Міністерство охорони здоров'я України
Проект № 9315-UA
«Додаткове фінансування проекту "Екстрене реагування на COVID-19 та вакцинація в Україні"»

ЗАПИТ ДО ПОДАННЯ ЦІНОВИХ ПРОПОЗИЦІЙ
№ RFQ-1.1.17
Впровадження контрольованої та сегментованої мережі

1. Україна одержала позику Міжнародного банку реконструкції та розвитку (далі – Банк) № 9315-UA на фінансування проекту «Додаткове фінансування проекту "Екстрене реагування на COVID-19 та вакцинація в Україні"» (далі – Проект). Частина коштів цієї Позики має бути використана для покриття витрат в рамках договору, до якого відноситься цей запит до подання цінових пропозицій (далі – Запит).

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, встановлення, налаштування та інтеграцію мережевих комутаторів, точок доступу Wi-Fi, програмного модулю автентифікації і контроля доступу, програмно-апаратного комплексу Next Generation Firewall, програмного комплексу eXtended Detection and Response.

   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 Запиту. 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 Запитом та Технічними вимогами до нього.

4. Цінова пропозиція українською мовою за формою, наведеною у Додатку 3 «Цінова пропозиція», а також необхідна додаткова інформація» 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: moz.wb.procurement@gmail.com, обов'язкова копія на m.k.dymytrenko@moz.gov.ua. В полі «Тема» електронного повідомлення **обов'язково зазначити** «**Пакет № RFQ-1.1.17**».

   Також за зверненням за вищевказаною адресою зацікавленими учасниками може бути отримана довідкова інформація. Процедура розкриття для цієї закупівлі не передбачена.

5. Кінцевим терміном для отримання пропозицій Замовником за адресою вказаною в п. 4 вище встановлюється: **13 жовтня 2023 року, 17:00 за місцевим часом**.

   Замовник не розглядає жодних цінових пропозицій, які надходять після кінцевого терміну подання конкурсних пропозицій. Пропозиції, отриманні Замовником після кінцевого

терміну подання цінових пропозицій, будуть оголошені такими, що надійшли із запізненням, та відхилені.

6. До своїх пропозицій Ви маєте додати документацію, що підтверджує відповідність запропонованих товарів Технічним вимогами, та відповідні відомості, що підтверджують відповідність встановленим кваліфікаційним вимогам.

7. Процедура закупівлі – Запит до подання цінових пропозицій відповідно до вимог Правил закупівель Світового банку для позичальників в рамках фінансування інвестиційних проектів (ФІП), в редакції від листопада 2020 року.

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

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

   (ii) ОЦІНКА ПРОПОЗИЦІЙ. Пропозиції, які визнані такими, що задовольняють Технічним вимогам та Запиту, 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 Запиту.

   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 учасник прийняти вказані корегування, його цінова пропозиція буде відхилена.

   (iii) ПРИСУДЖЕННЯ ДОГОВОРУ Договір присуджуватиметься учаснику, який запропонує найнижчу загальну ціну, та пропозиція якого відповідає умовам, встановленим Технічними та іншими вимогами цього Запиту, а Постачальник відповідає встановленим обов'язковим кваліфікаційним вимогам. З обраним Постачальником буде укладено договір за формою, наведеною у Додатку 4 «Договір».

   Період очікувань не застосовується.

   (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 Запиту.

8. **ПЕРЕВІРКИ ТА АУДИТ**

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

   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 Запиту та Вашої участі у торгах.**

Додатки:

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

ДОДАТОК 1

до Запиту до подання цінових пропозицій № RFQ-1.1.17
Впровадження контрольованої та сегментованої мережі

УМОВИ ПОСТАЧАННЯ

1. Ціна пропозиції

№ з/п	Опис (детальний опис наведено в відповідному пункті Технічних вимог)	Одиниця виміру	Кількість	Ціна за одиницю ***[вказати валюту]***, без ПДВ	Загальна ціна ***[вказати валюту]***, без ПДВ
1.	Мережевий комутатор рівня L2 *[вказати виробника, модель]*	шт.	*[вказати кількість згідно Варіанту 1 або Варіанту 2]*		
2.	Мережевий комутатор рівня L3 *[вказати виробника, модель]*	шт.	*[вказати кількість згідно Варіанту 1 або Варіанту 2]*		
3.	Точка доступу Wi-Fi *[вказати виробника, модель]*	шт.	24		
4.	Програмний продукт автентифікації і контроля доступу Wired и Wireless(ZTNA) *[вказати виробника, модель]*	ліцензія	1		
5.	Програмно-апаратний комплекс Next Generation Firewall *[вказати виробника, модель]*	комплект	3		
6.	Програмний комплекс eXtended Detection and Response *[вказати виробника, модель]*	ліцензія	300		
7.	Супутні послуги	послуга	1		
ЗАГАЛЬНА ЦІНА ПРОПОЗИЦІЇ БЕЗ ПДВ:					
ПДВ (20%):					
ЗАГАЛЬНА ЦІНА ПРОПОЗИЦІЇ З ПДВ:					

Примітка: 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 45 (сорока п’яти) календарних днів від дати кінцевого терміну отримання пропозицій, встановленої в п. 5 Запиту до подання цінових пропозицій.

3. Фіксована ціна
Наведені вище ціни є фіксованими, включають усі податки, митні збори, доставку, завантаження, розвантаження, супутні послуги до ДП «Медичні закупівлі України», м. Київ, вул. Хрещатик, 22 і жодним змінам не підлягають, включаючи період виконання Договору.

4. Право Покупця змінювати кількість послуг 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 виконання
Постачання товарів разом із відповідними документацією, інструкціями з експлуатації та додатковими послугами (згідно з Технічними Вимогами, що додаються) має бути здійснено протягом 180 (сто вісімдесят) 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 по кожній поставці 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 якщо Виконавець не усуває недоліки у виконанні своїх зобов'язань за Договором протягом 1 (одного) робочого дня в разі невиконання поставки Товарів згідно наведених умов через 21 день після отримання відповідного письмового повідомлення від 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 Запиту 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 Запиту до подання цінових пропозицій № RFQ-1.1.17
Впровадження контрольованої та сегментованої мережі

ТЕХНІЧНІ ВИМОГИ

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

У зв'язку з повномасштабною війною російської федерації проти України, ДП "Медичні закупівлі України" зіштовхнулося з необхідністю мінімізації ризиків здійснення цілеспрямованих кібератак на IT-інфраструктуру підприємства.

Враховуючи рекомендації міжнародні стандарти та кращих практик - критично провести сегментацію мережі, дозволить розбити мережу на цільові під мережі. Такий підхід забезпечить краще контролювання трафіку у кожному сегменті, моніторинг дій пов'язаних з отриманням доступу користувачами до активів підприємства.

Зважаючи на той факт, що ДП "Медичні закупівлі України" і ДП "Укрмедпостач" знаходяться у процесі об'єднання планується збільшення обсягу робіт по налаштуванню IT-інфраструктури у тому числі із кібербезпеки та сегментації. Впровадження сегментації та контролю інфраструктури позитивно вплине на інтеграційні процеси між зазначеними державними підприємствами.

Мета:
- Захист від зовнішніх атак та шкідливого коду (Next Generation Firewall).
- Захист та контроль виконання коду на рівні ОС (eXtended Detection and Response).
- Централізований збір події інформаційної безпеки (Next Generation Firewall та ОС робочих станцій і серверів).
- Впровадження технологій для ідентифікації користувачів під час запитів на доступ до ресурсів підприємства.
- Контроль доступу користувачів до додатків підприємства.
- Контроль над діями привілейованих користувачів в IT-інфраструктурі.

Очікувані результати:
- Захист від кіберзагроз та зовнішніх втручань
- Запобігання крадіжкам, спотворенню, знищенню та витоку даних.
- Забезпечення на рівні операційної системи захисту виконання шкідливого коду.
- Логування дій користувачів та кіберінцендентів (з метою проведення їх подальшого аналізу, прийняття відповідних рішень з посилення кіберзахисту)

Термін або скорочення	Визначення
Замовник	Міністерство охорони здоров'я України (для ДП "Медичні закупівлі України" Міністерства охорони здоров'я України).
ZTNA	Zero Trust Network Access - рішення для побудови контрольованої IT-інфраструктури, що забезпечує захищений видалений доступ до додатків, даних, сервісів тощо.

