**Оголошення про проведення спрощеної закупівлі**

**1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, його категорія.**

1.1. Найменування: ГОЛОВНЕ УПРАВЛІННЯ ДПС У ХАРКІВСЬКІЙ ОБЛАСТІ

1.2. Місцезнаходження: 61057, Україна, Харківська обл., Харків, вул. Пушкінська, буд. 46

1.3. Код згідно за ЄДРПОУ: 43983495

1.4. Категорія замовника: орган державної влади, місцевого самоврядування або правоохоронний орган.

**2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності).**

Послуги з постачання антивірусного програмного продукту

 «ESET PROTECT Entry з локальним управлінням»

ДК 021:2015:48760000-3 - Пакети програмного забезпечення для захисту від вірусів

**3. Інформація про технічні, якісні та інші характеристики предмета закупівлі.**

3.1. Технічні, якісні та кількісні вимоги до предмета закупівлі зазначено у додатку 1 до оголошення про проведення спрощеної закупівлі.

**4. Кількість та місце поставки товарів або обсяг і місце виконання робіт чи надання послуг:**

4.1 Кількість послуг: одна послуга (Поновлення. На 1 рік. Для захисту 796 об’єктів), одна послуга (Пільгова. На 1 рік. Дозакупка понад 796 об’єктів. Для захисту 354 об’єктів)

4.2 Місцезнаходження Замовника: 61057, Україна, Харківська обл., м. Харків,
вул. Пушкінська, буд. 46.

**5. Строк поставки товарів, виконання робіт, надання послуг:** Строк надання Послуг – до 31 грудня 2022 року.

**6. Умови оплати:**

Розрахунки за надані Послуги здійснюються у безготівковій формі шляхом перерахування грошових коштів в національній валюті України на поточний рахунок Виконавця на підставі підписаного Сторонами Акту приймання – передачі Послуг протягом 15 (п’ятнадцяти) днів після отримання Акту приймання – передачі Послуг, за умови надходження коштів з Державного бюджету України на реєстраційний рахунок Замовника на цілі, визначені Договором (з урахуванням наявності фінансового ресурсу на Єдиному казначейському рахунку)

**7. Очікувана вартість предмета закупівлі: 448000.00 грн. без ПДВ**

**8. Період уточнення інформації про закупівлю (не менше трьох робочих днів з дня оприлюднення оголошення про проведення спрощеної закупівлі в електронній системі закупівель):** до 17:00 год., 20.10.2022.

**9. Кінцевий строк подання пропозицій (строк для подання пропозицій не може бути менше ніж два робочі дні з дня закінчення періоду уточнення інформації про закупівлю):** до 17:00 год., 25.10.2022.

**10. Перелік критеріїв та методика оцінки пропозицій із зазначенням питомої ваги критеріїв:** єдиним критерієм оцінки є ціна. Питома вага цього критерію – 100%. Учасник повинен зазначити ціну пропозиції:

- з ПДВ: у разі, коли учасник є платником податку на додану вартість;

- без ПДВ: у разі, коли учасник не є платником ПДВ.

Учасник визначає ціну пропозиції, з урахуванням технічних, якісних та кількісних характеристик предмету закупівлі, всіх податків і зборів, що сплачуються або мають бути сплачені, у тому числі податку на додану вартість (ПДВ), у разі якщо учасник є платником ПДВ, усіх інших витрат, що необхідні для здійснення закупівлі на умовах цього оголошення.

**11. Розмір та умови надання забезпечення пропозицій учасників (якщо замовник вимагає його надати):** не вимагається.

**12. Розмір та умови надання забезпечення виконання договору про закупівлю (якщо замовник вимагає його надати):** не вимагається.

**13. Розмір мінімального кроку пониження ціни під час електронного аукціону в межах від 0,5 відсотка до 3 відсотків або в грошових одиницях очікуваної вартості закупівлі:** 0,5%

**14. Інша інформація.**

Закупівля здійснюється у відповідності до норм Постанови Кабінету Міністрів України про деякі питання здійснення оборонних та публічних закупівель товарів, робіт і послуг в умовах воєнного стану від 28.02.2022 № 169 в порядку проведення спрощених закупівель, встановленого Законом України «Про публічні закупівлі» (далі - Закон). Оголошення розроблено відповідно до вимог Закону. Терміни, які використовуються в цьому оголошенні, вживаються у значенні, наведеному в Законі.

