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.

Запитання:
Чи існує чинна угода між Державною судовою адміністрацією та Міністерством цифрової трансформації щодо push-повідомлень через Дію; чи буде надано технічну документацію та тестовий контур API Дія Push на етапі проєктування?

Відповідь:
У межах предмета закупівлі передбачається, що Власник Системи або визначений Державною судовою адміністрацією України розпорядник Системи забезпечить необхідні організаційні та технічні передумови для здійснення відповідної інтеграції, зокрема шляхом укладення угод про інформаційну взаємодію, якщо це передбачено встановленими процедурами.

Після виконання необхідних організаційних заходів Виконавцю буде надано документацію, технічні специфікації, параметри взаємодії та доступ до тестового середовища, необхідні для реалізації та перевірки інтеграції. При цьому склад і порядок надання відповідних матеріалів визначатимуться Власником Системи з урахуванням вимог до інформаційної безпеки та правил взаємодії із зовнішніми інформаційними системами.

Запитання:
Чи прийнятний канал WhatsApp з огляду на те, що з 23.10.2025 доступний лише Cloud API, хостований Meta (транзит через закордонну інфраструктуру, модерація шаблонів Meta)?

Відповідь:
Відповідно до розділу 5.2.2 Технічних вимог Система повинна забезпечувати можливість взаємодії із зовнішніми провайдерами доставки повідомлень, зокрема шляхом інтеграції з офіційними чат-ботами Viber, Telegram та WhatsApp. При цьому Технічні вимоги визначають функціональну можливість використання відповідних каналів, а не конкретний спосіб їх технічної реалізації.

Остаточне рішення щодо використання конкретного каналу, зокрема WhatsApp, ухвалюватиметься з урахуванням вимог законодавства України, політик інформаційної безпеки, порядку обробки інформації в ЄСІКС, умов використання відповідного сервісу та наявних технічних обмежень. У разі невідповідності

певного каналу встановленим вимогам можуть застосовуватися альтернативні способи доставки повідомлень, передбачені Технічними вимогами.

Запитання:
Хто укладає та оплачує договори з SMS/Viber-агрегаторами (поштучна тарифікація — операційні витрати Власника); чи є чинні договори, під API яких слід адаптуватися?

Відповідь:
Договори із провайдерами доставки повідомлень (SMS, Viber, Telegram, WhatsApp та іншими) укладаються та оплачуються Власником Системи або визначеним Державною судовою адміністрацією України розпорядником Системи. Відповідні витрати належать до операційних витрат, пов'язаних з експлуатацією ЄСІКС, і не входять до предмета цієї закупівлі.

Запитання:
Яка очікувана політика маршрутизації каналів (частки платних SMS/Viber проти in-app/e-mail/push) — для операційного бюджету на 1,1 млрд повідомлень/рік (вилка 15–180 млн грн/рік)?

Відповідь:
Політика маршрутизації повідомлень визначатиметься з урахуванням функціонального призначення повідомлення, персональних налаштувань користувача, вимог законодавства України щодо обов'язкових способів інформування, доступності відповідних каналів зв'язку, а також вимог до надійності, швидкості доставки та інформаційної безпеки.

На цьому етапі конкретні цільові показники щодо співвідношення між платними та безоплатними каналами доставки повідомлень (SMS, Viber, push-повідомлення, електронна пошта, внутрішні повідомлення тощо) не визначені. Відповідна політика маршрутизації, пріоритетність каналів і правила їх використання будуть деталізовані під час підготовки та погодження технічного завдання.

Водночас зазначений підхід не обмежує можливості застосування механізмів оптимізації витрат, зокрема шляхом пріоритетного використання внутрішніх повідомлень, електронної пошти та push-сповіщень у випадках, коли це не суперечить вимогам законодавства та функціональним вимогам Системи.

Запитання:
Імпорт історичних даних нотифікацій: з яких систем, у якому обсязі та за який період підлягають перенесенню повідомлення/журнали доставки?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Склад історичних даних, що підлягатимуть перенесенню, визначатиметься на етапі аналізу джерел даних, підготовки Методології міграції та формування технічного завдання. Остаточний перелік даних погоджуватиметься Адміністратором Системи з урахуванням їхньої актуальності, цінності для функціонування ЄСІКС, вимог законодавства та технічної доцільності такого перенесення.

Відповідно до пункту 6.14 Технічних вимог, Виконавець повинен забезпечити можливість перенесення не лише основних даних, а й метаданих, журнальних активностей та інших подій, склад яких уточнюватиметься під час підготовки технічного завдання.

Запитання:
Семантика показника «Нотифікації через ЕК — к-ть створених» (1,1 млрд/2025): одиниця виміру — подія, нотифікація отримувачу чи доставка в канал; чи враховано розмноження однієї події на кількох отримувачів (fan-out); це статистика, прогноз чи вимога до приймання?

Відповідь:
Показник «Нотифікації через ЕК — кількість створених» відображає статистичну кількість сформованих нотифікацій для окремих отримувачів. У разі коли одна подія є підставою для інформування кількох користувачів, кожна сформована для відповідного отримувача нотифікація враховується окремо, тобто показник включає розмноження повідомлень за отримувачами.

Запитання:
Профіль пікового навантаження доставки (бізнес-рівень): очікувані інтенсивність × тривалість піку, допустимий вік черги невідправлених повідомлень, цільові строки доставки P95/P99 за класами пріоритету (робочий коефіцієнт — ×20…×100)?

Відповідь:
Детальні параметри навантаження, зокрема очікувана інтенсивність і тривалість пікових періодів, допустимий час перебування повідомлень у черзі, цільові показники часу доставки (P95, P99), а також класи пріоритетності повідомлень визначатимуться на етапі формування та погодження технічного завдання.

Водночас під час проєктування рішення Виконавець повинен враховувати статистичні показники фактичного навантаження, вимоги щодо відмовостійкості, масштабованості та безперервності роботи Системи, а також забезпечити можливість горизонтального масштабування компонентів сервісу нотифікацій.

Лабораторія
законодавчих ініціатив

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

Остаточні значення зазначених показників будуть визначені за результатами аналізу бізнес-процесів, історичних даних та цільових сценаріїв використання Системи.

Запитання:
Viber/Telegram/WhatsApp: доставка через офіційний чат-бот (лише підписники, як буквально у п.9.2) чи розсилка за номером (Business Messages через агрегатора — інша цінова/юридична модель)?

Відповідь:
Сервіс нотифікацій повинен підтримувати обидва сценарії взаємодії з месенджерами: доставку повідомлень через офіційні чат-боти користувачам, які підписалися на відповідного бота, а також надсилання повідомлень за номером телефону через офіційні бізнес-інтерфейси месенджерів або визначених агрегаторів.

Можливість застосування кожного сценарію визначатиметься з урахуванням технічних можливостей і правил відповідного месенджера, наявності необхідної згоди та контактних даних користувача, вимог законодавства, політик інформаційної безпеки, а також укладених Власником Системи або визначеним Державною судовою адміністрацією України розпорядником Системи договорів із провайдерами. Детальні правила використання каналів та конкретні інтеграційні механізми будуть визначені на етапі формування і погодження технічного завдання.

Запитання:
Чи обходять обов'язкові нотифікації (недоступні для вимкнення) часові рамки і вибір каналів користувача; порядок резервної ескалації каналів та граничні строки для процесуально значущих повідомлень?

Відповідь:
Алгоритми формування, маршрутизації, повторного надсилання та ескалації повідомлень, зокрема правила обробки обов'язкових нотифікацій, порядок використання резервних каналів зв'язку, допустимі часові інтервали надсилання повідомлень, а також цільові строки доставки повідомлень різних категорій визначатимуться на етапі формування та погодження технічного завдання.

Під час визначення зазначених алгоритмів враховуватимуться вимоги законодавства України, функціональне призначення повідомлень, їхній пріоритет, персональні налаштування користувачів, а також вимоги до надійності, безперервності функціонування та інформаційної безпеки Системи.

Для процесуально значущих повідомлень можуть бути передбачені окремі правила обробки та доставки, якщо така необхідність випливатиме з вимог законодавства або затверджених бізнес-процесів.

Лабораторія
законодавчих ініціатив

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

Запитання:
Який строк зберігання повідомлень (retention) вимагається для сповіщень та міжмодульних подій (впливає на обсяг дискової підсистеми)?

Відповідь:
Технічні вимоги не встановлюють строку зберігання повідомлень у компоненті «Черга повідомлень». Пункт 7.4.6.2 визначає лише умову збереження — «збереження повідомлень до моменту успішного підтвердження отримання підписником», а також вимагає механізмів повторних спроб і переміщення повідомлень, які не вдалося обробити після визначеної кількості спроб, до окремої черги недоставлених повідомлень для подальшого аналізу та ручної обробки. Згідно з пунктом 7.4.6.1 компонент виконує функцію приймання, маршрутизації, тимчасового та/або постійного зберігання й гарантованої доставки повідомлень; зберігання самих нотифікацій та журналів доставки належить до сервісу нотифікацій (розділ 5.2.2).

Запитання:
Який очікуваний піковий коефіцієнт (пік/середнє) для потоку сповіщень ~1,1 млрд/рік? Прийняте у розрахунках значення ×20 потребує підтвердження

Відповідь:
Технічні вимоги не встановлюють пікового коефіцієнта. Розділ 6.11 наводить показники очікуваного навантаження, зокрема кількість створених нотифікацій через ЕК за 2025 рік — 1 100 000 000, та вимоги до часу обробки інформаційного запиту: 90 % запитів протягом 1 секунди, 95 % — протягом 2 секунд. Цей самий розділ встановлює загальну вимогу: «Архітектура системи має бути розрахована на пікові навантаження, у тому числі під час виникнення надзвичайних подій», а деградація часу відповіді під навантаженням має бути передбачуваною.

