Виконуючому обов'язки директора Спеціалізованого комунального підприємства «Київтелесервіс» Чернікову Павлу Олександровичу

Начальника відділу інформаційної безпеки Стревалюка Антона Сергійовича

СЛУЖБОВА ЗАПИСКА

місто Київ «31» серпня 2022 року

Конкретна назва предмета закупівлі – Засіб зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки); 32420000-3 – Мережеве обладнання за ДК 021:2015 Єдиного закупівельного словника).

Обґрунтування доцільності закупівлі:

Забезпечення захисту від загроз інформаційної безпеки, шляхом оновлення системи захисту периметру Міської мережевої інфраструктури що забезпечить більш детальну інспекцію трафіку на наявність інформаційних загроз, а також забезпечення своєчасного доступу до оновлень ПЗ та сигнатур безпеки, відповідно до пункту 16.9 «Створення, розвиток, модернізація та супроводження сервісної мережевої інфраструктури та мереж доступу» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 13.03.2022 № 4547/4588).

Обґрунтування обсягів закупівлі:

Проведення робіт із покращення захисту від загроз інформаційної безпеки, шляхом оновлення системи захисту периметру Міської мережевої інфраструктури що забезпечить більш детальну інспекцію трафіку на наявність інформаційних загроз, а також забезпечення своєчасного доступу до оновлень ПЗ та сигнатур безпеки. Постачальник зобов'язується поставити Замовнику товар та надати супутні послуги з урахуванням технічних вимог.

Обґрунтування якісних характеристик закупівлі:

Предмет закупівлі повинен відповідати технічним, якісним та кількісним вимогам, наданим у Додатку 1.

Технічні вимоги до предмета закупівлі рекомендовані протоколом № 65 від 26 серпня 2022 року засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 – 2022 роки.

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 41 929 380,4 (сорок один мільйон дев'ятсот двадцять дев'ять тисяч триста вісімдесят гривень 40 копійок) з ПДВ.

Джерело фінансування закупівлі – місцевий бюджет, КЕКВ 3210 Капітальні трансферти підприємствам (установам, організаціям).

Процедура закупівлі – відкриті торги з публікацією англійською мовою.

Вид предмету закупівлі – товар.

Кількість товарів – 2 (дві) штуки.

Місце поставки товарів – 03113, Україна, Київська область, місто Київ, вулиця Дегтярівська, будинок 37 (ЦОД КМДА).

Строк поставки товарів – по 31 грудня 2022 року.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 3 - 8 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 9 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 10 арк.

Ініціатор закупівлі _____ **А. С. Стревалюк**

«ПОГОДЖЕНО»:

Головний бухгалтер _____ **Г. А. Букша**

Заступник головного бухгалтера з Економічних питань _____ **Ю.В. Волочаєва**

Провідний юрисконсульт _____ **В. В. Тихонов**

Заступник директора з технічних питань _____ **О. Ф. Поліщук**

Перший заступник директора _____ **О.О. Биструшкін**

Додаток 1

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ)

Придбання засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки); 32420000-3 – Мережеве обладнання за ДК 021:2015 Єдиного закупівельного словника).

На виконання пункту 16.9 «Створення, розвиток, модернізація та супроводження сервісної мережевої інфраструктури та мереж доступу» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 13.03.2022 № 4547/4588).

Метою закупівлі є покращення захисту від загроз інформаційної безпеки, шляхом оновлення системи захисту периметру СКП «Київтелесервіс», що забезпечить більш детальну інспекцію трафіку на наявність інформаційних загроз.

Склад закупівлі :

Засіб зв'язку для забезпечення захисту периметру мережі, аналізу трафіку, забезпечення антивірусних інспекцій та захисту від втручання зловмисників.

Вимоги до засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки)
Кількість – 2 комплекти.

Опис	Вимога
Загальні вимоги	Мережевий пристрій безпеки та SD-WAN маршрутизації повинен являти собою пристрій що здійснює інтелектуальну маршрутизацію трафіку (SD-WAN), інспекцію мережевого трафіку та захист корпоративної інфраструктури відповідно до нижченаведених вимог. Якщо відповідно до функціональності пристрою або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем, пристроїв або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки. Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення. На обладнання не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника. Усі функціональні вимоги та кількісні показники продуктивності повинні мати підтвердження у документації виробника.
Архітектура та форм-фактор	Програмно-апаратний комплекс (ПАК) для встановлення в стандартну монтажну шафу 19". Наявність Trusted Platform Module (TPM).

