Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

Послуги з налаштування та впровадження засобів захисту інформації та кібербезпеки
(відповідно до пункту 4-1 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

1. Замовник: Державна установа «Центр обробки статистичних даних», код ЄДРПОУ 45101912, адреса: вул. Еспланадна 4-6, м. Київ, 01601.

2. Процедура закупівлі: відкриті торги (з особливостями).

3. Ідентифікатор закупівлі: UA-2026-10-27-007077-a
Ідентифікатор плану закупівлі: UA-P-2026-10-27-007822-a

4. 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 з налаштування та впровадження засобів захисту інформації та кібербезпеки, код ДК 021:2015: 72220000-3 Консультаційні послуги з питань систем та з технічних питань.

5. Обґрунтування технічних та якісних характеристик предмета закупівлі:

1. ЗАГАЛЬНІ ВІДОМОСТІ

Послуги надаються відповідно до Договору.
Замовник – Державна установа «Центр обробки статистичних даних»
Кількість співробітників з ліцензіями Microsoft 365 – до 1000.
Плановий строк надання послуг:
з моменту підписання Договору до 23 грудня 2026 року включно.
Послуги виконуються у середовищі Microsoft 365 Замовника та мають бути спрямовані на підвищення рівня захищеності облікових записів, пристроїв, застосунків, електронної пошти та корпоративних даних.

1.1. ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

Термін	Визначення
Microsoft 365	Хмарне середовище Замовника, у якому використовуються Microsoft 365 та пов’язані служби.
Microsoft Entra ID	Служба керування ідентичностями та доступом.
Intune	Microsoft Intune – служба керування пристроями, застосунками та політиками безпеки.
Conditional Access	Механізм Microsoft Entra ID для визначення умов і правил доступу до корпоративних ресурсів.
BYOD	Використання особистих пристроїв для доступу до корпоративних ресурсів.
DLP	Data Loss Prevention – засоби запобігання витоку даних.
Цільова конфігурація	Узгоджений із Замовником стан налаштувань засобів безпеки Microsoft 365,

	який має бути досягнутий за результатами послуг.
Пілотна група	Визначена Замовником група користувачів та пристроїв для первинного впровадження політик.

Інші терміни та скорочення визначаються відповідно до термінології програмного продукту Microsoft 365 Technical documentation | Microsoft Learn

1.2. НОРМАТИВНО-ПРАВОВА ТА МЕТОДИЧНА БАЗА

Під час надання послуг Виконавець має керуватися чинними нормативно-правовими актами України у сферах захисту інформації та кібербезпеки, внутрішніми документами Замовника, що стосуються інформаційної безпеки, а також актуальними рекомендаціями та технічною документацією Microsoft щодо Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender та Microsoft Purview.

Закон України «Про інформацію»;
Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
Закон України «Про основні засади забезпечення кібербезпеки України»;
постанова Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» – у частині, що застосовується до предмета послуг;
внутрішні політики та нормативні документи Замовника у сфері інформаційної безпеки та кіберзахисту.
Зазначений перелік не є вичерпним та може уточнюватися у разі набрання чинності новими нормативними документами.

2. МЕТА НАДАННЯ ПОСЛУГ

Мета послуг - підвищення рівня захищеності середовища Microsoft 365 E3 шляхом проведення аудиту поточного стану, розроблення цільової конфігурації, налаштування та впровадження засобів керування ідентичностями, доступом, пристроями, застосунками та даними, а також передачі Замовнику комплекту документації та знань для подальшої експлуатації.

Під час виконання послуг Виконавець має застосовувати принципи Zero Trust у межах функціональних можливостей та ліцензій, наявних у Замовника. Microsoft рекомендує для Microsoft 365 E3/E5 відповідні конфігурації ідентичності та доступу із застосуванням Entra ID, Conditional Access та Intune.

