**Технічні вимоги**

**на створення**

**програмного продукту «Модуль інформаційного обміну»**

**та**

**програмного продукту «Модуль збору інформації»**

**Київ 2025**

Зміст

[Скорочення та термінологія 4](#_Toc206943989)

[1 Загальні відомості про зміст робіт 6](#_Toc206943990)

[1.1 Повне найменування об’єкта інформатизації 6](#_Toc206943991)

[1.2 Інформація про замовника 6](#_Toc206943992)

[1.3 Перелік документів, які мають враховуватись під час розробки 6](#_Toc206943993)

[2 Призначення та цілі інформатизації 7](#_Toc206943994)

[2.1 Призначення 7](#_Toc206943995)

[2.2 Цілі інформатизації 7](#_Toc206943996)

[3 Характеристики об’єкта інформатизації 8](#_Toc206943997)

[4 Вимоги до засобу інформатизації 11](#_Toc206943998)

[4.1 Вимоги до структури та функціонування засобу інформатизації 11](#_Toc206943999)

[4.2 Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи 13](#_Toc206944000)

[4.3 Вимоги до безпеки 14](#_Toc206944001)

[4.3.1 Вимоги до розмежування та контролю доступу 14](#_Toc206944002)

[4.3.2 Вимоги до автентифікації та авторизації 15](#_Toc206944003)

[4.3.3 Вимоги до шифрування та захисту даних 15](#_Toc206944004)

[4.3.4 Вимоги до логування та аудиту 16](#_Toc206944005)

[4.3.5 Сумісність з антивірусним захистом та межі відповідальності 16](#_Toc206944006)

[4.3.6 Інші вимоги до безпеки 16](#_Toc206944007)

[4.4 Вимоги до ергономіки та технічної естетики 18](#_Toc206944008)

[4.5 Вимоги до захисту інформації 19](#_Toc206944009)

[4.6 Вимоги до стандартизації та уніфікації 19](#_Toc206944010)

[4.7 Вимоги до надійності засобу інформатизації та збереженості інформації 21](#_Toc206944011)

[4.7.1 Загальні вимоги до надійності 21](#_Toc206944012)

[4.7.2 Критерії надійності 22](#_Toc206944013)

[4.7.3 Відновлення після збоїв 22](#_Toc206944014)

[4.7.4 Вимоги до можливостей резервного копіювання та відновлення 23](#_Toc206944015)

[4.8 Вимоги до способів і засобів зв’язку для інформаційного обміну між компонентами засобу інформатизації 23](#_Toc206944016)

[4.9 Вимоги до режимів функціонування та продуктивності засобу інформатизації 23](#_Toc206944017)

[4.10 Вимоги до функцій (завдань), що виконуються засобом інформатизації 25](#_Toc206944018)

[4.10.1 Орієнтовна принципова схема пропонованого рішення 25](#_Toc206944019)

[4.10.2 Загальні вимоги до функціональності ПП 31](#_Toc206944020)

[4.10.3 Загальні вимоги до програмного продукту «Модуль інформаційного обміну» 33](#_Toc206944021)

[4.10.4 Функціональні вимоги до Програмного продукту «Модуль інформаційного обміну» 36](#_Toc206944022)

[4.10.5 Принципи роботи з даними 38](#_Toc206944023)

[4.10.6 Загальні вимоги до програмного продукту «Модуль збору інформації» 44](#_Toc206944024)

[4.10.7 Функціональні вимоги до Програмного продукту «Модуль збору інформації» 45](#_Toc206944025)

[5 Вимоги до розробки та передачі послуг 55](#_Toc206944026)

[5.1 Вимоги до розробки 55](#_Toc206944027)

[5.2 Вимоги до передачі 55](#_Toc206944028)

[5.2.1 Вимоги до порядку розгортання 55](#_Toc206944029)

[5.2.2 Вимоги до функціонального тестування 56](#_Toc206944030)

[5.2.3 Вимоги до тестування на проникнення ПП 56](#_Toc206944031)

[5.2.4 Порядок приймання 56](#_Toc206944032)

[5.2.5 Вимоги до підтримки виробником 57](#_Toc206944033)

[5.2.6 Вимоги до навчання персоналу 57](#_Toc206944034)

[5.3 Вимоги до гарантійної підтримки 57](#_Toc206944035)

[6 Висновки 61](#_Toc206944036)

[7 Додатки 62](#_Toc206944037)

[7.1 Додаток 1. Макет інформаційної картки по суб’єкту перевірки 62](#_Toc206944038)

[7.2 Додаток 2. Перелік зовнішніх джерел інформації 63](#_Toc206944039)

[7.3 Додаток 3. Графік реалізації етапів 64](#_Toc206944040)

[7.4 Додаток 4. Вимоги до потенційних виконавців 65](#_Toc206944041)

# Скорочення та термінологія

|  |  |
| --- | --- |
| Скорочення | Визначення |
| API | Інтерфейс програмування (англ. Application Programming Interface) |
| АРМ | Автоматизоване робоче місце |
| БД | База даних |
| Виконавець | Юридична особа, яка буде обрана за результатами відкритого конкурсу для розробки та впровадження ПП. |
| ВККСУ | Вища кваліфікаційна комісія суддів України |
| Джерела інформації | Електронний реєстр - інформаційно-комунікаційна система, що забезпечує збирання, накопичення, захист, облік, відображення, оброблення реєстрових даних та надання реєстрової інформації |
| ДП ІСС | Державне підприємство «Інформаційні судові системи» |
| ДСА | Державна судова адміністрація України |
| ЄСІКС | Єдина судова інформаційно-комунікаційна система або Єдина судова інформаційно-телекомунікаційна система (до моменту уніфікації назви в нормативно-правових актах) |
| Закон | Закон України «Про судоустрій і статус суддів» |
| Замовник | Для програмного продукту «Модуль інформаційного обміну»:  • Державна судова адміністрація України.  Для програмного продукту «Модуль збору інформації»:  • Вища кваліфікаційна комісія суддів України. |
| ЗДІ | Зовнішні джерела інформації |
| ЗКЗІ | Засіб криптографічного захисту інформації |
| Інтерфейс | Набір правил і протоколів, що забезпечують взаємодію між користувачем і комп'ютером або між різними програмними компонентами |
| Інші модулі ЄСІКС | Інші спеціалізовані програмні модулі ЄСІКС, які реалізують ініціалізацію запитів через програмний продукт «Модуль інформаційного обміну» до зовнішніх джерел інформації та аналіз отриманих відповідей від них |
| ІС | Інформаційна система |
| КЕП | Кваліфікований електронний підпис |
| КНЕДП | Кваліфікований надавач електронних довірчих послуг |
| КСЗІ | Комплексна система захисту інформації |
| Логування | Процес запису інформації про події, які відбуваються в операційній системі, програмах або мережах (англ. logging) |
| ОС | Операційна система; програмне забезпечення, яке управляє апаратними ресурсами комп'ютера або сервера та забезпечує виконання програм. Вона є основою для роботи інших програм і забезпечує інтерфейс між користувачем і комп'ютерним обладнанням |
| ПЗ | Програмне забезпечення; набір інструкцій, даних або програм, які використовуються для управління комп'ютерним обладнанням та виконання певних завдань. Воно включає в себе операційні системи, прикладні програми та утиліти, які забезпечують функціонування комп'ютерної системи та взаємодію з користувачем |
| ПП | Програмний продукт «Модуль збору інформації» та Програмний продукт «Модуль інформаційного обміну» |
| Програмний продукт | 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 |
| Програмний продукт «Модуль збору інформації» | Програмний продукт, який реалізує збір та опрацювання отриманої з ЗДІ інформації для проведення перевірки інформації щодо дотримання суддею (кандидатом на посаду судді) правил професійної етики та відповідності судді (кандидата на посаду судді) критерію доброчесності, в тому числі відповідність витрат і майнового стану судді (кандидата на посаду судді) та членів його сім’ї. |
| Програмний продукт «Модуль інформаційного обміну» | Програмний продукт, який реалізує електронну інформаційну взаємодію з зовнішніми джерелами інформації (реєстри, бази даних, інше) |
| РНОКПП | Реєстраційний номер облікової картки платника податків |
| САРП (ВККСУ) | Система автоматизації робочих процесів Вищої кваліфікаційної комісії суддів України |
| СКБД | Система керування базами даних |
| Транзакція | Завершений логічний блок операцій у інформаційній системі, виконання яких забезпечує цілісність і узгодженість даних. Кожна транзакція має унікальний номер для ідентифікації та реєстрації у разі помилки або некоректної обробки. |
| Трембіта | Система електронної взаємодії державних електронних інформаційних ресурсів (Міністерство цифрової трансформації України) |
| ЦОД | Центр обробки даних |

# Загальні відомості про зміст робіт

## Повне найменування об’єкта інформатизації

Повне найменування об’єкта інформатизації:

* Програмний продукт «Модуль інформаційного обміну»;
* Програмний продукт «Модуль збору інформації».

(далі по тексту разом – ПП).

## Інформація про замовника

Інформація про замовника програмного продукту «Модуль інформаційного обміну»:

* Державна судова адміністрація України (далі – ДСА).

Інформація про замовника програмного продукту «Модуль збору інформації»:

* Вища кваліфікаційна комісія суддів України (далі – ВККСУ).

## Перелік документів, які мають враховуватись під час розробки

При проектуванні та створенні ПП мають враховуватися вимоги таких чинних нормативно-правових документів:

* Закон України «Про судоустрій і статус суддів» (далі – Закон);
* Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;
* Закон України «Про запобігання корупції»;
* Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
* Закон України «Про захист персональних даних»;
* Закон України «Про інформацію»;
* Закон України «Про публічні електронні реєстри»;
* Закон України «Про доступ до публічної інформації»;
* Закон України «Про основні засади забезпечення кібербезпеки України»;
* Указ Президента України від 27.09.1999 № 1229 «Про затвердження Положення про технічний захист інформації в Україні» (зі змінами);
* Постанова Кабінету Міністрів України від 21 лютого 2025 р. № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» (зі змінами);
* Постанова Кабінету Міністрів України від 26.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах» (зі змінами);
* Постанова Кабінету Міністрів України від 27 січня 2010 р. № 55 «Про впорядкування транслітерації українського алфавіту латиницею» (зі змінами);
* ДСТУ ISO/IEC/IEEE 12207:2018 «Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів»;
* ДСТУ ISO/IEC 40500:2015 «Інформаційні технології. Настанова з доступності веб-контенту W3C (WCAG) 2.0»;
* ДСТУ ISO/IEC 27001:2022 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги.;
* Рішення Вищої ради правосуддя від 17 січня 2019 № 141/0/15-19 «Про затвердження Положення про Державну судову адміністрацію України» (зі змінами).

# Призначення та цілі інформатизації

## Призначення

ПП призначені для автоматизації процесу введення, передавання, опрацювання, представлення інформації і доступу до неї про суддів та кандидатів на посаду судді, у тому числі членів їхніх сімей та близьких (ч.1 Стаття 86 Закону України «Про судоустрій і статус суддів») осіб, з відкритих та спеціалізованих реєстрів та інформаційних систем.

ПП забезпечують:

* ініціалізацію запитів до уповноважених державних органів та електронних реєстрів;
* отримання відповідей на запити та результатів їх обробки;
* автоматизовану обробку отриманих даних;
* формування уніфікованого звіту (інформаційної картки по суб’єкту перевірки; надано в Додатку 1).

ПП орієнтовані на використання ДСА та ВККСУ в межах повноважень, визначених Законом України «Про судоустрій і статус суддів» та Законом України «Про запобігання корупції», для проведення добору кандидатів для призначення на посаду судді, проведення кваліфікаційного оцінювання, ведення суддівського досьє та досьє кандидата на посаду судді, а також здійснення інших повноважень, визначених Законом.

## Цілі інформатизації

Основними цілями інформатизації є:

1. Підвищення ефективності перевірки суддів і кандидатів на посаду судді за рахунок автоматизації процесів збору та аналізу даних із зовнішніх джерел.
2. Забезпечення прозорості визначених Законом процедур перевірки.
3. Забезпечення достовірності інформації, що використовується у визначених Законом процедурах добору суддів, призначення та переведення на посаду судді, кваліфікаційного оцінювання суддів.
4. Зниження адміністративного навантаження на працівників ВККСУ шляхом автоматизації повторюваних операцій.
5. Підвищення якості та повноти оцінювання суддів і кандидатів на посаду судді за рахунок використання широкого спектру джерел даних, включно з реєстрами нерухомості, транспортних засобів, деклараціями, даними про родинні зв’язки тощо.
6. Можливість інтеграції з іншими зовнішніми джерелами інформації (далі – ЗДІ), зокрема через «Трембіта», для забезпечення актуальності та оперативності отриманої інформації.
7. Створення єдиного уніфікованого звіту з можливістю перегляду, аналізу, збереження та експорту отриманої інформації в структурованому вигляді.
8. Забезпечення правомірної та безпечної обробки персональних даних відповідно до вимог законодавства.
9. Забезпечення релевантності: інформація, яка надходить, оброблюється та зберігається в суддівському досьє повинна відповідати цілям її збирання та не бути надмірною для реалізації мети ведення суддівського досьє.

# Характеристики об’єкта інформатизації

ДСА є державним органом у системі правосуддя, який здійснює організаційне та фінансове забезпечення діяльності органів судової влади в межах повноважень, установлених законом, з метою створення належних умов функціонування судів і діяльності суддів (пункт 1 Положення про Державну судову адміністрацію України).

Одним з основних завдань ДСА є забезпечення належних умов діяльності судів, Вищої кваліфікаційної комісії суддів України, Національної школи суддів України та органів суддівського самоврядування в межах повноважень, визначених законом (пункт 2 Положення про Державну судову адміністрацію України).

ДСА відповідно до визначених завдань, в тому числі, забезпечує впровадження електронного суду, здійснює заходи щодо організації обміну електронними документами між судами та іншими державними органами і установами (підпункт 12 пункту 5 Положення про Державну судову адміністрацію України).

ВККСУ проводить перевірку відомостей щодо особи, яка претендує на зайняття посади, яка передбачає зайняття відповідального або особливо відповідального становища, та посад з підвищеним корупційним ризиком відповідно до статті 793 Закону.

Відповідно до статті 75 Закону після ухвалення рішення про допуск кандидатів на посаду судді до спеціальної перевірки ВККСУ надсилає до уповноважених державних органів запити на отримання відомостей стосовно кандидатів щодо їх відповідності вимогам, визначеним Законом, та достовірності поданих особою документів.

Перелік уповноважених державних органів, строки та вимоги до інформації, що повинна бути надана або отримана, визначаються ВККСУ з урахуванням інформації, що міститься в досьє кандидатів на посаду судді або суддівському досьє.

У разі отримання ВККСУ відомостей шляхом електронної взаємодії з автоматизованими інформаційними і довідковими системами, реєстрами та банками даних, держателями (адміністраторами) яких є органи державної влади, інші державні органи або органи місцевого самоврядування, письмові запити до відповідних органів не надсилаються.

Для формування суддівського досьє (досьє кандидата на посаду судді), проведення спеціальної перевірки, перевірки повідомлень недостовірності тверджень в деклараціях доброчесності та родинних звʼязків ВККСУ також має право безоплатно отримувати інформацію стосовно судді (кандидата на посаду судді) та членів його сім’ї або близьких осіб у порядку, передбаченому статтею 86 Закону, в тому числі ВККСУ має право безоплатно отримувати інформацію та копії документів і матеріалів (у тому числі з обмеженим доступом) щодо судді (кандидата на посаду судді) та членів його сім’ї або близьких осіб від будь-яких осіб, які є власниками або розпорядниками інформації (документів, матеріалів), що запитуються.

Відповідно до статті 85 Закону суддівське досьє має містити інформацію щодо дотримання суддею правил професійної етики та відповідності судді критерію доброчесності, в тому числі відповідність витрат і майна судді та членів його сім’ї, а також близьких осіб задекларованим доходам, у тому числі копії відповідних декларацій, поданих суддею відповідно до законодавства у сфері запобігання корупції.

Відповідно до пункту 3 частини п’ятої статті 85 Закону досьє кандидата на посаду судді має містити матеріали проведення спеціальної перевірки та іншу інформацію щодо відповідності кандидата на посаду судді критерію доброчесності, зокрема, відповідність витрат і майна кандидата на посаду судді та членів його сім’ї задекларованим доходам, у тому числі копії декларацій, поданих відповідно до цього Закону та законодавства у сфері запобігання корупції

Відповідно до статті Стаття 60 Закону повна перевірка декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, яка подається суддею, здійснюється НАЗК, та полягає у з’ясуванні достовірності задекларованих відомостей, точності оцінки задекларованих активів, перевірці на наявність конфлікту інтересів та ознак незаконного збагачення.

