Обґрунтування необхідності та вартості придбання програмної продукції для розгортання системи захисту електронної пошти

В інформаційно-телекомунікаційній системі Укрпатенту для захисту поштового серверу від небажаної кореспонденції (спаму) та небезпечного програмного забезпечення (вірусів) використовується програмно-апаратний пристрій Barracuda Email Security Gateway 300, який має ідентифікатор компанії виробника Barracuda Networks, Inc.: № BAR-SF-207360.

Зазначене обладнання повинно забезпечувати стабільну роботу електронної пошти, та безпеку інформації, яка нею передається.

З впровадженням електронного документообігу спостерігається значне збільшення потоків електронної кореспонденції. Це збільшує навантаження на обладнання захисту електронної пошти, що призводить до виникнення черг на обробку та несвоєчасної доставки кореспонденції. Будь який збій, або несправність, у цьому обладнанні може призвести до тривалої зупинки у роботі електронної пошти, що негативно вплине на роботу усього підприємства.

Для забезпечення чіткої та надійної роботи електронної пошти пропонуємо забезпечити резервування існуючого обладнання, додатково створивши віртуальну систему захисту електронної пошти. Додаткова віртуальна система захисту електронної пошти дозволить зменшити навантаження на існуючий пристрій та забезпечити безперебійність захисту електронної кореспонденції.

Для побудови віртуальну систему захисту електронної пошти та її повноцінної сумісної роботи з існуючим обладнанням необхідно закупити програмну продукцію виробництва Barracuda Networks, Inc., а саме «Barracuda Email Security Gateway Virtual License 400 Subscription, 36 Month» з терміном дії 3 (три роки).

Орієнтовна вартість програмної продукції розраховувалася, як середнє арифметичне комерційних пропозицій, отриманих від українських компаній (додаються):

(650648,59+663431,47+639144) / 3 = 651 074,69 грн.

Враховуючи інфляцію 7,3%

651 074,69 х 0,073 = 47 528,45 грн.

Розрахункова орієнтовна вартість програмної продукції становитиме:

651 074,69 + 47 528,45 = 698 603,14 грн.

Приймаємо приблизну вартість програмної продукції Barracuda Email Security Gateway Virtual License 400 Subscription, 36 Month у розмірі **700 000,00 грн**.

Інформація
про необхідні технічні, якісні та кількісні характеристики предмета закупівлі
Найменування предмета закупівлі:
ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки (програмна продукція для розгортання системи захисту електронної пошти)

Розділ І. Загальний опис предмету закупівлі.

Предметом закупівлі є програмна продукція для розгортання системи захисту електронної пошти.

Розділ ІІ. Вимоги до програмної продукції, що є предметом закупівлі:

Форма розгортання	• Віртуальна машина (VM), що буде встановлюватися на відповідний сервер з системою віртуалізації.
	• Підтримка гіпервізорів:
	  ○ VMware ESXi
	  ○ Citrix / OpenSource XenServer
	  ○ Microsoft Hyper-V
	  ○ KVM
	Апаратне обладнання та гіпервізори для розгортання програмної продукції, що є предметом закупівлі надаються Замовником.

Загальні вимоги	• На програмну продукцію не має бути анонсів end-of-sale та end-of life (EOS/EOL) від виробника
Продуктивність	• Продуктивність маршрутизації електронної пошти на типових повідомленнях розміром 100 KB - не менше ніж 65 000 за годину; • Продуктивність маршрутизації електронної пошти з антивірусною та антиспам перевіркою на типових повідомленнях розміром 100 KB - не менше ніж 50 000 за годину; • Підтримка не менше ніж 100 поштових доменів; • Підтримка від 500 до 2000 користувачів поштової системи.
Режими роботи	• MTA relay (gateway); • Поштовий сервер + MTA relay; • Прозорий MTA relay (transparent).
Підтримка режимів високої доступності (high availability)	• Active – Passive; • Active – Active.
Системні функції	• фільтрація вхідної та вихідної електронної пошти, перевірка на антиспам, антивірус, DLP; • Підтримка протоколів HTTPS, SMTPS, SMTP over SSL/TLS, IMAPS та POP3S; • SMTP-аутентифікація за допомогою LDAP, RADIUS, POP3, IMAP; • Підтримка перевірки сертифікатів SMTP-серверів під час встановлення з ними SMTP-сесії; • Перевірка адреси одержувача (recipient address verification); • Шифрування повідомлень на основі S/MIME стандарту; • Заміна адреси одержувача будь-якого “зараженого” повідомлення або спам-повідомлення, на іншу адресу, наприклад, адміністратора (rewrite recipient email address);

	• Наявність персонального (доступного користувачу) та системного (доступного адміністратору) карантину для спам-повідомлень або повідомлень, що містять malware; • Зберігання карантинних повідомлень в централізованому карантині, що розміщується на одному з пристроїв або на окремій системі, яка має бути у комплекті поставки; • Архівування вхідних та вихідних повідомлень на локальному диску або на мережевому сервері; • Можливість інтеграції з Microsoft Office 365 (у разі додаткового ліцензування); • Можливість фільтрації вхідної та вихідної електронної пошти шляхом перевірки з використанням контентного захисту, захисту від невідомих (0-day) та просунутих загроз (у разі додаткового ліцензування).
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 або сторонніх анті-спам систем (anti-spam engines); • 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/banned word scan/dictionary rules); • 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 (spam outbreak / outbreak filters); • Налаштування користувацьких списків IP-адрес та адрес електронної пошти, які або звільняються від класифікації як спам, або завжди класифікуються як спам (safe list/block list) • Налаштування користувацьких списків слів, які звільняються від класифікації як спам (safe list word);

	• Виявлення спаму завдяки аналізу графічних зображень у повідомленнях (GIF, JPG, PNG, тощо); • Виявлення підроблення IP-адреси відправника повідомлення шляхом співставлення його IP-адреси та наявного запису канонічне ім'я хоста (forged IP/ forged email); • Виявлення спаму завдяки аналізу PDF-файлів; • Налаштування максимального розміру повідомлення для сканування; • Налаштування різних дій з повідомленнями при знаходженні спаму, включаючи маркування та зміну повідомлень (tag subject, insert new header, тощо).
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 програм або файлів, які не класифікуються як virus/malware); • Аналіз стислих та архівних файлів (ZIP, GZIP, BZIP, RAR, ARJ, XZ, EGG, CPIO, LHA, LZMA, MS-CAB, MS-WIM, 7Z, ACE, TAR); • 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 дій з повідомленнями при знаходженні вірусів/malware, включаючи маркування та зміну повідомлень (tag subject, insert new header, тощо); • 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).
Функціонал запобігання витоку інформації Data leak prevention (DLP)	• Запобігання витоку конфіденційних даних шляхом перевірки повідомлень за допомогою шаблонів з використанням слів, фраз, регулярних виразів; • Запобігання витоку конфіденційних даних шляхом перевірки за допомогою заздалегідь визначеної інформації або шаблонів (credit card numbers, SIN numbers, тощо).
Керування пристроєм	• Графічний веб-інтерфейс (Web GUI); • Інтерфейс командного рядка (CLI); • Ролевий адміністративний доступ;