Розрахунковий піковий коефіцієнт визначатиметься на етапі формування та погодження технічного завдання за результатами аналізу історичних даних і цільових сценаріїв використання Системи, з подальшою перевіркою під час тестування під навантаженням (пункт 9.1.4). Незалежно від прийнятого значення компонент має забезпечувати вимогу пункту 7.4.6.2 щодо горизонтального масштабування — «можливість динамічного збільшення кількості обробників для забезпечення високої пропускної здатності в пікові періоди навантаження».

Запитання:
ТВ 6.6 вимагає георозподілення між дата-центрами; Концепція ЄСІКС (посилання у примітці нижче) передбачає три географічно розподілені центри обробки даних на відстані не менше 10 км у режимі «Active-Active-Standby» з доступністю 99,95% та вимогами рівня TIER III. Чи є ця цільова топологія чинною та чи наявні відповідні майданчики на момент впровадження?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Цільова топологія, визначена Концепцією ЄСІКС, залишається чинною. Під час проєктування та реалізації Системи Виконавець повинен враховувати вимоги щодо географічного розподілення центрів обробки даних, забезпечення відмовостійкості, безперервності функціонування та досягнення встановлених показників доступності.

Водночас предметом закупівлі є розроблення, налаштування, впровадження та супровід програмних компонентів Системи, а не створення або модернізація фізичної інфраструктури центрів обробки даних. Необхідні обчислювальні ресурси, канали зв'язку, сховища даних та інші складові інфраструктури надаватимуться Власником Системи.

Розгортання програмних компонентів здійснюватиметься з урахуванням фактично доступної на момент впровадження інфраструктури та затвердженої цільової архітектури ЄСІКС.

Запитання:
Який режим георозподілення очікується для кластера черг повідомлень — один активний майданчик із резервним чи два активних?

Відповідь:
Конкретний режим географічного розподілення кластера сервісу обробки повідомлень, зокрема використання конфігурацій «Active-Standby», «Active-Active» або іншої моделі, визначатиметься на етапі формування технічного завдання та погодження цільової архітектури, запропонованої Виконавцем.

Під час вибору відповідної архітектури мають бути враховані вимоги щодо відмовостійкості, масштабованості, продуктивності, безперервності функціонування, цілісності даних, допустимого часу відновлення, а також особливості обраних технологічних рішень.

Запропонована Виконавцем архітектура повинна відповідати загальним вимогам до географічного розподілення компонентів ЄСІКС та забезпечувати можливість функціонування Системи в цільовій інфраструктурі, що надаватиметься Власником Системи.

Запитання:
Який допустимий показник можливої втрати даних (RPO) між майданчиками для кластера черг повідомлень?

Відповідь:
Пункт 6.6 визначає лише RTO — не більше 2 годин, і водночас містить вимогу: «Збереження інформації, що обробляється в складових Системи, повинно бути гарантоване у повному обсязі, втрата даних не допускається». У межах одного

майданчика збереження підтверджених повідомлень забезпечується вимогою пункту 7.4.6.2 щодо гарантованої доставки та кластерним розгортанням за пунктом 7.4.6.3.

Допустимий показник можливої втрати даних між майданчиками, а також механізм реплікації визначатимуться на етапі формування та погодження технічного завдання.

Запитання:
Чи вимагаються сертифіковані засоби КЗІ (експертний висновок ДССЗЗІ) для шифрування даних у стані спокою в підсистемі управління ключами, чи достатньо OSS-механізмів у складі КСЗІ?

Відповідь:
На поточному етапі пріоритетним є використання механізмів шифрування та управління ключами, реалізованих на базі програмного забезпечення з відкритим вихідним кодом (OSS), за умови забезпечення відповідності затвердженим вимогам у сфері захисту інформації.

Водночас конкретний перелік засобів криптографічного захисту інформації, зокрема вимоги щодо використання сертифікованих засобів КЗІ, порядку управління ключами, алгоритмів шифрування та підтвердження відповідності профілям безпеки, визначатиметься на етапі формування технічного завдання та доведення затверджених профілів безпеки.

Використання сертифікованих засобів або окремих компонентів, що мають експертний висновок чи інші документи про відповідність вимогам законодавства України, може бути передбачене в тих випадках, коли така вимога випливатиме з чинних нормативно-правових актів або затверджених профілів безпеки Системи.

Запитання:
Чи допускається зберігання секретів у Kubernetes Secrets (у сховищі etcd із шифруванням у стані спокою) після синхронізації з центрального сховища, чи виключно пряме отримання сервісами?

Відповідь:
Порядок зберігання, синхронізації, кешування та використання секретів визначатиметься на етапі формування технічного завдання та погодження цільової архітектури рішення.

На поточному етапі Технічні вимоги не встановлюють обов'язкової реалізації виключно через пряме отримання секретів сервісами або виключно через їх зберігання в Kubernetes Secrets після синхронізації із централізованого сховища секретів.

Лабораторія
законодавчих ініціатив

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

Під час вибору відповідного підходу Виконавець повинен враховувати вимоги щодо захисту інформації, управління життєвим циклом секретів, журналювання дій, ротації ключів і сертифікатів, забезпечення відмовостійкості та безперервності функціонування Системи, а також вимоги затверджених профілів безпеки.

Запитання:
Чи існують затверджені регламенти ротації системних паролів і ключів (періодичність, ролі), чи їх розроблення входить у межі проєкту?

Відповідь:
Регламенти ротації системних паролів, ключів шифрування, сертифікатів та інших криптографічних матеріалів визначатимуться відповідно до затверджених профілів безпеки, які будуть доведені в установленому порядку.

Під час проєктування та впровадження Системи Виконавець повинен забезпечити технічну можливість реалізації затверджених політик і процедур управління секретами, ключами та сертифікатами відповідно до вимог профілів безпеки.

Запитання:
Чи розповсюджується вимога збереження попередніх версій на всі бакети, чи лише на електронні документи/справи? Для яких категорій потрібен WORM/Object Lock і з якими термінами утримання?

Відповідь:
Вимоги щодо застосування механізмів версіонування об'єктів, збереження попередніх версій, використання режимів WORM (Write Once Read Many), Object Lock, а також строків утримання даних визначатимуться на етапі формування технічного завдання та погодження цільової архітектури Системи.

Під час визначення відповідних підходів мають бути враховані вимоги законодавства України, правила архівного зберігання, вимоги щодо цілісності та незмінності даних, профілі безпеки Системи, а також особливості життєвого циклу окремих категорій інформації.

Запитання:
Який допустимий показник можливої втрати даних (RPO) для об'єктного сховища при асинхронній реплікації між ЦОД? Чи існує другий ЦОД на момент старту, або його підготовка перебуває поза межами цього тендера?

Відповідь:
Цільові значення показників допустимої втрати даних (RPO), допустимого часу відновлення (RTO), а також вимоги до механізмів реплікації даних між центрами

обробки даних визначатимуться на етапі формування технічного завдання та погодження цільової архітектури Системи.

Водночас підготовка, модернізація, оснащення та забезпечення функціонування центрів обробки даних не входять до предмета цієї закупівлі. Необхідні ресурси інфраструктури надаватимуться Власником Системи відповідно до затвердженої цільової архітектури та фактичної готовності відповідних майданчиків на момент впровадження Системи.

Запитання:
ТВ 6.14 визначає міграцію даних із джерел (Електронний суд, Д3, ДСС, Кадри-веб, ЄДРСР, ВКЗ), проте перенесення файлів/документів окремо не описано. Чи входить в обсяг робіт міграція історичних файлів (~180 млн, що фігурують у супровідних матеріалах) до нового об'єктного сховища: з яких сховищ, у яких форматах/протоколах, який обсяг у ТБ?

Відповідь:
Міграція файлів не входить до обсягу робіт у межах цієї закупівлі.

Міграція в межах поточного проєкту охоплює лише ті категорії даних, які прямо визначені технічними вимогами та методологією міграції, що розроблятиметься Виконавцем і погоджуватиметься Власником Системи.

Запитання:
Який сервер антивірусної перевірки (за протоколом ICAP) використовує або планує Замовник? Чи допустиме рішення з відкритим кодом (c-icap + ClamAV), чи передбачено комерційний антивірус (у цьому разі — застосування моделі §6.12 для комерційного ПЗ)?

Відповідь:
Конкретне рішення для антивірусної перевірки об'єктів за протоколом ICAP, зокрема використання програмного забезпечення з відкритим вихідним кодом або комерційного антивірусного продукту, визначатиметься на етапі формування технічного завдання та погодження цільової архітектури Системи.

Запитання:
«Холодне» сховище: чи вимагається фізично окремий носій/клас обладнання для архівного рівня зберігання, чи достатньо логічного класу зберігання в межах кластера?

Відповідь:
Вимоги до реалізації архівного («холодного») рівня зберігання, зокрема щодо використання фізично відокремлених носіїв або окремих класів обладнання чи застосування логічного поділу в межах єдиного кластера, визначатимуться на етапі формування технічного завдання та погодження цільової архітектури

Лабораторія
законодавчих ініціатив

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

Системи з урахуванням вимог до продуктивності, вартості зберігання, строків утримання даних, відмовостійкості, безпеки та безперервності функціонування Системи.

Запитання:
Який інтерфейс приймання подій підтримує зовнішня SIEM (SOC): syslog RFC 5424, CEF, інший? Транспорт (TCP+TLS/UDP), адресація, очікуваний обсяг і категорії журналів?

Відповідь:
Конкретний інтерфейс передавання подій до зовнішньої SIEM (SOC), формат повідомлень, транспортний протокол, параметри адресації, категорії журналів та очікувані обсяги подій визначатимуться на етапі формування технічного завдання та погодження цільової архітектури Системи з урахуванням технічних можливостей наявної SIEM та вимог інформаційної безпеки.

