Міністерство охорони здоров'я України
Проект № 8475-UA
"Поліпшення охорони здоров'я на службі у людей"

ЗАПРОШЕННЯ ДО ПОДАННЯ ЦІНОВИХ ПРОПОЗИЦІЙ
за пакетом № SH-5.23
«Серверне обладнання для НУОЗ України ім. П.Л. Шупика»

1. Уряд України одержав позику Міжнародного банку реконструкції та розвитку (далі - Банк) № 8475-UA на фінансування проекту «Поліпшення охорони здоров'я на службі у людей» (далі – Проект). Частина коштів цієї Позики має бути використана для покриття витрат в рамках договору, до якого відноситься це запрошення до подання цінових пропозицій (далі – Запрошення).
2. Міністерство охорони здоров'я України (далі – Замовник) цим листом запрошує правомочних учасників торгів (тобто учасників, товари та/або програмне забезпечення, які вони пропонують, не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України) надіслати цінові пропозиції щодо постачання наступних товарів: сервер тип 1 у форм-факторі Rackmount – 1 шт., сервер тип 2 у форм-факторі Rackmount – 1 шт., сервер тип 3 у форм-факторі Rackmount – 1 шт., система зберігання даних у форм-факторі Rackmount у комплекті – 1 шт., комутатор оптичний, рівня ядра, з можливістю об'єднання в стек – 2 шт., серверна шафа – 1 шт., програмно-апаратний комплекс (ПАК) для захисту мережі та системи керування – 2 шт., джерело безперебійного живлення (ДБЖ) – 2 шт.

   Інформація щодо Технічних вимог та необхідних кількостей вказана в Додатках.

3. Учасник подає лише одну цінову пропозицію. Всі пропозиції учасника, який надав більше одної цінової пропозиції, будуть відхилені. Пропозиції мають бути повними (включати усі позиції) відповідно до цього Запрошення. Неповні пропозиції будуть відхилені. Цінові пропозиції оцінюватимуться за всіма позиціями та договір буде присуджено фірмі, яка запропонувала найменшу оцінену вартість всіх позицій та відповідає усім умовам, встановленим цим Запрошенням та Технічними вимогами до нього. Замовник не розглядає жодних цінових пропозицій, які надходять після кінцевого терміну подання конкурсних пропозицій, встановленого в п. 5 даного Запрошення. Пропозиції, отриманні Замовником після кінцевого терміну подання цінових пропозицій, будуть оголошені такими, що надійшли із запізненням, та відхилені.

4. Цінова пропозиція українською мовою за формою, наведеною у Додатку 3 «Цінова пропозиція» в сканованому вигляді разом з додатковою інформацією мають надсилатися за наступною електронною адресою:

   Міністерство охорони здоров'я України
   Офіс Групи консультаційної підтримки Проекту (ГКПП)
   Ел. пошта: oszhyganov@gmail.com, **обов'язкова копія** на m.k.dymytrenko@moz.gov.ua.
   В полі «Тема» ел. повідомлення **обов'язково зазначити «Пакет № SH-5.23».**
   Також за зверненням за вищевказаною адресою зацікавленими учасниками може бути отримана довідкова інформація. Запити на додаткову інформацію мають бути надіслані не пізніше, ніж за 3 доби до кінцевого терміну отримання пропозицій, встановленого в п. 5 даного Запрошення. Після настання цього терміну запити на додаткову інформацію чи роз'яснення не приймаються. Процедура розкриття для цієї закупівлі не передбачається.

5. Кінцевим терміном для отримання пропозицій Замовником за адресою вказаною в п. 4 вище встановлюється: **21 лютого 2024 року, 17:00 за місцевим часом**.

6. До своїх пропозицій Ви маєте додати відповідну документацію, що вимагається Технічними вимогами.

7. Проведення цієї закупівлі здійснюється у відповідності до процедури «Закупівля товарів у вільній торгівлі» (шопінг) «Посібника з питань закупівель у рамках позик МБРР та кредитів МАР» в редакції від травня 2011 року ("Посібник із закупівлі товарів"), в якому визначається політика Світового Банку щодо конфлікту інтересів.

   Будь ласка, надайте Ваші цінові пропозиції відповідно до інструкцій у Запрошенні та Договору, що додається. «Умови надання послуг» та «Технічні вимоги», що додаються, є складовою частиною Договору.

   (i) ЦІНИ. Ціни мають бути виражені в будь-якій валюті, включати ціну товарів у Місцях призначення, вказаних у Додатку 1 «Умови постачання», та включати усі обов'язкові платежі (податки, мито, тощо), та вартість додаткових та інших послуг, як зазначено у вищезгаданому Додатку.

   (ii) ОЦІНКА ПРОПОЗИЦІЙ. Пропозиції, які визнані такими, що задовольняють Технічним вимогам та Запрошення, оцінюватимуться шляхом порівняння загальної ціни відповідно до встановлених вимог, як вказано в п. (i) вище. У випадку подання цінових пропозицій у іншій валюті, з метою порівняння, Замовник конвертує всі ціни у валюту країни Замовника (українська гривня) по обмінному курсу продажу, опублікованому Національним банком України (https://bank.gov.ua/ua/markets/exchangerates) на дату кінцевого терміну отримання пропозицій, встановленого в п. 5 даного Запрошення.

   При оцінці пропозицій, Замовник визначить для кожної цінової пропозиції оціночну вартість шляхом коригування цінової пропозиції з метою виправлення арифметичних помилок таким чином:

   а) якщо у будь-якому місці є невідповідність між сумою цифрами та прописом, сума прописом буде вважатися вірною;

   б) якщо у будь-якому місці є невідповідність між ціною за одиницю та загальною сумою, яка обчислюється шляхом перемноження ціни за одиницю на кількість, ціна за одиницю буде вважатися вірною;

   в) якщо Постачальник відмовиться прийняти вказані корегування, його цінова пропозиція буде відхилена.

   (iii) ПРИСУДЖЕННЯ ДОГОВОРУ. Договір присуджуватиметься учаснику, який запропонує найнижчу загальну ціну, та пропозиція якого відповідає умовам, встановленими Технічними вимогами та Запрошення. З обраним Постачальником буде укладено договір за формою, наведеною у Додатку 4 «Договір».

   (iv) ТЕРМІН ЧИННОСТІ ПРОПОЗИЦІЙ: запропоновані цінові пропозиції повинні бути чинними протягом 45 (сорока п'яти) календарних днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 даного Запрошення.

8. **ПЕРЕВІРКИ ТА АУДИТ**

   Постачальник повинен виконувати всі вказівки Замовника, які відповідають застосованому законодавству країни Замовника.

   Постачальник повинен дозволяти, та забезпечити дозвіл всіх своїх підрядників та консультантів, на перевірку Банком та/або особами призначеними Банком всіх офісів Постачальника та всіх рахунків та документів, пов'язаних з впровадженням Договору та підготовкою цінової пропозиції, та дозволяти перевірку цих рахунків та документів аудитором, призначеним Банком, якщо це вимагатиме Банк. Увага Постачальника та

його підрядників та консультантів звертається на статтю 5 «Шахрайство та корупція» Форми Договору, яка передбачає, серед іншого, що дії спрямовані на суттєве перешкоджання реалізації Банком його прав щодо перевірок та аудиту, становлять заборонену практику, яка може бути підставою для розірвання Договору (а також визнання Постачальника неправомочним відповідно до процедур Світового Банку щодо застосування санкцій).

9. **Будь ласка, надайте письмове підтвердження (електронною поштою) отримання цього Запрошення та Вашої участі у торгах.**

Додатки:

Додаток 1. Умови надання послуг
Додаток 2. Технічні вимоги
Додаток 3. Цінова пропозиція
Додаток 4. Договір

ДОДАТОК 1

до Запрошення до подання цінових пропозицій № SH-5.23

УМОВИ ПОСТАЧАННЯ

Назва пакету: «Серверне обладнання для НУОЗ України ім. П.Л. Шупика»
Номер пакету: SH-5.23
Покупець: Міністерство охорони здоров'я України

1. Ціна пропозиції

№	Опис	Кільк., шт.	Ціна за одиницю [вказати валюту], включаючи усі податки, митні збори, доставку, завантаження, розвантаження, додаткові послуги без ПДВ	Загальна ціна [вказати валюту], без ПДВ
1.	Сервер тип 1 у форм-факторі Rackmount [вказати виробника, модель]	1		
2.	Сервер тип 2 у форм-факторі Rackmount [вказати виробника, модель]	1		
3.	Сервер тип 3 у форм-факторі Rackmount [вказати виробника, модель]	1		
4.	Система зберігання даних у форм-факторі Rackmount у комплекті [вказати виробника, модель]	1		
5.	Комутатор оптичний, рівня ядра, з можливістю об'єднання в стек [вказати виробника, модель]	2		
6.	Серверна шафа [вказати виробника, модель]	1		
7.	Програмно-апаратний комплекс (ПАК) для захисту мережі та системи керування [вказати виробника, модель]	2		
8.	Джерело безперебійного живлення (ДБЖ) [вказати виробника, модель]	2		
ЗАГАЛЬНА ЦІНА **ПРОПОЗИЦІЇ** БЕЗ ПДВ				
ПДВ				
ЗАГАЛЬНА ЦІНА **ПРОПОЗИЦІЇ** З ПДВ				

Примітка 1: у разі розбіжності між сумою, підрахованою шляхом перемноження ціни за одиницю на кількість, та загальною ціною, підрахованою учасником торгів, чинною вважається загальна ціна, вирахувана на основі цін за одиницю.

2. Термін чинності цінової пропозиції

Запропонована цінова пропозиція є чинною протягом сорока п'яти (45) днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 Запрошення до подання цінових пропозицій.

3. Фіксована ціна

Наведені вище ціни є фіксованими, включають усі податки, митні збори, доставку, завантаження, розвантаження, додаткові послуги до м. Київ, вул. Дорогожицька, 9 і жодним змінам не підлягають, включаючи період виконання Договору.

4. Право Покупця змінювати кількість товарів під час присудження Договору

Покупець залишає за собою право під час присудження Договору збільшувати або зменшувати на 1-15% кількість товарів, визначених у «Запрошенні до подання цінових пропозицій» за умови, що не вноситься будь-яких змін до одиничних цін та інших умов постачання товарів.

5. Терміни та умови постачання

Постачання товарів разом із відповідними документацією та інструкціями з експлуатації та додатковими послугами (згідно з Технічними Вимогами, що додаються) має бути здійснено протягом 14 (чотирнадцяти) календарних днів від дати підписання Договору.

6. Оплата

Сто відсотків (100%) загальної ціни поставлених Товарів буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та видаткової накладної, підписаної Покупцем, після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань.

У разі відмінності валюти цінової пропозиції від української гривні – оплата буде здійснюватись в українській гривні за офіційним курсом Національного банку України на день підписання Покупцем видаткової накладної.

7. Гарантійні зобов'язання

Поставлені товари повинні мати гарантію Постачальника не менше, ніж строк, передбачений у Додатку № 2 «Технічні вимоги». Постачальник надає Покупцю гарантійні документи на товари разом з рахунком до сплати та видатковою накладною.

Протягом гарантійного періоду усі дефекти мають бути виправлені Постачальником без жодних витрат для Покупця не пізніше ніж через 30 днів з дати отримання повідомлення від Покупця.

8. Наслідки невиконання договору Постачальником

Покупець має право розірвати Договір без будь-яких зобов'язань перед Постачальником в разі невиконання поставки Товарів згідно наведених умов через 21 день після відповідного письмового повідомлення Покупцем.

За порушення строків поставки Товарів з Постачальника стягується неустойка у розмірі 0,2% від вартості Товарів, щодо яких допущено прострочення, за кожен календарний день прострочення. Неустойка, що стягується, не має перевищувати 10% вартості недопоставлених у строк Товарів.

9. Технічні вимоги

Наведені у Додатку 2 до Запрошення до подання цінових пропозицій. Постачальник має підтвердити відповідність запропонованих товарів специфікаціям по кожній позиції або навести усі розбіжності.

10. Інструкції з пакування та маркування

Постачальник має виконати стандартне пакування Товарів як вимагається для запобігання їх пошкодження чи порчі протягом транспортування до місця призначення як це вказано у Договорі.

11. Дефекти та недоліки

Усі дефекти та недоліки має бути виправлено Постачальником без будь-яких витрат з боку Покупця протягом 30 днів з дати повідомлення Покупцем про них.

[НАЗВА ВИКОНАВЦЯ]
Підпис уповноваженої особи:
Печатка компанії
Місце:
Дата:

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК 2

до Запрошення до подання цінових пропозицій № SH-5.23

ТЕХНІЧНІ ВИМОГИ

Назва пакету: «Серверне обладнання для НУОЗ України ім. П.Л. Шупика»
Номер пакету: SH-5.23
Покупець: Міністерство охорони здоров'я України

ЗАГАЛЬНІ ВИМОГИ

(i) Усі Товари повинні бути поставлені в заводській упаковці, разом з усіма кабелями живлення та необхідними з'єднувальними кабелями для роботи в об'єднанні одних товарів з іншими, під'єднання одних компонентів до інших та інструкціями по обслуговуванню та драйверами.

(ii) Прийнятними вважаються будь-які товари, які забезпечують параметри, визначені в Технічних вимогах.

(iii) Товар, що є предметом закупівлі, має бути оригінальним, новим, таким що не було у вжитку, не відновленим і не зібраним з відновлених компонентів, працездатним і забезпечувати передбачену виробником функціональність.

(iv) Товар, що є предметом закупівлі, включаючи всі компоненти, що входять до його складу (пам'ять, процесори, накопичувачі, адаптери, блоки живлення), повинні бути встановлені і зібрані в готовий виріб.

(v) Якість Товару повинна відповідати державним стандартам, технічним регламентам та законодавству щодо показників якості такого роду/виду товарів, а також має бути засвідчено його якість належними підтверджувальними документами, дійсними на момент поставки Товару.

(vi) Товар повинен відповідати вимогам охорони праці, екології (захисту довкілля) та пожежної безпеки. Також Товар повинен мати високу якість матеріалів, використаних для його виготовлення, бездоганну обробку, високу якість технічного виконання.

Для підтвердження відповідності технічним, якісним та кількісним характеристикам предмету закупівлі Учасник додатково подає (у формі сканованих копій) такі документи:

а) лист від виробника обладнання (сервера, системи збереження даних, комутаторів, точок доступу, мережевих екранів, джерела безперебійного живлення), або його офіційного представника\цтва в Україні, з зазначенням торгової марки запропонованого товару, найменування, моделі, підтвердженням технічних характеристик, які зазначені Учасником в таблиці відповідності, можливості легітимної поставки товару в необхідній кількості, підтвердженням стандартних гарантійних зобов'язань виробника щодо запропонованого товару, підтвердженням права Учасника на продаж запропонованих товарів на території України.

б) гарантійний лист у довільній формі за власноручним підписом уповноваженої особи Учасника та завірений печаткою (у разі її використання) в якому він повинен підтвердити надання гарантії на запропоноване обладнання не менше ніж зазначено Замовником у технічних вимогах до предмета закупівлі.

ВАЖЛИВО:

Технічні специфікації вказані в колонці «Технічні вимоги Покупця» є **мінімально** необхідними.

Учасник торгів має заповнити колонку «Відповідність та опис запропонованих товарів» по кожному запропонованому товару, а також обов'язково зазначити виробника та модель товарів, які він пропонує. На підтвердження відповідності запропонованого обладнання (сервера, системи збереження даних, комутаторів, точок доступу, мережевих екранів, джерела безперебійного живлення) технічним вимогам надати детальну заповнену технічну специфікацію (таблицю відповідності) із зазначенням країни походження та повної характеристики і назви товару, що пропонується у складі пропозиції. **Якщо запропоноване обладнання не відповідає технічним вимогам Покупця в повному обсязі, в колонці напроти відповідного товару мають зазначатися розбіжності по кожному пункту**.

