**ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ**

(відповідно до пункту 41 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

**1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, його категорія:** ДЕРЖАВНА УСТАНОВА "ЦЕНТР ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ"; 03151, Україна, м. Київ, вул. Володимира Сікевича, 28; категорія замовника – бюджетна неприбуткова установа.

## 2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності): Послуги зі створення комплексної системи захисту інформації інформаційно-комунікаційної системи екстреної допомоги населенню за єдиним телефонним номером 112 для комунікаційного центру «Служба 112» у м. Львові з підтвердженням її відповідності і з комплектуванням засобами захисту інформації, за кодом CPV за ЄЗС ДК 021:2015 – 72240000-9 *«*Послуги з аналізу та програмування систем»

**3. Ідентифікатор закупівлі: —** UA-2024-05-09-007757-а

## 4. Обґрунтування технічних та якісних характеристик предмета закупівлі: Послуги зі створення комплексної системи захисту інформації інформаційно-комунікаційної системи екстреної допомоги населенню за єдиним телефонним номером 112 для комунікаційного центру «Служба 112» у м. Львові з підтвердженням її відповідності і з комплектуванням засобами захисту інформації, за кодом CPV за ЄЗС ДК 021:2015 – 72240000-9 *«*Послуги з аналізу та програмування систем»

**ТЕХНІЧНІ ВИМОГИ**

1. **Загальні вимоги**

Процес надання послуг зі створення комплексної системи захисту інформації інформаційно-комунікаційної системи екстреної допомоги населенню за єдиним телефонним номером 112 для комунікаційного центру «Служба 112» у м. Львові (етапи проєктування, попередніх випробувань та дослідної експлуатації) з підтвердженням її відповідності і з комплектуванням засобами захисту інформації повинен проходити відповідно до вимог нормативних та нормативно-правових документів у сфері захисту інформації.

1. **Вимоги до складу заходів**

Процес надання послуг передбачає такі етапи:

1. Постачання та налаштування криптографічних засобів захисту інформації, які входять до складу КЗЗ КСЗІ ІКС 112 Львів.
2. Розробка техноробочого проєкту КСЗІ ІКС 112 Львів.
3. Розробка експлуатаційної документації КСЗІ ІКС 112 Львів.
4. Попередні випробування та дослідна експлуатація КСЗІ ІКС 112 Львів.
5. Організація та супроводження проведення первинної державної експертизи КСЗІ ІКС 112 Львів.

*Постачання та налаштування технічних та криптографічних засобів захисту інформації, які входять до складу КЗЗ КСЗІ ІКС 112 Львів містить:*

1. Здійснення Виконавцем постачання та налаштування криптографічних засобів захисту інформації, які входять до складу КЗЗ КСЗІ ІКС 112 Львів, у відповідності до вимог, що наведені нижче.

*Розробка техноробочого проєкту КСЗІ ІКС 112 Львів містить:*

1. Проєктування КСЗІ ІКС 112 Львів (п. 6.4 НД ТЗІ 3.7-003-2023).
2. Розробку техноробочого проєкту КСЗІ ІКС 112 Львів (п. 6.4.3 НД ТЗІ 3.7-003-2023, НД ТЗІ 2.5-004-99).

*Розробка експлуатаційної документації КСЗІ ІКС 112 Львів містить:*

1. Розробку експлуатаційної документації КСЗІ ІКС 112 Львів (п. 6.4.4 НД ТЗІ 3.7-003-2023).

*Попередні випробування та дослідна експлуатація КСЗІ ІКС 112 Львів містить:*

1. Створення комісії з попередніх випробувань та дослідної експлуатації КСЗІ ІКС 112 Львів.
2. Організацію служби захисту інформації ІКС, призначення адміністраторів ІКС.
3. Проведення попередніх випробувань КСЗІ ІКС 112 Львів.
4. Проведення дослідної експлуатації КСЗІ ІКС 112 Львів.
5. Здійснення додаткового налагоджування та конфігурування компонентів КСЗІ ІКС 112 Львів (за необхідності);
6. Здійснення коригування проєктної та експлуатаційної документації (за необхідності).

