

**«Послуги зі створення чотирьох комплексних систем захисту інформації в автоматизованих системах класу «1», призначених для обробки інформації, що становить державну таємницю та однієї комплексної системи захисту інформації в автоматизованій системі класу «1», призначеній для обробки службової інформації» (ДК 021:2015:72220000-3 Консультаційні послуги з питань систем та з технічних питань).**

**«Відкриті торги з особливостями.**

Дата оприлюднення: 30 листопада 2022 17:54 год. за київським часом.

Звернення за роз'ясненнями: до 05 грудня 2022 року 00:00 год за київським часом.

Оскарження умов закупівлі: до 05 грудня 2022 року 00:00 год за київським часом.

Кінцевий строк подання тендерних пропозицій: 08 грудня 2022 року 00:00 год за київським часом.

Очікувана вартість: 490 000,00 УАН з ПДВ.

Розмір мінімального кроку пониження ціни: 4900,00 УАН з ПДВ.

Розмір мінімального кроку пониження ціни, %: 1,00 %.

Мова (мови), якою (якими) повинні готуватися тендерні пропозиції: Мова тендерної пропозиції українська

№	Розділ I. Загальні положення	
1	2	3
1	<b>Терміни, які вживаються в тендерній документації</b>	Тендерну документацію розроблено відповідно до вимог Закону України «Про публічні закупівлі» від 25.12.2015 № 922 -VIII (зі змінами в редакції від 16.08.2022) з урахуванням «Особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування» затверджених постановою Кабінету Міністрів України від 12 жовтня 2022 року № 1178 (далі – Особливості). Терміни вживаються у значеннях, визначених Законом України «Про публічні закупівлі» (далі – Закон) та Особливостями.
2	<b>Інформація про замовника торгів</b>	
2.1	повне найменування	<b>Сумська обласна прокуратура</b>

2.2	місцезнаходження	вул. Герасима Кондратьєва, буд. 33, м. Суми, 40000
2.3	прізвище, ім'я та по батькові, посада та електронна адреса однієї чи кількох посадових осіб замовника, уповноважених здійснювати зв'язок з учасниками	<b>ПІБ: Іванов Сергій Васильович;</b> <b>посада: головний спеціаліст відділу матеріально-технічного забезпечення та соціально-побутових потреб Сумської обласної прокуратури, уповноважена особа.</b> <b>Адреса: вул. Герасима Кондратьєва, буд. 33, м. Суми, 40000, тел. (099)3632574), електронна пошта: sergey_ms31@ukr.net</b>
3	<b>Процедура закупівлі</b>	Відкриті торги з особливостями
4	<b>Інформація про предмет закупівлі</b>	
4.1	назва предмета закупівлі	<b>«Послуги зі створення чотирьох комплексних систем захисту інформації в автоматизованих системах класу «1», призначених для обробки інформації, що становить державну таємницю та однієї комплексної системи захисту інформації в автоматизованій системі класу «1», призначеній для обробки службової інформації».</b> <b>(ДК 021:2015-72220000-3 Консультаційні послуги з питань систем та з технічних питань).</b>
4.2	опис окремої частини або частин предмета закупівлі (лота), щодо яких можуть бути подані тендерні пропозиції	Закупівля здійснюється щодо предмета закупівлі в цілому, без поділу на окремі частини (лоти).
4.3	кількість товару та місце його поставки або місце, де повинні бути виконані роботи чи надані послуги, їх обсяги	Місце надання послуг: вул. Герасима Кондратьєва, 33, м. Суми, Україна, 40000 (склад). Обсяг надання послуг згідно із додатком 1 до тендерної документації (5 послуг).
4.4	строки поставки товарів, виконання робіт, надання послуг	Строк надання послуг до <b>25.12.2022.</b>

**ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ, У ТОМУ ЧИСЛІ ВІДПОВІДНА ТЕХНІЧНА СПЕЦИФІКАЦІЯ.**

**«Послуги зі створення чотирьох комплексних систем захисту інформації в автоматизованих системах класу «1», призначених для обробки інформації, що становить державну таємницю та однієї комплексної системи захисту інформації в автоматизованій системі класу «1», призначеній для обробки службової інформації**

(ДК 021:2015-72220000-3 Консультаційні послуги з питань систем та з технічних питань).

**Загальні вимоги:**

Надання послуг здійснюється виконавцем за адресою замовника: вул. Герасима Кондратьєва, 33, м. Суми, 40000.