Запитання:
Уточнити термін зберігання журналів у діапазоні 30–90 днів: чи диференціюється за категоріями (безпекові vs технічні); чи входить архівування >90 днів у Систему, чи на боці SOC?

Відповідь:
Вимоги щодо строків зберігання журналів, їх категоризації, порядку архівування, а також розподілу відповідальності між Системою та зовнішньою SIEM (SOC) визначатимуться на етапі формування технічного завдання та погодження цільової архітектури Системи.

Запитання:
Чи є розподілений трейсинг обов'язковим для першої черги поставки, чи допускається введення у гарантійний період (у ТВ — «бажано»; в естімейті закладено)?

Відповідь:
Розподілений трейсинг має бути включений до складу рішення. Детальні вимоги до його функціональності, технічної реалізації та строків упровадження будуть визначені на етапі формування технічного завдання та погодження цільової архітектури Системи.

Запитання:
Яке затверджене джерело точного часу (внутрішній NTP замовника / державний еталон) для синхронізації, або вибір NTP-джерела — проєктне рішення виконавця?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Вибір джерела точного часу визначатиметься під час формування технічного завдання та проєктування цільової архітектури Системи. Виконавець формує та пропонує відповідне архітектурне рішення, яке підлягає погодженню з Власником Системи та Замовником.

Запитання:
Чи є обмеження на ресурси обладнання для підсистеми спостережуваності (окремі ноди/пул), що впливають на вибір між OpenSearch та легшими альтернативами?

Відповідь:
Питання щодо виділення окремих обчислювальних ресурсів, нод або пулів для підсистеми спостережуваності не належить безпосередньо до вимог пункту 6.11 Технічних вимог. Необхідні ресурси та архітектура розміщення відповідних компонентів визначатимуться Виконавцем на етапі формування технічного завдання і проєктування цільової архітектури Системи з урахуванням очікуваного навантаження, вимог до продуктивності та обраного технологічного рішення та підлягатимуть погодженню із Замовником і Власником Системи.

Запитання:
Яка вимога до довговічності сесій за повної відмови вузла кешу: чи допустима повторна автентифікація частини користувачів (втрата ≤1 с при AOF everysec), чи вимагається синхронний запис (always)?

Відповідь:
Конкретні вимоги до забезпечення цілісності та збереження сесій користувачів у разі відмови окремих вузлів кешування, а також допустимі сценарії повторної автентифікації користувачів, визначатимуться на етапі формування технічного завдання та доведення профілів безпеки з урахуванням вимог, визначених у розділах 5.1 «Керування доступом — управління ідентифікацією та доступом (IAM)» та 7.4.2 «Кешування даних та оперативне зберігання сесій користувачів». Конкретні параметри синхронізації, реплікації та забезпечення стійкості до відмов також визначатимуться на зазначеному етапі.

Запитання:
Який очікуваний піковий профіль одночасних сесій (година-пік, сезонність судової активності)?

Відповідь:
Детальний профіль пікового навантаження, зокрема очікувана кількість одночасних сесій, часові інтервали найбільшої активності та сезонні коливання, буде визначено на етапі формування технічного завдання за результатами аналізу історичних даних і сценаріїв використання Системи. Водночас архітектура має проєктуватися з урахуванням показників, наведених у розділі

Лабораторія
законодавчих ініціатив

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

6.11 Технічних вимог, можливого зростання кількості користувачів, масових автоматизованих запитів та пікових навантажень, із забезпеченням передбачуваної деградації продуктивності та встановлених показників часу відповіді.

Запитання:
Чи належить кешування до контуру георезервування, чи достатньо відновлення в межах одного ЦОД (RTO 2 год)?

Відповідь:
Так, компонент кешування даних та оперативного зберігання сесій належить до контуру георезервування. Відповідно до розділів 6.6 та 7.4.2 Технічних вимог він є критичним інфраструктурним компонентом, має працювати у кластерному режимі та підтримувати георозподілення між дата-центрами для забезпечення відмовостійкості й збереження кешованих даних у разі виходу з ладу окремих вузлів. Відновлення лише в межах одного ЦОД не є достатнім; при цьому загальний показник RTO для відновлення працездатності компонентів Системи становить не більше 2 годин.

Запитання:
Чи має ДСА чинний договір підключення до ІСЕІ (id.gov.ua) і тестовий контур, придатний для ЄСІКС, чи підключення оформлюється заново?

Відповідь:
Договір про надання послуги приєднання інформаційної та/або інформаційно-комунікаційної системи до інтегрованої системи електронної ідентифікації укладено визначеними адміністратором і розпорядником ЄСІКС із технічним адміністратором ІСЕІ (ДП «ДІЯ»). У разі розширення переліку інформаційних ресурсів та оновлення складових ЄСІКС відповідні зміни забезпечуватимуться шляхом подання нових заявок у встановленому порядку. Необхідні деталі щодо використання тестового та промислового контурів будуть уточнені на етапі формування технічного завдання.

Запитання:
Яка криптобібліотека для КЕП прийнятна з огляду на §6.12: пропрієтарна ІІТ (окрема ліцензія; чи є вже придбані ліцензії у ДСА?) чи OSS-стек (UAPKI)?

Відповідь:
Обрана криптографічна бібліотека для роботи з КЕП повинна відповідати вимогам чинного законодавства України та мати необхідні документи, що підтверджують її відповідність. Конкретне рішення буде визначене після погодження цільової архітектури Системи, а відповідна бібліотека та необхідні ліцензії будуть надані Виконавцю Власником Системи або визначеним ДСА України розпорядником Системи до початку розроблення відповідної функціональності.

Лабораторія
законодавчих ініціатив

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

Запитання:
Чи є BankID НБУ обов'язковим каналом ідентифікації на етапі впровадження, чи достатньо id.gov.ua з додаванням BankID пізніше?

Відповідь:
Так, підтримка BankID НБУ є обов'язковою вимогою на етапі впровадження Системи відповідно до вимог розділу 5.1 «Керування доступом — управління ідентифікацією та доступом (IAM)».

Запитання:
Яке джерело правди для правового статусу користувача (майстер-реєстр?) і хто відповідає за його ведення?

Відповідь:
Джерелами достовірних даних щодо правового статусу користувача є відповідні державні реєстри та профільні інформаційні системи. Отримані з них дані консолідуються у відповідних майстер-реєстрах ЄСІКС, які виступають єдиною точкою доступу до актуальної інформації для інших складових Системи та зменшують кількість прямих запитів до зовнішніх джерел.

Ведення та актуалізація первинних відомостей здійснюються розпорядниками відповідних державних реєстрів, а за функціонування, синхронізацію та надання даних із майстер-реєстрів у межах ЄСІКС відповідають визначені Власником Системи адміністратор і розпорядник ЄСІКС.

Запитання:
Вимоги до делегування прав: часові межі, часткове делегування, ланцюжки повторного делегування, вимоги до журналу делегувань?

Відповідь:
Вимоги до механізму делегування повноважень повинні відповідати положенням розділу 5.1 «Керування доступом — управління ідентифікацією та доступом (IAM)», зокрема в частині підтримки тимчасового делегування ролей і прав доступу, встановлення строків дії делегування, можливості делегування як адміністратором, так і користувачем, автоматичного припинення делегованих повноважень після завершення визначеного строку, ведення аудиту всіх операцій делегування та підтримки багаторівневого делегування.

Детальні вимоги щодо часових обмежень, часткового делегування повноважень, допустимої кількості рівнів делегування, правил повторного делегування, а також складу й строків зберігання журналів аудиту будуть визначені на етапі формування технічного завдання.

Лабораторія
законодавчих ініціатив

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

Запитання:
Через який інтерфейс і з якою періодичністю синхронізується структура судів і штатних розписів з майстер-реєстрів: подієво (Kafka), REST, файловий обмін?

Відповідь:
Пріоритетним механізмом синхронізації структури судів і штатних розписів із майстер-реєстрами є подієва взаємодія через Компонент «Черга повідомлень». REST API, файловий обмін або інші інтерфейси можуть застосовуватися як альтернативні механізми у разі технічних обмежень профільних систем або як додаткові засоби звірки та актуалізації даних. Конкретна періодичність синхронізації, формат подій і правила повторної обробки будуть визначені на етапі формування технічного завдання та погодження інтеграційної архітектури.

Запитання:
Які кваліфіковані надавачі довірчих послуг eIDAS мають підтримуватись; чи є вимога до конкретного вузла сумісності (нотифікованої схеми ЄС)?

Відповідь:
Сумісність із кваліфікованими надавачами електронних довірчих послуг держав — членів ЄС та відповідними схемами електронної ідентифікації забезпечуватиметься через інтеграцію з ICEI (id.gov.ua), зокрема під час використання віджета автентифікації та віджета підпису.

Водночас для базового сервісу «Крипто-сервіс» необхідно передбачити реалізацію максимально можливої сумісності з вимогами eIDAS з урахуванням функціональних можливостей обраної криптографічної бібліотеки. Вимоги щодо підтримки конкретних кваліфікованих надавачів довірчих послуг (QTSP) або окремого вузла сумісності (нотифікованої схеми) Європейського Союзу будуть визначатися відповідно до можливостей обраного технологічного рішення та вимог, актуальних на момент впровадження.

Запитання:
Чи прийнятна модель супроводу з регулярними мажорними оновленнями Keycloak (OSS-гілка без LTS), чи очікується «заморожена» версія з розширеною підтримкою (платна підписка Red Hat)?

Відповідь:
Виконавець може запропонувати різні моделі супроводу та оновлення Keycloak або іншого обраного IAM-рішення, зокрема використання актуальної OSS-гілки з регулярними мажорними оновленнями чи рішення з розширеною комерційною підтримкою. Запропонований підхід має передбачати регулярне оновлення технологічного стеку для підтримки сучасної функціональності та належного рівня інформаційної безпеки, а також містити розрахунок сукупної вартості володіння (TCO); остаточна модель визначатиметься під час формування технічного завдання та погодження цільової архітектури Системи.

