**ОБГРУНТУВАННЯ кількісні та якісні характеристики**

**ТЕХНІЧНІ ВИМОГИ на закупівлю по предмету**

код ДК 021:2015 72250000-2 Послуги, пов’язані із системами та підтримкою (закупівля послуг технічної підтримки та супутніх послуг) послуги технічної підтримки центру обробки даних (далі - ЦОД) НДСЛ Охматдит МОЗ України

1. **МЕТА НАДАННЯ ПОСЛУГ**
	1. Послуги технічної підтримки центру обробки даних (далі - ЦОД) надаються з метою:
* Безперебійного функціонування обладнання ЦОД наданого у таблиці 2.1;
* Налаштування та оновлення сервісної підтримки для забезпечення безперебійного функціонування в ЦОД міжмережевого екрану Sophos XG 450, згідно вимог Замовника;
* Налаштування та оновлення пакетів програмного забезпечення для захисту від вірусів та розслідування інцидентів, Sophos NGEP XDR.
* Забезпечення своєчасної експертної підтримки функціонування обладнання ЦОД, вказаного у п.2.1, п.2.2 включаючи обслуговування на базі підтримки виробника обладнання, налаштування та обслуговування технічних засобів та програмного забезпечення, підтримку 24х7 по телефону та електронній пошті, оновлення версій програмних продуктів.
1. **СКЛАД ТА ЗМІСТ ПОСЛУГ**
	1. **Виконавець повинен надати Замовнику сервісну підписку від виробника обладнання та технічну підтримку на один рік (12 календарних місяців) технічних засобів ЦОД відповідно до наступної специфікації, вказаної у табл. 2.1:**

Табл. 2.1

|  |  |  |
| --- | --- | --- |
| **Номер** | **Найменування обладнання** | **Кількість** |
| 1 | Оптичний комутатор Dell Force10 MXL 10/40 GbE з комплектом оптичних трансиверів  | 2 |
| 2 | Серверне блейд-шасі Dell PE M1000e Blade Enclosure 2x CMC KVM 9x Fans 6xPSU 3000W 3Yr PS NBD  | 1 |

2.1.1 Усі пакети з сервісної підтримки апаратного і програмного забезпечення, які пропонуватимуться у відповідь на це Оголошення про тендер, повинні бути новими та невживаними, з датою реєстрації у Виробника обладнання не раніше 01.01.2023 рік.

2.1.2. Для реалізації всіх функцій, закладених в існуючий ЦОД НДСЛ «Охматдит» МОЗ України, необхідно використовувати тільки сумісні з цім обладнанням рішення – компоненти.

2.1.3. Послуги з технічного обслуговування обладнання DELL (розширення гарантії) мають надаватися за програмою гарантії Next Business Day On-Site Service, Custom Other Services, Reinstatement Fee,Enterprise за наступним регламентом:

 - підтримка в режимі 24/7/365;

- заміна апаратних компонентів серверів;

- підтримка на місці 24/7 при критичних проблемах;

- підключення технічного спеціаліста для вирішення критичних заявок та виділених експертів для вирішення складних проблем;

- пріоритизація критичних заявок та вирішення проблем;

- підтримка системного ПЗ;

- оперативне усунення зауважень в роботі апаратного забезпечення серверів на протязі терміну надання послуг

- прискорена заміна несправних компонентів Dell On-line Self Dispath без затримки на діагностику (діагностика здійснюється адміністратором або службою підтримки замовника системи);

- заведення та відслідковування стану заявки в онлайн.

2.1.4 Наявність у учасника служби сервісної підтримки, яка працює в режимі 24/7, про що надається гарантійний лист у складі тендерної пропозиції.

* 1. **Виконавець повинен надати, інсталювати та налаштувати Замовнику програмне забезпечення та оновити сервісну підтримку, згідно вимог Замовника, для міжмережевого екрану Sophos XG 450 (обладнання встановлено у кількості 2 одиниці).**

2.2.1. Вимоги до програмного забезпечення

Програмне забезпечення повинне включати активацію наступних функцій міжмережевого екрану Sophos XG 450:

* підтримка IPSec VPN,
* підтримка SSL Inspection,
* підтримка SSL VPN,
* підтримка Web content filtering,
* підтримка NGFW,
* підтримка Intrusion Prevention System,
* підтримка Advanced Threat Protection,
* підтримка Antivirus,
* підтримка Antimalware,
* підтримка Web Control (protection),
* підтримка App control (protection),
* підтримка Clientless VPN,
* підтримка Email Protection and Control,
* підтримка Email Quarantine Management,
* підтримка Email Encryption and DLP
* підтримка Cloud Sandbox

Послуги с ліцензування та налаштування повинні забезпечувати доступність та працездатність функцій міжмережевого екрану Sophos XG 450 протягом одного календарного року (12 місяців).