ДЕТАЛЬНІ ВИМОГИ

Характеристика	Технічні вимоги Покупця	**Відповідність та опис запропонованих товарів** [по-позиційно вказати відповідність (так/ні), та навести детальний опис параметру]
1. Сервер тип 1 у форм-факторі Rackmount		[вказати виробника, модель]
Загальні вимоги	- форм фактор серверу для встановлення у стандартну серверну шафу 19 дюймів; - висота серверу не більше 2U стандартної 19 дюймової серверної шафи; - наявність телескопічних рейок кріплення для установки в шафу; - наявність організатору кабеля.	
Процесор	- наявність встановлених не менше двох фізичних процесорів, з базовою тактовою частотою не менше 2.6 ГГц, з не менше ніж 18 ядрами (не менш ніж 36 потоками) та кеш-пам'яттю не менше 24 МБ, на кожний процесор; - максимальна частота одного ядра при використанні технології Turbo Boost Technology(або аналогічної), не нижче ніж 3.9 ГГц; - обов'язкова підтримка таких технологій та інструкцій, як VT-x/VT-d, AVX, AVX2, AVX-512.	
Налаштування продуктивності	- сервер повинен підтримувати та мати вибір з передконфігурованих профілів навантаження для простої оптимізації продуктивності під різні обчислювальні задачі, та можливість зміни та їх модифікації, в разі необхідності перепрофілювання серверу під інші задачі.	
Оперативна пам'ять	- наявність встановленої не менше 256 ГБ та не гірше ніж Registered DDR4-2993MT/c; - весь об'єм пам'яті повинен бути встановлено модулями не більше за 64 ГБ кожний; - повинні бути наявні не менше 20 вільних слотів для швидкого розширення об'єму пам'яті без необхідності заміни наявних модулів;	

	- наявність можливості збільшення максимального об’єму пам’яті до не менше 2 ТБ (можливо з заміною встановлених модулів пам’яті); - усі модулі пам'яті повинні бути від виробника серверу (рекомендовані виробником) та мати відповідне маркування, якщо таке передбачено у виробника; - наявність забезпечення виявлення одно- та багатобітових помилок в пам’яті та виправлення однобітових помилок (ECC); - наявність забезпечення виправлення багатобітових помилок у мікросхемі модуля пам’яті або виходу її з ладу (Advanced ECC/SDDC), наявність можливості роботи в режимі виправлення багатобітових помилок у двох мікросхемах модуля пам’яті або виходу їх з ладу (DDDC); - підтримка дзеркалювання пам’яті, як повного, так і часткового (дзеркалювання окремих зон); - наявність можливості регулярного контрольного автоматичного зчитування блоків пам’яті для запобіганню накопиченню виправлених помилок і запис виправлених даних у разі виникнення помилки.	
Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження)	- наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокоду процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера; - наявність окремого захищеного внутрішнього депозиторію базових мікрокодів, для відновлення в разі визначення пошкодження або несанкціонованої модифікації мікрокодів сервера; - наявність підтримки механізму захищеного завантаження операційної системи.	
Дискові контролери	Має бути встановлено апаратний контролер, що може працювати як внутрішній HBA та віддавати ОС кожен накопичувач як фізичний диск, а також підтримувати побудову наступних рівнів RAID 0, 1, 5, 6, 10, 50, 60;	

	- кеш пам’ять контролеру не менше 2ГБ з забезпеченням зберігання даних в ній, через наявність батарейного модуля або конденсатора великої ємності; - контролер повинен бути підключеним по інтерфейсу не нижче PCIe Gen 3.0 та не повинен займати класичного слоту розширення PCIe; - підтримка технології 12Gb SAS/ 6Gb SATA; - наявність підтримки «гарячої заміни» дисків; - наявність підтримки оптимізації роботи з SSD дисками; - наявність можливості створення до 64 логічних дисків.	
Дискова підсистема	- повинно бути встановлено не менше двох (2) накопичувачів, що підтримують «гарячу заміну» типу 2.5” Mixed Use SSD з DWPD не нижче ніж 3.0 та об’ємом не менше 3.84ТБ кожний; - повинна бути наявна можливість розширення загальної кількості 2.5” SAS/SATA накопичувачів, що підключені до одного апаратного дискового контролеру, до не менше восьми (8) штук, лише додаванням самих дисків. - усі накопичувачі повинні бути від виробника серверу (рекомендовані виробником) та мати відповідне маркування, якщо таке передбачено у виробника.	
Мережеві адаптери	- наявність не менше одного мережевого адаптера, який повинен мати не менше двох портів зі швидкістю 1Гбіт/с з інтерфейсом RJ-45; - наявність не менше двох мережевих адаптерів, кожен з яких повинен мати не менше двох портів зі швидкістю 10/25Гбіт/с з інтерфейсом SFP28 з кожен з 2 (двома) встановленими оптичними модулями 10Gb SFP+ SR. - наявність не менше одного двохпортового 16Гбіт/с fibre channel адаптера зі встановленими двома оптичними модулями 16Gb SFP+ SW.	
Порти в сервері	- загальна кількість портів USB 3.0 не менше 5 (п’яти). Мають бути наявні не менше двох захищених внутрішніх	

	портів USB (з загальної кількості портів) без доступу з зовні серверу; - наявність відео (VGA) порту; - наявність можливості встановлення послідовного порту (роз'єм DB9). - повинна бути можливість управління сервером не лише через окремий Ethernet порт, що знаходиться на задній частині серверу, а й через окремий USB порт, що розташований на передній частині серверу, та має бути реалізовано через відповідний адаптер, що може бути придбано пізніше, окремо, в разі виникнення такої необхідності.	
Відеопідсистема	- будь яка з підтримкою максимальної роздільної здатності не нижче 1920 х 1200 та частотою не нижче 60Гц.	
Блоки живлення	- повинно бути встановлено не менше двох блоків живлення; - потужність кожного блоку живлення не менше 800 Вт, з підтримкою «гарячої заміни», напруга ~220В 1 фазні, частота 50 Гц; - повинна бути забезпечена відмовостійкість не гірше ніж 1+1; - енергоефективність блоків живлення не менше ніж 94% при напрузі живлення 230В; - наявність двох кабелів живлення в комплекті.	
Система охолодження	- повинно бути встановлено повний комплект вентиляторів охолодження для запропонованої конфігурації серверу; - повинно бути забезпечено відмовостійкість вентиляторів N+1, де N більше ніж 1.	
Гіпервізори та операційні системи, що підтримуються	- наявність ліцензії Microsoft Windows Server 2022 Standard на всі потужності сервера; - підтримка Red Hat Enterprise Linux 8.x, 9.x - підтримка SUSE Linux Enterprise Server 15. - підтримка VMware vSphere 7.0 U3, 8.0, 8.0 U1, 8.0 U2. (сервер повинен мати офіційну підтримку виробника та сертифікацію на веб-сайті VMware: https://www.vmware.com/resources/compatibility/search.php)	

	- обов’язкова наявність сертифікації серверу під власною торговою маркою (сертифікація лише платформи неприйнятна).	
Функції керування	- наявність вбудованого програмного забезпечення для віддаленого керування сервером з відповідними ліцензіями на весь термін дії гарантії серверу. - наявність вбудованих в сервер процесора з окремим мережевим портом 1Гбіт: - збирання статистики з сервера, - відслідковування його електроживлення та температури, стан компонентів сервера як до, так і після завантаження операційної системи (без необхідності встановлення агентів в операційній системі), - call-home (самостійний зв’язок з сайтом підтримки для автоматичних повідомлень про стан, зміну конфігурації, вихід з ладу), - завантаження сервера для конфігурування, розгортання та встановлення сумісної операційної системи без встановлення в сервер або віддаленого підключення додаткових медіа носіїв. - наявність віртуальної консолі з функціоналом: - доступу до графічної консолі сервера через браузер, та до текстової консолі через термінальний емулятор, - збереження виводу графічної консолі та текстового виводу текстової консолі з функцією відтворення для діагностування, - підключення до сервера локальних носіїв інформації станції керування (як фізичних носіїв, так і образів CD/DVD або каталогів файлової системи). - наявність захищеного зв’язку с процесором керування з використанням SSL, AES, 3DES, сертифікатів. Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження):	

	- всі мікрокоди повинні мати цифровий підпис виробника, - наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокода процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера, - наявність окремого захищеного внутрішнього депозиторія базових мікрокодів, для відновлення в разі визначення пошкодження або несанкціованої модифікації мікрокодів, - повинна бути підтримка механізму захищеного завантаження операційної системи. Має підтримувати керування кількома серверами як одним через - груповий контроль живлення, - групове обмеження потужності, - групове оновлення мікрокодів, - конфігурацію групи, - групування віртуальних носіїв та зашифрованих віртуальних носіїв. Сервер повинен мати інформаційну панель безпеки, що відображає статус важливих функцій безпеки, загальний стан безпеки системи та поточну конфігурацію для функцій стану безпеки та блокування конфігурації сервера. Повинна бути функція безпечного стирання даних пристрою однією кнопкою, що призначена для виведення з експлуатації/перепрофілювання серверу.	
Забезпечення керування апаратною інфраструктурою з наступними параметрами	- наявність єдиної панелі керування ресурсами запропонованого серверного обладнання, - панель стану, з підтримкою швидкого сканування керованих ресурсів, яка демонструє загальний стан обладнання, вона повинна візуалізовувати сумарний стан обладнання авторизованого для спостерігання користувачем: - стан керованих ресурсів повинен відображатися кольором, зеленим для штатного функціонування, жовтим для стану, який вимагає уваги, червоним для критичного стану, індикатор ресурсу повинен бути пов’язаний з	

	інтерфейсом керування ресурсу для одержання додаткової інформації простим вибором індикатора курсору. - вигляд карти, яка візуалізує взаємодію між керованими ресурсами - вигляд активностей, з історією стану ресурсів - наявність функціональності створення серверних профілів, з такими параметрами як: - версії мікрокоду - налаштування BIOS - параметри завантаження - налаштування процесора керування сервера. - наявність централізованого керування мікрокодами обладнання з порівнянням встановлених версій з рекомендованими, для забезпечення підтримуваного рівня встановлених мікрокодів - функціональність створення локальної бібліотеки мікрокодів з завантаженням потрібних версій з веб сайта виробника і автоматизованим оновленням мікрокодів керованого обладнання - наявність екрану термічного стану всього керованого обладнання з урахуванням його просторового розміщення в шафі/комп'ютерному залі, для легкої ідентифікації гарячих точок в конкретній шафі - візуалізація як актуального енергоспоживання і актуальної температури, так і історичних даних та тенденцій і генерація детальних звітів - підтримка автоматичного визначення просторового розміщення обладнання - наявність функціональності збирання і зберігання інформації по утилізації процесорів в керованих серверах - підтримка видачі і збирання даних за допомогою REST API - наявність функціональності розгортання операційних систем Windows, Linux та ESXi для зменшення часу необхідного для запуску - наявність функціональності розгортання операційних систем на багатьох серверах одночасно та розгортання операційних систем за розкладом	

	- можливість конфігурування обладнання та зміни параметрів обладнання під час розгортання операційної системи, а також можливість запису параметрів серверів і відтворення їх на інших серверах - підтримка моделі ресурсів з використанням розширюваного HTML5 інтерфейсу і стандартних в індустрії REST API, для забезпечення керування запропонованими серверною інфраструктурою з власних консолей додатків, щонайменше таких як VMware vCenter Server, Microsoft System Center. Наявність Zero Touch Provisioning (ZTP) за допомогою Simple Service Discovery Protocol (SSDP) з можливістю віддаленого доступу. Повинна бути інформаційна панель для інформування, щодо базових версій мікрокодів, що здійснюється під час виконання перевірки на мінімально допустиму версію мікрокоду та виділення компонент, які не відповідають вимогам, для оновлення із обраної базової версії мікрокодів.	
Термін гарантії та сервісної підтримки	- не менше 36 місяців з дати придбання (весь термін гарантії має бути від виробника серверу); - цілодобовий доступ до засобів для самостійного усунення несправностей, доступ до відео з технічними порадами від експертів, щодо найкращих практик, а також цілодобовий доступ для можливості реєстрації сервісної заявки; - час реакції по телефону не більше ніж 3 години з моменту реєстрації сервісного запиту в рамках робочих годин, не гірше ніж 9x5 (9:00-18:00, Пн.-Пт. за виключенням святкових та вихідних днів), виконання робіт по гарантійному обслуговуванню, в робочі години, з понеділка по п’ятницю (за виключенням святкових та вихідних днів), з прибуттям сервісного інженера на місце розташування обладнання, в разі необхідності; - гарантія повинна включати доступ до оновлень мікрокодів обладнання, а також віддалену діагностику і підтримку з боку центру технічної підтримки виробника;	

	- повинна бути можливість цілодобово відкривати сервісні заявки за телефоном гарячої лінії 0-800-ххх-ххх та електронною поштою; - повинна бути обов'язково запропонована можливість автоматичного відкриття заявок, щодо сервісних випадків.	
Додаткові можливості, щодо сервісної підтримки	В період дії технічної підтримки, повинен бути запропонований та наданий безкоштовний цілодобовий безперешкодний доступ до захищеного хмарного порталу, що базується на використанні технологій машинного навчання та розташований на ресурсах виробника обладнання, що пропонується. Замовник повинен мати можливість розмежувати права доступу на портал до інформації щодо обладнання: лише для читання, надати доступ для свого сервісного партнеру, повний доступ для адміністратору. Щонайменше портал повинен мати наступний функціонал: - можливість відслідковування стану гарантії; - можливість відслідковування стану серверу (включений чи виключений); - відслідковування стану «здоров'я серверу», з можливою зміною статусу не пізніше ніж один раз на добу; - можливість отримання на електронну пошту листа з інформацією, щодо зміни «здоров'я серверу»; - можливість автоматичного відкриття сервісних заявок, щодо гарантійних випадків; - інформацію про актуальність мікрокодів серверу. В разі, якщо даний функціонал платний, то його вартість повинна бути включена в пропозицію. Сервер та всі його компоненти повинні бути від одного виробника, новими, такими, що не були в експлуатації та мати відповідне маркування, в разі якщо таке передбачено виробником.	
Додаткові відомості	Сервер, що пропонується, повинен бути від виробника, що раніше не знаходився та й не знаходиться зараз, під санкціями країн-постачальників основних компонент (наприклад, ASIC,	

	процесорів тощо) або повністю готових виробів.	
2. Сервер тип 2 у форм-факторі Rackmount		[вказати виробника, модель]
Загальні вимоги	- форм фактор серверу для встановлення у стандартну серверну шафу 19 дюймів; - висота серверу не більше 1U стандартної 19 дюймової серверної шафи; - наявність телескопічних рейок кріплення для установки в шафу.	
Процесор	- наявність встановленого не менше одного фізичного процесору, з базовою тактовою частотою не менше 3.6 ГГц, з не менше ніж 8 ядрами (не менш ніж 16 потоками) та кеш-пам'яттю не менше 24 МБ; - можливість додавання другого процесору у майбутньому; - максимальна частота одного ядра при використанні технології Turbo Boost Technology(або аналогічної), не нижче ніж 4.4 ГГц; обов'язкова підтримка таких технологій та інструкцій, як VT-x/VT-d, AVX, AVX2, AVX-512.	
Налаштування продуктивності	- сервер повинен підтримувати та мати вибір з передконфігурованих профілів навантаження для простої оптимізації продуктивності під різні обчислювальні задачі, та можливість зміни та їх модифікації, в разі необхідності перепрофілювання серверу під інші задачі.	
Оперативна пам'ять	- наявність встановленої не менше 64 ГБ та не гірше ніж Registered DDR4-2993MT/c; - весь об'єм пам'яті повинен бути встановлено модулями не більше за 32 ГБ кожний; - повинні бути наявні не менше 22 вільних слотів для швидкого розширення об'єму пам'яті без необхідності заміни наявних модулів; - наявність можливості збільшення максимального об'єму пам'яті до не менше 2 ТБ (можливо з заміною встановлених модулів пам'яті й додаванням другого процесору); - усі модулі пам'яті повинні бути від виробника серверу (рекомендовані	