Лабораторія
законодавчих ініціатив

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

Запитання:
Трактування КЕП в автентифікації: КЕП — альтернативний самостійний спосіб входу (перший фактор), чи другий фактор поверх пароля/OTP для окремих категорій користувачів? Друге трактування потребує спеціалізованих компонентів автентифікації

Відповідь:
КЕП розглядається як самостійний засіб автентифікації та використовується як перший фактор. Як другий фактор автентифікації передбачається використання одноразового коду (OTP), сформованого відповідно до погодженого стандарту, або іншого еквівалентного механізму. При цьому рішення має забезпечувати можливість налаштування строку дії одноразового коду та параметрів багатофакторної автентифікації для окремих категорій користувачів.

Детальні вимоги до сценаріїв автентифікації, категорій користувачів, для яких застосовуватиметься другий фактор, а також до відповідних компонентів IAM будуть визначені на етапі формування технічного завдання.

Запитання:
CAPTCHA на формі входу: чи прийнятний self-hosted механізм (наприклад, ALTCHA) замість Google reCAPTCHA, використання якої передбачає взаємодію із зовнішнім сервісом поза контуром Системи?

Відповідь:
Конкретний механізм реалізації CAPTCHA, зокрема можливість використання self-hosted-рішень (наприклад, ALTCHA) або зовнішніх сервісів, визначатиметься на етапі формування технічного завдання та погодження цільової архітектури Системи.

Під час вибору рішення враховуватимуться вимоги щодо інформаційної безпеки, функціональної відповідності, відмовостійкості, продуктивності, захисту персональних даних, а також допустимості взаємодії із зовнішніми сервісами за межами контуру Системи.

Запитання:
«Призначення способу автентифікації окремому користувачу»: чи означає це заборону всіх інших способів входу для такого користувача (наприклад, лише КЕП на захищеному носії)? Таке обмеження не є штатною можливістю Keycloak і потребує окремого механізму

Відповідь:
Так, зазначена вимога передбачає можливість призначення окремому користувачеві або визначеній категорії користувачів конкретного способу автентифікації з одночасним обмеженням використання інших способів входу. Наприклад, для окремих категорій користувачів може бути встановлена вимога

щодо автентифікації виключно за допомогою КЕП, зокрема КЕП, що зберігається на захищеному носії.

Конкретний механізм реалізації зазначеної функціональності, включаючи необхідність використання додаткових компонентів або розширень базової платформи IAM, визначатиметься на етапі формування технічного завдання та погодження цільової архітектури Системи.

Запитання:
Другий фактор для зовнішніх користувачів: чи достатньо застосунку-автентифікатора (TOTP/HOTP), чи очікується OTP через SMS/e-mail (потребує окремої розробки та інтеграції з підсистемою нотифікацій)?

Відповідь:
Для зовнішніх користувачів достатнім є використання застосунків-автентифікаторів, що підтримують стандарти TOTP або HOTP. Реалізація другого фактора автентифікації через SMS-повідомлення або електронну пошту в межах поточних вимог не є обов'язковою.

Водночас запропоноване рішення має забезпечувати можливість подальшого розширення переліку підтримуваних механізмів багатофакторної автентифікації за потреби.

Запитання:
Первинне наповнення IAM: з яких існуючих систем переносяться облікові записи, у якому обсязі (орієнтовно ~170 тис. зовнішніх + 24 тис. внутрішніх), які ідентифікатори (РНОКПП/УНЗР) доступні для зіставлення та дедуплікації?

Відповідь:
Інформація щодо вимог до міграції даних та орієнтовних обсягів наведена в розділах 6.11 «Вимоги до потужності системи» та 6.14 «Вимоги до міграції даних» технічної документації.

Орієнтовна кількість облікових записів, що підлягають міграції станом на 2025 рік, становить 300–500 тисяч.

Детальний аналіз структури даних, визначення остаточного переліку інформаційних об'єктів, що підлягають перенесенню, а також уточнення схем баз даних та інших технічних особливостей систем-джерел виконуватимуться на етапі розроблення технічного завдання. Виконавцю буде забезпечено доступ до інформації, необхідної для виконання робіт з аналізу, проєктування та міграції даних, в обсязі, визначеному технічним завданням та з дотриманням вимог інформаційної безпеки.

Лабораторія
законодавчих ініціатив

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

Запитання:
Узгодження ТВ 9.2 (повний CRUD організацій в компоненті керування доступом) з ТВ 9.3 (автоматичне створення/оновлення з майстер-реєстру): чи є майстер-реєстр єдиним джерелом запису організацій, а створення в ІАМ — винятковим сценарієм з наступним узгодженням?

Відповідь:
Остаточний механізм створення, оновлення та синхронізації записів про організації між майстер-реєстром і компонентом «Керування доступом» буде визначено на етапі формування технічного завдання та погодження інтеграційної архітектури. Зокрема, на цьому етапі мають бути визначені джерело достовірних даних, допустимі сценарії створення або редагування організацій безпосередньо в ІАМ, правила подальшого узгодження змін із майстер-реєстром, а також порядок вирішення конфліктів і ведення історії змін.

Запитання:
Доступ до ЄРАУ (валідація адвокатів) та ЄДР (дані ЮО/ФОП): чиї договори/підключення, чи є тестові контури, які протоколи доступу?

Відповідь:
Перед початком виконання робіт Виконавцеві буде надано доступ до відповідних середовищ для інтеграції, що забезпечуються Власником Системи або визначеним Розпорядником Системи. Укладення договорів, необхідних для отримання такого доступу та взаємодії із зовнішніми інформаційними ресурсами, забезпечується Власником Системи або визначеним Розпорядником Системи.

Інформація щодо наявності тестових середовищ, порядку підключення, підтримуваних протоколів обміну даними та інших технічних аспектів інтеграції з ЄРАУ та ЄДР буде надана додатково на етапі формування технічного завдання та виконання робіт з проєктування Системи.

Запитання:
Перелік спеціалізованих профілів (присяжні, арбітражні керуючі, виконавці, експерти, нотаріуси, прокурори): зафіксувати вичерпний перелік і межу першої черги у ТЗ; для кожного профілю — джерело та процедура підтвердження статусу (зовнішній державний реєстр, ручне підтвердження адміністратором, документальне)

Відповідь:
Вичерпний перелік спеціалізованих профілів користувачів першої черги наведено в розділі 5.2.5 «Сервіс майстер-реєстрів». Водночас допускається коригування обсягу та складу майстер-реєстрів у межах до 30 % від визначеного обсягу.

Лабораторія
законодавчих ініціатив

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

Остаточний перелік спеціалізованих профілів, джерела отримання даних, способи підтвердження статусу користувачів, а також порядок інтеграції із зовнішніми державними реєстрами або застосування інших механізмів верифікації будуть визначені на етапі формування та погодження технічного завдання.

Запитання:
«Юридично достовірна модель змін» реєстру фізичних осіб: які НПА застосовні та які вимоги до фіксації змін (форма, підпис, строки)?

Відповідь:
Під терміном «юридично достовірна модель змін» розуміється сукупність правил, механізмів та подій, які забезпечують створення, оновлення, використання, простежуваність і збереження відомостей про фізичну особу відповідно до положень законодавства України, нормативно-правових актів, що регулюють діяльність судової влади, процесуальних кодексів, а також внутрішніх положень ЄСІКС.

З огляду на те, що реєстр фізичних осіб є централізованим обліковим ядром ЄСІКС та охоплює всіх фізичних осіб, пов'язаних із процесами здійснення правосуддя, система повинна забезпечувати накопичення даних протягом усього життєвого циклу, ведення історії змін, простежуваність джерел походження даних, фіксацію підстав внесення змін, а також збереження зв'язків між обліковими записами та пов'язаними інформаційними об'єктами.

Остаточний перелік нормативно-правових актів, склад подій, що підлягають обов'язковій фіксації, вимоги до підтвердження, підписання, зберігання та актуалізації відповідних відомостей будуть визначені на етапі формування технічного завдання.

Запитання:
Чи існує затверджений перелік спільних довідників базових сервісів; хто постачає еталонне джерело даних КАТОТТГ та інших зовнішніх класифікаторів? Просимо також підтвердити назву класифікатора — КАТОТТГ (у ТВ 5.2.1 зазначено «КАТОТГ»).

Відповідь:
Мається на увазі класифікатор КАТОТТГ; зазначення «КАТОТГ» у пункті 5.2.1 Технічних вимог є технічною помилкою.

Затверджений вичерпний перелік спільних довідників базових сервісів на цьому етапі не визначений. Відповідно до пункту 5.2.1 точний склад і наповнення довідників та класифікаторів визначатимуться під час детального аналізу предметної області відповідних складових ЄСІКС і фіксуватимуться в технічних завданнях.

Лабораторія
законодавчих ініціатив

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

Виконавець має врахувати, що для кожної складової ЄСІКС очікується в середньому від 5 до 20 довідників та/або класифікаторів. З огляду на концепцію побудови системи, яка передбачає створення близько 10 основних складових (підсистем), орієнтовний загальний обсяг може становити від 20 до 100 довідників та класифікаторів різного рівня складності, включаючи лінійні, ієрархічні та ієрархічно-фасетні структури.

Еталонними джерелами для КАТОТТГ та інших зовнішніх класифікаторів мають бути офіційні державні інформаційні ресурси або відповідні розпорядники таких даних. Конкретні джерела, порядок отримання, формат і періодичність оновлення будуть визначені на етапі формування технічного завдання та погодження інтеграційної архітектури.

