ПЕРЕЛІК СКОРОЧЕНЬ

№ з/п	Скорочення	Зміст скорочення
1	API	Прикладний програмний інтерфейс (англ. Application programming interface)
2	AWS	Amazon Web Services
3	CMS	Система керування контентом (англ. Content Management System)
4	DDoS	Розподілена атака типу “відмова в обслуговуванні” (англ. Distributed Denial of Service)
5	JSON	JavaScript Object Notation
6	MVP	Мінімально життєздатний продукт (англ. Minimum Viable Product)
7	АРМ	Автоматизоване робоче місце
8	БД	База даних
9	ВОС	Військово-облікова спеціальність
10	ГУІТ	Головне управління інформаційних технологій
11	ДСК	Департамент стратегічних комунікацій
12	ДССЗЗІ	Державна служба спеціального зв’язку та захисту інформації України
13	ЗСУ	Збройні Сили України
14	ІКС	Інформаційно-комунікаційна система
15	ІКТ	Інформаційно-комунікаційні технології
16	ІТ	Інформаційні технології
17	КЕП	Кваліфікований електронний підпис
18	КСЗІ	Комплексна система захисту інформації
19	МОУ	Міністерство оборони України
20	НД	Нормативний документ
21	ПЗ	Програмне забезпечення
22	СКБД	Система керування базами даних
23	ТЗ	Технічне завдання
24	ТЗІ	Технічний захист інформації
26	ЦКБ	Центр реагування на кіберінциденти

ЗМІСТ

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Повна назва системи та її умовне найменування

Повна назва: Інформаційно-комунікаційна система "Українське Військо"
Умовне найменування: ІКС "Українське Військо"
Веб-адреса системи: https://army.gov.ua/

1.2. Код (номер) договору

220/65/53

1.3. Найменування зацікавлених сторін

1.3.1 Розпорядник ІКС

Департамент стратегічних комунікацій Міністерства оборони України

1.3.2 Споживач ІКС

- Департамент стратегічних комунікацій Міністерства оборони України

1.3.3 Володілець інформації в ІКС

Департамент стратегічних комунікацій Міністерства оборони України

1.3.4 Користувачі ІКС

- Військовозобов'язані громадяни України
- Діючі військовослужбовці ЗСУ
- Адміністратори та редактори контенту Міністерства оборони України

1.3.5 Замовник ІКС

Департамент стратегічних комунікацій Міністерства оборони України

1.3.6 Відповідальний за проєктування ІКС

Головне управління інформаційних технологій Міністерства оборони України

1.3.7 Відповідальний за впровадження захисту інформації та кіберзахист в ІКС

Головне управління інформаційних технологій Міністерства оборони України, Центр реагування на кіберінциденти

1.3.8 Військове представництво

Не застосовується

1.3.9 Відповідальний за реагування на інциденти кібербезпеки

Центр реагування на кіберінциденти

1.4 Перелік документів, на підставі яких створюється система

- Конституція України
- Закон України "Про оборону України"
- Закон України "Про Збройні Сили України"
- Закон України "Про військовий обов'язок і військову службу"
- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"
- Закон України "Про захист персональних даних"
- Закон України "Про електронні довірчі послуги"
- Закон України "Про основні засади забезпечення кібербезпеки України"
- Постанова Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"
- НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу"
- НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу"
- ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги"

1.7 Порядок оформлення і пред'явлення результатів робіт

Результати робіт оформлюються у вигляді:

- Актів виконаних робіт за кожним етапом
- Протоколів випробувань (попередніх, дослідної експлуатації, приймальних)
- Комплекту проєктної та експлуатаційної документації
- Програмного забезпечення та вихідного коду
- Навчальних матеріалів для користувачів та адміністраторів

Всі документи надаються в 3-х примірниках у паперовому вигляді та в електронному вигляді на оптичних носіях.

2. ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ ІКС

2.1. Призначення ІКС

ІКС "Українське Військо" призначена для створення єдиного інформаційного порталу з питань мобілізації, служби за контрактом та рекрутингу до лав Збройних Сил України. Система забезпечує інформаційну підтримку процесів залучення громадян до військової служби та надання актуальної інформації діючим військовослужбовцям.

