Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі у 2026 році:
(відповідно до пункту 4[1] постанови КМУ від 11.10.2016 № 710 "Про ефективне використання державних коштів")

І. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб:

Державна служба статистики України;
вул. Шота Руставелі, 3, м. Київ, 01601;
код за ЄДРПОУ – 37507880

ІІ. Назва предмета закупівлі:

"ДК 021:2015 "Єдиний закупівельний словник": 72220000-3 – Консультаційні послуги з питань систем та з технічних питань (Послуги з авторизації з безпеки інформаційно-комунікаційної системи органів державної статистики)"

ІІІ. Обґрунтування технічних та якісних характеристик предмета закупівлі:

ТЕХНІЧНІ ВИМОГИ

на послуги: ДК 021:2015 – 72220000-3 – Консультаційні послуги з питань систем та з технічних питань (Послуги з авторизації з безпеки інформаційно-комунікаційної системи органів державної статистики)

1. ЗАГАЛЬНІ ВІДОМОСТІ

Послуги надаються відповідно до Договору.
Замовник – **Державна служба статистики України.** Виконавець – _____.
Планові терміни надання послуг:
Початок надання послуг: з моменту підписання Договору.
Закінчення надання послуг: до 23 грудня 2026 року включно.

1.1. ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

Терміни	Визначення
Держстат	Державна служба статистики України
Замовник	Замовник послуг з авторизації з безпеки інформаційно-комунікаційної системи органів державної статистики
Виконавець	Виконавець робіт з авторизації з безпеки інформаційно-комунікаційної системи органів державної статистики
Держспецзв'язку	Державна служба спеціального зв'язку та захисту інформації України
ІКС ОДС	Інформаційно-комунікаційна система органів державної статистики, яка є сукупністю взаємопов'язаних інформаційно-комунікаційних систем (ІКС), інформаційних ресурсів, програмно-технічних комплексів, комунікаційних мереж, засобів оброблення та захисту статистичної інформації, фізичного й хмарного середовищ, а також персоналу та процесів, що забезпечують функціонування та підтримку інформаційних систем

Авторизація з безпеки ІКС ОДС	Послуги з авторизації з безпеки інформаційно-комунікаційної системи органів державної статистики (ІКС ОДС)
КЗЗ	Комплекс засобів захисту (сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації)
НД	Нормативний документ
НД ТЗІ	Нормативний документ системи технічного захисту інформації
БПБ	базовий профіль безпеки – мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється в інформаційно-комунікаційній системі (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення такої системи
ТЗІ	Технічний захист інформації
КЗІ	Криптографічний захист інформації
Наказ	Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація»
Повідомлення	Повідомлення про включення ІКС до переліку авторизованих
	систем з безпеки, що надсилається Адміністрацією Держспецзв'язку за результатами розгляду авторизаційного листа
ЦПБ	Цільовий профіль безпеки - взаємопов'язана сукупність заходів із захисту інформації, визначених Виконавцем та затверджених Замовником для ІКС з урахуванням мінімальних вимог щодо таких заходів із захисту (БПБ), вимог законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, а також, політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування системи, результатів проведеної оцінки (аналізу) ризиків безпеки

1.2. НОРМАТИВНО-ПРАВОВА БАЗА НАДАННЯ ПОСЛУГ

Під час надання Послуги Виконавець має керуватися вимогами таких нормативно-правових та нормативних документів:

- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;
- Закон України «Про основні засади забезпечення кібербезпеки України»;
- Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури»;
- Постанова КМУ від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;
- Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація»;
- Наказ Адміністрації Держспецзв'язку від 11.07.2025 № 434 «Про затвердження Порядку ведення переліку авторизованих систем з безпеки»;
- Наказ Адміністрації Держспецзв'язку від 17.12.2025 № 836 «Про встановлення вимог

щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власниками або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури»;

- НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
- НД ТЗІ 2.3-025-24 Т1 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем);
- НД ТЗІ 2.3-025-24 Т2 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
- НД ТЗІ 2.3-025-24 Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
- НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем;

Даний список нормативно-правових документів не є вичерпним та може бути уточненим під час виконання робіт з забезпечення авторизації ІКС.