Під час попередніх випробувань перевіряються працездатність КСЗІ та її відповідність до вимог ТЗ КСЗІ ІКС 112 Львів.

Попередні випробування повинні бути проведені згідно з Програмою та методиками випробувань. Програму й методики випробувань готує Розробник КСЗІ ІКС 112 Львів. Програму випробувань узгоджує Замовник. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами (п. 6.5.6 НД ТЗІ 3.7-003-2023).

Попередні випробування організовує Замовник, а проводить розробник КСЗІ ІКС 112 Львів спільно із Замовником. Для проведення попередніх випробувань КСЗІ ІКС 112 Львів Замовником створюється комісія. Головою комісії призначається представник Замовника (п. 6.5.6 НД ТЗІ 3.7-003-2023).

Результати попередніх випробувань оформлюються протоколом, де міститься висновок щодо можливості прийняття КСЗІ ІКС 112 Львів у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт (п. 6.5.6 НД ТЗІ 3.7-003-2023).

Після усунення недоліків, у випадку їх наявності, коригування проєктної та експлуатаційної документації КСЗІ оформлюється Акт про приймання КСЗІ ІКС 112 Львів у дослідну експлуатацію (п. 6.5.7 НД ТЗІ 3.7-003-2023).

За результатами дослідної експлуатації КСЗІ ІКС 112 Львів повинен бути складений акт за довільною формою про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ ІКС 112 Львів на державну експертизу (п. 6.5.7 НД ТЗІ 3.7-003-2023).

*Організація та супроводження проведення первинної державної експертизи КСЗІ ІКС 112 Львів.*

Державна експертиза проводиться з метою визначення відповідності КСЗІ ІКС 112 Львів технічному завданню на створення КСЗІ, вимогам НД ТЗІ і визначення можливості введення КСЗІ ІКС 112 Львів в експлуатацію.

Державна експертиза КСЗІ ІКС 112 Львів проводиться згідно з Положенням про державну експертизу у сфері технічного захисту інформації.

Виконавець зобов’язаний організувати та забезпечити проведення Державної експертизи в галузі технічного захисту інформації КСЗІ ІКС 112 Львів, оплатити за власний рахунок вартість проведених Організатором експертних робіт та забезпечити отримання Атестату відповідності, зареєстрованого у Держспецзв’язку.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна державна експертиза.

1. **Вимоги до засобів КЗЗ КСЗІ ІКС 112 Львів**

З метою криптографічного захисту інформації, реалізації політик інформаційної безпеки та інших вимог щодо захисту інформації, Виконавець повинен здійснити постачання таких криптографічних засобів захисту інформації, які будуть входити до складу КЗЗ ІКС:

**3.1. Постачання криптографічних засобів захисту інформації**

Таблиця 1. Вимоги до спеціалізованого ПЗ

| **№ з/п** | **Вимоги до спеціалізованого ПЗ** | **Деталізація вимог** |
| --- | --- | --- |
| **1. Підсистема захисту інформації, що передається між ЦОД (Київ) та ЦОД (Львів)** | | |
| 1.1 | Реалізація шлюзів у вигляді образу віртуальної машини (Virtual Appliance) з попередньо налаштованими операційною системою та програмним забезпеченням у віртуальній інфраструктурі основного (Київ) і резервного (Львів) ЦОД. | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware |
| 1.2 | Забезпечення пропускної здатності захищеного каналу між ОЦОД і РЦОД | Не менше 2 Гбіт/с |
| 1.3 | Можливість горизонтального масштабування пропускної здатності за рахунок збільшення кількості шлюзів (Virtual Appliance) | Можливість збільшення до 4 екземплярів |
| 1.4 | Використання сучасних криптографічних алгоритмів для забезпечення конфіденційності через симетричного шифрування та автентичності інформації через імітовставку як національних, так і міжнародних | * ГОСТ 34.311-95+ДСТУ ГОСТ 28147:2009; * ДСТУ 7564:2014+ДСТУ 7624:2014; * ДСТУ 7564:2014+ДСТУ 8845:2019 (бажано); * SHA-256+AES |
| 1.5 | Використання сучасних механізмів стиснення трафіку (дані, що передаються, базуються на форматах XML, JSON) | * LZO; * LZ4;   Інші |
| 1.6 | Засоби КЗІ повинні мати відповідний діючий позитивний експертний висновок (сертифікат відповідності) Держспецзв’язку України | Обов’язково |
| 1.9 | Підтримка віртуальних мереж. | Обов’язково |
| 1.10 | Підтримка маршрутизації пакетів на рівні L3, що дозволяє відмовитися від додаткових маршрутизаторів. | Обов’язково |
| 1.11 | Віддалене управління VPN-шлюзами через web-інтерфейс | Обов’язково |
| 1.12 | Можливість агрегації каналів, для збільшення пропускної здатності захищених каналів | Обов’язково |
| 1.13 | Віддалений централізований моніторинг навантаження за SNMP. | Обов’язково |

