ВИКОНАВЧИЙ КОМІТЕТ ПІВДЕННІВСЬКОЇ МІСЬКОЇ РАДИ
ОДЕСЬКОГО РАЙОНУ ОДЕСЬКОЇ ОБЛАСТІ

ОБҐРУНТУВАННЯ

технічних та якісних характеристик ***закупівлі «Інформаційно-консультаційні послуги з підготовки проектів нормативних документів з питань цифровізації та створення авторизованої системи безпеки інформації»,*** *розміру бюджетного призначення, очікуваної вартості предмета закупівлі – (оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))*

Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія:

Виконавчий комітет Південнівської міської ради Одеського району Одеської області, 65481, Одеська область, Одеський район, м. Південне, проспект Григорівського десанту, 18, категорія замовника - юридична особа, яка забезпечує потреби держави або територіальної громади .

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 й частин предмета закупівлі (лотів) (за наявності): «Інформаційно-консультаційні послуги з підготовки проектів нормативних документів з питань цифровізації та створення авторизованої системи безпеки інформації» (ДК 021:2015 "Єдиний закупівельний словник" - 72220000-3 Консультаційні послуги з питань систем та з технічних питань)»

Вид процедури закупівлі: Відкриті торги з особливостями

Ідентифікатор процедури закупівлі: UA-2026-05-25-011944-a

Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі:

402 000,00 (чотириста дві тисяч гривень 00 копійок)

Міністерством розвитку економіки, торгівлі та сільського господарства України затверджена примірна методика визначення очікуваної вартості предмета закупівлі від 18.02.2020 No275, якою передбачені методи визначення очікуваної вартості предмета закупівлі, а саме: 1) здійснення пошуку, збору та аналіз загальнодоступної інформації про ціну товару (тобто інформація про ціни, що містяться в мережі інтернет у відкритому доступі, спеціалізованих торгівельних майданчиках, в електронних каталогах, в електронній системі закупівель «Прозоро», тощо; 2) отримання комерційних (цінових) пропозицій від виробників, офіційних представників (дилерів), постачальників; 3) у разі обмеження конкуренції на ринку певних товарів та враховуючи їх специфіку при розрахунку використовуються ціни попередніх закупівель аналогічного товару та/або минулих періодів (з урахуванням індексу інфляції, зміни курсів іноземних валют).
Відповідно до вказаної методики розрахунок очікуваної вартості здійснювався методом порівняння ринкових цін, а саме: здійснено пошук, збір та аналіз інформації про ціну Послуги, що міститься у мережі Інтернет у відкритому доступі, у тому числі каталогів з переліком Послуг на сайтах виробників. Крім цього, був проведений аналіз закупівель аналогічних Послуг через офіційний портал оприлюднення інформації про публічні закупівлі України «ProZorro». Також враховувався Річний план закупівель на 2026 рік та кошторис на 2026 рік.

Розмір бюджетного призначення: 402 000,00 грн згідно з потребою на 2026 рік.

Обґрунтування технічних та якісних характеристик предмета закупівлі. Термін постачання по 31.12.2026 року.

ТЕХНІЧНІ ВИМОГИ ДО ПРЕДМЕТА ЗАКУПІВЛІ,
СПЕЦИФІКАЦІЯ НА ЗАКУПІВЛЮ

Невиконання вимог цього розділу ТД у тендерній пропозиції Учасника призводить до її відхилення.

Розділ І. Опис предмету закупівлі:

Найменування предмета закупівлі:	72220000-3 – Консультаційні послуги з питань систем та з технічних питань
Вид предмета закупівлі:	Послуга
Кількість, обсяг надання послуг:	Інформаційно-консультаційні послуги з підготовки проектів нормативних документів з питань цифровізації та створення авторизованої системи безпеки інформації (одна послуга)
Місце надання Послуг:	Україна, Одеська обл., м. Південне, пр-т. Григорівського десанту, 18.
Термін надання Послуг:	з дати укладання Договору до 31.12.2026 включно
Очікувана вартість:	402 000,00 грн. з ПДВ

Розділ ІІ. Порядок підготовки проєктів організаційних документів з питань цифровізації Південнівської міської ради

З метою підвищення рівня цифровізації Південнівської міської ради, розширення переліку цифрових послуг та створення належних умов для обробки інформації, вимога щодо захисту якої встановлена законом, передбачається надання консультативних послуг з впровадження Цифрової платформи Південнівської міської ради. Зазначені заходи спрямовані на створення (модернізацію) інформаційно-комунікаційної системи Південнівської міської ради (далі - ІКС), впровадження заходів захисту у відповідності до вимог законодавства України й кращих міжнародних практик у сфері захисту інформації та кіберзахисту.

