ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з ДК 021:2015 код 72260000-5 “Послуги, пов’язані з програмним забезпеченням” (Послуга у сфері інформатизації з постачання програмного забезпечення для роботи з електронною поштою на виконання п. 4.5. завдань регіональної програми інформатизації “Дніпропетровщина: цифрова трансформація” на 2023–2025 роки)

1. Замовник

Департамент цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської облдержадміністрації.

2. Підстави закупівлі

Закупівля здійснюється відповідно до пункту 4.5. завдань регіональної програми інформатизації “Дніпропетровщина: цифрова трансформація” на 2023–2025 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 14 жовтня 2022 року № 216-13/VIII..

Метою закупівлі є забезпечення програмним продуктом поштового серверного обладнання електронного комунікаційного центру (ЕКЦ) області корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації для захисту електронної пошти відповідно до вимог комплексної системи захисту інформації.

Відповідно до вимог комплексної системи захисту інформації необхідно здійснювати дієві заходи щодо захисту системи електронного листування від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп’ютерного обладнання та захисту інформації на них, а саме: забезпечувати багаторівневий захист від усього спектра загроз, що передаються електронною поштою, допомагати виявляти та запобігати атакам через електронну пошту, включаючи спам, фішинг, розсилку шкідливих програм та посилань, заміну відправника та компрометацію корпоративної електронної пошти (BEC).

Одним з найдієвіших заходів для вирішення вищезазначених завдань є встановлення відповідного програмного забезпечення на ЕКЦ області.

Ліцензія на існуюче програмне забезпечення має термін дії 12 місяців. Тому існує потреба у щорічному продовженні її дії.

Продовження терміну дії ліцензії на існуюче програмне забезпечення дозволить суттєво підвищити рівень захисту серверного обладнання ЕКЦ області, автоматизованих робочих місць користувачів корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп’ютерного обладнання та захисту інформації на них.

3. Очікувана вартість предмета закупівлі: 240 000 грн з ПДВ (обласний бюджет).

Очікувана вартість сформована з використанням примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Мінекономіки від 18.02.2020 №275, на підставі запиту безпосередньо до представника виробника програмної продукції, самостійного аналізу цін на аналогічні за технічними характеристиками типи програмної продукції через мережу Інтернет та в електронній системі закупівель Prozorro, а також з урахуванням необхідності забезпечення економії бюджетних коштів в умовах дії правового режиму воєнного стану в Україні..

4. Технічні та якісні характеристики предмета закупівлі

Найменування програмного забезпечення	Кількість, од.
Програмне забезпечення FortiMail-VM02 1 Year 24x7 FortiCare and FortiGuard Base Bundle Contract	1

Анти-спам сервіси

- Перевірка на основі поведінки сервера, що відправляє повідомлення (greylisting)
- Перевірка повідомлень на основі бази адрес Spam DNS (domain name, ip-address) відправників пошти
- Перевірка повідомлень на основі бази Spam URI аналізуючи посилання URI (web sites, URL) у повідомленнях
- Перевірка повідомлень на основі сторонніх баз Spam DNS та Spam URI
- Перевірка повідомлень на основі бази Spam Checksum вираховуючи контрольну суму повідомлення (checksum)
- Перевірка повідомлень на основі Bayesian бази, аналізуючи слова у повідомленнях (email header та body)
- Глибока інспекція заголовку повідомлення (email header)
- Перевірка повідомлень за допомогою евристичних правил (heuristic)
- Виявлення спаму на основі словників заборонених слів (dictionary scan та banned word scan)
- Виявлення спаму за допомогою поведінкового аналізу (behavioral analysis)
- Виявлення спаму за допомогою перевірки IP-адреси відправника повідомлення (MTA) з IP-адресою у DNS уповноваженого MTA для певного поштового домену (Sender Policy Framework – SPF Scan)
- Виявлення спаму за допомогою перевірки підпису повідомлень приватним доменим ключом (Domain Keys Identified Mail – DKIM)
- Виявлення спаму за допомогою перевірки SPF DNS запису та DKIM підпису (Domain-Based Message Authentication - DMARC)
- Виявлення спаму під час спалахів спаму за рахунок декількох перевірок повідомлень рознесених у часі (spam outbreak)
- Виявлення підробки повідомлень, що надходять з зовнішній електронних адрес але з відображенням ім’я внутрішнього користувача (impersonation analysis / business email compromise)
- Налаштування користувацьких списків IP-адреси та адреси електронної пошти, які або звільняються від класифікації як спам, або завжди класифікуються як спам (safe list / block list)
- Налаштування користувацьких списків слів, які або звільняються від класифікації як спам (safe list word)
- Виявлення спаму завдяки аналізу графічних зображень у повідомленнях (GIF, JPG, PNG)
- Виявлення підроблення IP-адреси відправника повідомлення шляхом співставлення його IP-адреси та наявного запису канонічне ім'я хоста (forged IP)
- Виявлення спаму завдяки аналізу PDF-файлів
- Налаштування максимального розміру повідомлення для сканування (включаючи без обмежень)
- Налаштування скасування сканування повідомлень на визначення спаму для аутентифікованих сесій
- Налаштування різних дії з повідомленнями при знаходженні спами, включаючи маркування та зміну повідомлень (tag subject, insert new header)
-