Замовник відхиляє пропозицію в разі, якщо:

1) пропозиція учасника не відповідає умовам, визначеним в оголошенні про проведення спрощеної закупівлі, та вимогам до предмета закупівлі;

2) учасник, який визначений переможцем спрощеної закупівлі, відмовився від укладення договору про закупівлю;

3) якщо учасник протягом одного року до дати оприлюднення оголошення про проведення спрощеної закупівлі відмовився від підписання договору про закупівлю більше двох разів із замовником, який проводить таку спрощену закупівлю.

Інформація про відхилення пропозиції протягом одного дня з дня прийняття рішення замовником оприлюднюється в електронній системі закупівель та автоматично надсилається учаснику, пропозиція якого відхилена через електронну систему закупівель.

Учасник, пропозиція якого відхилена, може звернутися до замовника з вимогою надати додаткову аргументацію щодо причин невідповідності його пропозиції умовам, визначеним в оголошенні про проведення спрощеної закупівлі, та вимогам до предмета закупівлі. Не пізніше ніж через три робочих дні з дня надходження такого звернення через електронну систему закупівель замовник зобов’язаний надати йому відповідь.

Замовник відміняє спрощену закупівлю в разі:

1) відсутності подальшої потреби в закупівлі товарів, робіт і послуг;

2) неможливості усунення порушень, що виникли через виявлені порушення законодавства з питань публічних закупівель;

3) скорочення видатків на здійснення закупівлі товарів, робіт і послуг.

Спрощена закупівля автоматично відміняється електронною системою закупівель у разі:

1) відхилення всіх пропозицій згідно з частиною 13 статті 14 Закону України «Про публічні закупівлі»;

2) відсутності пропозицій учасників для участі в ній.

Замовник може укласти договір про закупівлю з учасником, який визнаний переможцем спрощеної закупівлі, на наступний день після оприлюднення повідомлення про намір укласти договір про закупівлю, але не пізніше ніж через 20 днів.

Проєкт договору складається замовником з урахуванням особливостей предмету закупівлі. Разом з документацією замовником подається проєкт договору про закупівлю з обов’язковим зазначенням порядку змін його умов.

Договір про закупівлю укладається відповідно до норм Цивільного кодексу України та Господарського кодексу України з урахуванням особливостей, визначених цим Законом.

Пропозиції подаються в електронному вигляді через електронну систему закупівель шляхом завантаження сканованих документів, у форматі: .pdf / jpeg(сканованого оригіналу документа/ сканованої копії документа, засвідченої підписом учасника/ уповноваженої особи учасника та відбитком печатки учасника (у разі її використання учасником)), або у формі електронних документів через електронну систему закупівель. Скановані документи мають бути належного рівня зображення (чіткими та розбірливими для читання).

Документи, що складаються учасником та які учасник подає у складі пропозиції спрощеної закупівлі не у формі електронного документа, повинні бути оформлені належним чином у відповідності до вимог чинного законодавства в частині дотримання письмової форми документу, складеного суб’єктом господарювання, в тому числі за власноручним підписом учасника/уповноваженої особи учасника.

Вимога щодо засвідчення того чи іншого документу пропозиції спрощеної закупівлі власноручним підписом учасника/уповноваженої особи учасника не застосовується до документів (матеріалів та інформації), що подаються у складі пропозиції, якщо такі документи (матеріали та інформація) надані учасником у формі електронного документа через електронну систему закупівель із накладанням електронного підпису(далі - КЕП), що базується на кваліфікованому сертифікаті електронного підпису, відповідно до вимог закону України «Про електронні довірчі послуги» на кожен з таких документів (матеріал чи інформацію). Відповідно до частини третьої статті 12 Закону під час використання електронної системи закупівель з метою подання тендерних пропозицій та їх оцінки, документи та дані створюються та подаються з урахуванням вимог законів України «Про електронні документи та електронний документообіг» та «Про електронні довірчі послуги», тобто пропозиція, у будь-якому випадку, повинна містити накладений кваліфікований електронний підпис (або удосконалений електронний підпис згідно з постановою Кабінету Міністрів України від 03.03.2020 № 193) учасника/уповноваженої особи учасника спрощеної закупівлі, повноваження якої щодо підпису документів пропозиції підтверджуються відповідно до поданих документів, що вимагаються згідно з пунктом 1 розділу «Документи, які необхідно подати учаснику для підтвердження відповідності пропозиції учасника умовам, визначеним в оголошенні про проведення спрощеної закупівлі, та вимогам до предмета закупівлі (документи, які повинні бути завантажені учасником через електронну систему закупівель)».

