ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з предметом закупівлі: ДК 021:2015 код 72260000-5 "Послуги, пов'язані з програмним забезпеченням" (Послуги у сфері інформатизації з постачання програмного забезпечення для комплексної системи захисту інформації СІАЗ області (захист вебресурсів та електронної пошти) 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 комплексом програмних продуктів для захисту вебсервісів, поштових систем та захисту від невідомих загроз (0-day) робочих станцій, серверів та мобільних пристроїв користувачів системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації відповідно до вимог комплексної системи захисту інформації.

Відповідно до завдань регіональної програми інформатизації "Дніпропетровщина: цифрова трансформація" на 2023–2025 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 14.10.2022

№ 216-13/VIII та на яку отримано погодження від Міністерства цифрової трансформації України (лист від 18.08.2022 № 3009/0/526-22) передбачено реалізацію заходів із забезпечення захисту, цілісності та резервування інформації пріоритетних регіональних інформаційних ресурсів та сервісів місцевих органів влади системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації відповідно до вимог комплексної системи захисту інформації.

Відповідно до ст.8 Закону України "Про захист інформації в інформаційно-комунікаційних системах", постанови Кабінету Міністрів України від 29 березня 2006 року № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах" (зі змінами), розпорядження голови облдержадміністрації від 31 серпня 2007 року № Р-363/0/3-07 "Про забезпечення захисту інформації в облдержадміністрації", в рамках реалізації регіональної програми інформатизації "Електронна Дніпропетровщина" у 2021 році на систему інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації створено комплексну систему захисту інформації (Атестат відповідності, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 вересня 2021 року за № 23391).

Одним із головних компонентів комплексної системи захисту інформації є програмне забезпечення із захисту, цілісності та резервування інформації.

На даний час система інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації функціонує на базі захищеного електронного комунікаційного центру області комунального підприємства "Головний інформаційно-комунікаційний і науково-виробничий центр" Дніпропетровської обласної ради", який об'єднує 47 серверів,

6 технологічних систем, 4 сховища даних та має більш ніж 2000 користувачів корпоративної мережі, до якої входять: працівники апарату та структурних підрозділів облдержадміністрації, обласної ради, райдержадміністрацій, відповідних органів місцевого

самоврядування області.

На базі захищеного ЕКЦ області активно функціонують та розвиваються корпоративні хмарні сервіси (система електронного документообігу, реєстр територіальних громад, віртуальний офіс електронних послуг, платформа створення вебсайтів тощо).

За попередні роки за результатами проведених процедур відкритих торгів було закуплено:

Програмне забезпечення: FortiWeb-VM04 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics) – 1 од.

Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year 24x7 FortiCare and FortiGuard Base Bundle Contract – 1 од.

Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail – 1 од.

Зазначені програмні продукти були встановлені на серверне обладнання ЕКЦ області. Програмне забезпечення потребує щорічного продовження дії ліцензій для забезпечення захисту, цілісності та резервування інформації пріоритетних регіональних інформаційних ресурсів та сервісів місцевих органів влади.

3. Очікувана вартість предмета закупівлі: 1610000,00 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.

Ідентифікатор закупівлі в електронній системі закупівель:

UA-2025-08-19-000831-a.

4. Технічні та якісні характеристики предмета закупівлі

ТЕХНІЧНА СПЕЦИФІКАЦІЯ

Найменування програмного забезпечення	Кількість, од.
FortiWeb-VM04 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)	1
Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year 24x7 FortiCare and FortiGuard Base Bundle Contract	1
Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail	1

ТЕХНІЧНІ ВИМОГИ
ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Найменування програмного забезпечення	Кількість, од.
FortiWeb-VM04 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)	1

Найменування вимоги	**Вимоги до 1 одиниці**
Загальні вимоги	• Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки • Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення • На запропоноване рішення не має бути анонсів end-of-sale та end-of life (EOS/EOL) від виробника • Запропоноване рішення повинно мати чинні експертні висновки Державної служби спеціального зв'язку та захисту інформації України на відповідність вимогам законодавства в галузі захисту інформації або проходити відповідну державну експертизу на момент подання Учасником пропозиції конкурсних торгів
Архітектура та форм-фактор	Система має поставлятись як віртуальна машина (VM), що буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником
Продуктивність (Throughput)	• Кожна одиниця цієї системи (яка може складатись з кластеру) має продуктивність обробки трафіку не менше ніж 500 Mbps
Ліцензування	• Необмежена кількість веб-додатків що захищаються • Ліцензія захисту від botnet, malicious IP, phishing URLs, anonymous proxies, Trojan, ddos sources • Ліцензія для балансування навантаження на сервери на 7 рівні (Load balancing) • Інші ліцензії, що потребують задоволенню наведених функціональних вимог
Резервування, відмовостійкість	• Active / Passive • Active / Active
Режими функціонування	• Зворотний проксі (Reverse Proxy) • Прозорий режим (Transparent / Bridge) • Прозорий проксі режим (Transparent Reverse Proxy) • Офлайн-режим (Non-inline sniffer / Off-line Sniffing) • WCCP
Мережевий функціонал	• Статична маршрутизація (Static routing) • Маршрутизація на основі політик (Policy-based routing)