Інтерфейси та інтерфейсні модулі	Не менше ніж 16 * 10GE RJ45/1GE RJ45; Не менше ніж 16 * 25GE SFP28 / 10GE SFP+/ 1GE SFP; Не менше ніж 4 * 40GE QSFP+/100GE QSFP28; Не менше ніж 2 * 1/10GE SFP/SFP+ HA портів: Не менше ніж 2 * GE RJ45 management порт (OOB MGMT); Не менше ніж 1 * RJ45 консольний порт; Не менше ніж 1 * USB порт; Не менше ніж 2 * інтерфейсні модулі 10GE SFP+ (оптика, тип SR) у комплекті.
Живлення	2 блоки живлення (100-240V AC, 50-60 Hz), що підтримують "гарячу" заміну.
Маршрутизація та SD-WAN	Статична маршрутизація та маршрутизація по політиках (PBR); Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4; Одночасне використання фізичних та логічних інтерфейсів з різнотипними підключеннями (MPLS, broadband Internet, LTE, тощо) для ефективної маршрутизації трафіку; Оцінка якості каналів зв'язку SD-WAN шляхом відправлення пакетів чи запитів до певних вузлів у мережі або пасивними методами; Контроль характеристики каналів зв'язку в режимі реального часу (packet loss, jitter, latancy) та їх графічне відображення (gui real-time monitor); Контроль SLA для користувацьких додатків (applications) на основі характеристик каналів зв'язку (packet loss, jitter, latancy) у реальному часі; Визначення різнопланових алгоритмів/стратегій вибору каналів зв'язку для маршрутизації трафіку додатків та сервісів виходячи з критеріїв відповідності SLA, кращих значень характеристик каналів зв'язку, тощо; Визначення правил маршрутизації трафіку додатків та сервісів через канали SD-WAN з урахуванням алгоритмів/стратегій та SLA; Автоматичне балансування навантаження, переключення і резервування каналів зв'язку для користувацьких додатків та сервісів при зміні характеристик мережевих з'єднань (loss, jitter, latancy) у реальному часі; Динамічне виправлення втрати пакетів або відновлювання пакетів з помилками, що викликані несприятливими умовами WAN-каналів під час роботи через VPN - Forward Error Correction та Packet duplication; Балансування пакетів однієї сесії через декілька IPSec VPN тунелів.
Продуктивність сервісів безпеки	Кількість одночасних TCP-сесій: не менше ніж 24 000 000; Кількість нових TCP-сесій/секунду: не менше ніж 1 000 000; Пропуска здатність на пакетах розміром 450 байт або Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 17 Гбіт/с;

	Пропуска здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 20 Гбіт/с.
Продуктивність VPN	Пропускна здатність IPSec VPN: не менше ніж 55 Гбіт/с; Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 30 000; Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 100 000; Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 20 000.
Віртуалізація	Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10.
Висока доступність (high availability)	Active-Active; Active-Standby.
L2 функціонал та мережеві служби	Агрегація портів (802.3ad); VLAN (802.1Q та Trunking); Вбудовані DHCP, NTP, DNS сервера.
NAT	Статичний NAT; Динамічний NAT; PAT.
Multicast	Sparse та dense режим; Підтримка PIM.
Сервіси безпеки	Stateful Firewall; Ідентифікація та контроль застосувань (AC/AVC); Захист від загроз на основі сигнатурного аналізу (IPS); Захист від malware (Antivirus/AMP); Web та DNS-фільтрація; Інспектування/сканування SSL/TLS трафіку на загрози; Захист від невідомих загроз (0-day); Запобігання витоку даних (DLP); Захист від DOS-атак; IPSec VPN, SSL VPN; Аналізатор рівня безпеки NGFW.
Stateful Firewall	Режими роботи: NAT/маршрутизатор; прозорий режим (міст); Підтримка VoIP трафіку: глибока інспекція та захист від атак на протокол SIP; Виконання ролі проксі для аналізу, інспектування та забезпечення коректної роботи сесій різних протоколів (session helpers, application layer gateway).
Ідентифікація та контроль застосувань (AC/ AVC)	Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control); Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур; Конфігурація виключень у діях з певними додатками (exemption/override); Створення користувацьких (custom) сигнатур додатків

