**Обґрунтування очікуваної вартості закупівлі програмної продукції для обладнання інформаційної безпеки**

В інформаційно-телекомунікаційній системі (далі – ІТС) Укрпатенту для захисту від зовнішніх загроз з мережі Інтернет використовується обладнання інформаційної безпеки, яке складається з мережевого екрану, побудованого на двох програмно-апаратних комплексах Check Point 5600 та програмно-апаратного комплексу для захисту від таргетованих атак та атак «нульового» дня Check Point SandBlast TE Appliance TE100X.

Право використання встановленого на цих програмно-апаратних комплексах програмного забезпечення закінчується 31.12.2021 року.

Для забезпечення подальшого функціонування обладнання інформаційної безпеки ІТС Укрпатенту необхідно у 2022 році здійснити придбання наступної програмної продукції:

- Check Point 5600 Next Generation Threat Prevention, CPSB-NGTX-5600-1Y, терміном на 1 рік, у кількості 1 шт.
- Check Point 5600 Next Generation Threat Prevention and Sandblast (NGTX) for High Availability, CPSB-NGTX-5600-1Y-HA, терміном на 1 рік, у кількості 1шт.
- SandBlast TE100X, CPSB-NGTX-SBTE100X-1Y, терміном на 1 рік, у кількості 1шт.
- Check Point Next Generation Security Management Software for 5 gateways (SmartEvent & SmartReporter Package 1 year) CPSB-EVS-5-1Y, терміном на 1 рік, у кількості 1 шт.
- SandBlast Agent Complete - 1 year. Provides Advanced Threat Prevention (Inc.Threat Emulation and Extraction), Forensics, Anti-Virus, Data Protection, Access Control and VPN.Cloud management included, CPEP-SBA-COMPLETE-1Y, терміном на 1 рік, у кількості 10 шт.
- Web App Protector Enterprise Service up to 10 Mbps and 1 Application for 1 year, CP-CG-WAF-10MBPS-1-MS-1Y у кількості 1 шт.
- Web App Protector 5 Applications Add-On for 1 year, CP-CG-WAF-5-ADD-1Y, у кількості 10 шт.
- Premium Direct Enterprise Support For 1 Year, CPES-SS-PREMIUM-ONSITE-ADD, терміном на 1 рік, у кількості 1 шт.
- Standard Direct Enterprise Support For 1 Year, CPES-SS-STANDARD-ADD, терміном на 1 рік, у кількості 1 шт.,
- Check Point Standard Direct Enterprise Support For 1 Year CPES-SS-STANDARD для CPSM-NGSM5. терміном на 1 рік, у кількості 1 шт.

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

(2 014 227,00 + 2 212 236,22 + 2 344 864,37) / 3 = 2 190 442,53≈2 200 000,00 грн.

Приймаємо вартість програмної продукції для обладнання інформаційної безпеки Check Point 5600 та Check Point SandBlast TE Appliance TE100X у розмірі **2 200 000,00** 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 обладнання інформаційної безпеки)**

**Розділ І. Загальні відомості**

**1.** Для забезпечення інформаційної безпеки у замовника застосовується система мережевого захисту на базі обладнання Check Point, яке має ідентифікатор компанії-виробника Check Point Software Technologies Ltd.: Account ID – 0007922402 (далі –комплекс мережевого захисту).

До складу комплексу мережевого захисту входить таке обладнання та програмна продукція:

- Check Point 5600 Next Generation Threat Prevention Appliance;
- Check Point 5600 Next Generation Threat Prevention and SandBlast (NGTX) Appliance for High Availability;
- SandBlast TE Appliance TE100X;
- Light Out Management module appliances;
- Memory Upgrade Kit from 8GB to 32GB for 5400, 5600, 5800 appliances;
- Програмна продукція Check Point Security Services - Enterprise Based Protection CPEBP-NGTX;
- Програмна продукція Check Point Next Generation Security Management Software for 5 gateways (SmartEvent & SmartReporter Package 1 year) CPSB-EVS-5-1Y;
- Програмна продукція SandBlast Agent Complete - 1 year. Provides Advanced Threat Prevention (Inc.Threat Emulation and Extraction), Forensics, Anti-Virus, Data Protection, Access Control and VPN.Cloud management included, CPEP-SBA-COMPLETE-1Y;
- Програмна продукція Check Point Standard Direct Enterprise Support For 1 Year, CPES-SS-STANDARD-ONSITE-ADD;
- Програмна продукція Check Point Premium Direct Enterprise Support For 1 Year, CPES-SS-PREMIUM-ONSITE-ADD;
- Програмна продукція Check Point Standard Direct Enterprise Support For 1 Year CPES-SS-STANDARD для CPSM-NGSM5;
- Програмна продукція Web App Protector Enterprise Service up to 10 Mbps and 1 Application for 1 year, CP-CG-WAF-10MBPS-1-MS-1Y;
- Програмна продукція Web App Protector 5 Applications Add-On for 1 year, CP-CG-WAF-5-ADD-1Y;

**Розділ ІІ. Опис предмета закупівлі**

Предметом закупівлі є програмна продукція для обладнання комплексу мережевого захисту.

Перелік. програмної продукції, що є предметом закупівлі:

| № п/п | Найменування програмної продукції | Термін дії | Кількість | Призначення |
|---|---|---|---|---|
| 1 | Програмна продукція Check Point 5600 Next Generation Threat Prevention - 1 year, CPSB-NGTX-5600-1Y | Протягом 12 календарних місяців з | 1 | Забезпечення функціонування комплексу мережевого |

| | | | | |
|---|---|---|---|---|
| | | моменту активації | | захисту |
| 2 | Програмна продукція Check Point 5600 Next Generation Threat Prevention and SandBlast (NGTX) for High Availability - 1 year, CPSB-NGTX-5600-1Y-HA | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення функціонування комплексу мережевого захисту |
| 3 | Програмна продукція SandBlast TE100X - 1 year, CPSB-NGTX-SBTE100X-1Y | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення функціонування комплексу мережевого захисту |
| 4 | Програмна продукція Check Point Next Generation Security Management Software for 5 gateways (SmartEvent & SmartReporter Package 1 year) CPSB-EVS-5-1Y (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення функціонування комплексу мережевого захисту |
| 5 | Програмна продукція Check Point SandBlast Agent Complete_renewal- 1 year. Provides Advanced Threat Prevention (Inc.Threat Emulation and Extraction), Forensics, Anti-Virus, Data Protection, Access Control and VPN.Cloud management included, CPEP-SBA-COMPLETE REN-1Y (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Встановлення на комп'ютери користувачів для забезпечення їх взаємодії з обладнанням SandBlast TE Appliance TE100X |
| 6 | Програмна продукція Web App Protector Enterprise Service up to 10 Mbps and 1 Application for 1 year, CP-CG-WAF-10MBPS-1-MS-1 Y (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Сервіс забезпечення захисту ВЕБ-ресурсів |
| 7 | Програмна продукція Web App Protector 5 Applications Add-On for 1 year, CP-CG-WAF-5-ADD-1Y (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Розширення на 5 сайтів сервісу забезпечення захисту ВЕБ-ресурсів |
| 8 | Програмна продукція Check Point Standard Direct Enterprise Support For 1 Year CPES-SS-STANDARD (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення виробником гарантійної підтримки комплексу мережевого захисту |
| 9 | Програмна продукція Check Point Standard Direct Enterprise Support For 1 Year, CPES-SS-STANDARD-ONSIT E-ADD (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення виробником гарантійної підтримки комплексу мережевого захисту |

| | | | | |
|---|---|---|---|---|
| 10 | Програмна продукція Check Point Premium Direct Enterprise Support For 1 Year, CPES-SS-PREMIUM-ONSITE -ADD (або еквівалент) | Протягом 12 календарних місяців з моменту активації | 1 | Забезпечення виробником гарантійної підтримки комплексу мережевого захисту |

**Розділ ІІІ. Вимоги до програмної продукції що є предметом закупівлі**

1. Вимоги до програмної продукції, зазначеної у пунктах 1–4 Розділу ІІ Додатку 2 до тендерної документації (далі – програмна продукція).