При виконанні робіт повинні виконуватись обов'язкові вимоги щодо створення, адміністрування та функціонування засобів інформатизації в державному секторі, що передбачає певну стадійність робіт та обов’язковість розроблення техніко-експлуатаційної документації відповідно до законодавства України.

Підготовка проєктів організаційних документів з питань цифровізації Південнівської міської ради здійснюється такими етапами:

- Розробка концепції розвитку Цифрової платформи.
- Розробка Положення про Цифрову платформу.
- Розробка Технічних вимог до Цифрової платформи.
- Розробка Генеральної схеми організації Цифрової платформи.
- Розробка Структурної схеми організації Цифрової платформи.
- Розробка технічного завдання для ІКС.

Розділ ІІІ. Порядок запровадження заходів захисту ІКС та оцінювання дотримання вимог цільового профілю безпеки

3.1. Запровадження заходів захисту з безпеки ІКС проводиться з метою створення належних умов для функціонування системи з урахуванням відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного, криптографічного захисту інформації та кіберзахисту. В ІКС передбачається обробка державних інформаційних ресурсів та взаємодія з публічними електронними реєстрами.

Запровадження заходів захисту з безпеки ІКС це сукупність необхідних організаційних та технічних заходів, засобів і методів технічного захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікацій у ІКС.

Найвищий ступінь обмеження доступу до інформації, яка циркулюватиме в ІКС та підлягатиме захисту - конфіденційна інформація (персональні дані).

За порядком доступу інформація, яка циркулюватиме в зазначеній ІКС, поділяється:

– відкрита інформація (підлягає захисту в частині збереження її цілісності, автентичності, доступності);

– конфіденційна інформація (персональні дані, підлягають захисту в частині збереження їх конфіденційності, цілісності, доступності);

– технологічна інформація (призначена для використання уповноваженими користувачами з числа адміністраторів ІКС, підлягає захисту в частині збереження її конфіденційності, цілісності, доступності).

3.2. Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об'єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, мають оброблятися в авторизованих системах з безпеки.

Базовий профіль безпеки системи (далі - базовий профіль, БПБ) - мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення такої системи.

Цільовий профіль безпеки системи (далі - цільовий профіль, ЦПБ) - взаємопов'язана сукупність заходів із захисту інформації, визначених органами державної влади, іншими державними органами, державними підприємствами, установами та організаціями, органами місцевого самоврядування (далі - власник або розпорядник системи) для відповідних систем з урахуванням мінімальних вимог щодо таких заходів із захисту (базового або галузевого профілю), вимог законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, а також галузевого профілю (за наявності), політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування системи, результатів проведеної оцінки (аналізу) ризиків безпеки.

Оцінювання дотримання вимог цільових профілів безпеки системи - 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 криптографічного та технічного захисту інформації, кіберзахисту.

Первинна авторизація з безпеки системи є основним видом авторизації та здійснюється з метою початку функціонування (експлуатації) системи.

Підставою для подання системи на первинну авторизацію з безпеки системи є позитивні результати оцінювання дотримання вимог цільового профілю.

Авторизація з безпеки системи, в яких обробляється інформація, що не становить державну таємницю, здійснюється на підставі авторизаційного листа, поданого власником або розпорядником такої системи до Адміністрації Держспецзв'язку.

За результатами включення системи до переліку авторизованих систем з безпеки Адміністрація Держспецзв'язку протягом п'яти робочих днів з дня включення надсилає власнику або розпоряднику системи повідомлення.

