Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

Роз’яснення
від 4 серпня 2026 року

Цим роз'ясненням громадська організація «Лабораторія законодавчих ініціатив» надає відповіді на запитання, що надійшли від потенційного учасника процедури закупівлі.

1.Запитання:
Чи передбачається адаптація існуючих систем (як то Keycloak для керування доступом та xWiki для організації бази знань) замість їх розробки? Які критерії використовуються, щоб визначити, що адаптація існуючої системи є прийнятною з урахуванням її можливостей і обмежень, які можуть не мати повної відповідності вимогам?

Відповідь:
Так, у межах реалізації Системи допускається використання, адаптація, розширення та інтеграція наявних програмних рішень, зокрема таких, як Keycloak, xWiki та інших компонентів із відкритим вихідним кодом або комерційних продуктів, за умови погодження відповідного рішення з Власником Системи та Замовником.

У разі якщо певна функціональність не підтримується обраним рішенням у повному обсязі, Виконавець повинен надати обґрунтування прийнятності відповідних обмежень, опис компенсуючих заходів та оцінку їх впливу на архітектуру, експлуатацію, безпеку, вартість і строки реалізації проєкту. Остаточне рішення щодо можливості використання такого підходу ухвалюється Власником Системи та Замовником.

2.Запитання:
Чи має замовник чинні інтеграції з Diia, BankId, Viber, Telegram, WhatsApp, SMS провайдерами та іншими переліченими в вимогах поставниками послуг, включаючи відповідні контракти?

Відповідь:
Так, Власник Системи та Замовник уже мають чинні інтеграції та необхідні договірні відносини з низкою зовнішніх постачальників послуг, зокрема із сервісами електронної ідентифікації, обміну повідомленнями та іншими інформаційними системами, визначеними вимогами до Системи.

Перед початком виконання робіт Виконавцю буде надано доступ до відповідних середовищ розроблення, тестування та інтеграції, а також усю необхідну

технічну документацію, облікові дані, сертифікати, ключі доступу та інші артефакти в обсязі, необхідному для виконання робіт.

Водночас слід ураховувати, що перелік інтеграцій, їхня конфігурація, порядок підключення, умови використання та склад доступних середовищ можуть відрізнятися залежно від конкретного постачальника послуг. У разі необхідності укладення додаткових договорів, розширення чинних угод або зміни умов взаємодії відповідні питання вирішуватимуться Власником Системи та Замовником.

3.Запитання:
Чи правильним є припущення: розроблюваний компонент не виконує підпис документів, не виконує обробку ключів користувачів, не виконує збереження ключів користувачів; компонент виконує інтеграцію з зазначеними державними засобами ідентифікації та підпису та перевіряє надані ними дані та накладені ними підписи?

Відповідь:
Ні, зазначене припущення є правильним лише частково. Відповідно до технічних вимог робота з довірчими послугами забезпечується трьома окремими складовими:

• **крипто-сервіс** забезпечує перевірку електронних підписів, об’єднання підписаних даних, а також підписання сформованих Системою довідок, витягів та інших документів;

• **віджет автентифікації** використовується для автентифікації користувачів;

• **віджет підпису** забезпечує виконання користувачем юридично значущих дій шляхом накладення КЕП/УЕП.

Таким чином, Система не лише перевіряє дані та підписи, отримані від зовнішніх державних засобів, а й забезпечує накладення підпису користувачем через відповідний віджет. Для окремих сценаріїв віджет підпису також має підтримувати збереження зчитаного ключа в межах активної сесії для подальшого накладення підписів без повторного вибору ключа та введення пароля — за налаштуванням користувача та з урахуванням визначених обмежень.

4.Запитання:
Яким чином передбачається затверджувати структуру майстер-реєстрів з урахуванням наявності тільки загальних відомостей про їх наповнення? Який термін та яка відповідальність сторін передбачаються для остаточного затвердження?

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

Відповідь:
Структура, склад атрибутів, правила ведення, моделі даних, зв'язки між сутностями, вимоги до якості даних, а також порядок синхронізації та наповнення майстер-реєстрів є складовою етапу формування та погодження технічного завдання.

На зазначеному етапі Виконавець повинен провести аналіз наявних даних, бізнес-процесів, інтеграційних взаємодій, нормативних вимог та особливостей функціонування окремих підсистем, після чого підготувати відповідні пропозиції щодо структури майстер-реєстрів. Остаточне рішення щодо їх складу та структури ухвалюється Власником Системи та Замовником.