З метою підготовки проведення спеціальної перевірки стосовно кандидата на посаду судді, відповідно до статті 793 Закону, статей 56–58 Закону України «Про запобігання корупції» ВККСУ може отримати від НАЗК наступну інформацію:

* інформацію щодо наявності в Єдиному державному реєстрі осіб, які вчинили корупційні або пов’язані з корупцією правопорушення, відомостей про кандидата;
* інформацію щодо достовірності відомостей, зазначених кандидатом у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, за минулий рік;
* відомості, які можуть указувати на відповідність або невідповідність кандидата критеріям професійної етики, компетентності або доброчесності (за наявності).

Поєднана інформація з декларації особи та результатів перевірки НАЗК інформації, вказаної декларантом в декларації, в тому числі інформації, щодо майна членів його сім’ї, є для ВККСУ достовірним джерелом інформації, щодо майнового стану судді (кандидата) та членів його сім’ї та відповідності витрат. Натомість, отримана від НАЗК інформація, щодо майнового стану особи, стосується виключно результату перевірки декларації особи, в якій особа вказує членів своєї сім’ї у відповідності до ст. 1 Закону «Про запобігання корупції», примітки до ст. 46 Закону «Про запобігання корупції», а саме:

* осіб, які перебувають у шлюбі із суб’єктом декларування (чоловік / дружина) станом на останній день звітного періоду, – незалежно від спільного проживання із суб’єктом декларування упродовж звітного періоду;
* дітей суб’єкта декларування до досягнення ними повноліття, незалежно від їх спільного проживання із суб’єктом декларування упродовж звітного періоду;
* будь-яких осіб, які станом на останній день звітного періоду (за умови спільного проживання із суб’єктом декларування впродовж 30 календарних днів, що передували останньому дню звітного періоду) або сукупно протягом не менше 183 днів протягом року, що передує року подання декларації:
  + спільно проживали;
  + були пов’язані спільним побутом;
  + мали взаємні права та обов’язки із суб’єктом декларування (крім осіб, взаємні права та обов’язки яких не мають характеру сімейних), у тому числі особи, які спільно проживали із суб’єктом декларування, але не перебували у шлюбі.

Усі інші особи, за відсутності хоча б однієї із вказаних вище ознак, для цілей декларування не вважаються членами сім’ї суб’єкта декларування.

ВККСУ для проведення перевірки інформації щодо дотримання суддею правил професійної етики та відповідності судді критерію доброчесності, в тому числі відповідності витрат і майна судді та членів його сім’ї, використовує інший принцип формування пов’язаності, наприклад, стаття 61 Закону для заповнення декларації родинних зв’язків судді до осіб, з якими у судді є родинні, належать:

* особи, які спільно проживають, пов’язані спільним побутом і мають взаємні права та обов’язки із суддею (крім осіб, взаємні права та обов’язки яких із суддею не мають характеру сімейних), у тому числі особи, які спільно проживають, але не перебувають у шлюбі з суддею;
* незалежно від зазначених у пункті 1 умов - чоловік, дружина, а також родичі кожного з подружжя чи родичі осіб, які спільно проживають, але не перебувають у шлюбі з суддею (батько, мати, вітчим, мачуха, син, дочка, пасинок, падчерка, брат, сестра, дід, баба, прадід, прабаба, внук, внучка, правнук, правнучка, зять, невістка, тесть, теща, свекор, свекруха, племінник, племінниця, рідний дядько, рідна тітка, двоюрідний брат, двоюрідна сестра, усиновлювач, усиновлений).

Таким чином, ВККСУ потребує рішення, щодо створення системи збору та аналізу інформації для проведення перевірки інформації, щодо дотримання кандидатами на посади суддів, суддями правил професійної етики та відповідності суддів критерію доброчесності, в тому числі відповідності витрат майну суддів та членів сім’ї та близьких осіб.

Технічним адміністратором ПП буде Державне підприємство «Інформаційні судові системи» (далі – ДП «ІСС») - державне комерційне підприємство, яке засноване на державній власності та належить до сфери управління ДСА (статут підприємства затверджений наказом ДСА 26.11.2019 № 1142).

# Вимоги до засобу інформатизації

## Вимоги до структури та функціонування засобу інформатизації

Рішення щодо побудови ПП повинно базуватись на наступних принципах:

* використання сучасних інформаційних технологій;
* реалізація концепції єдиного інформаційного простору в межах Єдиної судової інформаційно-комунікаційної системи (далі – ЄСІКС), а також інтеграції з зовнішніми інформаційними системами;
* дотримання принципу централізованого обміну інформацією;
* підтримка актуальності, повноти, узгодженості, цілісності та доступності даних;
* надійний захист інформації від порушення цілісності, несанкціонованого доступу, витоку та блокування, у тому числі із застосуванням механізмів шифрування та хешування, відповідно до вимог нормативно-правових актів у сфері інформаційної безпеки;
* висока надійність та резервування компонентів технічної інфраструктури;
* централізоване управління, постійний моніторинг працездатності та централізоване налаштування програмного забезпечення та його компонентів;
* застосування сучасних методів програмної інженерії під час розробки прикладного програмного забезпечення.

Архітектура ПЗ повинна передбачати максимальну незалежність програмно-технічних компонентів від розробника таким чином, щоб їх подальшим розвитком міг займатися технічний адміністратор ПП та / або підрядні організації з відповідним рівнем кваліфікації.

Кожен ПП повинен мати такі характеристики та функціональність:

* мати єдину центральну базу даних інформації для тимчасового зберігання транзитної інформації. Термін зберігання, має бути додатково погоджений Виконавцем із Замовником на етапі «Розробка технічного завдання»;
* підтримувати використання системи керування базами даних (далі – СКБД) відкритого типу (програмне забезпечення з відкритим вихідним кодом);
* передбачати необхідні засоби автоматизованого контролю цілісності даних і несуперечності збереженої інформації, персоніфікації даних, створених різними користувачами, ведення журналу операцій, які виконуються;
* забезпечувати механізми для адміністрування користувачів та їх повноважень, а також забезпечувати захист персональних даних відповідно до чинного законодавства України;
* обов’язково документувати АPI у відповідності до міжнародних типів специфікацій та екосистем, таких як: Swagger, RAML, API Blueprint або аналогів для використання внутрішніми/сторонніми сервісами. Перевага надається засобу, який передбачає найкращу підтримку на момент розробки компонентів з точки зору бібліотек, фреймворків, націлених на використання в різних мовах програмування, їх зрілості;
* використання форматів інформаційного обміну даними на основі таких протоколів та стандартів: HTTPS, JSON, REST (Restfull).

WEB-компоненти ПП повинні бути доступні з АРМ користувачів без необхідності встановлення у них клієнтських програмних компонентів ПП (дана вимога може не розповсюджуватися на криптографічні бібліотеки для кваліфікованого електронного підпису).

Всі сторонні програмні компоненти, що ліцензуються окремо та плануються до використання в ПП, вартість їх ліцензій та технічної підтримки мають бути подані у складі пропозиції, в тому числі Виконавець повинен надати окремий розрахунок вартості володіння на 10 років. Виконавець повинен надати інформацію про всі сторонні компоненти прикладного ПЗ та СКБД, що плануються до використання в ПП (дана вимога може не розповсюджуватися на криптографічні бібліотеки для кваліфікованого електронного підпису). Також на вказане ПЗ розповсюджуються вимоги щодо гарантійного обслуговування. Замовник залишає за собою право отримувати ліцензії на ПЗ від сторонніх розробників за окремою процедурою.

Для своєї роботи ПП можуть спиратися на програмні продукти і рішення та використовувати бази даних, які розповсюджуються як вільне ПЗ (примітка: англ. FLOSS — free/libre/open source software — програмне забезпечення, що розповсюджується за, так званими, вільними або відкритими ліцензійними угодами).

Будь-які програмні продукти (бібліотеки, залежності чи частини програмного коду) з відкритим вихідним кодом, що будуть використовуватись в компонентах ПП, повинні бути схвалені Замовником. Вимоги до гарантійного підтримки, в тому числі до програмних рішень третіх сторін, вказані в розділі 5.3 «Вимоги до гарантійної підтримки».

ПП повинні передбачати горизонтальне масштабування за принципами мікросервісної архітектури.

ПП повинні бути побудовані по клієнт-серверній архітектурі та повинні мати трирівневу архітектуру, тобто в архітектурі ПП повинні бути виділені рівень інтерфейсу користувача (браузер), рівень застосунків (сервер застосувань) та рівень даних (база даних).

ПЗ ПП повинно підтримувати розвиток можливостей ПП для підключення додаткового обладнання, тобто продуктивність ПП легко збільшуватиметься шляхом додавання додаткових технічних ресурсів без модифікації вихідного коду ПЗ.

Підключення додаткового обладнання (додавання додаткових технічних ресурсів) для підвищення продуктивності ПП не повинно вимагати модифікації вихідного коду ПЗ.

Клієнтська частина ПП повинна відповідати таким вимогам:

* на користувацьких робочих станціях уся функціональність клієнтської частини ПП (повнофункціональний веб-клієнт) повинна бути доступна за допомогою використання Інтернет-браузера у вигляді веб-клієнта (Google Chrome, Mozilla FireFox, Opera або інший браузер, який буде відповідати вимогам до безпеки та надійності, які пред’являються до функціонування даних ПП) та працювати під керуванням ОС Windows або ОС Linux/Unix як найбільш масово вживаних;
* на клієнтських робочих станціях може вимагатися встановлення Інтернет-браузера, а також ПЗ, що відповідає за роботу ПП з кваліфікованим електронним підписом та периферійними пристроями, що забезпечує безпеку даних.

ПП повинні бути розраховані на експлуатацію в складі програмно-технічного комплексу Замовника. Технічний і фізичний захист апаратних компонентів ПП, носіїв даних, безперебійне енергопостачання, резервування ресурсів, поточне обслуговування реалізується Замовником технічними та організаційними засобами, передбаченими в ІТ-інфраструктурі Замовника.

Повинна бути забезпечена можливість здійснення регламентних робіт з технічного обслуговування ПП із гарантією збереження та автоматичного відновлення неопрацьованих завдань, що перебували у чергах обробки на серверній стороні. Перелік регламентних робіт, їх періодичність, відповідальні особи та порядок протоколювання результатів повинні бути затверджені у відповідному розпорядчому документі Замовника на етапі після дослідної експлуатації ПП.

## Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

Технічним адміністратором засобу інформатизації, що створюється, буде призначено ДП «Інформаційні судові системи» (далі – ДП ІСС), яке створене з метою надання послуг з технічного, технологічного забезпечення створення та супроводження програмного забезпечення ведення автоматизованих систем (електронних баз даних), зокрема, державних реєстрів, що створюються відповідно до законів України, нормативно-правових актів Кабінету Міністрів України, наказів ДСА (Відповідно до статуту підприємства ДП ІСС, що затверджений наказом ДСА від 26.11.2019 № 1142).

Штатна та фактична чисельність ДП ІСС дозволяє виконувати технічну підтримку ПП.

ДП «ІСС» забезпечено кваліфікованим персоналом який володіє наступною кваліфікацією:

* налаштування, установка серверної та клієнтської частин;
* налаштування і експлуатація застосувань;
* установка, налаштування, забезпечення резервування і відновлення даних, експлуатація СКБД;
* установка, налаштування і експлуатація програмних засобів, подібних до ПП.

Впровадження та функціонування ПП буде виконано на технічній базі ДП «ІСС» та за безпосередній участі адміністраторів ДП «ІСС».

На етапі підготовки документу «Технічне завдання» Виконавець повинен надати вимоги до чисельності та кваліфікації адміністраторів ПП.

Всі робочі місця уповноважених осіб ВККСУ оснащені персональним комп’ютером зі встановленою операційною системою Microsoft Windows, офісним пакетом Microsoft Office та програмним забезпеченням, що дозволяє працювати з документами у форматі PDF.

ВККСУ забезпечено необхідною кількістю периферійного обладнання (принтери, сканери, багатофункціональні пристрої) для виконання поточних функцій з перевірки суб’єктів та з урахуванням функціонального об’єму ПП.

В ВККСУ відсутні незадіяні (тобто такі, що повністю або частково не використовуються іншими системами) серверні потужності, фізичні сховища даних та системи резервного та архівного зберігання даних, які можливо використати для функціонування ПП в режимі промислової експлуатації. Тому таке обладнання Замовнику необхідно врахувати в загальній спроможності ДП ІСС з наступним використанням вказаного обладнання.

Налаштування персональних комп’ютерів, програмного забезпечення, периферійного обладнання здійснюється фахівцями управління ІТ ВККСУ.

Штатна та фактична чисельність управління ІТ ВККСУ дозволяє виконувати технічну підтримку користувачів систем, що наразі використовуються ВККСУ, та ПП, що проектуються.

Кількість користувачів програмного продукту «Модуль збору інформації»:

* Кількість внутрішніх користувачів – до 500.
* Одночасна кількість користувачів не повинна бути менше ніж 100 з можливістю масштабування.
* Пікова кількість одночасних користувачів повинна бути не менше ніж 200 з можливістю масштабування.

Кількісні показники щодо суб’єктів перевірки (орієнтовно на 2025-2026 рік):

* Кількість суб’єктів перевірки – 10 000.
* Кількість членів родини – 75 000.
* Кількість запитів до ЗДІ – 2 000 000.

## Вимоги до безпеки

### Вимоги до розмежування та контролю доступу

Усі кінцеві користувачі ПП, включаючи адміністраторів, повинні бути ідентифіковані окремо; у одного користувача повинно бути не більше одного облікового запису; права кінцевому користувачеві повинні надаватися згідно з розробленою моделлю керування доступом на основі ролей.

Повинні бути забезпечені засоби для керування ролями користувачів. Повинно забезпечуватись розподілення прав доступу користувачів до даних. При призначенні користувачу ролей у ПП адміністратор повинен спиратися на існуючу організаційну структуру та посадові обов’язки користувача.

Система прав повинна бути "дозвільного" типу, тобто вважається, що користувач має тільки ті права, які йому безпосередньо було надано адміністратором. Будь-яка спроба виконати операцію, права на яку надано не було, повинна блокуватись.

Система прав повинна забезпечити такі рівні розмежування доступу:

* можливість розмежування доступу на рівні екземплярів сутностей;
* можливість розмежування доступу до операцій над сутностями.

### Вимоги до автентифікації та авторизації

Використовувані безпечні протоколи автентифікації повинні відповідати галузевим стандартам (протоколи шифрування, що використовуються, не були скомпрометовані) і найкращим практикам.

Сторінки входу повинні захищати всі конфіденційні дані, що вводяться, і повинні видавати лише загальну помилку у разі помилки входу.

### Вимоги до шифрування та захисту даних

ПП повинні забезпечувати криптографічний та організаційно-технічний захист інформації відповідно до вимог чинних нормативно-правових актів у сфері технічного захисту інформації, у тому числі НД ТЗІ України.

Захист інформації у стані зберігання (at rest):

* Інформація, що підлягає захисту, повинна зберігатися у зашифрованому вигляді із застосуванням засобів криптографічного захисту інформації (ЗКЗІ), які мають допуск Адміністрації Держспецзв’язку до використання в державних інформаційних системах.
* Рекомендовано використання алгоритмів шифрування, реалізованих у сертифікованих ЗКЗІ (наприклад, на базі ДСТУ 7624:2014, ГОСТ 28147-89, або інших, дозволених до застосування в ІТС відповідного класу).

Захист інформації під час передавання (in transit):

* Передавання даних між компонентами ПП або із зовнішніми системами повинно здійснюватися із забезпеченням конфіденційності та цілісності інформації відповідно до НД ТЗІ 2.5-004-99.
* Використання протоколів захищеного зв’язку (TLS 1.2 або новіших) є обов’язковим. Сертифікати повинні відповідати вимогам чинних криптографічних стандартів України або бути видані довіреним сертифікаційним центром.
* Використання застарілих та вразливих протоколів (SSL, TLS 1.0/1.1) не допускається.

Управління ключами:

* Ключі повинні зберігатися в захищеному середовищі, недоступному для несанкціонованого доступу (наприклад, у сертифікованих апаратних модулях або захищених сховищах).
* Застосування жорстко закодованих або незахищених ключів у програмному коді заборонено.

Контроль цілісності та доступ:

* Для перевірки цілісності даних повинні використовуватися криптографічні хеш-функції відповідно до затверджених стандартів (наприклад, ДСТУ ISO/IEC 10118 або рекомендацій НД ТЗІ).
* Доступ до конфіденційної інформації (включно з обліковими даними, токенами та ключами) повинен реалізовуватися з дотриманням принципу мінімальних привілеїв (Least Privilege) та контролю доступу на основі ролей.