3. ОБСЯГ ПОСЛУГ

Послуги мають включати щонайменше такі етапи:

Обстеження та аудит поточного стану середовища Microsoft 365.
Розроблення цільової конфігурації безпеки.
Налаштування засобів ідентичності та доступу.
Налаштування Microsoft Intune та політик безпеки пристроїв.
Налаштування BYOD та захисту мобільних пристроїв
Налаштування безпеки електронної пошти та спільної роботи.
Налаштування захисту корпоративних даних і DLP.
Пілотне впровадження та перевірка політик. Масове впровадження погоджених налаштувань
Підготовка документації, навчання та передача результатів Замовнику.

4. ЕТАП 1. ОБСТЕЖЕННЯ ТА АУДИТ

Виконавець має провести комплексне обстеження середовища Microsoft 365 та підготувати звіт про його поточний стан.

аудит Microsoft 365 тенанту та формування початкового стану;
аналіз призначених користувачам ліцензій і доступних сервісних планів;

інвентаризація користувачів, груп, адміністративних ролей та привілейованих облікових записів;
аналіз способів автентифікації та використання MFA;
аналіз застарілих типів автентифікації та визначення можливостей їх блокування;
аудит існуючих Conditional Access політик;
аудит Microsoft Intune, зареєстрованих пристроїв та наявних політик;
аналіз конфігурації Windows-пристроїв, BitLocker, Defender Antivirus, firewall та security baselines;
аналіз існуючих GPO та визначення політик, які можуть бути перенесені до Intune;
аналіз мобільних пристроїв та сценаріїв BYOD;
аналіз SharePoint Online, OneDrive та зовнішнього спільного доступу;
аналіз налаштувань Exchange Online та механізмів захисту електронної пошти;
аналіз доступних засобів Microsoft Purview та DLP;
визначення винятків, конфліктів політик та інших ризиків.
Результат: звіт про поточний стан, перелік виявлених ризиків та рекомендації з пріоритетами.

5. ЕТАП 2. РОЗРОБЛЕННЯ ЦІЛЬОВОЇ КОНФІГУРАЦІЇ

Виконавець на підставі результатів обстеження розробляє та погоджує із Замовником цільову конфігурацію.

цільова модель ідентичності та доступу;
матриця Conditional Access policies;
цільова модель груп та адміністративних ролей;
цільова модель керування пристроями через Intune;
перелік Security Baselines та Endpoint Security policies;
цільові вимоги до відповідності пристроїв (Compliance Policies);
цільова модель BYOD та App Protection Policies;
цільові налаштування захисту електронної пошти;
цільові налаштування спільного доступу SharePoint/OneDrive;
цільова модель DLP та захисту інформації;
мінімальні вимоги до пристроїв, операційних систем та параметрів конфігурації зовнішніх служб та компонентів;
план пілотного і масового впровадження.

Рішення мають враховувати фактично доступні Замовнику ліцензії рівня не нижче M365 E3. Функціональність, яка потребує окремої ліцензії або додаткового продукту, не повинна вважатися обов’язковим результатом, якщо така ліцензія не входить до предмета закупівлі.

6. ЕТАП 3. ІДЕНТИЧНІСТЬ ТА КЕРУВАННЯ ДОСТУПОМ

Етап передбачає налаштування та впровадження механізмів управління ідентичністю та доступом, зокрема багатофакторної автентифікації (MFA), політик умовного доступу (Conditional Access), груп Microsoft Entra ID, реєстрації та управління пристроями в Microsoft Intune, самообслуговування щодо відновлення пароля (SSPR) та політик захисту паролів Microsoft Entra Password Protection, а саме:
налаштування та оптимізація MFA;
налаштування Authentication Methods;
розроблення та впровадження Conditional Access;
блокування застарілих типів автентифікації, де це технічно можливо та погоджено;
застосування вимог до compliant devices для доступу до визначених ресурсів;
окремі правила захисту привілейованих облікових записів;
захист emergency/break-glass accounts;
налаштування SSPR;
налаштування Microsoft Entra Password Protection;
перевірка та обмеження адміністративних ролей за принципом найменших привілеїв;

перевірка сторонніх застосунків та процесів надання їм дозволів.

7. ЕТАП 4. MICROSOFT INTUNE ТА ЗАХИСТ КОРПОРАТИВНИХ ПРИСТРОЇВ

Етап передбачає налаштування та впровадження політик щодо кінцевих пристроїв:

налаштування Microsoft Intune;
налаштування device enrollment;
налаштування Device Compliance Policies;
налаштування Configuration Profiles;
налаштування Security Baselines;
налаштування Endpoint Security Policies;
налаштування BitLocker;
налаштування Microsoft Defender Antivirus;
налаштування Windows Firewall;
налаштування Attack Surface Reduction у погодженому режимі;
налаштування Windows LAPS;
налаштування контролю оновлень операційної системи;
налаштування вимог до Secure Boot, TPM та інших параметрів відповідності, де підтримується.

Налаштування політик Intune має враховувати аналіз та перенесення налаштувань безпеки та частини Group Policy.

8. ЕТАП 5. BYOD ТА ЗАХИСТ МОБІЛЬНИХ ПРИСТРОЇВ

Етап передбачає налаштування та впровадження політик щодо мобільних пристроїв:

налаштування Intune App Protection Policies для підтримуваних застосунків;
застосування вимоги використання захищених корпоративних застосунків;
обмеження copy/paste між корпоративними та некерованими застосунками;
обмеження збереження корпоративних даних у персональне сховище;
застосування PIN/біометричної автентифікації для корпоративних даних;
налаштування selective wipe для корпоративних даних у підтримуваних сценаріях;
визначення мінімальних підтримуваних версій ОС та застосунків.

9. ЕТАП 6. ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ ТА СПІЛЬНОЇ РОБОТИ

Етап передбачає налаштування та впровадження політик щодо електронної пошти:

аудит та оптимізація антиспам-політик;
налаштування anti-phishing та захисту від spoofing у межах доступної функціональності;
налаштування політик Safe Links/Safe Attachments;
налаштування карантину та правил його оброблення;
аналіз та налаштування SPF, DKIM і DMARC;
обмеження небезпечного автоматичного пересилання;
аудит зовнішнього спільного доступу SharePoint та OneDrive;
налаштування погоджених обмежень зовнішнього доступу.

10. ЕТАП 7. ЗАХИСТ ДАНИХ ТА DLP

аналіз доступних можливостей Microsoft Purview;
розроблення/налаштування sensitivity labels у межах погодженої Замовником моделі класифікації;
налаштування DLP для Exchange Online, SharePoint Online та OneDrive у межах доступної ліцензії;
визначення правил виявлення та запобігання передачі визначених категорій даних;
налаштування режиму audit/test перед переходом до блокування, якщо це погоджено Замовником;
формування звітності про спрацювання DLP.

Модель класифікації інформації, назви категорій та строки зберігання інформації визначаються Замовником. Виконавець не має права самостійно змінювати правила доступу до інформації без узгодження із Замовником.

11. ЕТАП 8. ПІЛОТНЕ ТА ПРОМИСЛОВЕ ВПРОВАДЖЕННЯ

До початку промислового впровадження Виконавець має виконати пілотне впровадження на погодженій Замовником групі, а саме виконати на цьому етапі наступні роботи:

визначення пілотної групи;
застосування погоджених політик;
перевірка доступу до Microsoft 365;
перевірка MFA та Conditional Access;
перевірка compliance;
перевірка BitLocker та засобів захисту кінцевих точок;
перевірка роботи корпоративних застосунків;
виявлення та усунення конфліктів;
оформлення протоколу результатів пілоту;
після погодження Замовником результатів пілотного впровадження – масове впровадження.

12. ЕТАП 9. ДОКУМЕНТАЦІЯ ТА НАВЧАННЯ

За результатами послуг Виконавець має передати Замовнику:

звіт про початковий стан;
цільову конфігурацію безпеки Microsoft 365;
опис налаштованих Conditional Access policies;
опис Intune policies та Security Baselines;
опис політик захисту даних та DLP;
опис налаштувань електронної пошти;
перелік винятків та погоджених виключень;
схему архітектури налаштованих засобів безпеки;
опис регламентних робіт з описом відповідних ролей;
рекомендації щодо подальшого розвитку.

