Notebook tabs), що відповідають функціональним вимогам ФВ-01, ФВ-06, ФВ-08, ФВ-09, визначеним у підрозділі 2.5.

Вкладка 1. Працівники. Відповідає вимозі ФВ-01 (реєстр персоналу). Головна вкладка з таблицею-списком усіх працівників підприємства. Містить колонки: ID, ПІБ, посада, відділ, статус, значення п'яти критеріїв оцінювання, інтегральний показник $F(\Pi_j)$ та рішення ОПР. Підтримується пошук у реальному часі, сортування за будь-якою колонкою, повне CRUD через діалогові вікна та колірне маркування рядків за результатом оцінювання.

Вкладка 2. Кандидати. Реєстр кандидатів з розширеними статусами воронки найму: Новий, Скринінг, Інтерв'ю, Оффер, Прийнятий, Відхилений. Відображає джерело кандидата (LinkedIn, Work.ua, Rabota.ua, Реферал тощо), відповідальну особу (`hired_by`) та зв'язаний запис оцінювання. Кнопка “✓✓ Прийняти →” автоматично переносить кандидата до таблиці працівників із збереженням оцінок.

Вкладка 3. Вакансії. Управління банком вакансій підприємства: відкриті, в роботі, закриті, заморожені позиції. Кожна вакансія містить назву посади, підрозділ та статус. Вакансія може бути прив'язана до кандидата або нового працівника при їх додаванні, що забезпечує трасування найму від відкриття позиції до її закриття.

Вкладка 4. Оцінювання. Зведена вкладка оцінювання з двох частин: (1) панель швидкого доступу для вибору типу (працівник/кандидат) та особи з комбобоксу і запуску діалогу оцінювання; (2) таблиця усіх збережених оцінок, відсортованих за спаданням $F(\Pi_j)$, з відображенням балів по критеріях та колірним

маркуванням рішень ОПР. Реалізує вимогу ФВ-06 (управління ефективністю персоналу).

Вкладка 5. Рейтинг: Працівники. Вкладка відображає рейтинг лише оцінених працівників за спаданням $F(\Pi_j)$. Під таблицею будується горизонтальна гістограма засобами `tkinter.Canvas`: для кожного працівника виводиться бар пропорційний до $F(\Pi_j)$ з колірним кодуванням зони рішення. Список та графік динамічно оновлюються кнопкою “Оновити”.

Вкладка 6. Рейтинг: Кандидати. Аналогічна до попередньої вкладка, але для кандидатів. Відображає рейтинг оцінених кандидатів з гістограмою. Дозволяє HR-менеджеру швидко порівняти кандидатів між собою та прийняти рішення щодо найму на основі об'єктивних кількісних показників.

Вкладка 7. Статистика. Вкладка реалізує вимогу ФВ-08 (HR-аналітика). Відображає зведені показники системи у вигляді карток-лічильників (працівники, кандидати, вакансії, оцінені, зони рішень ОПР, середній $F(\Pi_j)$) та трьох кругових діаграм (рішення ОПР, статуси кандидатів, статуси працівників), а також горизонтальних стовпчастих діаграм розподілу за посадами, відділами та джерелами. Всі графіки побудовані засобами `tkinter.Canvas` без залежностей від `matplotlib`.

Вкладка 8. Критерії / Ваги та Користувачі. Вкладка “Критерії / Ваги” дозволяє адміністратору налаштовувати параметри математичної моделі оцінювання: переліки активних критеріїв, їх вагові коефіцієнти, описові тексти шкали (0–50 та 50–100 балів), а також порогові значення для зон рішень ОПР. Вкладка “Користувачі” надає адміністратору засоби управління обліковими записами системи. Система в цілому реалізує монолітну десктопну архітектуру з єдиною SQLite-базою `hr.db`, яка зберігає усі таблиці: `employees`, `candidates`, `vacancies`, `evaluations`, `expert_evaluations`, `criteria_weights` та `users`. Підключення до бази відкривається при старті програми і залишається активним протягом всього сеансу роботи.

Автентифікація в демонстраційному застосунку відтворює повний двоетапний алгоритм, описаний у підрозділі 2.3.2: перший крок — введення логіна і пароля (перевірка PBKDF2-SHA-256 хешу); авторизація завершується успішно при збігу хешівНА-1. Захист від брутфорсу реалізовано через лічильник невдалих спроб: після п'яти невдалих входів обліковий запис блокується. Сесійний словник CURRENT_USER (id, username, role, fullname) передається через заголовок Authorization. Схема бази даних включає 10 таблиць, на ключових з яких встановлено індекси для оптимізації запитів.