Строк надання послуг: до 25 грудня 2022 року.

**Вимоги до предмета закупівлі:**

**1. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**1) Опис автоматизованих систем.**

Відповідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю, а підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку встановленому законодавством.

Автоматизована система (АС) призначена для обробки інформації з обмеженим доступом (службової інформації або інформації, що становить державну таємницю) та відкритої інформації, вимоги щодо захисту якої встановлено законом.

Вимоги до забезпечення захисту інформації в системі:

- інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення;
- модифікувати інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження;
- спроби модифікації чи знищення інформації користувачами, які не мають на це повноважень, не ідентифікованими користувачами або користувачами з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.
- під час обробки інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

У системі повинна здійснюватися обов'язкова реєстрація, зокрема:

- результатів ідентифікації та автентифікації користувачів;
- результатів виконання користувачем операцій з обробки інформації;
- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки.

Крім того, повинна забезпечуватись можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі.

Реєстрація повинна здійснюватися автоматичним способом, а реєстраційні дані захищатися від модифікації та знищення користувачами, які не мають відповідних повноважень. Реєстрація спроб несанкціонованих дій з інформацією повинна супроводжуватися повідомленням про них адміністратора безпеки.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі, повинна здійснюватися автоматизованим способом.

Елементи системи будуються, зважаючи на принцип розмежування повноважень різних категорій користувачів щодо доступу (перегляду) та внесення (будь-якої модифікації) інформації.

## **2) Мета створення комплексної системи захисту інформації.**

Метою створення комплексної системи захисту інформації (далі – КСЗІ) АС є забезпечення конфіденційності, цілісності та доступності інформації, яка циркулює в АС.

### **2. НОРМАТИВНО-ПРАВОВА БАЗА.**

Учасник повинен надати послуги зі створення КСЗІ АС та організації проведення її державної експертизи у відповідності до вимог державних стандартів та чинних нормативних документів сфери технічного захисту інформації (далі – НД ТЗІ).

Послуги, що є предметом закупівлі, повинні надаватись відповідно до вимог таких нормативно-правових та нормативних актів:

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про інформацію»;
- Закон України «Про захист персональних даних»;
- постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 № 93, зареєстровано в Міністерстві юстиції України 16.07.07 за № 820/14087;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
- НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;
- НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

### **3. ВИМОГИ ДО ЗМІСТУ ПОСЛУГ**

3.1. Відповідно до вимог нормативних документів з технічного захисту інформації, створення КСЗІ АС складається з двох етапів: етапу формування загальних вимог до КСЗІ та етапу введення КСЗІ АС в дію.

3.1.1. На етапі формування загальних вимог до КСЗІ АС, проведення організаційно-технічних заходів, складання технічної та експлуатаційної документації надавач послуг повинен (відповідно до однієї АС):

- придбати та встановити генератор електромагнітного шуму (не стосується АС, яка призначена для обробки службової інформації);
- придбати та встановити комплекс засобів захисту від несанкціонованого доступу «Лоза-1»;
- придбати та встановити програмне забезпечення антивірусного захисту;

- здійснити обстеження середовища функціонування АС та підготовку проєкта акта обстеження;
- розробити Політику безпеки та оформити План захисту інформації в АС;
- розробити технічне завдання на КСЗІ АС;
- розробити техноробочий проєкт КСЗІ;
- провести спеціальні дослідження (інструментальний контроль захищеності інформації) АС від витоку інформації каналами побічних електромагнітних випромінювань та наведень (не стосується АС, яка призначена для обробки службової інформації);
- провести атестацію комплексу технічного захисту інформації (не стосується АС, яка призначена для обробки службової інформації);
- здійснити розробку та оформлення експлуатаційної документації на КСЗІ.

3.1.2. На етапі введення КСЗІ АС в дію надавач послуг повинен (відповідно до однієї АС):

- спільно із замовником провести попередні випробування КСЗІ АС;
- взяти участь у проведенні дослідної експлуатації КСЗІ АС. Згідно з вимогами НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

3.2. Державна експертиза КСЗІ АС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ у складі АС в експлуатацію.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такої 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 послуг, проводиться повторна експертиза.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проєктування.

3.3. Виконавцю дозволяється змінювати послідовність надання послуг, здійснювати одночасно надання декількох послуг, зазначених у п. 4 цього додатку, якщо це не призводить до зниження їх якості і не суперечить цілям їх надання.