2.2. Мета створення ІКС

Метою створення ІКС "Українське Військо" є:

- Централізація інформації про військову службу в єдиному веб-порталі
- Підвищення ефективності рекрутингових процесів ЗСУ
- Забезпечення прозорості та доступності інформації про умови служби
- Автоматизація процесу подачі заявок на військову службу
- Інтеграція з існуючими системами обліку військових вакансій
- Покращення інформування громадян про різні форми військової служби

3. СФЕРА ВИКОРИСТАННЯ

3.1. Об'єкти, на яких передбачається розгортання

- Хмарна інфраструктура AWS (основне розгортання)

- Робочі місця адміністраторів та редакторів контенту в підрозділах Міністерства оборони України
- Публічний доступ через мережу Інтернет для всіх категорій користувачів

3.2. Процеси (завдання), що цифровізуються

- Інформування громадян про умови та порядок проходження військової служби
- Подача заявок на контрактну службу та участь у мобілізаційних заходах
- Вибір військово-облікової спеціальності через інтерактивний опитувальник
- Отримання актуальної інформації про військові вакансії
- Надання відповідей на типові запитання щодо військової служби
- Збір та обробка анкетних даних потенційних військовослужбовців

4. ВИМОГИ ДО СИСТЕМИ В ЦІЛОМУ

4.1. Загальний опис вимог

Система повинна:

- Забезпечувати цілодобовий доступ користувачів через веб-інтерфейс
- Підтримувати одночасну роботу до 10 000 користувачів
- Обробляти до 1 000 000 щоденних відвідувань
- Забезпечувати час відгуку не більше 3 секунд при стандартних операціях
- Мати адаптивний дизайн для коректного відображення на різних пристроях
- Забезпечувати доступність системи на рівні 99.9%
- Відповідати вимогам WCAG 2.1 рівня AA для доступності

4.2. Вимоги верхньорівневої архітектури

Система будується на основі трирівневої архітектури:

Презентаційний рівень:

- Веб-інтерфейс користувача (React.js або Next.js)
- Адаптивний дизайн (responsive design)

- Підтримка сучасних браузерів (Chrome, Firefox, Safari, Edge)

Рівень бізнес-логіки:

- Headless CMS Strapi 5 як основа
- RESTful API для взаємодії з клієнтськими додатками
- Інтеграційний шар для взаємодії з зовнішніми системами

Рівень даних:

- База даних Amazon RDS for PostgreSQL версії 16 LTS або вище
- для зберігання структурованих даних
- Об'єктне сховище AWS S3 для медіафайлів
- Система кешування Redis для оптимізації продуктивності

4.3. Вимоги до складу системи

Система повинна включати наступні компоненти:

Функціональні модулі:

- Модуль управління контентом (CMS)
- Модуль обробки форм та заявок
- Модуль інтеграції з LobbyX
- Модуль інтерактивного вибору ВОС (wizard)
- Модуль пошуку та фільтрації
- Модуль аналітики та звітності

Інфраструктурні компоненти:

- Веб-сервер (AWS EC2 або ECS)
- Балансувальник навантаження (AWS ALB)
- CDN для статичного контенту (CloudFlare)
- Система резервного копіювання (AWS Backup)
- Система моніторингу (AWS CloudWatch)

4.4. Технічні вимоги до складових системи

Вимоги до CMS Strapi:

- Версія не нижче 5.0
- Підтримка української локалізації інтерфейсу адміністратора
- Можливість створення користувацьких типів контенту
- Підтримка медіа-бібліотеки з категоризацією
- Версіонування контенту та можливість відкату змін
- Підтримка ролей та прав доступу

Вимоги до бази даних:

- Amazon RDS for PostgreSQL версії 16 LTS або вище
- Підтримка репликації для забезпечення відмовостійкості
- Автоматичне резервне копіювання кожні 6 годин
- Шифрування даних at rest

Вимоги до хостингу AWS:

- Розміщення в регіоні EU
- Використання Auto Scaling для масштабування
- Multi-AZ deployment для високої доступності
- Для захисту від веб-атак використовується рішення класу Web Application Firewall, а саме Cloudflare WAF у складі плану Cloudflare Enterprise

4.5. Вимоги до захисту інформації, кібербезпеки та кіберзахисту

Система повинна забезпечувати:

Захист від DDoS-атак:

- Використання CloudFlare Enterprise план
- Налаштування Rate Limiting
- Захист форм через CloudFlare Turnstile

Аутентифікація та авторизація:

- Двофакторна аутентифікація для адміністраторів
- Парольна політика (мінімум 12 символів, різні регістри, цифри, спецсимволи)

- Автоматичне блокування після 5 невдалих спроб входу
- Сесії з обмеженим часом життя (30 хвилин неактивності)

Шифрування:

- HTTPS для всіх з'єднань (TLS 1.2 мінімум)
- Шифрування бази даних та резервних копій
- Шифрування персональних даних користувачів

Аудит та моніторинг:

- Логування всіх адміністративних дій
- Моніторинг аномальної активності
- Збереження логів протягом 1 року
- Система повинна забезпечувати обов'язкове автоматизоване сканування вразливостей із застосуванням методів динамічного та статичного аналізу коду перед кожним випуском нової версії програмного забезпечення та після впровадження оновлень функціональних можливостей системи
- Для системи має проводитись тестування на проникнення з періодичністю не рідше одного разу на рік, а також регресійне тестування безпеки після кожного значного випуску оновлень системи
- Весь програмний код системи підлягає обов'язковій перевірці на безпеку перед інтеграцією до основної гілки розробки з метою виявлення бекдорів, шкідливого коду, вразливостей та недоліків архітектури безпеки
- Інформаційно-комунікаційна система "Українське Військо" має бути інтегрована з інформаційно-комунікаційною системою "Система виявлення вразливостей та реагування на кіберінциденти та кібератаки Міністерства оборони України", (шифр – "CSOC") для забезпечення безперервного моніторингу подій безпеки, централізованого виявлення кіберінцидентів, своєчасного реагування на кіберзагрози
- Система має забезпечувати детальне журналювання всіх запитів до прикладних програмних інтерфейсів із фіксацією часу запиту, ідентифікатора користувача або системи, типу операції, параметрів запиту, отриманої відповіді та коду стану обробки запиту
- Система повинна вести детальний журнал дій користувачів, включаючи спроби автентифікації (успішні та невдалі), операції зміни даних у системі, виконання критичних операцій адміністрування, зміну налаштувань безпеки та доступу до конфіденційної інформації з обов'язковим зазначенням часової мітки, ідентифікатора користувача та IP-адреси джерела
- Веб-сайт та програмні інтерфейси системи підлягають обов'язковому захисту засобами Cloudflare, що включає застосування Web Application Firewall для фільтрації шкідливого трафіку, захист від розподілених атак типу "відмова в обслуговуванні" (DDoS), обмеження частоти запитів (rate-limiting) для запобігання зловживанням та автоматизованим атакам

- Система має забезпечувати детальне журналювання всіх операцій з базо. даних Amazon RDS for PostgreSQL версії 16 LTS або вище
- , включаючи запити на читання, запис, зміну та видалення даних, а також операцій із об'єктним сховищем AWS S3, зокрема завантаження, видалення та модифікацію файлів з обов'язковою фіксацією ідентифікатора ініціатора операції та часової мітки
- Архітектура безпеки системи та розроблене програмне забезпечення повинні відповідати вимогам проєкту OWASP Top 10 щодо десяти найпоширеніших вразливостей веб-додатків та стандарту OWASP Application Security Verification Standard у частині перевірки безпеки додатків
- У системі має бути реалізована процедура управління оновленнями безпеки (патч-менеджмент), що передбачає систематичний моніторинг доступних оновлень програмного забезпечення, своєчасне застосування критичних патчів безпеки протягом 72 годин з моменту їх випуску розробником, планове оновлення некритичних компонентів та ведення реєстру застосованих оновлень

Захист персональних даних:

- Відповідність вимогам Закону України "Про захист персональних даних"
- Анонімізація даних для аналітики