2. ПІДСТАВА ДЛЯ НАДАННЯ ПОСЛУГ

Підставою для надання послуг є Договір.

3. МЕТА НАДАННЯ ПОСЛУГ

Метою авторизації з безпеки ІКС ОДС є створення системи безпеки ІКС ОДС та отримання рішення (повідомлення) щодо можливості її функціонування (експлуатації) з урахуванням відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах ТЗІ та КЗІ, кіберзахисту.

4. ЗАГАЛЬНІ ПОЛОЖЕННЯ

В цьому документі наведені технічні та якісні характеристики, перелік та терміни виконання Послуг з авторизації з безпеки ІКС ОДС.

Виконавець має провести авторизацію з безпеки ІКС ОДС, яка засвідчена повідомленням Адміністрації Держспецзв'язку про включення зазначеної ІКС до переліку авторизованих систем з безпеки.

Усі розроблені документи повинні надаватись у наступних формах:

– один екземпляр (оригінал) – у паперовому вигляді;

– один екземпляр – в електронному вигляді.

5. НАДАННЯ ПОСЛУГИ З РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ БЕЗПЕКИ ІКС ОДС ВКЛЮЧАЄ НАСТУПНІ ПІДЕТАПИ:

Підетап 1 – обстеження середовища функціонування та проведення оцінки ризиків ІКС ОДС з поданням звітних матеріалів.

Виконавцем проводиться аналіз організаційно-розпорядчих документів Замовника і нормативно-правових документів в області захисту інформації, на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначити необхідність забезпечення захисту інформації в ІКС ОДС згідно з іншими критеріями.

При обстеженні середовищ функціонування ІКС ОДС розглядається як організаційно-технічна система, яка за своєю сукупністю поєднує інформаційно-комунікаційні системи (зокрема інформаційні системи обробки статистичної інформації, статистичних реєстрів,

електронної звітності, електронного документообігу, бухгалтерського обліку та фінансової звітності, вебресурси та інші інформаційно-комунікаційні системи), обчислювальну систему, фізичне середовище, хмарне середовище, середовище користувачів, оброблювану статистичну інформацію і технологію її обробки.

Метою обстеження є опис кожного середовища функціонування ІКС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних підетапах авторизації.

Стратегія (політика) управління ризиками визначає загальні принципи, підходи, ролі та процедури управління ризиками інформаційної безпеки в ІКС ОДС, має містити опис методів і критеріїв ідентифікації, оцінки, обробки та моніторингу ризиків, а також політику щодо прийнятного рівня ризику.

Процес оцінки ризику має включати визначення ймовірності і потенційного збитку від виявлених загроз, заходів індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності.

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику, який має включати проведення:

– оцінки ймовірності загроз і вразливостей, які можливі;

– розрахунку впливу, який може мати загроза на кожен актив;

– кількісної або якісної вартості ризику.

Оцінка ризиків має містити системний підхід до визначення кількісно оціненого ризику (аналізування ризику) та процесу його порівняння з критеріями ризику для встановлення його значимості (визначеного стратегією).

Результати обстеження, оцінки ризиків та викладення стратегії (політики) управління ризиками може надаватись у вигляді окремих проєктів документів, або об'єднані в єдиний комплект (документ).

Перелік документів за підетапом 1, що можуть бути оформлені окремо або єдиним комплектом:

– акт обстеження середовищ функціонування;

– актуалізована стратегія (політика) управління ризиками;

– результати оцінки ризиків;

– перелік ІКС із визначенням пріоритетності розроблення та впровадження ЦПБ.

Підетап 2 – розроблення та затвердження для ІКС ЦПБ.

За результатами проведеної оцінки ризиків визначаються відповідні дії та пріоритети з управління ризиками інформаційної безпеки та з впровадження ЦПБ, вибраного для захисту від цих ризиків.