	виробником) та мати відповідне маркування, якщо таке передбачено у виробника; - наявність забезпечення виявлення одно- та багатобітових помилок в пам'яті та виправлення однобітових помилок (ECC); - наявність забезпечення виправлення багатобітових помилок у мікросхемі модуля пам'яті або виходу її з ладу (Advanced ECC/SDDC), наявність можливості роботи в режимі виправлення багатобітових помилок у двох мікросхемах модуля пам'яті або виходу їх з ладу (DDDC); - підтримка дзеркалювання пам'яті, як повного, так і часткового (дзеркалювання окремих зон); - наявність можливості регулярного контрольного автоматичного зчитування блоків пам'яті для запобіганню накопиченню виправлених помилок і запис виправлених даних у разі виникнення помилки.	
Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження)	- наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокоду процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера; - наявність окремого захищеного внутрішнього депозиторію базових мікрокодів, для відновлення в разі визначення пошкодження або несанкціонованої модифікації мікрокодів сервера; - наявність підтримки механізму захищеного завантаження операційної системи.	
Дискові контролери	Має бути встановлено апаратний контролер, що може працювати як внутрішній HBA та віддавати ОС кожен накопичувач як фізичний диск, а також підтримувати побудову наступних рівнів RAID 0, 1, 5, 6, 10, 50, 60; - кеш пам'ять контролеру не менше 2ГБ з забезпеченням зберігання даних в ній, через наявність батарейного модуля або конденсатора великої ємності; - контролер повинен бути підключеним по інтерфейсу не нижче PCIe Gen 3.0 та	

	не повинен займати класичного слоту розширення PCIe; - підтримка технології 12Gb SAS/ 6Gb SATA; - наявність підтримки «гарячої заміни» дисків; - наявність підтримки оптимізації роботи з SSD дисками; - наявність можливості створення до 64 логічних дисків.	
Дискова підсистема	- повинно бути встановлено не менше двох (2) накопичувачів, що підтримують «гарячу заміну» типу 2.5” Read Intensive SSD з DWPD не нижче ніж 0.8 та об’ємом не менше 960ГБ кожний; - повинна бути наявна можливість розширення загальної кількості 2.5” SAS/SATA накопичувачів, що підключені до одного апаратного дискового контролеру, до не менше восьми (8) штук, лише додаванням самих дисків. - усі накопичувачі повинні бути від виробника серверу (рекомендовані виробником) та мати відповідне маркування, якщо таке передбачено у виробника.	
Мережеві адаптери	- наявність не менше одного мережевого адаптера, який повинен мати не менше чотирьох портів зі швидкістю 1Гбіт/с з інтерфейсом RJ-45; - наявність не менше одного двохпортового 16Гбіт/с fibre channel адаптера зі встановленими двома оптичними модулями 16Gb SFP+ SW.	
Порти в сервері	- загальна кількість портів USB 3.0 не менше 5 (п’яти). Мають бути наявні не менше двох захищених внутрішніх портів USB (з загальної кількості портів) без доступу з зовні серверу; - наявність відео (VGA) порту; - наявність можливості встановлення послідовного порту (роз’єм DB9). - повинна бути можливість управління сервером не лише через окремий Ethernet порт, що знаходиться на задній частині серверу, а й через окремий USB порт, що розташований на передній частині серверу, та має бути реалізовано через відповідний адаптер, що може	

	бути придбано пізніше, окремо, в разі виникнення такої необхідності.	
Відеопідсистема	- будь яка з підтримкою максимальної роздільної здатності не нижче 1920 х 1200 та частотою не нижче 60Гц.	
Блоки живлення	- повинно бути встановлено не менше двох блоків живлення; - потужність кожного блоку живлення не менше 800 Вт, з підтримкою «гарячої заміни», напруга ~220В 1 фазні, частота 50 Гц; - повинна бути забезпечена відмовостійкість не гірше ніж 1+1; - енергоефективність блоків живлення не менше ніж 94% при напрузі живлення 230В; - наявність двох кабелів живлення в комплекті.	
Система охолодження	- повинно бути встановлено повний комплект вентиляторів охолодження для запропонованої конфігурації серверу; - повинно бути забезпечено відмовостійкість вентиляторів N+1, де N більше ніж 1.	
Гіпервізори та операційні системи, що підтримуються	- наявність ліцензії Microsoft Windows Server 2022 Standard на всі потужності сервера; - підтримка Red Hat Enterprise Linux 8.x, 9.x - підтримка SUSE Linux Enterprise Server 15. - підтримка VMware vSphere 7.0 U3, 8.0, 8.0 U1, 8.0 U2. (сервер повинен мати офіційну підтримку виробника та сертифікацію на веб-сайті VMware: https://www.vmware.com/resources/compatibility/search.php) Обов'язкова наявність сертифікації серверу під власною торговою маркою (сертифікація лише платформи неприйнятна).	
Функції керування	- наявність вбудованого програмного забезпечення для віддаленого керування сервером з відповідними ліцензіями на весь термін дії гарантії серверу. - наявність вбудованих в сервер процесора з окремим мережевим портом 1Гбіт: - збирання статистики з сервера,	

	- відслідковування його електроживлення та температури, стан компонентів сервера як до, так і після завантаження операційної системи (без необхідності встановлення агентів в операційній системі), - call-home (самостійний зв'язок з сайтом підтримки для автоматичних повідомлень про стан, зміну конфігурації, вихід з ладу), - завантаження сервера для конфігурування, розгортання та встановлення сумісної операційної системи без встановлення в сервер або віддаленого підключення додаткових медіа носіїв. - наявність віртуальної консолі з функціоналом: - доступу до графічної консолі сервера через браузер, та до текстової консолі через термінальний емулятор, - збереження виводу графічної консолі та текстового виводу текстової консолі з функцією відтворення для діагностування, - підключення до сервера локальних носіїв інформації станції керування (як фізичних носіїв, так і образів CD/DVD або каталогів файлової системи). - наявність захищеного зв'язку с процесором керування з використанням SSL, AES, 3DES, сертифікатів. Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження): - всі мікрокоди повинні мати цифровий підпис виробника, - наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокода процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера, - наявність окремого захищеного внутрішнього депозиторія базових мікрокодів, для відновлення в разі визначення пошкодження або	

	несанкціованої модифікації мікрокодів, - повинна бути підтримка механізму захищеного завантаження операційної системи. Має підтримувати керування кількома серверами як одним через - груповий контроль живлення, - групове обмеження потужності, - групове оновлення мікрокодів, - конфігурацію групи, - групування віртуальних носіїв та зашифрованих віртуальних носіїв. Сервер повинен мати інформаційну панель безпеки, що відображає статус важливих функцій безпеки, загальний стан безпеки системи та поточну конфігурацію для функцій стану безпеки та блокування конфігурації сервера. Повинна бути функція безпечного стирання даних пристрою однією кнопкою, що призначена для виведення з експлуатації/перепрофілювання серверу.	
Термін гарантії та сервісної підтримки	- не менше 36 місяців з дати придбання (весь термін гарантії має бути від виробника серверу); - цілодобовий доступ до засобів для самостійного усунення несправностей, доступ до відео з технічними порадами від експертів, щодо найкращих практик, а також цілодобовий доступ для можливості реєстрації сервісної заявки; - час реакції по телефону не більше ніж 3 години з моменту реєстрації сервісного запиту в рамках робочих годин, не гірше ніж 9x5 (9:00-18:00, Пн.-Пт. за виключенням святкових та вихідних днів), виконання робіт по гарантійному обслуговуванню, в робочі години, з понеділка по п’ятницю (за виключенням святкових та вихідних днів), з прибуттям сервісного інженера на місце розташування обладнання, в разі необхідності; - гарантія повинна включати доступ до оновлень мікрокодів обладнання, а також віддалену діагностику і підтримку з боку центру технічної підтримки виробника; - повинна бути можливість цілодобово відкривати сервісні заявки за телефоном	

	гарячої лінії 0-800-ххх-ххх та електронною поштою; - повинна бути обов'язково запропонована можливість автоматичного відкриття заявок, щодо сервісних випадків.	
Додаткові можливості, щодо сервісної підтримки	В період дії технічної підтримки, повинен бути запропонований та наданий безкоштовний цілодобовий безперешкодний доступ до захищеного хмарного порталу, що базується на використанні технологій машинного навчання та розташований на ресурсах виробника обладнання, що пропонується. Замовник повинен мати можливість розмежувати права доступу на портал до інформації щодо обладнання: лише для читання, надати доступ для свого сервісного партнеру, повний доступ для адміністратору. Щонайменше портал повинен мати наступний функціонал: - можливість відслідковування стану гарантії; - можливість відслідковування стану серверу (включений чи виключений); - відслідковування стану «здоров'я серверу», з можливою зміною статусу не пізніше ніж один раз на добу; - можливість отримання на електронну пошту листа з інформацією, щодо зміни «здоров'я серверу»; - можливість автоматичного відкриття сервісних заявок, щодо гарантійних випадків; - інформацію про актуальність мікрокодів серверу. В разі, якщо даний функціонал платний, то його вартість повинна бути включена в пропозицію. Сервер та всі його компоненти повинні бути від одного виробника, новими, такими, що не були в експлуатації та мати відповідне маркування, в разі якщо таке передбачено виробником.	
Додаткові відомості	Сервер, що пропонується, повинен бути від виробника, що раніше не знаходився та й не знаходиться зараз, під санкціями країн-постачальників основних компонент (наприклад, ASIC, процесорів тощо) або повністю готових виробів.	

3. Сервер Тип 3 у форм-факторі Rackmount		[вказати виробника, модель]
Загальні вимоги	- форм фактор серверу для встановлення у стандартну серверну шафу 19 дюймів; - висота серверу не більше 2U стандартної 19 дюймової серверної шафи; - наявність телескопічних рейок кріплення для установки в шафу.	
Процесор	- наявність встановлених не менше двох фізичних процесорів, з базовою тактовою частотою не менше 2.8 ГГц, з не менше ніж 8 ядрами (не менш ніж 16 потоками) та кеш-пам’яттю не менше 12 МБ, на кожний процесор; - максимальна частота одного ядра при використанні технології Turbo Boost Technology(або аналогічної), не нижче ніж 3.6 ГГц; обов’язкова підтримка таких технологій та інструкцій, як VT-x/VT-d, AVX, AVX2, AVX-512.	
Налаштування продуктивності	- сервер повинен підтримувати та мати вибір з передконфігурованих профілів навантаження для простої оптимізації продуктивності під різні обчислювальні задачі, та можливість зміни та їх модифікації, в разі необхідності перепрофілювання серверу під інші задачі.	
Оперативна пам’ять	- наявність встановленої не менше 128 ГБ та не гірше ніж Registered DDR4-3200MT/c; - весь об’єм пам’яті повинен бути встановлено модулями не більше за 32 ГБ кожний; - повинні бути наявні не менше 28 вільних слотів для швидкого розширення об’єму пам’яті без необхідності заміни наявних модулів; - наявність можливості збільшення максимального об’єму пам’яті до не менше 8 ТБ (можливо з заміною встановлених модулів пам’яті); - усі модулі пам'яті повинні бути від виробника серверу (рекомендовані виробником) та мати відповідне маркування, якщо таке передбачено у виробника; - наявність забезпечення виявлення одно- та багатобітових помилок в	

	пам’яті та виправлення однобітових помилок (ECC); - наявність забезпечення виправлення багатобітових помилок у мікросхемі модуля пам’яті або виходу її з ладу (Advanced ECC/SDDC), наявність можливості роботи в режимі виправлення багатобітових помилок у двох мікросхемах модуля пам’яті або виходу їх з ладу (DDDC); - підтримка дзеркалювання пам’яті, як повного, так і часткового (дзеркалювання окремих зон); - наявність можливості регулярного контрольного автоматичного зчитування блоків пам’яті для запобіганню накопиченню виправлених помилок і запис виправлених даних у разі виникнення помилки.	
Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження)	- наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокоду процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера; - наявність окремого захищеного внутрішнього депозиторію базових мікрокодів, для відновлення в разі визначення пошкодження або несанкціонованої модифікації мікрокодів сервера; - наявність підтримки механізму захищеного завантаження операційної системи; - наявність встановленого модуля TPM 2.0.	
Дискові контролери	Має бути встановлено апаратний контролер, що може працювати як внутрішній HBA та віддавати ОС кожен накопичувач як фізичний диск, а також підтримувати побудову наступних рівнів RAID 0, 1, 5, 10; - контролер повинен бути підключеним по інтерфейсу не нижче PCIe Gen 3.0 та не повинен займати класичного слоту розширення PCIe; - підтримка технології 12Gb SAS/ 6Gb SATA; - наявність підтримки «гарячої заміни» дисків;	

	- наявність підтримки оптимізації роботи з SSD дисками; - наявність можливості створення до 64 логічних дисків.	
Дискова підсистема	- повинно бути встановлено не менше двох (2) накопичувачів, що підтримують «гарячу заміну» типу 2.5” Read Intensive SSD з DWPD не нижче ніж 0.8 та об’ємом не менше 3.84ТБ кожний; - повинна бути наявна можливість розширення загальної кількості 2.5” SAS/SATA накопичувачів, що підключені до одного апаратного дискового контролеру, до не менше восьми (8) штук, лише додаванням самих дисків. - усі накопичувачі повинні бути від виробника серверу (рекомендовані виробником) та мати відповідне маркування, якщо таке передбачено у виробника.	
Мережеві адаптери	- наявність не менше одного мережевого адаптера, який повинен мати не менше двох портів зі швидкістю 1Гбіт/с з інтерфейсом RJ-45; - наявність не менше одного мережевого адаптера, який повинен мати не менше двох портів зі швидкістю 10/25Гбіт/с з інтерфейсом SFP28, форм-фактору OCP3, що не займає слот PCIe; - наявність не менше одного двохпортового 16Гбіт/с fibre channel адаптера зі встановленими двома оптичними модулями 16Gb SFP+ SW.	
Порти в сервері	- загальна кількість портів USB 3.0 не менше 5 (п’яти). Мають бути наявні не менше двох захищених внутрішніх портів USB (з загальної кількості портів) без доступу з зовні серверу; - наявність відео (VGA) порту; - наявність можливості встановлення послідовного порту (роз’єм DB9). - повинна бути можливість управління сервером не лише через окремий Ethernet порт, що знаходиться на задній частині серверу, а й через окремий USB порт, що розташований на передній частині серверу, та має бути реалізовано через відповідний адаптер, що може	

	бути придбано пізніше, окремо, в разі виникнення такої необхідності.	
Відеопідсистема	- будь яка з підтримкою максимальної роздільної здатності не нижче 1920 х 1200 та частотою не нижче 60Гц.	
Блоки живлення	- повинно бути встановлено не менше двох блоків живлення; - потужність кожного блоку живлення не менше 800 Вт, з підтримкою «гарячої заміни», напруга ~220В 1 фазні, частота 50 Гц; - повинна бути забезпечена відмовостійкість не гірше ніж 1+1; - енергоефективність блоків живлення не менше ніж 94% при напрузі живлення 230В; - наявність двох кабелів живлення в комплекті.	
Система охолодження	- повинно бути встановлено повний комплект вентиляторів охолодження для запропонованої конфігурації серверу; - повинно бути забезпечено відмовостійкість вентиляторів N+1, де N більше ніж 1.	
Гіпервізори та операційні системи, що підтримуються	- наявність ліцензії Microsoft Windows Server 2022 Standard на всі потужності сервера; - підтримка Red Hat Enterprise Linux 8.x, 9.x - підтримка SUSE Linux Enterprise Server 15. - підтримка VMware vSphere 7.0 U3, 8.0, 8.0 U1, 8.0 U2. (сервер повинен мати офіційну підтримку виробника та сертифікацію на веб-сайті VMware: https://www.vmware.com/resources/compatibility/search.php) Обов'язкова наявність сертифікації серверу під власною торговою маркою (сертифікація лише платформи неприйнятна).	
Функції керування	- наявність вбудованого програмного забезпечення для віддаленого керування сервером з відповідними ліцензіями на весь термін дії гарантії серверу. - наявність вбудованих в сервер процесора з окремим мережевим портом 1Гбіт: - збирання статистики з сервера,	