Загальні положення:

* ПП повинні мати можливість оновлення криптографічних механізмів (алгоритмів, бібліотек, протоколів) у зв’язку зі зміною нормативної бази або появою нових вимог з боку Замовника.
* У разі потреби у використанні іноземних криптографічних засобів, їх застосування має бути попередньо погоджено із Замовником та відповідати вимогам законодавства України.

### Вимоги до логування та аудиту

ПП повинні забезпечувати ведення журналів (логування) подій.

Зміни налаштувань безпеки (навіть ті, що внесені адміністратором) повинні реєструватися, відстежуватися та сповіщатись (або налаштовуватись для цього).

Усі події безпеки необхідно реєструвати та точно помічати час, який має бути синхронізований за допомогою NTP (мережевий протокол часу), щоб забезпечити точне співвідношення часових позначок у джерелах журналу.

Журнали аудиту ПП повинні бути захищені від втручання користувачів і адміністраторів ПП.

### Сумісність з антивірусним захистом та межі відповідальності

Розроблене програмне забезпечення повинно бути сумісним із засобами антивірусного захисту, які використовуються на інфраструктурі Замовника, та не перешкоджати їхньому функціонуванню. Робота ПП повинна здійснюватися з урахуванням стандартних сценаріїв перевірки виконуваних файлів, мережевої активності та доступу до файлів.

Наявність антивірусного захисту, його конфігурація, оновлення та ліцензування не входять до обсягу цієї розробки та забезпечуються силами Замовника або відповідального адміністратора ІТ-інфраструктури.

У разі необхідності Виконавець повинен надати технічні рекомендації щодо винятків, які можуть бути застосовані у налаштуваннях антивірусного ПЗ з метою забезпечення стабільної роботи програмного забезпечення без зниження рівня інформаційної безпеки.

### Інші вимоги до безпеки

Інші вимоги до безпеки:

* Розмежування прав доступу до інформації та операцій в ПЗ за рахунок наявності індивідуальних наборів доступів для кожного користувача та\або групи користувачів відповідно до їх ролі.
* Забезпечення типізації помилок, які можуть виникати під час роботи ПЗ.
* Забезпечення розробки механізмів обробки аварійних ситуацій. Це включає, але не обмежується, наступними аспектами:
  + виявленням та логуванням помилок,
  + оповіщенням відповідальних осіб або систем,
  + автоматичним відновленням після помилок,
  + забезпечення резервних процедур для мінімізації впливу помилок на роботу ПП.
* Забезпечення використання засобів накладання та перевірки КЕП, що сертифіковані згідно з законодавством України в галузі криптографічного захисту інформації.
* Забезпечення ефективними заходами безпеки для захисту від загроз, таких як: cross-site scripting (XSS), SQL-ін'єкції та інші.
* Забезпечення зберігання критичних даних (паролів, ключів API, сертифікатів, токенів тощо) поза кодовою базою та файлами конфігурації. Для управління такими даними слід використовувати стандартні галузеві практики, такі як системи управління секретами (напр., HashiCorp Vault, AWS Secrets Manager, Azure Key Vault) або, як мінімум, змінні середовища (environment variables). Файли конфігурації можуть містити посилання на секрети, але не самі секрети у відкритому вигляді. Доступ до сховища секретів має бути суворо обмежений на основі принципу мінімальних привілеїв.
* Забезпечення зберігання паролів в маскованому вигляді, недоступному для перегляду звичайними засобами перегляду.

В таблиці 1 наведено основні аспекти безпеки, щодо яких повинні дотримуватись під час реалізації функціональних складових ПП, та створенні API для взаємодії:

Таблиця 1.

|  |  |
| --- | --- |
| **Аспект безпеки** | **Керівництво з перевірки безпеки коду** |
| Параметри безпеки / Дозволи | Роль і дозволи користувача перевіряються на сервері. |
| Перевірка введених даних | Перевірка введених даних виконується на сервері. |
| Ін'єкції | Введені користувачем дані очищені від неочікуваних спеціальних символів. |
| Спеціальні символи та Unicode | Введені користувачем дані зберігаються в оригінальному кодуванні. |
| Збереженні персональних даних | Персональні дані не зберігається в журналах/кеші. |
| Виконання оболонки  (Shell execution) | Аргументи команд оболонки та імена файлів очищені від неочікуваних спеціальних символів. |
| Шифрування даних | Під час передачі всі дані шифруються. |
| **Рекомендації щодо безпеки API:** | |
| Серіалізація/відображення даних | Виключно поля з «білого» списку об’єкту передачі даних повинні бути зіставлені. Жодні інші поля не повинні зчитуватись. |
| Неавторизовані виклики API | Жодні методи не повинні бути дозволені для неавторизованих користувачів. |
| Атрибути файлів cookie | Маркери сеансу повинні мати атрибути «Secure», «HttpOnly», «SameSite», префікс «\_\_Host-». Відповіді мають містити X-Content-Type-Options: nosniff and Strict-Transport-Security: max-age=15724800 |
| Міжкомпонентна інтеграція | Виклики інтеграції мають бути належним чином перевірені, щоб клон служби не міг публікувати результати, як справжня служба тощо. Вихідний код не повинен містити жорстко закодованих маркерів інтеграції.  Для інтегрованих компонентів необхідно врахувати наступне:   * Методи автентифікації; * Безпечний контроль сесії; * Перевірка даних; * Очищення даних. |

## Вимоги до ергономіки та технічної естетики

Інтерфейс користувача повинен бути адаптивний: залежно від розміру вікна Інтернет-браузера, в якому відображається інформація, розміри, склад та взаємне розташування елементів інтерфейсу та контенту повинні динамічно змінюватися.

Основним інструментом для проектування компонентів дизайн-системи має бути Figma.

Для управління кодовою базою та забезпечення безперебійної інтеграції необхідно налаштувати репозиторії в GitLab із відповідними політиками доступу, pull-request-ами та автоматичним тестуванням.

Користувацький інтерфейс ПП має бути виконаний українською мовою.

Пошук інформації повинен здійснюватися з використанням пошукових індексів, що підтримують кирилицю (українську мову) та латиницю (англійську мову).

Всі навчальні матеріали повинні бути розроблені українською мовою.

Документація, що розробляється в межах створення ПП, має бути надана українською мовою.

## Вимоги до захисту інформації

ПП повинні відповідати вимогам нормативних документів з технічного захисту інформації.

Створення комплексної системи захисту інформації (далі – КСЗІ) з проведенням її державної експертизи та/або отримання сертифіката відповідності стандарту інформаційної безпеки ПП не є предметом даної закупівлі, а повинно бути виконано на наступних етапах побудови ЄСІКС в цілому.

Учасник закупівлі, якому буде присуджений договір, зобов’язаний виправити усі помилки в програмному забезпеченні, які будуть виявлені на етапі створення КСЗІ (отримання сертифіката відповідності стандарту інформаційної безпеки), в тому числі в період гарантійного обслуговування.

З метою підготовки щодо створення комплексної системи захисту інформації (отримання сертифіката відповідності стандарту інформаційної безпеки) Виконавець повинен підготувати та передати Замовнику повний комплект документації на створення ПП відповідно до вимог Постанови КМУ від 21 лютого 2025 р. № 205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації” (зі змінами).

Для автентифікації користувачів мають використовуватись криптографічні бібліотеки для кваліфікованого електронного підпису. Для цього повинні використовуватися бібліотеки “ІІТ Користувач ЦСК-1” (надаються Замовником), які мають працювати у вигляді окремого сервісу, до якого звертатиметься сервіс автентифікації.

## Вимоги до стандартизації та уніфікації

З метою забезпечення сумісності, інтероперабельності, однозначного тлумачення даних та спрощення подальшої підтримки, ПП повинні розроблятися з дотриманням загальновизнаних міжнародних та галузевих стандартів (детальний перелік може бути уточнено за погодженням Замовника на етапі підготовки технічного завдання).

Стандартизація форматів даних:

Усі дані, що обробляються та передаються ПП, повинні відповідати наступним стандартам для забезпечення їх уніфікованого представлення:

* Дата та час: Формат дати та часу має відповідати стандарту ISO 8601. Для обміну даними, що включають часові зони, використовувати RFC 3339. Часові зони повинні ідентифікуватися згідно з базою даних IANA Time Zone Database.
* Формати обміну даними: Основним форматом для структурованих даних є JSON (RFC 8259). Для табличних даних допускається використання CSV (RFC 4180).
* Грошові одиниці: Коди валют повинні відповідати стандарту ISO 4217 (напр., UAH, USD).
* Країни та регіони: Коди країн повинні відповідати стандарту ISO 3166-1 Alpha-2 або Alpha-3.
* Телефонні номери: Формат телефонних номерів має відповідати міжнародному стандарту ITU-T E.164.
* Одиниці виміру: Фізичні величини та одиниці виміру мають відповідати Міжнародній системі одиниць (SI) та стандарту ISO/IEC 80000.

Уніфікація інтерфейсів та документації:

* Документація API повинна розроблятися відповідно до специфікації OpenAPI Specification (OAS) v3.x, що забезпечить можливість автоматичної генерації клієнтського коду та інтерактивної документації.
* Веб-сервіси та інтерфейси мають дотримуватися рекомендацій консорціуму W3C (WCAG 2.0) з рівнем AA щодо доступності та веб-стандартів.

Уніфікація програмного коду:

* У процесі розробки мають бути визначені та дотримуватися єдині правила іменування змінних, функцій та компонентів (coding conventions).
* Мають бути застосовані уніфіковані підходи до обробки помилок, логування та конфігурування компонентів системи.

Для забезпечення максимальної сумісності з існуючою інфраструктурою та експертизою Замовника, рекомендується орієнтуватися на наступні технології та підходи:

* ПЗ має бути побудованою на клієнт-серверній архітектурі з використанням веб-технологій, що не вимагають додаткового ліцензування;
* клієнтська частина повинна бути побудована на стандартних веб-технологіях, що не вимагають встановлення додаткових компонентів на комп’ютер (не рекомендується використовувати Flash або Java-аплети);
* включена підтримка JavaScript та cookies;
* Web-Server – Nginx;
* DB - PostgreSQL, MariaDB;
* NoSQL DB - Redis, MongoDB;
* брокер - Rabbit або Kafka;
* Front - ReactJS, VueJS;
* Back - Java, NodeJS;
* контейнеризація (Docker) + оркестрація (Kubernetes);
* CI/CD - з автоматичним розгортанням (Gitlab);
* використання S3 Compatible Object Storage;
* Dashboards - Superset, Grafana;
* Transaction Monitoring – OpenTelemetry;
* User Monitoring - ELK Stack;
* програмні сервери ПП повинні бути реалізовані на безкоштовних Linux-подібних операційних системах;
* всі компоненти мають бути розроблені з урахуванням георозподіленості, дублювання та горизонтального масштабування;
* розробникам заборонено або слід максимально обмежити використання бази даних для запуску скриптів, що не належать до основного функціоналу додатка/сервісу;
* рівень доступності сервісу не нижче 98,5.

Учасник може запропонувати альтернативні технологічні рішення, якщо вони є еквівалентними або кращими за функціональними, продуктивними чи безпековими характеристиками. У такому випадку, пропозиція Учасника повинна містити детальне обґрунтування вибору альтернативних технологій та докази їх відповідності вимогам цих технічних вимог.

## Вимоги до надійності засобу інформатизації та збереженості інформації

### Загальні вимоги до надійності

Надійність засобу інформатизації визначається його здатністю зберігати працездатність та цілісність даних в умовах штатних та пікових навантажень, а також при виникненні апаратних чи програмних збоїв.

Надійність забезпечується на наступних рівнях:

1. Архітектура високої доступності (High Availability):

* Резервування компонентів: Усі критичні компоненти інформаційно-комунікаційної системи в цілому (сервери застосунків, бази даних, брокери повідомлень, балансувальники навантаження) повинні бути розгорнуті у відмовостійкій кластерній конфігурації за схемою не менше ніж N+1.
* Автоматичне переключення на резерв (Failover): У разі відмови основного компонента система повинна автоматично, без втручання адміністратора, переключати навантаження на резервний вузол. Час переключення не повинен призводити до перевищення показників, визначених у п. 4.7.3.
* Балансування навантаження: інформаційно-комунікаційна система в цілому повинна включати програмні або апаратні балансувальники навантаження для рівномірного розподілу запитів між вузлами кластера, що забезпечує стабільну продуктивність та високу доступність.

1. Цілісність та збереженість даних (Data Integrity and Durability):

* Транзакційна цілісність: Операції, що змінюють пов'язані між собою дані, повинні виконуватися в межах атомарних транзакцій (ACID). Це гарантує, що операція буде або повністю виконана, або повністю скасована, залишаючи дані в узгодженому стані.
* Реплікація даних: Для ключових баз даних має бути налаштована реплікація даних у реальному часі на один або декілька резервних серверів, у тому числі в географічно віддаленому ЦОД, для мінімізації втрати даних у разі аварії (RPO - Recovery Point Objective).
* Резервне копіювання: Повинна бути реалізована політика автоматизованого резервного копіювання даних та конфігурацій. Політика має визначати частоту (повне, інкрементне, диференціальне копіювання) та глибину зберігання копій. Процедури відновлення з резервних копій мають бути задокументовані та регулярно тестуватися.
* Надійність інформаційного обміну: Для гарантування цілісності та повноти інформації під час обміну з зовнішніми системами, повинні використовуватись механізми контролю (напр., контрольні суми), валідації даних за схемою та підтвердження доставки (напр., механізми повторних спроб, квитанції), що визначені у відповідних протоколах обміну.

1. Діагностика та моніторинг:

* Централізоване логування: ПП повинні вести детальні журнали подій, помилок та операцій.
* Інформативність повідомлень про помилки: У разі виникнення аварійної події чи помилки, в журналі має бути зафіксована вичерпна інформація для діагностики, що включає (але не обмежується):
  + Точний час виникнення події;
  + Унікальний ідентифікатор транзакції/запиту;
  + Тип та текстовий опис помилки;
  + Детальна технічна інформація для діагностики (напр., stack trace, контекст виконання);
  + Рівень критичності помилки.
* Проактивний моніторинг: інформаційно-комунікаційна система в цілому повинна надавати метрики для моніторингу стану її компонентів (використання CPU, пам'яті, дискового простору, кількість запитів в секунду тощо) для завчасного виявлення потенційних проблем.

### Критерії надійності

Інформаційно-комунікаційна система в цілому повинна працювати і бути доступною в режимі 24/7 (забезпечувати мінімальний час простою).

Простій ПП для виконання регламентних робіт супроводу або відновлення працездатності при аваріях у середньому не повинен перевищувати 8 годин на місяць.

### Відновлення після збоїв

Відновлення доступності в разі збою для роботи не повинне перевищувати 4 години. При збої інформація в БД має лишатися коректною та цілісною, втрати збережених даних у БД бути не повинно.

Механізми відновлення після збою (в межах ПЗ ПП) мають бути регламентовані та описані Виконавцем.

### Вимоги до можливостей резервного копіювання та відновлення

Відповідальність за налаштування та виконання процедур резервного копіювання в промисловому середовищі покладається на Технічного адміністратора.

Примітка: Конкретні параметри, такі як інтервал виконання процедур копіювання/відновлення, частота та місце зберігання резервних копій (напр., у двох географічно рознесених ЦОД), визначаються в регламентах експлуатації, які розробляються Технічним адміністратором на основі наданої Виконавцем документації та можливостей ПЗ.

## Вимоги до способів і засобів зв’язку для інформаційного обміну між компонентами засобу інформатизації

Взаємодія (інформаційний обмін) з іншими автоматизованими системами, інформаційними базами та ресурсами повинна забезпечувати можливість інформаційного обміну (імпорт, експорт даних) з іншими автоматизованими системами та інформаційними ресурсами на основі використання протоколу REST API, SOAP та реалізації відповідних веб-сервісів. Протоколи мають бути уточнені на етапі створення Технічного завдання.

Інформаційна взаємодія з іншими державними електронними інформаційними ресурсами здійснюється інформаційно-комунікаційними засобами в електронній формі у порядку, визначеному спільним актом Державної судової адміністрації України та відповідного державного органу (установи).

## Вимоги до режимів функціонування та продуктивності засобу інформатизації

ПП повинні підтримувати три основні режими функціонування:

1. Штатний режим:

Основний режим, в якому ПП працюють 24 години на добу, 7 днів на тиждень (24/7) та виконують всі свої робочі процеси. Цей режим передбачає повну доступність усіх сервісів для користувачів та автоматизованих систем у межах визначених показників продуктивності.

