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

1. Замовник:	
Назва замовника	Національний фонд досліджень України
Код за ЄДРПОУ	42734019
Місцезнаходження	01001, м. Київ, вул. Бориса Грінченка, 1
2. Номер закупівлі в електронній системі Prozorro	UA-2025-11-04-015011-a
3. Предмет закупівлі:	
Вид предмета закупівлі	Відкриті торги з особливостями
Конкретна назва предмета закупівлі	Міжмережевий екран (шлюз безпеки фарм-фактор 1U)
Коди та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності)	ДК 021:2015: 32420000-3 — Мережеве обладнання
4. Обґрунтування очікуваної вартості предмета закупівлі, розмір бюджетного призначення	Очікувану вартість предмету закупівлі визначено відповідно до Наказу Міністерства розвитку економіки, торгівлі та сільського господарства України № 275 від 18.02.2020 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі» (далі – Методика). Метод, що застосовано відповідно до Методики: розрахунок очікуваної вартості товарів/послуг на підставі отриманих комерційних пропозицій. Розмір бюджетного призначення – 1 076 970,00 грн (один мільйон сімдесят шість тисяч дев'ятсот сімдесят гривень 00 копійок) з ПДВ
5. Строк поставки товарів (надання послуг, виконання робіт)	до 15 грудня 2025 року
6. Обґрунтування технічних та якісних характеристик предмета закупівлі	**Загальні вимоги до предмету закупівлі**: 1. Товар, запропонований Учасником, повинен бути новим (таким що не був у використанні) та відповідати параметрам, зазначеним в технічних вимогах Замовника (Таблиця 1) з обов'язковим відображенням порівняльних характеристик. Має бути зазначена назва торгової марки (виробника), модель пристрою, країна походження Товару *(надати гарантійний лист).* 2. Гарантійний лист від Учасника, що Товар, який пропонується ним до постачання, є оригінальним, не контрафактним та офіційно завезеним на територію України. 3. Товар обов'язково повинен мати оригінальну упаковку виробника, яка не може бути пошкодженою або заміненою на іншу. 4. Якість Товару повинна відповідати вимогам, нормам, правилами та стандартам якості, що встановлені до такого виду Товару та є загальнообов'язковими на території України (*надати гарантійний лист, складений у довільній формі, із зазначенням відповідності товару вимогам, вказаним в цьому пункті)*. 5. Виробник Товару або Учасник мають забезпечити гарантійне сервісне обслуговування Товару протягом гарантійного строку, який

	передбачений відповідно до рекомендації Виробника Товару (*надати гарантійний лист із зазначенням сервісних центрів в місті Києві)*. 6. Учасник гарантує, що Товар не обтяжений ніякими зобов'язаннями перед третіми особами (у тому числі не є об'єктом застави) і по відношенню до нього не існує інших обставин, що обмежують можливість його придбання та використання Замовником (*надати гарантійний лист*). 7. В ціну Товару включаються всі витрати з урахуванням податків і зборів, що сплачуються або мають бути сплачені. Будь-які витрати Учасника, в тому числі всі транспортні витрати по доставці Товару до місця поставки, розвантаження Товару, занесення до приміщення Замовника за адресою: вул. Бориса Грінченка, 1, вважаються включеними в ціну за Товар та додатково не сплачуються Замовником (*надати гарантійний лист*). Поставка Товару повинна включати його доставку, розвантаження та налаштування фахівцями Учасника. Процес постачання має охоплювати такі етапи: 1. Інсталяція та первинна конфігурація Товару, налаштування у відповідності до технічних вимог Замовника. 2. Тестування функціональності: перевірка системи на відповідність необхідним вимогам безпеки та продуктивності. 3. Технічна підтримка на період інтеграції: супровід процесу введення в експлуатацію. Постійна технічна підтримка: забезпечення обслуговування протягом гарантійного строку використання Товару. **Міжмережевий екран Check Point 1600 Base Appliance with SandBlast subscription package, включаючи технічну підтримку рівня Premium Collaborative** **Гарантійні вимоги:** Гарантійні зобов'язання від виробника строком 36 (тридцять шість) місяців з рівнем підтримки Premium Collaborative, що відповідає щонайменше наступним параметрам: 1. Щоденний (9/5) прийом заявок через офіційний спеціалізований ресурс (веб-сайт, чат-бот, телефон тощо). 