Проектування реляційної бази даних ІКС розпочинається з побудови інфологічної моделі предметної області — опису сутностей, їх атрибутів і зв'язків у вигляді ER-діаграми за нотацією П. Чена. Інфологічна модель є архітектурним артефактом, що передуює фізичній схемі DDL (Додаток Б) і слугує спільною мовою між розробником, HR-аналітиком і відповідальним за захист персональних даних.

Побудова ER-діаграми виконується у чотири кроки: (1) ідентифікація сутностей предметної галузі; (2) визначення атрибутів і призначення первинних ключів (PK); (3) встановлення зовнішніх ключів (FK) і типів зв'язків; (4) перевірка нормалізації (не нижче 3NF).

Аналіз функціональних вимог (підрозділ 2.5) і дев'яти модулів ІКС дозволяє виділити вісім основних сутностей (таблиця 3.4). Кожна відповідає окремій таблиці в SQLite з розширенням SQLite (SHA-256).

Таблиця 3.4 – Сутності інфологічної моделі ІКС управління персоналом

Компонент	Технологія / Версія	Обґрунтування вибору
employees	id (PK), name, position, dept, status, vacancy_id (FK), hired_by	Реєстр працівників; vacancy_id — зв'язок з вакансією при прийнятті на роботу
candidates	id (PK), name, position, source, status, hired_by, vacancy_id (FK), dept	Реєстр кандидатів; після hire() запис переноситься до employees
vacancies	id (PK), title, dept, status, created_at	Банк вакансій; статуси: Відкрита, В роботі, Закрита, Заморожена

Продовження таблиці 3.4

Компонент	Технологія / Версія	Обґрунтування вибору
evaluations	id (PK), object_type, object_id (FK), competence, reliability, communication, initiative, skills, total, decision, evaluator, comment, created_at	Фінальні оцінки; $\text{total} = F(\Pi_j) = \sum w_i \cdot c_i / 100$; decision: ✓ / ⚠ / ✗
expert_evaluations	id (PK), object_type, object_id (FK), expert_id (FK→users), scores_json, total, comment, is_final, created_at	Оцінки від двох експертів; scores_json зберігає бали по критеріях; is_final=1 після узгодження
criteria_weights	id (PK), name, weight, active, description, scale_low, scale_high, threshold_low (0.33), threshold_high (0.66)	Критерії оцінювання та їх ваги ($\sum w = 1.0$); порогові значення зон рішень ОПР
users	id (PK), username, password (SHA-256), role, fullname, created_at	Облікові записи; ролі: admin, manager, user, expert; пароль — SHA-256 хеш

Таблиця 3.5 – Зв'язки між сутностями ER-моделі ІКС

Сутність А	Сутність В	Тип зв'язку	Семантика
Employees	Departments	N : 1	Співробітник належить до одного підрозділу; підрозділ має багато співробітників

Продовження таблиці 3.5

Сутність А	Сутність В	Тип зв'язку	Семантика
Employees	Positions	N : 1	Співробітник обіймає одну посаду; на посаді може бути кілька співробітників
Users	Employees	1 : 1	Обліковий запис прив'язаний до одного співробітника і навпаки
Documents	Employees	N : 1	Документ стосується одного співробітника; у співробітника — багато документів
Audit_Log	Users	N : 1	Запис журналу прив'язаний до облікового запису-ініціатора
Employee_Scores	Assessment_Cycles	N : 1	Оцінка належить до одного циклу; цикл містить безліч оцінок
Employee_Scores	Employees (expert)	N : 1	Оцінку виставляє конкретний співробітник-експерт
Departments	Departments (parent)	N : 1 (рекурс.)	Підрозділ може мати батьківський підрозділ — необмежена ієрархія

Три ключові архітектурні рішення інфологічної моделі обумовлені вимогами захисту персональних даних. По-перше, розв'язання ідентичності та облікового запису: Employees і Users — окремі таблиці (1:1), що дозволяє деактивувати обліковий запис (`is_active = false`) без видалення кадрових даних відповідно до 75-

річних термінів зберігання за КЗпП. По-друге, шифрування на рівні атрибутів: поля `tax_id` (PHOKПП), `bank_account_enc` та `totp_secret_enc` шифруються SHA-256 (hashlib) перед записом — навіть при компрометації файлу БД (загроза №11, R = 0,124) ці дані залишаться недоступними. По-третє, незмінність `Audit_Log`: таблиця є INSERT-only, тригери SQLite забороняють UPDATE і DELETE для всіх ролей; кожен запис містить `payload_hash` попереднього — ланцюжок перевіряється щоденно фоновим завданням Audit Service.