**3.1.1. Вимоги до наявності моніторингу спеціалізованого ПЗ**

Спеціалізоване ПЗ повинно надавати можливість онлайн-аналізу даних кожної підсистеми та кожного модуля спеціалізованого ПЗ за протоколом SNMP, а саме:

лог- журнали:

доступу;

інтеграцій;

помилок;

метрики обладнання:

завантаженість процесорів;

завантаженість оперативної пам’яті;

завантаженість фізичних дисків;

завантаженість мережних інтерфейсів.

**3.1.2. Вимоги до інформаційного обміну з державними електронними інформаційними реєстрами**

Спеціалізоване ПЗ повинно забезпечити можливість проведення інформаційного обміну з державними електронними інформаційними реєстрами, накладання/перевірки КЕП під час проведення інформаційного обміну згідно з вимогами нормативних документів Кабінету Міністрів України, Міністерства юстиції України, Держспецзв’язку, ЦЗО.

**3.1.3. Вимоги до ліцензії**

Виконавець надає невиключну ліцензію на спеціалізоване ПЗ у такому обсязі:

Замовник має право використовувати спеціалізоване ПЗ будь-яким способом на власний розсуд на всій території світу протягом всього строку дії авторських прав на спеціалізоване ПЗ, що передбачене законодавством, в тому числі (але не виключно) для комерційної діяльності та виконання робіт та/або надання послуг третім особам. Право на використання програмного забезпечення виникає у Замовника з моменту отримання ліцензії на програмне забезпечення;

Замовник має право інтегрувати програмне забезпечення до наявних у нього автоматизованих або інформаційних систем, програмних забезпечень, комп’ютерних програм тощо, в тому числі для взаємодії з інформаційними системами третіх осіб з використанням АРІ і технологій обміну даними (REST, JSON тощо);

Замовник має право відтворювати програмне забезпечення для продуктивного середовища в кількості, що відповідає наявним ЦОД, в яких встановлено спеціалізоване програмне забезпечення, а з метою тестування – в будь-якій кількості;

Замовник не має права комерційного продажу спеціалізованого ПЗ та не має права передачі його третім особам.

**3.1.4. Відповідність до вимог законодавства й нормативних актів України**

Спеціалізоване ПЗ повинно забезпечити виконання вимог законодавства й нормативних актів України до інформаційно-телекомунікаційних систем, що здійснюють інформаційний обмін з державними електронними інформаційними ресурсами України та передають персональні дані.

**3.1.5. Вимоги до розподілу ролей між фахівцями, які працюють зі спеціалізованим ПЗ**

Спеціалізоване ПЗ повинно мати розподіл ролей між фахівцями за їх функціональними обов’язками, які забезпечують працездатність та функціонування цього програмного забезпечення відповідно до вимог таких документів:

Постанови Кабінету Міністрів України від 7 листопада 2018 р. № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;

Постанови Кабінету Міністрів України від 18 грудня 2018 р. № 1215 «Про затвердження Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг».