	Ідентифікація та контроль протоколів індустріальних систем ICS, SCADA.
Захист від загроз на основі сигнатурного аналізу (IPS)	Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system); Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур; Конфігурація виключень у діях з певними сигнатурами (exemption/override); Створення користувацьких (custom) IPS-сигнатур; Інспектування та застосування дій до протоколів індустріальних систем ICS, SCADA.
Захист від malware (Antivirus/AMP)	Anti-Virus / Anti-malware захист; Виявлення та блокування небажаних програм або файлів (grayware); Виявлення та блокування файлів на основі налаштованих порогових значень їх розміру для різних протоколів; Захист від зловмисних програм для мобільних пристроїв.
Web та DNS-фільтрація	Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація); Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація); Виявлення та блокування доступу до Botnet мереж; Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо); Статичні blacklists та whitelists.
SSL/TLS-інспекція	Перехоплення, розшифрування та інспекція HTTPS, FTPS-сесій, тощо; Конфігурація виключень з SSL/TLS-інспекції певних IP-адрес, URL, тощо (exemption/override); Інспектування SSL/TLS-сертифікату на відповідність певному web-ресурсу до якого здійснюється підключення та строку дійсності (SSL/TLS certificate inspection); Повноцінне інспектування контенту зашифрованих сесій (full SSL/TLS inspection); Інспектування SSL/TLS-трафіка має включати наступні інспекції: IPS, AC/AVC, AV/AMP, Web-фильтрацію, DLP.
Запобігання витоку даних (Data Loss Prevention)	Запобігання витоку конфіденційних даних шляхом перевірки трафіку (за назвою файлів, типом файлів, розміром файлів, регулярними виразами); Запобігання витоку конфіденційних даних шляхом перевірки трафіка за допомогою заздалегідь визначеної інформації (credit card numbers, SIN numbers, тощо); Функціонал DLP має запобігати витоку через наступні протоколи: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP, тощо.
Захист від DOS-атак	Можливість розпізнавання та блокування DoS атак: TCP Syn flood; TCP/UDP/SCTP port scan; ICMP sweep; TCP/UDP/SCTP/ICMP session flooding.

IPSec VPN, SSL VPN	Алгоритми шифрування: 3DES, AES128, AES192, AES256; Алгоритми хешування: MD5, SHA256, SHA384, SHA512 Diffie-Hellman Group: 1, 2, 5, 14 Підтримка Hub & Spoke топології, mesh топології, DMVPN/ADVPN або аналог.
Аналізатор рівня безпеки NGFW	Функціонал автоматичного визначення критичних вразливостей та слабкість конфігурації системи шляхом аналізу її налаштувань/конфігурації; Надання рекомендацій щодо приведення системи до стану, що відповідаю кращим практикам виробника, покращення безпеки та ефективності роботи системи; Аналіз системи на відповідність аудиторським перевіркам (PCI, тощо).
IoT	Виявлення та ідентифікація Internet of Things (IoT) пристроїв у мережі.
QoS	Traffic Shaping; Traffic Policing.
Автентифікація, авторизація та облік (AAA)	Локальна база даних користувачів; Підтримка протоколів LDAP, RADIUS, TACACS+; Підтримка 2-факторної автентифікації (two-factor authentication) на основі програмних токенів; Не менше ніж 2 програмні токени для встановлення на мобільні пристрої (смартфони); Single Sign-On: інтеграція с Windows AD; PKI та сертифікати: X.509, SCEP support, створення Certificate Signing Request (CSR), автоматичне поновлення сертифікатів до закінчення терміну дії, підтримка OCSP.
Керування, звітність, інтеграція	Графічний веб-інтерфейс (Web GUI); Інтерфейс командного рядка (CLI); Підтримка централізованої системи керування; Підтримка централізованої системи збору журнальних файлів, їх аналізу та побудови звітів; Ролевий доступ адміністраторів (RBAC); Підтримка REST API; Ведення журналів подій (logging); Функціонал запису пакетів з мережевих інтерфейсів для подальшого їх аналізу (packet capture); Функціонал резервного копіювання та відновлення файлів конфігурації; SNMP v1, v2, v3; sFlow v5 / Netflow v9 або аналог, syslog.
Технічна сервісна підтримка	Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 3 роки з рівнем сервісу 24*7; Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7; Постійний авторизований доступ до сайту виробника 24*7; Отримання актуальних репутаційних баз, сигнатур та всіх необхідних оновлень для сервісів безпеки; Отримання основних та проміжних релізів програмного забезпечення;

	Можливість реєстрації сервісних випадків в режимі 24*7; Доставка і заміна запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника).