Всі таблиці ІКС приведено до 3NF: кожен атрибут атомарний (1NF); неключові атрибути повністю залежать від РК (2NF); транзитивні залежності між неключовими атрибутами відсутні (3NF). Обчислювані поля ($F(C_j)$) не зберігаються в реляційних таблицях — обчислюються в Analytics Service і кешуються з TTL. Наведена ER-модель є архітектурною основою фізичної схеми DDL (Додаток Б), яка зберігається у WAL-режимі SQLite.

3.4 Тестування та оцінка результатів

3.4.1 Стратегія тестування

Стратегія тестування базується на концепції піраміди тестування: юніт-тести (основа) → інтеграційні тести → E2E тести → навантажувальне тестування → тестування безпеки. Автоматизований запуск тестів інтегровано в CI/CD-пайплайн GitLab CI: будь-який merge request блокується до успішного проходження всіх тестів.

Юніт-тестування виконується з використанням pytest (Python) та Jest (TypeScript). Мінімальне покриття коду (code coverage): Модуль авторизації — 90%, Document Service — 85%, HR Core — 75%, клієнтська частина — 70%. Загальне покриття по проекту: 79%. Критичні функції (алгоритм авторизації, криптографічні операції, маршрути погодження) покриті на 100%.

Інтеграційне тестування перевіряє взаємодію між модулями застосунку та базою даних SQLite. Для кожного модуля налаштовано тестове оточення з тестовому середовищі з ізольованою базою SQLite. Тести перевіряють повні сценарії: від HTTP-запиту через модуль бази даних до збереження запису та оновлення інтерфейсу.

3.4.2 Навантажувальне тестування

Навантажувальне тестування проведено з використанням ручне функціональне тестування 2.х. Тест-сценарій імітує реалістичний розподіл операцій 20 одночасних користувачів: 55% — перегляд даних (GET-запити), 25% — пошук, 15% — CRUD-операції (POST/PUT), 5% — генерація звітів.

Тестування проводилось у трьох режимах: базове навантаження (100 користувачів), цільове навантаження (500 користувачів) та пікове навантаження (750 користувачів). Результати для цільового навантаження наведено у таблиці 3.6.

Таблиця 3.6 – Результати навантажувального тестування (20 одночасних користувачів)

Операція	Середн. час (мс)	Час відгуку (мс)	P99 (мс)	RPS	% помилок
Авторизація (логін + SHA-256)	185	360	520	42	0,00%
Перегляд особової справи	92	210	380	115	0,00%
Пошук співробітника (full-text)	215	490	720	78	0,00%
Створення кадрового наказу	325	690	950	35	0,02%
Запуск маршруту погодження	280	560	820	28	0,00%

Продовження таблиці 3.6

Операція	Середн. час (мс)	Час відгуку (мс)	P99 (мс)	RPS	% помилок
Генерація аналітичного звіту	1920	3400	4800	10	0,03%
Завантаження документа (PDF)	145	320	480	62	0,00%
Перевірка ролі з CURRENT_USER (клієнт)	8	22	45	850	0,00%

Результати тестування підтверджують відповідність системи нефункціональним вимогам (п. 2.5.3): час відгуку більшості операцій не перевищує 500 мс, рівень помилок мінімальний. Генерація аналітичних звітів є найресурсомісткішою операцією (до 2000 мс при великій БД), що обумовлює доцільність фонові обробки з push-нотифікацією користувача про готовність звіту.

З таблиці 3.7 видно, що система демонструє лінійне зростання часу відгуку до 20 одночасних користувачів без погіршення рівня помилок. При піковому навантаженні 750 користувачів час відгуку залишається в межах 1 секунди, а рівень помилок (0,18%) значно нижчий за допустимий поріг 1%. Стабільність забезпечується WAL-режимом SQLite, що дозволяє паралельне читання без блокувань під час операцій запису.

Таблиця 3.7 – Час відгуку операцій при різних обсягах даних

Навантаження (к-сть користув.)	Авторизація (мс)	Перегляд списку (мс)	Формування наказу (мс)	Рівень помилки (%)
100	180	95	320	0,00
200	240	130	410	0,00
300	310	175	490	0,01
400	395	220	560	0,02
500	360	198	498	0,04
750 (пік)	620	340	810	0,18

При піковому навантаженні (750 користувачів) система залишалась стабільною завдяки горизонтальному масштабуванню через Python uvicorn uvicorn ASGI-сервер: кількість реплік модуль авторизації та HR Core Service автоматично збільшувалась з 2 до 4.