Послуга з технічної підтримки для міжмережевого екрану Sophos XG 450 повинна продовжити функціонування всіх необхідних ліцензій для забезпечення необхідного функціоналу міжмережевого екрану про що надається гарантійний лист у складі тендерної пропозиції.

- Гарантійний термін обслуговування не менше ніж 12 місяців з умовами гарантійної заміни RMA, включаючи обслуговування на базі підтримки виробника обладнання, підтримку по телефону та електронній пошті 24х7, оновлення патчів продукту, характеристик та інших оновлень, про що надається гарантійний лист у складі тендерної пропозиції.

- Наявність у учасника служби сервісної підтримки, яка працює в режимі 24/7, про що надається гарантійний лист у складі тендерної пропозиції.

- Наявність у учасника повного комплексу засобів (інструментальних та програмних) для можливості встановлення ПЗ Sophos (зміни параметрів, заміни, додавання або видалення налаштувань та ін.), про що надається гарантійний лист у складі тендерної пропозиції.

**2.3 Виконавець повинен надати, інсталювати та налаштувати Замовнику програмне забезпечення та оновити сервісну підтримку, згідно вимог Замовника, а саме пакети програмного забезпечення для захисту від вірусів та розслідування інцидентів, Sophos NGEP XDR**

2.3.1. Вимоги до програмного забезпечення та кількість ліцензій

|  |  |  |
| --- | --- | --- |
| **Номер** | **Найменування програмного забезпечення** | **Кількість** |
| 1 | Впровадження/оновлення підписки Central Intercept X Advanced with XDR - 12 MOS - GOV | 650 |
| 2 | Впровадження/оновлення підписки Central Intercept X Advanced for Server with XDR - 12 MOS - GOV | 40 |