Ініціатор закупівлі **А. С. Стревалюк**

Додаток 2

Кваліфікаційні критерії процедури закупівлі та перелік документів, що підтверджують інформацію учасників про відповідність їх таким критеріям

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність обладнання та матеріально-технічної бази**	Довідка в довільній формі за підписом уповноваженої особи учасника та завірена печаткою (у разі її використання) про наявність обладнання та матеріально-технічної бази, що будуть використовуватись для поставки товару, що є предметом закупівлі, із зазначенням найменування обладнання та матеріально-технічної бази, кількості та інформації про власність (власне/орендоване). Для підтвердження наявності матеріально-технічної бази необхідно надати скановані документи на право власності/користування офісу, технічного приміщення, складу чи іншого приміщення (документація має передаватися в PDF-форматі, сканована з оригіналу документу).
2.	**Наявність працівників відповідної кваліфікації, які мають необхідні знання та досвід**	Довідка в довільній формі за підписом уповноваженої особи учасника та завірена печаткою (у разі її використання), що підтверджує наявність в учасника працівників відповідної кваліфікації, які мають необхідні знання (вищу освіту) із зазначенням: посади, прізвища, ім'я, по батькові, освіти та загального стажу роботи.
3.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії: виконаного договору, видаткової видаткових) накладної (накладних), листа-відгука від замовника або інші документи, що підтверджують його виконання. ** Під аналогічним договором розуміється договір подібний за предметом закупівлі за період з 2014 року по теперішній час. Якщо в довідці учасник вказує декілька аналогічних договорів, то всі документи щодо підтвердження виконання таких договорів надаються щодо кожного із вказаних в довідці договорів.*
4.	**Інформація про технічні, якісні та кількісні характеристики предмета закупівлі**	Для підтвердження відповідності тендерної пропозиції технічним, якісним та кількісним характеристикам (вимогам) замовника Учасник у складі тендерної пропозиції повинен надати: 1) інформацію про можливість поставки товару з урахуванням технічних вимог; 2) інформацію у довільній формі щодо застосування Учасником заходів із захисту довкілля; 3) авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника,

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
		дистриб'ютора в Україні, який підтверджує наявність у Учасника статусу партнера та права на здійснення продажу запропонованого Учасником товару, виданого на адресу Замовника із посиланням на процедуру закупівлі.

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **А. С. Стревалюк**

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ)

Придбання засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки); 32420000-3 – Мережеве обладнання за ДК 021:2015 Єдиного закупівельного словника).

На виконання пункту 16.9 «Створення, розвиток, модернізація та супроводження сервісної мережевої інфраструктури та мереж доступу» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 13.03.2022 № 4547/4588).

Метою закупівлі є покращення захисту від загроз інформаційної безпеки, шляхом оновлення системи захисту периметру СКП «Київтелесервіс», що забезпечить більш детальну інспекцію трафіку на наявність інформаційних загроз.

Склад закупівлі :

Засіб зв'язку для забезпечення захисту периметру мережі, аналізу трафіку, забезпечення антивірусних інспекцій та захисту від втручання зловмисників.

Вимоги до засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки)

Кількість – 2 комплекти.

Опис	Вимога
Загальні вимоги	Мережевий пристрій безпеки та SD-WAN маршрутизації повинен являти собою пристрій що здійснює інтелектуальну маршрутизацію трафіку (SD-WAN), інспекцію мережевого трафіку та захист корпоративної інфраструктури відповідно до нижченаведених вимог. Якщо відповідно до функціональності пристрою або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем, пристроїв або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки. Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення. На обладнання не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника. Усі функціональні вимоги та кількісні показники продуктивності повинні мати підтвердження у документації виробника.