4.6. Вимоги до надійності

- Доступність системи: 99.9% (не більше 8.76 годин простою на рік)
- Середній час між відмовами (MTBF): не менше 720 годин
- Середній час відновлення (MTTR): не більше 1 години
- RPO (Recovery Point Objective): 6 годин
- RTO (Recovery Time Objective): 2 години
- Автоматичне перемикання на резервні компоненти при збоях

4.7. Вимоги до модернізації системи

- Модульна архітектура для легкого додавання нового функціоналу
- Підтримка версіонування API для забезпечення зворотної сумісності
- Можливість горизонтального масштабування
- Документована процедура оновлення системи без втрати даних
- Підтримка blue-green deployment для безперервного оновлення

4.8. Вимоги до технічного адміністрування

Інтерфейс адміністрування повинен забезпечувати:

- Управління користувачами та ролями
- Моніторинг стану системи в реальному часі
- Перегляд та аналіз логів
- Управління резервними копіями
- Налаштування параметрів безпеки
- Генерацію звітів про роботу системи

Автоматизація:

- Автоматичне резервне копіювання за розкладом
- Автоматичне очищення старих логів та тимчасових файлів
- Автоматичні сповіщення про критичні події

4.9. Вимоги до сумісності з іншими системами

Інтеграція з LobbyX:

- Отримання даних через публічний API (JSON)
- Періодична синхронізація даних (кожні 30 хвилин)
- Кешування отриманих даних
- Обробка помилок при недоступності API

Інтеграція з Microsoft 365:

- Використання Graph API для відправки email
- OAuth 2.0 для аутентифікації
- Підтримка шаблонів листів

4.10. Вимоги до живучості та стійкості від зовнішніх впливів

- Географічно розподілене розміщення компонентів
- Використання CloudFlare для захисту та кешування

- Автоматичне масштабування при збільшенні навантаження
- Graceful degradation при недоступності зовнішніх сервісів
- Резервні канали зв'язку для критичних компонентів

5. ВИМОГИ ДО ФУНКЦІЙ ІКС

5.1. Перелік функціональних підсистем

5.1.1. Підсистема управління контентом

- Створення та редагування сторінок
- Управління медіафайлами (фото, відео, документи)
- Версіонування контенту
- Планування публікацій
- Управління меню та навігацією

5.1.2. Підсистема обробки заявок

- Прийом та валідація даних форм
- Відправка заявок на email через Microsoft 365 Graph API
- Збереження деперсонифікованих заявок в базі даних
- Формування звітів по заявках

5.1.3. Підсистема інтерактивного вибору ВОС (Wizard)

- Дерево питань з логікою розгалуження (до 4 рівнів)
- Кожен рівень містить 5-8 варіантів відповіді
- Збереження прогресу проходження
- Видача рекомендацій на основі відповідей
- Можливість повернення на попередні кроки
- Налаштування дерева питань через JSON файл який зберігається в базі даних
- Інтерфейс редагування JSON файла дерева питань

5.1.4. Підсистема інтеграції з LobbyX

- Автоматичне отримання списку вакансій через API
- Парсинг JSON з полями: назва посади, опис, логотип, посилання, вид-рід військ, спеціальність, звання, умови
- Відображення вакансій з фільтрацією та пошуком
- Переадресація на LobbyX для подачі заявки

5.1.5. Підсистема пошуку

- Повнотекстовий пошук по контенту сайту
- Фільтрація результатів за типом контенту
- Пошукові підказки (автодоповнення)
- Збереження історії пошуків для аналітики

5.2. Вимоги до організації вхідних та вихідних даних

Вхідні дані:

- Текстовий контент від редакторів (markdown, HTML)
- Медіафайли (зображення до 10MB, відео до 500MB, PDF до 50MB)
- Дані форм від користувачів (валідація на клієнті та сервері)
- JSON-дані від LobbyX API

Вихідні дані:

- HTML-сторінки для браузерів
- Email-повідомлення з даними заявок

Валідація даних:

- Перевірка форматів email, телефонів
- Захист від SQL-injection та XSS
- Обмеження розмірів завантажуваних файлів
- Перевірка типів файлів (whitelist)
- Усі файли, що завантажуються користувачами до системи, підлягають обов'язковій автоматизованій перевірці антивірусним програмним забезпеченням на наявність шкідливого коду та верифікації відповідності заявленого типу файлу його фактичному вмісту шляхом аналізу MIME-типу

та сигнатури файлу для запобігання завантаженню замаскованих виконуваних файлів та шкідливих скриптів

5.3. Вимоги до розмежування доступу

Ролі користувачів:

1. **Адміністратор** (до 2 осіб):
   - Повний доступ до всіх функцій системи
   - Управління користувачами та ролями
   - Налаштування системних параметрів
   - Доступ до логів та аудиту
2. **Редактор** (до 10 осіб):
   - Створення та редагування контенту
   - Завантаження медіафайлів
   - Перегляд статистики
   - Не має доступу до системних налаштувань
3. **Відвідувач** (необмежено):
   - Перегляд публічного контенту
   - Заповнення форм
   - Проходження wizard
   - Пошук інформації

6. ВИМОГИ ДО ВИДІВ ЗАБЕЗПЕЧЕННЯ

6.1. Вимоги до інформаційного забезпечення

Структура бази даних повинна включати:

- Таблиці для зберігання контенту (сторінки, новини, FAQ)
- Таблиці для користувачів та ролей
- Таблиці для заявок та анкетних даних
- Таблиці для логів та аудиту
- Таблиці для кешу вакансій з LobbyX

Вимоги до даних:

- Використання UTF-8 для всього текстового контенту
- Нормалізація бази даних до 3NF

- Індексація полів для оптимізації пошуку
- Партиціонування таблиць логів за датою

6.2. Вимоги до програмного забезпечення

Серверне ПЗ:

- Операційна система: Ubuntu Server 22.04 LTS або Amazon Linux 2023
- Node.js версії 18 LTS або вище
- Strapi CMS версії 5.0 або вище
- Amazon RDS for PostgreSQL версії 16 LTS або вище
- Redis 7.0 або вище
- Nginx або AWS Application Load Balancer

Клієнтське ПЗ:

- Підтримка браузерів: Chrome 90+, Firefox 88+, Safari 14+, Edge 90+
- JavaScript повинен бути увімкнений
- Підтримка cookies для збереження сесій

6.3. Вимоги до лінгвістичного забезпечення

- Інтерфейс користувача: виключно українською мовою
- Інтерфейс адміністратора: українська мова
- Весь контент: українська мова
- Повідомлення про помилки: українська мова
- Технічна документація: українська мова

6.4. Вимоги до правового забезпечення

Система повинна відповідати вимогам:

- Законодавства України про захист персональних даних
- Законодавства про електронні довірчі послуги
- Нормативних документів ДСТЗЗІ
- Авторських прав на використовувані компоненти

Розробник повинен передати Замовнику всі майнові права на розроблене ПЗ.

6.5. Вимоги до метрологічного забезпечення

Моніторинг та логування:

- Централізований збір логів з усіх компонентів
- Моніторинг доступності (uptime monitoring)
- Моніторинг продуктивності (response time, throughput)
- Моніторинг використання ресурсів (CPU, RAM, disk, network)
- Алерти при перевищенні порогових значень

Метрики для моніторингу:

- Кількість одночасних користувачів
- Час відгуку сторінок (P50, P95, P99)
- Кількість помилок (4xx, 5xx)
- Використання CPU/RAM
- Розмір бази даних та швидкість росту
- Кількість поданих заявок

Інструменти:

- AWS CloudWatch для інфраструктурного моніторингу
- Application Performance Monitoring (APM) для моніторингу додатку
- Централізоване логування через AWS CloudWatch Logs

6.6. Вимоги до організаційного забезпечення

Організаційна структура підтримки:

- Призначення відповідальних за адміністрування
- Призначення відповідальних за контент
- Визначення процедур резервного копіювання
- Регламент реагування на інциденти
- План навчання користувачів

Документація:

- Інструкція адміністратора системи

- Інструкція редактора контенту
- Керівництво користувача
- Регламент технічного обслуговування

6.7. Вимоги до технічного забезпечення

Мінімальні вимоги до АРМ користувача:

- Процесор: 2 ядра, 2 GHz
- Оперативна пам'ять: 4 GB
- Роздільна здатність екрану: 1366x768
- Підключення до Інтернет: 10 Mbps

Мінімальні вимоги до АРМ адміністратора:

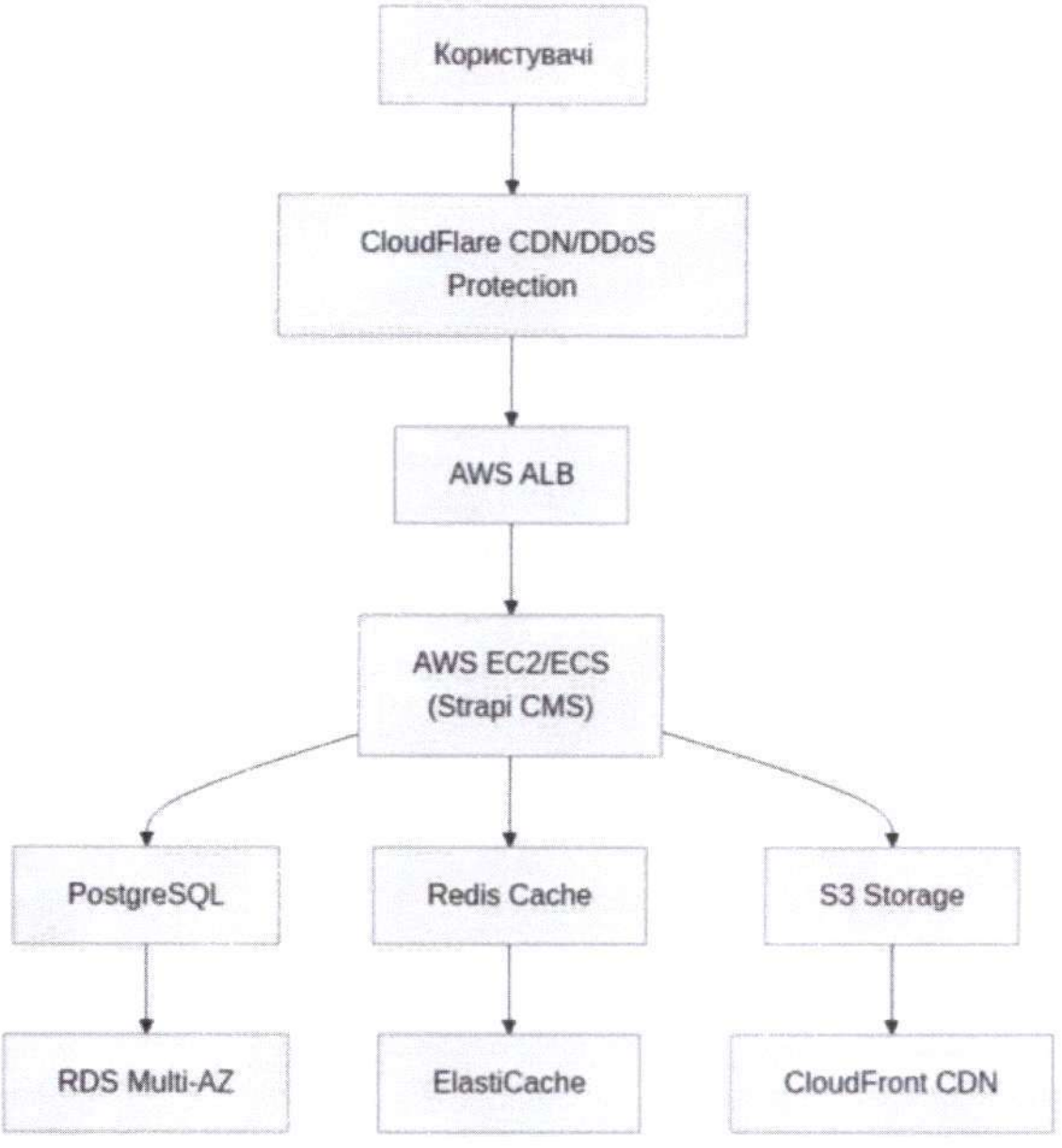
- Процесор: 4 ядра, 2.5 GHz
- Оперативна пам'ять: 8 GB
- Роздільна здатність екрану: 1920x1080
- Підключення до Інтернет: 50 Mbps