Термін або скорочення	Визначення
Next Generation Firewall	Міжмережевий екран нового покоління.
Low-level Design	Детальний опис усіх компонентів, конфігурацій та процесів ІТ-рішення, яке проектується
Extended Detection and Response	Рішення для розширеного виявлення та реагування на складні загрози та цільові атаки.
ДП “МЗУ”	ДП “Медичні закупівлі України”

2. ДЕТАЛЬНІ ВИМОГИ

ВАЖЛИВО:

Технічні специфікації вказані в колонці «Технічні вимоги Покупця» є **мінімально** необхідними. Пропоновані учасниками товари повинні відповідати встановленим вимогам або мати кращі характеристики

Учасник має заповнити колонку «Відповідність та опис запропонованих товарів» по кожному запропонованому товару, а також обов'язково зазначити виробника та модель товарів, які він пропонує. Учасник торгів робить відмітку «**відповідає**», у випадку, якщо товар повністю відповідає технічним вимогам Покупця.

Всі характеристики повинні бути вказані у відповідності до технічної документації виробника та підтверджені виданими виробником копіями технічних документів.

Якщо запропонований товар не відповідає технічним вимогам Покупця в повному обсязі, в колонці напроти відповідної позиції мають зазначатися розбіжності по кожному пункту.

2.1. Мережевий комутатор рівня L2

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Форм-фактор та архітектура	• комутатор фіксованої або модульної конфігурації; • монтаж в стандартну телекомунікаційну стійку 19'' • Варіант 1: 6 комутаторів на 48 портів, які можуть працювати на L2 рівні моделі OSI, що дозволить сегментувати продуктивну мережу на канальному рівні; • Варіант 2: 12 комутаторів на 24 порти, які можуть працювати на L2 рівні моделі OSI, що дозволить сегментувати продуктивну мережу на канальному рівні Примітка: Учасник має запропоновувати або Варіант 1 або Варіант 2. Пропозиції з будь якими	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	комбінаціями комутаторів з 24 та 48 портами будуть відхилені.	
Максимальні характеристики продуктивності комутатора	• максимальна пакетна продуктивність комутації/маршрутизації не менше: 130 млн. пакетів / с • максимальна пропускна спроможність переадресації на систему, не менше: 176 Гбіт / с	
Наявність інтерфейсів	• Не менше 48 х 10/100/1000; • Не менше 4 х 1/10G SFP+;	
В комплект поставки кожного пристрою повинно бути включено оптичні модулі та кабелі	• кабель 10G SFP+ SFP+ Direct-Attach Copper, 1,2 м – 1 шт. • кабелі та модулі повинні офіційно підтримуватись виробником для даного типу обладнання.	
Підтримка PoE	• IEEE 802.3at Power over Ethernet (PoE+) • загальна потужність, що може віддаватися на живлення PoE пристроїв (PoE бюджет) без додаткового блоку живлення, не менше: 370Вт; • загальна потужність, що може віддаватися на живлення PoE пристроїв (PoE бюджет) з додатковим блоком живлення, не менше: 740Вт;	
Характеристики масштабованості, не гірше	• максимальна кількість записів MAC-адрес, не менше: 16 000 • максимальна кількість IPv4/IPv6 маршрутів, не менше: 512 / 256 • максимальна кількість агрегованих з'єднань / максимальна кількість активних портів в агрегованому з'єднанні, не менше: 128 / 8	
Підтримка протоколів та функцій рівня 2	• віртуальні локальні мережі VLAN (IEEE 802.1Q) не менше 2000; • протокол Spanning Tree (стандарти IEEE 802.1D STP, IEEE 802.1w (RSTP), IEEE 802.1s (MSTP));	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• протокол Multiple VLAN Registration Protocol (MVRP); • функції відслідковування повідомлень протоколів управління багатоадресними групами та оптимізації багатоадресного трафіку (IGMP snooping, MLD snooping та PIM snooping для IPv4 та IPv6); • multicast VLAN для IPv4 and IPv6; • протокол агрегації з'єднань IEEE 802.3ad (LACP); • протокол IEEE 802.3x, управління потоком даних; • протокол IEEE 802.1ab (LLDP); • IEEE 802.3az Energy Efficient Ethernet (EEE); • підтримка надвеликих (Jumbo) фреймів розміром не менше 9К	
Підтримка протоколів та функцій безпеки	• списки контролю доступу для вхідного та вихідного трафіку, що дозволяють використовувати поля заголовків рівня 2, 3 та 4, можливість застосовувати правила ACL з урахуванням дати/часу; • протоколи автентифікації, авторизації та обліку (AAA): RADIUS, TACACS+; • керування доступом на основі визначених ролей; • системний журнал; • захищений протокол віддаленого керування SSHv2 • підтримка IEEE 802.1x, можливість автентифікації користувача з динамічним призначенням ACL та VLAN; • функції захисту протоколу STP (Root Guard, BPDU protection);	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• функції захисту протоколу DHCP; • функції захисту протоколу ARP (Dynamic ARP protection/inspection); • ізоляція портів, Private VLAN.	
Підтримка функцій та протоколів моніторингу та управління	• Повністю керований комутатор (CLI); • Протокол SNMPv1, v2, v3; • Протокол sFlow (RFC 3176); • Протокол Remote monitoring (RMON); • Протокол синхронізації часу Network Time Protocol (NTP); • Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил; • Дзеркалювання трафіку (створення копії трафіку що відповідає визначеним умовам (порт, VLAN, ACL) та передача його на локальний порт моніторингу);	
Простір, який займається у серверній шафі	• Не більше 1 U	
Вимоги до сервісної підтримки або гарантії у складі пропозиції	• Термін не менше 36 місяців • Повинна включати заміну компонентів, що вийшли з ладу, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника. • Послуга повинна надаватися в режимі 9 х 5 з часом реагування NBD	

2.2. Мережевий комутатор рівня L3

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Форм-фактор та архітектура	• комутатор фіксованої або модульної конфігурації • Варіант 1: 2 комутатори на 48 портів, які можуть працювати на L3 рівнях моделі OSI, що дозволить сегментувати продуктивну мережу на рівні IP-адресації • Варіант 2: 4 комутатори на 24 порти, які можуть працювати на L3 рівнях моделі OSI, що дозволить сегментувати продуктивну мережу на рівні IP-адресації Примітка: Учасник має запропоновувати або Варіант 1 або Варіант 2. Пропозиції з будь якими комбінаціями комутаторів з 24 та 48 портами будуть відхилені.	
Характеристики продуктивності комутатора	• максимальна пакетна продуктивність комутації/маршрутизації на систему, не менше: 214 млн. пакетів / с • максимальна пропускна спроможність переадресації на систему, не менше: 288 Гбіт / с	
Наявність інтерфейсів наступних типів	• не менше 24 інтерфейсів 10/100/1000 Base-T POE+ • 4 x 10G SFP+ • можливість встановлення додатково інтерфейсів (або наявність вбудованих в разі використання комутатору фіксованої конфігурації) • 2 x 40G QSFP+	
Підтримка PoE	• IEEE 802.3at Power over Ethernet (PoE+)	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• загальна потужність, що може віддаватися на живлення PoE пристроїв (PoE бюджет) без додаткового блоку живлення, не менше: 720Вт; • загальна потужність, що може віддаватися на живлення PoE пристроїв (PoE бюджет) з додатковим блоком живлення, не менше: 1440Вт;	
Необхідна початкова апаратна конфігурація компонент	• блоків живлення: повинен бути встановлений 1 блок живлення • блоків вентиляторів охолодження: - повинен бути встановлений повний комплект вентиляторів • повинна бути забезпечена відмовостійкість не гірше 1+1	
Характеристики масштабованості (не гірше)	• максимальна кількість записів MAC-адрес, не менше: 32 000 • максимальна кількість IPv4/IPv6 маршрутів, не менше: 32 000 / 16 000	
Підтримка протоколів та функцій рівня 2	• Віртуальні локальні мережі VLAN (IEEE 802.1Q) не менше 2000; • Протокол Spanning Tree (стандарти IEEE 802.1D STP, IEEE 802.1w (RSTP), IEEE 802.1s (MSTP)); • Протокол Multiple VLAN Registration Protocol (MVRP); • 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;	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Протокол IEEE 802.1AB (LLDP); • Підтримка надвеликих (Jumbo) фреймів розміром не менше 9К	
Підтримка протоколів та функцій рівня 3	• статичні маршрути для IPv4/IPv6; • протоколи динамічної маршрутизації IPv4: RIP, BGP, OSPFv2 та ISIS; • протоколи динамічної маршрутизації IPv6: RIPng, BGP+, OSPFv3 та IS-IS for IPv6; • протокол резервування віртуальних маршрутизаторів IPv4 (VRRP); • протокол резервування віртуальних маршрутизаторів IPv6 (VRRPv3); • виявлення двонаправленої передачі (BFD); • маршрутизація за призначеними політиками (PBR); • балансування трафіку за маршрутами з однаковою метрикою (ECMP) • протокол реєстрації багатоадресних груп (IGMP), з підтримкою версій IGMP v1, v2, v3 • протокол багатоадресної маршрутизації PIM для IPv4 та IPv6, включаючи PIM-DM, PIM-SM, PIM-SSM; • підтримка технології Multiprotocol Label Switching (MPLS), включаючи: • протокол розподілення міток Label Distribution Protocol (LDP); • мультипротокольні розширення протоколу BGP (MP-BGP);	
Підтримка протоколів та функцій безпеки	• списки контролю доступу для вхідного та вихідного трафіку, що дозволяють використовувати поля заголовків рівня 2, 3 та 4, можливість застосовувати правила ACL з урахуванням дати/часу;	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• протоколи автентифікації, авторизації та обліку (AAA): • RADIUS, TACACS+; • керування доступом на основі визначених ролей; • системний журнал; • захищений протокол віддаленого керування SSHv2	
Підтримка віртуалізації комутаторів	• можливість об'єднання декількох комутаторів в один віртуальний пристрій (стек), що має єдине управління, виглядає як один вузол для мережевих протоколів L2/L3, в тому числі можливість крос-шасі LACP агрегації з'єднань до іншого активного обладнання; • Повинна підтримуватись можливість об'єднання в стек не менше 9 комутаторів.	
Підтримка функцій та протоколів моніторингу та управління	• Протокол SNMPv1, v2, v3; • Протокол sFlow (RFC 3176); • Протокол Remote monitoring (RMON); • Протокол синхронізації часу Network Time Protocol (NTP); • Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил; • Дзеркалювання трафіку (створення копії трафіку що відповідає визначеним умовам (порт, VLAN, ACL) та передача його на локальний або віддалений порт моніторингу);	
Функції відмовостійкості та високої доступності	• Підтримка резервування компонент пристрою: блоків вентиляторів охолодження, блоків живлення;	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Підтримка гарячої заміни блоків вентиляторів охолодження, блоків живлення; • Підтримка ОС можливості встановлення патчів без переривання обслуговування; • Підтримка функціональності оновлення ОС без переривання обслуговування (ISSU).	
Простір, який займається у серверній шафі	• Не більше 1 U	
Вимоги до сервісної підтримки у складі пропозиції	• Термін не менше 36 місяців; • Повинна включати заміну компонент, що вийшли з ладу, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника, а також ремонт на технічному майданчику місцезнаходження обладнання в разі необхідності. • Послуга повинна надаватися в режимі 9 х 5 з часом реагування 2 години	