|  |  |
| --- | --- |
| **Найменування**  | **Вимоги** |
| **Функціональне призначення** | Впровадження/оновлення програмного продукту для забезпечення захисту робочих станцій від шкідливого програмного забезпечення (в т.ч. вірусів) з можливістю розслідування інцидентів інформаційної безпеки. |
| **Інтегрований менеджмент управління** | * Повинна бути уніфікована консоль для управління кількома продуктами.
* Наявність єдиної хмарної консолі централізованого управління антивірусним захистом хостів та мережевим брандмауером.
* Повинна включати розширений захист кінцевих точок, веб-шлюз, безпеку сервера.
* Усі налаштування мають проводитись з центральної інформаційної панелі без необхідності доступу додаткових консолей.
* Запропонована система повинна підтримувати багатоплатформене управління кінцевими точками на операційних системах Windows, Mac та Linux з однієї консолі.
* Запропонована система повинна підтримувати інтеграцію з ПАК NGFW Sophos XG для автоматичного виявлення скомпрометованих робочих станцій та їх ізоляції.
* Рішення повинно бути в списку лідерів в рейтингу Gartner Magic Quadrant протягом останніх 5 років.
 |
| **Оновлення та споживання пропускної здатності** | * Оновлення кінцевих точок має мати можливість встановлювати попередньо налаштовану пропускну здатність, яка використовується як для оновлення програмного забезпечення, так і для оновлень визначення загроз (наприклад, 64, 128, 256 Кбіт/с, тощо).
* Повинно мати можливість налаштування серверу оновлення кешу в локальному мережевому середовищі, щоб мінімізувати велике навантаження під час оновлення модуля програмного забезпечення.
* Повинно бути реалізована функція додавання політик керування оновленнями, щоб дозволити встановлювати розклади для проведення оновлення на кінцевій точці.
 |
| **Варіанти розгортання агентів** | * Розгортання агента кінцевої точки має підтримувати таку методологію:
* електронна пошта;
* за допомогою сценарію запуску/завершення роботи AD;
* сценарій входу в систему AD;
* SCCM;
 |
| **Механізм глибокого навчання та запобігання зараженню** | * Система повинна мати можливість сканувати ОС, протягом 20 мілісекунд, а також мати можливість витягти мільйони функцій з файлу, провести глибокий аналіз та визначити, чи є файл доброякісним чи шкідливим. Весь цей процес відбувається перед виконанням файлу.
* Повинен бути в змозі запобігти як відомому, так і ніколи не баченому шкідливому програмному забезпеченню, а також повинен мати можливість блокувати шкідливе програмне забезпечення перед його виконанням.
* Повинен захищати систему навіть в автономному режимі і не буде покладатися на підписи.
* Потрібно класифікувати файли як шкідливі, потенційно небажані програми (PUA) або доброякісні. Поглиблене навчання також має зосередитися на портативних виконуваних файлах Windows.
* Можливість виконувати нове сканування загроз у 0-day дні в автономному режимі (без доступу до Інтернету).
* Модель глибокого навчання повинна відстежувати та оцінювати моделі наскрізь, використовуючи передові розроблені пакети, такі як Keras, Tensorflow та Scikit-learn.
* Контролю завантажувального контенту на основі репутації і виявлення шкідливого трафіку.
* Можливість блокувати завантаження з Інтернету файлів за вказаною розширенням.
* Автоматична антивірусна перевірка і контроль змінних носіїв, периферії (USB, Floppy disc, BT, flash).
* Контроль і захист додатків (Java, HTA, медіа, офісні) на основі категоризації.
* Блокування небажаних програм, PUA.
* Виявлення шкідливого ПО без сигнатур за допомогою технологій штучного інтелекту, глибокого вивчення «deep learning».
* Наявність системи виявлення вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності.
* Можливість захисту від: шкідливих програм; троянського ПЗ; клавіатурних шпигунів; рекламного ПЗ; фішингу; шпигунського ПЗ; руткітів; скриптів потенційного небажаного і небезпечного ПЗ.
* Можливість використання технології, яка забезпечує захист від загроз типу "ботнет".
* Захист вразливостей мережевого протоколу, який покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC і т.д.
* Виявлення, блокування та видалення експлойтів і інтерактивний захист (Anti-Exploit).
* Запобігання комп'ютерних вторгнень, захист процесів (функції запобігання виконання коду (DEP), Reflective DLL Injection, Bottom-up ASLR, шелл-код, захист від підвищення привілеїв).
* Можливість придушення стекових атак, і атак типу ROP на основі розгалуження.
* Захист від крадіжки облікових даних.
* Модуль захисту документів, який перевіряє макроси на шкідливий код.
* Можливість захисту від втрати даних, DLP, перевірка вкладень вихідних повідомлень, передачі даних (контроль контенту, формату, назви, атрибутів файлу).