2. Необмежена кількість відкриття заявок (кейсів) на протязі дії гарантійного строку. 3. Час реакції на відкриту заявку найвищого рівня критичності щодо проблеми або заміни компоненту Комплексу - не більше 30 (тридцяти) хвилин. Під найвищим рівнем критичності розуміється помилка або режим роботи Комплексу, що призводять до катастрофічного наслідку (наприклад, Комплекс повністю не працездатний й не виконує заявлені функції). 4. Час реакції на відкриту заявку інших рівнів критичності щодо проблеми або заміни Комплексу - не більше 4 (чотирьох) годин. Під іншими рівнями критичності розуміється будь-яка аномалія або режим роботи Комплексу, що погіршують продуктивність послуги, що надається, або частково обмежують її використання (наприклад, відбувається зависання або збій деяких компонентів Комплексу), при цьому, наслідки такого режиму роботи лише частково (або несуттєво) впливають на загальну функціональність Комплексу та систем, з якими він взаємодіє, а саме: Помилка, яка веде до зменшення продуктивності або відчутно обмежує функціональність Комплексу. Комплекс можливо використовувати в обмеженому режимі, при непрацездатних його

	додаткових компонентах. Комплекс можливо використовувати, але деякі функції недоступні. Приклад: систематичне зависання. Помилки приводять до мінімального впливу на використання Комплексу, існують помилки в роботі ліцензійного програмного забезпечення. Помилка може приводити до певних функціональних обмежень Комплексу. Приклад: незначний системний або операційний збій, помилки в журналах системи. Аномалія, яка в незначній мірі обмежує зручність використання Комплексу. Дана проблема може бути передана розробникові як запит на поліпшення Комплексу. Помилки, які носять несистематичний характер і не приводять до серйозних обмежень у використанні програмно-апаратного комплексу. До даної категорії звернень відноситься також і надання консультацій по функціональних можливостях продукту або зміні існуючої конфігурації. 5. Підтримка від виробника в режимі 5x9. 6. Доступ до виправлень та оновлень програмного забезпечення виробника. 7. Доступ до баз сигнатур, репутації, перевірки на предмет загроз тощо для сервісів захисту, що є складовою Комплексу. 8. Доступ до баз знань виробника рівня та доступ до технічних форумів виробника. 9. Стандартна заміна обладнання (без локального підмінного фонду в Україні). **Фізичні вимоги:** 1. Один WAN порт 10/100/1000 Base-T стандарту RJ-45 (1GbE Copper/Fiber). 2. Один DMZ порт 10/100/1000 Base-T стандарту RJ-45 (1GbE Copper/Fiber). 3. Шістнадцять мережевих портів 10/100/1000 Base-T стандарту RJ-45 (1GbE Copper). 4. Два порти стандарту USB 3.0. 5. Один консольний порт стандарту USB-C та один консольний порт стандарту RJ-45. 6. Робота в мережах змінного струму напругою 100-240 В частотою 50-60 ГЦ, підключення в звичайну розетку типу 7. Окреме місце для підведення заземлюючого кабелю (клеми). **Функціональні вимоги:** 1. Наявність функціоналу створення відмовостійких конфігурацій Active/Passive на рівні 2 або 3 мережевої моделі OSI. 2. Наявність функціоналу брандмауера (Firewall), в тому числі - відстеження стану з'єднань (stateful inspection). 3. Наявність функціоналу інтеграції з каталогами користувачів Замовника (LDAP, AD тощо) з метою отримання різноманітних даних про користувачів (належність до групи, телефон, підрозділ тощо) та застосування правил до груп або окремих користувачів. 4. Наявність функціоналу віддаленого безпечного підключення користувачів до інфраструктури Замовника (VPN з'єднання типу Site to Client) й побудови безпечних з'єднань між віддаленими сайтами Замовника (VPN з'єднання типу Site to Site). 5. Наявність функціоналу контролю доступу користувачів до веб-ресурсів (URL Filtering або аналог). 6. Наявність функціоналу аналізу об'єктів (файлів), що перевіряються екраном, за допомогою сигнатурного аналізу антивірусу (Antivirus або аналог).