Запровадження заходів захисту ІКС та оцінювання дотримання вимог ЦПБ здійснюється такими етапами:

- підготовка організаційно-розпорядчої документації;
- визначення стратегії оцінки ризиків інформаційної безпеки;
- обстеження середовища функціонування ІКС;
- розробка та затвердження ЦПБ ІКС відповідно до базового профілю безпеки та результатів оцінки ризиків;
- впровадження заходів щодо ІКС відповідно до ЦПБ;
- оцінювання дотримання вимог ЦПБ;
- надання рекомендацій з формування авторизаційного листа про проведення авторизації з безпеки до Адміністрації Держспецзв'язку.

3.3. Мають бути надані наступні послуги, в рамках запровадження заходів захисту ІКС та оцінювання дотримання вимог ЦПБ ІКС за адресою: Україна, Одеська обл., м. Південне, пр-т. Григорівського десанту, 18:

- розробка та надання Замовнику на затвердження для системи ЦПБ відповідно до обраного базового

профілю безпеки та результатів оцінки ризику;

- супроводження впровадження заходів щодо ІКС відповідно до ЦПБ;
- організація оцінювання реалізації цільового профілю безпеки;
- надання рекомендацій з формування авторизаційного листа про проведення авторизації з безпеки до Адміністрації Держспецзв'язку.

3.4. Обстеження середовища функціонування та проведення оцінки ризиків ІКС передбачає 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 визначатися необхідність забезпечення захисту інформації в ІКС згідно з іншими критеріями.

При обстеженні середовищ функціонування ІКС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану 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 етапах запровадження заходів захисту.

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

Процес оцінки ризику включає 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. Вона включає в себе:

– оцінку ймовірності загроз і вразливостей, які можливі;
– розрахунок впливу, який може мати загроза на кожен актив;
– визначення 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 управління ризиками може надаватись у вигляді окремих документів, або об'єднані в єдиний комплект (документ).

Перелік документів за результатами обстеження та оцінки ризиків, що можуть бути оформлені окремо або єдиним комплектом:

– акт обстеження середовищ функціонування;
– стратегія управління ризиками;
– результати оцінки ризиками.

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

ЦПБ розробляється для ІКС, що підлягає авторизації з безпеки, 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;
– особливостей функціонування ІКС, її призначення та структурно-функціональних характеристик;
– політик безпеки;
– результатів проведеної оцінки (аналізу) ризиків безпеки.

Вхідними даними для формування ЦПБ є: БПБ, структура, склад та особливості функціонування ІКС, визначені в акті обстеження, стратегія та результати оцінювання ризиків, внутрішні політики або безпеки.

Під час розроблення ЦПБ надавач послуг з запровадження заходів захисту ІКС та оцінювання

дотримання вимог цільового профілю безпеки (далі - Виконавець) здійснює вибір національних стандартів у сферах технічного та криптографічного захисту інформації, кіберзахисту, засобів і методів здійснення таких заходів, погоджуючи їх із Замовником.

Розроблення ЦПБ системи здійснюється з урахуванням рекомендацій, затверджених наказом Адміністрації Держспецзв'язку від 08.12.2025 № 811, 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 особливостями функціонування ІКС щодо захисту інформації.

Рішення щодо визначення параметрів заходів захисту під час налаштування мають враховувати різні фактори управління ризиками безпеки, сформованими за результатами проведення обстеження середовища функціонування ІКС.

Налаштування заходів захисту та формування ЦПБ має здійснюватися відповідно до 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 сформований проєкт документу ЦПБ, створений на основі відповідного БПБ.

3.6. Впровадження заходів захисту ІКС відповідно до затвердженого ЦПБ здійснюється з дотриманням вимог, передбачених частиною 7 статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Після затвердження Замовником ЦПБ ІКС Виконавець має розробити комплект технічної, робочої та експлуатаційної документації на ІКС для забезпечення належного рівня захисту інформації.

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 засобів захисту на території Замовника, де розгорнуто ІКС. У разі неможливості реалізувати вимоги ЦПБ у деяких компонентів системи безпеки ІКС Виконавець повинен надати Замовнику письмове підтвердження з цього питання та узгодити з Замовником варіанти виконання окремих вимог ЦПБ.

Мінімальний перелік документів щодо впровадження заходів захисту включає:

– комплект техніко-експлуатаційної документації, що містить:
  - 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.
– відповідні політики безпеки, які визначені в ЦПБ системи.