1. Сервісний (технологічний) режим:

Режим, призначений для проведення планових технічних робіт, які неможливо виконати в штатному режимі. Перехід у сервісний режим має бути плановим та супроводжуватися завчасним сповіщенням користувачів. У цьому режимі виконуються такі завдання:

* Встановлення оновлень програмного забезпечення.
* Зміна конфігурації, що потребує перезапуску ключових сервісів.
* Виконання регламентних робіт з обслуговування баз даних.
* Інші роботи, що вимагають тимчасового обмеження функціональності.

Під час сервісного режиму доступ до ПП для кінцевих користувачів може бути обмежений або повністю призупинений.

1. Аварійний режим:

Режим, в який ПП переходять автоматично у разі виникнення критичної відмови одного або декількох компонентів, що унеможливлює штатне функціонування. В аварійному режимі ПП повинні:

* Надати адміністраторам засоби для діагностики та відновлення.
* Забезпечити можливість створення резервної копії даних перед початком відновлювальних робіт.

Вимоги до продуктивності та масштабованості:

1. Час відповіді системи:

* Синхронні операції: Для інтерактивних операцій користувача та синхронних запитів API, що не залежать від зовнішніх систем, час відповіді на рівні сервера (server-side processing time) не повинен перевищувати 500 мілісекунд для 95% запитів при штатному навантаженні.
* Асинхронні операції: Для довготривалих операцій (напр., запити до зовнішніх реєстрів) система повинна використовувати асинхронний механізм. Після отримання запиту система має негайно зареєструвати його, повернути ініціатору унікальний ідентифікатор та статус "в обробці". Ініціатор повинен мати можливість перевірити кінцевий результат виконання операції за цим ідентифікатором.

1. Горизонтальна масштабованість:

Архітектура ПЗ повинна бути розроблена за принципами, що дозволяють горизонтальне масштабування. Продуктивність системи має лінійно або майже лінійно зростати при додаванні нових обчислювальних ресурсів (серверних вузлів) без необхідності внесення змін до програмного коду.

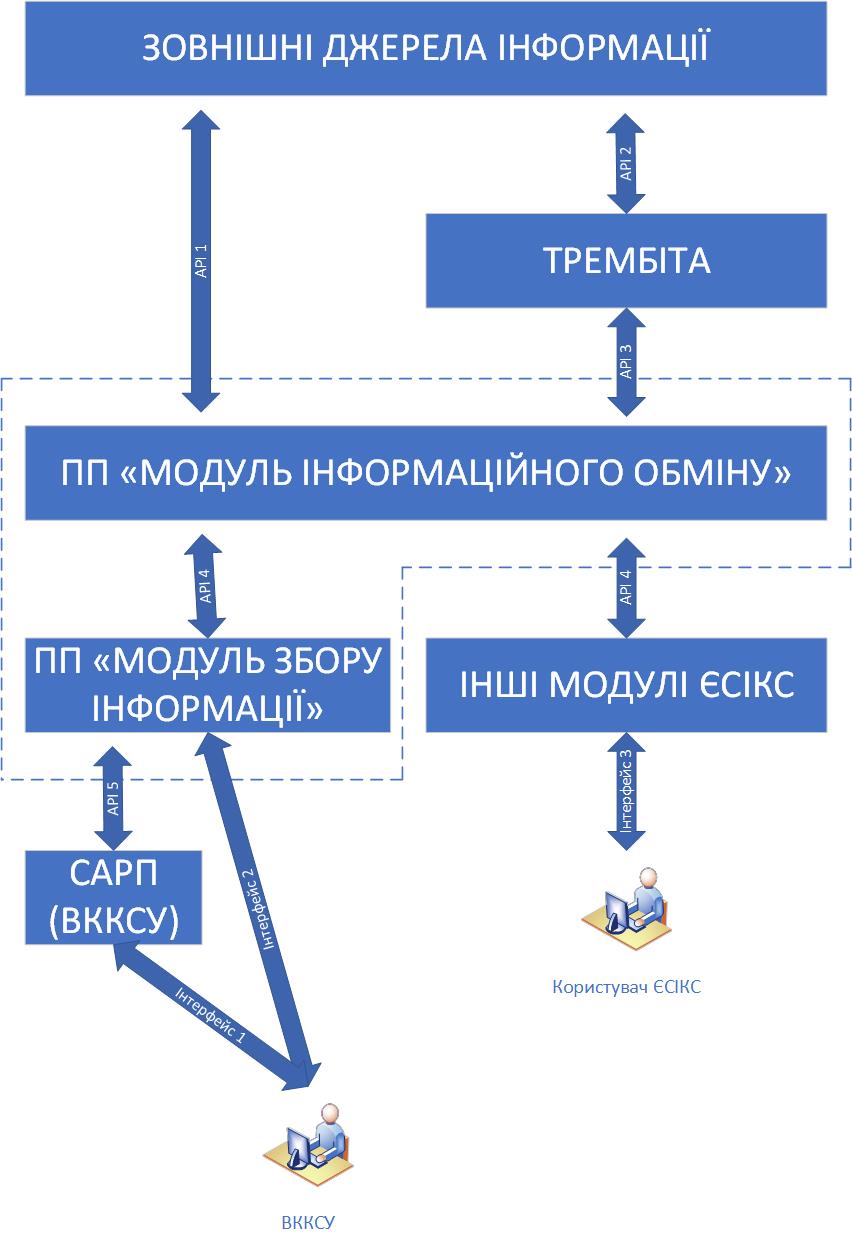
1. Робота під навантаженням:

Система повинна стабільно функціонувати при пікових навантаженнях, які можуть виникати внаслідок зростання кількості одночасних користувачів або масових автоматизованих запитів. Деградація часу відповіді під навантаженням має бути плавною та передбачуваною.

## Вимоги до функцій (завдань), що виконуються засобом інформатизації

### Орієнтовна принципова схема пропонованого рішення

Орієнтовна принципова схема пропонованого рішення надана на наступній схемі:



Опис елементів схеми:

|  |  |
| --- | --- |
| Зовнішні джерела інформації | Електронний реєстр - інформаційно-комунікаційна система, що забезпечує збирання, накопичення, захист, облік, відображення, оброблення реєстрових даних та надання реєстрової інформації |
| Трембіта | Система електронної взаємодії державних електронних інформаційних ресурсів (Міністерство цифрової трансформації України) |
| Програмний продукт «Модуль інформаційного обміну» | Програмний продукт, який реалізує електронну інформаційну взаємодію з зовнішніми джерелами інформації (реєстри, бази даних, інше) |
| Програмний продукт «Модуль збору інформації» | Програмний продукт, який реалізує збір та опрацювання отриманої з ЗДІ інформації для проведення перевірки інформації щодо дотримання суддею (кандидатом на посаду судді) правил професійної етики та відповідності судді (кандидата на посаду судді) критерію доброчесності, в тому числі відповідність витрат і майнового стану судді (кандидата на посаду судді) та членів його сім’ї. |
| Інші модулі ЄСІКС | Інші спеціалізовані програмні продукти та модулі ЄСІКС, які реалізують ініціалізацію запитів через програмний продукт «Модуль інформаційного обміну» до зовнішніх джерел інформації та аналіз отриманих відповідей від них |
| САРП (ВККСУ) | Система автоматизації робочих процесів Вищої кваліфікаційної комісії суддів України |
| API 1 | Організація безпосереднього доступу програмного продукту «Модуль інформаційного обміну» до зовнішніх реєстрів за допомогою інтерфейсу прикладного програмування (API) відповідно до погоджених з володільцями відповідних реєстрів протоколів обміну або використовуючи опис публічного API |
| API 2 | Організація доступу програмного продукту «Модуль інформаційного обміну» до зовнішніх реєстрів за допомогою інтерфейсу прикладного програмування (API) відповідно до погоджених з володільцями відповідних реєстрів протоколів обміну або використовуючи опис публічного API за умови використання «Трембіта» (дана частина знаходиться поза межами сегменту Замовника) |
| API 3 | Організація доступу програмного продукту «Модуль інформаційного обміну» до зовнішніх реєстрів за допомогою інтерфейсу прикладного програмування (API) відповідно до погоджених з володільцями відповідних реєстрів протоколів обміну або використовуючи опис публічного API за умови використання системи «Трембіта» (дана частина знаходиться в межах сегменту ДСА) |
| API 4 | Ініціалізація запитів через програмний продукт «Модуль інформаційного обміну» до зовнішніх джерел інформації та отримання результуючих відповідей від них.  API повинен бути реалізований як для програмного продукту «Модуль збору інформації» безпосередньо, так і для можливого використання іншими програмними продуктами та модулями ЄСІКС |
| API 5 | Організація доступу до програмного продукту «Модуль збору інформації» для ініціалізації «старту» проведення перевірки по конкретному суб’єкту перевірки та отримання результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного аналізу).  Примітка: доопрацювання САРП не входить в обсяг робіт даних Технічних вимог та не виконується Виконавцем |
| Інтерфейс 1 | Автоматизоване робоче місце працівника ВККСУ для роботи в САРП.  Регламентується документацією до САРП та внутрішніми процедурами ВККСУ.  Примітка: доопрацювання САРП не входить в обсяг робіт даних Технічних вимог та не виконується Виконавцем |
| Інтерфейс 2 | Автоматизоване робоче місце працівника ВККСУ для роботи безпосередньо в програмному продукті «Модуль збору інформації».  Регламентується документацією до програмного продукту «Модуль збору інформації» та внутрішніми процедурами ВККСУ.  Користувач може здійснювати доступ до програмного продукту «Модуль збору інформації» безпосередньо через інтерфейс програмного продукту «Модуль збору інформації» для:   * ініціалізації «старту» проведення перевірки по конкретному суб’єкту перевірки (допустимий пакетне завантаження, наприклад у форматі CSV) та * отримання результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного аналізу) з можливістю пошуку, перегляду, копіювання та роздрукування інформації, отримання (завантаження) документів у погоджених форматах. |
| Інтерфейс 3 | Автоматизоване робоче місце користувача ЄСІКС для роботи в відповідному програмному продукті або модулі ЄСІКС.  Регламентується документацією до відповідного програмного продукту або модуля ЄСІКС та внутрішніми процедурами володільця ЄСІКС.  Примітка: доопрацювання програмних продуктів або модулів ЄСІКС не входить в обсяг робіт даних Технічних вимог та не виконується Виконавцем. |

Орієнтовний алгоритм формування результатів автоматизованої перевірки судді (кандидата):

1. Ініціалізація перевірки: до програмного продукту «Модуль збору інформації» передається дані про суб’єкта перевірки (ПІБ, дата народження, РНОКПП – тут і далі повний перелік атрибутів буде уточнено на етапі формування технічного завдання) за допомогою Інтерфейсу 2 (в тому числі пакетного завантаження, наприклад, у форматі CSV) та/або API 5 (примітка: формат АРІ 5 буде уточнено на етапі формування технічного завдання; дана функціональність реалізовується Виконавцем виключно в межах функціональності програмного продукту «Модуль збору інформації»; доопрацювання САРП не входить в обсяг робіт даних технічних вимог та не виконується Виконавцем).
2. Створення в програмному продукті «Модуль збору інформації» індивідуальної картки для кожного суб’єкта перевірки.
3. Ініціалізація запиту до програмного продукту «Модуль інформаційного обміну» для отримання інформації про членів сім’ї суб’єкта перевірки.
4. Програмний продукт «Модуль інформаційного обміну» звертається до Державного реєстру актів цивільного стану громадян Міністерства юстиції України для отримання інформації про членів сім’ї суб’єкта перевірки.
5. Програмний продукт «Модуль збору інформації» отримує від програмного продукту «Модуль інформаційного обміну» інформацію про членів сім’ї суб’єкта перевірки та зберігає в Анкеті суб’єкта перевірки. Додатково, враховуючи обмежену функціональність API Державного реєстру актів цивільного стану громадян Міністерства юстиції України, користувачеві надається можливість «ручного» введення інформації про членів сім’ї та/або близьких осіб суб’єкта перевірки.
6. Ініціалізація запиту до програмного продукту «Модуль інформаційного обміну» для отримання інформації від «Єдиний реєстр довіреностей» про наявні доручення суб’єкта перевірки та кожного члена його сім’ї, або видані на них.
7. Ініціалізація запиту до програмного продукту «Модуль інформаційного обміну» для отримання інформації від погодженого переліку державних реєстрів про майновий стан та доходи суб’єкта перевірки, кожного члена його сім’ї та інших осіб, внесених в його картку.
8. Програмний продукт «Модуль інформаційного обміну» звертається до відповідних реєстрів для отримання інформації від державних реєстрів про майновий стан та доходи суб’єкта перевірки та кожного члену його сім’ї, близьких осіб у відповідності до погоджених протоколів обміну (в т.ч. з використанням «Трембіта»).
9. Всі отримані відповіді зберігаються в оригінальному виді (JSON, тощо) в базі даних програмного продукту «Модуль інформаційного обміну».
10. Програмний продукт «Модуль збору інформації» отримує від програмного продукту «Модуль інформаційного обміну» отриману інформацію про майновий стан та доходи суб’єкта перевірки та кожного члена його сім’ї, близької особи та зберігає визначений перелік інформації в анкету суб’єкта перевірки (макет надано в Додатку 1; перелік атрибутів буде уточнено на етапі формування технічного завдання) з одночасним зберіганням первинної відповіді та посиланням на первинну відповідь від державного реєстру, яка зберігається в програмному продукті «Модуль інформаційного обміну».

Примітка: при необхідності користувач програмного продукту «Модуль збору інформації» може подивитися первинну відповідь, але потрібно розуміти, що формат інформації буде «технічний», наприклад, JSON, а не звичний «бланк», який зазвичай користувач отримує при доступі до відповідного реєстру з використанням спеціалізованого WEB-інтерфейсу відповідного реєстру.

Умовно, анкета суб’єкта перевірки буде складатися з розділами у чіткій відповідності до кількості зовнішніх реєстрів, з яких буде отримуватися інформація. Наприклад, інформація про об’єкти нерухомості будуть в окремому розділі: один об’єкт – один рядок інформації. За базовий варіант колонки для відповідних розділів пропонується взяти форму, яка надана в Додатку 1.

1. Отримання результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного аналізу) в досьє судді (кандидата) САРП.

Примітка: формат АРІ 5 буде уточнено на етапі формування технічного завдання; дана функціональність може бути реалізована лише за умови доопрацювання САРП, не входить в обсяг робіт за даними Технічними вимогами та не виконується Виконавцем.

1. Отримання користувачем результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного збору інформації) з можливістю пошуку, перегляду, копіювання та роздрукування інформації, отримання (завантаження) документів у погоджених форматах безпосередньо в програмному продукті «Модуль збору інформації» з використанням автоматизованого робочого місця працівника ВККСУ.

Запропонована схема реалізації за модульним принципом забезпечить можливе масштабування використання програмного продукту «Модуль інформаційного обміну» іншими програмними продуктами та модулями ЄСІКС.

Перелік реєстрів, з яких є потреба отримання інформації надано в Додатку 2.

Примітка: В рамках реалізації проекту Виконавець має забезпечити реалізацію інформаційної взаємодії з ЗДІ, щодо надання та отримання даних, з власниками яких на момент завершення етапу підготовки Технічного завдання будуть підписані відповідні документи (договори, протоколи обміну, інше), які встановлюють правові відносини, щодо інформаційної взаємодії.

### Загальні вимоги до функціональності ПП

Для організації ефективного обміну інформації, ПП повинні виконувати процес отримання та оновлення довідникових даних, необхідних для досягнення організації якісного обміну інформації з іншими програмними продуктами та модулями ЄСІКС та ЗДІ.

ПП повинні опрацьовувати запити на обмін інформацією в синхронному та/або асинхронному режимах, незалежно від серверного навантаження та кількості запитів.

Вимоги до API розповсюджуються на інтерфейси обміну відповідно до орієнтовної принципіальної схеми (див.п.4.10.1).

Заміна (додавання нових) зовнішніх програмних продуктів та модулів ЄСІКС та ЗДІ не повинна потребувати доопрацювання API ПП, крім відповідного АРІ, який буде змінено (додаватися).

ПП мають підтримувати версійність API. Не повинно бути ситуації, коли нова версія ПП не підтримує попередню версію API, а отже необхідна адаптація API інших програмних продуктів чи модулів.

API повинен забезпечувати:

* підтримку прикладних функцій авторизації. Авторизація має здійснюватися через підсистему автентифікації та авторизації методом отримання ключа (Token). Має підтримуватися один з протоколів авторизації, наприклад, oAuth;
* підтримку роботи як у синхронному так і в асинхронному режимах;
* надання можливості багатопотокової роботи;
* повторення запитів, якщо вони не були доставлені через недоступність інтерфейсу.