2.3. Точка доступу Wi-Fi

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Форм-фактор та виконання	• точка для використання в приміщеннях із внутрішніми антенами • в комплект поставки включено монтажний комплект для монтажу на рівну поверхню.	
Основні апаратні характеристики	• два радіо (WiFi) для одночасної роботи в діапазонах 2,4 ГГц та 5 ГГц та підтримкою 2x2 MIMO;	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• підтримка стандартів IEEE 802.11n, IEEE 802.11ac wave 2, IEEE 802.11ax ; • максимальна швидкість бездротової передачі даних (data rate) в діапазоні 2,4 ГГц –547 Мбіт/с; • максимальна швидкість бездротової передачі даних (data rate) в діапазоні 5 ГГц –1200 Мбіт/с; • мережеві інтерфейси для підключення до дротової мережі: 1 x 100/1000Base-T; • підтримка можливості одночасної роботи з декількома клієнтами на різних просторових потоках (MU-MIMO) • підтримуються наступні варіанти живлення: від комутатора з підтримкою POE 802.3af/at; • від AC адаптера. • для діапазону 2.4GHz: 21 дБм • для діапазону 5 GHz: 21 дБм • додаткове радіо Bluetooth Low Energy (IEEE 802.15), що може використовуватись в якості бездротового консольного інтерфейса або для взаємодії з підтримуваною IoT інфраструктурою що використовує цей протокол;	
Підтримуються наступні режими роботи	• Автономний; • Кластер (або «віртуальний контролер») з централізованим управлінням та моніторингом групи точок без використання виділеного апаратного контролеру; • Інфраструктурний режим з виділеним апаратним контролером (можливе переведення точки під управління контролера при подальшому зростанні інфраструктури);	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Точка поставляється з ПЗ та ліцензіями для роботи в кластері.	
Характеристики масштабованості	• Максимальна кількість клієнтів на радіо: 50 • Максимальна кількість SSID на радіо: 16 • При роботі в кластері: • Максимальна кількість точок в єдиному кластері: 128 • Максимальна кількість SSID на кластер: 6	
Підтримуються наступні протоколи та функції управління радіочастотним ресурсом (RRM)	• Автоматичний оптимальний вибір радіочастотних каналів та потужності випромінювання між точками в кластері; • Автоматичне переведення клієнтських пристроїв, що підтримують роботу в двох діапазонах 2,4 та 5 ГГц в менш завантажений частотний діапазон (band steering); • Автоматичне динамічне регулювання потужності випромінювання та радіочастотних каналів точок кластеру в разі відмови однієї з точок кластеру або змін в оточенні для усунення зон із поганим покриттям; • Спектральний аналіз: моніторинг оточення для динамічного виявлення та класифікації джерел радіочастотної інтерференції в робочих діапазонах, як Wi-Fi так і не-Wi-Fi походження, в тому числі мінімізація інтерференції від сотових мереж 3G/4G. • Вся перелічена функціональність підтримується для режиму «кластера». В запропоновану конфігурацію включені всі ліцензії, необхідні для підтримки переліченої функціональності.	
Підтримуються наступні протоколи та функції безпеки	• відповідність IEEE 802.11i (WPA2) та WPA3 Enterprise/CNSA, Personal (SAE), Enhanced Open (OWE)	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• автентифікація клієнтів бездротової мережі з використанням MAC-автентифікації, попередньо погодженого ключа (pre-shared) спільного для всіх пристроїв або індивідуального (MPSK), 802.1X (підтримуються протоколи EAP-PEAP, EAP-TTLS та LEAP та ін.); • можливість автентифікації користувачів з використанням вбудованого RADIUS серверу та зовнішнього RADIUS серверу (наявні режими коли кластер/віртуальний контролер виконує роль RADIUS проксі та коли кожна точка кластеру конфігурується як окремий RADIUS клієнт); • можливість автентифікації гостей вбудованого веб-порталу (captive portal) з використанням внутрішньої або зовнішньої бази автентифікації; • можливість визначення типу та ОС клієнтського пристрою за непрямими ознаками (OS Fingerprinting); • контроль доступу до мережі та призначення політик безпеки та якості обслуговування на основі ролі користувача; • розширення стандарту 802.11 щодо забезпечення захисту службових фреймів 802.11w • Вся перелічена функціональність підтримується для режиму «кластера». В запропоновану конфігурацію включені всі ліцензії, необхідні для підтримки переліченої функціональності.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Підтримуються наступні протоколи та функції якості обслуговування	• Балансування клієнтів/навантаження між всіма радіо точок кластеру; • Динамічний вибір та асоціація клієнта з оптимальною для нього точкою доступу; • Можливість призначення політик якості обслуговування для SSID або групи користувачів • Розширення стандарту 802.11 щодо забезпечення та покращення роботи роумінгу в бездротовій мережі: 802.11r, 802.11k, 802.11h, 802.11v; • Забезпечення рівного доступу клієнтів різних поколінь (802.11ac, 802.11n, 802.11a, 802.11g, 802.11b) до радіоефіру в змішаних оточеннях (airtime fairness); • Вся перелічена функціональність підтримується для режиму «кластера». В запропоновану конфігурацію включені всі ліцензії, необхідні для підтримки переліченої функціональності; • Підтримується функціональність «меш» при роботі в режимі кластеру та інфраструктурному режимі.	
Підтримуються наступні протоколи та функції L2	• Віртуальні локальні мережі VLAN (IEEE 802.1Q) • Протокол IEEE 802.3az Energy Efficient Ethernet (EEE) • Протокол IEEE 802.1ab (LLDP);	
Підтримуються наступні протоколи та функції моніторингу та управління	• Єдиний веб-інтерфейс для управління кластером; • Протокол SNMPv1, v2, v3; • Протокол синхронізації часу Network Time Protocol (NTP);	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил; • Опція управління декількома кластерами з використанням «хмарної» системи управління; • Опція управління декількома кластерами з використанням централізованої «наземної» корпоративної системи управління. • Наявність засобів автоматизації конфігурування пристрою з системи централізованого управління без початкового настроювання адміністратором (zero-touch provisioning)	
Гарантія або сервісна підтримка	• До конфігурації включено всі ліцензії, необхідні для підтримки зазначеної функціональності у складі пропозиції • Термін не менше 36 місяців • Повинна включати заміну компонент, що вийшли з ладу, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника. • Послуга повинна надаватися в режимі 9 х 5 з часом реагування NBD	