	7. Наявність функціоналу аналізу об’єктів (файлів), що перевіряються екраном, за допомогою евристичного аналізу та техніками машинного аналізу та штучного інтелекту. 8. Наявність функціоналу аналізу об’єктів (файлів, посилань, листів тощо), що перевіряються мережевим екраном, за допомогою емуляції в окремому апаратному або хмарному середовищі («пісочниці» \ Sandbox або аналог) з метою виявлення раніше невідомих загроз (0day або аналог). 9. Наявність функціоналу запобіганню з’єднань з командними центрами зловмисників та сайтами зловмисників (що використовуються з метою завантаження шкідливих додатків), а також функціонал виявлення мережевих з'єднань, характерних для комунікацій ботів та бот-мереж (Anti-Bot або аналог). 10. Наявність функціоналу виявлення на рівні 7 (відповідно до мережевої моделі OSI) застосунків по сигнатурам (Application Control або аналог). 11. Наявність функціоналу аналізу трафіку на базі відомих сигнатур з можливістю детектування та блокування підозрілого або шкідливого потоку даних (IPS - Intrusion Prevention System або аналог). 12. Наявність функціоналу маршрутизації трафіку через декілька інтернет-з'єднань на основі продуктивності, таких як затримка або втрати пакетів. 13. Наявність функціоналу автоматично направляти певний трафік через оптимальні канали для кращої роботи додатків і більш ефективного використання ресурсів мережі. **Технологічні вимоги:** **1. Робота з мережевими стандартами та протоколами:** Підтримка статичної маршрутизації та протоколів динамічної маршрутизації BGP, OSPF v2, RIP. Підтримки режимів роботи Transparent та Bridge. Підтримка IPv6, включаючи ідентифікацію додатків та користувачів. Підтримка маршрутизації між VLAN. Підтримка тегування кадрів по 802.1Q. Підтримка розміру таблиці MAC-адрес та ARP-записів. **2. Побудова захищених тунелів, а саме:** Механізм побудови топології Site-to-Site VPN («кожен з кожним» або mesh). Механізм побудови топології Hub and Spoke VPN (віддалений майданчик з'єднується з іншим віддаленим майданчиком через центральний майданчик). Механізм побудови мереж типу Remote Access (Client-to-site) VPN з використанням спеціалізованого клієнтського програмного забезпечення. Механізм встановлення VPN мережі між кількома міжмережевими екранами, що мають динамічні публічні IP-адреси. Аналіз IPSec VPN що будується на основі сертифікатів, випущених власним центром сертифікатів. Аналіз IPSec VPN що будується на основі сертифікатів, випущених стороннім центром сертифікатів. **3. Інспектування за допомогою антивірусного(-их) механізму(-ів), механізмів виявлення бот-активності та механізмів виявлення атак на основі DNS, а саме:** Багаторівневий механізм детектування, котрий містить такі технології як репутаційна база IP-адрес, URL та DNS-адрес, а також

	аналізатор мережевих з'єднань, що виявляє ознаки, характерні для комунікацій ботів. Виявлення та блокування вірусів-шифрувальників (Wannacry, Cryptlocker, CryptoWall тощо) за допомогою статичного та динамічного аналізу. Виявлення та блокування об'єктів, що використовують фішингові атаки. Пошук загроз (вірусів) в архівах. Виявлення та запобігання вихідних комунікацій з C&C (Command Center) DNS з використанням таких функцій (технологій): - запобігання доступу користувачів до шкідливих веб-сайтів; - новлення репутації в режимі реального часу (в разі використання хмарних репутаційних сервісів виробника). 4. **Інспектування та контроль в трафіку застосунків (Application Control або аналог) та URL-фільтрація веб-ресурсів**, а саме: Механізм інспектування протоколів HTTP та HTTPv2, щонайменше – вхідного трафіку. Механізму створення правил фільтрації, що містить декілька URL-категорій. Виявлення в мережевому трафіку: - СКБД: Microsoft SQL, Oracle, DB2, Postgres, Sybase; - Файлових сервісів (щонайменше Microsoft SMB); - Систем електронного документообороту Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; - Протоколів обміну поштовими повідомленнями SMTP, POP3, IMAP; - Сервісів оновлень, щонайменше антивірусного програмного забезпечення Microsoft Update, Adobe, Java, Apple; - Протоколів для віддаленого доступу Telnet, SSH, VNC, Radmin; - Програмних додатків соціальних мереж та SaaS сервісів, щонайменше Skype, ICQ, Jabber, IRC, MSN, GoToMeeting,, Google Drive, Box, SkyDrive, WebDav, Facebook, Google+, Linkedln; Механізм створення правил що можуть застосовуватися до користувачів або групи користувачів або їх комбінації. Механізм категоризації програмних додатків та URL-адреси за ступенем ризику. Застосування створеного(-их) правила(-ил) щодо контролю програмних додатків та URL-фільтрації до конкретного користувача. База виробника з сигнатурами\даними що дозволяють: - Контроль (виявлення) програмних додатків, в кількості не менш ніж 9000 (дев'яти тисяч) штук. - Контроль категорій URL-ресурсів, в кількості не менш ніж 100 (сто) категорій. 