Виняток: якщо електронні документи пропозиції видано іншою організацією і на них уже накладено КЕП цієї організації, учаснику не потрібно накладати на нього свій КЕП.

Замовник перевіряє КЕП/удосконалений електронний підпис учасника на сайті центрального засвідчувального органу за посиланням <https://czo.gov.ua/verify>. Під час перевірки КЕП/удосконаленого електронного підпису повинні відображатися прізвище та ініціали особи, уповноваженої на підписання пропозиції спрощеної закупівлі (власника ключа). У випадку відсутності даної інформації або у випадку не накладення учасником КЕП/удосконаленого електронного підпису відповідно до умов оголошення спрощеної закупівлі учасник вважається таким, що не відповідає умовам оголошення про проведення спрощеної закупівлі та його пропозицію буде відхилено на підставі пункту 1 частини 13 статті 14 Закону.

Документи пропозиції, які складаються безпосередньо учасником відповідно до вимог цього оголошення про проведення спрощеної закупівлі, повинні бути викладені українською мовою.

Пропозиції, підготовлені учасниками та всі документи у складі пропозицій учасників можуть бути викладені іншою мовою, при цьому повинні мати переклад українською мовою завірений учасником або бюро перекладів, або нотаріусом. Визначальним є текст, викладений українською мовою.

Всі документи пропозиції спрощеної закупівлі подаються в електронному вигляді через електронну систему закупівель (шляхом завантаження сканованих документів або електронних документів в електронну систему закупівель) до кінцевого строку подання пропозицій.

***Документи, що не передбачені законодавством для учасників - юридичних, фізичних осіб, у тому числі фізичних осіб - підприємців, не подаються ними у складі пропозиції, про що такому учаснику необхідно зазначити у своїй пропозиції, включаючи обґрунтування та причини неподання документів та інформації учасника.***

**Документи, які необхідно подати учаснику для підтвердження відповідності пропозиції учасника умовам, визначеним в оголошенні про проведення спрощеної закупівлі, та вимогам до предмета закупівлі (документи, які повинні бути завантажені учасником через електронну систему закупівель)**

**1.** Витяг з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань з інформацією актуальною на момент надання пропозицій.

**2.** Документи, що підтверджують повноваження особи учасника спрощеної закупівлі щодо підпису документів пропозиції спрощеної закупівлі та на право підписання договору про закупівлю за результатами спрощеної закупівлі:

1) оригінал чи копія протоколу зборів засновників про призначення директора/президента/голови правління, або виписка (витяг) з нього, та оригінал чи копія наказу про його призначення або про вступ на посаду, - необхідно подати учаснику – юридичній особі, у випадку якщо пропозицію (документи пропозиції)та/або договір про закупівлю підписує уповноважена посадова (службова) особа учасника – юридичної особи, яку уповноважено підписувати пропозицію та вчиняти інші юридично значущі дії від імені учасника на підставі положень установчого (установчих) документа (документів);

2) довіреність/доручення та документальне підтвердження повноважень особи, яка видала довіреність/доручення, щодо видачі довіреності/доручення, - необхідно подати учаснику – юридичній особі, у разі якщо пропозицію (документи пропозиції)та/або договір про закупівлю підписує службова (посадова) учасника – юридичної особи, чиї повноваження не визначені установчим документом (статутом);

3) для підтвердження повноважень щодо підпису договору за результатами спрощеної закупівлі, необхідно подати довідку, складену у довільній формі, з інформацією про особу, яку уповноважено на підписання договору про закупівлю. При наявності у особи, яку уповноважено учасником – юридичною особою на підписання договору про закупівлю,обмежень у статуті або в іншому установчому документі(з урахуванням вимог діючого законодавства України) щодо права уповноваженої особи учасника на підписання договору про закупівлю за результатами даної спрощеної закупівлі, учаснику – юридичній особі необхідно подати довідку, складену у довільній формі, про наявність таких обмежень та документальне підтвердження права уповноваженої особи учасника на підписання договору про закупівлю за результатами даної спрощеної закупівлі (копію рішення загальних зборів учасників (засновників), або інший документ згідно з законодавством, який дає право уповноваженій особі учасника на підписання договору про закупівлю);

