

ЗАТВЕРДЖУЮ

Голова Державної служби
спеціального зв'язку та захисту
інформації України

Юрій МИРОНЕНКО

«серпень» 2024 р.**ЗАТВЕРДЖУЮ**

Генеральний директор
ДП «УСС»

Михайло ДМИТРИЧЕНКО

«серпень» 2024 р.**ТЕХНІЧНІ ВИМОГИ**

**на модернізацію програмного забезпечення інформаційної системи
«Програмна платформа для розгортання та супроводження державних
електронних реєстрів»
(для версії 1.9.8)**

Терміни, визначення та скорочення

Терміни та скорочення	Визначення
Автентифікація	Електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних;
Інформаційна система «Програмна платформа для розгортання та супроводження державних електронних реєстрів» (далі – Платформа)	Інформаційно-комунікаційна система, призначена для уніфікованого, автоматизованого та стандартизованого процесу створення, адміністрування та ведення публічних електронних реєстрів з використанням загальних принципів проектування, програмування та захисту інформації в публічних електронних реєстрах
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
Інстанс	Примірник інстальованого програмного забезпечення, що функціонує як відокремлена інформаційно-комунікаційна система
ICEI	Інтегрована система електронної ідентифікації
КЕП	Кваліфікований електронний підпис в розумінні Закону України «Про електронні довірчі послуги»
КЗЗ	Комплекс засобів захисту

Терміни та скорочення	Визначення
НД	Нормативна документація
Публічний електронний реєстр (далі – реєстр)	Інформаційно-комунікаційна система, що забезпечує збирання, накопичення, захист, облік, відображення, оброблення реєстрових даних та надання реєстрової інформації
Програмний продукт, ПЗ	Програмне забезпечення, результат комп'ютерного програмування у вигляді операційної системи, системної, прикладної, розважальної та/або навчальної комп'ютерної програми (їх компонентів), а також у вигляді інтернет-сайтів та/або онлайн-сервісів та доступу до них, примірники (копії, екземпляри) комп'ютерних програм, їх частин, компонентів у матеріальній та/або електронній формі, у тому числі у формі коду (кодів) та/або посилань для завантаження комп'ютерної програми та/або їх частин, компонентів у формі коду (кодів) для активації комп'ютерної програми чи в іншій формі, криптографічні засоби захисту інформації;
ТЗІ	Технічний захист інформації
API	Application Programming Interface - опис способів взаємодії однієї комп'ютерної програми з іншими
SOAP	Simple Object Access Protocol- це протокол обміну XML-повідомленнями, якігії використовується для обміну структурованою і тішизованою інформацією між системами
ПІБ	Прізвище, ім'я, по батькові
Віджет	Візуальний компонент, що реалізує певну функцію, наприклад віджет автентифікації id.gov.ua
URL	Uniform Resource Locator - унікальний ідентифікатор (ім'я) мережевого ресурсу
Control plane	Панель керування налаштуваннями реєстру
ФОП	Фізична особа - підприємець
ФО	Фізична особа
Пайплайн	Від англійського pipeline тобто певний процес із певною послідовністю дій. Наприклад пайплайн розгортання реєстру - певна послідовність дій та перевірок, які мають пройти автоматично для розгортання реєстру

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Передумови

Надійна робота цифрових реєстрів є запорукою сталого функціонування України, особливо під час воєнного стану. Працюючі реєстри дозволяють гарантовано надавати адміністративні послуги громадянам та бізнесу в Україні. Реєстри є запорукою захисту прав та свобод юридичних та фізичних осіб та є інструментами, направленими, в тому числі, і на відновлення України. На виконання пункту 43 Плану пріоритетних дій Уряду на 2021 рік, затвердженого розпорядженням Кабінету Міністрів України від 24 березня 2021 р. № 276-р, забезпечено налагодження роботи електронних реєстрів шляхом створення платформи для побудови великих майстер-реєстрів. Також постановою Кабінету Міністрів України від 18 квітня 2023 р. № 356 затверджено Положення про інформаційну систему «Програмна платформа для розгортання та супроводження державних електронних реєстрів».

З метою підтримки розвитку системи публічних електронних реєстрів, зокрема підвищення якості ведення існуючих реєстрів та створення нових, Платформа потребує оновлень функціоналу та модернізації.