При обміні даними повинен здійснюватися контроль цілісності та повноти прийнятої та відправленої інформації.

ПП повинні розроблятись з використанням безкоштовних програмних засобів з відкритими кодами, такими як: PostgreSQL, MySQL або аналогів. Взаємодія між сервером додатків та клієнтом для кінцевого користувача повинна виконуватися за протоколом HTTPS (криптографічним протоколом).

Створення та подальший розвиток ПП має здійснюватися з дотриманням Постанови КМУ від 21 лютого 2025 р. № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» (зі змінами), що передбачає використання відкритих технологій, прозорість реалізації та можливість подальшого масштабування і модифікації програмних рішень. Рішення повинні відповідати таким загальним вимогам:

* орієнтація на вирішення критично важливих задач з метою підвищення продуктивності, зокрема у межах функціонування програмного продукту «Модуль інформаційного обміну»;
* забезпечення високої якості, надійності та стабільності роботи ПП, з унеможливленням втрат або дублювання даних;
* підтримка прозорих, стандартизованих і документованих інтеграційних механізмів;
* дотримання вимог інформаційної та технічної безпеки відповідно до чинного законодавства та нормативних документів у сфері захисту інформації;
* забезпечення конфіденційності персональних даних громадян відповідно до вимог законодавства України;
* ведення повної історії змін і журналювання дій користувачів;
* впровадження механізмів резервування ключових програмних компонентів ПП;
* відкритість, прозорість і доступність вихідного коду всіх програмних компонентів, що постачаються або впроваджуються в межах цієї закупівлі, відповідно до умов ліцензування вільного програмного забезпечення (Open Source);
* надання повного комплекту актуальної супровідної та експлуатаційної документації.

Загальний опис архітектури ПП з вказанням технологій та програмних засобів, на базі яких будуватимуться ПП, повинен бути наданий Виконавцем в рамках тендерної пропозиції.

Детальний опис та підходи до реалізації ПП повинні бути сформовані Виконавцем на етапі «Розробка технічного завдання» на основі наданих Замовником відомостей.

### Загальні вимоги до програмного продукту «Модуль інформаційного обміну»

Програмний продукт «Модуль інформаційного обміну» забезпечує ефективну, уніфіковану та безпечну взаємодію між програмними продуктами та модулями ЄСІКС та ЗДІ.

Основні аспекти призначення програмного продукту «Модуль інформаційного обміну»:

* Інтеграція та взаємодія:
  + Забезпечення механізмів підключення нових інформаційних сервісів та організація їх взаємодії із ЗДІ.
  + Надання можливості електронної взаємодії між програмними продуктами та модулями ЄСІКС та ЗДІ зокрема через уніфіковані API.
* Управління інформаційними потоками:
  + Координація та управління електронною взаємодією програмних продуктів та модулів ЄСІКС та ЗДІ.
  + Надання запитів від програмних продуктів та модулів ЄСІКС до ЗДІ.
  + Нормалізація даних ЗДІ відповідно до вимог програмних продуктів та модулів ЄСІКС.
  + Передача відповідей від ЗДІ до програмних продуктів та модулів ЄСІКС.
* Функціональність для інтеграції та обміну даними:
  + Забезпечення автоматизованого обміну даними, включаючи підтримку запитів, відповідей і нормалізації даних.
  + Підтримка використання сучасних протоколів і форматів обміну даними (REST API, JSON, XML).
  + Можливість налаштування інтеграційних параметрів для адаптації до змін в параметрах аутентифікації та взаємодії.
* Автономність та технологічність:
  + Діяльність як автономного технологічного ПП ЄСІКС, який може функціонувати незалежно, забезпечуючи надійність і стабільність роботи всієї системи.
  + Підтримка масштабованості та адаптивності для зростання обсягів даних і кількості користувачів.
* Забезпечення єдиного інформаційного простору:
  + Побудова інтегрованого програмного продукту для централізованого зберігання, обробки та обміну даними.
  + Підтримка цілісності, актуальності та надійності даних у процесі їх використання.

Таким чином, програмний продукт «Модуль інформаційного обміну» є ключовим елементом ЄСІКС, що забезпечує інтеграцію, управління та координацію інформаційних потоків для підвищення ефективності взаємодії між судовою владою, державними органами та іншими зовнішніми суб’єктами електронної взаємодії.

В межах даних технічних вимог програмний продукт «Модуль інформаційного обміну» повинен реалізувати електронну взаємодію відповідно до погоджених Замовником з володільцями відповідних реєстрів протоколів обміну або використовуючи опис публічного API:

* з усіма підсистемами ЄСІКС які готові на момент запуску ПП та терміну його гарантійного обслуговування (API 4 - детально описано в п.4.10.1);
* з ІС, реєстрами, базами даних державних органів, органів місцевого самоврядування, міжнародних організацій, суб’єктів господарювання та правоохоронних органів інших держав, в тому числі, що здійснюються за допомогою системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» (API 3 - детально описано в п.4.10.1);
* у разі відсутності технічної можливості передачі даних з використанням системи електронної взаємодії державних електронних інформаційних ресурсів “Трембіта” електронна інформаційна взаємодія суб’єктів електронної взаємодії може здійснюватися з використанням інших інформаційно-комунікаційних систем із застосуванням в них відповідних комплексних систем захисту інформації з підтвердженою відповідністю за результатами державної експертизи в порядку, встановленому законодавством (API 1 - детально описано в п.4.10.1).

Цілі створення програмного продукту «Модуль інформаційного обміну»:

* Централізація управління інформаційними взаємодіями:
  + Створення єдиного елементу ЄСІКС для координації всіх інтеграційних процесів між програмними продуктами та модулями ЄСІКС та ЗДІ.
  + Забезпечення уніфікованого механізму обміну даними через єдину точку доступу.
* Уніфікація та нормалізація даних:
  + Реалізація механізмів нормалізації даних.
  + Гарантування високої якості та цілісності даних у процесі інформаційної взаємодії.
* Автоматизація управління інформаційними взаємодіями:
  + Реалізація автоматизованої маршрутизації запитів між системами на основі їхніх специфікацій та пріоритетів.
  + Підтримка асинхронної обробки запитів для підвищення продуктивності системи.
* Масштабованість та адаптивність:
  + Побудова програмного продукту, який легко масштабується для обробки зростаючих обсягів запитів і нових інформаційних взаємодій.
  + Налаштування правил інформаційних взаємодій для швидкої адаптації до змін у вимогах.
* Підвищення безпеки інформаційних взаємодій:
  + Впровадження сучасних механізмів автентифікації та авторизації (OAuth, JWT).
* Моніторинг та управління:
  + Інтеграція систем моніторингу для виявлення проблем у роботі програмного продукту.
  + Надання адміністраторам інструментів для аналізу продуктивності та усунення помилок.
* Розширення функціональності ЄСІКС:
  + Забезпечення гнучкої платформи для інтеграції нових сервісів і підсистем у майбутньому.
  + Підтримка версійності API для мінімізації впливу змін на існуючі інтеграції.

Програмний продукт «Модуль інформаційного обміну» повинен реалізовувати наступні функціональні можливості:

* Підтримка стандартних протоколів та форматів:
  + Основний стек: Пріоритетним є використання RESTful веб-сервісів з форматом даних JSON. Система повинна підтримувати стандартні HTTP-методи (GET, POST, PUT, PATCH, DELETE).
  + Сумісність з іншими системами: Для взаємодії з існуючими або специфічними системами має бути забезпечена можливість роботи з протоколом SOAP (з використанням XML) та іншими форматами даних (напр., CSV, XML). Можливість трансформації даних між різними форматами має бути закладена архітектурно.
  + Безпека передачі даних: Уся взаємодія (за виключенням, якщо взаємодія реалізована на використанні Національної системи конфіденційного зв'язку) з зовнішніми системами повинна відбуватися виключно за захищеним протоколом HTTPS.
* Архітектурна гнучкість та розширюваність:
  + Модульні адаптери (конектори): Архітектура програмного продукту «Модуль інформаційного обміну» повинна дозволяти розробку та підключення специфічних адаптерів для інтеграції з різними зовнішніми інформаційними системами. Кожен адаптер має інкапсулювати логіку взаємодії з конкретним зовнішнім API, включаючи автентифікацію, авторизацію та трансформацію даних.
* Гнучкі механізми ініціації обміну. Програмний продукт «Модуль інформаційного обміну» повинен підтримувати різні способи ініціації обміну даними:
  + За розкладом: Виконання регламентних завдань для періодичного обміну даними (наприклад, щоночі).
  + За подією: Ініціація обміну в реальному часі за фактом настання певної події в одній із систем (API 4).
  + За запитом користувача: Можливість ручного запуску обміну через інтерфейс адміністратора.
* Аудит та контроль виконання:
  + Детальне логування: Ведення журналу кожної операції обміну із фіксацією ключових параметрів: ідентифікатор транзакції, час початку та завершення, статус виконання (успішно/помилка) та повідомлення про помилки.
  + Автоматичне сповіщення (алертинг): Налаштування автоматичних повідомлень для відповідальних адміністраторів у разі невдалого виконання операцій експорту/імпорту даних для забезпечення швидкого реагування на інциденти.

### Функціональні вимоги до Програмного продукту «Модуль інформаційного обміну»

Програмний продукт «Модуль інформаційного обміну» виконує електронну взаємодію відповідно до погоджених Замовником з володільцями відповідних реєстрів протоколів обміну або використовуючи опис публічного API.

Далі наведено типовий приклад інформаційної взаємодії програмного продукту «Модуль інформаційного обміну» з ЗДІ.

Згідно з протоколом автоматизованого обміну програмний продукт «Модуль інформаційного обміну» направляє http-запити про надання відомостей у форматі JSON або CSV або XML (текстових форматах для представлення табличних даних) до ЗДІ. Результатом запиту є файл у форматі JSON\CSV\XML такої ж структури.

Атрибутами такого файлу є:

* ідентифікатор запиту;
* дані запиту, зашифровані за допомогою бібліотеки користувача ЦСК "Підпис (модуль розширення PHP)";
* КЕП на дані запиту.

Інформаційний обмін здійснюється із накладанням кваліфікованого електронного підпису та шифруванням інформації з використанням бібліотеки користувача ЦСК "Підпис (модуль розширення PHP)" програмного комплексу користувача центру сертифікації ключів "IIT Користувач ЦСК-1" (надається Замовником).

Процес обміну розділений на кілька частин, а саме: підготовка даних, відправка даних, перевірка стану запитів, отримання даних.

Обмін з ЗДІ організовано у вигляді драйверів (конекторів) обміну з ЗДІ, згідно відповідних затверджених Замовником протоколів обміну.

**Підготовка даних**

Початок роботи кожної частини програмного продукту «Модуль інформаційного обміну» здійснюється за допомогою планувальника завдань, який виконує виклик відповідної частини функціоналу обміну, які знаходяться в контролері програмного продукту.

Підготовка даних починається з компонента обміну, в якому завантажується перелік драйверів (конекторів) та їх налаштуваннями, завантажується список даних, що потребують формування запитів в ЗДІ. Дані щодо яких необхідно здійснити запит на пошук інформації до ЗДІ, передаються до відповідних драйверів (конекторів), в яких формуються запити до ЗДІ у необхідному форматі, згідно протоколів обміну.

Для кожного запиту в базі даних програмного продукту «Модуль інформаційного обміну» формується запис з параметрами обміну.

Методи обміну даними реалізує механізм відправки та отримання даних:

* відправка даних запитів на вказану адресу або посилання;
* контроль кодів відповіді;
* отримання та формування заголовків запитів;
* підтримка авторизації та автентифікації.

Частини обміну, такі як відправка даних, перевірки стану та отримання даних, залежать від ЗДІ та реалізовано згідно протоколу обміну. Обмін з ЗДІ працює за різними протоколами, тому деякі частини системи обміну можуть бути не задіяні.

У разі отримання запитів на доступ до даних, що містять персональні дані користувачів, програмний продукт «Модуль інформаційного обміну» повинен забезпечувати фіксацію кожного такого запиту. Запис повинен містити: ідентифікатор запитувача, тип запитуваних даних, мету запиту та дату/час обробки, у відповідності до вимог щодо прозорості обробки персональних даних, згідно з Законом України “Про захист персональних даних”. Усі операції з персональними даними повинні бути зафіксовані у журналах подій, які забезпечують аудит доступу та контролю відповідності законодавчим нормам. Збереження таких записів повинно відповідати вимогам інформаційної безпеки, зокрема щодо обмеження доступу виключно уповноваженим особам.

**Перевірка стану запитів**

Програмний продукт «Модуль інформаційного обміну» повинен дозволяти ініціаторам (програмні продукти та модулі ЄСІКС) запиту перевіряти стан відправленого запиту, а також надавати можливість повторної відправки запиту у випадках збоїв в роботі ЗДІ.

**Отримання даних**

Програмний продукт «Модуль інформаційного обміну» повинен обробляти запити від програмних продуктів та модулів ЄСІКС на отримання даних в випадках коли:

* Користувачеві ЄСІКС для виконання посадових обов’язків необхідно перевірити актуальність даних, зазначених в сутностях ЄСІКС;
* Користувачеві ЄСІКС для виконання посадових обов’язків необхідно створити в ЄСІКС сутність на основі актуальних даних, отриманих від інших ЗДІ;
* В інших випадках, які можуть бути додатково описані на етапі створення технічного завдання.

Програмний продукт «Модуль інформаційного обміну» має забезпечити уніфікацію, типізацію та кодування однотипної інформації, яка може використовуватись великою кількістю користувачів, незалежно від їхньої ролі в ЄСІКС.

Програмний продукт «Модуль інформаційного обміну» повинен надавати можливість переглядати відповіді від інших систем та державних реєстрів, які надійшли у вигляді JSON-файлів з однією або декількома сутностями, або у вигляді згенерованих документів, в залежності від алгоритмів обробки запитів ЗДІ.

Програмний продукт «Модуль інформаційного обміну» повинен надавати можливість вказати значення в наборі фільтраційних параметрів, дозволених для відповідних запитів до ЗДІ, для зручності пошуку конкретних запитів/відповідей.

Для спрощення та оптимізації роботи користувачів, програмний продукт «Модуль інформаційного обміну» повинен надавати їм можливість отримати інформацію про ЗДІ, необхідну для створення сутностей всередині ЄСІКС, наприклад, опис протоколу обміну тощо.

**Обробка та тимчасове зберігання отриманих даних**

Після отримання набору даних від ЗДІ, програмний продукт «Модуль інформаційного обміну» повинен в автоматичному режимі виконати конвертації, необхідні для використання даних ініціатором запиту (програмні продукти та модулі ЄСІКС).

Програмний продукт «Модуль інформаційного обміну» повинен зберігати дані, отримані від ЗДІ, в чистому вигляді тільки протягом певного часу, визначеного в налаштуваннях програмного продукту «Модуль інформаційного обміну».

Процедуру та терміни тимчасового зберігання отриманих даних та їх видалення з БД програмного продукту «Модуль інформаційного обміну» має бути додатково погоджено Виконавцем із Замовником на етапі «Розробка технічного завдання».

**Структура даних**

Системні дані повинні бути представлені у структурованому вигляді.

У структурі даних повинні бути чітко визначені правила зберігання інформації для забезпечення точної ідентифікації даних в програмному продукті «Модуль інформаційного обміну», якщо це визначено діловим процесом роботи з даними.

**Організація даних**

Організація даних у програмному продукті «Модуль інформаційного обміну» повинна забезпечувати цілісне, ефективне та уніфіковане управління всією інформацією, необхідною для виконання прикладних задач:

* інформаційні масиви повинні бути єдиними та використовуватись спільно для всіх функціональних завдань програмного продукту «Модуль інформаційного обміну»;
* структура даних має бути оптимізована для забезпечення мінімальних витрат на зберігання, доступ, обробку та внесення змін.

**Логування**

Програмний продукт «Модуль інформаційного обміну» повинен забезпечити збір та зберігання усіх типів логів, основними серед яких:

* логи сервісів (реєстрація, авторизація, автентифікація, інформаційна взаємодія);
* системні логи (операційна система, зміни конфігурації, збої, розгортання нових сервісів, метрики);
* логи безпеки;
* логи дій користувачів (версійність даних, фіксація змін з зазначенням особи, що внесла або змінила дані).

Програмний продукт «Модуль інформаційного обміну» повинен забезпечувати логування та ведення журналу подій.

У разі аварійних ситуацій або помилок інструменти діагностики повинні фіксувати необхідну інформацію для ідентифікації проблеми.

Діагностика та обробка інформації мають проводитися для кожного компонента підсистеми та її робочих процесів.