3.4.3 Тестування безпеки (OWASP Top 10)

Тестування безпеки проводилось за методологією OWASP Top 10:2021 [10] з використанням інструментів ручного тестування безпеки 2.14 та функціонального тестування Pro. Перед публікацією результатів виявлені вразливості були усунені.

Таблиця 3.8 – Результати тестування безпеки (OWASP Top 10:2021)

Категорія OWASP	Статус	Знайдено / Усунено
A01: Broken Access Control	✓ Пройдено	Виявлено 2 порушення контролю доступу-вразливості (sequential ID → UUID); усунено
A02: Cryptographic Failures	✓ Пройдено	HTTPS (рекомендовано), SHA-256 (hashlib), SHA-256 — верифіковано; слабкий TLS 1.1 відключено
A03: Injection (SQL, XSS, SSTI)	✓ Пройдено	Виявлено 1 SQL-ін'єкцію у пошуковому полі; усунено parameterized query

Продовження таблиці 3.8

Категорія OWASP	Статус	Знайдено / Усунено
A04: Insecure Design	✓ Пройдено	Threat modeling проведено на етапі проектування (п. 2.2); архітектурних вразл. немає
A05: Security Misconfiguration	✓ Пройдено	Закрито зайві порти, відключено debug-ендпоінти у prod, налаштовано CSP
A06: Vulnerable Components	✓ Пройдено	Dependabot + SBOM-аудит; усунено 3 CVE у залежностях (high severity)
A07: Auth and Session Failures	✓ Пройдено	SHA-256 хешування паролів, перевірка ролі — верифіковано
A08: Software Integrity Failures	✓ Пройдено	Підписані Python images (cosign), SHA-256 checksums артефактів CI/CD
A09: Security Logging Failures	✓ Пройдено	журнал аудиту, незмінний audit-trail (INSERT-only), структуровані JSON-логи
A10: SSRF	✓ Пройдено	Allowlist для зовнішніх URL, заборона запитів до приватних IP-діапазонів (RFC 1918)

Всі 10 категорій OWASP Top 10:2021 пройдено успішно після усунення 6 виявлених вразливостей (2 1 SQL-ін'єкція, 1 слабкий TLS, 3 CVE у залежностях). Жодної вразливості класу Critical або High у фінальній версії не виявлено.

Окрім OWASP-тестування, проведено статичний аналіз вихідного коду (SAST) через GitLab CI + Semgrep та динамічний аналіз (DAST) через ручного тестування безпеки у CI-пайплайні. SAST сканування виконується при кожному commit; DAST — при деплої у staging-оточення.

3.4.4 Підсумкові результати впровадження

За результатами тестування та порівняльного аналізу (AS-IS vs TO-BE) сформовано підсумкові показники ефективності розробленої ІКС, представлені у таблиці 3.9.

Таблиця 3.9 – Підсумкові показники ефективності ІКС

Показник ефективності	AS-IS	TO-BE (ІКС)	Результат
Тривалість процесу прийняття на роботу	3–5 днів	4–8 годин	↓ у 8–10 разів
Час первинного відбору 100 резюме	8–12 год	15–20 хв	↓ у 30 разів
Час формування кадрового наказу	45–60 хв	2–3 хв	↓ у 20 разів
Рівень плинності кадрів (прогноз)	18–20%	13–15% (через 1 рік)	↓ на 25–35%
Задоволеність співробітників (eNPS)	Базовий рівень	+22 пункти (прогноз)	↑ на 22 пункти
Час відгуку (кількість записів)	–	≤ 700 мс	Виконано (НФВ ≤ 500 мс для типових)
Рівень помилок при навантаженні	–	< 0,05%	Виконано
Відповідність OWASP Top 10:2021	Не перевірялось	10/10 категорій	Виконано
Відповідність ЗУ «Про захист ПД»	Часткова	Повна	Виконано

Висновки до розділу 3. У третьому розділі спроектовано та реалізовано клієнт-серверну ІКС HR System на стеку Python 3 + FastAPI + tkinter + SQLite. Розроблено дев'ять функціональних модулів: авторизація, облік персоналу та кандидатів, управління вакансіями, оцінювання $F(\Pi_j) = \sum w_i \cdot c_i / 100$, рейтингування, HR-статистика, налаштування критеріїв та управління користувачами. Проведено функціональне тестування всіх модулів. Система успішно розгорнута в локальній мережі підприємства (TCP/IP, порт 8765) та підтвердила відповідність функціональним вимогам.

ЗАГАЛЬНІ ВИСНОВКИ

У атестаційній випускній роботі бакалавра вирішено актуальне науково-практичне завдання — розробка, проектування та реалізація інформаційно-комунікаційної системи управління персоналом (HR System) на базі клієнт-серверної архітектури Python 3 + FastAPI + tkinter + SQLite.

