Інформація на виконання постанови Кабінету Міністрів України № 1266 від 16 грудня 2020 року

Автоматизоване робоче місце (Моноблок із ПЗ)

28.05.2021 р.

На виконання постанови Кабінету Міністрів України № 1266 від 16 грудня 2020 року, що вносить зміни до постанови КМУ від 11 жовтня 2016 року № 710 «Про ефективне використання державних коштів», ДУ «ГМЦ МВС України» (код ЄДРПОУ 08735882; адреса: вулиця Бердичівська, 1, м. Київ, 04116) надає інформацію про процедуру відкритих міжнародних торгів.

Назва предмету закупівлі: ДК 021:2015 – 30210000-4 Машини для обробки даних (апаратна частина)-Автоматизоване робоче місце (Моноблок із ПЗ).

Номер процедури закупівлі у електронній системі закупівель: UA-2021-05-27-003484-b.

Закупівля здійснюється за кошти державного бюджету згідно кошторисних призначень.

Визначення очікуваної вартості закупівлі здійснено згідно проведеного інтернет моніторингу цін за предметом закупівлі, та, враховуючи потребу. Орієнтовна вартість закупівлі становить – 750000,00 грн з ПДВ.

Технічні характеристики (вимоги) до предмету закупівлі наведені в тендерній документації відповідно до предмету закупівлі: : ДК 021:2015 – 30210000-4 Машини для обробки даних (апаратна частина)-Автоматизоване робоче місце (Моноблок із ПЗ) (30 комплектів):

Технічні вимоги Замовника	**Відповідність (так/ні) з обов'язковим посиланням на сторінку з технічної документації виробника**
Моноблок	
Процесор: - базова частота - не менше ніж 2,6 ГГц; - максимальна частота – не менше 3,5 ГГц; - кількість ядер - не менше ніж 2; - кількість обчислювальних потоків - не менше ніж 4; - кеш пам'ять 4 МБ або більше. Оперативна пам'ять: - Не менше 8 ГБ DDR4; - не менше ніж два слоти для оперативної пам'яті; - максимальний об'єм підтримуваної пам'яті – 32 Гб. Відео карта: Інтегрований відеоадаптер – так; Накопичувач - не гірше 256 ГБ SSD; Наявність CardReader – так, вбудований; Оптичний диск – так, вбудований. Комунікаційні технології - - З'єднування RJ-45; - Швидкість передачі даних по мережі (Ethernet), що підтримується – 100/1000 Мб/с; - Безпровідна технологія WiFi - не гірше 802.11ac; - Не гірше – Bluetooth 4.2. Звукова карта - Інтегрована HD-Audio. Наявність вбудованих динаміків. Екран - Діагональ екрану – не менше 21.5"; Роздільна здатність екрану – не менше 1920x1080; Тип матриці – не гірше IPS. Веб-камера - Наявність інтегрованої веб-камери – так, вбудована, не гірше 5 Мп; Роз'єми :	

- не менше HDMI порт – 1шт; - не менше USB – 4 шт, з яких не менше USB 3.2 Gen 1 – 2 шт; - не менше аудіопорт – 1 шт; Безпека: - наявність Trusted Platform Module; - наявність слоту для замка типу Кенсінгтон. Блок живлення – потужністю не більше 65 Вт та енергоефективністю не менше 89%; Операційна система – не гірше, ніж передвстановлена виробником Windows 10 Pro; Клавіатура та миша від виробника моноблоку – так, в комплекті поставки, USB. Гарантія - не менше 12 місяців від виробника (з можливістю відстеження строку гарантії на сайті виробника)	
Антивірусне програмне забезпечення	
Консоль керування • Формування списку систем за групами, як в ручному режимі так і синхронізації структури служби каталогів; • Розгортання модулів захисту в автоматичному та в ручному режимі; • Можливість пошуку в мережі систем, що не мають модулів захисту; • Підтримка розгорнутих систем в актуальному стані (оновлення ПЗ, синхронізація політик); • Контроль стану кінцевих точок в режимі реального часу (за наявності мережевого з'єднання); • Підтримка мінімум трьох гілок пакетів (поточний, попередній, випробування); • Автоматичне сортування систем за їх типом, апаратними ресурсами та іншими властивостями; • Побудова графіків, діаграм, звітів та інформаційних шкал за даними з кінцевих точок; • Побудова розгалуженої деревовидної структури дзеркал оновлення (SMB, Web, FTP); • Можливість призначати різні політики (налаштування) на рівні окремих систем та груп систем; • Вбудований механізм планування задач по розгортанню, оновленню та супроводу модулів захисту; • Можливість вибіркового виконання завдань на рівні структури компанії, групи або підгрупи, окремих кінцевих точок; • Зберігати каталог політик з можливістю їх копіювання та переналаштування під певні групи; • Наявність інструменту порівняння налаштувань політик та задач; • Обов'язковий журнал аудиту дій операторів консолі; • Рольова модель доступу з можливістю формування певних шаблонів рівня доступу; • Автентифікація по локальній базі користувачів та можливість використання облікових записів AD; • Прийом та обробку журналів подій із кінцевих точок; • Фіксований інтервал комунікації кінцевих точок із консоллю керування; • Можливість ініціалізації позапланового сеансу зв'язку як з боку консолі так і з кінцевої точки;	•