Архітектура та форм-фактор	Програмно-апаратний комплекс (ПАК) для встановлення в стандартну монтажну шафу 19". Наявність Trusted Platform Module (TPM).
Інтерфейси та інтерфейсні модулі	Не менше ніж 16 * 10GE RJ45/1GE RJ45; Не менше ніж 16 * 25GE SFP28 / 10GE SFP+/ 1GE SFP; Не менше ніж 4 * 40GE QSFP+/100GE QSFP28; Не менше ніж 2 * 1/10GE SFP/SFP+ HA портів: Не менше ніж 2 * GE RJ45 management порт (OOB MGMT); Не менше ніж 1 * RJ45 консольний порт; Не менше ніж 1 * USB порт; Не менше ніж 2 * інтерфейсні модулі 10GE SFP+ (оптика, тип SR) у комплекті.
Живлення	2 блоки живлення (100-240V AC, 50-60 Hz), що підтримують “гарячу” заміну.
Маршрутизація та SD-WAN	Статична маршрутизація та маршрутизація по політиках (PBR); Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4; Одночасне використання фізичних та логічних інтерфейсів з різнотипними підключеннями (MPLS, broadband Internet, LTE, тощо) для ефективної маршрутизації трафіку; Оцінка якості каналів зв'язку SD-WAN шляхом відправлення пакетів чи запитів до певних вузлів у мережі або пасивними методами; Контроль характеристики каналів зв'язку в режимі реального часу (packet loss, jitter, latancy) та їх графічне відображення (gui real-time monitor); Контроль SLA для користувацьких додатків (applications) на основі характеристик каналів зв'язку (packet loss, jitter, latancy) у реальному часі; Визначення різнопланових алгоритмів/стратегій вибору каналів зв'язку для маршрутизації трафіку додатків та сервісів виходячи з критеріїв відповідності SLA, кращих значень характеристик каналів зв'язку, тощо; Визначення правил маршрутизації трафіку додатків та сервісів через канали SD-WAN з урахуванням алгоритмів/стратегій та SLA; Автоматичне балансування навантаження, переключення і резервування каналів зв’язку для користувацьких додатків та сервісів при зміні характеристик мережевих з’єднань (loss, jitter, latancy) у реальному часі; Динамічне виправлення втрати пакетів або відновлювання пакетів з помилками, що викликані несприятливими умовами WAN-каналів під час роботи через VPN - Forward Error Correction та Packet duplication; Балансування пакетів однієї сесії через декілька IPSec VPN тунелів.
Продуктивність сервісів безпеки	Кількість одночасних TCP-сесій: не менше ніж 24 000 000; Кількість нових TCP-сесій/секунду: не менше ніж 1 000 000;

	Пропуска здатність на пакетах розміром 450 байт або Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 17 Гбіт/с; Пропуска здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 20 Гбіт/с.
Продуктивність VPN	Пропускна здатність IPSec VPN: не менше ніж 55 Гбіт/с; Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 30 000; Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 100 000; Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 20 000.
Віртуалізація	Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10.
Висока доступність (high availability)	Active-Active; Active-Standby.
L2 функціонал та мережеві служби	Агрегація портів (802.3ad); VLAN (802.1Q та Trunking); Вбудовані DHCP, NTP, DNS сервера.
NAT	Статичний NAT; Динамічний NAT; PAT.
Multicast	Sparse та dense режим; Підтримка PIM.
Сервіси безпеки	Stateful Firewall; Ідентифікація та контроль застосувань (AC/AVC); Захист від загроз на основі сигнатурного аналізу (IPS); Захист від malware (Antivirus/AMP); Web та DNS-фільтрація; Інспектування/сканування SSL/TLS трафіку на загрози; Захист від невідомих загроз (0-day); Запобігання витоку даних (DLP); Захист від DOS-атак; IPSec VPN, SSL VPN; Аналізатор рівня безпеки NGFW.
Stateful Firewall	Режими роботи: NAT/маршрутизатор; прозорий режим (міст); Підтримка VoIP трафіку: глибока інспекція та захист від атак на протокол SIP; Виконання ролі проксі для аналізу, інспектування та забезпечення коректної роботи сесій різних протоколів (session helpers, application layer gateway).
Ідентифікація та контроль застосувань (AC/ AVC)	Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control);

	Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур; Конфігурація виключень у діях з певними додатками (exemption/override); Створення користувацьких (custom) сигнатур додатків Ідентифікація та контроль протоколів індустріальних систем ICS, SCADA.
Захист від загроз на основі сигнатурного аналізу (IPS)	Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system); Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур; Конфігурація виключень у діях з певними сигнатурами (exemption/override); Створення користувацьких (custom) IPS-сигнатур; Інспектування та застосування дій до протоколів індустріальних систем ICS, SCADA.
Захист від malware (Antivirus/AMP)	Anti-Virus / Anti-malware захист; Виявлення та блокування небажаних програм або файлів (grayware); Виявлення та блокування файлів на основі налаштованих порогових значень їх розміру для різних протоколів; Захист від зловмисних програм для мобільних пристроїв.
Web та DNS-фільтрація	Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація); Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація); Виявлення та блокування доступу до Botnet мереж; Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо); Статичні blacklists та whitelists.
SSL/TLS-інспекція	Перехоплення, розшифрування та інспекція HTTPS, FTPS-сесій, тощо; Конфігурація виключень з SSL/TLS-інспекції певних IP-адрес, URL, тощо (exemption/override); Інспектування SSL/TLS-сертифікату на відповідність певному web-ресурсу до якого здійснюється підключення та строку дійсності (SSL/TLS certificate inspection); Повноцінне інспектування контенту зашифрованих сесій (full SSL/TLS inspection); Інспектування SSL/TLS-трафіка має включати наступні інспекції: IPS, AC/AVC, AV/AMP, Web-фильтрацію, DLP.
Запобігання витоку даних (Data Loss Prevention)	Запобігання витоку конфіденційних даних шляхом перевірки трафіку (за назвою файлів, типом файлів, розміром файлів, регулярними виразами); Запобігання витоку конфіденційних даних шляхом перевірки трафіка за допомогою заздалегідь визначеної інформації (credit card numbers, SIN numbers, тощо);

	Функціонал DLP має запобігати витоку через наступні протоколи: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP, тощо.
Захист від DOS-атак	Можливість розпізнавання та блокування DoS атак: TCP Syn flood; TCP/UDP/SCTP port scan; ICMP sweep; TCP/UDP/SCTP/ICMP session flooding.
IPSec VPN, SSL VPN	Алгоритми шифрування: 3DES, AES128, AES192, AES256; Алгоритми хешування: MD5, SHA256, SHA384, SHA512 Diffie-Hellman Group: 1, 2, 5, 14 Підтримка Hub & Spoke топології, mesh топології, DMVPN/ADVPN або аналог.
Аналізатор рівня безпеки NGFW	Функціонал автоматичного визначення критичних вразливостей та слабкість конфігурації системи шляхом аналізу її налаштувань/конфігурації; Надання рекомендацій щодо приведення системи до стану, що відповідаю кращим практикам виробника, покращення безпеки та ефективності роботи системи; Аналіз системи на відповідність аудиторським перевіркам (PCI, тощо).
IoT	Виявлення та ідентифікація Internet of Things (IoT) пристроїв у мережі.
QoS	Traffic Shaping; Traffic Policing.
Автентифікація, авторизація та облік (AAA)	Локальна база даних користувачів; Підтримка протоколів LDAP, RADIUS, TACACS+; Підтримка 2-факторної автентифікації (two-factor authentication) на основі програмних токенів; Не менше ніж 2 програмні токени для встановлення на мобільні пристрої (смартфони); Single Sign-On: інтеграція с Windows AD; PKI та сертифікати: X.509, SCEP support, створення Certificate Signing Request (CSR), автоматичне поновлення сертифікатів до закінчення терміну дії, підтримка OCSP.
Керування, звітність, інтеграція	Графічний веб-інтерфейс (Web GUI); Інтерфейс командного рядка (CLI); Підтримка централізованої системи керування; Підтримка централізованої системи збору журнальних файлів, їх аналізу та побудови звітів; Ролевий доступ адміністраторів (RBAC); Підтримка REST API; Ведення журналів подій (logging); Функціонал запису пакетів з мережевих інтерфейсів для подальшого їх аналізу (packet capture); Функціонал резервного копіювання та відновлення файлів конфігурації; SNMP v1, v2, v3; sFlow v5 / Netflow v9 або аналог, syslog.

Технічна сервісна підтримка	Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 3 роки з рівнем сервісу 24*7; Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7; Постійний авторизований доступ до сайту виробника 24*7; Отримання актуальних репутаційних баз, сигнатур та всіх необхідних оновлень для сервісів безпеки; Отримання основних та проміжних релізів програмного забезпечення; Можливість реєстрації сервісних випадків в режимі 24*7; Доставка і заміна запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника).