1.2. Загальні положення

У цьому документі наведені вимоги законодавства (розділ 2), функціональні (розділ 3) і нефункціональні (розділ 4) вимоги щодо модернізації програмного продукту.

Реалізоване програмне забезпечення повинно відповідати таким загальним вимогам:

- веб-орієнтованість;
- універсальність;
- функціональна достатність (повнота);
- надійність (автоматично зберігати всі дані та коректно завершувати роботу без втрати даних);
- придатність до модернізації та масштабування;
- модульність;
- мати інтуїтивно зрозумілий для користувача інтерфейс;
- захищеність від зовнішніх впливів;
- фіксація всіх дій користувачів.

1.3. Мета

Основною метою модернізації програмного забезпечення Платформи є розширення вже існуючих функціональних можливостей та розробка нового функціоналу, включаючи розширення можливостей компонентів, з яких побудована Платформа, у тому числі Open Source компонентів.

1.4. Призначення

Програмне забезпечення Платформи призначено для розгортання інстансів Платформи, що забезпечують створення, адміністрування та ведення публічних електронних реєстрів, інформаційно-комунікаційних систем.

1.5. Обмеження

Програмні продукти розроблені/поставлені третіми особами, включені до Програмного продукту, мають розповсюджуватись/використовуватись на умовах безоплатної ліцензії, яка зокрема, не передбачає виплату будь-якої винагороди правовласнику. Строк таких ліцензій має бути не меншим строку чинності виключних майнових прав інтелектуальної власності на Програмний продукт, що поставляється за цими вимогами. Ліцензія має поширюватись на території всіх держав світу, зокрема на територію України.

До програмних продуктів з відкритим кодом, що розповсюджуються за ліцензіями Open Source мають бути дотримані вимоги їх використання відповідно до діючих ліцензій використання.

2. ВИМОГИ ЗАКОНОДАВСТВА

Програмне забезпечення повинне відповідати вимогам таких нормативно-правових актів:

- Закон України «Про публічні електронні реєстри»;
- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закон України «Про захист персональних даних»;
- Закон України «Про електронні довірчі послуги»;
- Закон України «Про електронні документи та електронний документообіг»;
- Постанова Кабінету Міністрів України від 01.09.2023 № 969 «Про функціонування Реєстру публічних електронних реєстрів»;
- Постанова Кабінету Міністрів України від 04.02.1998 № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»;
- Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;
- Постанова Кабінету Міністрів України від 18.04.2023 р. № 356 «Деякі питання створення та функціонування державних електронних платформ для ведення публічних електронних реєстрів»;

- Постанова Кабінету Міністрів України від 8 вересня 2016 р. № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів»;
- Постанова Кабінету Міністрів України від 21 липня 2023 р. № 757 «Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі»;
- Постанова Кабінету Міністрів України від 12 серпня 2009 р. № 869 «Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів»;
- Постанова Кабінету Міністрів України від 10 вересня 2003 р. № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади».

Цей перелік не є вичерпним. Вимоги законодавства можуть бути уточнені.

3. ФУНКЦІОНАЛЬНІ ВИМОГИ

3.1. Оновлення кабінетів користувачів

1) Забезпечення можливості оновлення кабінетів користувачів для більш гнучкої адаптації під вимоги двомовності (українська англійська):

а) потрібно додати та адаптувати відповідні елементи управління та елементи дизайну, які мають працювати з урахуванням ключових аспектів двомовності (українська та англійська);

б) потрібно розглянути систему кабінетів користувачів як продукт, що дозволяє адміністраторам під час створення реєстру задати мову інтерфейсу та кабінетів з однієї з передбачених (українська англійська) у частині:

- елементів управління: додавання і адаптація елементів управління для підтримки двомовності;

- елементи дизайну: розширення елементів дизайну для підтримки двомовності. Це означає адаптацію графічних елементів, шрифтів, іконок та іншого візуального контенту.

2) Забезпечення стабільної роботи кабінетів користувачів в веб-браузері Safari на базі операційних систем родини macOS. Оскільки кількість користувачів, що використовують у своїй роботі ноутбуки Apple становить суттєву частину, необхідно забезпечити стабільну роботу на таких пристроях у штатному веб-браузері Safari.