	- відслідковування його електроживлення та температури, стан компонентів сервера як до, так і після завантаження операційної системи (без необхідності встановлення агентів в операційній системі), - call-home (самостійний зв'язок з сайтом підтримки для автоматичних повідомлень про стан, зміну конфігурації, вихід з ладу), - завантаження сервера для конфігурування, розгортання та встановлення сумісної операційної системи без встановлення в сервер або віддаленого підключення додаткових медіа носіїв. - наявність віртуальної консолі з функціоналом: - доступу до графічної консолі сервера через браузер, та до текстової консолі через термінальний емулятор, - збереження виводу графічної консолі та текстового виводу текстової консолі з функцією відтворення для діагностування, - підключення до сервера локальних носіїв інформації станції керування (як фізичних носіїв, так і образів CD/DVD або каталогів файлової системи). - наявність захищеного зв'язку с процесором керування з використанням SSL, AES, 3DES, сертифікатів. Захист внутрішнього програмного забезпечення (мікрокоди та початкове завантаження): - всі мікрокоди повинні мати цифровий підпис виробника, - наявність внутрішнього цифрового секретного ключа за яким на апаратному рівні здійснюється контроль мікрокода процесора керування, а процесор керування в свою чергу перевіряє підписи всіх мікрокодів сервера, - наявність окремого захищеного внутрішнього депозиторія базових мікрокодів, для відновлення в разі визначення пошкодження або	

	несанкціованої модифікації мікрокодів, - повинна бути підтримка механізму захищеного завантаження операційної системи. Має підтримувати керування кількома серверами як одним через - груповий контроль живлення, - групове обмеження потужності, - групове оновлення мікрокодів, - конфігурацію групи, - групування віртуальних носіїв та зашифрованих віртуальних носіїв. Сервер повинен мати інформаційну панель безпеки, що відображає статус важливих функцій безпеки, загальний стан безпеки системи та поточну конфігурацію для функцій стану безпеки та блокування конфігурації сервера. Повинна бути функція безпечного стирання даних пристрою однією кнопкою, що призначена для виведення з експлуатації/перепрофілювання серверу.	
Термін гарантії та сервісної підтримки	- не менше 36 місяців з дати придбання (весь термін гарантії має бути від виробника серверу); - цілодобовий доступ до засобів для самостійного усунення несправностей, доступ до відео з технічними порадами від експертів, щодо найкращих практик, а також цілодобовий доступ для можливості реєстрації сервісної заявки; - час реакції по телефону не більше ніж 3 години з моменту реєстрації сервісного запиту в рамках робочих годин, не гірше ніж 9х5 (9:00-18:00, Пн.-Пт. за виключенням святкових та вихідних днів), виконання робіт по гарантійному обслуговуванню, в робочі години, з понеділка по п’ятницю (за виключенням святкових та вихідних днів), з прибуттям сервісного інженера на місце розташування обладнання, в разі необхідності; - гарантія повинна включати доступ до оновлень мікрокодів обладнання, а також віддалену діагностику і підтримку з боку центру технічної підтримки виробника; - повинна бути можливість цілодобово відкривати сервісні заявки за телефоном	

	гарячої лінії 0-800-ххх-ххх та електронною поштою; - повинна бути обов'язково запропонована можливість автоматичного відкриття заявок, щодо сервісних випадків.	
Додаткові можливості, щодо сервісної підтримки	В період дії технічної підтримки, повинен бути запропонований та наданий безкоштовний цілодобовий безперешкодний доступ до захищеного хмарного порталу, що базується на використанні технологій машинного навчання та розташований на ресурсах виробника обладнання, що пропонується. Замовник повинен мати можливість розмежувати права доступу на портал до інформації щодо обладнання: лише для читання, надати доступ для свого сервісного партнеру, повний доступ для адміністратору. Щонайменше портал повинен мати наступний функціонал: - можливість відслідковування стану гарантії; - можливість відслідковування стану серверу (включений чи виключений); - відслідковування стану «здоров'я серверу», з можливою зміною статусу не пізніше ніж один раз на добу; - можливість отримання на електронну пошту листа з інформацією, щодо зміни «здоров'я серверу»; - можливість автоматичного відкриття сервісних заявок, щодо гарантійних випадків; - інформацію про актуальність мікрокодів серверу. В разі, якщо даний функціонал платний, то його вартість повинна бути включена в пропозицію. Сервер та всі його компоненти повинні бути від одного виробника, новими, такими, що не були в експлуатації та мати відповідне маркування, в разі якщо таке передбачено виробником.	
Додаткові відомості	Сервер, що пропонується, повинен бути від виробника, що раніше не знаходився та й не знаходиться зараз, під санкціями країн-постачальників основних компонент (наприклад, ASIC, процесорів тощо) або повністю готових виробів.	

4. Система зберігання даних у форм-факторі Rackmount у комплекті		[вказати виробника, модель]
Загальні вимоги. Розмір та можливості по розширенню	- наявність не менше двох контролерів, що мають можливість працювати в режимі Active/Active; - наявність не менше 24GB кеш пам'яті для даних, операцій керування та даних операційної системи масиву; - наявність не менше восьми портів 16Gb Fibre Channel; - наявність не менше восьми оптичних модулів 16Gb SW FC SFP+. - наявність не менше 6 шт. оптичних патчкордів стандарту LC-LC OM3 MMF, довжиною не коротше ніж 2м. - наявність не менше ніж дванадцять (12) HDD SAS 12Gb, об'ємом не менше 2.4ТБ кожний, швидкість не нижче 10K RPM. Обов'язково наявна можливість установки додатково не менше ніж ще дванадцяти (12) накопичувачів цього типу, шляхом додавання лише самих дисків, а не будь-яких інших компонент. - наявна можливість розширення не менше ніж до 240 HDD та/або SSD накопичувачів на два контролери; - встановлені накопичувачі повинні бути від виробника СЗД та мати відповідне маркування, якщо таке передбачене виробником СЗД. - розмір запропонованої конфігурації СЗД повинен не перевищувати 2U (юніти).	
Функціональність	- система зберігання повинна забезпечувати віртуалізацію ресурсів зберігання на рівні контролера, з можливістю використання алгоритмів наступних типів - RAID 1, 5, 6, 10, а також такий рівень зберігання (окремий), який забезпечує продуктивність, доступність, гнучкість і менший час для відновлення відмовостійкості даних в порівнянні з іншими групами дисків (від 12 до 128 дисків або більше). - система має підтримувати побудову віртуалізованих RAID груп, в яких кожний том може бути розподілений між всіма дисками групи;	

	- повинна бути підтримка не лише глобальних дисків оперативного гарячого резерву (global hot spare disks), а й можливість використання розподіленого простору «гарячого резерву» по всіх дисках певної групи. - система зберігання повинна обов'язково підтримувати наступні типи накопичувачів: - NL-SAS 12Gb 7200 обертів/хвилину 6TB, 8TB, 10TB, 12TB, 14TB, 16TB, 18TB, 20TB дисками 3,5 дюйми (LFF). - SAS 12Gb 10000 обертів/хвилину, об'ємом 600GB, 1.2TB, 1.8TB, 2.4TB дисками 2,5 дюйми (SFF). - SAS 12Gb 15000 обертів/хвилину, об'ємом 900GB або більше 2,5 дюйми (SFF). - SAS SSD 12Gb розміром 960GB, 1.92TB, 3.84TB, 7.68TB дисками 2,5 дюйми (SFF). - система зберігання повинна мати можливість зупиняти механічні диски, що не розподілені та не використовуються для економії енергії та збереження їх ресурсу. - система зберігання даних, що пропонується, повинна використовувати окремі механізми обробки(ASIC, co-процесори, тощо), окрім ядер центрального процесора, щонайменше для розрахунку надлишкової інформації щодо RAID.	
Ефективне керування простором	- наявність ефективного керування простором (Thin Provisioning) для 100% всіх додатків для всіх томів системи зберігання, та всіх рівнів RAID, що підтримує СЗД.	
Багаторівневе зберігання (Tiering)	- СЗД повинна мати функціонал переміщення блоків даних з одних типів дисків на інші, в залежності від інтенсивності доступу до цих блоків, з кількістю рівнів не менше трьох, без зупинки додатків; цей функціонал може вимагати додаткової ліцензії; - в разі задіяння/використання функціоналу описаного вище та наявності накопичувачів різних типів, повинен бути функціонал автоматичного оптимального розміщення даних томів на різних типах носіїв в залежності від інтенсивності	

	доступу до даних та від політики тому даних назначеної адміністратором (архівний, загальний або швидкісний том); - в разі задіяння/використання функціоналу описаного вище, сканування інтенсивності доступу та перенос даних повинні відбуватися безперервно (кожні декілька секунд), з інтенсивністю, що запобігає зниженню продуктивності системи; - алгоритм переносу повинен виключати дані, які мають часто повторювану зміну інтенсивності доступу.	
Швидке створення копій даних	- система зберігання повинна забезпечувати створення віртуальних копій, зокрема також автоматичне створення і знищення віртуальних копій за розкладом; - наявність функціоналу створення не менше 64 віртуальних копій, що працюють в режимі читання/запис. Має бути можливість збільшення до 512 копій у разі активації додаткової ліцензії.	
Реплікація між системами зберігання даних	- повинна бути наявна можливість використання функціоналу асинхронної реплікації томів на аналогічну систему зберігання; цей функціонал може вимагати додаткової ліцензії; - система зберігання даних, що пропонується, повинна підтримувати реплікацію на кілька масивів зберігання одного і того ж сімейства в режимі «одна до декількох» (fan-out). Повинен підтримуватися принаймні режим 1:4; цей функціонал може вимагати додаткової ліцензії; - після початкової синхронізації повинні передаватися тільки зміни даних. - можливість синхронізації тільки змін при failback без необхідності повної ресинхронізації.	
Керування	- система зберігання повинна постачатися з інструментами для керування та моніторингу в реальному режимі часу. - система зберігання повинна підтримувати єдиний графічний інтерфейс користувача (GUI), - GUI повинно працювати як на Windows, так і на Linux.	

	- система зберігання повинна підтримувати перенаправлення протоколу всіх подій на окремий сервер, - інформація про продуктивність в реальному режимі часу різних компонент системи та її логічних об'єктів повинна бути доступна через GUI та командний рядок (CLI) одночасно, - система зберігання повинна мати вбудований механізм накопичення та аналізу історичних даних продуктивності та звітності за період не менше як один тиждень. - система зберігання даних, що пропонується повинна мати плагін для VMware vCenter, Microsoft System Center, а також vStorage API (VAAI) для інтеграції масиву.	
Підтримка роботи ОС серверів	СЗД повинна підтримувати операційні системи та гіпервізори: – Microsoft Windows Server 2016, 2019, 2022; – SUSE Linux Enterprise 12 SP4 та SP5, 15 SP1-SP4; – Red Hat Enterprise Linux 7.8, 7.9, 8-8.7, 9-9.3; – Oracle Linux(UEK) 7.8, 7.9, 8.2-8.7, 9-9.2; – VMware vSphere 6.7 U3. 7.0 - 7.0 U3, 8.0 – 8.0 U2; – Citrix Virtualization 8.2.	
Відмовостійкість	- система зберігання повинна підтримувати можливість розширення/додавання (дискових полиць, дисків) без зупинки додатків. - модернізація мікрокодів та програмного забезпечення масиву повинна підтримувати можливість здійснення без зупинки додатків(за виключенням оновлення мікрокодів накопичувачів). - система зберігання повинна підтримувати неперервність операцій в разі виходу з ладу будь-якого з компоненту системи: диск, блок живлення, контролер, порт, пам'ять, вентилятор, тощо. - підтримка підключення серверів, як мінімум, двома шляхами для дублювання каналів доступу (path	

	failover), необхідне ПЗ дублювання повинно бути в комплекті. - кеш даних повинен безпечно скидатися у постійне сховище у випадку зникнення електричного живлення, а не тільки забезпечуватися через живлення батарейки, також кеш даних не повинен в нормальному режимі функціонування системи займати простір на механічних чи SSD накопичувачах системи зберігання, призначених для зберігання даних.	
Додатковий інструментарій	- повинна бути передбачена можливість використання інструменту (наприклад, із хмари), який надає користувачам уявлення про загальний стан здоров'я системи зберігання даних. - інструмент, що може передбачити збої до того, як вони відбудуться(наприклад перевіряючи датчики у системі зберігання даних). - інструмент, повинен видавати рекомендації, щодо кращих практик налаштування СЗД, а також рекомендації, щодо наявності доступних оновлень мікрокодів. - вивантаження звіту у зручному форматі: pdf або doc.	
Термін гарантії та сервісної підтримки	- не менше 36 місяців з дати придбання (весь термін гарантії має бути від виробника обладнання); - цілодобовий доступ до засобів для самостійного усунення несправностей, доступ до відео з технічними порадами від експертів, щодо найкращих практик, а також цілодобовий доступ для можливості реєстрації сервісної заявки; - час реакції по телефону не більше ніж 2 години з моменту реєстрації сервісного запиту в рамках робочих годин, не гірше ніж 9х5 (9:00-18:00, Пн.-Пт. за виключенням святкових та вихідних днів), виконання робіт по гарантійному обслуговуванню, в робочі години, з понеділка по п’ятницю (за виключенням святкових та вихідних днів), з прибуттям сервісного інженера на місце розташування обладнання, в разі необхідності; - гарантія повинна включати доступ до оновлень мікрокодів обладнання, а також віддалену діагностику і	

	підтримку з боку центру технічної підтримки виробника; - повинна бути можливість цілодобово відкривати сервісні заявки за телефоном гарячої лінії 0-800-ххх-ххх та електронною поштою.	
Додаткові відомості	Всі комплектуючі системи зберігання даних повинні бути від одного Виробника. СЗД що пропонується, повинна бути від виробника, що раніше не знаходився та й не знаходиться зараз, під санкціями країн-постачальників основних компонент (наприклад, ASIC, процесорів тощо) або повністю готових виробів.	
5. Комутатор оптичний, рівня ядра, з можливістю об'єднання в стек		[вказати виробника, модель]
Форм-фактор та архітектура	- Комутатор фіксованої конфігурації.	
Характеристики продуктивності комутатора	- Максимальна продуктивність комутації/маршрутизації на систему: 131 млн. пакетів / с - Максимальна пропускна спроможність переадресації на систему: 176 Гбіт / с.	
Наявні інтерфейси наступних типів:	- 48 інтерфейсів 10/100/1000 Base-T - 2 інтерфейси 10G SFP+ - 2 інтерфейси 10GBASE-T ports	
Характеристики масштабованості:	- Максимальна кількість записів MAC-адрес: 16К - Максимальна кількість IPv4/IPv6 маршрутів: 32 / 32	
Підтримка протоколів та функцій рівня 2	- Віртуальні локальні мережі VLAN (IEEE 802.1Q) - Протокол Spanning Tree (стандарти IEEE 802.1D STP, IEEE 802.1w (RSTP), IEEE 802.1s (MSTP)); - Функції відслідковування повідомлень протоколів управління багатоадресними групами та оптимізації багатоадресного трафіку (IGMP snooping та MLD snooping); - Протокол агрегації з'єднань IEEE 802.3ad (LACP); - Протокол IEEE 802.3x, управління потоком даних; - Протокол IEEE 802.1AB (LLDP) та розширення LLDP-MED ; Підтримка надвеликих (Jumbo) фреймів розміром 9К	

Підтримка протоколів та функцій безпеки	Підтримка протоколів та функцій безпеки - Списки контролю доступу для вхідного та вихідного трафіку ; - Функцій захисту Link Flap prevention, BPDU filtering; - Функцій захисту від атак на протоколу ARP: ARP attack prevention; - Функцій Port security: обмеження кількості MAC адрес на порту, прив'язка MAC до порту, блокування неавторизованих MAC адрес; - Функцій захисту протоколу DHCP: DHCP snooping and IP Source Guard; - Протоколи автентифікації, авторизації та обліку (AAA): RADIUS, TACACS+; - Підтримка методів автентифікації користувачів: 802.1X, WEB автентифікації, та MAC автентифікації; - Керування доступом на основі визначених ролей; - Системний журнал; - Захищений протокол віддаленого керування HTTPS для доступу до графічного інтерфейсу керування Global Trust Mode.	
Підтримка протоколів та функцій якості обслуговування	- Підтримка приорітезації IEEE 802.1p, - Підтримка класифікації трафіка за критеріями: значення полів IEEE 802.1p; - Дії для трафіку, що відповідають умовам класифікатору: Traffic shaping, Traffic prioritization; - Дисципліни якості обслуговування: Class of Service (CoS);	
Підтримка функцій та протоколів моніторингу та управління:	- Протокол SNMP v1, v2, v3; - Протокол Remote monitoring (RMON); - Протокол синхронізації часу Simple Network Time Protocol (SNTP); - Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил;	

	- Наявність засобів автоматизації конфігурування пристрою з системи централізованого управління без початкового настроювання адміністратором (zero-touch provisioning); - Дзеркалювання трафіку Port mirroring; Підтримка управління з хмарного сервісу виробника без додаткових ліцензій та платежів;	
Простір, який займається у серверній шафі	- Не більше 1 U	
Гарантія / сервісна підтримка у складі пропозиції:	- Обмежена пожиттєва гарантія до моменту оголошення End of Support (EOST) виробником; - Включає заміну компонент, що вийшли з ладу, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника в режимі 8 х 5.	
6. Серверна шафа		[вказати виробника, модель]
Розмір	42 юніти, глибина не менш ніж 1000м.	
7. Програмно-апаратний комплекс (ПАК) для захисту мережі та системи керування		[вказати виробника, модель]
Загальні вимоги до ПАК	• Пропонована програмно-апаратна продукція повинна складатися з двох програмно-апаратних мережевих екранів (Next-Generation Firewall – далі NGFW) з можливістю: - Вияву та попередження загроз (Intrusion Detection / Prevention Systems - IDS/IPS), перевірки файлів на наявність відомого і невідомого шкідливого ПО (Anti-malware / Anti-Virus, Sandbox). - Вияву і попередженню комунікацій з бот центрами (Anti-bot / Anti-spyware). - Блокування сучасних атак з використанням DNS-протоколу (DNS Security). - Контролю доступу до ресурсів Інтернет (URL Filtering) та функціоналу контролю якості каналів (SD-	

	WAN). • Програмно-апаратні мережеві екрани повинні підтримувати відмовостійкість.	
Вимоги до продуктивності ПАК	• Програмно-апаратні мережеві екрани повинні підтримувати відмовостійкість. • Пропускна здатність пристрою в режимі мережевого екранування із забезпеченням ідентифікації додатків і користувачів (змішаний трафік, appmix) – не менш 2.2 Гбіт/сек.; • Пропускна здатність пристрою в режимі попередження і захисту від загроз (Application Control, IPS, Anti-Virus, Anti-spyware чи Anti-bot, Zero Day Attacks Detection and Analysis та логування на пристрої) – не менш 1 Гбіт/сек. (); Цей показник повинен бути виміряний з appmix пакетами. Ці дані мають бути опубліковані на офіційному сайті виробника. • Пропускна здатність функціоналу IPsec VPN повинна бути не менше 1.6 Гбіт/сек.; • Пристрій повинен підтримувати не менше 2 800 site to site тунелей; • Максимальна кількість нових сесій у секунду – не менш 34 000; • Максимальна кількість підтримуваних сесій – не менш 200 000.	
Вимоги до апаратних параметрів розгортання ПАК	• ПАК повинен бути виконаний у вигляді єдиного пристрою висотою не більш 1 Rack unit, з можливістю установки в стандартну монтажну стійку. • Блоки живлення повинні бути сумісні з 200-240В (50-60Гц) змінного току. Рішення повинно опційно підтримувати відмовостійкість блоків живлення. • Система повинна постачатися з максимальною кількістю пам'яті яку вона підтримує. • Кожен пристрій повинен складатися з двох програмно та	

	апаратно розділених компонент - компоненти управління пристроєм і компоненти обробки трафіка. Кожна компонента повинна мати свій набір процесорів (CPU), оперативної пам'яті (RAM) та інтерфейсів (Ethernet port). Компоненти управління та обробки трафіку повинні бути незалежні один від одного для того щоб надати можливість керування пристроєм у випадку критичного навантаження трафіком, зокрема під час DoS/DDoS атак. • Вбудована компонента управління повинна буди керована за допомогою веб інтерфейсу з можливістю налаштування політик безпеки та мережевих конфігурацій з єдиної веб консолі без необхідності встановлення додаткових програм на ПК. • Пристрій повинен мати наступні інтерфейси: - Щонайменше 4 мідних порти стандарту 1G RJ45, - Щонайменше 4 мідних порти стандарту 1G RJ45/PoE - Щонайменше 1 оптичний комбо порт стандарту 1G SFP/RJ45 combo. • Порт управління (Management port) повинен бути програмно ізольований та апаратно знаходитися окремо від мережевих портів для обробки трафіку. Порт управління (Management port) повинен підтримувати відмовостійкість (Management HA port) на пристрої.	
Вимоги до підтримуваних протоколів і режимів функціонування ПАК	• Підтримка статичної маршрутизації IPv4/IPv6 та протоколів динамічної маршрутизації BGPv4, OSPFv2/v3, RIP v2. Якщо цей функціонал потребує ліцензії, вона повинна бути включена в пропозицію.	

	• Підтримка роботи мережевих інтерфейсів у режимах прослуховування «дублюючого» трафіка з Span-Портів комутаційного устаткування, що підключається, у прозорому режимі без зміни MAC і IP-Адрес (Virtual Wire), у режимі комутації трафіка (Layer 2), у режимі маршрутизації трафіка (Layer 3). • Підтримка одночасної роботи різних мережевих інтерфейсів у будь-яких перерахованих режимах у будь-якій комбінації без обмежень в рамках одного віртуального мережевого екрану. • Підтримка зміни режиму функціонування портів (Layer 2, Layer 3, прозорий режим та режим прослуховування) без необхідності перезавантажувати пристрій. • Пристрій повинен вміти працювати в режимі комутатора (тобто мати можливість виділити більше 2х портів для роботи в режимі комутатора) • Пристрій повинен вміти здійснювати VLAN трансляцію на L2 рівні між підмережами. • Підтримка Static та Dynamic (Hide) NAT. • Підтримка NAT у прозорому режимі. • Підтримка IPV6, включаючи ідентифікацію додатків і користувачів. • Підтримка multicast маршрутизації і протоколів – PIM-SM, PIM-SSM, IGMP v1, v2, v3. • Підтримка маршрутизації між VLAN, організованими на мережевому екрані. • Пристрій повинен підтримувати не менше 4000 vlan. • Підтримка функціонала трансляції адрес NAT, сервера DHCP і DHCP relay. • Підтримка тегування фреймів по 802.1.	

	• Підтримка агрегування інтерфейсів по 802.3ad (підтримка LACP). • Підтримка передачі більших пакетів (Jumbo frames). • Підтримка SNMPv3. • Підтримка Netflow. Netflow профіль повинен визначатися на основі фізичних портів. • Підтримка протоколу LLDP (Link Layer Discovery Protocol). Таким чином, пристрій повинен мати можливість подавати інформацію про інші пристрої (адреса MAC, ім'я системи, підключений до нього порт). • Підтримка політик Policy Based Forwarding для IPv4 та IPv6 протоколів. • Підтримка BFD (Bidirectional Forward detection). Це дозволить швидше адаптуватися до будь-яких змін на рівні маршрутизації. • Підтримка віртуальних маршрутизаторів – не менш 10 шт. • Підтримка зон безпеки – не менш 50 шт. • Підтримка site-to-site та client-to-site IPsec VPN. • Число максимально можливих Client SSL VPN – не менш 1 000. • Число максимально можливих Clientless VPN – не менше 100. • Число IPSEC VPN тунелів (Site to site) – не менш 2 800. • Число одночасних сеансів розшифрування SSL – не менш 25 000.	
Вимоги до відмовостійкості ПАК	• Підтримка побудови відмовостійкого кластеру високої доступності High-Availability (HA) – Active/Passive та одночасної роботи обох міжмережевих екранів кластеру в активному режимі – Active/Active. • Для переключення між компонентами кластеру повинен здійснюватися моніторинг інтерфейсів (interface monitoring)	

	та шляху до вказаних ресурсів (path monitoring).	
Вимоги до функціоналу системи ПАК	• Пристрій має контролювати стан сесій (Stateful inspection) з фільтрацією пакетів та ідентифікацією застосунків. • Пристрій повинен бути зонним мережевим екраном (Zone-based). Один або більше інтерфейсів або субінтерфейсів можуть належати одній зоні. Політики доступу (firewall rules) та політики NAT повинні бути засновані на зонах. • Політики NAT повинні мати свій набір правил, незалежно від політик доступу (firewall rules). • Розпізнавання і блокування мережевих додатків на сьомому рівні моделі OSI по трафіку, що проходить через мережевий екран, у тому числі індивідуально для всіх додатків, що використовують загальний порт, у тому числі 80 і 443, що й використовують динамічні TCP/ UDP-Порти; • Управління додатками повинно показувати залежності додатку, щоб мати можливість будувати білі списки без помилок. • Розпізнавання трафіку що інспектується на Layer-7 моделі OSI по сигнатурах, наступного програмного забезпечення (додатків), протоколів або сервісів: - Сервісів автентифікації, включаючи Microsoft Active Directory, LDAP, RADIUS, TACACS+, Kerberos, SAML, Syslog Monitoring/Parser (Пристрій повинен підтримувати зіставлення user-to-ip, обробляючи повідомлення від Syslog); - СУБД, включаючи Microsoft SQL, Oracle, тощо; - Файлові сервісів, включаючи Microsoft SMB; - Систем електронного документообігу й обміну повідомленнями, у тому числі	

	Microsoft Sharepoint, Exchange, Office 365, Google Docs; - Протоколів обміну електронною поштою: SMTP, POP3, IMAP; - Протоколів VOIP і аудіо-відео-конференцій, включаючи SIP, H.323, H.245, H.225, Webex; - Сервісів відновлення програмного забезпечення, включаючи Microsoft Update, антивірусного ПО, Adobe, Java; - Сервісів резервного копіювання; - Сервісів віртуалізації й термінального доступу, включаючи Vmware, Microsoft RDP; - Протоколів дистанційного доступу, включаючи Telnet, SSH, VNC, Radmin; - Мережеві протоколи, включаючи протоколи динамічної маршрутизації й SSL, IPSec VPN; - Електронної пошта; - Соціальних мереж; - Засобів миттєвого обміну повідомленнями; - Засобів аудіо-відео-конференцій; - Потокового аудіо-відео (незалежно від веб-сайту), аудіо й відео по HTTP; - Засобів публікації робочого стола й надання дистанційного доступу, включаючи Team-Viewer; - Зовнішніх проксі-сервери й анонімайзерів, включаючи Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy; - Засобів побудови VPN і тунелів поверх інших додатків, включаючи Freenet, Open-vpn, Vtun, Rdp-to-Tcp, Tcp-over-Dns; • Рішення повинно підтримувати режим "Безпечний пошук" для	

	YouTube та CIPA-сумісного пошуку Google (Рішення не повинно працювати в режимі проксі). • Надання вбудованих у мережевому екрані засобів створення власних сигнатур додатків по регулярним вираженням з використанням декодерів HTTP(S), FTP, SMB, SMTP, RPC і ін., а також по масці для вмісту TCP/ UDP-Пакетів; • Розпізнавання мережевих додатків по зашифрованому SSL (підтримка ключів RSA до 2048 біт) і SSHv2 трафіку, що проходить через мережевий екран (дешифрація SSL, SSHv2), - як для вхідних, так і для вихідних підключень, прозоро для користувачів у домені, з можливістю контролю окремих функцій додатків, включаючи відправлення повідомлень у соціальних мережах, файловий обмін, потокове аудіо, відео; • Послідовне розпізнавання різних додатків, використовуваних у рамках однієї сесії; • Правила контролю доступу повинні підтримувати можливість враховувати час, день, дата та період надання такого доступу. • Розпізнавання користувачів, що використовують мережеві додатки, за рахунок інтеграції з корпоративними сервісами аутентифікації користувачів, такими як Microsoft Active Directory, Microsoft Exchange, LDAP; • Можливість створення правил на основі груп користувачів та окремих користувачів. Система повинна зберігати інформацію про користувачів у відповідних логах. • Інтеграція з Microsoft Active Directory, повинна здійснюватися без змін в Active Directory та не повинна використувати	

	обліковий запис адміністратору Active Directory домену. • Можливість інтеграції з іншими сервісами аутентифікації (наприклад, контролерами бездротових мереж) через відкритий XML API; • Можливість створення користувач-ай-пі меппінгу (user-IP mapping) завдяки парсингу syslog повідомлень відправлених системою що аутентифікувала користувачів. • Можливість створювати та використовувати у правилах динамічні групи користувачів. Динамічні групи користувачів дозволяють “на льоту” видаляти користувача з групи (додавати користувача в групу) без необхідності змін у відповідній директорії (наприклад Active Directory) та без необхідності встановлювати політики. Це дає можливість уповноваженим адміністраторам або зовнішнім систем видаляти користувача з динамічної групи користувачів, наприклад у випадку компрометації відповідного користувача. • Створення правил у єдиній політиці безпеки, використовуючи в якості класифікаторів дані про IP-адреса відправника, одержувача, використовуваних сервісів (TCP/UDP-Портів), імена користувачів, груп користувачів і використовуваних користувачем або групою користувачів додатків або певних категорій додатків. • У створюваних політиках повинна бути можливість реалізації наступних дій: - Дозволу або заборони; - Дозволу конкретному додатку або категорії додатків використовувати тільки стандартні або строго певні TCP/ UDP-Порти. При цьому ці порти	

	не повинні бути використані іншими додатками без політики, що дозволяє такі взаємодії в явному виді; - Дозволу або заборони, заснованого на розкладі, користувачі або групі користувачів; - Застосувати маркування DSCP і обмеження по трафіку, використовуючи політики QOS на основі додатків, IP-адрес, DSCP, користувачів і груп користувачів; - Реалізація QOS для real-time трафіка, ідентифікованого на рівні додатків; - Можливість маркування QoS на основе адреса джерела/призначення, порту, L7 застосунку; - Можливість застосовувати перенаправлення трафіка на основі політик (Policy Based Forwarding) на основі IP адреси (source та/або destination), користувача, застосунку або URL; - Можливість маршрутизації трафіку різних застосунків по різних маршрутам передачі даних; - Можливість маршрутизації трафіку різних URL-запитів по різних маршрутам передачі даних; - Можливість заборони окремого функціоналу у додатках; -Можливість використовувати будь-яку комбінацію з вищенаведених дій; - Можливість побудови whitelist/blacklist політики для окремо взятих користувачів. • Інспекція змісту трафіка протоколів: - Generic Routing Encapsulation; - Non-encrypted IPsec traffic (NULL Encryption Algorithm for IPsec and transport mode AH IPsec). • Система повинна мати базовий	