**3.1.6. Вимоги до показників навантаження**

Спеціалізоване ПЗ та його налаштування повинні забезпечувати:

час обробки будь-яких запитів під час дотримання обмежень за кількістю одночасних діючих користувачів та/або згенерованих запитів із наданням релевантних відповідей - не більше 1-2 секунд;

зберігання історії документів та даних відповідно до вимог законодавства й нормативних актів України, але в будь-якому разі не менше 3 місяців;

можливість нарощування кількості користувачів/одночасних запитів та об’ємів БД без потреби будь-яких додаткових доробок.

**3.1.7. Вимоги до надійності роботи**

Архітектура та налаштування спеціалізованого ПЗ повинні забезпечувати функціонування в режимі 24/365 (24 години на добу, 365 діб на рік) у віртуальній інфраструктурі з допустимим часом простою не більше 6 годин на рік за умови виконання регламентних профілактично-технічних робіт, які описані в інструкціях адміністраторів.

Надійність повинна забезпечуватися за рахунок:

можливості використання кластеризації критичних компонентів та/або реплікації даних між хостами;

режиму автоматичного аналізу поточного стану (у режимі реального часу) та фіксації повідомлень про аварії та збоїв;

організації систематичного резервного копіювання та наявності можливості відновлення інформації з резервних копій у ручному режимі.

**3.1.8. Вимоги до експлуатації, технічного обслуговування та гарантійних зобов’язань**

Режим експлуатації спеціалізованого ПЗ – 24/365 (24 години на добу/365 діб на рік).

Під час експлуатації спеціалізованого ПЗ:

технічне обслуговування повинне виконуватись обслуговуючим персоналом Замовника згідно з вимогами інструкції з експлуатації, інструкцій адміністраторів, які надаються Виконавцем;

супровід програмного забезпечення виконується персоналом Замовника та/або Виконавця відповідно до переліку несправностей/дефектів, які наведені в інструкції з експлуатації, інструкціях адміністраторів, які надаються Виконавцем.

Виконавець забезпечує гарантійну (технічну) підтримку спеціалізованого ПЗ протягом 12 місяців з дати підписання акта приймання-передачі послуг впровадження спеціалізованих програмних засобів. Під гарантійною підтримкою розуміється зобов’язання Виконавця безоплатно виправляти виявлені помилки протягом гарантійного періоду.

Якщо протягом терміну гарантійної (технічної) підтримки виявляються дефекти або невідповідність у роботі спеціалізованого ПЗ, Виконавець повинен власними силами і за власні кошти усунути помилки, недоліки, збої в роботі в такі строки:

перша реакція на повідомлення про будь-який інцидент – не більше ніж 4 години в робочий час та не більше ніж 6 годин у неробочий час;

визначення причини інциденту – не більше ніж 6 годин у робочу добу та не більше ніж 8 годин у вихідні та святкові дні;

відновлення працездатності, якщо причиною інциденту є програмний збій, руйнування бази даних – у будь-якому разі за термін не більше ніж 24 години;

відновлення працездатності, якщо причиною є помилки в роботі, які викликані змінами в порядку інформаційного обміну з державними електронними інформаційними ресурсами України (якщо такі зміни впроваджуються під час гарантійного строку) – не більше 24 годин з моменту отримання опису змін.

Одночасно з цим строк гарантійної (технічної) підтримки спеціалізованого ПЗ продовжується на строк, який погоджений Замовником і Виконавцем, для усунення виявлених дефектів, помилок, неполадок, збоїв у роботі програмного забезпечення.

**3.1.9. Вимоги до інформаційної безпеки**

**3.1.9.1. Захист інформації від несанкціонованого доступу**

Для забезпечення захисту інформації від несанкціонованого доступу в спеціалізованому ПЗ повинно бути передбачено:

1. Механізми управління доступом, що забезпечують виконання таких функцій захисту:

ідентифікація користувачів (закріплення за кожним об’єктом персонального ідентифікатора);

автентифікація користувачів (визначення достовірності об’єкта або суб’єкта за поданим ним ідентифікатором);

двофакторна автентифікація користувачів з адміністративними правами доступу та тих користувачів, які отримують доступ до інформації з обмеженим доступом, що застосовується під час входу в систему.