Усі транзакції повинні мати унікальні номери, при некоректній обробці транзакції номер та помилка мають бути записані в журнал подій.

**Автоматичне ведення журналів взаємодії з ЗДІ**

Програмний продукт «Модуль інформаційного обміну» автоматично фіксує взаємодії із ЗДІ.

Фіксуються також зміни статусу роботи, компонентів та помилки, що виникають під час їхньої роботи.

Усі події логування необхідно реєструвати та точно помічати час за допомогою NTP (мережевий протокол часу), щоб забезпечити точне співвідношення часових позначок у журналах логів.

Лише у користувача з відповідними правами доступу повинна бути можливість переглядати лог-файли.

Наведений перелік логів не є вичерпним. Детальний перелік логів, що мають зберігатися в програмному продукті «Модуль інформаційного обміну», а також період їх зберігання, має бути додатково погоджений Виконавцем із Замовником на етапі «Розробка технічного завдання».

**Вимоги до рольової моделі**

Вимоги до рольової моделі програмного продукту «Модуль інформаційного обміну» мають бути верифіковані Виконавцем та погоджені з Замовником на етапі розробки технічного завдання.

Сервіс автентифікації та авторизації користувачів використовує КЕП, що забезпечує перевірку доступу користувачів до функціональних можливостей програмного продукту «Модуль інформаційного обміну».

При успішній авторизації користувач входить в програмний продукт «Модуль інформаційного обміну».

На сторінці профілю користувача повинно бути реалізовано перегляд профілю користувача, під яким було виконано вхід в програмний продукт «Модуль інформаційного обміну», з відображенням інформації про користувача, його контактними даними.

Основні ролі:

* Адміністратор

Обов’язки:

* + Управління користувачами, їхніми ролями та правами доступу.
  + Налаштування параметрів API (ключі, URL, тайм-аути, політики безпеки).
  + Моніторинг стану системи, логів та журналів.
  + Вирішення технічних проблем та реагування на інциденти.
  + Визначення загальних параметрів програмного продукту «Модуль інформаційного обміну».

Рівень доступу:

* + Повний доступ до всіх функціональних складових системи.
  + Можливість вносити зміни до конфігурації API та системних налаштувань.
* Інтеграційний менеджер

Обов’язки:

* + Налаштування та підтримка інтеграцій із ЗДІ.
  + Управління запитами до ЗДІ.
  + Координація інтеграційних проектів із внутрішніми (ЄСІКС) та зовнішніми системами (ЗДІ).

Рівень доступу:

* + Доступ до налаштувань інтеграційних сервісів.
  + Обмежений доступ до журналів запитів і відповідей.
* Ініціатор запиту (відповідно до погоджених API 4; див. п.4.10.1)

Обов’язки:

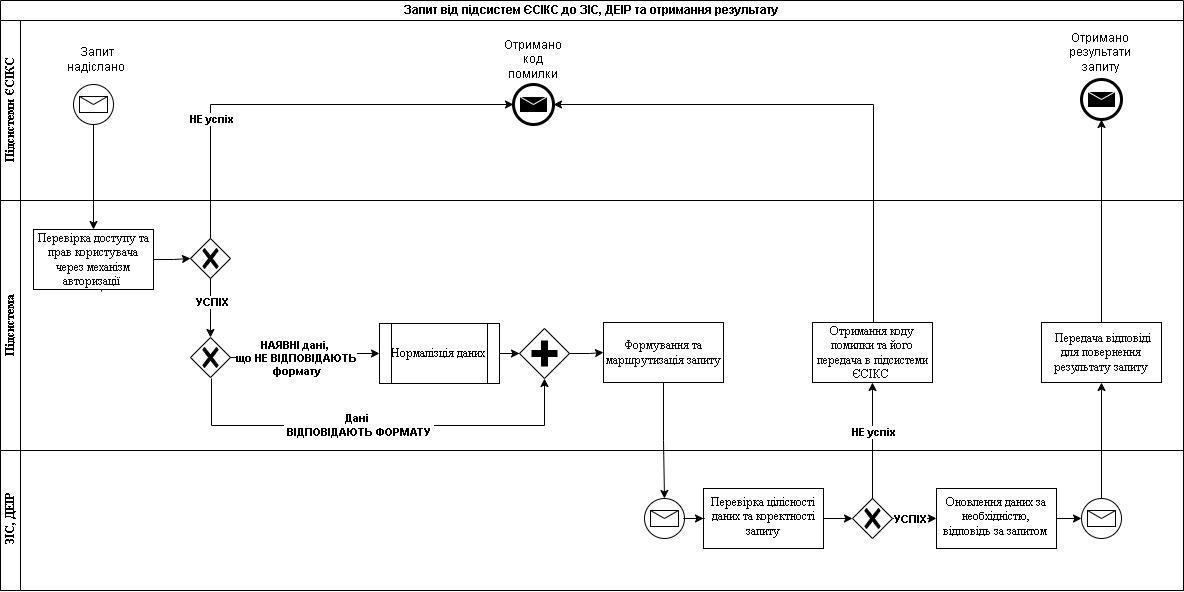
* + Взаємодія з програмним продуктом «Модуль інформаційного обміну» через інтерфейси зовнішніх систем.
  + Надання необхідних запитів до програмного продукту «Модуль інформаційного обміну» або отримання даних.

Рівень доступу:

* + Доступ до специфічних API, які обмежені контекстом їхнього використання.

**Базовий робочий процес Запит від ЄСІКС до ЗДІ**

Базовий робочий процес Запит від ЄСІКС до ЗДІ та отримання результату надано на наступному малюнку:



**Підпроцеси роботи програмного продукту «Модуль інформаційного обміну»**

1. Ініціалізація запиту

Учасники:

* інші програмні продукти та модулі ЄСІКС.

Дії:

* Формування запиту з використанням API 4 через інтерфейс користувача відповідного програмного продукту чи модуля ЄСІКС.
* Перевірка доступу та прав до АРІ 4 через механізм авторизації (OAuth, JWT).

Результат:

* Успішна авторизація та ініціалізація запиту.

1. Передача запиту

Учасники:

* Система API.

Дії:

* Прийом запиту API.
* Перевірка цілісності даних та коректності запиту.
* Маршрутизація запиту до відповідного внутрішнього компонента програмного продукту «Модуль інформаційного обміну» для обробки.

Результат:

* Запит прийнято та передано на обробку.

1. Обробка запиту

Учасники:

* програмний продукт «Модуль інформаційного обміну» та ЗДІ.

Дії:

* Нормалізація (підготовка форматів даних для запитів до ЗДІ) даних:
  + Перетворення структури даних запиту у формат, що відповідає стандартам цільового ЗДІ.
  + Валідація даних для забезпечення їхньої відповідності специфікаціям.
* Взаємодія з цільовими системами:
  + Виконання запитів до ЗДІ.
  + Отримання та обробка відповідей.

Результат:

* Дані нормалізовано, отримано відповідь, оновлено в програмному продукті «Модуль інформаційного обміну».

1. Повернення результату

Учасники:

* Програмний продукт «Модуль інформаційного обміну».

Дії:

* Формування відповіді на основі отриманих результатів.
* Передача відповіді до ініціатора (програмні продукти та модулі ЄСІКС).
* Логування дій в програмному продукті «Модуль інформаційного обміну» для забезпечення прозорості.

Результат:

* Відповідь повернуто до ініціатора.

1. Моніторинг та управління

Учасники:

* Адміністратор системи, Інтеграційний менеджер.

Дії:

* Моніторинг роботи API через відповідні інструменти (журнали подій).
* Аналіз продуктивності запитів.
* Виявлення та усунення інцидентів (помилки, збої тощо).

Результат:

* Безперервна підтримка стабільності роботи ПЗ.

**Вимоги до кабінету користувачів програмного продукту «Модуль інформаційного обміну»**

Кабінет користувача програмного продукту «Модуль інформаційного обміну» являє собою веб-сторінку, на якій відображається функціонал програмного продукту «Модуль інформаційного обміну», доступний користувачеві відповідно до рольової моделі та прав доступу.

Загальні вимоги до кабінетів:

* Адаптивність:
  + Інтерфейс кабінетів повинен бути зручним для використання на робочих станціях.
* Безпека:
  + Використання HTTPS для шифрування даних, що передаються.
  + Контроль сесій із автоматичним виходом після періоду бездіяльності.
* Логування дій:
  + Всі дії в кабінетах повинні логуватися з вказанням часу, користувача та результату.
* Персоналізація:
  + Кабінети повинні дозволяти налаштування інтерфейсу відповідно до потреб користувача (фільтри, сортування).
  + Структура кабінетів повинна забезпечувати розмежування доступу відповідно до ролей, зручність у виконанні завдань та дотримання стандартів безпеки.

На основі запропонованої рольової моделі, кабінети користувачів повинні забезпечувати доступ до функціональності відповідно до ролі, підтримувати зручність використання та відповідати діючим стандартам безпеки. Нижче наведено основні вимоги для кожної ролі:

1. Кабінет адміністратора

Функціональність:

* Управління ролями та правами доступу користувачів.
* Конфігурація параметрів API (ключі, URL, тайм-аути, політики доступу).
* Перегляд логів дій користувачів та подій системи.
* Налаштування безпеки.
* Моніторинг продуктивності API та стану системи
* Інструменти для реагування на інциденти.

Інтерфейс:

* Інтуїтивно зрозумілий дашборд із графіками та індикаторами стану системи.
* Модуль для перегляду та фільтрації журналів подій.
* Панель для швидкого доступу до налаштувань безпеки.

1. Кабінет інтеграційного менеджера

Функціональність:

* Налаштування інтеграцій із ЗДІ.
* Перегляд статусу запитів та відповідей.
* Внесення змін до параметрів інтеграцій (конектори, адаптери, протоколи обміну).
* Формування та управління чергами запитів до ЗДІ.

Інтерфейс:

* Список активних інтеграцій із можливістю редагування.
* Візуалізація стану інтеграцій (успішність запитів, затримки, збої).
* Панель повідомлень про помилки або порушення в роботі інтеграцій.

Для зручності користування програмним продуктом «Модуль інформаційного обміну» мають бути реалізовані наступні функції, які доступні в усіх розділах:

* Сортування таблиць (при відображенні інформації в табличній формі);
* Вибір кількості записів для відображення на сторінці (при відображенні інформації в табличній формі);
* Посторінковий перехід (при відображенні інформації в табличній формі);
* Відображення повідомлень про помилки у разі некоректного заповнення полів у формах.

### Загальні вимоги до програмного продукту «Модуль збору інформації»

Програмний продукт «Модуль збору інформації» забезпечує створення та перегляд запитів до ЗДІ.

Основні аспекти призначення програмного продукту «Модуль збору інформації»:

* Управління інформаційними потоками:
  + Ініціалізація до програмного продукту «Модуль інформаційного обміну» запитів до ЗДІ для збору інформації про суб’єкти перевірки.
  + Отримання від програмного продукту «Модуль інформаційного обміну», опрацювання, групування та зберігання відповідей на запити до ЗДІ.
  + Нормалізація даних ЗДІ відповідно до вимог обліку інформації про суб’єкти перевірки.
* Функціональність для інтеграції та обміну даними:
  + Забезпечення автоматизованого обміну даними, включаючи підтримку запитів, відповідей і нормалізації даних.
  + Підтримка використання (зберігання, вивантаження, опрацювання) сучасних протоколів і форматів обміну даними (REST API, JSON, XML).
  + Можливість налаштування інтеграційних параметрів для адаптації до змін в параметрах аутентифікації та взаємодії.
* Забезпечення єдиного інформаційного простору:
  + Підтримка цілісності, актуальності та надійності даних у процесі їх використання.

В межах даних технічних вимог Модуль збору інформації повинен реалізувати електронну взаємодію:

* на етапі ініціалізації запиту до програмного продукту «Модуль збору інформації» передається дані про суб’єкта перевірки (ПІБ, дата народження, РНОКПП – тут і далі повний перелік атрибутів буде уточнено на етапі формування технічного завдання) за допомогою Інтерфейсу 2 (в тому числі пакетного завантаження, наприклад, у форматі CSV) та/або API 5 (примітка: формат АРІ 5 буде уточнено на етапі формування технічного завдання; дана функціональність реалізовується Виконавцем виключно в межах функціональності програмного продукту «Модуль збору інформації»; доопрацювання САРП не входить в обсяг робіт даних технічних вимог та не виконується Виконавцем);
* отримання результуючих відповідей від програмного продукту «Модуль інформаційного обміну».

Програмний продукт «Модуль збору інформації» повинен забезпечувати:

* Використання файлів погодженого формату API4 для обміну інформацією з програмним продуктом «Модуль інформаційного обміну» (формати будуть узгоджені між Виконавцем та Замовником на етапі розробки технічного завдання).
* Можливість налаштування регламентного обміну даними, або за фактом настання певних подій;
* Ведення журналів обміну даними із фіксацією головних параметрів (дата, час запуску та закінчення виконання пакету, стан виконання);
* Забезпечити можливість збереження інформації про суб’єкти перевірки в БД програмного продукту «Модуль збору інформації»;
* Управління безпекою та політиками доступу до сервісів і даних.

### Функціональні вимоги до Програмного продукту «Модуль збору інформації»

Згідно з протоколом автоматизованого обміну Програмний продукт «Модуль збору інформації» направляє запити та отримує результати запитів у погодженому (API4) форматі.

Обов’язковими атрибутами таких запитів є:

* ідентифікатор запиту;
* дані запиту, зашифровані за допомогою бібліотеки користувача ЦСК "Підпис (модуль розширення PHP)";
* КЕП на дані запиту.

Інформаційний обмін здійснюється із накладанням кваліфікованого електронного підпису та шифруванням інформації з використанням бібліотеки користувача ЦСК "Підпис (модуль розширення PHP)" програмного комплексу користувача центру сертифікації ключів "IIT Користувач ЦСК-1" (надається Замовником).

Робота системи збору інформації розділена на декілька частин, а саме: підготовка даних, відправка даних, перевірка стану запитів, отримання даних.

Обмін з ЗДІ організовано виключно через програмний продукт «Модуль інформаційного обміну».

**Підготовка даних**

Початок збору інформації за конкретним суб’єктом перевірки здійснюється з заведення ключових даних по даному суб’єкту перевірки:

* ПІБ;
* дата народження;
* РНОКПП;
* підстава формування запита.

Додатково, враховуючи обмежену функціональність API Державного реєстру актів цивільного стану громадян Міністерства юстиції України, користувачеві надається можливість «ручного» введення інформації згідно вищевказаного переліку атрибутів про членів сім’ї та близьких осіб суб’єкта перевірки. Оскільки запити до ЗДІ по кожному члену сім’ї та близьких осіб суб’єкта перевірки ініціюються окремо, додавання в перелік «нових» членів сім’ї та близьких осіб суб’єкта для отримання по ним інформації з ЗДІ дозволяється виконувати на будь-якому етапі збору інформації про суб’єкт перевірки.

Робота програмного продукту «Модуль збору інформації» здійснюється за допомогою планувальника завдань, який виконує виклик відповідної частини функціоналу обміну.

Дані про суб’єкти перевірки, їх членів сім’ї та близьких осіб, щодо яких необхідно здійснити запит на пошук інформації до ЗДІ, передаються до Програмного продукту «Модуль інформаційного обміну», згідно протоколів обміну (API4).

Для кожного запиту в базі даних формується запис з параметрами обміну.

У разі отримання запитів на доступ до даних, що містять персональні дані, програмний продукт «Модуль збору інформації» повинен забезпечувати фіксацію кожного такого запиту. Запис повинен містити: ідентифікатор запитувача, тип запитуваних даних, мету запиту та дату/час обробки, у відповідності до вимог щодо прозорості обробки персональних даних, згідно з Законом України “Про захист персональних даних”. Усі операції з персональними даними повинні бути зафіксовані у журналах подій, які забезпечують аудит доступу та контролю відповідності законодавчим нормам. Збереження таких записів повинно відповідати вимогам інформаційної безпеки, зокрема щодо обмеження доступу виключно уповноваженим особам.

**Перевірка стану та управління процесом збору інформації**

Програмний продукт «Модуль збору інформації» повинен дозволяти користувачам в реальному часі перевіряти загальний стан процесу збору інформації по суб'єкту, а також детальний статус запитів до кожного окремого реєстру (напр., "в обробці", "успішно виконано", "помилка").

У разі масового збою, коли значна частина запитів до реєстрів не була виконана, користувач повинен мати можливість ініціювати повторний запуск всього процесу збору інформації про конкретного суб'єкта. Програмний продукт «Модуль збору інформації» повинен бути достатньо інтелектуальним, щоб повторно відправляти лише ті запити, які не були успішно виконані раніше.