	DLP функціонал з налаштуванням через графічний інтерфейс з можливістю пошуку заданої інформації через регулярні вирази, попередньо-налаштовані шаблони або властивостей файлів (відповідна ліцензія повинна бути додана у пропозицію). • Пристрій Повинен забезпечуватися функціонал оптимізації політик, зокрема на основі використання додатків; виявлення та видалення невикористаних правил політики. • Для створення більш суворих правил та оптимізації політики в інтерфейсі управління на пристрої повинні бути доступні наступні функції: - Повідомляти про правила з невизначеними застосунками/додатками, ідентифікувати додатки що проходять через ці правила, та активувати їх у правилі, вибравши потрібні з перелічених додатків; - Система може повідомляти про додатки, які визначені та не використовуються в правилах. Про невикористані підписи заявки можна повідомити за останні 7, 15, 30 днів; - Система має можливість повідомляти інформацію про першу та останню дату ідентифікації додатку, який ідентифікувалися в правилі, та скільки пропускної здатності він спожив за останні 30 днів; - Система ідентифікує правила, які не використовувались протягом останніх 30 днів і 90 днів. • Правила безпеки можуть застосовуватися відповідно до географічних регіонів; до правила можна додати кілька географічних регіонів. • Обмеження пропускної здатності може застосовуватися на основі	

	імені користувача / групи, IP-адреси цілі / джерела та програми. • Можливість автоматично блокувати трафік з певних джерел окремою частиною мережевого екрана, до того, як ці пакети будуть використовувати ресурси основного процесора або буфера пакетів віртуального NGFW. • Наявність сервісу сканування нових потенційно шкідливих файлів у середовищі Microsoft Windows, включаючи файли, що виконуються (у тому числі EXE, DLL, SCR, BAT, і ін.), передані по мережі, у поштових повідомленнях SMTP/POP3, включаючи шифровані повідомлення за допомогою SSLз, що забезпечує, поведінки підозрілих файлів і посилань у приватному або зовнішній хмарі («пісочниці»), виявлення нового шкідливого ПО й автоматичну генерацію антивірусної сигнатури протягом 24 годин хвилин і оновлення репутаційної бази URL протягом 30 хв. • Мати розвинені функції візуалізації: візуалізація в простому та зручному форматі, активності мережевих додатків, виявлених і блокованих мережевих загроз додатків, що використовують користувачі. Можливість фільтрації інформації, використовуючи різні фільтри (по додатках, по погрозах, по користувачах, IP-адресам, TCP/ UDP-Портам, зонам безпеки, типам погроз і ін.); • Мати можливість створення звітів. Мережевий екран повинен мати функції по автоматичній генерації звітів і звітів за розкладом по різних тематичним функціям по ручному налаштуванню створюваних звітів. Повинна бути можливість перегляду звітів як безпосередньо	

	через графічний веб-інтерфейс керування (GUI) мережевим екраном, так і можливість експортування звітів у формати PDF і CSV; • Мати можливість інтеграції з підсистемою централізованого керування, логування, звітності, відновлення програмного забезпечення мережевих екранів того ж виробника; • Мати можливість буферизації логів локально на виділений дисковий простір віртуальної машин у випадку короткочасної неприступності підсистеми централізованого логування; • Мати можливість інтеграції зі сторонніми SIEM-Системами по протоколу Syslog із забезпеченням гнучкого налаштування формату логів; • Мати рольове керування доступом локальних адміністраторів: - Можливість обмежити область перегляду й керування на рівні віртуального пристрою в цілому, а також окремих віртуальних систем (контекстів); - Можливість надати доступ у режимі виправлення або тільки для читання, або заборонити доступ до будь-якого розділу веб-інтерфейсу мережевого екрану; - Можливість надати доступ у режимі виправлення або тільки для читання, або заборонити доступ до CLI мережевого екрану. • Мати наявність єдиного інтерфейсу керування для керування політиками безпеки, профілями та налаштуваннями пристроїв та мереж, без спеціальних пристроїв керування • Керування політиками безпеки та мережевими налаштуваннями повинне здійснюватися по протоколах HTTPS і SSH без необхідності установки якого-небудь додаткового ПО	

	керування на робочу станцію адміністратора та без використання хмарних серверів управління; [Система повинна передбачити можливість додати централізований сервер керування у майбутньому]. • Інтерфейс керування мережевими екранами (веб і CLI) повинен бути уніфікований з підсистемою централізованого керування, логування, звітності, відновлення програмного забезпечення; [Система повинна передбачити можливість додати централізований сервер керування у майбутньому]. • Підтримка міток Cisco TrustSec SGT Tag; • Підтримка функціоналу динамічних груп адрес (Dynamic Address Group) та динамічних груп користувачів (Dynamic User Group), що дозволяє динамічно, за допомогою XML API, оновлювати такі групи в правилах безпеки без необхідності встановлювати політики безпеки. • Пристрій повинен мати сучасну програмно-апаратну архітектуру з використанням виділених статичних чипів ASIC та перепрограмованих чипів FPGA. Повинна існувати можливість за допомогою цих чипів виконувати окремі задачі, такі як обробка шифрованого трафіка, обробка протоколів маршрутизації, ARP-запитів, тощо. Таким, чином, при великому навантаженні на пристрої, окремі апаратні чіпи повинні мати можливість виконувати критичні задачі (такі як робота з протоколами динамічної маршрутизації) незалежно від задачі обробки трафіку. • Пристрій повинен використовувати апаратні чіпи для прискорення обробки IPS. • Пристрої повинні мати	

	можливість виконувати розшифрування SSL/TLS та SSH. Підтримка розшифрування протоколів TLS 1.0, TLS 1.1, TLS 1.2 та TLS 1.3. • Пристрій повинен мати можливість перевіряти трафік HTTPS та застосовувати IPS, контроль додатків, фільтрування URL-адрес та антивірусні засоби захисту. • Пристрій повинен здійснювати розшифрування HTTPS у вхідному (inbound) та вихідному (outbound) напрямках. • Пристрій повинен підтримувати інтеграцію з HSM (hardware security module) для управління цифровими ключами. • Підтримка інспекції тунелів VxLAN. • Пристрій повинен мати можливість застосовувати IPS, Application Control та Anti-virus, досліджуючи трафік HTTPS. • Пристрій може проводити перевірку HTTPS у вхідному та вихідному напрямку. • Правила інспектування (дешифрування) трафіку HTTPS повинні створюватися на основі імені користувача / групи користувачів, джерела IP (source IP) / мережі / зони, цільового IP (destination IP) / Цільової мережі / Цільової зони та категорії URL. • Пристрій повинен надавати можливість створювати правила виключення дешифрування у випадках, коли вміст трафіку HTTPS не слід бачити (банківські операції тощо). • Повинна бути можливість перевіряти сертифікат HTTPS сесій та запобігати сесії із закінченими, ненадійними або відкликаними сертифікатами. • Пристрій повинен вміти дешифрувати SSL веб трафік і відправляти копію дешифрованого трафіку на зовнішні пристрої аналітики,	

	використовуючи функціонал дзеркалювання трафіка. Відповідна ліцензія повинна бути додана в пропозицію. • Пристрої повинні мати можливість розшифровувати на ньому клієнтський веб-трафік SSL/TLS та надсилати цей розшифровувати трафік стороннім пристроям або системам обробки даних трафіку (IPS, Network Forensic тощо). Сторонні пристрої або системи, про які йдеться, повинні бути в змозі забезпечити продовження проходження трафіку шляхом відправки цього трафіку назад на ПАК і знову зашифрувати його після виконання необхідних операцій над трафіком. • Пристрій повинен мати можливість дзеркалювати та пересилати UDP/TCP трафік на сторонні інструменти аналітики для інспекції цього трафіку та повернення його назад для подальшої передачі клієнту та/або серверу. • Система повинна мати можливість застосовувати правила безпеки у відповідності до географічної зони, з можливістю створення одного правила з декількома географічними зонами.	
Вимоги до можливостей запобігання вторгнень, розпізнавання й блокування шкідливого або забороненого трафіка в системі ПАК	• Пристрої повинні мати архітектурну перевірку, фільтрацію пакетів IP та функції розпізнавання додатків та мати такі служби безпеки: - Брандмауер наступного покоління (NGFW) - IPSEC VPN, SSL VPN - Контроль додатків (Application Control) - Антивірус (Antivirus/Antimalware) - Запобігання вторгненням (IPS) - Антишпигунське (antispyware/antibot) - Блокування атак з	

		використанням DNS протоколу (DNS Security) - Фільтрація URL посилань (URL filtering) - Аналітика мережевого трафіку (NTA) - Інтеграція з каталогами для ідентифікації користувачів (Identity Awareness) - Можливість інспекції переданого через мережевий екран умісту трафіка в реальному режимі часу в потоці по сигнатурах і поведінці, захист від вразливостей, мережевих атак і шкідливого програмного забезпечення, розпізнавання типів файлів по їхнім сигнатурам, визначення вірусів, переданих по веб, через електронну пошту, FTP, SMB, шпигунського програмного забезпечення, мережевих «worms», блокування передачі певного вмісту з використанням регулярних виразів, у тому числі для додатків, що використовують шифрування SSL і SSHv2; - Антивірусний захист, захист від шпигунського програмного забезпечення, захист від вразливостей і мережевих атак (система виявлення й запобігання вторгнень), URL-Фільтрація з використанням динамічної репутаційної бази, що підтримує категоризацію для різних розділів того самого веб-сайту, включаючи підтримку категорій для веб-сайтів на різних мовах, блокування передачі файлів по типах, певних сигнатур; - Можливість використання додаткових функцій сканування нових потенційних шкідливих файлів у середовищі Microsoft	

	і Android, включаючи файли, що виконуються (у тому числі EXE, DLL, SCR, BAT, і ін.), документи форматів PDF (перевірка на різних версіях Adobe Reader), MS Office 2003, 2007 і вище, Java і Flash, Android APK, посилання http:// і https:// виявлення нового шкідливого програмного забезпечення й автоматичну генерацію антивірусної сигнатури в режимі реального часу; - Автоматична кореляція логів різного типу (мережеве екранування, захист від погроз, контроль передачі файлів, URL-Фільтрація), згенерованих у рамках однієї сесії. - Пристрій повинен мати наступні функції системи протидії вторгнень (IPS): a. Можливість створення різних політик IPS для різних користувачів або груп користувачів. b. Можливість пошуку IPS сигнатур на пристрої за допомогою CVE, рівнів критичності та типу хосту (клієнт/сервер). c. Можливість індивідуального налаштування сигнатур IPS системи реагувати на атаки наступним чином: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-IP. Блокування на основі IP повинно бути виконуватися на основі source IP та одночасно source та destination IP. d. Фільтри IPS, які використовуються для протидії атакам, повинні бути в змозі оновлюватися з файлу оновлення або через Інтернет. Крім того, за необхідності оновлення сигнатур повинно робитися автоматично без втручання користувача. e. Запропоноване	

	функціональність IPS повинна включати технологію детектування аномалій в використовуваних аномаліях (Protocol Anomaly Detection) які дозволяють блокувати атаки, не спираючись на наявні сигнатури. • Функціональність IPS повинна бути в змозі протистояти наступним атакам: - Brute Force - Code/Command execution - Sql-injection - Exploit-kit - Denial of Service - Info-leak - Overflow - Scan • Пристрій повинен мати функціональність Anti-Spyware/Anti-bot для виявлення та блокування з наступними можливостями: a. Цей функціонал повинен працювати незалежно від порта і протоколу і повинен перевіряти весь IP трафік в Інтернет. b. Виявляти запити на визначення (resolution requests) IP адрес командних центрів ботнетів (Botnet command and control centers) і блокувати їх через ДНС запити. c. Функціонал DNS Sinkhole у випадку запиту шкідливого доменного імені повинен видавати IP address призначену адміністратором. Таким, чином інфіковані системи можуть бути легко ідентифіковані. d. Функціонал блокування відомих ботнетів за допомогою сигнатур. Система повинна надавати можливість адміністратору налаштовувати ботнет сигнатури. e. Наступні дії для дій сигнатур повинні бути доступні: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip. f. Різні політики Anti-spyware повинні створюватися для різних	

	користувачів і груп користувачів. g. Функціональність Anti-spyware повинна включати ідентифікацію та блокування наступних атак: - adware - Botnets - Backdoor - Browser-Hijacker - Data-theft - keylogger - spyware - net-worm - p2p-communication • Пристрій повинен мати Anti-Virus функціонал для виявлення і попередження з наступними можливостями: a. Блокування відомого шкідливого ПО на основі сигнатур. b. Повинен мати можливість потокового сканування. Повинен сканувати архівні файли. c. Архітектура Anti-virus повинна мати можливість інтегруватися з Active Directory таким чином що б правила Anti-virus могли бути визначені на основі користувача чи групи користувачів в Active Directory. d. Можливість виключити антивірусні сигнатури із бази даних сигнатур (можливість задавати виключення). e. Різні політики Anti-virus повинні створюватися для різних користувачів і груп користувачів. f. Anti-virus повинен блокувати шкідливі файли, передані через протоколи FTP, HTTP, SMB, POP3. • Запропонована система повинна мати функціонал захисту від атак нульового дня за допомогою сканування файлів що передаються у трафіку. • Пристрій повинен використовувати додаткову локальну або хмарну пісочницю (sandbox) для аналізу файлів. • Пристрій повинен бути здатним відправляти підозрілі файли	

	(наступні формати файлів повинні підтримуватися: 7-ZIP, RAR, ZIP, Adobe Flash, APK, JAR, PDF, MS-Office DOC, DOCX, RTF, XLS, XLSX, PPT, PPTX, .exe, .dll, а також лінки в пошті, ELF формат файлів ОС Linux, формати файлів Mach-O, DMG, та PKG операційної системи Mac OS X) в пісочницю локальну або хмарну пісочницю. • Пристрій повинен мати можливість отримувати відповідні оновлення в режимі реального часу для забезпечення захисту від шкідливих файлів із локальної або хмарної пісочниці. • Пристрій повинен мати можливість ідентифікувати та блокувати в режимі реального часу невідомі шкідливі портативні виконувані файл та скрипти PowerShell за допомогою алгоритмів машинного навчання, оцінюючи деталі файлу, включаючи поля та шаблони декодера. Цей рівень захисту повинен забезпечувати розширене охоплення файлів, сигнатури для яких ще не існують. • Запропоноване рішення повинно ідентифікувати користувачів, які завантажували шкідливі файли. • Пристрій повинен мати функціонал DNS Security протидії атакам із зловмисним використанням протоколу DNS, що включає в себе: - Аналіз підозрілих DNS-Запитів і локалізація заражених станцій за допомогою технології DNS sinkhole (підміна відповіді DNS-Сервера); - Блокування відомих зловмисних доменних імен за допомогою репутаційних баз. - Функціонал повинен використовувати алгоритми машинного навчання в хмарі для ідентифікації потенційно	

	шкідливих доменних імен. - Виявлення та блокування DNS-тунелів (DNS tunneling) за допомогою машинного навчання, що аналізує якість та поведінку DNS-запитів (частота запитів, ентропію тощо). - Повинен здійснюватися аналіз та виявлення DGA (domain generation algorithm) та Dictionary DGA, тобто визначення чи домен згенерований машиною, а не людиною, шляхом реверсивної інженерії та аналізу інших часто використовуваних методів. У випадку виявлення що домен створений DGA алгоритмом він може бути заблокований. - Функціонал DNS Security повинен вміти виявляти низку інших типів атак таких як: a. ultra-slow DNS tunneling b. dangling DNS. c. NSNX DDoS attacks d. fast-flux domains e. DNS rebinding f. Виявлення нових зареєстрованих доменів (NRD); • Пристрій повинен мати функціонал URL-фільтрації з наступними можливостями: - Функція фільтрації URL-адрес повинна працювати в інтеграції з Active Directory, завдяки чому правила фільтрації URL-адрес можуть бути визначені на основі користувачів та груп користувачів, визначених в Active Directory. - Наявність та можливість змінювати портал блокування та попередження відвідування неприйнятних URL-адрес. - Можливість динамічно оновлювати списки C&C (Command and Control) та сайтів що містять шкідливе програмного забезпечення.	

