Інформація що до виконання вимог пункту 4-1 постанови Кабінету Міністрів України від 11 жовтня 2016 №710 «Про ефективне використання державних коштів».

1	Найменування замовника	Територіальне управління БЕБ у Волинській області
2	Найменування предмету закупівлі, згідно з класифікатором ДК021:2015	код ДК 021: 2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів
3	Посилання на реквізити оголошення про проведення конкурентної процедури закупівлі, оприлюдненої в електронній системі Прозоро чи повідомлення про намір укласти договір відповідно до п. 13 Постанови № 1178	https://prozorro.gov.ua/tender/UA-2023-11-02-006447-a
4	Обґрунтування технічних та якісних характеристик предмета закупівлі	З метою забезпечення захисту робочих станцій від вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ та інших кіберзагроз під час роботи у мережі Інтернет, інформаційними ресурсами, електронною поштою та носіями (USB флеш носії) ТУ БЕБ у Волинській області необхідно у відповідності до вимог Закону та Постанови № 1178 провести процедуру відкритих торгів (з особливостями). Технічні та якісні характеристики предмету закупівлі визначені відповідно до потреб замовника з урахуванням вимог законодавства та внутрішніх нормативно-розпорядчих документів БЕБ України, а саме: - Запропоновані рішення повинні мати діючий експертний висновок ДССЗЗІ; - Інтерфейс та документація до продукту державною мовою; - - Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ. - - 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. - - 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 поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним. - - Надання захисту від потенційно небезпечних програми - комерційного легального ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.

		- - Надання захисту від підозрілих програм – програм, які стиснуті пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення. - - Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі. - - Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. - - Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи. - - Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС. - - Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. - - Забезпечення антивірусного захисту в режимі реального часу. - - Використання евристичних технологій власної розробки під час сканування. - - Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. - - Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. - - Можливість сканування файлів під час запуску ОС. - - Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін. - - Сканування комп'ютера у неактивному стані. - - 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. - - Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків. - - Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomeware). - - 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. - - 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. - - Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. - - Автоматична антивірусна перевірка змінних носіїв. - - 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. - - Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою. - - Можливість створювати групи дозволених або заборонених зовнішніх пристроїв. - - Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену. - - Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв. - - 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. - Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену. - - Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації. - - Регламентне оновлення вірусних баз не менше 24 разів за добу. - - 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. - - Можливість створення дзеркала оновлень засобами антивірусної ПП. - - Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне. - - Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею. - - Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну. - - Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. - - Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС. - - 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. - - Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі. - - Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час. - - Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання. - - Локальне зберігання журналів на робочих станціях. - - 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, а також за умови виникнення конкретних подій. - - Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. - - 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. - - Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування. - - Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення. - - Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності. - - Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача. - - Низьке споживання ресурсів ПК актуальними антивірусними продуктами (сукупно усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору. - - Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову. - - Наявність інструменту віддаленого управління. - - Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи. - - Можливість крім основного вказати резервні сервери адміністрування.

		- - 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. - - Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. - Можливість роботи в кластерах як домена так і робочої групи - - Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування. - - Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.
5	Обґрунтування очікуваної вартості предмета закупівлі	Очікувана вартість предмета закупівлі Послуги з постачання антивірусного програмного забезпечення становить 131 340,00 грн. (сто тридцять одна тисяча триста сорок гривень 00 копійок) у тому числі ПДВ. та визначена на підставі наказу Мінекономіки від 18.02.2020 № 275 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі»