ОБҐРУНТУВАННЯ

технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі (відповідно до пункту 4[1] постанови Кабінету Міністрів України від 11.10.2016 № 710 «Про ефективне використання бюджетних коштів»)

1. Предмет закупівлі: Придбання (постачання) ліцензій на право користування програмною продукцією ESET PROTECT MDR код ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів

2. Вид процедури: відкриті торги з особливостями (закупівля через Централізовану закупівельну організацію – ДП «УСС»)

3. Номер оголошення закупівлі: UA-2026-10-21-010879-a

4. Обґрунтування технічних та якісних характеристик предмета закупівлі:
Забезпечення комплексного, багаторівневого антивірусного захисту, проактивного моніторингу, централізованого управління, розширеного виявлення і реагування на кіберзагрози (EDR/XDR) та цілодобового сервісу керованого виявлення та реагування (MDR 24/7/365) для всієї мережевої інфраструктури, робочих станцій, серверів та мобільних пристроїв Замовника.

Кількісні характеристики та компонентний склад закупівлі:

- Загальний обсяг постачання: Пакетний комплекс ліцензій ESET PROTECT MDR (або еквівалент), що забезпечує захист та покриття робочих станцій, серверів, мобільних пристроїв, хмарних сервісів та поштових систем у межах корпоративної мережі Замовника.
- Строк дії ліцензій та надання сервісу MDR: 36 місяців з моменту активації та постачання.
- **Склад комплектного програмного рішення включає:**
  - Сервер/консоль централізованого управління (з можливістю локального або хмарного розгортання);
  - Модулі захисту кінцевих точок (робочих станцій під ОС Windows, Linux, macOS);
  - Модулі захисту серверів (під ОС Windows Server, Linux Server, гіпервізорів Hyper-V/VMware);
  - Розширений захист мобільних пристроїв (Android, iOS);
  - Модуль повнодискового шифрування (Full Disk Encryption);
  - Модуль розширеного аналізу в хмарі (хмарна пісочниця / Cloud Sandbox);
  - Рішення для захисту хмарних застосунків (Microsoft 365, Google Workspace);
  - Захист поштових серверів (Exchange Server, Domino);
  - Модуль управління вразливостями та виправленнями (Vulnerability & Patch Management);
  - Рішення для розширеного виявлення та реагування (EDR/XDR);
  - Модуль багатофакторної автентифікації (2FA / MFA);
  - Сервіс керованого виявлення та реагування на кіберзагрози (MDR 24/7/365).

Технічні та якісні характеристики предмета закупівлі:
Вимоги до консолі (Сервера управління):

- Централізоване управління антивірусним захистом з єдиного веб-інтерфейсу (локально та/або у хмарі) англійською та українською мовами.

- Інвентаризація обладнання та ПЗ на робочих станціях і серверах під управлінням Windows, macOS, Linux; віддалена інсталяція/деінсталяція ПЗ та антивірусних агентів.
- Можливість побудови ієрархічної структури адміністрування, автентифікація через Active Directory, підтримка двофакторної автентифікації (2FA) для адміністраторів та ведення повного журналу аудиту дій.
- Інтеграція з SIEM-системами (Microsoft Sentinel, IBM QRadar, Splunk, Elastic, Wazuh тощо) через REST API та протокол Syslog.
- Наявність інструментів управління VDI-середовищами (VMware Horizon, Citrix XenServer) та майданчиками/філіями.

Вимоги до захисту кінцевих точок (Робочих станцій):

- Багаторівневий захист у режимі реального часу від вірусів, троянів, фішингу, шпигунського ПЗ, руткітів, потенційно небажаних (PUA) та потенційно небезпечних програм.
- Використання евристичного аналізу, 64-бітного ядра, технологій машинного навчання, модуля захисту від експлойтів, розширеного сканера пам'яті та захисту від програм-вимагачів (Ransomware Shield з функцією автоматичного відновлення зашифрованих файлів).
- Захист завантажувальних секторів (UEFI/MBR), сканування WMI та системного реєстру, сканування під час запуску ОС та у неактивному стані.
- Контроль пристроїв (USB, CD/DVD, периферія за серійними номерами, ID, виробником), персональний брандмауер, система виявлення вторгнень (HIPS/IDS), захист від ботнетів та мережевих вразливостей (SMB, RPC, RDP, CVE).
- Веб-контроль (27 категорій, понад 100 підкатегорій), фільтрація HTTP/HTTPS/SSL, захист банківських операцій/браузера, захист поштового трафіку (POP3, SMTP, IMAP) та локальний модуль антиспаму.

Низьке споживання системних ресурсів (50–100 МБ ОЗП, 2–35% ЦПУ).