4) копія паспорта (сторінка 1 – 6 (за наявності інформації на вказаних сторінках будь якої інформації/ фото, а також сторінка, що містить інформацію про останнє місце реєстрації особи), у випадку, якщо такий паспорт оформлено у вигляді книжки; або двосторонню копію паспорта громадянина України у випадку, якщо такий паспорт оформлено у формі картки, що містить безконтактний електронний носій та Додаток 13 до Постанови Кабінету Міністрів України від 2 березня 2016 № 207, або Витяг з Єдиного державного демографічного реєстру щодо реєстрації місця проживання або копія іншого документа, який посвідчує особу, передбаченого чинним законодавством України; та копія картки платника податків (довідки про присвоєння ідентифікаційного номеру), (вимога встановлюється для учасника фізичної особи-підприємця/фізичної особи). Фізична особа - підприємець, яка власноручно підписує пропозицію (документи пропозиції) від свого імені, не подає іншого документального підтвердження повноважень щодо підписання пропозиції та/або документів, що подаються у її складі;

5) якщо пропозиція подається об’єднанням учасників, до неї обов’язково включається документ про створення такого об’єднання.

**3.** Оригінал **або** копія Статуту (остання зареєстрована редакція), чи іншого установчого документу, **та/або** копія опису за підписом державного реєстратора, за допомогою коду якого є можливим перевірити останню редакцію такого установчого документу через офіційний веб-сайт (<https://usr.minjust.gov.ua/ua/freesearch>) (вимога встановлюється для учасника - юридичної особи). Якщо учасник здійснює діяльність на підставі модельного статуту, необхідно надати копію рішення засновників про створення такої юридичної особи.

**4**. **Документальне підтвердження статусу учасника, як платника податків:**

* довідка, складена у довільній формі, із зазначенням коду згідно з ЄДРПОУ/РНОКПП, дати реєстрації платником податку на додану вартість, індивідуального податкового номеру(вимога встановлюється для учасника, який є платником податкуна доданувартість).
* довідка, складена у довільній формі, із зазначенням коду згідно з ЄДРПОУ/РНОКПП, дати обрання або переходу на спрощену систему оподаткування (вимога встановлюється для учасника, який є платником єдиного податку).
* У випадку, якщо учасник перебуває на іншій системі оподаткування, необхідно подати довідку про це, складену у довільній формі.

**5.** Форма «Загальні відомості про учасника», за підписом уповноваженої особи учасника/учасника, яка повинна бути складена і заповнена за формою наведеною у **додатку 2** до оголошення про проведення спрощеної закупівлі.

Факт подання пропозиції учасником - фізичною особою чи фізичною особою-підприємцем, яка є суб’єктом персональних даних, вважається безумовною згодою суб’єкта персональних даних щодо обробки її персональних даних у зв’язку з участю в процедурі закупівлі, відповідно до абзацу 4 статті 2 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI.

В усіх інших випадках, факт подання пропозиції учасником – юридичною особою, що є розпорядником персональних даних, вважається підтвердженням наявності у неї права на обробку персональних даних, а також надання такого права замовнику, як одержувачу зазначених персональних даних від імені суб’єкта (володільця). Таким чином, відповідальність за неправомірну передачу замовнику персональних даних, а також їх обробку, несе виключно учасник процедури закупівлі, що подав тендерну пропозицію.

**6.** Учасник у складі своєї пропозиції повинен подати (завантажити через електронну систему закупівель) гарантійний лист за формою наведеною у додатку 4, за підписом уповноваженої особи учасника/учасника, засвідчений печаткою учасника (у разі її використання учасником), або П.І.Б. та підпис учасника-фізичної особи.

**7.** Лист-гарантія, за підписом уповноваженої особи Учасника та завіреним печаткою (за наявності) щодо дотримання Учасником в своїй діяльності норм чинного законодавства України, в тому числі:

- Закону України «Про санкції» від 14.08.2014р. № 1644-VII;

 - Указу Президента України від 15 травня 2017р. № 133/2017 р. «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій).