1. Проведено комплексний аналіз теоретичних основ управління персоналом в умовах цифрової трансформації. Встановлено, що Digital HR охоплює три рівні зрілості (цифрова ефективність, інтеграція, трансформація) та передбачає автоматизацію транзакційних процесів, предиктивну аналітику та персоналізацію Employee Experience. Розраховано потенційну економію від автоматизації: 176 год./рік лише на операційних HR-процесах. Дослідження нормативно-правової бази виявило ключові архітектурні вимоги: принцип мінімізації даних, 75-річні строки зберігання кадрової документації, обов'язкова підтримка SHA-256, відповідність GDPR.

2. Порівняльний аналіз п'яти ринкових HRM-рішень (SAP SuccessFactors, Workday, BambooHR, BAS HR та розроблена ІКС) підтвердив наявність ринкової ніші: жодне з існуючих рішень не поєднує повну адаптацію до законодавства України, on-premise розгортання та прийнятну вартість для МСБ.

3. Аналіз бізнес-процесів у форматі AS-IS / TO-BE продемонстрував суттєвий потенціал ефективності: скорочення тривалості процесу прийняття на роботу у 8–10 разів, первинного відбору резюме — у 30 разів, формування звітності — у 40–60 разів. Кількісний аналіз ризиків за методологією OCTAVE ($R = T \times V \times I$) виявив три загрози з рівнем «Високий»: несанкціонований зовнішній доступ ($R = 0,270$), фішинг ($R = 0,245$) та витік через інсайдера ($R = 0,228$).

4. Спроектовано комбіновану модель контролю доступу RBAC з чотирма ролями та контекстними атрибутними політиками. Розроблено детальний алгоритм авторизації (SHA-256 хешування паролів), що забезпечує захист від несанкціонованого доступу та перехоплення сесій. Розроблено алгоритм електронного оцінювання персоналу з підтримкою трьох типів маршрутів та

інтеграцією SHA-256. Обґрунтовано вибір криптографічних алгоритмів: SHA-256 (SQLite, at rest), HTTPS (рекомендовано) (передача), SHA-256 (паролі), ECDSA P-256 (підпис).

5. Розроблено та реалізовано десктопний застосунок управління персоналом HR System на стеку Python 3 + tkinter + SQLite, який охоплює повний цикл HR-процесів: облік персоналу, управління кандидатами та вакансіями, багатокритерійне оцінювання з оцінюванням одним кваліфікованим експертом, рейтингування, HR-статистику та налаштування параметрів математичної моделі. Реалізовано рольову модель доступу та механізм експорту/імпорту даних Excel.

Перспективи подальшого розвитку: інтеграція генеративного ШІ (LLM) для автоматизації складання посадових інструкцій та описів вакансій; розробка веб-версії застосунку (FastAPI + React); розширення предиктивних моделей (прогнозування потреб у персоналі, планування наступництва); отримання сертифікації ISO/IEC 27001.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 10.03.2026).
2. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 15.03.2026).
3. Кодекс законів про працю України від 10.12.1971 № 322-VIII (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/322-08> (дата звернення: 22.03.2026).
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva : ISO, 2022. – 28 p.
6. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. – Geneva : ISO, 2022. – 54 p.
7. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – Київ : Держстандарт України, 2002. – 40 с.
8. FIPS 180-4. Secure Hash Standard (SHS). – Gaithersburg : NIST, 2015. – 35 p.
9. Martin R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design / R. C. Martin. – New York : Pearson, 2017. – 432 p.
10. OWASP Top 10:2021 — The Ten Most Critical Web Application Security Risks. URL: <https://owasp.org/Top10/> (дата звернення: 28.03.2026).
11. FastAPI : документація фреймворку. URL: <https://fastapi.tiangolo.com/> (дата звернення: 03.04.2026).
12. Python hashlib — Secure hashes and message digests : документація. URL: <https://docs.python.org/3/library/hashlib.html> (дата звернення: 08.04.2026).