ЦПБ систем розробляється для ІКС, що підлягають авторизації з безпеки, з урахуванням:

– мінімальних вимог щодо таких заходів із захисту БПБ, затвердженого Наказом;

– галузевий профіль безпеки (за наявності);

– вимог законодавства та національних стандартів у сферах КЗІ та ТЗІ, кіберзахисту, нормативних документів системи ТЗІ та КЗІ, кіберзахисту;

– особливостей функціонування ІКС, її призначення та структурно-функціональних характеристик;

– політик безпеки;

– результатів проведеної оцінки (аналізу) ризиків безпеки.

Вхідними даними для формулювання ЦПБ є: БПБ, структура, склад та особливості функціонування ІКС визначені в акті обстеження, стратегія та результати оцінювання ризиків (сформульовані за результатами підетапу 1 послуг), внутрішні політики безпеки.

Під час розроблення ЦПБ Виконавець самостійно обирає національні стандарти у сферах ТЗІ та КЗІ, кіберзахисту, засоби і методи здійснення таких заходів і погоджує їх з Замовником.

Розроблення ЦПБ ІКС здійснюється з урахуванням рекомендацій, затверджених

Адміністрацією Держспецзв'язку та оформлюється окремим документом.

Вибір БПБ здійснюється виходячи з виду інформації за максимальним рівнем обмеження доступу який обробляється в ІКС.

ЦПБ являє собою процедуру налаштування БПБ з метою узгодження заходів захисту з конкретними потребами Замовника та ІКС щодо захисту інформації.

Рішення щодо визначення параметрів заходів захисту під час налаштування мають враховувати різни фактори управління ризиками безпеки, сформульованими за результатами проведення підетапу 1.

Налаштування заходів захисту, формування ЦПБ, має здійснюватися відповідно до окремого змісту (додатків) НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

У якості результату наданих послуг Виконавцем має бути сформульований проєкт документу «ЦПБ створений на основі БПБ для ІКС, де обробляється відкрита або конфіденційна інформація, затвердженого Наказом».

Підетап 3 – впровадження системи безпеки ІКС відповідно до затвердженого ЦПБ.

Авторизація з безпеки систем здійснюється з дотриманням вимог, передбачених частиною 7 статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Після погодження Замовником ЦПБ для ІКС Виконавець має розробити комплект технічної, робочої та експлуатаційної документації на ІКС на його впровадження, в якому надається опис, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься ІКС.

Під час розробки комплекту технічної, робочої та експлуатаційної документації на ІКС обґрунтовуються проектні рішення, які забезпечать можливість реалізувати вимоги ЦПБ, сумісність і взаємодію різних компонентів системи безпеки ІКС, а також різних заходів і способів захисту інформації.

В результаті створюється комплект технічної, робочої та експлуатаційної документації, необхідної для забезпечення авторизації з безпеки ІКС . Перелік та склад зазначеної документації, політик, порядків та інструкцій має відповідати вимогам затвердженого ЦПБ.

Зазначена документація має розроблятися Виконавцем відповідно до вимог НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» та з урахуванням вимог чинних нормативно-правових актів України у сфері захисту інформації та кібербезпеки.

Під час доопрацювання комплекту технічної, робочої та експлуатаційної документації на ІКС Виконавець повинен виконати роботи з модернізації та налагодження КЗЗ на території Замовника, на технологічних площадках де розгорнуто ІКС. У разі неможливості реалізувати вимоги ЦПБ у деяких компонентів системи безпеки ІКС надати Замовнику письмове підтвердження з цього питання Адміністрації Державної служби спеціального зв'язку та захисту інформації України та узгодити з Замовником варіанти виконання вимог ЦПБ.

Мінімальний перелік документів за підетапом 3, включає:

– комплект техноробочого проєкту, що містить:

- пояснювальну записку;
- опис комплексу технічних засобів;
- опис програмного забезпечення;

– перелік експлуатаційної документації, що може бути оформлений за окремими документами або об'єднанні у певні комплекти:

- інструкції адміністративного персоналу;
- інструкція користувача;
- план реагування на інциденти;
- план захисту;

- порядок модернізації ІКС;
- порядок резервування та відновлення інформації в ІКС;
- порядок зберігання записів аудиту;

– політика обміну даними з зовнішніми організаціями і системами;

– проєкт формуляру.