	- Функція фільтрації URL-адрес повинна мати функцію XFF (X-forwarded-for). - Можливість написання політик обмеження пропускної здатності для категорій URL-адрес. - Можуть класифікувати URL-адреси як високо-ризиковані (шкідлива активність, пов'язана з URL-адресами за останні 30 днів), так і URL-адреси із середнім ризиком (шкідлива діяльність, пов'язана з URL-адресою за останні 60 днів). - Мати можливість класифікувати URL-адреси, зареєстровані за останні 30 днів (нові зареєстровані домени). - Мати можливість зберігати та передавати детальні журнали URL-адрес, до яких здійснюється доступ у зовнішні системи через syslog. • Функціонал URL-фільтрації повинен мати можливість застосовувати машинне навчання на веб-сторінках, щоб запобігти потраплянню шкідливих варіантів експлойтів JavaScript та фішингу у мережу. Цей функціонала машинного навчання повинен динамічно аналізувати та виявляти шкідливий вміст, оцінюючи різні деталі веб-сторінок, використовуючи ряд моделей машинного навчання в режимі реального часу. • Функціонал URL-фільтрації повинен використовувати хмарну технологію перевірки веб-трафіку на основі Машинного Навчання (ML) у режимі реального часу та мати можливість виявлення та запобігання невідомим розширеним безфайловим веб-атакам, включаючи цільовий фішинг, зловмисне програмне забезпечення, що доставляється через Інтернет а також експлойти, соціальну інженерії та інші види	

	веб-атак. • Міжмережеві екрани повинні мати ліцензію для Аналітики мережевого трафіку (NTA) в хмарі за допомогою рішення Cortex XDR. Це рішення повинно ідентифікувати нормальну поведінку мережевих пристроїв та виявляти аномалії. • Ліцензія для аналітики мережевого трафіку повинна включати можливість зберігання до 5 ТБ мережевих логів. • Міжмережеві Екрани повинні підтримувати можливість створення розширених логів для аналітики мережевого трафіку. • Міжемережеві екрани повинні мати можливість відправляти розширені мережеві логи в Cortex Data Lake для їх подальшої аналітики за допомогою Cortex XDR. • Пристрій повинен мати функціонал захисту від фішингових атак за допомогою функції контролю ідентичності користувача. Запропоноване рішення повинно мати можливість запобігти надсиланню/викраденню інформації про користувача (логіну) та паролю на рівні HTTP / HTTPS POST. Він повинен мати можливість контролювати облікові дані користувачів в інтеграції з Active Directory. Відповідна ліцензія повинна бути включене в запропоноване рішення. • Пристрій повинен мати функціонал фільтрації даних (Data filtering) і працювати використовуючи правила. Ідентифікація типу файлу повинна здійснюватися за допомогою ключових слів регулярних виразів. Ліцензії, необхідні для цього, будуть включені в пропозицію. • Пристрій повинен мати функціонал виміру якості каналу	

	та динамічного використання декількох провайдерів (SD-WAN), зокрема підтримувати: - Статична маршрутизація та маршрутизація по політиках (PBR) - Одночасне використання фізичних та логічних інтерфейсів з різнотипними підключеннями (лінії безпосереднього зв'язку, broadband Internet, LTE, тощо) для ефективної маршрутизації трафіку - Оцінка якості каналів зв'язку SD-WAN шляхом відправлення пакетів чи запитів до певних вузлів у мережі або пасивними методами - Контроль характеристики каналів зв'язку в режимі реального часу (packet loss, jitter, latancy) та їх графічне відображення - Контроль SLA для користувацьких додатків (applications) на основі характеристик каналів зв'язку (packet loss, jitter, latancy) у реальному часі, як VPN трафіку, так і трафіку фізичних каналів зв'язку. В тому числі для додатків SaaS. - Визначення різнопланових алгоритмів/стратегій вибору каналів зв'язку для маршрутизації трафіку додатків та сервісів виходячи з критеріїв відповідності SLA, кращих значень характеристик каналів зв'язку, тощо. - Визначення правил маршрутизації трафіку додатків та сервісів через VPN та фізичні канали SD-WAN з урахуванням алгоритмів/стратегій та SLA. - Автоматичне переключення каналів зв'язку для користувацьких додатків та	

	сервісів при зміні характеристик мережевих з'єднань (loss, jitter, latancy) у реальному часі.	
Додаткові обов'язкові вимоги до NGFW	• Більше одного адміністратора може одночасно змінювати конфігурацію пристрою. • Зміни правил повинні бути активними після проведення операції "Встановити". Операція "встановити" повинна мати опцію - встановити зміни зроблені всіма адміністраторами або вибрати зміни якого адміністратора потрібно застосувати. • У кожній операції завантаження правил пристрій може автоматично зробити резервну копію конфігурації. • Пристрій повинен мати функцію управління правилами для запобігання конфлікту правил у своєму веб-інтерфейсі управління. Система має попереджати адміністратора, якщо правило буде дублюватися чи затінятися існуючими правилами. • Журнали можуть надсилатися до зовнішніх систем управління журналом через SNMP, syslog. • Журнали повинні зберігатися локально. Також повинна існувати опція надсилати журнали до центральної системи управління, якщо така буде встановлена. • Запропонована система повинна мати системний жорсткий диск типу eMMC розміром 128 GB (сто двадцять вісім) ГБ. • Пристрій повинен мати можливість надсилати журнали за допомогою snmp, syslog з можливістю використання спеціально визначених фільтрів. • Пристрій повинен підтримувати створення зовнішніх динамічних списків блокування IP / URL / домену. Пристрій повинен отримувати доступ до цього	

	списку по HTTP протоколу. При внесенні змін в цей список пристрій повинен автоматично заблокувати (або дозволити - в залежності від встановленої політики) ці IP / URL / домени без необхідності встановлювати (застосувати) політики на самом пристрої. Ємність списків повинен включати в себе не менше ніж 50 000 IP та URL та не менше ніж 1 000 000 доменних імен. • Підтримка динамічних списків блокування для зовнішніх джерел ThreatIntelligence • Перелік шкідливих IP-адрес, виявлених виробником у службі кібер-розвідки, повинно постійно оновлюватися на пристрої. Таким чином, доступ до цих ІС може бути заблокований. • Система повинна мати опцію налаштування порогової кількості одночасних сесій для протистояння SYN Flood, UDP Flood, ICMP Flood. • Система повинна вміти ідентифікувати заблокувати сканування портів: TCP port scan, UDP Ports scan та sweep scan. • Резервні правила повинні відновлюватися та активуватися без необхідності перезавантаження. • NGFW повинно бути побудовано на моделі безпеки із застосуванням білого списку, а не чорного списку та мати просту модель управління політиками. Керування за допомогою простих графічних інструментів та редактора політик, що об'єднує налаштування програм, користувачів та контенту разом; • Всі сервіси, що використовуються NGFW мають можливість отримувати оновлення ПЗ та сигнатур безпеки (а саме - Application Control, IPS, Antivirus, Antispyware, DNS Security, SSL	

	Decryption, URL filtering, Data Filtering, SD-WAN), на протязі не менш ніж 12 місяців з дня активації NGFW.	
Вимоги до сервісної підтримки NGFW	• Сервісна підтримка програмного забезпечення не менше, ніж 12 місяців, з можливістю: - Локального звернення до першої лінії підтримки від виробника NGFW в Україні із сертифікованими інженерами; - Звернення телефоном або через Інтернет (чат та електронна пошта); - Доступу до завантаження оновлень, виправлень; - Доступу до документації.	
8. Джерело безперебійного живлення (ДБЖ)		[вказати виробника, модель]
Тип:	Не гірше ніж: On-line з подвійним перетворенням	
Потужність:	не менше 5000VA (5000W)	
Коефіцієнт вихідної потужності:	не менше 1	
Вхідні параметри		
Діапазон вхідної напруги без переходу на батареї:	не гірше 176-280V при повному навантаженні	
Частота:	50-60Hz ±5%	
Максимальний струм на вході:	Не менше 27,5 А	
Сумарний коефіцієнт гармонійних спотворень струму на вході:	Не гірше THDi < 3%	
Коефіцієнт потужності на вході:	≥ 0,99 (при повному лінійному навантаженні)	
Вихідні параметри		
Робоча номінальна вихідна напруга:	• 230 V ± 1%, регульоване 220/230/240 V змінного струму	
Частота:	50/60 Hz ±4 Hz (auto sense) / 50/60 Hz ±0.1 Hz (battery mode)	
"Чиста" синусоїда:	Так	
Коефіцієнт викривлення	• не гірше ≤ 3% (при повному лінійному навантаженні)	

синусоїдальної кривої напруги:	• не гірше ≤7% (при повному нелінійному навантаженні)	
Здатність до перевантажень:	Не гірше: <105% continuous 105% ~ 125% for 5 minutes. 125% ~ 150% for 1 minute.	
Захисні параметри		
Типовий час перемикання на батарейне живлення:	Не більше 0ms	
Байпас:	внутрішній автоматичний байпас	
Захист від перенавантаження:	• Електронний захист від перевантажень і коротких • замикань. • Аварійне відключення живлення (EPO). Захист від перегріву	
Ефективність		
В лінійному режимі при повному навантаженні:	не гірше 93,5 %	
Батареї та час автономної роботи		
Батарейна шафа	1	
Батареї:	Не менше, ніж: 16 x 12V/5Ah	
Час заряджання:	не більше 4 години до 90% ємності	
Час автономної роботи при навантаженні 50%:	не менше 10 хвилини	
Час автономної роботи при навантаженні 100%:	2хв 50сек при 5000Вт (100%)	
З'єднання та комунікації		
Вихідні з'єднання:	клемні колодки	
Вхідні з'єднання:	клемні колодки	
Програмне забезпечення:	ПЗ для ОС Windows і Linux безкоштовно скачується з сайту виробника обладнання. • відображення всіх виконуваних операцій і діагностичних даних в разі виникнення проблем; • налаштування спеціальних функцій. • можливість підключення зовнішніх датчиків температури/вологості з	

	моніторингом в оригінальному ПЗ виробника.	
Дисплей і індикатори:	Наявність дисплею та кнопок зі світлодіодами, для контролю в реальному часі стану і основних параметрів	
USB port:	Так	
RS-232 port:	Так	
Слот розширення:	так, для карт SNMP	
Параметри оточуючого середовища		
Рівень шуму:	не більше 55 дБА	
Робоча температура:	Від 0°С до + 40°С	
Робоча відносна вологість	Не гірше 0% - 95% без утворення конденсату	
Ступінь захисту:	Не гірше, ніж IP 20	
Комплектність та габарити		
Вага ДБЖ, кг:	Не більше 56кг ДБЖ з батареями, батарейний відсік не відокремлюється.	
Комплект поставки:	• ДБЖ • керівництво з експлуатації • USB кабель • мережева карта • батарейна шафа • кріплення для стійки 2 комплект кронштейнів 2	
Термін та умови гарантії:	• Обладнання повинно мати повну гарантію не менше 24 місяців з дати поставки - Обов'язкова наявність офіційних сервіс-центрів у м. Києві	

[НАЗВА ВИКОНАВЦЯ]
Підпис уповноваженої особи:
Печатка компанії
Місце:
Дата:

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК 3

до Запрошення до подання цінових пропозицій № SH-5.23

[НА БЛАНКУ ОРГАНІЗАЦІЇ]

ЦІНОВА ПРОПОЗИЦІЯ

Міністерство охорони здоров'я України

01601, Україна, Київ,
вул. М. Грушевського, 7

Шановні панове,

Ми пропонуємо виконання договору № SH-5.23 «Серверне обладнання для НУОЗ України ім. П.Л. Шупика» відповідно до «Умов постачання» та «Технічних вимог», які надаються разом із цією ціновою пропозицією, за ціною договору _____ *(сума прописом і цифрами)* (_____) *(назва валюти)*. Ми пропонуємо завершити доставку Товарів, описаних в договорі в межах періоду в _____ календарних днів від дати підписання договору.

Ця цінова пропозиція і ваше письмове повідомлення про її прийняття становитимуть зобов'язання укласти з вами договір за формою, наведеною у Запрошенні до подання цінових пропозицій № SH-5.23. Ми розуміємо, що ви не зобов'язані приймати цінову пропозицію з найнижчою ціною, або будь-яку іншу цінову пропозицію, отриману вами.

Цим документом ми підтверджуємо, що:
а) дана цінова пропозиція є дійсною протягом сорока п'яти (45) днів з кінцевої дати надання цінової пропозиції зазначеної у п.5 Запрошення до подання цінових пропозицій № SH-5.23.
б) Постачальник та запропоновані ним товари та програмне забезпечення не підпадають під обмежувальні заходи (санкції) введені відповідно до чинних Указів Президента України.

_____ Дата: _____

[Підпис уповноваженої особи Постачальника] [День/Місяць/Рік]

П.І.Б. уповноваженої особи Постачальника: _____

Назва Постачальника: _____
Адреса: _____
_____
Тел. _____
Факс _____

Додаток 1: Умови постачання
Додаток 2: Технічні вимоги

[Примітка: Будь ласка ПІДПИШІТЬ та поставте ПЕЧАТКУ на ВСІ сторінки цього документу.]

ДОДАТОК 4

до Запрошення до подання цінових пропозицій № SH-5.23

ДОГОВІР № SH-5.23 /___

м. Київ _____ 2024 р.

Цей Договір укладено в день, місяць та рік, зазначені вище, між Міністерством охорони здоров'я України (далі – Покупець), в особі _____, заступника Міністра охорони здоров'я України, яка діє на підставі наказу Міністерства охорони здоров'я України від _____ № _____, з однієї сторони, та _____ (далі - Постачальник) в особі _____, який діє на підставі Статуту, з іншої сторони, які надалі разом іменуються «Сторони», а кожен окремо «Сторона».

Договір укладається в рамках реалізації Проекту « Поліпшення охорони здоров'я на службі у людей» (далі - Проект), що фінансується відповідно до Угоди про позику між Україною та Міжнародним банком реконструкції та розвитку (далі - Банк) від 19 березня 2015р. № 8475-UA (далі – Угода про позику).

1. ПРЕДМЕТ ДОГОВОРУ

1.1. Постачальник зобов'язується поставити Покупцеві комп'ютерну, офісну техніку та супутні товари (далі – Товари), а Покупець зобов'язується придбати (прийняти та оплатити) Товари на умовах даного Договору.
1.2. Вартість, асортимент, кількість та технічні специфікації Товарів вказуються в Додатку № 1 «Умови постачання» та Додатку № 2 «Технічні вимоги», які є невід'ємною частиною цього Договору.

2. ДОСТАВКА ТА ПРИЙМАННЯ

2.1. Постачальник здійснює поставку Товарів Покупцеві на адресу: м. Київ, вул. Дорогожицька, 9, не пізніше 14 (чотирнадцяти) календарних днів з дати підписання Договору.

2.2. Датою поставки Товарів вважається дата підписання Сторонами видаткової накладної. Видаткова накладна повинна бути підписана Покупцем в день поставки Товарів або протягом цього дня Покупець повинен надати Постачальнику письмову мотивовану відмову від підписання видаткової накладної. Факт підписання Сторонами видаткової накладної визначає момент переходу права власності на Товари від Постачальника до Покупця.

3. СУМА ДОГОВОРУ та ОПЛАТА

3.1. Сума Договору складає _____ (_____), включаючи усі податки, митні збори, доставку, завантаження, розвантаження та додаткові послуги включно із ПДВ у сумі _____. Сума Договору та одиничні ціни Товарів, вказані в Додатку № 1, є фіксованими і змінам не підлягають.

3.2. Сто відсотків (100%) загальної ціни поставлених Товарів буде сплачено Покупцем Постачальнику протягом тридцяти (30) календарних днів з дня надання Постачальником оригіналу рахунку-фактури та видаткової накладної, підписаної Покупцем, після виконання Постачальником всіх зобов'язань за Договором, окрім гарантійних зобов'язань.
У разі відмінності валюти договору від української гривні – оплата буде здійснюватись в українській гривні за офіційним курсом Національного банку України на день підписання Покупцем видаткової накладної.
3.3 Оплата за цим Договором здійснюється за рахунок коштів позики (Угода про позику між Україною та Міжнародним банком реконструкції та розвитку від 19 березня 2015р. № 8475-UA), передбачених у спеціальному фонді державного бюджету.