Серверна інфраструктура AWS:

- EC2 інстанси: мінімум t3.large для продуктивного середовища
- RDS для Amazon RDS for PostgreSQL версії 16 LTS або вище: db.t3.medium з Multi-AZ
- ElastiCache для Redis: cache.t3.micro
- S3 для зберігання медіафайлів
- CloudFront для CDN

7. ВИМОГИ ДО РОЗГОРТАННЯ СИСТЕМИ, ПОРЯДКУ СТВОРЕННЯ ТА ЗМІСТУ РОБІТ

7.1. Структурна схема розгортання Системи



7.2. Діаграма розгортання Системи

Система розгортається в AWS регіоні EU (EU-central-1 - Frankfurt):

Продуктивне середовище:

- 2x EC2 instances за Load Balancer
- Amazon RDS for PostgreSQL версії 16 LTS або вище
- ElastiCache Redis cluster
- S3 bucket для медіафайлів
- CloudFront distribution
- Auto Scaling Group (2-10 instances)

Тестове середовище:

- 1x EC2 instance
- Amazon RDS for PostgreSQL версії 16 LTS або вище
- Single-AZ
- ElastiCache Redis single node
- Окремий S3 bucket

7.3. Порядок створення та зміст робіт

№ з/п	Стадія розробки	Зміст робіт	Термін робіт
1	Ініціювання	- Формування проєктної команди - Деталізація вимог - Узгодження технологічного стеку - Підготовка інфраструктури AWS - Налаштування середовищ розробки	3 робочих днів
2	Проєктування	- Розробка дизайн-системи та макетів - Проєктування архітектури системи - Проєктування структури БД - Розробка API специфікації	7 робочих днів

№ з/п	Стадія розробки	Зміст робіт	Термін робіт
		- Планування інтеграцій	
3	Розробка MVP	- Встановлення та налаштування Strapi CMS - Розробка базових сторінок-Реалізація форм заявок - Базова інтеграція з LobbyX - Розгортання на staging	20 робочих днів
4	Розробка повної версії	- Реалізація wizard вибору BOC - Повна інтеграція з Microsoft 365 - Впровадження системи безпеки - Оптимізація продуктивності - Налаштування моніторингу	17 робочих днів
5	Тестування	- Функціональне тестування-Тестування безпеки - Навантажувальне тестування - Тестування сумісності - UAT тестування	7 робочих днів
6	Впровадження	- Розгортання на production - Міграція даних - Навчання користувачів - Підготовка документації - Запуск в промислову експлуатацію	7 робочих днів
Всього			**61 робочий день**

8. ВИМОГИ ДО ДОКУМЕНТУВАННЯ

Виконавець повинен розробити та надати наступну документацію:

Технічна документація:

- Архітектурний опис системи
- Опис API та інтеграцій

- Схема бази даних
- Інструкція з розгортання
- Інструкція з резервного копіювання та відновлення

Експлуатаційна документація:

- Керівництво адміністратора
- Керівництво редактора контенту
- Керівництво користувача
- Регламент технічного обслуговування
- План аварійного відновлення

Проєктна документація:

- Технічний проєкт
- Протоколи випробувань
- Акти виконаних робіт
- Звіт про навчання персоналу

Вся документація надається:

- У 3-х примірниках у паперовому вигляді
- В електронному вигляді (формати: DOCX, PDF)
- Українською мовою

9. ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ

Вимоги щодо забезпечення охорони державної таємниці під час виконання робіт не висуваються, оскільки система не передбачає обробку інформації з обмеженим доступом.

Тимчасово виконуючий обов'язки
заступника директора департаменту –
начальника управління Артем ШЕВЧУК