ПРОТОКОЛ № 65

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 - 2022 роки у 2021 – 2022 роках

м. Київ «26» серпня 2022 року

ПРИСУТНІ:

Члени робочої групи:
В. Жучков
В. Іцкович
І. Лагутіна
О. Поліщук
Т. Самойленко
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019–2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (із змінами) (далі – Програма), у 2022 році, а саме: проєктів технічних вимог до закупівель:

1.1. Придбання засобів зв'язку (мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки) (пункт 16.9 «Створення, розвиток, модернізація та супроводження сервісної мережевої інфраструктури та мереж доступу» переліку завдань і заходів Програми);

1.2. Доступ до глобальних мереж та сервісів (пункт 16.14 «Супровід та підтримка міської мережевої інфраструктури» переліку завдань і заходів Програми).

2. Різне.

По підпункту 1.1 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що з метою підвищення рівня кіберзахисту периметру мережі підприємства, аналізу трафіку, забезпечення антивірусних інспекцій та захисту від втручання зловмисників необхідно придбати відповідний засіб зв'язку та представив проєкт технічних вимог до

закупівлі «Придбання засобів зв’язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки)» (пункт 16.9 переліку завдань і заходів Програми).

В обговоренні брали участь: В. Жучков.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Придбання засобів зв’язку (мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки)» (пункт 16.9 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 6, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По підпункту 1.2 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що з метою реалізації програми «Wi-Fi в укриттях» для забезпечення учбового процесу під час повітряних тривог в закладах освіти восьми районів м. Києва необхідно забезпечити доступ до глобальних мереж та сервісів, функціонування міської мережевої інфраструктури Київської міської ради, виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста, та представив проєкт технічних вимог до закупівлі «Доступ до глобальних мереж та сервісів» (пункт 16.14 переліку завдань і заходів Програми).

В обговоренні брали участь: Д. Цвігун.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Доступ до глобальних мереж та сервісів» (пункт 16.14 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 6, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1414 **Дата реєстрації** 26.08.2022
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 26.08.2022 (Протокол № 65 від 26.08.2022)

Кількість файлів: 3 **Кількість ЕП:** 18

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
26.08.2022 № 075-1414

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Іцкович Вікторія Євгенівна **Кількість ЕП:** 3	29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ;	29.08.2022 11:01:44 Погодив;	29.08.2022 11:01:44 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 3	29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ;	29.08.2022 11:01:44 Погодив;	29.08.2022 11:01:44 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 3	29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ; 29.08.2022 11:01:44 ;	29.08.2022 11:01:44 Погодив;	29.08.2022 11:01:44 Погодив
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 3	26.08.2022 17:21:35 ; 26.08.2022 17:21:36 ; 26.08.2022 17:21:37 ;	26.08.2022 17:21:37 Погодив;	26.08.2022 17:21:37 Погодив

ЖУЧКОВ ВАСИЛЬ АНАТОЛІЙОВИЧ **Кількість ЕП:** 3	26.08.2022 16:29:08 ; 26.08.2022 16:29:09 ; 26.08.2022 16:29:10 ;	26.08.2022 16:29:10 Погодив;	26.08.2022 16:29:10 Погодив
ЛАГУТІНА ІННА ІГОРІВНА **Кількість ЕП:** 3	26.08.2022 16:02:32 ; 26.08.2022 16:02:34 ; 26.08.2022 16:02:35 ;	26.08.2022 16:02:35 Погодив;	26.08.2022 16:02:35 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 3	26.08.2022 15:45:37 ; 26.08.2022 15:45:45 ; 26.08.2022 15:45:47 ;		26.08.2022 15:45:47
Поліщук Олег Федорович (2684213893) **Кількість ЕП:** 3	26.08.2022 15:40:35 ; 26.08.2022 15:40:35 ; 26.08.2022 15:40:36 ;	26.08.2022 15:40:36 Погодив;	26.08.2022 15:40:36 Погодив

ALESTA

ТОВ «АЛЕСТА»
ЄДРПОУ 42232756 **ІПН** 422327526530
www.alesta.net.ua | info@alesta.net.ua | +380 50 326 49 49
02090, Україна, Київ, Харківське шосе, 19, офіс 2005

Вих. № 30/08/1
від «30» серпня 2022 р.

СКП «Київтелесервіс»

Комерційна пропозиція.

У відповідь на Ваш лист № 111-08/2022 від 26.08.2022 ТОВ «АЛЕСТА» висловлює свою повагу та вдячність щодо звернення.