***Уповноважена особа КЕП Сергій КОРОБЧЕНКО***

**Додаток 1**

до оголошення про проведення

спрощеної закупівлі

***Технічні, якісні та кількісні характеристики предмета закупівлі***

|  |  |  |
| --- | --- | --- |
| № з/п | Найменування товару | Кількістьшт. |
|  | Програмна продукція 'ESET PROTECT Entry з локальним управлінням'. На 1 рік. Поновлення. Для захисту 796 об’єктів. | 1 |
|  | Програмна продукція 'ESET PROTECT Entry з локальним управлінням'. На 1 рік. Пільгова. Дозакупка понад 796 об’єктів Для захисту 354 об'єктів | 1 |

Програмна продукція 'ESET PROTECT Entry з локальним управлінням'

**Вимоги до учасника**

Учасник повинен надати Авторизаційний лист від виробника або офіційного представника виробника в Україні, що підтверджує наявність партнерських відносин Учасника з компанією-виробником або офіційним представником виробника в Україні та уповноважує Учасника надавати цінові пропозиції, проводити переговори і підписувати Договір з Замовником на поставку Продукту.

**Вимоги до технічної підтримки**

* Запропонована антивірусна ПП повинна мати авторизований виробником центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог:

- обслуговування 24х7х365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні;

- розширені технічні консультації з питань конфігурації та функціонування антивірусної ПП по телефону (з можливостю зв’язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв’язку) та електронній пошті;

**Вимоги до рішення для захисту робочих станцій під управління несерверних ОС:**

1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
2. Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
3. Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.
4. Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
5. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
11. Забезпечення антивірусного захисту в режимі реального часу.
12. Використання евристичних технологій власної розробки під час сканування.
13. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
14. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.
15. Можливість сканування файлів під час запуску ОС.
16. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
17. Сканування комп'ютера у неактивному стані.
18. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.
19. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.
21. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.
22. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).
23. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
24. Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп’ютер від шкідливих програм і небажаної активності.
25. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.
26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
27. Автоматична антивірусна перевірка змінних носіїв.
28. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження.
29. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.
31. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
32. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
33. Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
34. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
35. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».
36. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
37. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
38. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
39. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
40. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
41. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
42. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.
43. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
44. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
45. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE
46. Регламентне оновлення вірусних баз не менше 24 разів за добу.
47. Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет.
48. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
49. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
50. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.
51. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
52. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
53. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
54. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
55. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
56. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
57. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
58. Локальне зберігання журналів на робочих станціях.
59. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми.
60. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
61. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
62. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
63. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
64. Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.
65. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
66. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
67. Можливість віддаленого встановлення на клієнтську робочу станцію
68. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
69. Сумісність з існуючим сервером централізованого керування та активація антивірусного ПЗ шляхом додавання ключа до існуючого сервера керування. Для підтвердження відповідності пропозиції Учасника цій характеристиці та можливості перевірки відповідності запропонованого рішення заявленим технічним вимогам, на вимогу Замовника, Учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.
70. Можливість крім основного вказати резервні сервери адміністрування.
71. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
72. Підтримка ОС:Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit, Ubuntu Desktop 20.04 LTS, Red Hat Enterprise Linux 7 та 8, SUSE Linux Enterprise Desktop 15
73. Запропоноване ПЗ повинне безпечуватись в Україні технічною підтримкою, яка працює в режимі 24х7х365, з можливістю зв’язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку).
74. Наявність експертного висновку Державної служби спеціального зв'язку та захисту інформації, що засвідчує відповідність програмного продукту (продукції) захисту інформації, вимогам нормативних документів з технічного захисту інформації (дійсний не менше ніж період використання ліцензії на програмну продукцію).

**Вимоги до рішення для захисту робочих станцій під управління серверних ОС:**

1. Підтримка ОС: Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8
2. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
3. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
4. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.
5. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
6. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.
7. Можливість сканування файлів під час запуску ОС.
8. Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
9. Сканування комп'ютера у неактивному стані.
10. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.
11. Автоматична антивірусна перевірка змінних носіїв.
12. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.
13. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows.
14. Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру.
15. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень.
16. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
17. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.
18. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
19. Регламентне оновлення вірусних баз не менше 24 разів за добу.
20. Можливість крім основного вказати резервні сервери адміністрування.
21. Наявність механізму контролю за актуальністю оновлень ОС.
22. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання.
23. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій.
24. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
25. Можливість роботи в кластерах як домена так і робочої групи.
26. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
27. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.
28. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
29. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
30. Можливість захисту від зміни параметрів антивірусного ПЗ паролем.
31. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.