#### **4. ВИМОГИ ДО СКЛАДУ ТА ЗМІСТУ ДОКУМЕНТАЦІЇ НА КСЗІ АС.**

Перелік документації, яка повинна бути розроблена надавачем послуг відповідно до змісту послуг та передана замовнику, наведена у таблиці (відповідно до однієї АС).

##### **Зміст послуг та перелік документації, яка надається замовнику:**

<b>№ з/п</b>	<b>Зміст послуг</b>	<b>Перелік звітної документації</b>
1.	Створення комплексної системи захисту інформації АС: <ul style="list-style-type: none"> <li>- здійснення обстеження середовища функціонування АС та підготовка проєкта акта обстеження;</li> <li>- розробка Політики безпеки та оформлення Плану захисту інформації в АС;</li> <li>- розробка Технічного завдання на КСЗІ;</li> <li>- розробка техноробочого проєкту;</li> <li>- розробка та оформлення експлуатаційної документації на КСЗІ;</li> <li>- налаштування комплексу засобів захисту інформації від несанкціонованого доступу;</li> <li>- налаштування генератора шуму (не стосується АС, яка призначена для обробки службової</li> </ul>	Підготовлено наступну документацію: <ul style="list-style-type: none"> <li>- Акт обстеження АС;</li> <li>- Політика безпеки інформації в АС;</li> <li>- План захисту інформації в АС;</li> <li>- Технічне завдання;</li> <li>- Матеріали техноробочого проєкту;</li> <li>- Комплект експлуатаційної документації на КСЗІ;</li> <li>- документація атестації комплексу технічного захисту інформації (не стосується АС, яка призначена для обробки службової інформації);</li> <li>- Проєкт наказу про введення в дію КСЗІ;</li> </ul>

	інформації); - проведення спеціальних досліджень (інструментальний контроль захищеності інформації) АС від витоку інформації каналами побічних електромагнітних випромінювань та наведень (не стосується АС, яка призначена для обробки службової інформації); - проведення атестації комплексу технічного захисту інформації (не стосується АС, яка призначена для обробки службової інформації); - попередні випробування КСЗІ; - дослідна експлуатація КСЗІ.	- Проект наказу про створення комісії та проведення попередніх випробувань; - Програма та методика попередніх випробувань; - Протокол попередніх випробувань; - Проект наказу про проведення дослідної експлуатації; - Акт завершення дослідної експлуатації.
2.	Організація проведення державної експертизи у сфері технічного захисту інформації КСЗІ.	Підготовка Декларації про відповідність КСЗІ вимогам НД ТЗІ

Примітки.

До матеріалів техноробочого проекту обов'язково додається пояснювальна записка.

2. Комплект експлуатаційної документації на КСЗІ повинен містити наступні документи:

- інструкції адміністраторів АС;
- інструкція про порядок забезпечення антивірусного захисту в АС;
- інструкція з модернізації АС;
- інструкція з організації резервного копіювання;
- інструкція про організацію контролю за функціонуванням комплексної системи захисту інформації;

- порядок здійснення процедур поновлення з резервних копій архівованої інформації інформаційних об'єктів АС.

Документація на КСЗІ АС, яка буде розроблена надавачем послуг та передана замовнику, повина відповідати вимогам чинних нормативних документів у сфері ТЗІ (НД ТЗІ 1.1-002-99; НД ТЗІ 3.7-003-2005; НД ТЗІ 1.4-001-2000; НД ТЗІ 3.7-001-99; НД ТЗІ 1.1-003-99; НД ТЗІ 2.5-004-99; НД ТЗІ 2.5-005-99) та містити повний опис проектних рішень. Експлуатаційна документація повинна містити опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу АС.

Оформлення документації на КСЗІ здійснюється надавачем послуг у відповідності до вимог чинних нормативних документів сфери ТЗІ.

### 5. ВИМОГИ ДО КСЗІ АС.

КСЗІ АС повинна відповідати вимогам нормативних документів в сфері технічного захисту інформації.