Повний перелік необхідної документації, що розробляється під час впровадження системи безпеки ІКС (підетап 3), визначається Виконавцем і погоджується із Замовником на підетапі 2 послуг (Розроблення та затвердження для ІКС ЦПБ).

Підетап 4 – супроводження процедури оцінювання ІКС на відповідність вимог ЦПБ.

Оцінювання дотримання вимог ЦПБ ІКС – процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації та кіберзахисту системи з метою встановлення стану захищеності систем або їх відповідності вимогам законодавства, національним стандартам, нормативним документам у сферах КЗІ та ТЗІ, кіберзахисту;

Оцінювання дотримання вимог ЦПБ та оформлення його результатів здійснюється юридичними особами, фізичними особами - підприємцями або фізичними особами (далі – Оцінювачами), які відповідають вимогам наказу Адміністрації Держспецзв'язку від 11.07.2025 № 438 «Про затвердження Вимог до юридичних осіб, фізичних осіб-підприємців, які здійснюють оцінювання реалізації ЦПБ інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

Оцінювання дотримання вимог ЦПБ ІКС має здійснюватися з урахуванням наказу Адміністрації Держспецзв'язку від 08.12.2025 № 810 «Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи» та НД ТЗІ 2.3-025-24.

Виконавець в рамках наданої цінової та технічної пропозиції повинен забезпечити супроводження проведення оцінювання ІКС, визначених та узгоджених із Замовником на підетапі 1, на відповідність вимог ЦПБ, який включає наступні заходи:

– аналіз пропозицій та визначення Оцінювача;

– формування листа-рекомендації щодо визначення Оцінювача;

– укладання договору на проведення оцінювання дотримання вимог ЦПБ ІКС із Оцінювачем, за умови погодження його Замовником;

– виправлення помилок та доопрацювання документації ІКС відповідно до висновків та пропозицій Оцінювача.

За результатами оцінювання щодо дотримання вимог цільового профілю ЦПБ Замовник має отримати звіт з оцінювання.

Перелік комплекту документації за підетапом 5 включає:

– лист-рекомендація на визначення (погодження) Оцінювача дотримання вимог ЦПБ;

– документально оформлений звіт з оцінювання дотримання вимог ЦПБ для цілей авторизації з безпеки ІКС.

Підетап 5 – підготовка проєктів авторизаційних листів та супроводження процедури їх розгляду в Адміністрації Держспецзв'язку.

Виконавцем в рамках виконання цього підетапу має бути сформовано проєкти авторизаційних листів для ІКС, що підлягають авторизації з безпеки, відповідно до додатку 1 Постанови КМУ «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» від 18 червня 2025 р. № 712 з метою передачі їх на розгляд Замовнику.

Авторизація з безпеки ІКС ОДС здійснюється на підставі відповідних авторизаційних листів, поданих Замовником до Адміністрації Держспецзв'язку.

У разі включення ІКС до переліку авторизованих систем з безпеки Адміністрацією Держспецзв'язку до Замовника надсилається відповідне повідомлення, що і є кінцевим результатом отримання послуг.

У разі отримання від Адміністрації Держспецзв'язку вимог на доопрацювання із

зазначенням рекомендацій щодо усунення недоліків та невідповідності виявлених під час розгляду авторизаційного листа, Виконавцем надається відповідна консультація / допомога щодо їх усунення.