5. **Інспектування об'єктів, за допомогою спеціального хмарного або локального середовища емуляції («пісочниці» \ Sandbox або аналог) для раніше невідомого шкідливого коду**, а саме: Механізм емуляції для об'єктів що надсилаються (скачуються або передаються) з веб-ресурсів що розташовані в інтернеті (незалежно від типу протоколу – HTTP, FTP, SMB тощо). Механізм емуляції бінарних файлів, архівних файли, документів Office та PDF, Java, Flash, щонайменше: .app, .bat, .csv, .com, .cpl , .dll , .dmg, .doc, .docx , .dot , .dotx, .dotm , .docm, .dylib, .exe , ..hwp , .iso , .iqy, .lnk, .msi, .msg, .o, .PIF , .pdf , .pkg, .ppt, .pptx, .pps , .pptm , .potx , .potm , .ppam, .ppsx , .ppsm , .ps1, .rtf, .elf, .scr, .sldx, .sldm, .slk, .swf,

	.udf, .uue, .xlt , .xls , .xlsx , .xlm, .xltx , .xlsm , .xltm , .xlsb, .xla , .xlam , .xll, .xlw, .udf, .img, .sh, .one, .wsf. Механізм емуляції файлів, що передаються наступними протоколами: HTTP, HTTPS, FTP, SMTP, CIFS (SMB), SMTP TLS. Механізм емуляції в різних середовищах емуляції, що емулюють роботу в операційних системах, щонайменше: Windows XP, Windows 7, Windows 8, Windows 10 . Механізм, що запобігає потраплянню в корпоративну мережу файлів, що проходять емуляцію, до результатів такої емуляції (функціонал Prevent). Механізм статичної фільтрації (за сигнатурами, поведінковим контролем, репутацією тощо) на стадії, що передує емуляції. Механізм емуляції файлів, розмір котрих перевищує 50 MB. Механізм виявлення загроз, що використовують складні техніки типу return oriented programming (ROP) та інші (наприклад, ескалацію привілеїв) шляхом відслідковування виконання інструкцій на рівні фізичного центрального процесора та оперативної пам'яті (не на рівні процедур та системних викликів операційної системи). 6. **Запобігання вторгненням (IPS або аналог),** а саме: Механізм детектування: сигнатур експлойтів, виявлення аномалій мережевих протоколів, контроль застосунків та наявність технік виявлення, що базуються на аналізі поведінки. Механізм детектування та запобігання наступним загрозам: нелегітимне використання протоколів, комунікація зловмисного програмного забезпечення з центрами зловмисників, спроби створення тунелів та загальні атаки без попередньо визначених (відомих) сигнатур. Механізм детектування та блокування з'єднань P2P, а також застосунків, що намагаються обійти захист екрану. Механізм задавання мереж та хостів, які повинні бути виключені з аналізу системою запобігання вторгненням. Механізм захисту від підміни DNS-імен в кеші (DNS Cache Poisoning), а також механізм запобігання доступу користувачів до заблокованих доменних адрес. Механізм захисту протоколів VOIP на базі сигнатур. Механізм виявлення та блокування застосунків для віддаленого контролю та управління, в тому числі таких застосунків, що підтримують можливість тунелювання через веб-трафік (HTTP\HTTPS). Механізм блокування вхідного та\або вихідного трафіку, керуючись критерієм належності джерела до тієї чи іншої країни, без необхідності ручного визначення груп IP-адрес, що репрезентують ту чи іншу країну. База виробника з сигнатурами для запобігання вторгненням в кількості не менш ніж 12000 (дванадцять тисяч) сигнатур. **7. Можливість гнучкої маршрутизації трафіку за допомогою SD-WAN :** Механізм динамічної маршрутизації: SD-WAN автоматично вибирає найкращий маршрут для трафіку на основі різних критеріїв, таких як затримка, втрата пакетів і пропускна здатність. Наявність політик маршрутизації: Адміністратори мають можливість налаштовувати політики маршрутизації в залежності від типу трафіку (наприклад, відео, VoIP) або джерела трафіку. Агрегація з'єднань: SD-WAN має можливість об'єднувати кілька типів з'єднань (наприклад, MPLS, LTE, широкосмуговий доступ) для підвищення надійності та пропускної здатності.