2.4. Програмний модуль автентифікації і контроля Wired и Wireless (ZTNA)

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Загальні вимоги до платформ	• Система повинна являти собою єдину універсальну платформу, що поєднує в сеті функціонал AAA, NAC, BYOD та забезпечення гостьового доступу на базі інформації про користувачів і пристрої, що підключаються, їх стану, тип і іншої розширеної інформації в рамках єдиного набору політик доступу до мережі. • Система повинна мати можливість масштабування до 5 000 пристроїв, що підключаються на кожну фізичну або віртуальну інсталяцію (appliance). • Система повинна підтримувати роботу з будь-якої існуючої дротової, бездротової або VPN мережі. • Повинна бути доступна оболонка CLI для виконання початкової конфігурації та базового налаштування системи. • Система повинна забезпечувати шифрування внутрішнього диска чи файлів. • Можливість змішувати та поєднувати віртуальні та апаратні інсталяції системи в одному розгортанні. • Система повинна підтримувати розгортання у моделі управління out-of-band та забезпечувати підтримку кластеризації з резервуванням N+1. • Система повинна надавати можливість запускати будь-яку роль або функцію системи на будь-якому пристрої кластера.	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Система повинна бути доступна для використання як у апаратному захищеному пристрої, так і у вигляді віртуальної машини.	
Загальні функціональні вимоги	• Система повинна мати сучасний Web-інтерфейс, який повинен включати кілька інструментів підвищення продуктивності, такі як майстер налаштування і набір попередньо налаштованих шаблонів і політик. • Система повинна інтегруватися та підтримувати взаємодію з будь-яким типом мережевих пристроїв (провідні пристрої, бездротові пристрої, пристрої VPN) та підтримувати різні методи автентифікації (802.1X, MAC автентифікація, Web-аутентифікація через портал). • Має бути доступна можливість поетапного підходу до реалізації функціоналу системи, починаючи з елемента управління політиками доступу (на основі ролей), а потім з можливістю включення додаткових заходів безпеки: перевірка стану та налаштувань кінцевих пристроїв (endpoint health), контроль доступу до мережі для підводних пристроїв. • Система повинна включати повний набір інструментів для створення звітів, аналізу та усунення несправностей. Дані щодо спроб і подій доступу повинні бути організовані за допомогою елементів даних, що налаштовуються, які використовуються для створення графіків, таблиць і звітів. Кореляція подій автентифікації та авторизації користувачів та подій підключення та	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	автентифікації пристрою повинна підтримуватися. • Функціонал NAC (Network Admission Control) повинен підтримувати агентські та безагентські методи перевірки, агенти перевірки відповідності політикам для кінцевих пристроїв мають бути доступні для ОС Windows, Linux та Mac OS. На додаток до аутентифікації користувачів, система повинна збирати додаткову інформацію про кінцевий пристрій, виконувати додаткові перевірки відповідності на платформах Windows (запущені сервіси, процеси, наявність peer-to-peer програми, ключі реєстру, використання USB-пристроїв, встановлені hot-fixи і патчі в Windows), а також виконувати стандартні перевірки працездатності на платформах Linux та Mac (наявність антивірусу, антишпигунського ПЗ та міжмережевий екран). • Рішення має бути простим в установці як у вигляді апаратної платформи, так і у вигляді віртуальної машини, має підтримувати політики, засновані на ідентифікації та розширеної інформації про користувача для надання безпечного доступу до мережі, а також включати інтегрований набір функціональних можливостей у рамках єдиної платформи: • Повноцінний AAA сервер - RADIUS та TACACS+; • Механізм профілювання пристроїв; • Вбудоване керування гостьовими пристроями, реєстрація пристроїв;	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Web-інтерфейс керування системою з єдиною панеллю керування (dashboard); • Сховище даних для інформації про користувачів, пристрої, інформацію про події тощо; • Багаті політики контролю доступу з використанням інформації про користувачів, пристрої, їх характеристики та інші елементи доступу; • Інструменти автоматичного розгортання та інсталяції. • Повинна підтримуватись гнучка модель ліцензування, заснована на необхідній функціональності (Onboard, Posture, Guest Access). • Система повинна підтримувати кореляцію інформації про користувачів, пристрої, а також дані про події автентифікації для полегшення пошуку та усунення несправностей, відстеження подій тощо. • Функціонал AAA повинен забезпечити повний поділ джерел автентифікації та авторизації. Наприклад, повинна підтримуватися автентифікація через Active Directory , а авторизації із зовнішньої бази даних SQL. • Повинна підтримуватися автентифікація або авторизація LDAP, AD, Kerberos, Token серверів, баз даних SQL. • Повинна забезпечуватися підтримка кількох методів ідентифікації та профілювання користувачів та пристроїв:	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Інтегрована, на основі мережі, профіль пристроїв за допомогою протоколів SNMP, DHCP, HTTP, AD, ActiveSync • Аудит кінцевих пристроїв за допомогою сканування інструментами Nessus чи Nmap • Підтримка наступних інструментів для створення політик: • Попередньо налаштовані шаблони • Майстер налаштування • LDAP браузер для швидкого перегляду атрибутів AD • Симулятор політик для моделювання та ін перевірки цілісності політики • Підтримка наступних методів застосування політик: - Призначення VLAN за допомогою RADIUS IETF атрибутів та VSA - Призначення VLAN та налаштування порту через SNMP - Списки контролю доступу - як статично визначені на пристрої та застосовувані за номером ID, так і динамічно завантажувані ACL. - Ролі або будь-які інші атрибути RADIUS конкретного виробника, які підтримуються мережевим пристроєм. - Застосування політик за допомогою Агента - налаштування інтерфейсів і відправлення повідомлень користувача. • Підтримується підключення до кількох доменів Active Directory для аутентифікації 802.1x PEAP.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Потрібно підтримуватися комплексне розгортання інфраструктури PKI, де TLS автентифікація вимагає перевірки сертифіката клієнта з кількох CA trust chain. Необхідно також підтримувати сертифікат сервера AAA, підписаний зовнішнім CA для перевірки внутрішніх клієнтських сертифікатів, підписаних PKI. • Функціонал профілювання повинен бути включений до базової ліцензії системи. • Система повинна підтримувати запити відразу в декілька AD domain та AD forest.	
Вимоги до надійності та відмовостійкості	• Програмно-апаратне забезпечення підсистеми контролю доступу має підтримувати кластеризацію в будь-якій комбінації як через LAN, так і через WAN з'єднання, забезпечуючи необмежене масштабування, резервування та балансування навантаження. • Платформа повинна підтримувати кластеризацію з використанням out-of-band інтерфейсів та забезпечити модель резервування N+1. • Відмова основного вузла не повинна впливати на здатність системи продовжувати обслуговувати абонентів. • Система повинна підтримувати кілька режимів розгортання, включаючи централізований, розподілений або гібридний. • Продукт повинен мати інсталяційну базу і продаватися на ринку протягом принаймні 4-х років.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Система повинна мати можливість масштабування до 1 мільйона унікальних кінцевих точок авторизації.	
Вимоги до функціонала надання гостьового доступу	• Система має бути здатна забезпечувати як "спонсорський" гостьовий доступ, так і доступ через портал із самостійною реєстрацією абонента. • Гостьовий web портал повинен мати можливість налаштування та кастомізації інтерфейсу, а також підтримувати автоматичне налаштування для різних розмірів екрану (планшети, смартфони тощо). • Можливість автоматичного відправлення гостьових облікових даних SMS або електронною поштою. • Можливість налаштування деталей облікового запису, включаючи тимчасові інтервали коли активний обліковий запис, параметри пропускної здатності і т.д. • Рішення має бути здатним забезпечити рекламні послуги • Система повинна використовувати окремі бази даних для гостьових та корпоративних користувачів. • Повинне підтримуватися кешування MAC-адрес, щоб уникнути необхідності повторної автентифікації при наступних підключеннях гостьових користувачів. • Підтримка автоматичного підключення гостьових абонентів (без надсилання облікових даних по SMS або електронною поштою). • Можливість автоматичної аутентифікації та застосування політик доступу до пристроїв, які	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	не мають інтерфейсу користувача і не підтримують введення даних для самостійної реєстрації. • Підтримка систем одноразових паролів. • Підтримка імпорту гостьових облікових записів з можливістю надсилання облікових даних електронною поштою. • Підтримка імпорту пристроїв NAS для великого розгортання. • Підтримка режиму спонсорського підтвердження після самостійної реєстрації гостьового абонента. • Можливість заборонити доступ співробітників до гостьової мережі за допомогою корпоративних абонентських пристроїв. • Підтримка відображення сторінки входу зі статистикою сеансу (обсяг дозволеного та спожитого трафіку). • Підтримка збереження URL, так щоб користувачі отримували доступ до спочатку запитаної веб-сторінки після входу в систему . • Підтримка відображення різних сторінок веб-порталу залежно від місця підключення користувача до мережі. • Система має підтримувати роботу з різними виробниками мережного обладнання. • Повністю настроюваний портал самостійної реєстрації з елементами управління інтерфейсу користувача, такими як списки, вибір опцій (check list, radio button). • Підтримка самостійної реєстрації довірених клієнтів (партнерів тощо).	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Можливість аутентифікації гостьових абонентів через соціальні мережі.	
Вимоги до додаткового функціоналу	• Підтримка підключення персональних пристроїв із процесом самостійного встановлення сертифікатів (BYOD). • Унікальні сторінки порталу, залежно від типу пристрою – IOS, Android. • Підтримка відкликання сертифіката. • Кореляція користувача, пристрої та інформації аутентифікації для полегшення пошуку та усунення несправностей. • Автоматизована реєстрація пристроїв для забезпечення безпечного доступу та конфігурації 802.1x саплікантів. • Можливість інтеграції з Active Directory, з ідентифікацією користувачів та/або атрибутів пристрою.	
Гарантія або сервісна підтримка	• Термін не менше 36 місяців • Повинна включати, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника.	