**Вимоги до інструменту віддаленого управління антивірусними рішеннями:**

1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати централізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам.
3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.
6. Віддалена інсталяція користувальницького програмного забезпечення.
7. Можливість віддаленого видалення встановленого користувальницького ПЗ.
8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac
9. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера.
10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування.
11. Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захисту.
12. Можливість аутентифікувати адміністраторів ERA за допомогою груп безпеки AD.
13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.
14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.
15. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів.
16. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
17. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
18. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.
19. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
20. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
21. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту.
22. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
23. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.
24. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.
25. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
26. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
27. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом.
28. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи.
29. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
30. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях
31. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту.
32. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.
33. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування).
34. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу
35. Можливість встановлення серверу адміністрування на ОС Windows та Linux.
36. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
37. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+.
38. Можливість обирати варіанти обробки ідентифікаторів клонованих комп’ютерів, такі як зіставляння з наявними комп’ютерами або створення нових комп’ютерів.
39. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.
40. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну ідентифікацію клонованих машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.
41. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
42. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
43. Можливість встановлення агенту управління на ARM64 процесорах.
44. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
45. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

**Додаток 2**

до оголошення про проведення

спрощеної закупівлі

*Форма «Загальні відомості про учасника» повинна бути складена і заповнена за нижченаведеною формою та подається у вигляді, наведеному нижче, на фірмовому бланку (у разі його наявності)*

**ФОРМА «ЗАГАЛЬНІ ВІДОМОСТІ ПРО УЧАСНИКА»**

|  |  |  |
| --- | --- | --- |
| № з/п | Найменування відомостей | Інформація учасника |
| 1 | Повне найменування (прізвище, ім’я, по батькові) |  |
| 2 | Код згідно з ЄДРПОУ (реєстраційний номер облікової картки платника податків) |  |
| 3 | Місцезнаходження (місце проживання) |  |
| 4 | Організаційно-правова форма учасника - юридичної особи |  |
| 5 | Телефон |  |
| 6 | Факс (у разі наявності) |  |
| 7 | Електронна адреса |  |
| 8 | Банківські реквізити, за якими буде здійснено розрахунок з учасником згідно з умовами договору про закупівлю (рахунок (рахунки), відкритий (відкриті) в обслуговуючому банку, найменування обслуговуючого банку), його адреса |  |
| 9 | Відомості про керівника учасника-юридичної особи (прізвище, ім`я, по батькові, посада, контактний телефон) |  |
| 10 | Прізвище, ім`я, по батькові особи, уповноваженої підписувати пропозицію від імені учасника, для учасника юридичної особи - посада особи |  |
| 11 | Прізвище, ім`я, по батькові особи, уповноваженої підписувати договір про закупівлю за результатами закупівлі, для учасника юридичної особи - посада особи |  |

Посада, прізвище, ініціали, підпис уповноваженої особи учасника, засвідчений печаткою учасника (у разі її використання учасником), або П.І.Б. та підпис учасника-фізичної особи

**Додаток 3**

до оголошення про проведення

 спрощеної закупівлі

# ПРОЄКТ ДОГОВОРУ ПРО ЗАКУПІВЛЮ

**ДОГОВІР**

**про надання послуг**

 **№\_\_\_\_\_\_\_\_\_\_\_**

м. Харків «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2022 р.

(розміщено в окремому файлі)

**Додаток 4**

до оголошення про проведення

спрощеної закупівлі

*Форма «Гарантійний лист» повинна бути складена і заповнена за нижченаведеною формою та подається у вигляді, наведеному нижче, на фірмовому бланку (у разі його наявності)*

* 1. **ГАРАНТИЙНИЙ ЛИСТ**

Ми(Я),\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(найменування Учасника), як учасник закупівлі: Послуги з постачання антивірусного програмного продукту «ESET PROTECT Entry з локальним управлінням» ДК 021:2015:48760000-3 - Пакети програмного забезпечення для захисту від вірусів ознайомлений та погоджуюся з умовами проєкту договору про закупівлю, наведеному у додатку 3 до оголошення про проведення спрощеної закупівлі

Ми(Я),\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(найменування Учасника), як учасник закупівлі: Послуги з постачання антивірусного програмного продукту «ESET PROTECT Entry з локальним управлінням» ДК 021:2015:48760000-3 - Пакети програмного забезпечення для захисту від вірусів, підтверджую, що несу повну відповідальність за достовірність інформації, наданої мною у своїй пропозиції.

*Дата (підпис) Посада, прізвище, ініціали*

***Посада, прізвище, ініціали, підпис уповноваженої особи учасника, засвідчений печаткою учасника (у разі її використання учасником), або П.І.Б. та підпис учасника-фізичної особи***