• Можливість налаштування інтервалу комунікації на рівні окремих кінцевих точок та груп; • Можливість синхронізації політик та трансферу керованих кінцевих точок між двома консолями керування; • Можливість вбудованого резервного копіювання бази даних; • Наявність вбудованого інструменту самодіагностики системи; • Можливість автоматизації типових дій, таких як автоматичне створення звітів з надсиланням їх на пошту відповідальним особам, періодичні видалення старих подій, синхронізація політик та задач між двома консолями тощо; • Підтримка передачі SNMP пасток для контролю за допомогою систем моніторингу мережі; • Підтримка передачі подій syslog на системи управління подіями безпеки; • Наявність API інтерфейсу для інтеграції зі сторонніми рішеннями. •	
Антивірусний захист • Сканування при доступі (т.з. On-Access) файлів, що зчитуються, записуються та їх тіньових копій • Зберігання інформації з минулої перевірки та використання кешу для прискорення сканування • Можливість використання хмарної або локальної перевірки репутації (в локальному розгорнутому сервері репутацій) контрольної суми файлу • Можливість блокування потенційно небезпечної поведінки додатків, не залежно від результатів сигнатурного та хмарного аналізів • Перевірка активного наповнення Web сторінок та поштових повідомлень • Можливість відправки файлу до локально розгорнутого рішення класу «Пісочниця» для захисту від складних загроз та проведення статичного та динамічного аналізу коду для упередження зараження цілеспрямованими загрозами або невідомими досі вірусними додатками • Можливість захисту налаштувань антивірусного модулю паролем (окремих або усіх) • Можливість автоматичного відновлення роботи захисних модулів якщо вони були призупинені користувачем • Система упередження вторгнень для серверних ОС з підтримкою захисту служб Web серверів • Наявність сигнатур по вразливостям серверних платформ та її своєчасне оновлення • Запобігання спроб експлуатації недоліків (вразливостей) серверних ОС та запущених додатків (Apache, Java, MySQL, CGI, PHP та ін.) • Мережевий брандмауер з підтримкою режиму навчання чи автоматичного режиму роботи • Наявність вбудованих правил для поширеного ПЗ (ОС, офісні та інтернет додатки) • Система упередження вторгнень з можливістю контролю пам'яті запущених процесів • Можливість захисту систем, які з різних причин не часто отримують оновлення ОС та ПЗ • Можливість перевірки репутації URL • Можливість блокування доступу до жерел певної категорії	•

• Створення т.з. «чорних списків» URL не залежно від їх репутації • Блокування спроб перехоплення системних служб та/або зупинки модулів захисту • Блокування запуску додатків та/або сценаріїв з каталогів тимчасових файлів • Блокування спроб реєстрації додатків у списку автозавантаження • Запобігання створення запускних файлів у системних каталогах • Блокування запуску додатків без цифрового підпису • Можливість створення власних правил захисту на рівні реєстру та файлової системи • Блокування запуску додатків без цифрового підпису • Захист налаштувань мережі, браузерів, захист від зміни файлових асоціацій • Активація механізму розподілу усіх запускних файлів за репутацією (Довірений, Невідомий, Підозрілий, Потенційно шкідливий, Підтверджено шкідливий) • Можливість блокувати запуск додатків по рівню їх репутації (довіри до них) • Локальний моніторинг, збір та накопичення контрольних сум (хешів) запускних файлів та їх репутації • Співставлення/перевірка репутації файлів із хмарним сервісом та локально розгорнутим севером репутацій • Можливість підключення бази даних про існуючі у світі загрози та кампанії атак, доступ до якої відбувається з консолі керування (див. вимоги «Консоль керування»); • База даних про існуючі у світі загрози та кампанії атак повинна мати детальний опис атакуючої кампанії, країн поширення, типу організацій, що знаходяться під атакою тощо та маркери компрометації кожної загрози; • Функціонал динамічної активації обмежень, що застосовуються для файлу, який запускає система чи користувач, а саме: • Заборона завершувати інші процеси • Заборона записувати в область пам'яті інших процесів • Зчитування чи зміна мережевих параметрів • Зчитування області пам'яті інших процесів • Зчитування та/або перезапис файлів на мережевих каталогах • Внесення змін до планувальника операційної системи • Зміна налаштувань вбудованого брандмауеру • Зміна біту атрибуту "тільки читання" • Зміна біту атрибуту "прихований" • Зміна списку/параметрів автозавантаження процесів; • Зміна файлових асоціацій за розширенням • Зміна екранних шпалер та/або зберігач екрану (скрінсейверу) • Запуск дочірніх процесів • Створення нових запускних файлів (.exe, .vbs, .job, .bat) • Спроба виділення пам'яті в області в іншому процесі • Зміна параметрів операційної системи	
Можливості інтеграції з Microsoft Defender (ОС Windows 10) • Можливість використання антивірусу Microsoft Defender у якості базового захисту одночасно з функціями посиленого захисту технологіями блокування атак нульового дня, захисту від безтілесних атак та технологіями машинного навчання. • Наявність спеціалізованого захисту від шифрувальників з можливістю усунення наслідків дій такого ПЗ (відкату змін файлів, ключів реєстру тощо) без використання точок відновлення. • Структуризація політик MS Defender Firewall та керування ними з єдиної консолі (див. вимоги «Консоль керування»)	•