2.5. Програмно-апаратний комплекс Next Generation Firewall

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Загальні вимоги	• Пропонована програмно-апаратна продукція повинна складатися з трьох 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), контролю доступу до ресурсів Інтернет (URL Filtering).	
Вимоги до продуктивності	• Пропускна здатність пристрою в режимі мережевого екранування із забезпеченням ідентифікації додатків і користувачів (змішаний трафік, appmix) – не менш 1.9 Гбіт/сек. • Пропускна здатність пристрою в режимі попередження і захисту від загроз (Application Control, IPS, Anti-Virus, Anti-spyware чи Anti-bot, Sandboxing, URL filtering та логування на пристрої) – не менш 1.0 Гбіт/сек. Цей показник повинен бути виміряний з http пакетами та розміром транзакції – 64КБ. Ці дані мають бути опубліковані на офіційному сайті виробника. • Пропускна здатність функціоналу IPsec VPN повинна бути не менше 1.8 Гбіт/сек. • Максимальна кількість нових сесій у секунду – не менш 13,000. • Максимальна кількість підтримуваних сесій – не менш 150,000.	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Вимоги до апаратних параметрів розгортання	• Підсистема повинна бути виконана у вигляді трьох пристроїв висотою не більш 1 Rack unit кожен, встановлених в стандартну монтажну стійку. • Встановлені блоки живлення (“PSU”) на пристрої ПАК повинні мати внутрішню відмовостійкість і можливість заміни “на гарячу”. Блоки живлення повинні бути сумісні з 100-240В (50-60Гц) змінного току. • 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 бути 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 10/100/1000 Rj45	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Щонайменше 4 оптичних порти стандарту 1G SFP • Щонайменше 4 оптичних порти стандарту 10G SFP+ • Порт управління (Management port) повинен бути програмно ізольований та апаратно знаходитися окремо від мережевих портів для обробки трафіку.	
Вимоги до підтримуваних протоколів і режимів функціонування	• 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 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 NAT у прозорому режимі.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• 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). • 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 зон безпеки – не менш 40 шт.	
Вимоги до функціоналу	• 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 суб інтерфейсів 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).	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Розпізнавання і блокування мережевих додатків на Layer-7 моделі OSI по трафіку, що проходить через мережевий екран; • 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; • 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; • 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, Novell eDirectory; • Можливість створення правил на основі груп користувачів та окремих користувачів. Система повинна зберігати інформацію про користувачів у відповідних логах.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Інтеграція з Microsoft Active Directory, повинна здійснюватися без змін в Active Directory та не повинна використовувати обліковий запис адміністратору Active Directory домену. • Можливість створення користувач-ай-пі меппінгу (user-IP mapping) завдяки парсингу syslog повідомлень відправлених системою що автентифікувала користувачів. • Можливість створювати та використовувати у правилах динамічні групи користувачів. • 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	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	на основі додатків, IP-адрес, DSCP, користувачів і груп користувачів; - Реалізація QOS для трафіка real-time, ідентифікованого на рівні додатків; - Можливість перемаркування QoS на основі адреси 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. • Правила безпеки можуть застосовуватися відповідно до географічних регіонів; до правила можна додати кілька географічних регіонів. • 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	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	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; • 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; • Інтерфейс керування мережевими екранами (веб і CLI) повинен бути уніфікований з підсистемою централізованого керування, логування, звітності, відновлення програмного забезпечення;	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Підтримка міток Cisco TrustSec SGT Tag; • Підтримка функціоналу динамічних груп адрес (Dynamic Address Group) та динамічних груп користувачів (Dynamic User Group) без необхідності встановлювати політики безпеки. • 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 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 • 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.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• 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.	
Вимоги до можливостей запобігання вторгнень, розпізнавання й блокування шкідливого або забороненого трафіка	• 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) • Безпечний віддалений доступ (Remote Access VPN) з перевіркою віддаленого хоста на відповідність вимогам (compliance check) • 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,	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	мережевих «worms», блокування передачі певного вмісту з використанням регулярних виразів, у тому числі для додатків, що використовують шифрування SSL і SSHv2; • Пристрій повинен мати наступні функції **системи протидії вторгнень (IPS):** - Можливість створення різних політик IPS для різних користувачів або груп користувачів. - 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: - Цей функціонал повинен працювати незалежно від порту і протоколу і повинен перевіряти весь IP трафік в Інтернет. - Виявляти запити на визначення (resolution requests) IP адрес командних центрів	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	ботнетів (Botnet command and control centers) і блокувати їх через ДНС запити. - Функціонал DNS Sinkhole у випадку запиту шкідливого доменного імені повинен видавати IP address призначену адміністратором. Таким, чином інфіковані системи можуть бути легко ідентифіковані. - Функціонал блокування відомих ботнетів за допомогою сигнатур. Система повинна надавати можливість адміністратору налаштовувати ботнет сигнатури. - Наступні дії для дій сигнатур повинні бути доступні: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip. - Різні політики Anti-spyware повинні створюватися для різних користувачів і груп користувачів. • Пристрій повинен мати **Anti-Virus функціонал** для виявлення і попередження з наступними можливостями: - Блокування відомого шкідливого ПО на основі сигнатур. - 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. - Можливість виключити антивірусні сигнатури із бази даних сигнатур (можливість задавати виключення). - Різні політики Anti-virus повинні створюватися для різних користувачів і груп користувачів.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	- Anti-virus повинен блокувати шкідливі файли, передані через протоколи FTP, HTTP, SMB, POP3. • Запропонована система повинна мати **<u>функціонал захисту від атак нульового дня</u>** 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	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	забезпечувати розширене охоплення файлів, сигнатури для яких ще не існують. - Запропоноване рішення повинно ідентифікувати користувачів, які завантажували шкідливі файли. • 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. - Функція фільтрації URL-адрес повинна мати функцію XFF (X-forwarded-for). - Можливість написання політик обмеження пропускної здатності для категорій URL-адрес. - 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	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	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. • 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 **віддаленого безпечного підключення (Remote Access VPN)** з наступними можливостями: - VPN клієнт повинен підтримати наступні ОС: Windows, MacOS, Android, Apple iOS	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	- Пристрій повинен підтримувати також безклієнтний доступ до ресурсів компанії (SSL VPN). - VPN клієнт повинен вміти працювати, використовуючи протокол IPSec, та мати можливість переключення на SSL/TLS - VPN клієнт повинен підтримувати аутентифікацію за допомогою сертифіката, включаючи попередню аутентифікацію (pre-logon) за допомогою машинного сертифікату - Пристрій повинен підтримувати логін користувача завжди увімкнений (always on), на вимогу (on demand), попередній вхід (pre-logon). - VPN клієнт повинен підтримувати функціональність профілів віддаленої перевірки хоста на відповідність заданим вимогам. - Профілі віддаленої перевірки хоста повинні включати: перевірки версії ОС, контроль встановлених патчів - Профілі перевірки віддаленого хоста повинні включати: перевірку на наявність зазначеного антивірусу, наявності шифрування, наявності резервної копії, DLP агенту, та/або корпоративного сертифікату - Профілі перевірки віддаленого хоста повинні включати в себе кастомізовані перевірки: наявність процесів і значень реєстру/plist • Міжмережевий екран повинен вміти будувати політики безпеки на основі відповідності профілям перевірки віддаленого хоста.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Додаткові обов’язкові вимоги до NGFW	• Більше одного адміністратора може одночасно змінювати конфігурацію пристрою. • 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. • Диски повинні замінюватися на “гарячу”. • Пристрій повинен мати можливість надсилати журнали за допомогою snmp, syslog з можливістю використання спеціально визначених фільтрів. • 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 програмного забезпечення, репутаційних баз та сигнатур безпеки (а саме - Application Control, IPS/IDS, Antivirus/Antimalware, Antispyware/Antibot, SSL Decryption, URL filtering, Data Filtering, Sandbox, IPSec та SSL VPN) протягом не менш ніж 36 місяців з дня активації NGFW.	
Вимоги до сервісної підтримки NGFW	• Термін не менше 36 місяців; • Повинна включати заміну компонент, що вийшли з ладу, доступ до оновлень ПЗ,	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	віддалену діагностику та підтримку з боку центру технічної підтримки виробника, а також ремонт на технічному майданчику місцезнаходження обладнання в разі необхідності.	