Ознайомившись із наданою версією Технічних вимог СКП «Київтелесервіс» до планового предмету закупівлі Придбання засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки); 32420000-3 – Мережеве обладнання за ДК 021:2015 Єдиного закупівельного словника), надаємо нижче в таблиці інформацію щодо орієнтовної вартості:

Назва	Од. вим.	К-ть	Ціна за одиницю без ПДВ, грн	ПДВ за одиницю, грн	Ціна за одиницю з ПДВ, грн	Вартість з ПДВ, грн
Мережевий екран FG-2600F-EU 4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with FortiGate-2600F 3 Year Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and FortiCare Premium)	шт.	2	17 505 427,50	3 501 085,50	21 006 513,00	42 013 026,00
					Всього з урахуванням ПДВ, грн	**42 013 026,00**

Всього вартість запропонованого товару становить **42 013 026,00** грн. (Сорок два мільйони тринадцять тисяч двадцять шість гривень 00 копійок), у тому числі ПДВ
7 002 171,00 грн (Сім мільйонів дві тисячі сто сімдесят одна гривня 00 копійок).

Звертаємо Вашу увагу на те, що надана комерційна оцінка є орієнтовною та може бути уточнена відповідно до вимог закупівлі.

Директор ТОВ «АЛЕСТА» Блінов А.А.

«АЛЕСТА» Ідентифікаційний код 42232756

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 78/08-2022
Від 30 08 2022 р.

LLC BELINTECH UKRAINE
56 Valeriia Lobanovskoho ave.,
Kyiv, 03037, Ukraine
Tel: (044) 222 82 93
www.bitech.com.ua

Вих. № 30/08-01 від 30.08.2022

В.о. директора
СКП «КИЇВТЕЛЕСЕРВІС»
П. Чернікову

Щодо надання орієнтовної вартості

Шановний пане Черніков!

На Ваш запит від 26.08.2022 року за №112-08/2022 щодо надання орієнтовної вартості закупівлі Система аналізу, обробки та зберігання подій інформаційної безпеки ТОВ «БІЛІНТЕХ УКРАЇНА» повідомляє про наступне.

Згідно наданих технічних вимог надаємо розрахунок вартості та специфікацію зазначеного товару:

№ п/п	Найменування обладнання	Од. виміру	К-ть	Ціна без ПДВ, грн	ПДВ ,грн	Ціна з ПДВ, грн	Вартість з ПДВ, грн
1	Брандмауер FortiGate-2600F 4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with FortiGate-2600F 3 Year Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and FortiCare Premium)	шт.	2	17 426 217,50	3 485 243,50	20 911 461,00	41 822 922,00
Загальна вартість, грн з ПДВ							**41 822 922.00**

З повагою
Генеральний директор **В.В. Шахов**

ТОВ «БІЛІНТЕХ УКРАЇНА»
Юр. адреса: 03037, м. Київ,
Проспект Валерія Лобановського, буд. 56
Тел: (044) 222 82 93
www.bitech.com.ua
sales@bitech.com.ua

ЄДРПОУ 37962954
ІПН 379629526571
Св-во ПДВ № 200046963
п/р UA623006140000026009500220903
в АТ "КРЕДІ АГРІКОЛЬ БАНК"
МФО № 300614

ТОВ «ОПТІДАТА»
04071, м. Київ,
вул. Кожум'яцька, 10а, р/р
26004300941299 у філії ГУ по
м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020,
МФО: 322669, ЄДРПОУ: 39693067

Вих.№ 08312022/2 від 08.31.2022
На №113-08/2022 від 26.08.2022

СКП "КИЇВТЕЛЕСЕРВІС"
В.о. Директора
П. Чернікову

Комерційна пропозиція

ТОВ «ОПТІДАТА», розглянувши Ваш запит від 26.08.2022 року за № 112-08/2022, надає орієнтовну вартість на Придбання засобів зв'язку (Мережевий пристрій безпеки з доступом до оновлень сигнатур безпеки); 32420000-3 – Мережеве обладнання за ДК 021:2015 Єдиного закупівельного словника), відповідно до наданих технічних вимог:

№ п/п	Найменування	Од. виміру	Кількість	Ціна без ПДВ	Вартість без ПДВ
1	Мережевий екран FG-2600F-EU 4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with FortiGate-2600F 3 Year Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and FortiCare Premium)	шт.	2	17 480 080,50	34 960 161,00
				Всього без ПДВ, грн.	34 960 161,00
				ПДВ, грн.	6 992 032,20
				Всього з пдв,грн.	41 952 193,20

З повагою,
Генеральний директор
ТОВ «ОПТІДАТА»

Білик М.А.

info@optidata.com
www.optidata.com.ua