Терміни підготовки, погодження та затвердження відповідних рішень визначатимуться календарним планом виконання робіт і положеннями технічного завдання. Кожна зі сторін несе відповідальність за своєчасне виконання покладених на неї обов'язків, зокрема щодо надання необхідних матеріалів, проведення аналізу, підготовки пропозицій та ухвалення рішень. У разі виникнення затримок, пов'язаних із несвоєчасним погодженням відповідних рішень, строки виконання робіт підлягатимуть перегляду за погодженням сторін.

5.Запитання:
Яким чином очікується виконання інтеграції з державними реєстрами, наприклад, ЄДР? Чи передбачається використання уніфікованого доступу через Трембіту? Які терміни закладаються замовником на заключення контрактів для доступу до державних реєстрів?

Відповідь:
Інтеграція з державними реєстрами та інформаційними системами, зокрема з ЄДР, повинна здійснюватися із застосуванням уніфікованих механізмів міжсистемної взаємодії. Пріоритетним підходом є використання системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», якщо відповідний сервіс доступний через зазначену систему.

У випадках, коли використання «Трембіти» є неможливим або недоцільним, можуть застосовуватися інші передбачені законодавством способи інтеграції, зокрема через API, захищені канали зв'язку, черги повідомлень або інші технологічні механізми, погоджені Власником Системи та Замовником.

До початку виконання відповідних робіт Власник Системи або її Розпорядник повинні забезпечити надання Виконавцю необхідних доступів, технічної документації, специфікацій, сертифікатів, тестових середовищ та інших матеріалів, необхідних для реалізації інтеграційної взаємодії.

Строки укладення договорів, отримання дозволів, організації інформаційної взаємодії та підключення до державних реєстрів не входять до сфери

відповідальності Виконавця та повинні бути забезпечені Власником Системи або її Розпорядником до початку виконання відповідних робіт. У разі виникнення затримок строки реалізації пов'язаних завдань підлягатимуть відповідному коригуванню.

6.Запитання:
Чи виконано правову та безпекову оцінку даних, що мають міститися в майстер-реєстрах; або, яким чином очікується надавати правову та безпекову оцінку цих даних?

Відповідь:
Правова та безпекова оцінка інформації, що обробляється в ЄСІКС, уже здійснюється в межах функціонування наявних підсистем, оскільки відповідні дані вже використовуються під час виконання визначених законодавством функцій.

Запровадження майстер-реєстрів не передбачає появи принципово нових категорій даних, а спрямоване насамперед на зменшення кількості міжсистемних запитів, забезпечення узгодженості інформації, підвищення якості даних і формування єдиного достовірного джерела інформації для всіх компонентів ЄСІКС.

Водночас склад даних, правила їх актуалізації, моделі доступу, механізми синхронізації, строки зберігання, порядок журналювання дій та інші організаційні й технічні аспекти функціонування майстер-реєстрів підлягатимуть додатковому опрацюванню під час формування технічного завдання.

У разі необхідності внесення змін до порядку оброблення інформації, складу даних або механізмів доступу відповідна правова та безпекова оцінка здійснюватиметься Власником Системи та Замовником із залученням профільних експертів.

7.Запитання:
Який підхід до керування ризиками та побудови реєстру ризиків (risk registry) передбачається замовником? Яким чином передбачається реагувати на ризики, які не вдалося оминути чи пом’якшити, зважаючи на фіксовану вартість проєкту?

Відповідь:
Виконавець може запропонувати власний підхід до управління ризиками у складі комерційної пропозиції. Після погодження із Замовником та Власником Системи він може бути використаний як єдиний механізм управління ризиками протягом усього життєвого циклу проєкту. Такий підхід може передбачати ведення реєстру ризиків (risk register), визначення власників ризиків, їх пріоритизацію, механізми ескалації та порядок реагування.

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

У разі реалізації ризиків, які не вдалося усунути або мінімізувати, подальші дії визначатимуться сторонами залежно від їхнього впливу на строки, обсяг робіт і результати проєкту. За потреби можуть застосовуватися передбачені договором механізми управління змінами, перегляду пріоритетів або коригування плану реалізації.