Повний перелік необхідної документації, що розробляється під час впровадження системи безпеки ІКС, визначається Виконавцем і погоджується із Замовником на етапі розроблення та затвердження ЦПБ ІКС.

3.7. Оцінювання дотримання вимог цільового профілю здійснюється юридичними особами, фізичними особами - підприємцями або фізичними особами, вимоги до яких затверджуються

Адміністрацією Держспецзв'язку відповідно до законодавства та з урахуванням особливостей, встановлених цим Порядком авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем.

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 криптографічного та технічного захисту інформації, кіберзахисту.

Оцінювання дотримання вимог ЦПБ та оформлення його результатів здійснюється юридичними особами, фізичними особами - підприємцями або фізичними особами (далі - Оцінювач), 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 цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

Оцінювання дотримання вимог цільового профілю 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.

Відповідно до наказу Адміністрації Держспецзв'язку від 08.12.2025 за №810 "Про затвердження рекомендацій з дотримання вимог цільового профілю безпеки системи" заходи щодо організації та проведення оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки проводяться з дотриманням таких принципів:

незалежність: оцінювачі та організації, що проводять оцінювання, діють незалежно від будь-яких осіб чи обставин, здатних вплинути на об'єктивність оцінювання. Незалежність є ключовою умовою забезпечення достовірності висновків і збереження довіри до результатів оцінювання;

неупередженість у прийнятті рішень: рішення та висновки оцінювання формуються виключно на підставі перевірених доказів. Жоден оцінювач не може допускати впливу особистих інтересів, тиску з боку керівництва, клієнта або третіх осіб;

відсутність конфлікту інтересів: оцінювання не може проводити організація, яка володіє або розпоряджується об'єктом оцінювання або брала участь у його створенні, щоб уникнути будь-якого конфлікту інтересів і забезпечити повну незалежність оцінювання;

об'єктивність доказів: висновки базуються лише на перевірених і задокументованих фактах, отриманих шляхом дослідження, опитування, випробування;

прозорість процесу: усі етапи оцінювання, критерії оцінки, методи та рішення документуються та є доступними для зацікавлених сторін у межах встановлених правил конфіденційності;

Відповідальність оцінювача: кожен оцінювач несе персональну відповідальність за дотримання принципів незалежності, професійної етики та об'єктивності.

Виконавець в пропозиції надає довідку про залучення Оцінювача (співвиконавця) щодо дотримання вимог ЦПБ ІКС, яка містить інформацію про Оцінювача (співвиконавця), а саме:

повне найменування;

юридична адреса;

поштова або фактична адреса;

код ЄДРПОУ підприємства (або ІПН ФОП);

банківські реквізити (поточний рахунок, назва банку, в якому відкритий рахунок та МФО);

тел./факс;

e-mail;

посада керівника підприємства та П.І.Б. (для ФОП зазначається П.І.Б);

копію документа, передбаченого пунктом 3 вимог до юридичних осіб, фізичних осіб – підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних, комунікаційних, інформаційно-комунікаційних, технологічних систем, затверджених наказом Адміністрації Держспецзв'язку від 11.07.2025 № 438, зареєстрованим в Міністерстві юстиції України 31.07.2025 за № 1125/44531.

Виконавець в рамках надання послуг повинен забезпечити супроводження проведення оцінювання ІКС на відповідність вимог ЦПБ, яке включає виправлення недоліків (зауважень) та доопрацювання документації ІКС відповідно до висновків та пропозицій Оцінювача.

За результатами оцінювання щодо дотримання вимог ЦПБ ІКС Замовник має отримати

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

3.8. Виконавцем в рамках надання рекомендацій має бути сформовано проєкт авторизаційного листа, що відповідає додатку 1 постанови Кабінету Міністрів України від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» з метою передачі його на розгляд Замовнику.

Авторизація з безпеки ІКС здійснюється на підставі авторизаційного листа, поданого 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 невідповідностей, виявлених під час розгляду авторизаційного листа, Виконавцем надається відповідна консультація/допомога щодо їх усунення.