* Захист від атак типу MitM, підтримка SafeBrowsing.
* Можливість виявлення і захисту від Meterpreter Shell, Code Cave.
* Можливість виявлення і захисту від Double Pulsar / AtomBombing. Підтримка APC Protection.
 |
| **Виявлення шкідливого трафіку (MTD)** | * Повинен бути здатним виявляти зв'язок між комп'ютерами кінцевих точок та серверами управління та керування, які беруть участь у ботнет-атаках або інших шкідливих програмах.
 |
| **Захист від програм вимагачів та шифрувальників** | * Захист від Ransomware. Автоматичне відновлення даних, захист від здирників, захист диска і MBR записи. Повинна бути передбачена можливість відкоту зашифрованих файлів до попередньо зашифрованого стану.
* Для захисту і виявлення від експлойтів та вимагачів не потрібно мати хмарне підключення.
* Повинна існувати функція (модуль), що реалізує аналіз підозрілої поведінки передбачуваному процесу, реєстратор даних повинен почати кешування даних, поки зазначена поведінка ретельно перевіряється, щоб визначити, чи програма є легітимною.
 |
| **Функції розслідування та аудиту** | * В системі повинна бути реалізована (RCA) «служба загроз», що відстежує дані і дозволяє визначити походження інфекції, будь -які наслідки пошкодження активів, потенційно відкриті дані та ланцюжок подій, що призводять до зупинки інфекції.
* Реалізовано можливість аналізу файлів, щоб визначити, чи є вони загрозою або потенційно небажаними.
* Аналітики повинні мати можливість легко бачити, які атрибути та сегменти коду подібні до файлів "відомо добре" та "відомо погано", щоб вони могли визначити, чи слід заблокувати чи дозволити файл.
* Реалізовано пошук показників компрометації в мережі
* Визначення пріоритети подій для подальшого розслідування та виявлення атак, які могли залишитися непоміченими
* Запис діяльності, що дозволить адміністраторам додавати примітки до справи. У цій колонці будуть перераховані всі примітки, що стосуються справи.
* Можливість надати адміністратору змінювати стан справ (Новий, В процесі, Закритий) та встановлювати пріоритет (Низький, Середній, Високий). При закритті адміністратор може додавати примітки, а також повинен підтвердити (за допомогою прапорців), що були вжиті заходи щодо виправлення: проаналізовано вплив на файли/активи та впроваджено відповідні екологічні покращення.
* Випадки загроз мають містити рекомендації щодо вирішення проблеми: Що слід шукати після нападу. Напр. Крім того, що файли відновлюються із зашифрованих, перевірте налаштування браузера, щоб упевнитися, що в результаті зараження не було створено вразливостей.
* Забезпечення табличне відображення про все, що постраждало під час нападу. З можливістю зміни елементів, фільтрування залежно від типу (файли, процеси, ключі реєстру). Адміністратор може переглядати інформацію про кожен елемент, наприклад. Ім'я файлу (файл жертви або агент шкідливого програмного забезпечення), ідентифікатор процесу, мітка часу початку/зупинки події.
* Можливість проводити розслідування під керівництвом, що дозволяє адміністраторам відповідати на складні запитання щодо інцидентів безпеки, надаючи інформацію про масштаби атаки, про те, як вона почалася, на що вплинула та як реагувати.
* Випадки загроз повинні чітко вказувати початок причини, що викликається, виділяючи серію подій, що виникли в результаті атаки, як сукупність вузлів. Кожен вузол містить конкретну інформацію про файли, процеси, ключі реєстру тощо, які беруть участь на цьому етапі.
* Можливість розширеного аналізу загроз SophosLabs на вимогу та з допомогою штучного інтелекту
* Випадки загроз повинні мати можливість направляти запит, щодо найновіших даних, натиснувши кнопку "Запит останніх даних", файл буде надіслано до лабораторії виробника, і це призведе до створення звіту через пару хвилин і відображення додаткової інформації.
* Наявність Live Response, дозволяє віддалено підключатися до пристроїв з хмарної консолі керування (Remote Terminal Access), щоб досліджувати й усувати можливі проблеми безпеки, зупиняти підозрілі процеси, перезавантажувати пристрої з незавершеними оновленнями, переглядати папки, видаляти файли тощо.
* Наявність Live Discover (перехресні SQL-запити для виявлення загроз і гігієни операцій ІТ-безпеки) із заздалегідь написаною бібліотекою стандартних запитів SQL, що дозволять отримати прямий доступ до пристрою, щоб зрозуміти його поточний стан роботи та історію активності та отримати відповіді на різноманітні запити, починаючи від «Як довго працює пристрій», до більш складних запитів, таких як «Які файли та ключі реєстру міг змінити процес, коли він запустився десять днів тому.
 |
| **Термін ліцензування** | * Підписка на оновлення сигнатур безпеки не менше 12 місяців;
 |