	• Автентифікація адміністраторів – локальна база, LDAP, RADIUS, PKI; • Обмеження адміністративного доступу до системи з довірених вузлів; • Конфігурація правил, щодо стійкості паролів (Password Policy); • Автоматичне блокування IP-адреси з якої здійснювалися спроби підбору паролю для проходження автентифікації доступу до адміністративних цілей (SSH, HTTP(S)); • Автоматичне блокування IP-адреси з якої здійснювалися спроби підбору паролю для проходження автентифікації доступу до поштових сервісів (SMTP(S), IMAP(S), POP3(S)); • Single Sign-On (SSO); • REST API для керування та моніторингу.
Моніторинг роботи системи	• Моніторинг системи за допомогою SNMP v1, v2c, v3 із зовнішніх систем; • Відправка traps за допомогою SNMP v1, v2c, v3 зовнішнім системам; • Налаштування граничних параметрів для системних характеристик (CPU, memory, disk, тощо), перевищення яких буде викликати відправку SNMP traps; • Налаштування системних подій (виявлення вірусу, спаму, зміна стану інтерфейсу, тощо), виявлення яких буде викликати відправку SNMP traps; • Налаштування категорій подій (виявлення вірусу, різних системних подій, закінчення строку дійсності ліцензії, тощо), настання яких буде викликати відправку поштового повідомлення адміністраторам системи.
Реєстрація подій (logging)	• Збереження журналів подій на диску пристрою або на віддаленому сервері (syslog-сервер або ftp-сервер); • Реєстрація системних подій пов'язаних з роботою безпосередньо системи; • Реєстрація подій, пов'язаних з пересилкою пошти, роботи протоколів SMTP, POP3, IMAP; • Реєстрація подій, пов'язаних з виявлення вірусів та результатами фільтрації спаму; • Вибір рівня важливості (severity level) подій для їх реєстрації на самої системі та віддаленому сервері; • Вибір типів подій (types of log) для їх реєстрації на самої системі або віддаленому сервері; • Налаштування граничного розміру журнального файлу; • Налаштування граничного часу ведення одного журнального файлу; • Налаштування проміжку часу, через який система архівує поточний журнальний файл; • Експорт/завантаження з системи журнальних файлів у звичайному та CSV-форматі.
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.
Технічна сервісна підтримка	• Технічна сервісна підтримка від виробника (правовласника) строком не менше ніж 36 місяців; • Постійний доступ до центру технічної підтримки виробника (правовласника) через сайт, електронною поштою або за телефоном 24*7; • Постійний авторизований доступ до сайту виробника (правовласника) 24*7; • Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки; • Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника; • Можливість реєстрації сервісних випадків в режимі 24*7.
Умови ліцензування	• Програмна продукція повинна постачатися без права власності із невиключними майновими правами на її використання строком не менше 36 місяців з дати поставки Замовнику; • Умови ліцензії повинні забезпечувати протягом строку дії ліцензії використання Замовником всього вищезазначеного функціоналу програмної продукції.

III. Вимоги до постачання програмної продукції, що є предметом закупівлі.

1. Поставка здійснюється за рахунок учасника.

2. Під час поставки програмної продукції учасник повинен за власний рахунок здійснити:

- встановлення та налаштування поставленої програмної продукції;

- повну інтеграцію поставленої програмної продукції з існуючою інфраструктурою замовника забезпечивши безперебійність її роботи (з повним переносом існуючих у Замовника налаштувань обладнання захисту поштового сервера Barracuda Email Security Gateway, яке має ідентифікатор компанії виробника Barracuda Networks, Inc.: № BAR-SF-207360, політик та правил фільтрації). Вся інформація про політики та правила фільтрації буде надана учаснику після підписання відповідного Договору.

IV. Вимоги до підготовки тендерної пропозиції учасником.

На підтвердження відповідності пропозиції технічним, якісним та кількісним характеристикам предмета закупівлі в складі своєї пропозиції учасник повинен надати:

1. Довідку у довільній формі про можливість постачання програмної продукції з урахуванням вимог цього Додатку, яка обов'язкова повинна містити точне найменування запропонованої програмної продукції, найменування виробника (правовласника), умови ліцензування та строк дії невиключних

майнових прав інтелектуальної власності на використання програмної продукції, а також іншу інформацію, яка на думку учасника, стосується предмета закупівлі, що пропонується до постачання.

2. Копія документу, наданого на адресу Замовника, з посиланням на оголошення цих торгів від виробника (правовласника) програмної продукції або його офіційного представництва (представника) на території України із зазначенням переліку програмної продукції, що є предметом закупівлі та пропонується учасником, яким підтверджуються право або можливість учасника здійснювати продаж запропонованої програмної продукції.

3. У разі, якщо документ зазначений у пункті 2 Розділу IV Додатку 2 до тендерної документації надаються представником виробника (правовласника) програмної продукції, учасник процедури закупівлі у складі тендерної пропозиції повинен надати копію(ї) документу(ів) виданого(их) виробником (правовласником) запропонованої програмної продукції, що підтверджує повноваження (права) такої особи на видання зазначених документів.