Запитання:
Робоче припущення: посада судді/працівника апарату описується двома джерелами статусів — кадровою системою (штатний розпис) і рішеннями ВККС (кваліфікаційні провадження), які можуть тимчасово розходитись. Яке джерело є визначальним при розбіжності і в які строки вона має бути усунена?

Відповідь:
Бізнес-логіка формування, оновлення, синхронізації та пріоритезації даних майстер-реєстрів буде визначена на етапі формування технічного завдання.

Зокрема, на цьому етапі будуть визначені перелік систем-джерел, правила обробки розбіжностей між ними, механізми узгодження статусів, порядок вирішення конфліктних ситуацій, а також допустимі строки актуалізації даних.

Зазначений підхід стосується, зокрема, випадків, коли інформація щодо статусу судді або працівника апарату суду надходить із кількох джерел та може тимчасово відрізнятися залежно від особливостей відповідних бізнес-процесів.

Запитання:
Використання фотокарток «у сервісах ідентифікації»: візуальне звіряння уповноваженою особою чи автоматизована біометрична ідентифікація? Друге означає обробку біометричних персональних даних з підвищеними вимогами захисту

Відповідь:
Фотокартки в межах поточного обсягу робіт передбачені виключно для використання як елемент профілю користувача та не розглядаються як інструмент автоматизованої біометричної ідентифікації.

Використання фотозображень для візуального звіряння уповноваженими особами або застосування механізмів автоматизованої біометричної

ідентифікації не входить до обсягу першої черги реалізації та може бути предметом подальших етапів розвитку системи.

Запитання:
Вичерпний перелік GoldRecord-сутностей першої черги (організаційна структура, «Судді на посаді» — які ще?) та вимоги до правил вирішення конфліктів при злитті записів

Відповідь:
Вичерпний перелік Gold Record-сутностей першої черги буде визначено на етапі формування технічного завдання на підставі вимог, наведених у розділі 5.2.5 «Сервіс майстер-реєстрів», а також результатів аналізу джерел даних, визначених у розділі 6.14 «Вимоги до міграції даних».

При цьому Виконавець має врахувати, що централізоване зберігання та уніфікація даних охоплюватимуть, зокрема, інформацію про фізичних осіб, користувачів ЄСІКС, юридичних осіб та фізичних осіб-підприємців, представників сторін, організації, органи судової влади, довідники, класифікатори та інші інформаційні об'єкти, необхідні для функціонування системи.

Правила виявлення дублікатів, злиття записів, визначення пріоритетності джерел, обробки конфліктних даних, ведення історії змін та відновлення попередніх станів повинні бути розроблені Виконавцем у межах Методології міграції та подані на погодження Адміністратору Системи.

У випадках, коли конфлікти не можуть бути усунені автоматизованими засобами, Методологія міграції повинна передбачати порядок їх опрацювання із застосуванням додаткових процедур перевірки та валідації даних.

Запитання:
ТВ вимагає «двосторонні механізми призначення представників із забезпеченням всіх юридичних вимог до цієї процедури», але не деталізує саму процедуру. Як має виглядати цей механізм: хто ініціює (довіритель), чи потрібне явне підтвердження другою стороною (представником), чи потрібен КЕП-підпис обох сторін на акті призначення чи достатньо підпису довірителя, і як реалізується відкликання повноважень (довірителем вручну, автоматично за строком дії, чи обома способами)?

Відповідь:
Детальний порядок призначення, підтвердження, зміни та відкликання повноважень представників буде визначено на етапі формування технічного завдання з урахуванням вимог законодавства України, процесуальних кодексів, нормативно-правових актів у сфері електронних довірчих послуг, а також внутрішніх положень ЄСІКС.

Лабораторія
законодавчих ініціатив

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

Зокрема, на цьому етапі будуть визначені порядок ініціювання відповідних дій, перелік учасників процесу, необхідність підтвердження повноважень іншою стороною, вимоги до застосування кваліфікованого електронного підпису, умови набуття та припинення повноважень, а також порядок автоматичного або ручного відкликання таких повноважень.

Виконавець має врахувати, що реалізований механізм повинен забезпечувати юридичну значущість відповідних дій, їхню простежуваність, аудит і можливість підтвердження чинності повноважень на будь-який момент часу.

Запитання:
ТВ передбачає ведення облікових карток майстер-реєстрів, але не визначає їх обов’язковий атрибутивний склад. Який склад атрибутів облікових карток має підтримувати кожен майстер-реєстр?

Відповідь:
Обов'язковий склад атрибутів облікових карток для кожного майстер-реєстру буде визначено на етапі формування технічного завдання з урахуванням функціонального призначення відповідного реєстру, його взаємозв'язків з іншими компонентами ЄСІКС, вимог законодавства та особливостей процесів, які він забезпечує.

Зокрема, на цьому етапі буде визначено перелік обов'язкових і необов'язкових атрибутів, правила їх заповнення, джерела отримання даних, вимоги до валідації, порядок ведення історії змін, а також правила синхронізації даних між підсистемами.

Виконавець має врахувати, що атрибутивний склад облікових карток може відрізнятися залежно від типу сутності (фізична особа, юридична особа, організація, документ, довідник, класифікатор тощо), а також може розширюватися в міру розвитку функціональних можливостей системи.

Запитання:
Скільки контент-менеджерів працюватиме з Базою знань; хто виконує роль погоджувача у циклі «На погодженні»; чи потрібен багатокроковий маршрут?

Відповідь:
На поточному етапі орієнтовно передбачається, що з Базою знань працюватиме до 100 контент-менеджерів. Водночас остаточна кількість користувачів, їхні ролі, повноваження та модель розмежування доступу будуть визначені на етапі формування технічного завдання.

Роль погоджувача виконуватиме користувач, якому надано відповідні повноваження щодо перевірки та погодження матеріалів перед їх

оприлюдненням. Конкретний перелік таких ролей і правила їх призначення також будуть визначені під час підготовки технічного завдання.

Необхідність реалізації багатокрокових маршрутів погодження, умови їх застосування, порядок ескалації, а також правила автоматизації відповідних процесів будуть визначені на етапі деталізації вимог.

Запитання:
Чи вимагається спільне редагування статті кількома редакторами в реальному часі (у ТВ відсутнє — пропонуємо зафіксувати як таке, що не входить в обсяг робіт)?

Відповідь:
Функціональна можливість одночасного редагування однієї статті кількома користувачами в режимі реального часу не входить до обсягу робіт у межах поточної черги реалізації.

Передбачається використання стандартних механізмів створення, редагування, погодження, публікації, версіонування та аудиту змін контенту без реалізації режиму спільного редагування в реальному часі. У разі потреби зазначена функціональність може бути розглянута в межах подальших етапів розвитку системи.

Запитання:
Чи існує затверджений глосарій судової термінології для словника синонімів пошуку?

Відповідь:
На цей момент затверджений глосарій судової термінології для формування словника синонімів пошукового механізму відсутній.

Формування, наповнення та подальший розвиток словника синонімів, правил нормалізації термінів, урахування відмінків, скорочень, абревіатур, історичних назв та інших особливостей юридичної термінології будуть визначені на етапі формування технічного завдання.

Виконавець має врахувати необхідність забезпечення можливості централізованого адміністрування та подальшого розширення відповідних словників без необхідності внесення змін до програмного коду системи.

Запитання:
Чи має контекстна довідка бути доступною на публічних (неавтентифікованих) сторінках ЄППК?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Так, контекстна довідка має бути доступною для визначених публічних (неавтентифікованих) розділів ЄППК.

Остаточний перелік таких розділів, обсяг опублікованої інформації, правила її відображення, а також порядок адміністрування відповідного контенту будуть визначені на етапі формування технічного завдання.

Водночас Виконавець має передбачити можливість гнучкого налаштування доступності контекстної довідки залежно від типу сторінки, категорії користувачів, ролей, рівня автентифікації та інших параметрів доступу.

Запитання:
Відео-інструкції: чи достатньо відтворення з об'єктного сховища (послідовне завантаження, progressive download), чи вимагається транскодування та потокове відтворення (HLS)?

Відповідь:
Вимоги до механізму зберігання та відтворення відеоматеріалів будуть остаточно визначені на етапі формування технічного завдання.

Залежно від визначених нефункціональних вимог, обсягів контенту, очікуваної кількості одночасних користувачів, вимог до продуктивності та особливостей інфраструктури можуть бути застосовані як механізми послідовного завантаження відеофайлів (progressive download) з об'єктного сховища, так і потокове відтворення з використанням технології HLS або аналогічних рішень.

Виконавець має передбачити можливість масштабування відповідного рішення та його адаптації до остаточно визначених вимог.

Запитання:
Модель хостингу: де фізично розміщуються PROD та NON-PROD середовища (власні ЦОД ДСА / Адміністратора Системи, орендовані потужності, державна хмара)?

Відповідь:
Технічні вимоги визначають розподіл відповідальності за середовища, не встановлюючи моделі їх фізичного розміщення. Пункт 6.8: «Початкове розгортання DEV, QA, STAGE середовищ має бути реалізоване Виконавцем на ресурсах Адміністратора Системи. Розгортання PROD-середовища та його подальше адміністрування будуть виконуватися силами Адміністратора Системи». Пункт 6.2 додатково вимагає, щоб продуктивне та непродуктивне середовища були відокремлені, а в назвах об'єктів використовувалися префікси або суфікси, які однозначно вказують на середовище.