Також має бути проведено навчання адміністраторів/служби підтримки щодо експлуатації налаштованих засобів та передано базу знань по типовим зверненням користувачів, що буде напрацьована за час надання послуг.

13. ВИМОГИ ДО РЕЗУЛЬТАТІВ ПОСЛУГ

Усі налаштування виконуються у погодженому з Замовником режимі та документуються Виконавцем.

Зміни, що можуть вплинути на доступність або роботу користувачів, спочатку тестуються на пілотній групі.

Усі винятки з політик документуються із зазначенням підстави та строку перегляду.

Після впровадження Виконавцем разом із Замовником проводиться контрольна перевірка відповідності погодженій цільовій конфігурації.

Замовнику передаються необхідні адміністративні та експлуатаційні матеріали.

14. КАЛЕНДАРНИЙ ПЛАН НАДАННЯ ПОСЛУГ

Етап	**Строк**	**Очікуваний результат**
1. Обстеження та аудит	до 7 робочих днів	Звіт про поточний стан, ризики та рекомендації
2. Розроблення цільової конфігурації	до 10 робочих днів	Погоджена цільова конфігурація та план впровадження
3. Налаштування ідентичності та доступу	до 10 робочих днів	Налаштовані Entra ID, MFA, Conditional Access та пов’язані політики
4. Intune та захист пристроїв	до 15 робочих днів	Налаштовані політики Intune та захисту пристроїв

5. BYOD та захист мобільних пристроїв	до 15 робочих днів	Налаштовані погоджені політики
6. Захист електронної пошти та спільної роботи	до 10 робочих днів	Налаштовані параметри захисту
7. Захист даних та DLP	до 12 робочих днів	Налаштовані параметри захисту
8. Пілот	до 10 робочих днів	Протокол пілотного впровадження
9. Масове впровадження	до 20 робочих днів	Акт впровадження
10. Документація та навчання	до 10 робочих днів	Комплект документації, навчання, фінальний звіт

Строки надання послуг в рамках етапів можуть бути змінені за погодженням з Замовником за умови дотримання загальних строків послуг, що не перевищуватимуть 3 календарних місяці.
Окремі етапи можуть виконуватися паралельно.

15. ПОРЯДОК ПРИЙМАННЯ НАДАНИХ ПОСЛУГ

Приймання послуг здійснюється Замовником відповідно до умов Договору на підставі переданих результатів, актів та комплекту документації. Послуги вважається виконаною після виконання погодженого обсягу робіт та передачі передбачених цими Технічними вимогами результатів.

16. ОБМЕЖЕННЯ ПРЕДМЕТА ЗАКУПІВЛІ

придбання нових ліцензій Microsoft не входить до предмета закупівлі, якщо інше прямо не визначено тендерною документацією;
постачання нового апаратного забезпечення не входить до предмета закупівлі;
розроблення програмного забезпечення не входить до предмета закупівлі;
масове перевстановлення операційних систем не входить до предмета закупівлі, якщо інше не визначено календарним планом;
функціональність, доступна лише в Microsoft 365 E5, окремих add-on або інших ліцензіях, виконується лише за наявності відповідних ліцензій Замовника.

6. Обґрунтування розміру бюджетного призначення: закупівля проводиться на очікувану вартість на 2026 рік з урахуванням середньої ринкової вартості по Україні, а також з урахуванням бюджетного запиту на 2026 рік.

Код економічної класифікації видатків бюджету (КЕКВ) 2240 Оплата послуг (крім комунальних).

7. Очікувана вартість предмета закупівлі: 1 980 000,00 грн. з ПДВ.

8. Обгрунтування очікуваної вартості предмета закупівлі: очікувана ціна послуг за предметом закупівлі обраховується виходячи із попередніх закупівель аналогічних послуг та враховуючи ринкові ціни по Україні.