КСЗІ АС повинна забезпечувати:

- реалізацію політики безпеки інформації, прийнятої в АС;
- конфіденційність, цілісність, доступність інформації під час експлуатації АС;
- недопущення витоку інформації з обмеженим доступом та втрати матеріальних носіїв, що містять зазначену інформацію;
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного оповіщення адміністраторів АС про факти несанкціонованого доступу (ознайомлення, модифікації, знищення) до інформації, що обробляється та зберігається в АС;
- ефективне попередження, своєчасне виявлення та знешкодження загроз для ресурсів АС, причин та умов, які спричиняють або можуть привести до порушення її нормального функціонування;
- керування засобами захисту інформації, розмежування доступу користувачів до ресурсів АС, контроль за їх роботою з боку осіб, які відповідають за забезпечення безпеки

інформації в АС;

– створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування АС;

– організацію обліку, зберігання, обігу інформації, яка потребує захисту, та матеріальних носіїв, на яких вона накопичується;

– збір, реєстрацію, зберігання, обробку даних про всі події в АС, які мають відношення до безпеки інформації. Журнал реєстрації повинен містити інформацію, достатню для однозначної ідентифікації робочої станції, користувача, процесу або об'єкта, що мали відношення до кожної зареєстрованої події та мати захист від несанкціонованого доступу, модифікації та руйнування. Адміністратори безпеки повинні мати у своєму розпорядженні засоби перегляду і аналізу журналу реєстрації;

– доступності ресурсів АС для авторизованих користувачів. КСЗІ повинна забезпечувати розмежування доступу користувачів різних категорій до інформації незалежно від способу їх групування.

– стійкість АС до відмов та можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до окремих компонентів АС або до АС в цілому;

– відновлення АС після збоїв програмного або апаратного забезпечення спричинених помилковими діями користувачів, функціональною недостатністю програмного забезпечення, іншими непередбачуваними ситуаціями та повернення її у відомий захищений стан;

– виявлення і реєстрацію фактів порушення цілісності комплексу засобів захисту.

Рівень гарантії реалізації послуг безпеки повинен бути не нижчий, ніж Г2.

### **Розрахунок очікуваної вартості предмета закупівлі методом порівняння ринкових цін.**

**«Послуги зі створення чотирьох комплексних систем захисту інформації в автоматизованих системах класу «1», призначених для обробки інформації, що становить державну таємницю та однієї комплексної системи захисту інформації в автоматизованій системі класу «1», призначеній для обробки службової інформації» (ДК 021:2015:72220000-3 Консультаційні послуги з питань систем та з технічних питань).**

Для аналізу цін використовувалася електронна система закупівель Prozorro. Електронною поштою надіслано не менше 3 (трьох) запитів постачальникам відповідної продукції.

#### **Отриманий масив цінових даних.**

<b>Назва послуги</b>	<b>Учасник 1</b>	<b>Учасник 2</b>	<b>Учасник 3</b>
<b>Комплексна система захисту інформації</b>	<b>92000</b>	<b>117800</b>	<b>109200</b>

(державна таємниця).			
Комплексна система захисту інформації (службова інформація)	59000	67000	68300

Відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої Міністерством розвитку економіки, торгівлі, сільського господарства України від 18.02.2020 №275 очікувана ціна за одиницю, як середньоарифметичне значення масиву отриманих даних, розраховується за такою формулою:

$$Ц_{од} = (Ц_1 + \dots + Ц_k) / K,$$

де:  $Ц_{од}$  - очікувана ціна за одиницю;

$Ц_1, Ц_k$  - ціни, отримані з відкритих джерел інформації, приведені до єдиних умов.

**Комплексна система захисту інформації (державна таємниця).**

Розрахунок.

$$Ц_{од1} = (92000 + 117800 + 109200) / 3 = 106333,33 \text{ грн. Приймаємо} - 106333 \text{ грн.}$$

**Комплексна система захисту інформації (службова інформація).**

Розрахунок.

$$Ц_{од1} = (59000 + 67000 + 68300) / 3 = 64766,66 \text{ грн. Приймаємо} - 64767 \text{ грн.}$$

Очікувана вартість, розрахована методом порівняння ринкових цін за кожною номенклатурою:

$$ОВ_{мрц} = Ц_{од} \times V, \text{ де}$$

$ОВ_{мрц}$  – очікувана вартість, розрахована методом порівняння ринкових цін.

$V$  – кількість товару, що закуповується.

$$ОВ_{1мрц} = 106333 \times 4 \text{ посл.} = 425332 \text{ грн.}$$

$$ОВ_{2мрц} = 64767 \times 1 \text{ посл.} = 64767 \text{ грн.}$$

Очікувана вартість всієї закупівлі:  $425332 + 64767 = 490099$  гривень.

**Приймаємо – очікувана вартість всієї закупівлі 490000 гривень з ПДВ.**