Лабораторія
законодавчих ініціатив

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

Незалежно від обраної моделі застосовуються обмеження розділу 6: архітектура Системи та нефункціональні вимоги мають виключати технологічну залежність від конкретного постачальника хмарних або інфраструктурних сервісів; усі компоненти повинні мати можливість розгортання у середовищі власної інфраструктури або інфраструктури будь-якого постачальника без зміни прикладної логіки; не допускається використання пропрієтарних керованих сервісів, які не мають функціонально еквівалентних self-hosted реалізацій або істотно ускладнюють міграцію до альтернативного інфраструктурного середовища.
Конкретна модель хостингу (власні ЦОД, орендовані потужності, державна хмара) та клас дата-центрів у Технічних вимогах не зазначені; відповідні відомості визначаються Адміністратором Системи та надаватимуться на етапі формування та погодження технічного завдання.

Незалежно від обраної моделі застосовуються обмеження розділу 6: архітектура Системи та нефункціональні вимоги мають виключати технологічну залежність від конкретного постачальника хмарних або інфраструктурних сервісів; усі компоненти повинні мати можливість розгортання у середовищі власної інфраструктури або інфраструктури будь-якого постачальника без зміни прикладної логіки; не допускається використання пропрієтарних керованих сервісів, які не мають функціонально еквівалентних self-hosted реалізацій або істотно ускладнюють міграцію до альтернативного інфраструктурного середовища.

Запитання:
Чи наявні обидва територіально рознесені майданчики на момент впровадження, та які пропускна здатність і затримка каналу між дата-центрами? Параметри каналу визначають вибір механізмів реплікації між ЦОД.

Відповідь:
Пункт 6.6 містить загальну вимогу — «Система має забезпечувати георозподілення між дата-центрами», без зазначення кількості майданчиків. Для об'єктного сховища пункт 7.4.3.4 встановлює мінімальну конфігурацію: «синхронна або асинхронна реплікація даних між двома або більше територіально рознесеними дата-центрами».

Наявність і готовність майданчиків на момент впровадження, а також параметри каналу зв'язку між ними (пропускна здатність, затримка, доступність) Технічними вимогами не визначені. Відповідні відомості визначаються Адміністратором Системи та надаватимуться на етапі формування та погодження технічного завдання

Вибір механізму реплікації між майданчиками здійснюватиметься на етапі технічного проєктування на підставі фактичних параметрів каналу з урахуванням вимог розділу 6.11 до часу обробки інформаційного запиту (90 % запитів

протягом 1 секунди, 95 % — протягом 2 секунд) та вимог пункту 6.6 щодо збереженості інформації.

Запитання:
Чи передбачений закритий (ізольований від мережі Інтернет) сегмент мережі для окремих компонентів або даних Системи?

Відповідь:
Створення та експлуатація закритого (ізольованого від мережі Інтернет) сегмента мережі для окремих компонентів або даних Системи не входять до предмета цієї закупівлі.

Водночас під час проєктування та реалізації рішення Виконавець має враховувати можливість інтеграції Системи з відповідною інфраструктурою в майбутньому, якщо така потреба буде визначена Власником.

Архітектурні рішення, вимоги до мережевої взаємодії, порядок розгортання компонентів та додаткові вимоги щодо ізоляції окремих сегментів інфраструктури визначатимуться в межах відповідних проєктних рішень і не належать до обсягу поточної закупівлі.

Запитання:
Як організується віддалений доступ команди Виконавця до середовищ DEV/QA/STAGE (VPN, регламент доступу, чи виключно з робочих місць Замовника)?

Відповідь:
Перед початком виконання робіт Власник або Розпорядник Системи забезпечує надання Виконавцю доступу до відповідних середовищ DEV, QA та STAGE із застосуванням VPN-з'єднань та інших організаційних і технічних заходів із забезпечення інформаційної безпеки.

Порядок надання, зміни, тимчасового блокування та відкликання доступів, а також перелік вимог до робочих станцій, мережевої взаємодії, автентифікації користувачів, журналювання дій і використання засобів захисту інформації визначатимуться окремими регламентами та вимогами Власника або Розпорядника Системи.

Постійне виконання робіт виключно з робочих місць Власника або Розпорядника Системи не передбачається, якщо інше не буде визначено для окремих компонентів, середовищ або категорій даних.

Запитання:
Просимо уточнити розподіл витрат щодо NON-PROD: середовища DEV/QA/STAGE розгортаються «на ресурсах Адміністратора Системи»,

водночас «усі видатки, пов'язані із розгортанням, функціонуванням та адмініструванням DEV, QA, STAGE, покладаються на Виконавця». Чи надає обчислювальні ресурси Адміністратор Системи (Виконавець виконує розгортання та адміністрування), чи Виконавець має забезпечити власні потужності для NON-PROD?

Відповідь:
Обчислювальні ресурси для середовищ DEV, QA та STAGE надаються Власником, Адміністратором або Розпорядником Системи.

До обсягу відповідальності Виконавця входять розгортання, налаштування, конфігурування, адміністрування, оновлення та забезпечення працездатності програмних компонентів у відповідних середовищах.

Витрати, пов'язані з наданням обчислювальних ресурсів, мережевої інфраструктури, систем зберігання даних та інших базових інфраструктурних компонентів, покладаються на Власника, Адміністратора або Розпорядника Системи, тоді як витрати, пов'язані з виконанням робіт із розгортання, налаштування та супроводу програмного забезпечення, покладаються на Виконавця.

Запитання:
Чи означає «активна сесія користувача» у вимозі до віджета підпису (накладання УЕП/КЕП без повторного завантаження ключа, вибору ЦСК та введення пароля) ту саму сесію логіну (ТВ 4.1, п.1.11 — керування сесіями), тобто чи достатньо одноразової КЕП/УЕП-автентифікації на вході, щоб надалі підписувати документи протягом усієї сесії без повторного вводу пароля до ключа — включно з файловими ключами, де це означає утримання розшифрованого приватного ключа в пам'яті на весь час сесії (а не тільки на коротку серію підписань)?

Відповідь:
Під активною сесією користувача в межах зазначеної вимоги слід розуміти сесію, створену після успішного проходження автентифікації відповідно до вимог пункту 1.11 технічних вимог.

Автентифікація користувача з використанням КЕП або УЕП за допомогою відповідного віджета є окремою подією, що ініціює таку сесію.

Під час виконання першої юридично значущої дії користувач здійснює вибір засобу підписання та вводить необхідні реквізити доступу до ключа. Подальші операції підписання в межах активної сесії можуть виконуватися без повторного вибору носія ключа, кваліфікованого надавача електронних довірчих послуг та повторного введення пароля.

Лабораторія
законодавчих ініціатив

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

Водночас конкретні механізми реалізації зазначеної функціональності, зокрема порядок і тривалість зберігання відповідних криптографічних матеріалів у пам'яті, повинні відповідати вимогам законодавства України у сфері електронних довірчих послуг та вимогам інформаційної безпеки, визначеним Власником або Розпорядником Системи.

Запитання:
ТВ визначає «Трембіту» лише в глосарії, без переліку конкретних точок інтеграції. Чи вимагається взаємодія Системи із зовнішніми реєстрами або суміжними підсистемами через Трембіту (з розгортанням ШБО на стороні Системи), і якщо так — для яких саме інтеграцій; чи достатньо прямої API-взаємодії для підсистем усередині контуру судової влади?

Відповідь:
Технологія «Трембіта» є пріоритетним механізмом інтеграційної взаємодії Системи з державними реєстрами, державними інформаційними ресурсами та іншими зовнішніми інформаційно-комунікаційними системами, якщо використання такого механізму передбачено чинними нормативно-правовими актами, технічними вимогами або правилами взаємодії відповідних систем.

Остаточний перелік інтеграцій, для яких необхідно використовувати «Трембіту», а також вимоги щодо застосування шлюзу безпечного обміну (ШБО) визначатимуться на етапі підготовки технічного завдання та проєктування відповідних підсистем.

Для забезпечення взаємодії між компонентами та підсистемами в межах контуру судової влади передбачається використання компонента «Черга повідомлень», а також REST API або інших механізмів інтеграції залежно від функціональних і нефункціональних вимог, особливостей реалізації та характеристик відповідних сценаріїв взаємодії.

Запитання:
Який перелік функцій є обов'язковим для першої черги впровадження, а які можуть бути прийняті окремими етапами? Пріоритезація впливає на строк і базову ціну.

Відповідь:
Реалізація функціональних можливостей Системи здійснюватиметься за ітераційним підходом із поетапним введенням компонентів в експлуатацію.

На поточному етапі передбачається такий орієнтовний порядок поставки основних компонентів:
1. розгортання та налаштування інфраструктури;
2. створення та впровадження компонентів керування ідентифікацією та доступом (IAM);

3. реалізація ЄППК, майстер-реєстрів і пов'язаних базових сервісів;
4. виконання заходів із міграції даних та проведення фінального приймання.

Остаточний перелік функцій, їх пріоритетність, склад окремих етапів, критерії приймання та порядок введення в експлуатацію визначатимуться під час підготовки технічного завдання та формування плану реалізації проєкту.
Зазначена послідовність має орієнтовний характер і може бути уточнена залежно від результатів аналізу, архітектурних рішень, технічних обмежень і потреб Власника Системи.

Запитання:
Просимо підтвердити межу предмета закупівлі за тендерною документацією: чи обмежується він функціональними вимогами ТВ, чи включає також суміжні роботи — побудову й державну експертизу КСЗІ як окремий предмет, закупівлю обладнання та ліцензій третіх сторін, операційні витрати платних каналів зв'язку?

Відповідь:
Предмет закупівлі обмежується реалізацією функціональних можливостей Системи, а також виконанням робіт із розгортання та налаштування її компонентів відповідно до встановлених вимог, зокрема вимог профілів безпеки.

До предмета закупівлі не належать:
• побудова комплексної системи захисту інформації (КСЗІ) як окремого об'єкта;
• проведення державної експертизи, аудиту або інших процедур підтвердження відповідності вимогам у сфері захисту інформації;
• закупівля обладнання, програмно-апаратних комплексів, ліцензій третіх сторін та інших матеріально-технічних ресурсів;
• забезпечення функціонування платних каналів зв'язку та покриття відповідних операційних витрат.