Програмна продукція повинна керуватися дистанційно з консолі адміністратора.

Програмна продукція повинна забезпечувати можливість керування 5 (п’ятьма) пристроями (далі – шлюзи) та 500 агентами.

Програмна продукція повинна мати модуль керування безпекою, який повинен розмежування доступу адміністраторів на основі розподілу ролей. Наприклад, роль для налаштувань політик комплексу мережевого захисту або роль, яка надає можливість тільки для перегляду журналу подій.

Програмна продукція повинна мати можливість централізованого розповсюдження та застосування нових версій для всіх шлюзів, які контролюються сервером керування.

Програмна продукція повинна мати можливість працювати в режимі HTTP/HTTPS проксі/реверс-проксі.

Модулі Firewall, IPS, Anti-Virus, Anti-Bot повинні бути представлені на одній платформі.

База даних мережевих застосунків та їх категорій повинна налічувати не менше ніж 6000 відомих застосунків.

Програмна продукція повинна мати можливість категоризувати не менше 250 млн URL адрес.

Програмна продукція повинна мати модуль протидії бот-активності (anti-bot) та модуль виявлення шкідливого програмного забезпечення (anti-virus).

Модуль протидії бот-активності повинен використовувати багаторівневий механізм запобігання бот-атакам заснований на репутації IP-адрес, URL та DNS адрес.

Програмна продукція повинна мати можливість автоматичного захоплення (копіювання) трафіку при подіях, які виявляються модулем IPS (Intrusion Prevention System), для подальшого аналізу.

Програмна продукція повинна забезпечувати механізм оновлень у всіх додатках включаючи IPS, керування додатками, URL-фільтрацію, Anti-Bot та Anti-Virus.

Сервіс централізованого моніторингу та протоколювання подій повинен відповідати таким вимогам:

- бути частиною системи керування;
- мати можливість протоколювати усі правила, в тому числі системні;
- у засобах перегляду журналів подій повинна бути можливість індексованого пошуку;
- мати можливість протоколювання подій у всіх інтегрованих додатках безпеки на шлюзі (включаючи віртуальні шлюзи), включаючи Firewall, IPSEC VPN, IPS, ідентифікацію користувачів, мобільний доступ, DLP, керування додатками, URL-фільтрацію, Anti-Bot, Anti-Virus, Anti-Spam, Email Security, Threat Emulation та Threat Extraction (емуляція файлів повинна проводитись локальному пристрої, який забезпечить 100000 емуляцій на 30 днів);
- для запобігання перехопленням повинен забезпечуватися безпечний канал передачі даних, дані повинні бути зашифровані і проходити перевірку автентичності та цілісності;
- журнали подій повинні безпечно передаватися між шлюзом та сервером керування або виділеним сервером журналів і консоллю перегляду журналів в комп'ютері адміністратора;
- повинна бути передбачена можливість динамічного блокування

активного з'єднання в графічному інтерфейсі системи протоколювання подій без необхідності внесення змін до бази правил;

- повинна бути передбачена можливість установки порогових значень параметрів, при досягненні яких шлюз повинен здійснювати запис події, оповіщення, відправку SNMP trap, відправку електронного листа та виконання визначеного адміністратором попередження;
- повинні бути попередньо налаштовані графіки для моніторингу процесів в часі трафіку і системних лічильників: головні правила безпеки, основні користувачі P2P, VPN тунелі, мережевий трафік та інша корисна інформація. Повинна забезпечуватися можливість створення нових графіків з різними типами діаграм.