3.2. Оновлення та розширення веб-інтерфейсів управління Платформою

1) Адаптація інтерфейсу Адміністративного порталу для сумісності із кабінетами користувачів. Для забезпечення гарного користувацького досвіду усіх

користувачів Платформи, в тому числі адміністраторів та розробників, необхідно забезпечити в адміністративному інтерфейсі зміни внесені в кабінети громадянина та посадових осіб передбачені пунктом 3.1. 1).

2) Розширення веб-інтерфейсу "Підсистеми управління Платформою та реєстрами" підтримкою регіону обслуговування. Для більш комфортного управління мовами та представленнями потрібно створити можливість задати для реєстру регіон обслуговування, щоб автоматично відображати користувачу інтерфейси потрібною мовою.

3) Можливість вибору мови для реєстру та застосування її для веб-інтерфейсу моделювання регламенту.

4) Можливість вибору мови для інтерфейсу адміністративної панелі керування кластером та реєстрами.

5) Налаштування назви та логотипу для інтерфейсу адміністративної панелі керування кластером та реєстрами. Користувачам необхідно завжди чітко ідентифікувати систему, в якій вони працюють в даний момент і для цього необхідно надати можливість виділити для користувача такі значущі елементи як назва та логотип.

6) Можливість налаштування логотипу для кабінетів користувачів та Адмін Порталу. Користувачам необхідно завжди чітко ідентифікувати систему, в якій вони працюють в даний момент і для цього необхідно надати можливість виділити для користувача такі значущі елементи як назва та логотип.

7) Забезпечення базового управління ресурсами реєстру на рівні операційної конфігурації реєстру через Control Plane. Необхідно забезпечити більш зручне управління ресурсами реєстру не через конфігураційні файли, а через візуальні інструменти.

3.3. Оновлення підсистеми управління користувачами та ролями

Адаптація "Підсистеми управління користувачами та ролями" згідно налаштованого регіону обслуговування.

3.4. Оновлення підсистеми Автентифікації користувачів

Забезпечення автентифікації користувачів за допомогою сервісу ICEI id.gov.ua для отримувачів послуг та управління ключами шифрування.

3.5. Оновлення підсистеми побудови користувацьких форм

1) Перенесення кнопки збереження даних на формі з системних в кастомні кнопки форми для кабінетів користувачів. Кнопка збереження даних на формі

необхідна для забезпечення можливості проміжного збереження даних в процесі заповнення форм, але потрібно надати можливість моделювальнику самостійно визначати ті етапи в бізнес-процесі, де таке збереження має сенс та цінність для користувача для забезпечення кращого користувацького досвіду.

2) Можливість додавати в компонентах моделювання форм логіку для disabled стану елементів форм. В деяких випадках моделювальнику потрібно впливати на поведінку елементів форм в залежності від дій користувачів і керувати можливістю забороняти або дозволяти зміни в деяких елементах на формі в залежності від попередніх дій користувача.

3) Можливість побудови умови пошуку (Search Condition), яка може повернути контент файлу. Доволі часто моделювальнику потрібно виконати пошук та повернути користувачу файл, який вже збережений в базі даних реєстру і для цього потрібно надати можливість такого пошуку та відповідні механізми доставки такого файлу користувачу.

3.6. Оновлення підсистеми побудови API

1) Забезпечення розмежування доступу до API бізнес-процесів для зовнішніх систем. Для систем із великою кількістю різноманітних інтеграцій необхідно забезпечити більші можливості розмежування доступу до різних бізнес процесів.

2) Забезпечення налаштування рейту лімітів для окремих API не через Трембіту, до окремих бізнес процесів, окремих умов пошуку (Search Condition) та файлів.

3) Автоматична публікація REST API документації сервісів в загальну документацію проєкту (Антора).

3.7. Оновлення підсистеми побудови звітності Redash

1) Забезпечити можливість використання окремого аналітичного екземпляру PostgreSQL для побудови звітності. Для забезпечення більшої стійкості до можливих навантажень необхідно забезпечити виконання запитів до звітів на базі окремого аналітичного екземпляру бази даних.

2) Забезпечення підтримки двомовності (українська та англійська) інтерфейсів перегляду звітів для посадових осіб (Redash-Viewer) та інтерфейсу для створення та налаштування аналітичних звітів та дашбордів (Redash-Admin). Покращення в кабінетах користувачів та адміністративних інтерфейсах, пов'язаних із забезпеченням двомовності мають бути розповсюджені і на інтерфейси побудови звітності.