Вимоги до захисту серверів:

- Автоматичне визначення ролей сервера для формування виключень та мінімізації впливу на продуктивність.
- Сканування дисків гіпервізора Microsoft Hyper-V без встановлення агентів у віртуальні машини; підтримка роботи у кластерах (Domain, Workgroup, NLB).
- Підтримка широкого спектру серверних ОС: Microsoft Windows Server 2012–2025, RedHat Enterprise Linux, Rocky Linux, Ubuntu Server, Debian, SUSE Linux, Alma Linux, Oracle Linux, Amazon Linux.

Розширений захист мобільних пристроїв та повнодискове шифрування:

- Управління мобільними пристроями (Android 5+, iOS 9+) з єдиної хмарної консолі, підтримка реєстрації через Microsoft Intune, Entra ID, Apple Business Manager, функція віддаленого блокування/стирання даних, антифішинг, захист додатків.
- Віддалене повнодискове шифрування (FDE) для Windows та macOS із передзавантажувальною автентифікацією (Pre-boot authentication), підтримка TPM та OPAL, генерація паролів відновлення.

Хмарна пісочниця, захист хмарних застосунків та пошти:

- Автоматична та ручна відправка підозрілих об'єктів на аналіз у хмарну пісочницю (Cloud Sandbox) з виявленням загроз 0-го дня від кількох секунд до 6 хвилин.
- Захист хмарних сервісів Microsoft 365 (Exchange Online, OneDrive, Teams)

та Google Workspace (Gmail, Google Drive) від спаму (ефективність 99.99%), фішингу, Quishing (QR-фішинг) та зловмисного ПЗ.
- Захист поштових серверів (Exchange Server, HCL/IBM Domino) на рівні транспортного протоколу та баз даних.

Керування вразливостями, EDR/XDR та багатофакторна автентифікація (2FA):

- Автоматичне сканування, пріоритизація за критичністю та автоматичне/ручне застосування виправлень (Patch Management) для ОС Windows, Linux, macOS.
- Повнофункціональне рішення EDR/XDR: моніторинг аномальної поведінки, аналіз першопричин (Root Cause Analysis), вибудовування дерева процесів, сортування за матрицею MITRE ATT&CK, ізоляція скомпрометованих пристроїв від мережі в один клік, збір телеметрії.
- Модуль 2FA: захист входу в ОС (Windows, Linux, macOS), RDP, VPN, VDI, ADFS, Office 365, Web-додатки; підтримка Push-повідомлень, OTP, SMS, апаратних токенів (FIDO2, OATH), робота без доступу до Інтернету.

Сервіс керованого виявлення та реагування на кіберзагрози (MDR 24/7/365):

- Цілодобовий моніторинг, проактивний пошук загроз (Threat Hunting), аналіз та реагування на інциденти командами аналітиків SOC у режимі 24/7/365.
- Використання індикаторів компрометації (IoC) та атак (IoA), автоматизована ізоляція хостів, припинення процесів, закриття кейсів.
- Надання регулярно щотижневої та щомісячної звітності, дотримання регламенту обслуговування (SLA) та розмежування строків реакції та реагування.

Вимоги до документації, підтримки та відповідності законодавству України:

- Наявність інтерфейсу, довідкової системи та експлуатаційної документації («Посібник користувача/адміністратора») українською та англійською мовами.
- Наявність офіційного представництва виробника та сертифікованої технічної підтримки в Україні (телефон, email, виїзд).
- Надання у складі пропозиції авторизаційного листа від виробника або чинного партнерського сертифіката.
- Дотримання вимог ТЗІ України: надання копій чинних Експертних висновків, зареєстрованих в Адміністрації Держспецзв'язку України, що підтверджують відповідність програмного рішення вимогам нормативних документів системи технічного захисту інформації (ТЗІ).
- Наявність у виробника/сервісу сертифікацій ISO/IEC 27001:2022 та незалежного аудиторського звіту SOC 2 Type II / Type I.

5. Обґрунтування розміру бюджетного призначення:

Розмір бюджетного призначення визначено відповідно до кошторису Державного агентства України ПлейСіті на 2026 рік за бюджетною програмою КПКВК 2902010 «Керівництво та управління у сфері регулювання азартних ігор та лотерей».

6. Обґрунтування очікуваної вартості закупівель:

Згідно з абзацами одинадцятим та дванадцятим пункту 1 розділу III Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом

Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року № 275, за результатами запиту цінових пропозицій до компаній, проведеної аналітики на платформі Prozorro, а також з урахуванням потреби у забезпеченні службових комп’ютерів для захисту від вірусів, була визначена очікувана вартість 970 000,00 (дев'ятсот сімдесят тисяч гривень 00 копійок) з урахування ПДВ.