	Функціонал відновлення з'єднань: У разі відмови одного з з'єднань, SD-WAN повинен автоматично перенаправляти трафік через альтернативні з'єднання. Можливість шифрування: SD-WAN повинен здійснювати шифрування трафіку між філіями та центральною мережею, що забезпечує безпеку даних при їх передачі. Звіти і аналітика: Наявність функіоналу генерації звітів про використання мережі, продуктивність з'єднань і безпеку допомагає приймати обґрунтовані рішення. **Вимоги продуктивності:** 1. Пропускна здатність, при ввімкненому модулі запобігання вторгненням (**IPS** – **Intrusion Prevention System** або аналог) – *не менш ніж **3500Мбіт/сек** (три тисячі п'ятсот мегабіт в секунду)*. 2. Пропускна здатність, при ввімкненому модулі віддаленого контрольованого підключення користувачів (**VPN** на базі шифрування AES-128) - *не менш ніж **3200Мбіт/сек** (три тисячі двісті мегабіт в секунду).* 3. Пропускна здатність, при ввімкненому модулі брандмауера (**Firewall**) – *не менш ніж **4800Мбіт/сек** (чотири тисячі вісімсот мегабіт в секунду)* для реальних тестів в середовищі наближеному до реального та *не менш ніж **8Гбіт/сек** (вісім гігабіт в секунду)* для тестових середовищ (з використанням UDP пакетів розміром 1518Байт). 4. Пропускна здатність, при ввімкнених разом модулів: - брандмауера (**Firewall**), - запобігання вторгненням (**IPS** або аналог), - контролю додатків (**Application Control** або аналог) - та одночасному записі подій в журнал подій – *не менш ніж **3200Мбіт/сек** (три тисячі двісті мегабіт в секунду).* *5.* Пропускна здатність, при ввімкнених разом модулів: - брандмауера (**Firewall**), - запобігання вторгненням (**IPS** або аналог), - контролю додатків (**Application Control** або аналог), - контролю веб-ресурсів (**URL Filtering** або аналог), - активного антивірусного захисту (**Antivirus**), - захисту від бот-активностей (**Anti-Bot** або аналог), - перевірці в спеціальному середовищі емуляції (типу «пісочниця» \ **SandBox** або аналог) - та одночасному записі подій в журнал подій – *не менш ніж **1500Мбіт/сек** (одна тисяча п'ятсот мегабіт в секунду).* *6.* Кількість максимально можливих одночасних з'єднань – *не менш ніж **2 400 000** (два мільйони чотириста тисяч)*. Кількість максимально можливих з'єднань за секунду часу – *не менш ніж **55 000** (п'ятдесят п'ять тисяч).* **Обґрунтування:** посилання на конкретну торгівельну марку Товару пов'язане із запланованою закупівлею програмної продукції Check Point Smart-1 Cloud to manage 5 SMB (Gaia Embedded) gateways with up to 3 GB daily logs 3 months retention, including SmartEvent blade та програмної продукції Check Point Harmony Endpoint Advanced – Including Sandboxing, Web Protection, Attack Investigation, Threat Prevetion, Access Control and Threat Intelligence, включаючи технічну підтримку рівня Standart Collaborative Enterprise (для 80 кінцевих точок) з метою створення єдиного комплексу захисту мереж та кінцевих точок користувачів від єдиного виробника Check Point, що значно

	спростить адміністрування та задовільнить повний спектр потреб Замовника в інформаційній безпеці, розширену функціональність, сучасну підтримку, надійний і ефективний захист ІТ-інфраструктури Замовника.