8.Запитання:
Який підхід до керування змінами та побудови каталогу змін (change log) передбачено замовником? Яким чином передбачається обробляти зміни зважаючи на фіксовану вартість проєкту?

Відповідь:
Управління змінами здійснюватиметься в межах визначеного процесу керування вимогами та змінами до Системи.

Орієнтовний порядок опрацювання змін передбачає такі етапи:

• реєстрацію запиту на зміну із зазначенням його опису, обґрунтування, очікуваного результату, пріоритету та потенційного впливу на архітектуру, строки, бюджет і обсяг робіт;

• аналіз та погодження запиту на зміну Власником, Замовником, Адміністратором або іншими уповноваженими сторонами;

• визначення способу реалізації змін, оцінку необхідних ресурсів, строків та вартості виконання;

• реалізацію, тестування, введення змін в експлуатацію та їх документування.

Остаточний порядок управління змінами, перелік ролей, порядок ухвалення рішень, а також критерії класифікації змін визначатимуться на етапі ініціації проєкту.

9.Запитання:
Який підхід до керування продуктовим планом (product backlog) передбачається замовником? А саме, якими є підхід до пріоритетів вимог, очікувана тривалість ітерації, частота проміжних демонстрацій тощо?

Відповідь:
Виконавець може запропонувати власний підхід до формування та управління продуктовим планом (product backlog), зокрема принципи пріоритизації вимог, тривалість ітерацій, формат проведення демонстрацій, порядок планування робіт та механізми уточнення вимог. Після погодження зі стейкхолдерами проєкту відповідний підхід може бути використаний як базова модель управління реалізацією проєкту.

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

Водночас Замовник очікує поетапну реалізацію Системи з орієнтовною послідовністю, що передбачає створення інфраструктурного середовища, впровадження підсистеми керування доступом (IAM), реалізацію ЄППК та майстер-реєстрів, а також подальше виконання інтеграції, міграції даних і фінального приймання результатів робіт. Остаточний порядок реалізації визначатиметься під час планування проєкту.

10.Запитання:
Які безпекові заходи виконуються командами замовника (та на якому етапі) або очікуються від команди розробника? А саме: моделювання загроз (threat modeling), захист під час виконання (runtime protection), захист під час розгортання (deployment policies), тестування на проникнення (penetration testing).

Відповідь:
Виконавець повинен побудувати процес безпечної розробки, розгорнути та налаштувати середовища, CI/CD-конвеєри й інші компоненти інфраструктури відповідно до вимог розділу 6.4 «Вимоги до захисту інформації» та затверджених профілів безпеки. До обсягу відповідальності Виконавця належать, зокрема, опрацювання загроз під час проєктування архітектури, впровадження політик безпечного розгортання, автоматизованих перевірок коду, залежностей і конфігурацій, а також налаштування передбачених архітектурою механізмів захисту під час виконання Системи.

Виконавець може самостійно організовувати тестування на проникнення протягом розробки. Незалежне тестування на проникнення організовується Власником Системи та Замовником; виявлені зауваження середнього, високого та критичного рівнів мають бути усунені Виконавцем до приймання. Детальний розподіл заходів, строки їх виконання, методики та склад підтвердних артефактів визначатимуться під час формування технічного завдання й погодження процесу безпечної розробки.

11.Запитання:
Які саме засоби статичного та динамічного аналізу очікується використовувати? Чи очікується інтеграція цих засобів у процеси безперервної інтеграції?

Відповідь:
Так, очікується інтеграція засобів статичного та динамічного аналізу безпеки до процесів безперервної інтеграції та безперервного розгортання (CI/CD). Такі перевірки мають охоплювати аналіз вихідного коду, програмних залежностей, контейнерних образів, конфігурацій, інфраструктури як коду, а також інші перевірки, передбачені вимогами до безпечної розробки.

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

Водночас конкретний перелік інструментів, порядок їх застосування, періодичність виконання перевірок, критерії прийнятності результатів, а також вимоги щодо усунення виявлених недоліків визначатимуться на етапі формування та погодження технічного завдання. Виконавець також може запропонувати власний перелік інструментів і підходів, виходячи з обраного технологічного стеку та архітектури рішення.

12.Запитання:
Які система оцінки вразливостей використовується (vulnerability scoring system) замовником для визначення важливості вразливості?