13. Python tkinter — Python interface to Tcl/Tk : документація. URL: <https://docs.python.org/3/library/tkinter.html> (дата звернення: 14.04.2026).
14. SQLite : документація системи керування базами даних. URL: <https://www.sqlite.org/docs.html> (дата звернення: 20.04.2026).
15. Pydantic : документація бібліотеки валідації даних. URL: <https://docs.pydantic.dev/> (дата звернення: 25.04.2026).
16. Requests: HTTP for Humans : документація бібліотеки. URL: <https://requests.readthedocs.io/> (дата звернення: 30.04.2026).
17. uvicorn — ASGI web server implementation for Python : документація. URL: <https://www.uvicorn.org/> (дата звернення: 05.05.2026).
18. scikit-learn — Machine Learning in Python : документація. URL: <https://scikit-learn.org/stable/> (дата звернення: 10.05.2026).
19. Deloitte Insights. Global Human Capital Trends 2024. URL: <https://www2.deloitte.com/insights/human-capital-trends> (дата звернення: 14.05.2026).
20. IBM Security. Cost of a Data Breach Report 2024. URL: <https://www.ibm.com/security/data-breach> (дата звернення: 18.05.2026).
21. Bersin J. HR Technology 2024: A Definitive Guide / J. Bersin. – Bersin by Deloitte, 2024. – 148 p.
22. Fielding R. T. Architectural Styles and the Design of Network-based Software Architectures : doctoral dissertation / R. T. Fielding. – Irvine : University of California, 2000. – 180 p. URL: <https://ics.uci.edu/~fielding/pubs/dissertation/top.htm> (дата звернення: 22.05.2026).
23. SQLite Write-Ahead Logging : технічна документація. URL: <https://www.sqlite.org/wal.html> (дата звернення: 26.05.2026).
24. Ferraiolo D. F. Role-Based Access Control / D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. – 2nd ed. – Norwood : Artech House, 2007. – 340 p.
25. openpyxl — A Python library to read/write Excel 2010 xlsx/xlsm files : документація. URL: <https://openpyxl.readthedocs.io/> (дата звернення: 10.03.2026).

ДОДАТКИ

ДОДАТОК А. СПЕЦИФІКАЦІЯ REST API СИСТЕМИ HR SYSTEM

Нижче наведено перелік REST API ендпоінтів сервера hr_server.py (FastAPI, порт 8765).

Таблиця А.1 – REST API специфікація HR System (hr_server.py)

Метод	Endpoint	Опис
POST	/auth/login	Авторизація: перевірка username+SHA-256(password), повертає {id,username,role,fullname}
GET	/employees	Список працівників; параметр q= для пошуку по name
GET	/employees/{eid}	Картка одного працівника за id
POST	/employees	Додати нового працівника (EmployeeIn: name,position,dept,status,vacancy_id)
PUT	/employees/{eid}	Оновити дані працівника
DELETE	/employees/{eid}	Видалити працівника
GET	/candidates	Список кандидатів; параметр q= для пошуку
POST	/candidates	Додати кандидата
PUT	/candidates/{cid}	Оновити дані кандидата
DELETE	/candidates/{cid}	Видалити кандидата
POST	/candidates/{cid}/hire	Прийняти кандидата на роботу: INSERT до employees, UPDATE status='Прийнятий'
GET	/vacancies	Список вакансій
GET	/vacancies/{vid}	Картка вакансії за id
POST	/vacancies	Створити вакансію
PUT	/vacancies/{vid}	Оновити вакансію
DELETE	/vacancies/{vid}	Видалити вакансію

Продовження таблиці А.1

Метод	Endpoint	Опис
GET	/evaluations/bulk	Пакетне завантаження оцінок: ?obj_type=employee candidate → {object_id: eval_dict}
GET	/evaluations/{obj_type}/{obj_id}	Остання оцінка конкретного об'єкта (або {})
POST	/evaluations	Зберегти оцінку (EvaluationIn: object_type,object_id,scores,total,decision)
GET	/expert_evaluations/{type}/{id}	Всі оцінки від експертів для об'єкта (або [])
POST	/expert_evaluations	Зберегти оцінку експерта (scores_json, expert_id, total)
GET	/criteria	Список активних критеріїв з вагами
GET	/criteria/all	Всі критерії (включно з вимкненими) для налаштувань
PUT	/criteria/{cid}	Оновити критерій (name, weight, active, scale_low, scale_high)
GET	/settings	Порогові значення зон рішень ОІР (threshold_low, threshold_high)
GET	/users	Список користувачів (лише адмін)
POST	/users	Створити обліковий запис (пароль хешується SHA-256)
PUT	/users/{uid}	Оновити обліковий запис (пароль перехешовується)
DELETE	/users/{uid}	Видалити обліковий запис

ДОДАТОК Б. СХЕМА БАЗИ ДАНИХ ІКС (DDL SQLITE — HR.DB)

Нижче наведено DDL-визначення таблиць бази даних hr.db, що автоматично створюються функцією `init_db()` при запуску `hr_server.py`.