3.8. Оновлення інсталятора та компонента роботи з базою даних

- 1) Оновлення модуля роботи із базою коду (codebase operator).
- 2) Розширення інсталятора Платформи можливістю задати регіон обслуговування.

4. НЕФУНКЦІОНАЛЬНІ ВИМОГИ

4.1. Вимоги до інтерфейсу

Інтерфейси мають відповідати вимогам:

- Постанова Кабінету Міністрів України від 21 липня 2023 р. № 757 «Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі»;
- ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021-03), IDT). Інформаційні технології.

4.2. Вимоги до інформаційної безпеки

4.2.1. Захист від найбільш поширених типів атак.

Реєстр має бути захищена від найбільш поширених типів атак, наприклад SQL injection, XSS, отримання доступу методом перебирання паролів, тощо.

4.2.2. Непублічність інформації, що послаблює інформаційну безпеку.

Інформація, що послаблює інформаційну безпеку (така, як id сесії, id користувача, тощо), не повинна відображатись публічно.

4.3. Вимоги до інформаційного забезпечення

В рамках поставки мають бути надані:

- Інструкція по розгортанню Платформи на кластері для адміністратора Платформи в VSphere;
- Інструкція по розгортанню Платформи на кластері для адміністратора Платформи в AWS;
- Інструкція по ревью реєстру в розробці, етапності та переліку необхідних експертів для таких ревью;
- Референтний приклад для вводу дати (Україна);
- Референтний приклад та покращення компонента Textfield для вводу номера телефону (Україна);
- Пам'ятка виведення Платформи та реєстрів у промислову експлуатацію;
- Референтний приклад бізнес-процесу самореєстрації з додатковою модерацією іншим уповноваженим користувачем Кабінету користувача для уникнення

безконтрольної самореєстрації усіх власників ключа фізичної особи в кабінеті реєстру.

4.4. Вимоги до комплексу засобів захисту.

Конкретні вимоги до комплексу засобів захисту будуть визначені у технічному завданні.

5. ТЕХНОЛОГІЧНИЙ СТЕК

Технологічний стек Платформи складається з наступних компонентів: Openshift (OKD), Kubernetes, Docker, PostgreSQL, Camunda, Form.io,дія, Node.js, Groovy, Grafana, Kibana, Elasticsearch, Kafka, Gerrit, Swagger, Postman, Keycloak, Ceph, Kong, Velero.

При цьому важливо, щоб виконувалися ключові вимоги:

- Транзакційна модель змін у реєстрах, інформаційно-комунікаційних системах, тобто усі зміни фіксуються як окремі транзакції і можна відновити послідовність таких дій.
- Журнал транзакцій захищений від змін.
- Розподіл прав у Реєстрі та платформи в цілому повинен відбуватися на RBAC підходу.
- Моніторинг дій системних ролей, тобто тих ролей, які потрібні для налаштування Платформи.
- Шифрування:
 - даних у базі даних;
 - даних при передачі даних;
 - резервних копій.

6. ВИМОГИ ДЛЯ ПРИЙМАННЯ ПЗ

6.1. ПЗ повинно передаватися разом з виключними майновими правами інтелектуальної власності на всі частини/компоненти ПЗ за виключенням прав на ПЗ, що оприлюднене в Open Source.

ПЗ повинно мати таку документацію:

- загальна інструкція по встановленню, налаштуванню, резервному копіюванню даних та відновленню інформації;
- інструкції користувачів, адміністраторів, адміністраторів безпеки;
- висновок про проведення експертизи КЗЗ програмного забезпечення інформаційної системи «Програмна платформа для розгортання та супроводження державних електронних реєстрів» на відповідність вимогам НД ТЗІ 2.5-004-99.

6.2. Розгортання ПЗ

Розгортання створеного Програмного продукту має бути реалізовано самостійно.

6.3. Вимоги до гарантійної підтримки

Все програмне забезпечення (конфігурації), що буде розгорнуто при створенні системи, має забезпечуватись гарантійною підтримкою (виправлення помилок програмного забезпечення та оновлення версій) протягом не менше 12 календарних місяців з моменту підписання видаткової накладної.

**Начальник центру
побудови і розвитку НЦ та
інформаційно-комунікаційних систем**

 **Олексій МЕЛЬНИК**

Директор з виробництва

 **Павло ПОЛІВОД**