Відповідь:
Конкретна система оцінювання вразливостей (vulnerability scoring system), яка використовуватиметься в межах проєкту, буде визначена під час формування та погодження технічного завдання, а також відповідних процесів безпечної розробки та експлуатації.

Водночас Виконавець може запропонувати власний підхід до класифікації та пріоритизації вразливостей. Перевага надаватиметься загальновизнаним міжнародним практикам і стандартам, зокрема CVSS, CWE, CAPEC та OWASP ASVS. Остаточний порядок класифікації вразливостей, критерії визначення їх критичності, а також строки усунення виявлених недоліків погоджуватимуться сторонами окремо.

13.Запитання:
Які рішення передбачені замовником для керування ключами та сертифікатами? Які з цих рішень вже адаптовані замовником?

Відповідь:
Виконавець може запропонувати рішення для централізованого керування ключами шифрування, сертифікатами та системними паролями відповідно до вимог розділу 7.4.1 «Управління ключами шифрування та системними паролями». Запропоноване рішення має забезпечувати безпечне зберігання, видачу, ротацію, відкликання, аудит використання та розмежування доступу до ключів, сертифікатів і секретів, а також інтеграцію з компонентами Системи та процесами розгортання.

Конкретний програмний продукт, архітектура його розгортання та порядок використання визначатимуться на етапі формування і погодження технічного завдання та архітектури. Наявність уже адаптованого Замовником рішення технічними вимогами не визначена; у разі наявності відповідна інформація, доступи та інтеграційні вимоги будуть надані Виконавцю під час проєктування.

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

14.Запитання:
Яким чином буде проводитися обмежене та загальне тестування? А саме: протоколи тестування, кількість користувачів, терміни тестування та доробки продукту?

Відповідь:
Порядок проведення обмеженого та загального тестування, а також процедура приймання результатів робіт визначаються відповідно до вимог розділів 8 «Вимоги до супроводу та обслуговування засобу інформатизації» та 9 «Вимоги до приймання засобу інформатизації».

Очікується, що Виконавець розробить і погодить необхідні програми та методики випробувань, тестові сценарії, критерії успішного проходження тестування, порядок усунення виявлених недоліків, а також підготує відповідні звіти та підтвердні матеріали.

Кількість користувачів, тривалість окремих етапів тестування, обсяги навантаження, порядок проведення дослідної експлуатації, строки усунення зауважень і критерії переходу між етапами визначатимуться під час формування технічного завдання та погодження плану реалізації проєкту. При цьому Замовник залишає за собою право залучати до тестування представників різних категорій користувачів, адміністраторів, експертів та інших заінтересованих сторін.

15.Запитання:
Чи надає замовник профілі тестування на навантаження (кількість запитів, час тестування, об’єми даних), чи очікує їх розробку? На якій інфраструктурі передбачається проведення тестування на навантаження?

Відповідь:
Профілі навантажувального тестування повинні бути розроблені Виконавцем на підставі вимог технічного завдання, цільових показників продуктивності, архітектурних рішень, очікуваних сценаріїв використання Системи та прогнозованих обсягів даних.

Очікується, що такі профілі охоплюватимуть, зокрема, кількість одночасних користувачів, інтенсивність виконання операцій, допустимі показники затримок, тривалість тестування, обсяги даних, сценарії пікового навантаження, а також перевірку стійкості та відмовостійкості Системи.

Навантажувальне тестування проводитиметься на інфраструктурі Власника Системи. Детальні параметри середовища, необхідні обчислювальні ресурси, конфігурації, порядок проведення випробувань та критерії успішного проходження тестування визначатимуться на етапі формування та погодження технічного завдання.

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

16.Запитання:
Які інфраструктурні рішення передбачені замовником для загальнодоступного розгортання (prod середовище)? А саме: зовнішні захисні системи (DDOS and CAPTCHA protection), зовнішні мережеві шлюзи (gateways), внутрішні системи контролю трафіку (meshes), системи кластеризації (clusters), системи збору та аналізу телеметрії (telemetry collectors) та інше? Які з цих рішень вже адаптовані замовником?

Відповідь:
Інфраструктурні рішення для продуктивного середовища пропонуються Виконавцем за погодженням із Власником та Замовником Системи. Запропоновані рішення повинні відповідати вимогам, визначеним у розділі 6 «Нефункціональні вимоги» та розділі 7 «Технологічний стек».