1. Механізми моніторингу, що передбачають обов’язкову реєстрацію:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

даних про активність користувачів;

спроб несанкціонованих дій з інформацією;

результатів перевірки цілісності засобів захисту інформації (у випадку їх використання).

Примітка: Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають на це відповідних повноважень (адміністратор безпеки).

1. Зберігання паролів у системі повинно забезпечуватися з використанням методів хешування з використанням модифікатора (солі).

**3.1.9.2. Взаємодія із зовнішніми інформаційними системами**

У разі взаємодії із зовнішніми інформаційними системами передача інформації з обмеженим доступом з однієї системи до іншої повинна здійснюватися в зашифрованому вигляді або захищеними каналами зв’язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

**3.1.10. Вимоги до збереження інформації в разі аварій**

У разі виникнення аварійних подій або помилок у роботі спеціалізованого ПЗ подія/помилка повинна реєструватися у відповідному електронному журналі, а адміністратори повинні отримати відповідне повідомлення із зазначенням типу події/помилки.

До складу повідомлення щодо події аварійного типу повинні входити:

час;

текстова назва аварії;

код помилки та її опис.

Налаштування збереження інформації в разі аварій повинно забезпечувати такий режим роботи спеціалізованого ПЗ:

будь-яка операція, що виконана, повинна бути записана на основному та дублюючому сховищах даних, які розташовані на основному та резервному ЦОД відповідно;

якщо будь-яка операція повністю не виконана, то інформація про таку послугу повинна доводити стан/крок виконання цієї операції.

Збереження інформації повинно бути забезпечене в разі виникнення таких подій (аварій, відмов тощо):

відмови обладнання сервера/сховища даних;

вимкнення живлення на робочому місці та/або на сервері баз даних;

відмови обладнання робочої станції;

відмови ліній зв’язку.

З метою забезпечення зберігання інформації повинні використовуватися:

резервне копіювання;

відновлення даних під час збоїв у роботі мережного, програмного й апаратного забезпечень.

**3.1.11. Вимоги до патентної чистоти**

Спеціалізоване ПЗ має бути таким, що може бути вільно використане в Україні без загрози порушення діючих на її території прав інтелектуальної власності на технології та/або складові технологій, що посвідчуються охоронними документами України (патентами) та свідоцтвами, які належать третім особам, згідно з охоронними документами (патентами) і свідоцтвами на ці об᾿єкти та нормативно-правовими актами України, а також відповідно до конкретного періоду часу, обумовленого строком дії охоронних документів (патентів) і свідоцтв на технології та/або їх складові на території України.

Патентна чистота спеціалізованого ПЗ забезпечується й гарантується Виконавцем.

**3.1.12. Вимоги до документування**

Виконавець повинен надати Замовнику документацію в такому складі:

1. Ліцензія на спеціалізоване програмне забезпечення.
2. Експертні висновки на спеціалізоване ПЗ Адміністрації державної служби спеціального зв’язку та захисту інформації України.
3. Загальний опис спеціалізованого програмного забезпечення.
4. Загальний опис систем канального криптографічного захисту інформації.
5. Керівництво або інструкція з розгортання архіву тривалого зберігання електронних документів.
6. Керівництво або інструкція з розгортання спеціалізованого програмного забезпечення.
7. Керівництво або інструкція з експлуатації комунікаційного модуля центру реєстрації.
8. Керівництво або інструкція системного адміністратора.
9. Керівництво або інструкція з експлуатації адміністратора сертифікації.
10. Керівництво або інструкція з експлуатації адміністратора реєстрації.
11. Керівництво або інструкція з експлуатації адміністратора безпеки та аудиту.
12. Опис API спеціалізованого програмного забезпечення та керівництво з інтеграції.