2.6. Програмний комплекс eXtended Detection and Response

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Вимоги до антивірусу наступного покоління:	• Рішення, яке пропонується, повинно передбачати локальний аналіз на основі машинного навчання та запобігати загрозам. • Рішення, яке пропонується, має забезпечувати запобігання загрозам за допомогою поведінкового динамічного аналізу запущених процесів • Рішення, яке пропонується, повинно забезпечувати запобігання експлойтів за допомогою аналізу технік експлуатації, а не використання сигнатур для наступних ОС: Windows, MacOS and LinuxOS. • Рішення, яке пропонується, має забезпечувати запобігання відомим загрозам на основі інформації про загрози, наприклад, хеш-сум файлів. • Рішення, яке пропонується, має забезпечувати автоматизовану інтеграцію із хмарною службою запобігання шкідливим програмам (пісочницею), із звітами про аналіз та підтримкою розміру файлу не менше 100 МБ.	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов’язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Рішення, яке пропонується, має забезпечувати можливість захисту від зворотної оболонки (reverse shell), включаючи ОС Windows, MacOS та Linux. • Рішення, яке пропонується, повинно передбачати разове та планове сканування кінцевих точок. • Рішення, яке пропонується, повинно забезпечувати захист від шкідливого програмного забезпечення, програм-вимагачів та безфайлових атак • Рішення, що пропонується, повинно передбачати єдиний легкий агент для кінцевих точок для захисту, виявлення та реагування на загрози	
Розширені вимоги до захисту кінцевих точок	• Рішення, яке пропонується, має забезпечувати можливості брандмауера хоста для операційних систем Windows та MacOS. • Рішення, яке пропонується, повинно забезпечувати повне шифрування диска для операційних систем Windows та MacOS. • Рішення, яке пропонується, має забезпечувати можливості керування пристроями USB для операційних систем Windows і MacOS. • Рішення, яке пропонується, повинно передбачати правила запобігання, що дозволяють забезпечити захист та оповіщення на основі правил поведінкового аналізу.	
Вимоги до розслідування	• Рішення, яке пропонується, має забезпечувати автоматизований аналіз першопричини (root cause analysis) будь-якого сповіщення (Alert), включаючи мережеві сповіщення, де доступні дані з кінцевої точки.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Рішення, яке пропонується, має забезпечувати можливість перегляду ланцюгів виконання, що ведуть до оповіщення. • Рішення, яке пропонується, повинно передбачати аналіз часової шкали, щоб бачити всі дії та попередження на часовій шкалі. • Рішення, яке пропонується, повинно передбачати можливість здійснення запитів щодо показників компромісу (IoC) та поведінки кінцевих точок. • Рішення, яке пропонується, повинно передбачати запит щодо журналів мережевого трафіку від інтегрованих брандмауерів (міжмережевих екранів нового покоління). • Рішення, яке пропонується, має забезпечувати розширену мову запитів із підтримкою wildcard, регулярних виразів, JSON, агрегування даних, маніпулювання полями та значеннями, об’єднання даних з різних джерел та візуалізації даних. • Рішення, яке пропонується, повинно передбачати деталізовану фільтрацію та сортування результатів запиту • Рішення, що пропонується, повинно передбачати ідентифікацію того, чи подію заблокував агент кінцевої точки, брандмауер або інша технологія запобігання. • Рішення, яке пропонується, має забезпечувати автоматичне зшивання (об’єднання) оповіщень безпеки, таких як оповіщення брандмауера, до даних з кінцевих точок. • Рішення, яке пропонується, повинно забезпечити аналітиків контекстом тактик,	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	технік та процедур (ТТП) зловмисників, щоб використовувати отримані знання для допомоги у майбутніх розслідуваннях.	
Вимоги щодо управління інцидентами	• Рішення, що пропонується, повинно передбачати автоматичне групування відповідних повідомлень (алєртів) з різних джерел в один інцидент. • Рішення, яке пропонується, повинно містити перелік помічених артефактів з повідомлень та відповідну інформацію розвідувальних даних про загрози. • Рішення, яке пропонується, повинно містити список користувачів та хостів, які беруть участь у інцидентах, щоб швидко визначити масштаб інциденту. • Рішення, яке пропонується, має передбачати опціональне об’єднання інцидентів • Рішення, яке пропонується, повинно передбачати можливість надсилання даних про інциденти стороннім системам управління інцидентами. • Рішення, яке пропонується, повинно забезпечити можливість зміни рівня критичності інциденту.	
Вимоги до розвідки загроз (Threat Intelligence)	• Рішення, яке пропонується, має забезпечувати можливість повідомлення про відомі шкідливі об’єкти на кінцевих точках за допомогою правил ідентифікаторів (IOC rules). • Рішення, яке пропонується, повинно передбачати можливість автоматичного сканування історичних даних на наявність ідентифікаторів, коли вони додаються до системи, та видавати попередження.	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Вимоги до реагування	• Рішення, яке пропонується, має забезпечувати можливість віддаленого терміналу для ОС Windows, Linux та MacOS. • Рішення, яке пропонується, має забезпечувати повну підтримки для команд та сценаріїв консолі командної строки CMD, PowerShell та Python у Windows 7, 8 та 10. • Рішення, яке пропонується, має забезпечувати повну підтримку команд в Bash та Python на macOS та Linux • Рішення, яке пропонується, повинно забезпечувати можливість віддаленої ізоляції однієї кінцевої точки або декількох кінцевих точок підряд. • Рішення, яке пропонується, має забезпечувати віддаленого видалення файлу на одній з кінцевих точок або на декількох кінцевих точок підряд. • Рішення, яке пропонується, має забезпечувати можливість перегляду, призупинення або завершення запущених процесів або завантаження двійкових файлів за допомогою графічного диспетчера завдань для ОС Windows, macOS та Linux • Рішення, яке пропонується, має забезпечити графічний менеджер роботи з файлами з можливістю перегляду, завантаження, перейменування або переміщення файлів для Windows, macOS та Linux • Рішення, яке пропонується, має забезпечувати інтеграцію з брандмауерами для блокування доступу до шкідливих IP-адрес або доменів	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
Вимоги до видимості та виявлення загроз	• Рішення, яке пропонується, повинно забезпечувати поведінкову аналітику для профілю поведінки та виявляти аномалії, що свідчать про атаку, аналізуючи мережевий трафік, події кінцевих точок та події користувача з часом • Рішення, яке пропонується, повинно передбачати заздалегідь визначені та настроюванні правила виявлення на основі поведінки • Рішення, яке пропонується, має забезпечувати можливість отримання даних розвідки загроз із сторонніх джерел у форматах JSON та CSV • Запропоноване рішення повинно забезпечувати виявлення методів атаки протягом усього життєвого циклу атаки, включаючи виявлення, поперечний рух, взаємодію з центрами управління та контролю (CnC) та ексфільтрацію • Запропоноване рішення повинно забезпечити здатність виявляти тактики та техніки нападників за допомогою оцінок MITRE ATT&CK • Рішення, яке пропонується, має забезпечувати можливості управління вразливостями для відображення переліку вразливих виправлень ОС та програм із оцінками CVE. • Рішення, яке пропонується, повинно проводити інвентаризацію хоста з детальною інформацією про користувача, систему та додатки	
Вимоги до збору даних	• Рішення, яке пропонується, повинно забезпечувати можливість збору даних, описаних нижче - Інформація про користувача	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	▪ Домен та відмінне ім’я (Distinguished name) ▪ Поштова адреса ▪ Зареєстрований користувач (Logged-in user) ▪ Типовий користувач машини ▪ Користувач, який створює процес, що ініціював з’єднання ▪ Дані користувача з різних джерел, включаючи журнали мережевого трафіку, журнали подій Windows - Інформація про пристрій ▪ MAK-адреса (MAC address) ▪ Назва хосту пристрою ▪ Доменне ім’я ▪ Відмінне ім’я хосту (Distinguished name of host) ▪ Операційна система та версія - Інформація про процеси ▪ Мітка часу процесу ▪ Шлях та назва ▪ Ідентифікатор процесу ▪ Завантажені модулі ▪ Значення хешу, такі як MD5 і SHA-256 ▪ Аргументи командного рядка ▪ Запити RPC та дані введення коду, якщо це можливо ▪ Стан підпису - Інформація про створення, запис, доступ, відкриття, перейменування чи видалення файлу ▪ Мітка часу ▪ Шлях та назва	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	▪ Попереднє ім’я файлу та шлях до подій із перейменуванням файлу ▪ Значення хешу, такі як MD5 і SHA-256 ▪ Ім'я користувача - Мережева активність, включаючи вихідну, вхідні, та невдалі підключення ▪ Мітка часу ▪ IP-адреса джерела, IP-адреса призначення, порт джерела та порт призначення ▪ Кількість надісланих та отриманих байтів ▪ Протокол ▪ Дані геолокації ▪ Інформація про проксі ▪ Інтеграція з брандмауерами наступного покоління для повної видимості 7 рівня моделі OSI, включаючи назву програм/застосунків ▪ Тривалість з’єднання ▪ Дані рівня транзакції та розширена інформація про ключові протоколи, такі як DNS, HTTP, DHCP, RPC, ARP та ICMP - Дії реєстру, такі як створення ключа, зміна ключа, видалення ключа та перейменування ключа ▪ Мітка часу ▪ Назва ключа ▪ Значення та тип ▪ Попередня назва ключа до події перейменування - Системні події	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	▪ Подія зміни статусу користувача, наприклад, вхід в систему та вихід з неї ▪ Подія зміни стану хоста ▪ Подія зміни статусу агента	
Підтримка систем кінцевої точки агентом та вимоги до ресурсів кінцевих точок	• Рішення, яке пропонується, має забезпечувати підтримку всіх останніх версій Windows, включаючи Windows Server • Рішення, яке пропонується, має забезпечувати підтримку всіх останніх версій macOS та Mac OS X. • Рішення, яке пропонується, має забезпечувати підтримку захисту Android та Chrome OS • Рішення, яке пропонується, має забезпечувати підтримку всіх основних дистрибутивів Linux • Рішення, яке пропонується, має забезпечувати середнє використання центрального процесора менше 3% при ввімкнених усіх послугах • Рішення, яке пропонується, має передбачати опціональну можливість автоматичного оновлення агента • Рішення, яке пропонується, повинне передбачати опціональну можливість оновлення агента за допомогою peer-to-peer технології • Рішення, яке пропонується, повинно забезпечувати підтримку non-persistent VDI	
Вимоги щодо збереження даних	• Рішення, яке пропонується, повинно забезпечити видимість поперечного руху по мережі та інших частинах інфраструктури • Рішення, яке пропонується, має забезпечувати постійний збір та централізоване зберігання всіх даних безпеки для поведінкової аналітики	