Послуги с ліцензування та налаштування повинні забезпечувати доступність та працездатність функцій програмного забезпечення для захисту від вірусів та розслідування інцидентів, Sophos NGEP XDR протягом одного календарного року (12 місяців).

- Наявність у учасника служби сервісної підтримки, яка працює в режимі 24/7, про що надається гарантійний лист у складі тендерної пропозиції.

- Наявність у учасника повного комплексу засобів (інструментальних та програмних) для можливості встановлення ПЗ для захисту від вірусів та розслідування інцидентів, Sophos NGEP XDR (зміни параметрів, заміни, додавання або видалення налаштувань та ін.), про що надається гарантійний лист у складі тендерної пропозиції.

1. **ВИМОГИ ДО ПОСЛУГ ТЕХНІЧНОЇ ПІДТРИМКИ З УСУНЕННЯ ІНЦИДЕНТІВ**

До Усунення інциденту повинні належать наступні послуги з сервісної та технологічної підтримки апаратної ІТ-інфраструктури:

* Перевірка працездатності елементів апаратної ІТ-інфраструктури;
* З’ясування причин та обставин несправності та/або надання рекомендацій відповідальним особам Замовника по відновленню функціонування елементів апаратної ІТ-інфраструктури;
* Відновлення працездатності (функціонування) елементу апаратної ІТ-інфраструктури.
* Заміна елементів апаратної ІТ-інфраструктури з використанням комплекту запасних елементів (ЗІП) якщо .
* Оновлення внутрішнього ПЗ елементів апаратної ІТ-інфраструктури.
* Збирання та тестування елементів апаратної ІТ-інфраструктури.
* Створення кейсу (case) проблеми для звернення на зовнішній рівень підтримки Виробника, відстеження виконання і співпраця з Виробником, впровадження рішень та рекомендацій Виробника стосовно звернення.
* Налаштування елементів апаратної ІТ-інфраструктури у відповідності до інструкцій Виробника обладнання.

Послуги з відновлення працездатності обладнання із заміною запасних частин, який включає в себе:

* діагностика та заміна несправних модулів оперативної пам’яті та процесорів;
* діагностика несправностей систем живлення серверів і мережевого обладнання та заміна дефектних блоків;
* аналіз та впровадження оптимального рішення по відновленню працездатності обладнання;
* заміна дискових модулів RAID-масивів із запуском процедур відновлення інформації;
* заміна несправних компонентів обладнання;
* перевірка працездатності обладнання після отримання послуг з відновлення;
* сервісне обслуговування здійснюється за місцем установки обладнання;
* інші види робіт.

До усунення аварійних ситуацій належать роботи, які Виконавець виконує з метою відновлення працездатності обладнання, або його елементів, за допомогою діагностично-відновлювальних засобів програмного забезпечення (ПЗ) обладнання, а також ремонту та/або заміни елементів, що вийшли з ладу, з використанням комплекту запасних елементів (ЗІП). Комплект ЗІП для системи зберігання данних та обладнання, включеного в послугу підтримки вказану в п.1.1 надається Виконавцем, який забезпечує його придбання власним коштом та забезпечує його своєчасне поповнення. Ремонт елементів активного мережевого, серверного та іншого обладнання, що входять в систему збереження данних та обладнання, що включено в послуги по підтримці, вказані у п.1.1, виконує Виконавець власним коштом в офіційних сервісних центрах відповідних виробників обладнання. Виконавець повинен забезпечити первинну діагностику несправних елементів, за технічної можливості – відновлення даних елементів програмними засобами, та сприяння найшвидшому виконанню ремонту сервісними центрами.

Інциденти класифікуються Замовником відповідно до ступеню впливу на працездатність та важливість такого елементу комплексу обладнання. Виконавець повинен гарантувати час реакції на інцидент відповідного пріоритету та дотримуватися необхідного часу усунення згідно Таблиці №3.

*Таблиця №3 Класифікація інцидентів*

|  |  |  |  |
| --- | --- | --- | --- |
| *Пріори-**тет* | *Опис* | *Час реакції* | *Час усунення* |
| 1 | Відповідає аварійному пошкодженню (відмові) всього комплексу обладнання, або ключових (центральних) елементів, що впливає на роботу комплексу у цілому, та/або є дуже критичним. | негайний | 12 години |
| 2 | Відповідає аварійному пошкодженню (відмові) частини комплексу обладнання, або не ключових (в тому числі центральних) елементів , що впливає на роботу частини комплексу, та не є критичним, або відповідне обладнання може тимчасово (з обмеженнями) функціонувати завдяки засобам відмовостійкості (резервування). | 2 години | 16 годин |
| 3 | Відповідає експлуатаційному пошкодженню (відмові) незначної частини комплексу обладнання, або не ключового (в тому числі центрального) елементу , що не впливає на роботу комплексу, та не є критичним, або відповідне обладнання може повноцінно функціонувати завдяки засобам відмовостійкості (резервування). | 8 години | 24 години |

У випадку, якщо з об’єктивних причин (складність, численність пошкоджень і т.д) неможливо забезпечити визначений час усунення, Виконавець узгоджує із Замовником реальний час усунення. В цьому випадку допускається розроблення Виконавцем, та узгодження із Замовником тимчасового (аварійного) алгоритму функціонування відповідного елементу комплексу обладнання задля мінімізації впливу пошкодження на функціонування комплексу в цілому, та реалізує його на час усунення відповідного пошкодження.