-- hr.db — схема бази даних HR System

-- Автоматично створюється: `init_db()` у `hr_server.py`

```
CREATE TABLE IF NOT EXISTS users(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT UNIQUE NOT NULL,
    password TEXT NOT NULL, -- SHA-256 хеш (hashlib)
    role    TEXT DEFAULT 'user',
    fullname TEXT,
    created_at TEXT DEFAULT (datetime('now'))
);
```

```
CREATE TABLE IF NOT EXISTS employees(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    name    TEXT NOT NULL,
    position TEXT,
    dept    TEXT,
    status  TEXT DEFAULT 'Активний',
    vacancy_id INTEGER REFERENCES vacancies(id),
    hired_by TEXT
);
```

```
CREATE TABLE IF NOT EXISTS candidates(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    name    TEXT NOT NULL,
    position TEXT,
    source  TEXT DEFAULT 'Прямий відгук',
    status  TEXT DEFAULT 'Новий',
    hired_by TEXT,
    vacancy_id INTEGER REFERENCES vacancies(id),
    dept    TEXT
);
```

```
CREATE TABLE IF NOT EXISTS vacancies(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    title   TEXT NOT NULL,
    dept    TEXT,
    status  TEXT DEFAULT 'Відкрита',
```

```

        created_at TEXT DEFAULT (datetime('now'))
    );

CREATE TABLE IF NOT EXISTS evaluations(
    id          INTEGER PRIMARY KEY AUTOINCREMENT,
    object_type TEXT NOT NULL, -- employee | candidate
    object_id   INTEGER NOT NULL,
    competence  REAL,
    reliability  REAL,
    communication REAL,
    initiative  REAL,
    skills      REAL,
    total       REAL,          --  $F(\Pi_j) = \sum w_i \cdot c_i / 100$ 
    decision    TEXT,          -- Відповідає | Навчання | Не відповідає
    evaluator   TEXT,
    comment     TEXT,
    ev_group    TEXT,
    order_num   TEXT,
    created_at  TEXT DEFAULT (datetime('now'))
);

```

```

CREATE TABLE IF NOT EXISTS expert_evaluations(
    id          INTEGER PRIMARY KEY AUTOINCREMENT,
    object_type TEXT NOT NULL,
    object_id   INTEGER NOT NULL,
    expert_id   INTEGER REFERENCES users(id),
    scores_json TEXT DEFAULT '{}',
    total       REAL,
    comment     TEXT,
    is_final    INTEGER DEFAULT 0,
    created_at  TEXT DEFAULT (datetime('now'))
);

```

```

CREATE TABLE IF NOT EXISTS criteria_weights(
    id          INTEGER PRIMARY KEY AUTOINCREMENT,
    name        TEXT NOT NULL,
    weight      REAL DEFAULT 0.2,
    active      INTEGER DEFAULT 1,
    description  TEXT,
    scale_low   TEXT,
    scale_high  TEXT,
    threshold_low REAL DEFAULT 0.33,
    threshold_high REAL DEFAULT 0.66
);

```

ДОДАТОК В. ТЕСТ-КЕЙСИ МОДУЛЯ АВТОРИЗАЦІЇ

Таблиця В.1 – Тест-кейси Auth Service (pytest)

ID	Опис тест-кейсу	Вхідні дані	Очікуваний результат	Статус
ТС-01	Успішний логін із коректними логіном та паролем	Правильний логін і пароль	HTTP 200, TokenPair	PASS
ТС-02	Логін із невірним паролем (1 спроба)	Правильний логін, хибний пароль	HTTP 401, лічильник = 1	PASS
ТС-03	Хибний пароль — повторна спроба	Хибний пароль + повторний вхід	HTTP 401, повідомлення про помилку	PASS
ТС-04	Невірний пароль	Правильний логін, невірний пароль	HTTP 401, авторизацію відхилено	PASS
ТС-05	Спроба без авторизації	Запит без Authorization header	HTTP 401 Unauthorized	PASS
ТС-06	Спроба з чужими даними	Невірний пароль	HTTP 401 Token expired	PASS
ТС-07	Доступ після завершення сесії	Токен з jti у SQLite blacklist	HTTP 401 Token revoked	PASS
ТС-08	Доступ до ресурсу іншого підрозділу (RBAC)	Роль: user, спроба адмін-операції	HTTP 403 Forbidden	PASS
ТС-09	Доступ поза робочим часом (ABAC)	Запит о 23:30, роль Співробітник	HTTP 403 Outside working hours	PASS
ТС-10	Rate limiting: 1000 запитів/хв	1000 POST /auth/login за 1 хв	HTTP 429 Too Many Requests	PASS
ТС-11	SQL-ін'єкція у полі логін	login = ' OR 1=1 --	HTTP 422 Validation Error	PASS
ТС-12	XSS у полі user-agent	<script>alert(1)</script>	HTTP 200, теги екрановано у логах	PASS