Анти-вірус / анті-malware сервіси

- Виявлення та блокування загроз шляхом інспектування заголовків, тіла та вкладених файлів електронної пошти
- Сигнатурний антивірусний аналіз
- Евристичний антивірусний аналіз (heuristic)
- Створення власних файлів хеш-значень відомих вірусних файлів
- Імпорт та експорт файлів хеш-значень відомих вірусних файлів
- Виявлення Grayware-файлів (небажаних програми або файлів, які не класифікуються як virus/malware)
- Аналіз стислих файлів (ZIP, PKZIP, LHA, ARJ, RAR)
- Виявлення невідомих malware під час спалахів на основі репутації хеш значень файлів у базі/сервісі виробника до моменту оновлення баз на шлюзі захисту електронної пошти (virus outbreak)
- Налаштування різних дії з повідомленнями при знаходженні вірусів/malware, включаючи маркування та зміну повідомлень (tag subject, insert new header)
- Автоматичне розшифрування архівів, PDF та MS Office документів за допомогою списку паролів або виявлених слів у тілі електронної пошти
- Заміна “зараженого” файла повідомленням про заміну (replacement message), яке сповіщає користувача, що “заражений” файл був видалений
- Пересилання “зараженого” повідомлення як вкладення, залишаючи при цьому оригінальне тіло повідомлення без змін або замінюючи його (repackage email with customized or original content)

Захист від цілеспрямованих та раніше невідомих загроз

- Система має інтегруватися з системою захисту від цілеспрямованих та раніше невідомих загроз цього ТЗ, для здійснення ефективного захисту від таких загроз шляхом аналізу файлів та URI (URL) з повідомлень

Захист на основі визначення змісту (content detection)

- Виявлення та блокування фрагментованих повідомлень
- Виявлення та блокування зашифрованих файлів, до яких не може бути підібрано пароль
- Виявлення у MIME-файлах вбудовані об’єкти та інші файли (embedded component) та сканування їх на загрози
- Визначення гранічного розміру повідомлення
- Визначення максимальної кількості вкладень у повідомлені
- Визначення типів файлів та розширення файлів, які потрібно сканувати на загрози

Захист від просунутих загроз

- Функціонал видалення або нейтралізації потенційно небезпечного вмісту (hyperlinks, macros, active scripts, javascript) у повідомленнях електронної пошти та файлах вкладень (MS Office файли, PDF-файли)
- Функціонал запобігання озброєнню раніше надійних URL-посилань після доставки повідомлення у папку "Вхідні", шляхом перевірки на загрози URL-посилання при натисканні на нього користувачем.
-

Звітність (reporting)

- Звіти щодо загальної поштової статистики (mail, spam, non-spam, virus, тощо)
- Звіти за відправниками різних типів повідомлень (mail, spam, virus, тощо)
- Звіти за отримувачами різних типів повідомлень (mail, spam, virus, тощо)
- Налаштування проміжку часу за який буде сформовано звіт

- Налаштування поштових доменів для який буде сформовано звіт
- Налаштування напрямку поштових повідомлень (вхідні, вихідні) для який буде сформовано звіт
- Формування звітів за розкладом (scheduled) та за потреби (on-demand)
- Звітність у форматі HTML, PDF, тощо
- Відправка звітів електронною поштою

Експертний висновок

Учасник має підтвердити наявність експертного висновку Держспецзв'язку щодо відповідності обладнання захисту електронної пошти, що він пропонує за даними торгами, вимогам нормативних документів системи технічного захисту інформації в Україні, надавши копію відповідного експертного висновку

Технічна сервісна підтримка

- Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців 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 захисту та всіх необхідних оновлень для сервісів безпеки
- Отримання основних та проміжних релізів програмного забезпечення
- Можливість реєстрації сервісних випадків в режимі 24*7

Вимоги до учасників

Учасники торгів повинні належним чином здійснювати діяльність щодо предмету закупівлі. У зв'язку з цим для належного захисту інтересів Замовника щодо авторизованого джерела постачання послуг за даними торгами учасники торгів повинні надати інформаційний лист в довільний формі виданий Виробником програмного забезпечення (від головного офісу або від регіонального офіса/штаб-квартири виробника), що пропонується Учасником, або його офіційним представництвом в Україні (за наявності) про партнерські взаємовідносини (з зазначенням номеру оголошення про проведення торгів з ЦБД «Прозоро» та предмету закупівлі), які гарантують (вказують на) офіційність каналу постачання продукції від виробника програмного забезпечення із обов'язковим зазначенням найменування та номеру даних торгів, інформації щодо партнерських відносин між виробником програмного забезпечення та учасником закупівель.