Замовник інформує Виконавця про інцидент із зазначенням відповідного пріоритету. Виконавець має право аргументовано змінити (знизити, або підвищити) пріоритет за узгодженням з Замовником.

Виконавець повинен гарантувати Замовнику свою готовність до прийому повідомлень та виконання робіт з усунення аварійних ситуацій 7 днів на тиждень, 24 години на добу.

Виконавець повинен забезпечити прийом та обробку повідомлень про аварійні ситуації Замовника наступними засобами:

* Присутність від Виконавця мінімум одного інженера на об’єкті 7 днів на тиждень, 24 години на добу;
* Цілодобово: телефон (та/або мобільний телефон диспетчера сервісної служби, чергового інженера);
* У робочий час: електронна пошта або інформаційна система технічної підтримки СТП (Help Desk).

Виконавець може виконувати роботи за допомогою інженера технічної підтримки Виробника обладнання з використанням віддаленого доступу, при безпосередній участі інженера Виконавця на об’єкті Замовника.

1. **ВИМОГИ ДО СТРОКІВ НАДАННЯ ПОСЛУГ**
	1. Виконавець у строк до 30 робочих днів з моменту підписання Договору повинен, надати встановити та налаштувати Замовнику ліцензії, оновити підписки та програмне забезпечення (п.1.1. цих технічних вимог).
	2. Виконавець повинен надавати Замовнику протягом 12 місяців, починаючи з моменту підписання Договору, послуги технічної підтримки ЦОД відповідно до цих технічних вимог.
2. **ПОРЯДОК ПРИЙМАННЯ ПОСЛУГ**
	1. Послуги технічної підтримки ЦОД приймаються шляхом підписання Акту прийому-передачі послуг за фактом отримання Виконавцем інформації про активацію сервісної підписки та оновлення підтримки програмного забезпечення та обладнання на один рік.
	2. З метою прийняття Замовником послуг з технічної підтримки ЦОД, Виконавець, протягом строку надання технічної підтримки, один раз на місяць здійснює підготовку звіту про надані послуги. Виконавець повинен зазначений звіт з двома підписаними ним примірниками акту прийому-передачі наданих послуг передати Замовнику. Замовник приймає надані Виконавцем послуги та повертає Виконавцю підписаний акт прийому-передачі наданих Послуг. В разі, якщо надані послуги не відповідають умовам цих технічних вимог, Замовник готує та подає Виконавцю відповідно до Договору аргументовану відмову щодо прийняття послуг.
3. **ВИМОГИ ДО ДОКУМЕНТАЦІЇ**
	1. Зміни та доповнення до документації ЦОД повинні надаватися в паперовій та в електронній формах.
4. **ВИМОГИ ДО УЧАСНИКА**
	1. Гарантійний термін обслуговування не менше ніж 12 місяців з умовами гарантійної заміни RMA, включаючи обслуговування на базі підтримки виробника обладнання, підтримку по телефону та електронній пошті 24х7, оновлення версій програмних продуктів, характеристик та інших оновлень, про що надається гарантійний лист у складі тендерної пропозиції.
	2. Наявність у учасника служби сервісної підтримки, яка працює в режимі 24/7, про що надається гарантійний лист у складі тендерної пропозиції.
	3. Наявність у учасника повного комплексу засобів (інструментальних та програмних) для можливості встановлення ліцензій, підписок, програмного забезпечення на обладнання виробників торгових марок: DELL, Sophos зазначене у п.2.1, 2.2, 2.3 технічних вимог (зміни параметрів, заміни, додавання або видалення налаштувань та ін.), про що надається гарантійний лист у складі тендерної пропозиції.
	4. Авторизаційні листи від виробників обладнання/програмного забезпечення торгових марок: DELL, Sophos, зазначеного у п.2.1, п.2.2, п.2.3 технічних вимог або від офіційного представництва/представника виробника в Україні, що підтверджує наявність партнерських відносин Учасника з компанією-виробником або офіційним представництвом/ком виробника в Україні та дійсність гарантійних зобов’язань, наявність сервісної підтримки на території України. Авторизаційна форма обов’язково повинна містити посилання на номер оголошення, оприлюдненого на веб-порталі з питань державних закупівель, замовника та предмету закупівлі
	5. Учасник в складі пропозиції повинен надати довідку/сертифікат/посвідчення від виробника або від офіційного представництва/представника виробника в Україні про проходження навчання та надбання навичок по налаштуванню та підтримки обладнання/програмного забезпечення торгових марок: DELL, Sophos.
	6. Огляд об'єкта учасником перед подачею пропозиції є обов'язковим. Огляд проводиться на підставі офіційного листа-звернення на ім’я замовника (щодня з 08 год. 00 хв. до 16 год. 00 хв., крім суботи та неділі). Учасник у складі тендерної документації повинен надати довідку в довільній формі про огляд об’єкту, засвідчену замовником. Витрати на відвідування об’єкту Учасник несе за власні кошти. При цьому Замовник не несе відповідальності за будь-які майнові та немайнові ризики, пов’язані з ознайомлювальною поїздкою.
5. **ВИМОГИ ДО ЧИСЕЛЬНОСТІ І КВАЛІФІКАЦІЇ ПЕРСОНАЛУ ВИКОНАВЦЯ ТА РЕЖИМУ ЙОГО РОБОТИ**
	1. Вимоги до кількості персоналу:

Чисельність персоналу Виконавця, повинна відповідати нормам, обумовленим технічними вимогами до використовуваного типу систем.

Нижче приведений орієнтовний необхідний склад персоналу для супроводу Замовника:

• адміністратор локальної обчислювальної мережі і мережі Інтранет - 2 особи;

• адміністратор інформаційних систем - 2 особи;

• інженер супроводу комп’ютерних систем - черговий інженер - 2 особи;

* 1. Вимоги до кваліфікації персоналу

Адміністратори та інженери інформаційних систем повинні мати кваліфікацію iнженерiв з комп’ютерних систем із знанням:

 операційних систем типу: MS Windows Server, Linux, FreeBSD, NetWare, UNIX (AIX, HP-UX, Solaris).

СУБД і додатків: Microsoft Active Directory / SQL Server / Exchange Server / SharePoint Server, Oracle, Oracle RAC, MySQL, DB2.

Гіпевізорів: VMware, Microsoft Hyper-V, MS Azure

Технологій роботи мережевих протоколів та стандартів: MPLS, OSPF, IS-IS, QoS, IGMP / MLD / PIM, ARP, BFD, VRRP, Q-in-Q, TCP / IP, VLAN, NAT, DNS, DHCP, VPN, NetBIOS, SMB / CIFS, RDP, SSH

 Unix сервісів:(Zabbix, SQUID, і т.д., інтеграція з Active Directory),

Систем зберігання данних: NetApp, DELL

Систем резервного копіювання (створення скриптів резервного копіювання, технологій архівування резервних копій даних, ввикористовуючи програмне забезпечення системи зберігання данних та сервери резервного копіювання). Перед допуском до роботи інженер/ри Виконавця повинен/ні пройти навчання щодо керування обладнанням/програмним забезпеченням, зазначеному у табл. 2.2, 2.3. Учасник у складі своєї пропозиції повинен надати авторизаційний лист/и від виробника/ів обладнання вказанного у табл. 2.2 в ЦОД НДСЛ «ОХМАТДИТ» або його офіційного представництва/ка в Україні про підтвердження партнерського статусу, що підтверджує повноваження Учасника на встановлення, налаштування та обслуговування обладнання та гарантує дійсність належної сервісної підтримки виробником. Такий лист/и повинний бути адресований Замовнику даних торгів з зазначенням номеру оголошення в центральній базі даних (ЦБД) системи Prozorro.

* 1. Вимоги до режиму роботи персоналу

Режим роботи персоналу має відповідати затвердженим графікам роботи функціональних підрозділів установи Замовника та нормам встановленим трудовим законодавством України. В разі необхідності має бути передбачений позмінний графік роботи та ненормований робочий день.

*У разі, якщо в Технічному завданні міститься посилання на конкретні торгівельну марку чи фірму, патент, конструкцію або тип предмета закупівлі або виробника, мається на увазі «або еквівалент».*