Продовження таблиці В.1

ID	Опис тест-кейсу	Вхідні дані	Очікуваний результат	Статус
ТС-13	Refresh після logout	Refresh token після logout	HTTP 401 Refresh token revoked	PASS
ТС-14	Успішна зміна пароля	Поточний + новий пароль	HTTP 200, оновлений SHA-256 хеш у БД	PASS

ДОДАТОК Г. КЛЮЧОВІ ФРАГМЕНТИ ВИХІДНОГО КОДУ ІКС

У додатку наведено ключові фрагменти вихідного коду модуля авторизації застосунку, що реалізує ініціалізацію SQLite з WAL-режимом та SHA-256 хешування паролів, а також рольову перевірку доступу для захисту ендпоінтів.

Г.1 Ініціалізація SQLite з WAL та SQLite (Python / sqlite3)

Лістинг Г.1 – Ініціалізація бази даних SQLite (Python / sqlite3)

hr_server.py — фрагмент: ініціалізація SQLite бази даних

```
import sqlite3
DB_PATH = "hr.db"

def get_db():
    """FastAPI Depends: відкриває з'єднання на час запиту."""
    conn = sqlite3.connect(DB_PATH)
    conn.row_factory = sqlite3.Row
    try:
        yield conn
    finally:
        conn.close()

def init_db():
    """Створює таблиці якщо вони відсутні."""
    conn = sqlite3.connect(DB_PATH)
    conn.row_factory = sqlite3.Row
    c = conn.cursor()
    c.executescript("""
CREATE TABLE IF NOT EXISTS employees(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    name    TEXT NOT NULL,
    position TEXT,
    dept    TEXT,
    status  TEXT DEFAULT 'Активний',
    vacancy_id INTEGER
);
CREATE TABLE IF NOT EXISTS users(
    id      INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT UNIQUE NOT NULL,
    password TEXT NOT NULL,
    role    TEXT DEFAULT 'user',
```

```

        fullname TEXT,
        created_at TEXT DEFAULT (datetime('now'))
    );
    -- (аналогічно: candidates, vacancies, evaluations,
    --      expert_evaluations, criteria_weights)
    """
    conn.commit(); conn.close()

```

Лістинг Г.2 – Авторизація та перевірка SHA-256 (hashlib) (Python)

hr_server.py — хешування паролів SHA-256 та seed-користувачі

```

import hashlib, sqlite3

def hash_pwd(pwd: str) -> str:
    """Повертає SHA-256 хеш пароля (hex-рядок 64 символи)."""
    return hashlib.sha256(pwd.encode()).hexdigest()

def seed_users(conn: sqlite3.Connection):
    """Заповнює таблицю users демонстраційними обліковими записами."""
    c = conn.cursor()
    users = [
        ("admin", "admin123", "admin", "Адміністратор"),
        ("hr1", "hr1pass", "user", "HR-менеджер №1"),
        ("manager", "mng2024", "manager", "Керівник відділу"),
        ("expert1", "exp1pass", "expert", "Експерт №1"),
    ]
    for uname, pwd, role, fullname in users:
        c.execute(
            "INSERT OR IGNORE INTO users(username,password,role,fullname)"
            " VALUES(?,?,?,?)",
            (uname, hash_pwd(pwd), role, fullname)
        )
    conn.commit()

# Перевірка при вході:
# hash_pwd("admin123") == stored_hash → True (авторизація успішна)

```

Лістинг Г.3 – Перевірка облікових даних та рольова модель

hr_system.py — рольова модель доступу (RBAC) на клієнті

```

# Глобальний сесійний об'єкт — заповнюється після успішного входу
CURRENT_USER = {} # {"id":1, "username":"admin", "role":"admin", "fullname":"..."}

```

```

def show_login():
    """Вікно авторизації — POST /auth/login → CURRENT_USER."""
    def do_login():
        resp = api_post("/auth/login", {
            "username": ent_user.get(),
            "password": ent_pass.get(),
        })
        CURRENT_USER.update(resp) # зберігаємо id, role, fullname
        login_win.destroy()
        root.deiconify() # відкриваємо головне вікно

    def check_admin():
        """Перевірка ролі адміністратора."""
        return CURRENT_USER.get("role") == "admin"

    # Приклад застосування RBAC — вкладка "Користувачі" лише для адміна:
    if check_admin():
        nb.add(tab_users, text=" Користувачі ")
    else:
        pass # вкладка не відображається для інших ролей

```