	• Трансляція IP-адрес (NAT) • Віртуальні мережі (VLAN - IEEE 802.1Q) • Агрегація групи фізичних інтерфейсів в один логічний інтерфейс (LACP - IEEE 802.3ad)
SSL/TLS-обробка	• Обробка SSL/TLS (якщо для цього потрібні додаткові ліцензії, вони мають бути у комплекті поставки) • Дешифрування та інспектування SSL/TLS (SSL off-loading)
Створення еталонної моделі функціонування веб-додатків	• Створення еталонної моделі функціонування веб-додатків шляхом автоматичного навчання (auto learn) або машинного навчання (machine learning), які базуються на основі запитів користувачів до веб-додатків • Підтримка автоматизованого динамічного профілювання веб-додатків • Підтримка автоматизованого внесення змін в еталоную модель при зміні веб-додатків
Комплексний захист від атак OWASP top 10 та перевірка на вразливості	• Виявлення та попередження OWASP top 10 атак (https://www.owasp.org/index.php/Top_10-2017_Top_10) • Наявність вбудованого сканеру вразливостей або інтеграція зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічною підтримкою на такий саме термін, що й система захисту веб-серверів)
Захист від DOS/DDOS- атак, Bot-protection	• Виявлення та захист від атак повного перебору на облікові дані користувачів (Brute Force Login) • Захист від DoS-атак на 3/4 рівні OSI (TCP Flood Prevention) • Захист від DoS-атак на 7 рівні OSI (HTTP Flood Prevention) • Розпізнавання підключення до сайту програми (bot) чи людини за допомогою CAPTCHA-запиту (CAPTCHA request) чи з використанням тесту (Real Browser Enforcement / Bot Protection)
Відстеження користувачів та їх пристроїв	• Відстеження користувацьких сесій та поведінки користувачів після їх вдалої автентифікації (User Tracking) • Профілювання та відстеження пристроїв користувачів, визначення їх репутації безпеки на основі порушення ними політик безпеки та автоматизація відповідної реакції у реальному часі (Device Intelligence Service / Device identification tracking)
Функції захисту веб-додатків та веб-сайтів	• Розмежування та обмеження доступу на основі whitelist та blacklist • Захист від Botnet, Anonymous proxy, Phishing, tor, spam, ddos та інше на основі баз IP-репутації (IP Reputation) • Розмежування та обмеження доступу на основі баз IP-геолокації (IP Geolocation) • Перевірка відповідності HTTP RFC (Protocol validation) • Захист від відомих атак на основі сигнатур для веб-сервісів/додатків (Web services signatures) • Створення користувацьких сигнатур для захисту від атак на веб-сервіси/додатки (Custom signatures) • Запобігання витоків важливих даних (DLP signatures) • Додавання системних cookie у HTTP-запити без їх шифрування

	• Додавання системних cookie у HTTP-запити з їх шифруванням • Міжмережевий екран на 4 рівні OSI або списки керування доступу на 4 рівні OSI (Stateful Firewall / Access control lists / IP Filters) • Виявлення та блокування шкідливих програм (Malware detection) завдяки вбудованому антивірусу або завдяки інтеграції зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF) • Аналіз команд протоколу FTP (Allowed / Blocked commands) при доступі до сайту та перевірка на наявність шкідливих програм у файлах що завантажуються “на” чи “з” сервера (upload or download) • Захист на основі бази скомпрометованих облікових даних (Credential Stuffing Defense) (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF) • Захист на основі алгоритму машинного навчання для виявлення шаблонів атак, та присвоєння їм рівня серйозності (Threat Analytics) (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF)
Інтеграція з системою захисту від цілеспрямованих атак класу sandbox	• Запропоноване рішення повинно мати можливість інтеграції з існуючою у замовника системою захисту від цілеспрямованих атак класу sandbox (FortiSandbox) шляхом відправлення до неї файлів на перевірку та отримання результатів сканування • Запропоноване рішення повинно мати можливість інтеграції з системою захисту від складних атак нульового дня (хмарний сервіс від виробника обладнання - cloud sandbox), шляхом відправлення до неї файли на перевірку та отримання результатів сканування
Визначення логіки, порядку доступу до ресурсів сайту та цілісності структури сайту	• Визначення URL сайту, з якого має розпочинатись доступ до контенту сайту (Start Page Enforcement) • Визначення URL сайту, що мають бути доступні у певній черзі (Page Order Rules) • Дозвіл чи блокування доступу до певних URL сайту (URL access) • Дозвіл чи блокування певних методів доступу HTTP до сайту / URL (Allow / Deny HTTP Method) • Виявлення видалення, додавання чи зміни файлів на веб-сайті та автоматичне відновлення структури та контенту сайту (Web Defacement Protection)
Доставка та маршрутизация контенту додатків	• Переписування або переправлення запитів і відповідей HTTP (URL Rewriting, redirecting) • Маршрутизація запитів до серверів на основі HTTP контенту (HTTP content routing) • Можливість додавання чи зчитування оригінальної IP-адреси ініціатора сеансу з HTTP-заголовку (X-Forwarded-For / X-Real-IP / True-Client-IP)