Зокрема, це стосується рішень для захисту від DDoS-атак, механізмів CAPTCHA, зовнішніх шлюзів і балансувальників навантаження, сервісних мереж (service mesh), кластерних рішень, систем журналювання, моніторингу, збору телеметрії, централізованого керування конфігураціями та інших компонентів інфраструктурного контуру.

У разі наявності вже впроваджених компонентів або обмежень щодо використання окремих технологій відповідна інформація буде надана Виконавцю на етапі формування та погодження технічного завдання.

17.Запитання:
Які саме ресурси (параметри машин, наявність мережевих шлюзів, систем кластеризації, систем телеметрії і таке інше) надаються для розгортання?

Відповідь:
Власник Системи надає Виконавцю доступ до обчислювальних ресурсів, достатніх для розгортання необхідних середовищ, виконання робіт із розробки, тестування та впровадження Системи.

Конкретні параметри інфраструктури, зокрема характеристики віртуальних машин, параметри мережевої взаємодії, наявність балансувальників навантаження, шлюзів, кластерних рішень, засобів моніторингу, журналювання, збору телеметрії та інших компонентів інфраструктурного контуру, визначатимуться на етапі формування та погодження технічного завдання.

У разі недостатності наявних ресурсів Виконавець повинен надати обґрунтовані вимоги щодо їх розширення з урахуванням архітектурних рішень, запропонованих відповідно до вимог розділів 6 «Нефункціональні вимоги» та 7 «Технологічний стек».

Лабораторія
законодавчих ініціатив

оф. 404, вул. Воздвиженська, 45, Київ, 04071
info@parliament.org.ua | +38 (044) 531 37 68

18.Запитання:
Які інфраструктурні рішення передбачені замовником для безперервної інтеграції? А саме: сервера автоматизації (automation server), системи контролю походження (provenance systems), реєстри образів (image registries), специфікації інфраструктури (infrastructure as code)? Які з цих рішень вже адаптовані замовником? Які з цих рішень надаються замовником і не потребують розгортання командою розробки?

Відповідь:
Рішення, пов'язані із забезпеченням процесів безперервної інтеграції та безперервного постачання (CI/CD), повинні бути розгорнуті Виконавцем з нуля на обчислювальних ресурсах, наданих Власником Системи.

Зокрема, це стосується серверів автоматизації, реєстрів контейнерних образів, засобів керування конфігурацією та інфраструктурою як кодом (Infrastructure as Code), систем контролю походження артефактів (provenance systems), засобів автоматизованого тестування, а також інших компонентів, необхідних для забезпечення процесів розробки, тестування, постачання та супроводу Системи.

Архітектура відповідних рішень, порядок їх розгортання та склад компонентів визначаються Виконавцем і погоджуються із Власником та Замовником Системи з урахуванням вимог розділів 6 «Нефункціональні вимоги» та 7 «Технологічний стек».

Технічними вимогами не передбачено використання заздалегідь адаптованих або розгорнутих Замовником інструментів безперервної інтеграції, тому Виконавець повинен врахувати необхідність їх первинного розгортання та налаштування.

19. Запитання:
Які підходи до розгортання (rollout, blue-green, canary) очікується застосовувати та які інфраструктурні рішення для цього передбачені замовником? Які з цих рішень вже адаптовані замовником?

Відповідь:
Вибір відповідного підходу здійснюється Виконавцем та погоджується із Власником і Замовником Системи з урахуванням архітектури рішення, вимог до доступності Системи та особливостей її експлуатації.

Необхідні інфраструктурні рішення для підтримки відповідних механізмів розгортання пропонуються та розгортаються Виконавцем з нуля на обчислювальних ресурсах, наданих Власником Системи.

Зокрема, це може стосуватися балансувальників навантаження, шлюзів, засобів оркестрації контейнерів, сервісних мереж (service mesh), систем моніторингу,

журналювання, збору телеметрії та інших компонентів інфраструктурного контуру.

Усі запропоновані рішення повинні відповідати вимогам розділів 6 «Нефункціональні вимоги» та 7 «Технологічний стек». Технічними вимогами не передбачено використання заздалегідь адаптованих або розгорнутих Замовником рішень для реалізації зазначених підходів.