Характеристики	Вимоги	Відповідність та опис запропонованих товарів[1]
	• Рішення, яке пропонується, повинно забезпечувати збереження даних щонайменше 30 днів • Рішення, яке пропонується, повинно передбачати опціональне збереження даних протягом необмеженого періоду часу • Рішення, яке пропонується, має передбачати один рік зберігання журналів аудиту адміністративно-розшукової діяльності	
Гарантія або сервісна підтримка	• Термін не менше 36 місяців • Повинна включати, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника.	

2.7. Супутні послуги

Послуга	Вимоги	Відповідність та опис запропонованих товарів[1]
Впровадження захищеної мережевої інфраструктури (LAN, Wi-Fi)	• аналіз існуючої інфраструктури (IP адресація, маршрутизація, локації встановлення тощо). • підготовка низькорівневого дизайну нової інфраструктури (LLD). • підготовка плану включення в продуктивну мережу. • монтаж та комутація обладнання. (включаючи монтаж AP Wi-Fi). • запуск та налаштування комутаторів L2 та L3 рівнів моделі OSI (порти управління, порти комутації тощо).	

[1] По-позиційно вказати відповідність (так/ні) та навести детальний опис параметру. Обов'язково надаються копії технічних документів виробника, які підтверджують заявлену характеристику

Послуга	Вимоги	Відповідність та опис запропонованих товарів[1]
Впровадження керуючого модулю ZTNA та інтеграція з усіма складовими (LAN, Wi-Fi, NGFW)	• аналіз існуючої віртуальної інфраструктури (IP адресація, маршрутизація, локації встановлення тощо). • розгортання модулю у віртуальній інфраструктурі. • налаштування модулю (порти управління, мережеві доступи, тощо). • поступове налаштування усіх мережевих компонентів та їх підключення до модулю. • аналіз працездатності (спостереження за роботою користувачів та додатків, потенційні жалоби користувачів тощо).	
Впровадження Next Generation Firewall (NGFW)	• визначення периметру який потребує захисту. • підготовка та погодження плану включення в продуктивну мережу враховуючи дані отримані на попередньому етапі. • монтаж та комутація обладнання. • запуск та налаштування NGFW (порти консолі управління, порти комутації тощо). • поетапне включення NGFW в продуктивну мережу. • перевірка “видимості” сегментів мережі. • аналіз працездатності продуктивної мережі (спостереження за роботою додатків, потенційні жалоби користувачів тощо). • розгортання консолі управління міжмережевими екранами та підключення в неї всіх екземплярів NGFW.	
Впровадження XDR	• аналіз існуючих ОС в Інформаційних Системах та їх розташування по сегментам. • конфігурація центру керування програмним комплексом XDR включаючи рольову модель доступу для подальшого адміністрування.	

Послуга	Вимоги	Відповідність та опис запропонованих товарів[1]
	• налаштування політик в режимі моніторингу з метою вивчення особливостей функціонування інфраструктури, її користувачів та додатків (для внутрішніх поведінкових моделей необхідний мінімальний час збору аналітики - 2 тижні). • розгортання агентів на робочих станціях та серверах. • налаштування політик згідно виявленого security baseline в ДП “МЗУ”. • аналіз рівня фолс-позітів та тру-позітів (спостереження за роботою операційних систем, жалоби користувачів тощо). • інтеграція програмно-апаратного комплексу XDR з мережевими апаратно-програмними рішеннями для подальшої підготовки до збору подій інформаційної безпеки. • налаштування збору подій інформаційної безпеки з сегментованої мережі, серверів та робочих станцій з метою подальшого використання.	

2.7.1. В рамках **виконання** *договору Виконавець має надати наступні супутні послуги:*

- Розробка технічної документації;
- Встановлення, налаштування, та інтеграцію поставлених комплектів програмно-апаратних рішень відповідно до Технічних Вимог:
  - Мережевих комутаторів L2 та L3 рівня;
  - Точок доступу Wi-Fi;
  - Програмного забезпечення системи ZTNA;
  - Рішень мережевої безпеки NGFW;
  - Програмного забезпечення XDR
  - Додаткового програмного забезпечення (включаючи бази даних, тощо), зазначеного Постачальником;
- Навчання персоналу Замовника.
- Приймальні випробування.

2.7.2. Технічна документація повинна містити наступні документи::

- Архітектура комплексу
- Схеми мережевих зав'язків, інтеграції комплексу та опис інфраструктури
- Технічне завдання для кожного із елементів комплексу
- Керівництво операторів комплексу
- Програми та методики приймальних випробувань комплексу

2.7.3. Вимоги до встановлення, налаштування, та інтеграції

Для встановлення, налаштування, та інтеграції представники ДП «МЗУ» повинні надати Постачальнику:

- необхідні налаштування з боку інформаційних систем, які необхідні для реалізації інтеграції з ними;
- надані канали зв'язку та усі необхідні дозволи для підключення інженерів Виконавця до інформаційної системи ДП «МЗУ»;
- підготовлений перелік фахівців та інших відповідальних осіб з боку ДП «МЗУ»;
- виділені усі необхідні апаратні ресурси для розгортання елементів комплексу (згідно вимог вказаних у технічній документації)

Постачальник має виконати встановлення, налаштування, та інтеграцію поставлених в рамках Договору комплектів програмного забезпечення, а також приймальні випробування усіх функціональних систем з тим, щоб було забезпечено їх функціонування у відповідності до вимог, зазначених у Технічних вимогах, включаючи:

- Мережеві комутатори L2 та L3 рівня;
- Точки доступу Wi-Fi;
- Програмного забезпечення системи ZTNA;
- Рішень мережевої безпеки NGFW (Next-Generation Firewall);
- Програмного забезпечення XDR
- Додаткового програмне забезпечення (включаючи бази даних, тощо), зазначеного Постачальником.