Для прискорення роботи при проведенні періодичних або повторних перевірок, програмний продукт «Модуль збору інформації» повинен надавати функціонал для створення нового процесу збору інформації на основі даних існуючого. При використанні цієї функції система має створювати нову, "чисту" перевірку, автоматично копіюючи в неї всі вихідні дані про суб'єкта перевірки та пов'язаних з ним осіб (ПІБ, РНОКПП, дані про членів сім'ї тощо). Користувачу залишиться лише ініціювати новий старт збору інформації.

**Отримання даних**

Програмний продукт «Модуль збору інформації» повинен обробляти запити на отримання даних в випадках коли:

* Користувачеві для виконання посадових обов’язків необхідно перевірити актуальність даних, зазначених в сутностях програмного продукту «Модуль збору інформації»;
* Користувачеві для виконання посадових обов’язків необхідно створити в програмному продукті «Модуль збору інформації» сутність на основі актуальних даних, отриманих від програмного продукту «Модуль інформаційного обміну»;
* В інших випадках, які можуть бути додатково описані на етапі створення технічного завдання.

Програмний продукт «Модуль збору інформації» має забезпечити уніфікацію, типізацію та кодування однотипної інформації, яка може використовуватись великою кількістю користувачів, незалежно від їхньої ролі в програмному продукті «Модуль збору інформації».

Програмний продукт «Модуль збору інформації» повинен надавати користувачам можливість переглядати відповіді від інших систем та державних реєстрів, які надійшли у вигляді JSON-файлів з однією або декількома сутностями, або у вигляді згенерованих документів, в залежності від алгоритмів обробки запитів ЗДІ.

**Обробка та тимчасове зберігання отриманих даних**

Після отримання набору даних від програмного продукту «Модуль інформаційного обміну», програмний продукт «Модуль збору інформації» повинен в автоматичному режимі виконати конвертації, необхідні для використання даних користувачами програмного продукту «Модуль збору інформації».

Програмний продукт «Модуль збору інформації» повинен зберігати дані, отримані від програмного продукту «Модуль інформаційного обміну», в чистому вигляді тільки протягом певного часу, визначеного в налаштуваннях програмного продукту «Модуль збору інформації» (термін зберігання буде уточнено та погоджено з Замовником на етапі підготовки технічного завдання).

**Структура даних**

Системні дані повинні бути представлені у структурованому вигляді.

У структурі даних повинні бути чітко визначені правила зберігання інформації для забезпечення точної ідентифікації даних в програмному продукті «Модуль збору інформації», якщо це визначено робочим процесом роботи з даними.

**Принципи роботи з даними**

Робота з даними у програмному продукті «Модуль збору інформації» повинна відповідати таким принципам:

* цілісність та безперервність: дані повинні зберігати логічну цілісність, бути послідовними та узгодженими у процесі обробки, передачі й зберігання;
* надійність та захищеність: має бути забезпечено захист даних від втрат, пошкодження (корупції) та несанкціонованого доступу, включаючи засоби резервування та контролю доступу;
* актуальність і точність: повинні впроваджуватись механізми постійного контролю за достовірністю та оновленням даних;
* уніфікованість та стандартизація: дані мають відповідати встановленим форматам і стандартам, бути уніфікованими для забезпечення сумісності;
* гнучкість використання: хоча дані повинні бути єдиними у межах програмного продукту «Модуль збору інформації», архітектура повинна дозволяти їх адаптацію до різних прикладних задач;
* адаптивність до змін: програмний продукт «Модуль збору інформації» має бути здатним адаптуватися до змін у вимогах і джерелах даних без порушення загальної стабільності роботи;
* мінімізація помилок: слід впровадити інструменти валідації та контролю для зменшення ймовірності помилок під час введення, обробки та виведення даних.

**Організація даних**

Організація даних повинна забезпечувати єдність і зберігання всієї необхідної інформації для вирішення задач.

Інформаційні масиви повинні бути єдиними для всіх функціональних завдань програмного продукту «Модуль збору інформації».

Структура даних має бути оптимізована для забезпечення мінімальних витрат на зберігання, доступ, обробку та внесення змін.

**Логування**

Програмний продукт «Модуль збору інформації» повинен забезпечити збір та зберігання наступних логів:

* логи сервісів (реєстрація, авторизація, автентифікація, інформаційна взаємодія);
* системні логи (операційна система, зміни конфігурації, збої, розгортання нових сервісів, метрики);
* логи безпеки;
* логи дій користувачів (версіонування даних, фіксація змін з зазначенням особи, що внесла або змінила дані).

Програмний продукт «Модуль збору інформації» повинен забезпечувати логування та ведення журналу подій.

У разі аварійних ситуацій або помилок інструменти діагностики повинні фіксувати необхідну інформацію для ідентифікації проблеми.

Діагностика та обробка інформації мають проводитися для кожного компонента підсистеми та її робочих процесів.

Усі транзакції повинні мати унікальні номери, при некоректній обробці транзакції номер та помилка мають бути записані в журнал подій.

**Автоматичне ведення журналів взаємодії з зовнішніми системами**

Програмний продукт «Модуль збору інформації» автоматично фіксує взаємодії із програмним продуктом «Модуль інформаційного обміну».

Фіксуються також зміни статусу роботи, компонентів та помилки, що виникають під час їхньої роботи.

Усі події логування необхідно реєструвати та точно помічати час за допомогою NTP (мережевий протокол часу), щоб забезпечити точне співвідношення часових позначок у журналах логів.

У користувача з відповідними правами доступу повинна бути можливість переглядати лог-файли.

Детальний перелік логів, що мають зберігатися в програмному продукті «Модуль збору інформації», а також період їх зберігання, має бути додатково погоджений Виконавцем із Замовником на етапі «Розробка технічного завдання».

**Вимоги до рольової моделі**

Сервіс автентифікації та авторизації користувачів використовує КЕП, що забезпечує перевірку доступу користувачів до функціональних можливостей програмного продукту «Модуль збору інформації».

При успішній авторизації користувач входить в програмний продукт «Модуль збору інформації».

На сторінці профілю користувача повинно бути реалізовано перегляд профілю користувача, під яким було виконано вхід в програмний продукт «Модуль збору інформації», з відображенням інформації про користувача, його контактними даними та можливістю зміни паролю.

Основні ролі:

* Адміністратор

Обов’язки:

* + Управління користувачами, їхніми ролями та правами доступу.
  + Налаштування параметрів API (ключі, URL, тайм-аути, політики безпеки).
  + Моніторинг стану системи, логів та журналів.
  + Вирішення технічних проблем та реагування на інциденти.
  + Визначення загальних параметрів програмного продукту «Модуль збору інформації».

Рівень доступу:

* + Повний доступ до всіх функціональних складових системи.
  + Можливість вносити зміни до конфігурації API та системних налаштувань.
* Користувач-САРП (відповідно до погоджених API 5; див. п.4.10.1; за умови доопрацювання САРП Замовником; доопрацювання САРП не входить в обсяг робіт даних Технічних вимог та не виконується Виконавцем)

Обов’язки:

* + Взаємодія з Модулем збору інформації через зовнішні інтерфейси (API5).
  + Надання необхідних запитів до програмного продукту «Модуль збору інформації» (для ініціалізації «старту» проведення перевірки по конкретному суб’єкту перевірки) або отримання даних автоматизованої перевірки.

Рівень доступу:

* + Доступ до специфічних API5, які обмежені контекстом їхнього використання.
* Користувач-ВККСУ

Обов’язки:

* + Взаємодія з програмним продуктом «Модуль збору інформації» через інтерфейс програмного продукту «Модуль збору інформації» (Інтерфейс 2; див. п.4.10.1) для:
    - ініціалізації «старту» проведення перевірки по конкретному суб’єкту перевірки (допустимий пакетне завантаження, наприклад у форматі CSV) та
    - отримання результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного аналізу) з можливістю пошуку, перегляду, копіювання та роздрукування інформації, отримання (завантаження) документів у погоджених форматах.

Рівень доступу:

* + Заведення ключових даних по даному суб’єкту перевірки, в тому числі про членів сім’ї суб’єкта перевірки;
  + Повний доступ на перегляд інформації по суб’єкту перевірки;
  + Мінімальний рівень доступу до функцій, пов’язаних із їхньою роботою.
* Користувач-ВККСУ (тільки перегляд)

Обов’язки:

* + Взаємодія з програмним продуктом «Модуль збору інформації» через інтерфейс програмного продукту «Модуль збору інформації» (Інтерфейс 2; див. п.4.10.1) для:
    - отримання результатів автоматизованої перевірки (перелік пов’язаних осіб, відповіді з державних реєстрів, результат проведеного аналізу) з можливістю пошуку, перегляду, копіювання та роздрукування інформації, отримання (завантаження) документів у погоджених форматах.

Рівень доступу:

* + Повний доступ на перегляд інформації по суб’єкту перевірки;
  + Мінімальний рівень доступу до функцій, пов’язаних із їхньою роботою.

**Підпроцеси роботи Програмного продукту «Модуль збору інформації»**

1. Ініціалізація запиту

Учасники:

* Користувач-САРП
* Користувач-ВККСУ.

Дії:

* ініціалізації «старту» проведення перевірки по конкретному суб’єкту перевірки.

Результат:

* Успішна автентифікація та авторизація, ініціалізація запиту.

1. Передача запиту

Учасники:

* API4 (Програмний продукт «Модуль інформаційного обміну»).

Дії:

* Перевірка цілісності даних та коректності запиту.
* Передача запиту API4 до програмного продукту «Модуль інформаційного обміну».

Результат:

* Запит передано на обробку.

1. Обробка запиту

Учасники:

* API4 (Програмний продукт «Модуль інформаційного обміну»).

Дії:

* Нормалізація (підготовки форматів даних для запитів до ЗДІ) даних:
  + Отримання та обробка відповідей;
  + Перетворення структури даних відповіді у формат, що відповідає стандартам внутрішніх процесів (Інтерфейс 2) або цільових зовнішніх систем (API5).
  + Валідація даних для забезпечення їхньої відповідності специфікаціям.
* Взаємодія з цільовими внутрішніми процесами:
  + Ініціалізація запитів у разі отримання інформації про «нових» членів сім’ї суб’єкта перевірки.

Результат:

* Дані нормалізовано, отримано або оновлено в цільовій системі.
* Ініціалізовано запити у разі отримання інформації про «нових» членів сім’ї суб’єкта перевірки.

1. Повернення результату

Учасники:

* Програмний продукт «Модуль збору інформації».

Дії:

* Формування консолідованої інформації на основі отриманих результатів.
* Передача відповіді до користувача (Інтерфейс 2) або системи-ініціатора (відповідно до погоджених API 5; див. п.4.10.1; за умови доопрацювання САРП Замовником; доопрацювання САРП не входить в обсяг робіт даних Технічних вимог та не виконується Виконавцем).
* Логування дій у системі для забезпечення прозорості.

Результат:

* Відповідь повернуто до ініціатора.

1. Моніторинг та управління

Учасники:

* Адміністратор системи.

Дії:

* Моніторинг роботи API через відповідні інструменти (дашборди, журнали подій).
* Аналіз продуктивності запитів.
* Виявлення та усунення інцидентів (помилки, збої тощо).

Результат:

* Безперервна підтримка стабільності роботи програмного продукту «Модуль збору інформації».

**Вимоги до кабінету користувачів програмного продукту «Модуль збору інформації»**

Кабінет користувача програмного продукту «Модуль збору інформації», являє собою веб-сторінку, на якій відображається функціонал програмного продукту «Модуль збору інформації», доступний користувачеві відповідно до рольової моделі та прав доступу.

Загальні вимоги до кабінетів:

* Адаптивність:
  + Інтерфейс кабінетів повинен бути зручним для використання на робочих станціях.
* Безпека:
  + Використання HTTPS для шифрування даних, що передаються.
  + Контроль сесій із автоматичним виходом після періоду бездіяльності.
* Логування дій:
  + Всі дії в кабінетах повинні логуватися з вказанням часу, користувача та результату.
* Персоналізація:
  + Кабінети повинні дозволяти налаштування інтерфейсу відповідно до потреб користувача (фільтри, сортування).
  + Структура кабінетів повинна забезпечувати розмежування доступу відповідно до ролей, зручність у виконанні завдань та дотримання стандартів безпеки.

На основі запропонованої рольової моделі, кабінети користувачів повинні забезпечувати доступ до функціональності відповідно до ролі, підтримувати зручність використання та відповідати діючим стандартам безпеки. Нижче наведено основні вимоги для кожної ролі:

1. Кабінет адміністратора

Функціональність:

* Управління ролями та правами доступу користувачів.
* Конфігурація параметрів API (ключі, URL, тайм-аути, політики доступу).
* Перегляд логів дій користувачів та подій системи.
* Налаштування безпеки.
* Моніторинг продуктивності API та стану системи
* Інструменти для реагування на інциденти.

Інтерфейс:

* Інтуїтивно зрозумілий дашборд із графіками та індикаторами стану системи.
* Модуль для перегляду та фільтрації журналів подій.
* Панель для швидкого доступу до налаштувань безпеки.

1. Кабінет Користувач-ВККСУ

Функціональність:

* Перегляд статусу запитів та відповідей.
* Перегляд та внесення (за умови наявності повноважень) змін до списку суб’єктів перевірки та членів їх родин.

Інтерфейс:

* Список суб’єктів перевірки із можливістю редагування (за умови наявності повноважень).
* Візуалізація стану перевірки (успішність запитів, затримки, збої).

Для зручності користування програмним продуктом «Модуль збору інформації» мають бути реалізовані наступні функції, які доступні в усіх розділах:

* Сортування таблиць (при відображенні інформації в табличній формі);
* Вибір кількості записів для відображення на сторінці (при відображенні інформації в табличній формі);
* Посторінковий перехід (при відображенні інформації в табличній формі);
* Відображення повідомлень про помилки у разі некоректного заповнення полів у формах.

Для зручності опрацювання користувачами отриманої з ЗДІ інформації про суб’єкта перевірки, членів його родини та близьких осіб, та враховуючи специфіку кожного ЗДІ, інформаційну картку по суб’єкту перевірки потрібно формувати по відповідним розділам (орієнтовний макет надано в Додатку 1; остаточний вигляд повинен бути уточнений на етапі підготовки технічного завдання) за наступними принципами:

* перший розділ– інформація про суб’єкта перевірки;
* другий розділ – список членів сім’ї та близьких осіб суб’єкта перевірки (таблична форма; один рядок – один член сім’ї);
* кожен наступний розділ - відповідає окремому ЗДІ (дивись п.4.10.1):
  + таблична форма;
  + один рядок – одна відповідь від ЗДІ;
  + можливість перегляду отриманої відповіді в оригінальному виді (JSON, тощо);
  + за умови технічної можливості, можливість перегляду отриманої відповіді у вигляді візуального відображення (зі збереженням в PDF) з основними полями оригінальної відповіді.

# Вимоги до розробки та передачі послуг

## Вимоги до розробки

В процесі проектування архітектури ПП Виконавець повинен надати орієнтовні вимоги до апаратного забезпечення, що буде необхідне для запуску ПП (у тестовому та промисловому середовищах, враховуючи вимоги до резервного зберігання даних) із урахуванням вимог до продуктивності, що викладені у цьому документі.

По завершенню Виконавець повинен надати Замовнику остаточні вимоги до апаратного забезпечення, яке необхідне для функціонування ПП із урахуванням вимог до продуктивності, що викладені у цьому документі.

Орієнтовний графік реалізації етапів життєвого циклу ПП (проектування, розроблення та впровадження) надано в Додатку 3.

Вимоги до потенційних виконавців договору надано в Додатку 4.

## Вимоги до передачі

### Вимоги до порядку розгортання

Розгортання ПЗ передбачає декілька етапів робіт:

* Розробка або адаптація програмного забезпечення.

На цьому етапі Виконавець проводить розробку ПП, вибір, адаптацію та (або) прив’язку придбаних програмних засобів, розробку програмної документації у відповідності до вимог чинного законодавства, в тому числі документи «Програма та методика випробувань», «Інструкція з встановлення (розгортання)» та «Керівництво користувача (відповідно по кожній ролі)».

* Розгортання обладнання та ПЗ.

На цьому етапі Технічний адміністратор здійснює встановлення й налаштування необхідних складників загальносистемного програмного забезпечення, (за необхідності) інструментальних середовищ розроблення у тестовому (за наявності) та промисловому середовищі ПЗ, засобів конфігураційного управління. Встановлення розробленого ПЗ або його складника у сформованому середовищі у відповідності до документу «Інструкція з встановлення (розгортання)» та опрацювання (тестування) виявлених проблем.