3.9. Порядок захисту інформації в ІКС має регламентуватися такими нормативно-правовими актами та нормативними документами:

- 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 доступ до публічної інформації»;
- Закон України «Про електронні комунікації»;
- постанова Кабінету Міністрів України від 18.07.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;
- постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;
- наказ Адміністрації Держспецзв'язку від 08.12.2025 № 811 «Про затвердження Рекомендацій з розроблення цільового профілю безпеки системи»;
- наказ Адміністрації Держспецзв'язку від 08.12.2025 № 810 «Про затвердження Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи»;
- ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення, затверджено наказом Держстандарту України від 09.09.1993 № 126;
- ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення, затверджено наказом Держстандарту України від 11.10.1996 року № 423;
- ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення, затверджено наказом Держстандарту України від 11.04.1997 № 200;
- 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.

Даний список нормативно-правових документів не є вичерпним та може бути уточненим під час виконання робіт з запровадження заходів захисту ІКС та оцінювання дотримання вимог цільового профілю безпеки.

Розділ IV. Календарний план надання послуг

Календарний план надання послуг наведено в таблиці

№	Товари (роботи, послуги)	Термін виконання	ПРИМІТКИ
1	Розробка концепції розвитку Цифрової платформи	20 днів	від дати підписання Договору
2	Погодження та внесення пропозицій Замовником до концепції розвитку Цифрової платформи	3 днів	від дати надання проєкту концепції
3	Затвердження Замовником концепції розвитку Цифрової платформи	2 днів	від дати погодження концепції
4	Розробка Положення про Цифрову платформу	10 днів	від дати затвердження концепції
5	Погодження та внесення пропозицій Замовником до Положення про Цифрову платформу	3 днів	від дати надання проєкту Положення
6	Затвердження Положення про Цифрову платформу	2 днів	від дати погодження Положення
7	Розробка Технічних вимог до Цифрової платформи	10 днів	від дати затвердження Положення
8	Погодження та внесення пропозицій Замовником до Технічних вимог до Цифрової платформи	3 днів	від дати надання проєкту Технічних вимог
9	Затвердження Технічних вимог до Цифрової платформи	2 днів	від дати погодження Технічних вимог
10	Розробка Генеральної схеми організації Цифрової платформи	5 днів	від дати затвердження Положення
11	Погодження та внесення пропозицій Замовником до Генеральної схеми організації Цифрової платформи	2 дні	від дати надання проєкту Генеральної схеми
12	Затвердження Генеральної схеми організації Цифрової платформи	2 дні	від дати погодження Генеральної схеми
13	Розробка Структурної схеми організації Цифрової платформи	5 днів	від дати затвердження Положення
14	Погодження та внесення пропозицій Замовником до Структурної схеми організації Цифрової платформи	2 дні	від дати надання проєкту Структурної схеми
15	Затвердження Структурної схеми організації Цифрової платформи	2 дні	від дати погодження Структурної схеми
16	Розробка Технічного завдання для ІКС	10 днів	Від дати затвердження Технічних вимог
17	Погодження та внесення пропозицій Замовником до Технічного завдання на ІКС	5 днів	від дати надання проєкту Технічного завдання на ІКС
18	Затвердження Технічного завдання на ІКС	5 днів	від дати погодження Технічного завдання на ІКС
19	Підготовка організаційно-розпорядчої документації	10 днів	від дати затвердження Технічного завдання на ІКС
20	Обстеження середовища функціонування ІКС	5 днів	Від дати наказу щодо створення (модернізації) ІКС
21	Розробка та затвердження для ІКС цільового профілю безпеки відповідно до базового профілю безпеки	10 днів	Від дати обстеження ІКС та результатів оцінки ризиків
22	Впровадження заходів щодо ІКС відповідно до цільового профілю безпеки	30 днів	Від дати затвердження цільового профіля безпеки
23	Оцінювання дотримання вимог цільового профілю	20 днів	Від дати закінчення робіт щодо впровадження заходів захисту

24	Супроводження оформлення та надання Адміністрації Держспецзв'язку авторизаційного листа	1 день	Від дати отримання звіту з оцінювання дотримання вимог цільового профілю

Супровідні послуги (консультації, технічна підтримка) надаються Виконавцем протягом всього терміну надання послуг.