Зазначені роботи та закупівлі, за потреби, здійснюватимуться в межах окремих процедур закупівель.

Запитання:
Які критерії успіху та приймання встановлено для кожного етапу і хто з боку Замовника уповноважений підписувати результат етапу?

Відповідь:
Критерії успішності виконання робіт, порядок проведення випробувань, перелік необхідних артефактів, вимоги до підтвердження результатів, а також процедури приймання визначені в розділах 8 «Вимоги до супроводу та обслуговування засобу інформатизації» та 9 «Вимоги до приймання засобу інформатизації».

Лабораторія
законодавчих ініціатив

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

Детальні критерії приймання для окремих етапів, ітерацій, компонентів або релізів уточнюватимуться під час формування технічного завдання, календарного плану та іншої проєктної документації.

Запитання:
Який порядок зміни обсягу робіт після отримання відповідей на ці питання та під час подальшого уточнення вимог (процедура керування змінами)?

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.

Запитання:
Хто є власником вимог (Product Owner) та хто затверджує архітектуру, UX, рішення з безпеки і план міграції; які регламентні строки погодження?

Відповідь:
Функції власника вимог (Product Owner) виконують Власник Системи, Розпорядник Системи та Замовник у межах визначених повноважень і зон відповідальності.

Саме зазначені сторони здійснюють погодження функціональних вимог, архітектурних рішень, підходів до побудови користувацького інтерфейсу, рішень у сфері інформаційної безпеки, а також планів міграції даних і введення компонентів Системи в експлуатацію.
Зі свого боку Виконавець забезпечує підготовку відповідних проєктних артефактів, їх обґрунтування, презентацію та супровід у процесі погодження.

Регламентні строки розгляду, погодження та затвердження відповідних матеріалів мають бути запропоновані Виконавцем і погоджені сторонами до

початку виконання робіт, а також закріплені у відповідній проєктній документації та процедурах управління проєктом.

Запитання:
Які команди третіх сторін надають API, тестові контури, сертифікати, мережеві доступи та дані; які їхні строки надання та рівні обслуговування (SLA)?

Відповідь:
Надання доступів до зовнішніх систем, тестових середовищ, API, сертифікатів, мережевих ресурсів, облікових записів та інших необхідних компонентів забезпечується Власником Системи із залученням відповідних адміністраторів або власників таких систем.

Перелік необхідних ресурсів, середовищ і доступів визначається технічними вимогами, архітектурними рішеннями та затвердженим переліком інтеграцій.

Строки надання доступів, порядок взаємодії між сторонами, рівні доступності сервісів (SLA), а також порядок реагування на інциденти визначаються умовами чинних договорів, регламентів взаємодії та внутрішніх процедур відповідних власників і адміністраторів систем.
У випадках, коли виконання робіт залежить від залучення третіх сторін, строки реалізації відповідних завдань можуть уточнюватися з урахуванням фактичних строків надання необхідних ресурсів і доступів.

Запитання:
Чи наявні обладнання, майданчики ЦОД, мережі, служби DNS/PKI/NTP/SIEM та середовища NON-PROD до старту робіт; які дати їхньої готовності?

Відповідь:
До початку виконання робіт Власник Системи забезпечить надання Виконавцю доступу до необхідних обчислювальних ресурсів, призначених для розгортання та функціонування відповідних компонентів Системи.

Конкретний перелік ресурсів, зокрема центрів обробки даних, мережевої інфраструктури, служб DNS, PKI, NTP, SIEM, середовищ DEV, QA та STAGE, а також ступінь їхньої готовності визначатимуться відповідно до плану реалізації проєкту та архітектурних рішень, погоджених сторонами.

Інформація щодо фактичної готовності відповідних ресурсів, а також строки надання доступу до них доводитимуться до Виконавця в межах процедур підготовки до початку виконання робіт.

Лабораторія
законодавчих ініціатив

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

Запитання:
Хто оплачує та адмініструє експлуатаційні складові: платні канали (SMS/Viber/WhatsApp/Дія), комерційні криптобібліотеки, антивірусне ПЗ, підтримку OSS/enterprise, обладнання та канали зв'язку між ЦОД?

Відповідь:
Витрати, пов'язані з придбанням, ліцензуванням, експлуатацією, супроводом та адмініструванням відповідних сервісів і компонентів, покладаються на Власника або Розпорядника Системи.

Водночас у разі, якщо Виконавець пропонує використовувати у складі Системи комерційне програмне забезпечення третіх сторін, застосовується окремий порядок.

У такому випадку Виконавець зобов'язаний:

• попередньо погодити з Власником Системи перелік відповідного програмного забезпечення, його вартість, порядок ліцензування та умови подальшого оновлення;
• включити до вартості своєї пропозиції витрати на придбання відповідних ліцензій та їхню підтримку протягом 10 років;
• у разі використання моделі періодичних платежів (subscription) надати розрахунок сукупної вартості володіння (TCO) щонайменше на трирічний період.

Зазначені вимоги застосовуються як виняток із загального правила щодо фінансування та експлуатації відповідних компонентів Власником або Розпорядником Системи.

Запитання:
Які рівні обслуговування (SLA/SLO), години підтримки та строки реагування у гарантійний період; скільки годин або інцидентів включено в обсяг?

Відповідь:
Усі компоненти Системи повинні забезпечуватися гарантійною підтримкою протягом 12 місяців з моменту підписання акта приймання-передачі наданих послуг, якщо інше не буде визначено умовами договору між Замовником та Виконавцем.

Гарантійна підтримка охоплює, зокрема, усунення дефектів, помилок і невідповідностей технічному завданню, технічним вимогам, Концепції ЄСІКС та іншим погодженим проєктним артефактам.

Надання гарантійної підтримки здійснюється в режимі 9×7. Реагування на інциденти та виконання робіт здійснюються відповідно до рівня їх критичності.

Лабораторія
законодавчих ініціатив

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

Орієнтовні цільові показники передбачають такі строки реагування:
• для критичних інцидентів — до 2 робочих годин для підготовки первинної оцінки та до 4 робочих годин для початку виконання робіт;
• для інцидентів високого рівня критичності — до 4 та 8 робочих годин відповідно;
• для інцидентів середнього рівня критичності — до 24 та 40 робочих годин відповідно;
• для інцидентів низького рівня критичності — до 40 та 80 робочих годин відповідно.
Конкретні значення показників SLA та SLO, порядок ескалації інцидентів, перелік каналів взаємодії, а також обсяг гарантійної підтримки в годинах або кількості інцидентів визначатимуться договором та відповідними регламентами супроводу Системи.

Запитання:
Хто після завершення гарантії володіє репозиторіями Git, реєстром образів, конвеєрами CI/CD, секретами, доменами, обліковими записами постачальників і регламентами (runbooks)?

Відповідь:
Усі артефакти, створені в межах реалізації проєкту, зокрема вихідний код, репозиторії Git, реєстри контейнерних образів, конвеєри CI/CD, облікові дані, конфігурації, ключі, сертифікати, доменні імена, технічна документація, експлуатаційні регламенти (runbooks) та інші компоненти Системи, створюються та адмініструються з використанням обчислювальних ресурсів Власника або Розпорядника Системи.

Відповідно, після завершення гарантійного періоду право володіння, доступу та адміністрування зазначених компонентів зберігається за Власником або Розпорядником Системи.

Виконавець зобов'язаний забезпечити передачу всіх необхідних прав доступу, конфігурацій, облікових записів, секретів, технічної документації та експлуатаційних процедур, необхідних для подальшого функціонування, супроводу та розвитку Системи.
При цьому підхід, за якого критично важливі компоненти Системи перебувають під винятковим контролем Виконавця або розміщуються виключно на його власних ресурсах, не передбачається.

Запитання:
Який строк чинності комерційної пропозиції встановлено умовами процедури? Як процедура передбачає врахування зміни тарифів сторонніх постачальників (платні канали, комерційні ліцензії) — у складі операційних витрат Власника чи в інший спосіб?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Відповідно до умов процедури, учасник зобов'язаний не вносити змін до поданої комерційної пропозиції та дотримуватися її умов протягом усього строку її чинності, який становить 60 календарних днів з дати подання пропозиції.

Комерційна пропозиція може бути акцептована Замовником у будь-який момент до завершення зазначеного строку.

Водночас порядок урахування можливих змін вартості послуг сторонніх постачальників, зокрема платних каналів зв'язку, комерційних ліцензій, сервісів технічної підтримки та інших аналогічних складових, визначатиметься з урахуванням моделі фінансування відповідного компонента.
Якщо відповідні витрати належать до операційних витрат Власника або Розпорядника Системи, їх фінансування та подальше адміністрування здійснюються такими суб'єктами в межах окремих процедур закупівлі, укладених договорів або затверджених бюджетів.

Якщо ж використання певного комерційного програмного забезпечення запропоноване Виконавцем, до нього застосовуються вимоги щодо попереднього погодження, включення вартості ліцензій до складу пропозиції та надання розрахунку сукупної вартості володіння (TCO) відповідно до вимог тендерної документації.

Запитання:
Хто є володільцем/розпорядником персональних даних; які вимоги до локалізації даних, знеособлення (маскування) даних у середовищах NON-PROD, строків зберігання та видалення?

Відповідь:
Середовища, призначені для розроблення, тестування, інтеграції та інших непродуктивних сценаріїв (NON-PROD), повинні використовувати виключно тестові дані. Використання реальних даних допускається лише у виняткових випадках за умови їх попереднього знеособлення, маскування або застосування інших передбачених законодавством і внутрішніми політиками засобів захисту інформації.

Запитання:
Який точний склад результату щодо КСЗІ покладається на Виконавця (створення/погодження чи лише технічний внесок у документи) та хто відповідає за державну експертизу/оцінку відповідності?