2.7.4. Вимоги до навчання персоналу з адміністрування

Навчання персоналу ДП «МЗУ» з адміністрування модулів центру повинно бути проведено перед приймальними випробуваннями, і полягає у наступному:

- Виконавець проводить навчання не менше 2-ох фахівців ДП «МЗУ (за всіма системами, які перераховані в Технічній специфікації);

- Формат навчання: вебінар.

2.7.5. Вимоги до приймальних випробувань

Постачальник має виконати приймальні випробування усіх встановлених та налаштованих модулях комплексу з тим, щоб було забезпечено їх функціонування у відповідності до вимог, зазначених у Технічних специфікаціях.

- Приймання комплексу та його складових систем проводиться шляхом проведення приймальних випробувань. Приймальні випробування здійснюються приймальною комісією, в яку входять уповноважені представники ДП «МЗУ», Постачальника та інші особи відповідно до вимог договору на виконання робіт.
- Мета складається в підтвердженні працездатності компонентів системи і відповідності їх вимогам Технічних вимог.
- Види, склад, обсяг і методи випробувань визначаються програмою приймальних випробувань. Програми приймальних випробувань розробляється Постачальником і узгоджується ДП «МЗУ» не пізніше, ніж за 1 день перед початком випробувань.
- При виявленні під час приймальних випробувань недоліків, дефектів або інших відхилень від вимог технічного завдання, відповідні факти фіксуються в протоколі, в якому в тому числі вказується:
  - перелік недоліків (дефектів);
  - ступінь впливу зазначених недоліків на працездатність системи;
  - необхідні терміни усунення недоліків (дефектів).
- Протягом 10 робочих днів з моменту усунення недоліків, дефектів або інших відхилень від вимог до системи приймальна комісія повинна провести повторні приймальні випробування відповідного компонента.
- Результати приймальних випробувань оформлюються протоколом, який підписується членами Приймальної комісії з боку ДП «МЗУ». За фактом успішного проведення приймальних випробувань підписується Акт прийомки
- Виконавець повинен забезпечити Замовника документацією, яка відображає конфігурацію кожного елемента обладнання та самого обладнання взагалі, використовуючи скріншоти, лістинги команд, схему мережі, яка відображає фізичні з‘єднання обладнання із зазначенням використовуваних фізичних та логічних інтерфейсів – Технічний паспорт.

3. КВАЛІФІКАЦІЙНІ ВИМОГИ ДО УЧАСНИКА

1. Учасник має бути авторизованим партнером у виробників обладнання та ПЗ, яких він пропонує (потрібне офіційний лист від виробника або його офіційного представника в України).
2. Вимоги до персоналу Учасника, що буде залучений до виконання Договору: наявність спеціалістів, що мають досвід виконання аналогічних проектів (не менше 3 спеціалістів) наступних напрямків: керівник проекту (не менше 1 спеціаліста), інженер в сфері інформаційних, телекомунікаційних технологій або комп’ютерних систем (не менше 2 спеціалістів).

   Керівник проекту
   - Досвід управління проектами із впровадження мережевих рішень
   - вища освіта освітньо-кваліфікаційного рівня бакалавр або вище.

   Інженер в сфері інформаційних, телекомунікаційних технологій або комп’ютерних систем
   - Досвід роботи на проектах впровадження мережевих рішень.
   - вища освіта освітньо-кваліфікаційного рівня бакалавр або вище.

На підтвердження наявності спеціалістів надати документи, що підтверджують трудові відносини (трудова книжка, трудовий договір, наказ на призначення, цивільно-правовий договір, гіг-контракт чи інший тип закріплених відносин із спеціалістом) та сертифікати/свідоцтва про навчання, видані виробниками запропонованого Учасником програмного забезпечення/обладнання із відповідними документами (дипломами), що підтверджують рівень освіти.

3. Учасник має досвід виконання не менше одного аналогічного договору, а саме з постачання мережевого обладнання, серверів, програмного забезпечення із послугами по монтажу/налаштуванню/встановленню. На підтвердження надати копії виконаних договорів.

4. ГАРАНТІЙНІ ЗОБОВ'ЯЗАННЯ ТА ТЕХНІЧНА ПІДТРИМКА

1. Постачальник або виробник рішень програмного забезпечення повинен надавати їх технічну підтримку 24x7.
2. Постачальник або виробники рішень Програмного забезпечення повинні випускати оновлення в період життєвого циклу кожного із складових комплексу.
3. Постачальник або виробники апаратних рішень повинні надавати їх технічну підтримку 8x5, та повинні забезпечити можливість заміни несправного обладнання включно з терміном гарантії. Виконавець або виробник апаратних рішень повинні надавати повідомлення про закінчення термінів надання технічної підтримки та заміни несправного обладнання не менше ніж за один (1) рік.
4. Гарантійне обслуговування виробником програмно-апаратного комплексу 36 місяців з дати підписання Акту прийомки Товарів та Супровідних послуг.
5. Післягарантійне технічне обслуговування або подовження гарантійного обслуговування Постачальником або виробником:
6. По закінченні строку гарантійного обслуговування, за умовами аналогічними гарантійним та на підставі окремого договору.
7. З метою подальшого розвитку функціональності:
   - Постачальник повинен забезпечити можливість оновлення для виправлення помилок системи від виробника безкоштовно протягом усього періоду підтримки виробником, згідно з ліцензійною угодою та угодою технічної підтримки за умови наявності активного контракту технічної підтримки від виробника.
   - Постачальник повинен надавати оновлення версій від виробника згідно ліцензійних угод на програмне забезпечення за умови наявності активного контракту технічної підтримки від виробника

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

ДОДАТОК 3

до Запиту до подання цінових пропозицій № RFQ-1.1.17
Впровадження контрольованої та сегментованої мережі

[НА БЛАНКУ ОРГАНІЗАЦІЇ]

ЦІНОВА ПРОПОЗИЦІЯ

Міністерство охорони здоров'я України

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

Шановні панове,

Ми пропонуємо виконання договору № RFQ-1.1.17 «Впровадження контрольованої та сегментованої мережі» відповідно до «Технічних вимог», які надаються разом із цією ціновою пропозицією, за ціною договору _____(сума прописом і цифрами) (_____) (назва валюти)_____.

Ця цінова пропозиція і ваше письмове повідомлення про її прийняття становитимуть зобов'язання укласти з вами договір за формою, наведеною у Запиті до подання цінових пропозицій № RFQ-1.1.17. 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 дана цінова пропозиція є дійсною протягом 45 (сорока п'яти) діб з кінцевої дати надання цінової пропозиції зазначеної у п.5 Запиту до подання цінових пропозицій № RFQ-1.1.17.

_____ Дата: _____

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

П.І.Б. уповноваженої особи Виконавця: _____

Назва Виконавця: _____
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 Запиту до подання цінових пропозицій № RFQ-1.1.17
Впровадження контрольованої та сегментованої мережі

ДОГОВІР № RFQ-1.1.17/___

м. Київ _____ 2023 р.

Цей Договір укладено в день, місяць та рік, зазначені вище, між Міністерством охорони здоров'я України (далі – Покупець), в особі _____, який діє на підставі _____, 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 «Додаткове фінансування проекту "Екстрене реагування на COVID-19 та вакцинація в Україні"» (далі - Проект), що фінансується відповідно до Угоди про позику між Україною та Міжнародним банком реконструкції та розвитку (далі - Банк) від 13 грудня 2021р. № 9315-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 до ДП «Медичні закупівлі України» на адресу: м. Київ, вул. Хрещатик, 22, не пізніше 180 (сто вісімдесят) 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 по кожній поставці всіх зобов'язань за Договором, окрім гарантійних

зобов’язань. Постачальник може здійснювати поставку Товарів частинами, але не більше двох (2) поставок.

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 13 грудня 2021р. № 9315-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 __ _____ 2023 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:
	Розрахунковий рахунок
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	

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 № RFQ-1.1.16/_____
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.