	• Балансування навантаження на сервери на 7 рівні (Load balancing) • Перевірка доступності серверів (Health Check) для балансування навантаження за допомогою ICMP, TCP, HTTP • Стиснення файлів (Content compression) • Кешування контенту (Content caching) • SSL/TLS off-loading • Модернізація сторінок, що відображають код помилки при порушенні користувачами політик безпеки, недоступності веб-сайту, перевірки captcha
Підтримка та аналіз протоколів	• Підтримка та аналіз протоколів XML, JSON • Підтримка та аналіз протоколів HTTP/2 • Підтримка та аналіз протоколу WebSocket
Автентифікація	• Підтримка протоколів LDAP, RADIUS, TACACS+ • Підтримка 2-факторної автентифікації (two-factor authentication) • Підтримка єдиної автентифікації користувачів (single sign-on) через WAF для доступу до декількох веб-додатків в одному домені • Автентифікація на основі SSL-сертифікатів користувачів • Інтеграція з Public Key Infrastructure (PKI) • Модернізація сторінок автентифікації користувачів
Управління, звітність, інтеграція	• Графічний веб-інтерфейс (Web GUI) • Інтерфейс командного рядка (CLI) • Підтримка системи централізованого керування для декількох пристроїв • Підтримка REST API • Централізоване ведення журналів та звітності (logging and reporting) • Розмежування доступу різних груп адміністраторів, призначаючи їм різні адміністративні привілеї для підмножини політик і захищених імен хостів (Administrative domain / Administrative Partitions / Virtual domain) • Ролевий доступ адміністраторів (RBAC) • Повідомлення про події за допомогою SNMP, Syslog та Email • Пересилання та зберігання журналів подій на виділений пристрій за допомогою FTP/TFTP, Email • Функціонал запису пакетів з мережевого інтерфейсу для подальшого їх аналізу (packet capture) • Функціонал резервного копіювання та відновлення файлів конфігурації на виділений пристрій за допомогою FTP • Графічний інтерфейс відображення інформації щодо працездатності та основних характеристик системи у реальному часі • Підтримка інтеграції з системами типу SIEM • Інтегровані звіти
Технічна сервісна підтримка від виробника	• Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою від виробника 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 через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника • Можливість реєстрації сервісних випадків в режимі 24*7*365 в сервісній службі виробника

Найменування програмного забезпечення	Кількість, од.
Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year 24x7 FortiCare and FortiGuard Base Bundle Contract	1

Найменування вимоги	**Вимоги до 1 одиниці**
Загальні вимоги	• Ліцензії та сервісна технічна підтримка повинні покривати наявне у замовника рішення Fortinet FortiMail VM02
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 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. Таки посилання мають бути перевірені на загрози системою захисту електронної пошти, при необхідності відправлені на перевірку до sandbox (time of click protection)
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	• Запропонована технічна сервісна підтримка має надаватись 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

Найменування програмного забезпечення	Кількість, од.
Програмна продукція: примірник комп'ютерної програми FortiMail-VM02 1 Year FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail	1

Найменування вимоги	**Вимоги до 1 одиниці**
Загальні вимоги	• Запропоноване ПЗ має бути сумісне з захищеним поштовим шлюзом FortiMail-VM02 • Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем (кластеризації) або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки • Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення • На ПЗ не має бути анонсів end-of-sale та end-of life (EOS/EOL) від виробника
Захист від невідомих загроз (0-day)	• Інтеграція з системою захисту від цілеспрямованих та раніше невідомих загроз типу sandbox, що функціонує як хмарний сервіс сервіс від виробника обладнання - cloud sandbox • Повідомлення, що містять підозрілі вкладення не повинні перенаправлятися користувачу до закінчення інспекції (з позитивним висновком) на Sandbox

Додаткові вимоги:

1. Учасник повинен мати статус зареєстрованого партнера з виробником програмного забезпечення (ПЗ).

2. Наявність не менше 1 сертифікованого спеціаліста рівня NSE 2 або аналогічного.

3. Учасник повинен надати копії сертифікатів від виробника ПЗ.

4. Сертифікати повинні бути дійсними протягом строку надання послуг.

5. Учасник повинен надати документи, що підтверджують партнерські відносини (співпрацю) Учасника з виробником ПЗ або з офіційним представництвом виробника ПЗ, про те що Учасник є авторизованим партнером або офіційним представником виробника ПЗ з правом реалізації оригінального ПЗ відповідно, а саме:

- оригінал або копія листа (завірена Учасником) від виробника ПЗ/офіційного представництва виробника щодо авторизації Учасника та/або визнання його офіційним представником виробника, а також, що ПЗ, яке пропонує (реалізує) Учасник є оригінальним;
- та/або копія договору (завірена Учасником), що підтверджує партнерські відносини (співпрацю) Учасника та виробника ПЗ/офіційного представництва виробника ПЗ, в тому числі, в частині щодо наявності в Учасника права на реалізацію (продаж) оригінального ПЗ виробника.