* Підготовка Технічного адміністратора та Замовника до введення ПП у дію.

На цьому етапі проводять роботи щодо організаційної підготовки об’єкта автоматизації до введення ПП у дію, в тому числі:

* + Реалізацію проектних рішень у відповідності до організаційної структури Технічного адміністратора та Замовника.
  + Забезпечення підрозділів Технічного адміністратора та Замовника інструктивно-методичними матеріалами.
  + Впровадження класифікаторів інформації.
* Підготовка та навчання персоналу.

На цьому етапі проводять навчання персоналу та перевірку його здібності забезпечити функціонування ПП.

Виконавець зобов'язаний провести навчання для співробітників Замовника та Технічного адміністратора:

* + План навчання адміністраторів повинен містити теоретичні та практичні завдання щодо встановлення та експлуатації програмних компонентів, діагностики та усунення типових помилок (збоїв), що можуть виникати під час експлуатації ПП.
  + Навчання користувачів повинно охоплювати вивчення функціоналу та порядку роботи з ПП.
  + Для всіх видів навчання повинні бути розроблені та використовуватися:
    - Програми навчання.
    - Презентації.
    - Керівництва користувачів відповідно по кожній ролі.
  + Всі навчальні матеріали повинні бути розроблені українською мовою і доступні в електронному форматі.
  + Тривалість навчання становить 24 години для ролі Адміністратор та 16 годин для інших користувачів. Ці дані можуть бути уточнені в процесі розробки Технічного завдання та відображені в Технічному завданні.
* Пусконалагоджувальні роботи.

### Вимоги до функціонального тестування

Приймальні випробування проводяться у відповідності до вимог документа «Програма та методика випробувань», які передбачають перевірку виконання реалізованих функцій ПП.

Результати випробувань оформлюються протоколом відповідних випробувань за підписами представників Замовника за участі Виконавця, Технічного адміністратора та Замовника, додатком до протоколу випробувань повинен бути звіт з випробувань.

### Вимоги до тестування на проникнення ПП

Перед передачею Замовнику результатів робіт зі створення ПП розроблені ПП повинні бути перевірено тестуванням на проникнення та на навантаження силами Замовника з метою виявлення критичних та високих ризиків інформаційної безпеки. Виконавець повинен сповістити Замовника, що система готова до тестування, після чого Замовник організовує та проводить тестування протягом 2-х тижнів.

У разі фіксації критичних та високих ризиків в процесі проведення тестування на проникнення, Виконавець повинен забезпечити їх усунення в найкоротші терміни та прозвітувати щодо готовності до повторного тестування.

ПП не може бути прийнято Замовником поки не будуть виправлені та перевірені всі критичні та високі ризики інформаційної безпеки.

### Порядок приймання

Результати надання послуг приймаються комісією Замовника.

До участі у прийманні наданих послуг залучаються представники Виконавця.

Майнові, у тому числі виключні, права інтелектуальної власності на програмний продукт «Модуль інформаційного обміну», у тому числі передбачені Цивільним кодексом України, Законом України "Про авторське право і суміжні права", а також іншим законодавством України та міжнародними нормативно-правовими актами, з моменту розроблення (створення, модернізації) передаються ДСА на підставі відповідного договору про передачу майнових прав на програмний продукт «Модуль інформаційного обміну».

Майнові, у тому числі виключні, права інтелектуальної власності на програмний продукт «Модуль збору інформації», у тому числі передбачені Цивільним кодексом України, Законом України "Про авторське право і суміжні права", а також іншим законодавством України та міжнародними нормативно-правовими актами, з моменту розроблення (створення, модернізації) передаються ВККСУ на підставі відповідного договору про передачу майнових прав на програмний продукт «Модуль збору інформації».

### Вимоги до підтримки виробником

Користувачам ПП повинна бути надана вся необхідна контактна інформація та інструкції, що стосуються допомоги у разі несправностей ПП.

Адміністратори ПП повинні мати доступ до ефективних засобів реєстрації скарг одержувачів послуг ПП, планування завдань, надання інформації про методи вирішення проблем тощо (довідкова служба, база знань).

Складові вирішення проблем та бази знань повинні бути заповнені та накопичені з етапу тестування ПП. База знань повинна бути підготовлена на етапі дослідної експлуатації ПП, щоб вона могла використовуватися користувачами та адміністраторами при вирішенні найпоширеніших проблем.

### Вимоги до навчання персоналу

Виконавець повинен забезпечити навчання (інструктаж) адміністраторів та користувачів ПП щодо розроблених ПП.

Кількість персоналу для навчання:

* адмініструванню та супроводу експлуатації: не менше 2 (двох) професіональних ІТ-працівників Замовника та/або Технічного адміністратора;
* користувачів ПП: не менше 20 (двадцяти) працівників Замовника та/або Технічного адміністратора.

Додаткові вимоги до навчання вказані в п.5.2.1.

Вартість навчання повинна бути врахована в ціновій пропозиції Виконавця.

## Вимоги до гарантійної підтримки

Об’єктом гарантійного обслуговування повинно бути програмне забезпечення ПП, впроваджене відповідно до умов договору та до затвердженого Технічного завдання.

Гарантійне обслуговування ПП надається після введення ПП у промислову експлуатацію.

Гарантійне обслуговування повинно включати:

* безкоштовне виправлення помилок в програмному забезпеченні ПП;
* безоплатні послуги з реагування на інциденти, пов’язані з дефектами у програмному забезпеченні ПП;
* усунення розбіжностей між програмним забезпеченням ПП та затвердженим Технічним завданням, помилок та інших несправностей (несправністю ПЗ вважатиметься ситуація, коли користувачі не можуть виконати певні дії, що пов’язані з функціями ПП, за винятком ситуацій, коли таке невиконання є наслідком некоректної роботи апаратного забезпечення ПП або каналів зв’язку);
* інші гарантії, передбачені законодавчими та регуляторними актами України.

Послуги з гарантійного обслуговування ПП стосуються всього переліку програмного забезпечення, що надається Виконавцем, у тому числі СУБД.

Програмне забезпечення ПП повинно бути функціональним, надійним та швидко відновлюваним після виправлення помилок. Всі дії Виконавця на етапі гарантійного обслуговування повинні виконуватися відповідно до процедури, погодженої із Замовником, і призводити до забезпечення відновлення процесів діяльності Замовника для реалізації функціональних можливостей на основі вимог, представлених у цьому документі.

Гарантійна підтримка не розповсюджується на наступні випадки:

* неналежна експлуатація або технічне обслуговування ПП Замовником та/або Технічним адміністратором (неналежною експлуатацію вважається порушення умов та правил експлуатації ПП, які описані в експлуатаційній документації);
* використання в ПП елементів, не поставлених Виконавцем, якщо в вимогах не зазначено інший порядок, або якщо Виконавцем не схвалено інший порядок;
* в разі, якщо ПП або їх складові частини (програмний код та/або структура бази даних, апаратна частина, канали зв’язку, інше), будь-яким чином модифіковані Замовником або третіми особами без письмової згоди на це Виконавця, або порушені умови експлуатації ПП, визначені у Експлуатаційній документації.

Усі помилки роботи ПЗ ПП класифікуються як:

* критична помилка– у разі виявлення порушення або проблеми, яка заважає 10 відсоткам користувачів використовувати необхідні функції ПП і невідомо жодне інше альтернативне виконання цієї функції;
* некритична помилка або порушення – у разі виявлення порушення або проблеми, яка заважає користувачеві виконувати необхідні функції, але існує альтернативне виконання функції, або у разі виявлення порушення, що викликає труднощі при використанні ПЗ ПП, але це не впливає на роботу системних функцій ПП, або у разі, якщо помилка має незначний вплив на менше ніж 10 відсотків користувачів ПЗ ПП.

Виконавець повинен проаналізувати порушення або помилку та визначити спосіб її усунення не пізніше ніж через 12 годин після реєстрації в журналі помилок, незалежно від типу зареєстрованої помилки або порушення.

Терміни для усунення помилок або порушень узгоджуються із Замовником, але не можуть бути більше ніж:

* 24 годин для критичних;
* 14 днів для некритичних.

Розрахунок часового періоду починається з моменту повідомлення про порушення або помилку / критичну помилку Виконавцю.

Інформація про виправлені помилки або порушення оновлюється та подається у формі звітів раз на 3 місяці.

Замовник може, але не зобов’язаний, придбати додаткові робочі години послуг Виконавця для додаткової роботи з технічного обслуговування та розвитку ПЗ ПП. Потреба в придбанні цієї роботи може виникнути як результат:

* змін в правовому середовищі, що регулює діяльність Замовника;
* інші зовнішні фактори ризику, які не були передбачені під час проектування та впровадження ПЗ ПП;
* відсутність в Замовника фахівців необхідної кваліфікації для налаштування та підтримки працездатності ПЗ ПП.

Додаткові послуги з підтримки та розвитку ПП можуть включати:

* впровадження функціональних можливостей, що не передбачені вимогами до ПЗ ПП, тобто модифікації ПЗ згідно додаткової потреби у функціональності. У кожному окремому випадку, перед початком роботи Виконавець повинен детально розглянути та узгодити із Замовником опис запланованої розробки додаткових модифікацій, часові витрати з їх обґрунтуванням та кінцевий термін реалізації;
* надання підтримки у відновленні функціональних можливостей операційної системи, наприклад, після виникнення порушень в роботі бази даних або окремих її компонентів, коли характер порушень не є об’єктом сервісного обслуговування.

Замовник повинен купувати додаткові послуги з підтримки та розвитку ПП як окрему від основного контракту послугу.

При впровадженні додаткових послуг підтримки та розробки ПЗ ПП повинна зберігатись функціональність, надійність і забезпечуватись швидка відновлюваність ПП після порушень. Усі дії Виконавця із впровадження ПП при наданні додаткових послуг з підтримки та розробки ПП повинні виконуватися відповідно до процедури, погодженої з Замовником.

У разі якщо проблеми або помилки ПП спричинені внаслідок надання додаткових послуг підтримки та розробки ПП, описаних у цьому розділі, їх видалення та виправлення повинне здійснюватися як гарантійне.

# Висновки

Створення ПП є дієвим, ефективним та по суті необхідним засобом досягнення цілей, визначених Законом України «Про судоустрій і статус суддів», Законом України «Про запобігання корупції», стратегічних та програмних документах Кабінету Міністрів України, міжнародних документах щодо запобігання корупції в Україні.

Поліпшення якості робочих процесів, що автоматизуються, досягається завдяки максимальному впровадженню безпаперової технології на всіх етапах формування та аналізу інформації, прискоренню документообігу, використанню електронної ідентифікації з обов’язковим використанням КЕП, застосуванню дієвого контролю на всіх технологічних операціях, застосуванню більш сучасних технічних засобів, уніфікації форм документів та концентрацією обміну повідомленнями між різними системами (зовнішніми та внутрішніми) через єдину точку.

# Додатки

## Додаток 1. Макет інформаційної картки по суб’єкту перевірки

Розділ 1. Інформація про суб'єкта

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Прізвище | Імʼя | По батькові (за наявності) | РНОКПП (за наявності) | Дата народження |
|  |  |  |  |  |

Розділ 2. Інформація про членів сім’ї суб’єкта та близьких осіб

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Зв’язок із суб’єктом | Прізвище | Імʼя | По батькові (за наявності): | РНОКПП (за наявності) | Дата народження |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Розділ 3. Об'єкти нерухомості

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ПІБ суб’єкта або члена сім’ї | Вид об’єкта | Дата набуття права | Вартість на дату набуття | …  Інші ключові поля  … | Перегляд оригінальної відповіді | Перегляд візуального відображення |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Розділ 4. Транспортні засоби

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ПІБ суб’єкта або члена сім’ї | Вид об’єкта | Дата набуття права | Вартість на дату набуття | …  Інші ключові поля  … | Перегляд оригінальної відповіді | Перегляд візуального відображення |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Розділ Х. «Назва зовнішнього джерела інформації»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ПІБ суб’єкта або члена сім’ї | Вид об’єкта обліку | …  Інші ключові поля  … | Перегляд оригінальної відповіді | Перегляд візуального відображення |
|  |  |  |  |  |
|  |  |  |  |  |

## Додаток 2. Перелік зовнішніх джерел інформації

В рамках реалізації проекту Виконавець має забезпечити реалізацію інформаційної взаємодії з наведеними ЗДІ, щодо надання та отримання даних, з власниками яких на момент завершення етапу підготовки Технічного завдання будуть підписані відповідні документи (договори, протоколи обміну, інше), які встановлюють правові відносини, щодо інформаційної взаємодії.

|  |  |  |
| --- | --- | --- |
| № | Назва реєстру | Володілець / Технічний адміністратор |
| 1 | Державний реєстр актів цивільного стану громадян | Мінюст, НАІС |
| 2 | Державний реєстр речових прав на нерухоме майно | Мінюст, НАІС |
| 3 | Державний реєстр обтяжень рухомого майна | Мінюст, НАІС |
| 4 | Єдиний державний реєстр транспортних засобів | МВС |
| 5 | Єдиний реєстр довіреностей | Мінюст, НАІС |
| 6 | Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань | Мінюст, НАІС |
| 7 | Єдиний державний реєстр судових рішень | ДСА |
| 8 | Державний реєстр фізичних осіб – платників податків | Державна податкова служба України |
| 9 | Інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон, «АРКАН» | Адміністрація Державної прикордонної служби України |
| 10 | Державний земельний кадастр | Державна служба України з питань геодезії, картографії та кадастру |
| 11 | Інформаційні бази даних національної комісії з цінних паперів та фондового ринку | Національна комісія з цінних паперів та фондового ринку про ринок цінних паперів |

## Додаток 3. Графік реалізації етапів

**Орієнтовний графік реалізації етапів життєвого циклу ПП**

|  |  |  |
| --- | --- | --- |
| **Етап робіт** | **Результат етапу** | **Термін виконання** |
| 1. Технічне завдання | Технічне завдання - затверджено | 2 місяці з дати підписання договору |
| 1. Розроблення ПП | Програмний продукт - розроблено  Програмний продукт в достатньому для проведення попередніх випробувань обсязі - поставлено | 6 місяці з дати підписання договору |
| 1. Дослідна експлуатація ПП | Тестування програмного забезпечення ПП в обсязі попередніх випробувань – проведено.  Навчання користувачів – проведено.  Дослідна експлуатація ПП - проведена | 7 місяць з дати підписання договору |
| 1. Супровід ПП | Надання послуг щодо гарантійного обслуговування ПП – 12 місяців | 12 місяців з дати підписання Акту прийняття послуг Етапу «Дослідна експлуатація ПП» |

Допускається виконання окремих етапів проекту до завершення попередніх етапів, паралельне по часу виконання етапів проекту, включення нових етапів проекту з урахуванням специфіки ПП, що будуються.

## Додаток 4. Вимоги до потенційних виконавців

Враховуючи вимоги до ПП та обсяг робіт на їх створення, рекомендується встановити наступні кваліфікаційні вимоги до організацій-розробників, яких необхідно залучити до створення ПП, за наступними критеріями:

**Фінансова спроможність**

За останні 3 (три) роки учасник торгів повинен мати середній річний оборот не менше ніж сто тисяч (100 000) доларів США або еквівалент цієї суми в інших валютах за крос-курсом Національного банку України на кінець відповідного року.

**Досвід роботи та технічна спроможність**

За останні 5 (п’ять) років учасник торгів повинен був успішно виконати щонайменше два (2) договори на:

* розробку, постачання, впровадження, забезпечення гарантійного/післягарантійного обслуговування та/або технічного супроводу експлуатації аналогічних інформаційних систем (автоматизованих інформаційних систем, які мають схожі функціональні та технічні характеристики до ПП, що створюються);
* розробку та впровадження, або забезпечення технічного супроводження експлуатації автоматизованого обміну даних між державними реєстрами та інформаційними базами даних.

**Персонал**

Учасник торгів повинен мати кваліфікований персонал у наступному складі:

* Керівник проекту;
* Архітектор/керівник групи розробників ПЗ;
* Аналітик;
* Інженер баз даних;
* Розробник ПЗ (2 особи);
* DevOps;
* Спеціаліст з підготовки документації;
* Системний адміністратор;
* Тестувальник.

**Наявність обладнання та матеріально-технічної бази**

Учасник повинен володіти, чи мати доступ до матеріально-технічної бази, яка в повній мірі дозволить самостійно без використання інфраструктури Замовника реалізувати розробку програмного забезпечення ПП, а саме: наявність відповідних обчислювальних потужностей (сервери, комп’ютери та інші засоби автоматизації), телекомунікаційних (комутаційних) потужностей та ліцензійного програмного забезпечення.