3.4 На період дії воєнного стану в Україні оплата здійснюється у порядку черговості відповідно до Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану, затвердженого постановою Кабінету Міністрів України від 09 червня 2021 року № 590.

4. ПРИПИНЕННЯ ДІЇ ДОГОВОРУ

4.1 Припинення дії у зв'язку з невиконанням договірних зобов'язань

(a) Покупець, без шкоди будь-яким іншим заходам, пов'язаним із порушенням умов Договору, може розірвати Договір цілком або частково, надіславши Постачальнику в письмовій формі повідомлення про невиконання останнім зобов'язань за Договором:

(i) у разі, якщо Постачальник неспроможний поставити будь-які або всі товари в межах періоду, визначеного в Договорі, або в межах будь-якого наданого його продовження;

(ii) у разі, якщо Постачальник неспроможний виконати будь-яке інше зобов'язання за Договором; або

(iii) у разі, якщо Постачальник, на думку Покупця, був замішаний у корупції або шахрайстві, як зазначено в п. 5 нижче в процесі конкуренції за отримання або виконання Договору.

(b) Якщо Покупець розриває Договір повністю або частково, Покупець може, на прийнятних умовах і в доцільний спосіб, закупити аналогічні недопоставлені Товари, причому Постачальник буде нести перед Покупцем відповідальність за всі додаткові витрати, пов’язані з такими аналогічними Товарами. Однак Постачальник повинен продовжувати виконання Договору в тій його частині, що не була розірвана.

4.2 Розірвання Договору в силу неплатоспроможності

(a) Покупець може в будь-який час розірвати Договір, направивши Постачальнику відповідне письмове повідомлення, якщо Постачальник стає банкрутом або в інший спосіб оголошується неплатоспроможним. В цьому випадку розірвання здійснюється без виплати компенсації Постачальнику за умови, що таке розірвання не шкодить або не впливає на будь-які права щодо дій або коригувальних заходів, що були чи будуть згодом набуті Покупцем.

4.3 Розірвання Договору в силу доцільності

(a) Покупець може в будь-який час повністю або частково розірвати Договір в силу доцільності, надіславши Постачальнику відповідне письмове повідомлення У цьому повідомленні повинно бути зазначено, що таке розірвання здійснюється з міркувань доцільності для Покупця, визначено обсяг анульованих зобов’язань Постачальника за Договором, а також дату вступу в силу такого розірвання.

(b) Товари, вже готові до відправлення протягом двадцяти восьми (28) днів після одержання Постачальником повідомлення про розірвання, повинні бути прийняті Покупцем на умовах і за цінами Договору. По відношенню до інших Товарів Покупець може зробити наступний вибір:

(i) вимагати виготовлення і поставки будь-якої їхньої частини на умовах і за цінами Договору; та /або

(ii) відмовитися від Товарів.

5. ШАХРАЙСТВО ТА КОРУПЦІЯ

5.1 У разі, якщо Покупець виявить, що Постачальник та/або будь-хто з його працівників, агентів, субпідрядників, консультантів, надавачів послуг, постачальників та/або найманих працівників вдавались до корупційних або шахрайських дій, або до практики змови, примусу, перешкоджання розслідуванню в процесі конкурентного відбору або при виконанні цього Договору, у цьому випадку Покупець може припинити залучення Постачальника за Договором і дію Договору, письмово повідомивши про це Постачальника не пізніше, ніж за 14 днів до припинення дії Договору. При цьому положення пункту 4 застосовуються так ніби мало місце припинення дії Договору відповідно до пп.4.1.

5.2 Від Постачальника вимагається дотримання вимог Антикорупційного керівництва Банку та його переважаючих політик та процедур щодо санкцій, викладених в Санкційних правилах Банку, як визначено в Додатку 3 до Договору.

6. ПЕРЕВІРКИ ТА АУДИТ

6.1 Постачальник має виконувати всі вказівки Покупця, які відповідають чинному законодавству місця постачання товарів.

6.2 Постачальник дозволяє Банку і/або особам, призначеним Банком, а також має забезпечити отримання дозволу від своїх Субпідрядників та консультантів, інспектувати і/або проводити на вимогу Банку аудит рахунків, записів та інших документів, що мають відношення до подання тендерної пропозиції та виконання Договору. Звертаємо увагу Постачальника, його Субпідрядників та консультантів на п.5 Шахрайство та корупція, яким, окрім іншого, передбачається, що дії, спрямовані на суттєве обмеження реалізації Банком свого права на проведення перевірок та аудиту становить заборонену практику, яка тягне за собою розірвання договору і/або застосування Банком санкцій (включаючи визнання Постачальника неправомочним, але не обмежуючись цим) відповідно до стандартних процедур Банку щодо застосування санкцій.

7. ГАРАНТІЙНІ ЗОБОВ'ЯЗАННЯ

7.1. Товари повинні мати гарантію Постачальника не менше, ніж строк, передбачений у Додатку № 2 «Технічні вимоги». Постачальник надає Покупцю гарантійні документи на Товари разом з рахунком до сплати та видатковою накладною.

7.2. Протягом гарантійного періоду усі дефекти мають бути виправлені Постачальником без жодних витрат для Покупця не пізніше ніж через 30 днів з дати отримання повідомлення від Покупця.

8. ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ

8.1. Сторони звільняються від відповідальності за невиконання або неналежне виконання зобов'язань за цим Договором у разі виникнення обставин непереборної сили, які не існували під час укладання Договору та виникли поза волею Сторін (аварія, катастрофа, стихійне лихо, епідемія, епізоотія, війна тощо).

8.2. Сторона, що не може виконувати зобов'язання за цим Договором внаслідок дії обставин непереборної сили, повинна не пізніше ніж протягом 5 (п'яти) днів з моменту їх виникнення повідомити про це іншу Сторону у письмовій формі.

8.3. Доказом виникнення обставин непереборної сили та строку їх дії є відповідні документи, які видаються уповноваженими на це законами України органами.

8.4. У разі коли строк дії обставин непереборної сили продовжується більш ніж 30 (тридцять) днів, кожна із Сторін в установленому порядку має право розірвати цей Договір.

8.5. У разі здійснення Покупцем попередньої оплати та неможливості постачання Товарів Постачальником через настання обставин непереборної сили, Постачальник повертає Покупцю кошти протягом 3 (трьох) днів з дня розірвання Договору.

9. ВІДПОВІДАЛЬНІСТЬ СТОРІН

9.1 За невиконання або/та неналежне виконання умов даного Договору Сторони несуть майнову відповідальність згідно з даним Договором та діючим законодавством України.

9.2. За порушення строків поставки Товарів Покупець має право розірвати договір без будь-яких зобов‘язань перед Постачальником в разі невиконання поставки Товарів через 21 день від крайнього терміну поставки Товарів, вказаному в п. 2.1 цього Договору, після відповідного письмового повідомлення Покупцем.

9.3. За порушення строків поставки Товарів за пунктом 2.1 з Постачальника стягується неустойка у розмірі 0,2% від вартості Товарів, щодо яких допущено прострочення, за кожен календарний день прострочення. Неустойка, що стягується, не має перевищувати 10% вартості недопоставлених у строк Товарів.

9.4. Якщо Постачальник використовуватиме послуги субпідрядників, перевізників, експедиторів та інших компаній, які залучаються для своєчасного та належного виконання Договору, вся відповідальність перед Покупцем за будь-які втрати, збитки або за неналежне виконання Договору несе Постачальник.

10. ВИРІШЕННЯ СПОРІВ

10.1. Усі спори, що виникають внаслідок або у зв’язку з цим Договором, вирішуються шляхом переговорів між Сторонами.

10.2. Якщо Сторони не можуть дійти до згоди, то спір підлягає вирішенню у порядку, передбаченому чинним законодавством України.

11. СТРОК ДІЇ ДОГОВОРУ

11.1. Цей Договір набуває чинності в день підписання та діє до повного виконання Сторонами своїх зобов’язань, зокрема, в частині Постачання Товарів – відповідно до термінів, визначених у Статті 2, в частині розрахунків – до повного їх виконання, але не пізніше 31 березня 2024 року.

11.2. Договір складено в 2-х примірниках, які мають однакову юридичну силу, по одному для кожної Сторони.

12. ІНШІ УМОВИ

12.1 Усі зміни та доповнення до цього Договору здійснюються в письмовій формі шляхом укладення додаткових угод, що є невід’ємною частиною Договору.

12.2. Всі повідомлення будь-якої із Сторін цього Договору іншій Стороні повинні направлятись поштою, електронною поштою або факсом за адресами, вказаними у Договорі.

12.3. У випадку зміни адрес, банківських реквізитів, контактних телефонів тощо, вказаних у Договорі, Сторони зобов’язуються повідомляти про це іншу Сторону протягом 3 (трьох) робочих днів.

13. ЮРИДИЧНІ АДРЕСИ та РЕКВІЗИТИ СТОРІН

Міністерство охорони здоров'я України Адреса: вул. М. Грушевського, 7, м. Київ, 01601 Банківські реквізити Замовника: Код ЄДРПОУ 00012925 IBAN UA07 820172 0343111 0101 00000 199 в ДКСУ м. Київ МФО 820172	Адреса: Розрахунковий рахунок _____ _____ _____ _____

14. ПЕРЕЛІК ДОДАТКІВ

Додаток 1: Умови постачання
Додаток 2: Технічні вимоги
Додаток 3: Шахрайство та корупція

Засвідчуємо, що цей Договір підписано від імені Сторін вищевказаною датою:

Від Покупця	**Від Постачальника**
_____	_____

Додаток 3
до договору № SH-5.23/_____
від _____

ШАХРАЙСТВО ТА КОРУПЦІЯ

1. Мета

1.1 Антикорупційні настанови Банку та це доповнення застосовуються до закупівель в рамках операцій Банку з фінансування інвестиційних проектів.

2. Вимоги

2.1 Банк вимагає від Позичальників (включаючи отримувачів фінансування від Банку); учасників торгів (тих, хто подав заявки/пропозиції), консультантів, підрядників та постачальників; будь-яких субпідрядників, субконсультантів, надавачів послуг або постачальників; будь-яких агентів (заявлених чи ні); та їх співробітників дотримуватись найвищих етичних стандартів під час процесу закупівель, відбору та виконання контрактів, що фінансуються Банком, та утримуватись від шахрайства та корупції.

2.2 З цією метою Банк:

a. Визначає, для цілей цього пункту, наведені нижче терміни таким чином:

i. “корупційні дії” – це пропонування, надання, отримання або вимагання, прямо чи опосередковано, будь-чого цінного з метою неналежного впливу на дії іншої сторони;

ii. “шахрайські дії” – це будь-які дії або бездіяльність, включаючи викривлення інформації, які навмисно або ненавмисно вводять в оману або намагаються ввести в оману сторону для отримання фінансової або іншої вигоди або уникнення виконання обов’язків;

iii. “дії щодо змови” – це домовленості між двома або більше сторонами, спрямовані на досягнення неналежної мети, включаючи неналежний вплив на дії іншої сторони;

iv. “дії щодо примушування” – це негативний вплив або завдання шкоди, або погрози негативно вплинути чи завдати шкоди, прямо чи опосередковано, будь-якій стороні або її майну для здійснення неналежного впливу на дії сторони;

v. “перешкоджаючі дії” - це

(a) навмисне знищення, фальсифікація, зміна або приховування важливих для розслідування доказів або надання неправдивих заяв слідчим з метою суттєво завадити розслідуванню Банком звинувачень в корупційних або шахрайських діях, діях щодо змови або примушування, та/або погрози, домагання або залякування будь-якої сторони з метою недопущення розкриття нею відомостей, важливих для проведення розслідування, або подальшого проведення розслідування, або

(b) дії, спрямовані на суттєве перешкоджання реалізації Банком права на інспектування та аудит відповідно до пункту 2.2 e. нижче.

b. Відхиляє пропозицію щодо присудження контракту, якщо Банком буде з’ясовано, що рекомендований для укладання контракту консультант або його співробітники, агенти, субконсультанти, субпідрядники, надавачі послуг, постачальники та/або їх

співробітники прямо чи опосередковано брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час участі у конкурсі щодо зазначеного контракту;

c. На додаток до засобів правового захисту, визначених у відповідній угоді про позику, може вживати відповідні заходи, включаючи оголошення про порушення процедур закупівель, якщо Банком буде встановлено, що представники Позичальника або будь-якого з отримувачів будь-якої частини коштів Позики брали участь у корупційних або шахрайських діях, діях щодо змови або примушування або перешкоджаючих діях під час процесу відбору або виконання зазначеного контракту, і що Позичальником не було вжито своєчасних та належних заходів, що є задовільними на думку Банку, з метою реагування на такі дії на момент їх виникнення, включаючи відсутність своєчасного інформування Банку про такі дії;

d. Відповідно до Антикорупційних настанов Банку та згідно з поширеною на цей час санкційною політикою та процедурами Банку, може застосувати санкції до фірми або фізичної особи на невизначений або визначений період часу, включаючи публічне оголошення про позбавлення такої фірми або фізичної особи права: (i) на присудження контракту, що фінансується Банком, або отримання від нього будь-якої фінансової чи іншої вигоди[1]; (ii) на пропонування[2] в якості субпідрядника, консультанта, виробника, постачальника або надавача послуг іншої фірми, яка має право на присудження контракту, що фінансується Банком; та (iii) на отримання коштів в рамках будь-якої позики, наданої Банком, або на будь-яку подальшу участь у підготовці або реалізації проекту, що фінансується Банком;

e. Вимагає включення до тендерної документації/запитом до надання пропозицій та до контрактів, що фінансуються за рахунок позики Банку, вимоги до учасників (тих, хто подає заявки/пропозиції), консультантів, підрядників та постачальників, їх субпідрядників, субконсультантів, надавачів послуг, постачальників, агентів дозволити Банку інспектувати[3] всі рахунки, записи та інші документи, що стосуються процесу закупівель, відбору та/або виконання контракту, а також дозволити їх аудит призначеними Банком аудиторами.

[1] Для уникнення сумнівів, позбавлення сторони, до якої застосовано санкції, права на присудження контракту має поширюватись, без обмежень, на (i) подання заявки на передкваліфікацію, висловлення інтересу в наданні консультаційних послуг та подання заявок, прямо чи в якості пропонованого субпідрядника, пропонованого консультанта, пропонованого виробника або постачальника або номінованого надавача послуг щодо цього контракту, та (ii) внесення доповнень або змін, що спричиняють суттєву модифікацію існуючого контракту.

[2] Пропонований субпідрядник, пропонований консультант, пропонований виробник або постачальних або пропонований надавач послуг (використовуються різні назви в залежності від конкретної тендерної документації) це той, хто був (i) включений консультантом до передкваліфікаційної заявки через специфічний та надзвичайно важливий досвід та ноу-хау, що забезпечують відповідність учасника кваліфікаційним вимогам за конкретною заявкою; або (ii) призначений Позичальником.

[3] У цьому контексті інспекції носять слідчий характер (експертиза). Вони включають заходи із встановлення фактів, що вживаються Банком або особами, призначеними Банком, для реагування на конкретні питання, що стосуються розслідувань/аудитів, як то оцінка правдивості звинувачень у можливому шахрайстві та корупції, шляхом використання належних механізмів. Така діяльність включає, не обмежуючись: доступ та огляд фінансової документації та інформації фірми або фізичної особи, зняття копій у разі необхідності; доступ та огляд будь-яких інших документів, даних та інформації (у паперовому або електронному вигляді), що вважаються важливими для розслідування/аудиту, та зняття копій у разі необхідності; опитування співробітників та інших відповідних осіб; здійснення фізичних інспекцій та виїздів на місце; отримання підтверджень інформації з боку третіх осіб.