Перелік зазначеної документації не є вичерпним та може бути розширений під час укладання договору.

Документація повинна бути достатньою за повнотою і змістом для використання технічними фахівцями та користувачами.

Документи передаються Замовнику у двох примірниках на паперовому носії (один примірник для Замовника, другий – для Виконавця) та на електронному носії (кожний документ окремим файлом у форматах \*.docx та \*.pdf).

**3.1.13. Вимоги до проведення навчання**

Виконавець зобов’язаний провести навчання по роботі зі спеціалізованим ПЗ не менше ніж 2 працівників Замовника.

**3.1.14. Вимоги до проведення випробувань та дослідної експлуатації спеціалізованого ПЗ**

Замовник разом з Виконавцем проводять випробування спеціалізованого ПЗ відповідно до вимог документа «Програма та методика випробувань спеціалізованого програмного забезпечення» з використанням сертифікованого МКМ, який Виконавець тимчасово надає для проведення випробувань.

За підсумками випробувань складається протокол випробувань спеціалізованого ПЗ, який підписується представниками Замовника та Виконавця.

Примітка. Акт приймання-передачі спеціалізованого ПЗ складається за умови відсутності недоліків та зауважень під час проведення випробувань спеціалізованого ПЗ.

Після завершення впровадження спеціалізованого ПЗ Замовник разом із Виконавцем проводять дослідну експлуатацію спеціалізованого ПЗ, зокрема здійснюють перевірку обміну інформаційними даними з державними електронними інформаційними реєстрами відповідно до «Програми та методики дослідної експлуатації спеціалізованого програмного забезпечення».

За підсумками дослідної експлуатації складається протокол дослідної експлуатації спеціалізованого ПЗ, підписаний представниками Замовника та Виконавця.

Примітка. Акт завершення дослідної експлуатації спеціалізованого ПЗ складається за умови відсутності недоліків та зауважень під час проведення дослідної експлуатації.

**3.1.15. Додаткові вимоги до Спеціалізованого ПЗ**

Спеціалізоване ПЗ повинно бути від одного виробника та функціонувати як одне ціле, мати налаштовану інтеграцію між складовими частинами спеціалізованого програмного забезпечення, включаючи МКМ (окремо закуплені Замовником), інфраструктурою Центрального засвідчувального центру Міністерства цифрової трансформації України та мати можливість забезпечувати інформаційний обмін з державними електронними інформаційними ресурсами України.

## КАЛЕНДАРНИЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| **№ з/п** | **Найменування Послуг**  **(етапи та результати надання послуг)** | **Опис надання Послуг**  **(розроблені документи)** | **Термін виконання, робочих днів** |
| **1** | **Побудова КСЗІ ІКС 112 Львів**  **разом із комплектуванням засобами захисту інформації** | | |
| 1.1 | Постачання криптографічних та захисту інформації, які входять до складу КЗЗ КСЗІ ІКС 112 Львів разом із їх налаштуванням. | Поставлені засоби КЗЗ КСЗІ ІКС 112 Львів: | до 20 |
| 1. *Заповнюється Виконавцем відповідно до Вимог вказаних в п. 3* |
| 2. Налаштування криптографічних засобів захисту інформації, які входять до складу КЗЗ КСЗІ ІКС 112 Львів |
| 1.2 | Розробка Техноробочого проекту та експлуатаційної документації КСЗІ ІКС 112 Львів | 1. Техноробочий проєкт КСЗІ ІКС 112 Львів. 2. Нормативно-розпорядча документація КСЗІ ІКС 112 Львів:   посадові (функціональні) інструкції адміністраторів, користувачів ІКС;  технологічні (операційні) інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ ІКС 112 Львів;   1. Організаційно-розпорядча документація КСЗІ ІКС 112 Львів:   проєкт наказу про призначення комісії для проведення попередніх випробувань та дослідної експлуатації КСЗІ ІКС 112 Львів;  проєкт акта про приймання у дослідну експлуатацію КСЗІ;  проєкт акта про завершення дослідної експлуатації КСЗІ ІКС 112 Львів;  проєкт акта завершення робіт зі створення КСЗІ ІКС 112 Львів;   1. Супровідна документація КСЗІ:   формуляр ІКС 112 Львів. | до 30 |
| 1.3 | Проведення попередніх випробувань і дослідної експлуатації КСЗІ ІКС 112 Львів | Розроблена документація щодо проведення випробувань КСЗІ:  програма та методика проведення попередніх випробувань КСЗІ ІКС 112 Львів;  протокол проведення попередніх випробувань КСЗІ ІКС 112 Львів;  проєкт акта про приймання КСЗІ ІКС 112 Львів у дослідну експлуатацію;  проект акта завершення дослідної експлуатації КСЗІ ІКС 112 Львів. | до 20 |
| **2** | **Організація та супроводження проведення державної експертизи**  **КСЗІ ІКС 112 Львів** | | |
| 2.1 | Розробка експертною організацією програми та методики проведення експертних випробувань | Програма проведення експертних випробувань КСЗІ ІКС 112 Львів погоджена із Замовником  Методика проведення експертних випробувань КСЗІ ІКС 112 Львів | до 60 |
| 2.2 | Проведення випробувань КСЗІ на відповідність до вимог нормативних документів системи технічного захисту інформації України | Протокол виконання робіт відповідно до методики проведення експертних випробувань КСЗІ ІКС 112 Львів |
| 2.3 | Оформлення результатів експертних робіт і проєкту експертного висновку та направлення до Держспецзв’язку | Проєкт експертного висновку на КСЗІ ІКС 112 Львів надісланий до Держспецзв’язку. |
| 2.4 | Забезпечення супроводження процесу розгляду матеріалів експертизи в Адміністрації Державної служби спеціального зв’язку та захисту інформації до отримання Атестату відповідності КСЗІ ІКС 112 Львів | Атестат відповідності КСЗІ ІКС 112 Львів та експертний висновок на КСЗІ ІКС 112 Львів. |

\*Термін виконання визначається у робочих днях з моменту завершення попереднього етапу (стадії). Деякі етапи можуть виконуватись паралельно.

Учасник якого визначено переможцем процедури закупівлі, до укладання договору за результатом проведеної процедури закупівлі, бере зобов’язання щодо проведення експертизи вартості послуг (за свій рахунок, без витрат з боку Замовника), за результатом аукціону/розкриття тендерних пропозицій та надає Замовнику документ (висновок експертизи), що підтверджує вартість вказаних послуг. У разі надання документу де вартість послуг буде нижча ніж зазначив Учасник за результатом аукціону/розкриття тендерних пропозицій, Учасник-Переможець зобов’язується укласти разом із договором додаткову угоду до договору, на зменшення вартості договору у відповідності до підпункту 5 пункту 19 Особливостей. ***(надати у складі тендерної документації гарантійний лист)***.

**5. Обґрунтування розміру бюджетного призначення:** розмір бюджетного призначення визначено Законом України «Про Державний бюджет України на 2024 рік» за КПКВК 1001050 «Забезпечення діяльності органів, установ та закладів Міністерства внутрішніх справ України, підготовка кадрів закладами вищої освіти із спеціальними умовами навчання» відповідно до бюджетного запиту на 2024 рік.

**6. Очікувана вартість предмета закупівлі:** 786 716,67 грн. (сімсот вісімдесят шість тисяч сімсот шістнадцять гривень 67 коп.) з ПДВ.

**7. Обґрунтування очікуваної вартості предмета закупівлі:** Очікувана вартість визначена відповідно до частини 1 та 2 пункту 1 Розділу ІІІ «Методи визначення очікуваної вартості» Примірної методики визначення очікуваної вартості предмета закупівлі затвердженої Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 18.02.2020 № 275 та розрахована, як середньоарифметичне значення масиву отриманих даних, що розраховується за такою формулою: Цод = (Ц1 +… + Цк) / К.

**8. Процедура закупівлі:** Застосовується процедура відкритих торгів з особливостями.