Сервіс централізованої кореляції подій та звітів повинен відповідати таким вимогам:

- мати можливість кореляції подій з усіх додатків, включаючи Firewall, IPSEC VPN, IPS, ідентифікація користувачів, мобільний доступ, DLP, керування додатками, URL-фільтрація, Anti-Bot, Anti-Virus, Anti-Spam, Email Security, Threat Emulation та Threat Extraction;
- мати інструмент для кореляції подій з усіх функцій шлюзу та сторонніх пристроїв;
- забезпечувати графічне представлення подій на основі часу;
- забезпечувати можливість пошуку всередині списку подій, поглиблення в деталі для вивчення та розслідування інцидентів;
- мати попередньо визначені щогодинні, щоденні, щотижневі та щомісячні звіти, в тому числі, як мінімум, основні події, основні джерела, основні пункти призначення, основні сервіси, основні джерела та їх основні події, основні пункти призначення та їх основні події, основні сервіси та їх основні події;
- підтримувати автоматичне поширення звітів по електронній пошті, завантаження на FTP / Веб-сервер та скрипти розсилки зовнішніх звітів;

Оновлення баз даних сервісів безпеки (далі – Сервіс) повинно відповідати таким вимогам:

- Сервіс повинен функціонувати з наявним у замовника шлюзом;
- Сервіс повинен надавати можливість оновлення для таких програмних компонентів: фільтрація мережевих пакетів (Firewall), виявлення та протидія загрозам (IPS), контроль мережевих застосунків (Application Control), контроль мережевого трафіку на основі URL (URL Filtering), ідентифікація мережевих об’єктів (Identity Awareness), антивірус (Anti-Virus), анті-бот (Anti-Bot), анті-спам (Anti-Spam), захист пошти (Email Security), емуляції (Threat Emulation) та екстракції (Threat Extraction);
- Сервіс повинен забезпечувати регулярне отримання оновлень.

2. Вимоги до програмної продукції, зазначеної у пункті 5 Розділу II Додатку 2 до тендерної документації.

Для забезпечення захисту від атак 0-дня та невідомих раніше атак програмна продукція (далі – агент) повинна встановлюється на ПК користувачів.

- Агент повинен забезпечувати захист не менш ніж 10 ПК.
- Агент повинен виявляти та блокувати взаємодію з командними центрами бот-мереж й інформувати адміністратора;
- Агент повинен аналізувати та виявляти вірусну активність на змінних носіях та мережевих диска;
- Агент повинен блокувати доступ користувачів до фішингових веб-сайтів в режимі реального часу.
- Агент повинен забезпечувати статичне та евристичне виявлення підозрілих елементів на веб-сайтах;
- Агент повинен виявляти експлойти шляхом аналізу роботи компоненту захисту з оперативною пам’яттю;

- Агент повинен при виявленні експлойту зупиняти експлуатуючий процес;
- Агент повинен виявляти віруси шифрувальники на основі сигнатурного і поведінкового аналізу без доступу до мережі Інтернет;
- Агент повинен зберігати в кеш всі файли до яких звертається операційна система та відновлювати їх в автоматичному режимі в разі пошкодження вірусом шифрувальником;
- Агент повинен виявляти цілenаправлені атаки та атаки нульового дня шляхом емуляції файлів в ізольованому середовищі;
- Агент повинен мати механізм затримки файлу до моменту отримання результату емуляції файлу;
- Агент повинен надавати повну аналітику по інциденту інформаційної безпеки;
- Агент повинен забезпечити єдину систему захисту з існуючим обладнанням комплексу мережевого захисту та керуватися з єдиної консолі управління.

3. Вимоги до програмної продукції, зазначеної у пунктах 6-7 Розділу II Додатку 2 до тендерної документації

Програмна продукція, зазначена у пунктах 6-7 Розділу II Додатку 2 до тендерної документації, повинна відповідати таким вимогам:

- забезпечувати захист не менш ніж 6 (шести) ВЕБ-ресурсів;
- забезпечувати захист ВЕБ-ресурсів з легітимним трафіком не менш ніж 10 Mbps;
- забезпечувати захист ВЕБ-ресурсів від DDoS атак не менш ніж 1 Gbps;
- забезпечувати захист ВЕБ-ресурсів від атак OWASP top 10.