6. КАЛЕНДАРНИЙ ПЛАН НАДАННЯ ПОСЛУГ

Назва етапу/підетапу	Строк надання послуг	Очікувані результати надання послуг
1. Послуги з авторизації з безпеки ІКС ОДС		
1.1 Обстеження середовища функціонування та проведення оцінки ризиків ІКС ОДС з поданням звітних матеріалів.	30 днів з дати укладання договору	Акт обстеження середовища функціонування
1.2 Розроблення та затвердження для ІКС цільових профілів безпеки (ЦПБ)	40 днів з дати виконання підетапу 1.1	Узгоджений перелік документації, яка має бути розроблена під час надання послуг. Цільові профілі безпеки (ЦПБ)
1.3 Впровадження системи безпеки ІКС відповідно до затверджених ЦПБ	40 днів з дати виконання підетапу 1.2	Акт впровадження системи безпеки ІКС відповідно до затверджених ЦПБ. Пакет технічної, робочої та експлуатаційної документації на ІКС
1.4 Супроводження процедури оцінювання ІКС на відповідність вимогам ЦПБ	30 днів з дати підетапу 1.3	Лист-рекомендація на визначення (погодження) Оцінювача дотримання вимог ЦПБ. Звіт з оцінювання дотримання вимог ЦПБ для цілей авторизації з безпеки ІКС, оформлений в установленому порядку
1.5 Підготовка проєктів авторизаційних листів та супроводження процедури їх розгляду в Адміністрації Держспецзв'язку	не пізніше 23.12.2026	Проєкти авторизаційних листів до Адміністрації Держспецзв'язку. Повідомлення від Адміністрації Держспецзв'язку про включення ІКС ОДС до Переліку авторизованих систем з безпеки. Акт прийняття-передачі послуг.

7. ПОРЯДОК ПРИЙМАННЯ НАДАНИХ ПОСЛУГ

Приймання наданих послуг здійснюється Замовником у відповідності з умовами Договору.

8. ПОРЯДОК ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ ДО ТЕХНІЧНОГО ЗАВДАННЯ

Зміни та доповнення до даного ТЗ вносяться за взаємною згодою Сторін, оформлюються додатками до даного ТЗ та повинні бути погоджені в тому ж порядку, що і основний документ.

9. ПОРЯДОК НАДАННЯ ПОСЛУГ

Порядок та строки надання послуг визначаються умовами Договору.

IV. Обґрунтування розміру бюджетного призначення, очікуваної вартості предмета закупівлі:

Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених для Державної служби статистики Кошторисом на 2026 рік для апарату Держстату за бюджетною програмою КПКВК 0414010 "Керівництво та управління у сфері статистики" по КЕКВ 2240 "Оплата послуг (крім комунальних)" відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року № 275, за методом порівняння ринкових цін на закупівлі, що розміщені на порталі електронної системи закупівель https://prozorro.gov.ua/ .

З метою визначення очікуваної вартості закупівлі послуг із авторизації з безпеки інформаційно-комунікаційних систем Державної служби статистики України проведено аналіз відповідних закупівель, розміщених на порталі електронної системи закупівель https://prozorro.gov.ua/ . При розгляді закупівель враховувались пропозиції тих замовників, які мають подібні з Держстатом потреби та організаційну структуру.

Так, закупівлі послуг із авторизації з безпеки інформаційно-комунікаційних систем у 2026 році здійснювали такі замовники:

- Державна казначейська служба України: Послуги з авторизації з безпеки інформаційно-комунікаційних систем Державної казначейської служби України за кодом ДК 021:2015: 72220000-3 – Консультаційні послуги з питань систем та з технічних питань (https://prozorro.gov.ua/uk/tender/UA-2026-04-13-007257-a) – 1 121 500,00 грн;
- Антимонопольний комітет України: Послуги з побудови системи безпеки ІКС для авторизації безпеки автоматизованої системи класу 3 за кодом ДК 021:2015: 72220000-3 — Консультаційні послуги з питань систем та з технічних питань (https://prozorro.gov.ua/uk/tender/UA-2026-06-03-006936-a) – 1 150 985,00 грн;
- Державна податкова служба України: Послуга з проведення авторизації з безпеки інформаційно-комунікаційної системи "Е-аудит" за кодом ДК 021:2015: 72220000-3 – Консультаційні послуги з питань систем та з технічних питань (https://prozorro.gov.ua/uk/tender/UA-2026-05-28-009769-a) – 1 200 000,00 грн.

Так, було визначено очікувану ціну аналогічних послуг, як середньоарифметичне значення масиву отриманих даних, що розраховується за такою формулою:

Цод = (Ц1 +… + Цк) / К,

де: **Цод** - очікувана ціна аналогічних послуг;
Ц1, Цк - ціни аналогічних послуг;
К - кількість цін, отриманих з відкритих джерел інформації.

1 157 500,02 ≈ 1 157 495 грн = (1 121 500,00 + 1 150 985,00 + 1 200 000,00) / 3

Заступник директора департаменту
інформаційних технологій Олександра ДОРОХОВА