Відповідь:
Виконавець забезпечує реалізацію функціональних можливостей Системи, розгортання та налаштування програмної й інфраструктурної складових, а також впровадження організаційних і технічних заходів захисту інформації відповідно

до затверджених профілів безпеки, вимог законодавства, архітектурних рішень та технічних вимог.

До сфери відповідальності Виконавця входить підготовка технічних матеріалів, конфігурацій, описів архітектури, схем взаємодії компонентів, налаштувань засобів захисту інформації, а також надання іншого технічного сприяння, необхідного для подальшого створення комплексної системи захисту інформації.

Водночас побудова КСЗІ, розроблення повного комплекту експлуатаційної та організаційно-розпорядчої документації, проходження державної експертизи або оцінки відповідності, а також взаємодія з уповноваженими державними органами не входять до предмета цієї закупівлі та здійснюватимуться в межах окремого договору. Відповідальність за організацію та проходження відповідних процедур покладається на Власника Системи.

Запитання:
Хто проводить і фінансує незалежне тестування на проникнення, скільки повторних перевірок включено та які рівні критичності зауважень мають бути усунені до приймання?

Відповідь:
Виконавець має право самостійно організовувати та проводити тестування на проникнення на будь-яких етапах розроблення, тестування та підготовки до введення Системи в промислову експлуатацію з метою своєчасного виявлення та усунення вразливостей.

Водночас Власник Системи та Замовник забезпечать проведення незалежного тестування на проникнення із залученням визначених ними виконавців. Фінансування таких робіт здійснюватиметься за рахунок Власника Системи, Замовника або інших визначених ними джерел фінансування.

Кількість циклів повторного тестування визначатиметься з урахуванням результатів попередніх перевірок, характеру виявлених недоліків та етапу реалізації проєкту. До моменту приймання результатів робіт усі зауваження із середнім, високим та критичним рівнем критичності підлягають обов'язковому усуненню, а факт їх усунення має бути підтверджений результатами повторної перевірки. Зауваження низького рівня критичності можуть бути включені до плану подальшого вдосконалення Системи за погодженням із Власником Системи та Замовником.

Запитання:
Які браузери, пристрої та роздільності підтримуються, які вимоги до доступності (WCAG/ДСТУ) застосовуються та яка методика приймання доступності?

Лабораторія
законодавчих ініціатив

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

Відповідь:
Система повинна забезпечувати коректну роботу вебінтерфейсу в актуальних на момент проведення випробувань версіях браузерів Microsoft Edge, Safari та Google Chrome. Інтерфейс має бути адаптивним і забезпечувати зручне відображення та роботу на настільних комп'ютерах, ноутбуках, планшетах і смартфонах без створення окремої мобільної версії. Конкретні мінімальні роздільності екрана, перелік сценаріїв адаптивності та функціональність, для якої допускаються окремі обмеження на рівні підсистем, визначатимуться у технічному завданні.

Усі компоненти інтерфейсу повинні бути спроєктовані відповідно до останньої версії WCAG, чинної на момент реалізації. Конкретний рівень відповідності, застосовні вимоги ДСТУ та методика приймання доступності, включно з поєднанням автоматизованого тестування і ручної перевірки на визначених браузерах та пристроях, будуть встановлені на етапі формування технічного завдання з урахуванням сукупної вартості володіння та подальшої підтримки визначеного рівня доступності.

Запитання:
Яка юридично значуща процедура приймання міграції: контрольні суми, звірка кількості записів, вибіркова перевірка, акт розбіжностей і відповідальний за виправлення джерел даних?

Відповідь:
Процедура приймання результатів міграції визначатиметься в Методології міграції, яка розробляється Виконавцем та затверджується Адміністратором Системи. Зазначена Методологія повинна містити, зокрема, правила виправлення дефектів, алгоритми усунення конфліктів даних, порядок оброблення невідповідностей, що не можуть бути виправлені автоматично, а також методи перевірки результатів міграції.

Під час проведення міграції Виконавець зобов'язаний надати звіти, які підтверджують цілісність, повноту та коректність перенесених даних. Такі звіти можуть передбачати застосування контрольних сум, звірку кількості записів, перевірку зв'язності даних, вибіркову перевірку записів, формування протоколів виявлених розбіжностей та інші механізми контролю якості, визначені Методологією міграції.

Виявлені невідповідності повинні класифікуватися залежно від їх природи, а порядок їх усунення має бути окремо визначений для випадків, коли помилки виникли внаслідок процесу міграції, та для випадків, коли джерелом проблеми є початкові дані в системах-джерелах. Водночас відповідальність за внесення змін до вихідних систем, виправлення помилок у вихідних даних і погодження остаточних результатів міграції покладається на Власника Системи та інших уповноважених ним осіб.

Лабораторія
законодавчих ініціатив

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

Запитання:
Обсяг лінгвістичного забезпечення: чи вимагається повна англійська локаль інтерфейсу нарівні з українською, чи лише окремі розділи; хто постачає переклади (Виконавець/Замовник); чи потрібен адміністративний інтерфейс керування перекладами?

Відповідь:
Система повинна забезпечувати підтримку багатомовного інтерфейсу та містити централізований механізм керування локалізацією, який уможливлюватиме використання більше ніж однієї мовної версії. Остаточний перелік мов, а також обсяг локалізації окремих компонентів Системи визначатимуться на етапі деталізації вимог. Водночас архітектура рішення повинна передбачати можливість повної локалізації інтерфейсу, включно із системними повідомленнями, шаблонами, довідковими матеріалами та іншими текстовими елементами інтерфейсу.

Первинне наповнення мовних ресурсів здійснюється Виконавцем із подальшою передачею повноважень щодо їх адміністрування Власнику або Розпоряднику Системи. З цією метою має бути реалізований окремий адміністративний інтерфейс або інший штатний механізм керування перекладами, який не потребуватиме внесення змін до програмного коду Системи.

Запитання:
Обмеження інтенсивності запитів: які цільові пороги та політики (за користувачем, за IP, за ендпоінтом) очікуються і чи є вимога до адміністрування лімітів?

Відповідь:
Система повинна передбачати механізми обмеження інтенсивності запитів (rate limiting), спрямовані на забезпечення стабільності роботи, захист від зловживань, запобігання атакам типу denial-of-service та підтримання гарантованого рівня доступності сервісів.

Архітектура рішення має забезпечувати можливість застосування політик обмеження на різних рівнях, зокрема щодо окремих користувачів, ролей, IP-адрес, клієнтських застосунків, інтеграційних інтерфейсів, API-методів та інших категорій об'єктів. Конкретні порогові значення, правила застосування обмежень, механізми ескалації, а також порядок їх адміністрування визначатимуться на етапі проєктування та налаштування Системи з урахуванням фактичного навантаження, вимог безпеки та характеристик окремих компонентів.

Запитання:
Чи є вимога до формування переліку компонентів ПЗ (SBOM, формат CycloneDX/SPDX) та автоматизованого сканування залежностей і ліцензій (SCA) як частини постачання?

Лабораторія
законодавчих ініціатив

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

Відповідь:
У межах побудови процесу безпечної розробки Виконавець повинен забезпечити контроль складу програмних компонентів, сторонніх бібліотек, залежностей та їх ліцензійних обмежень із використанням автоматизованих засобів аналізу. Такий контроль має бути інтегрований у процеси безперервної інтеграції та постачання (CI/CD) і охоплювати перевірку відомих вразливостей, ліцензійних ризиків, актуальності версій компонентів, а також формування відповідної звітності.

Конкретні вимоги щодо формування переліку програмних компонентів (Software Bill of Materials, SBOM), форматів подання інформації (зокрема CycloneDX, SPDX або їх аналогів), порядку проведення Software Composition Analysis (SCA) та складу артефактів, що передаватимуться Власнику Системи, визначатимуться на етапі формування технічного завдання та деталізації вимог до процесів розроблення, експлуатації й забезпечення інформаційної безпеки Системи.

Запитання:
ТВ називає MongoDB у складі СКБД. Які дані/сценарії передбачають документне сховище (які модулі — споживачі); чи це обов'язковий компонент, чи допускається обґрунтована відмова на користь PostgreSQL (JSONB)?

Відповідь:
Пріоритетним є використання нереляційної СКБД MongoDB для сценаріїв, у яких доцільна документно-орієнтована модель зберігання даних. Конкретні категорії даних, модулі-споживачі та межі застосування MongoDB мають бути визначені на етапі формування технічного завдання та погодження архітектури Системи.

Водночас Виконавець може запропонувати альтернативне технічне рішення, зокрема використання PostgreSQL із JSONB, за умови надання належного обґрунтування щодо функціональної відповідності, продуктивності, масштабованості, відмовостійкості, інформаційної безпеки та сукупної вартості володіння. Застосування такої альтернативи допускається лише після погодження з Власником Системи та Замовником.

Запитання:
Який рівень відповідності WCAG (A/AA/AAA) і версія є обов'язковими; яка методика приймання доступності (автоматизований та ручний аудит, хто засвідчує результат)?

Відповідь:
Усі компоненти користувацького інтерфейсу Системи повинні бути спроєктовані та реалізовані відповідно до актуальної версії стандарту WCAG, чинної на момент виконання робіт. Конкретний рівень відповідності (A, AA або AAA) визначатиметься на етапі формування технічного завдання з урахуванням сукупної вартості володіння (TCO), витрат на впровадження та подальшу підтримку відповідного рівня доступності.

Лабораторія
законодавчих ініціатив

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

Порядок підтвердження відповідності вимогам доступності також буде визначений під час деталізації вимог. Водночас такий підхід має передбачати поєднання автоматизованого тестування та ручної перевірки, а результати оцінювання повинні бути документально зафіксовані та погоджені Власником Системи та Замовником.