• Керування функціями Exploit Guard в MS Defender з єдиної консолі керування (див. вимоги «Консоль керування») • Наявність інструменту візуалізації загроз та дій антивірусного рішення по реагуванню на вказані загрози.	
Контроль пристроїв • Моніторинг, примусове блокування або переведення в режим «readonly» зовнішніх носіїв (USB) • Моніторинг та/або блокування зовнішніх пристроїв на кшталт модемів, плат розширень та ін. • Можливість дозволити зарядження мобільних пристроїв Apple але блокувати доступ до їх пам'яті. • Формування «білих» та «чорних» списків пристроїв за багатьма параметрами (SN, PID&VID, ID) • Можливість блокування спроб запису/копіювання документів на зовнішні носії, що збігаються з цифровими відбитками або містять слова, словосполучення та регулярні вирази вказані замовником • Застосування правил до локальних та доменних користувачів • Можливість різної поведінки системи в залежності від стану системи (online / offline) • Можливість перехоплення тіньових копій файлів, які користувач копіює або записує на зовнішній носій або завантажує з нього • Можливість зберігання та логічного групування об'єктів, таких як словники, регулярні вирази, шаблони пристроїв тощо; • Наявність менеджеру інцидентів, що дозволяє: – Переглядати інформацію про інцидент (назва правила, дата та час тощо) – Групувати інциденти за певними ознаками (ім'я класифікації, ім'я користувача тощо); – Завантажувати тіньові копії інцидентів; – Переглядати співпадіння по словам та регулярним виразам; – Призначати відповідальних за інцидент людей (рецензентів); – Надсилати рецензентам повідомлення про порушення; – Видаляти події певної давності або при досягненні їх певної кількості; – Експорт подій;	
Підтримка ОС • Windows 7 та вище, Windows Server 2008 R2 та вище, Mac OS X Lion та вище	

1. Технічні, якісні характеристики Товару за предметом закупівлі повинні відповідати встановленим/зареєстрованим діючим нормативним актам діючого законодавства (державним стандартам), які передбачають застосування заходів із захисту довкілля, охорони праці, екології та пожежної безпеки.

2. Товар має бути новим, не перебувати під забороною відчуження, арештом, не бути предметом застави та іншим засобом забезпечення виконання зобов'язань перед будь якими фізичними або юридичними особами, державними органами і державою, а також не бути предметом будь-якого іншого обтяження чи обмеження, передбаченого чинним в Україні законодавством.

3. Товар має узгоджуватись з усіма електричними вимогами, що встановлені в Україні.

4. Гарантія на предмет закупівлі та обладнання, що входить до його комплекції, має бути надана виробником, офіційним представником або безпосередньо постачальником обладнання. За жодних умов, постачальник не може перекладати відповідальність за поломки і несправності на будь-яких третіх осіб. Треті особи можуть нести відповідальність за поломки і несправності перед постачальником, але не перед замовником.

Предмет закупівлі повинен мати гарантійний термін не менше 12 місяців з дати придбання його замовником. та включати безкоштовну заміну вузлів, які вийшли з ладу з вини виробника.

5. Упаковка повинна бути цілісна та непошкоджена, з необхідними реквізитами виробника.

6. Доставка товару здійснюється за власний рахунок та на власному транспорті переможця виїздом спеціаліста на адресу замовника для установки та введення в експлуатацію.

Строк поставки товару – до 31.12.2021 року.

Місце поставки: вулиця Бердичівська, 1, м. Київ, 04116.

У разі необхідності замовник має право вимагати надання по одному зразку товару, що пропонується до постачання для оцінювання Замовником його відповідності до вимог щодо технічним та якісним характеристикам.

Уповноважена особа **Юлія СТЕЛЬНИКОВИЧ**