4. Вимоги до програмної продукції, зазначеної у пунктах 8-10 Розділу II Додатку 2 до тендерної документації

Програмна продукція, зазначена у пунктах 8-10 Розділу II Додатку 2 до тендерної документації, повинна забезпечувати гарантійну підтримку виробником продукції комплексу мережевого захисту та включати такі активовані сервіси:

- розширення можливостей комплексу, оновлення програмної продукції та баз сигнатур;
- відновлення працездатності комплексу та програмної продукції після збоїв;
- надання допомоги при усуненні збоїв програмної продукції або комплексу мережевого захисту та їх наслідків;

Гарантійна підтримка має надаватися виробником комплексу мережевого захисту та/або програмної продукції;

Гарантійна підтримка має надаватися через офіційний сайт виробника комплексу мережевого захисту та/або програмної продукції, електронну пошту або по телефону.

**Розділ IV. Вимоги до підготовки тендерної пропозиції учасником.**

1. На підтвердження відповідності пропозиції технічним, якісним та кількісним характеристикам предмета закупівлі в складі своєї пропозиції учасник повинен надати довідку у довільній формі про можливість поставки замовнику програмної продукції з урахуванням вимог Розділів II та III Додатку 2 до тендерної документації.

2. На підтвердження відповідності пропозиції технічним, якісним та кількісним характеристикам предмета закупівлі в складі своєї пропозиції учасник повинен надати копію документу, наданого на адресу Замовника виробником (правовласником) запропонованої програмної продукції або його представництвом (представником), повноваження якого розповсюджується на територію України, що підтверджує право або можливість учасника здійснювати продаж запропонованої програмної продукції.

3. У разі, якщо документи зазначені у пункті 2 Розділу IV цього Додатку, надаються

представником виробника (правовласника), учасник процедури закупівлі у складі тендерної пропозиції повинен надати копію(ї) документу(ів) виданого(их) виробником (правовласником) програмної продукції, що підтверджує повноваження (права) такої особи на видання зазначених документів.

4. Будь-яке посилання у даному додатку на конкретні торговельну марку чи фірму, патент, конструкцію або тип предмета закупівлі, джерело його походження або виробника мається на увазі «або еквівалент».

5. Учасник має право запропонувати замовнику програмну продукцію аналогічну (еквівалент) зазначеній у таблиці 1 (Розділ ІІ Додатку 2 до тендерної документації) за умови, що технічні характеристики такої програмної продукції не будуть гіршими від наведених у Розділі ІІІ Додатку 2 до тендерної документації.

6. У разі, якщо учасником буде запропоновано еквівалент зазначеної у пунктах 1-10 таблиці 1 (Розділ ІІ Додатку 2 до тендерної документації) програмної продукції, у складі тендерної пропозиції учасник повинен надати довідку із зазначенням найменування та порівняльних характеристик програмної продукції, яка пропонуються учасником, та програмної продукції зазначеної у пунктах 1-10 таблиці 1 (Розділ ІІ Додатку 2 до тендерної документації), при цьому, така програмна продукція повинна відповідати вимогам наведеним у Розділі ІІІ цього Додатку.

7. У разі, якщо учасник пропонує еквівалент програмної продукції, зазначеної у Розділі ІІ Додатку 2 до тендерної документації, у складі тендерної пропозиції такий учасник має надати документ від виробника відповідного обладнання Замовника або його офіційного представництва (представника), повноваження якого розповсюджується на територію України, про можливість використання запропонованого учасником еквіваленту програмної продукції на наявному у Замовника обладнанні із збереженням умов гарантійного обслуговування з боку виробника обладнання та без погіршення функціональних та програмно-технічних характеристик обладнання, його ресурсу.

8. У разі, якщо документ зазначений у пункті 5 Розділу IV цього Додатку, надається представником виробника обладнання, учасник процедури закупівлі у складі тендерної пропозиції повинен надати копію(ї) документу(ів) виданого(их) виробником обладнання, що підтверджує повноваження (права) такої особи на видання зазначених документів

9. У разі якщо учасником пропонується еквівалент програмної продукції зазначеної у таблиці 1 (Розділ ІІІ Додатку 2 до тендерної документації), учасник має за власний рахунок та власними силами виконати повну інтеграцію запропонованого рішення з існуючою інфраструктурою замовника забезпечивши безперебійність її роботи.