ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

ДО:

ЗАИНТЕРОСОВАНИТЕ ЛИЦА

ПОКАНА

„Информационно обслужване" АД, със седалище и адрес на управление: гр. София, ул. „Панайот Волов" № 2, тел. 02/9420340, e-mail: office@is-bg.net, представлявано от **Ивайло Филипов – Изпълнителен директор**, Ви кани да участвате в процедура за избор на доставчик, при следните условия:

1. **Предмет на процедурата:**

„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване" АД".

Количествената и техническа спецификация на системата и абонаментната поддръжка е посочена в Техническо задание (Приложение № 1)

2. **Период на изпълнение** – 3 (три) години.

2.1. **Срок за доставка на системата и абонаментната поддръжка** – до 10 (десет) работни дни, считано от датата на сключване на договор.

3. **Критерии за оценка на предложенията:** най-ниска предложена цена за изпълнение.

Участниците се класират според предложената от тях обща цена в лева без ДДС. На първо място се класира участникът, предложил най-ниска цена. Оценката се извършва съгласно Методика за оценка на предложенията, приложена към настоящата покана (Приложение № 2).

4. **Списък на документите, които кандидатите следва да представят:**

4.1. Документи за идентификация и квалификация:
4.1.1. Документ/оторизация от производителя на софтуерното решение, удостоверяващ, че кандидатът е оторизиран доставчик за корпоративни клиенти.
4.1.2. Декларация по образец – Приложение № 5.
4.2. Техническо предложение, изготвено по образец – Приложение № 3.
4.3. Ценово предложение, изготвено по образец – Приложение № 4.

5. Начин на плащане - по банков път, на три годишни вноски в срок минимум 30 (тридесет) календарни дни след:

5.1. подписване на приемо-предавателен протокол и приемане без възражения и забележки от Възложителя и издадена фактура от Изпълнителя (за първата годишна вноска);

5.2. издадена фактура от Изпълнителя (за втората и третата годишна вноска).

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

6. **Максимална обща цена** - кандидатите следва да предложат цена, която не надвишава определената максимална обща цена в размер на **1 638 000 (един милион шестстотин тридесет и осем хиляди) лева** без ДДС за период от 3 години, като бъде предвидено заплащане на три годишни вноски, както следва:
   1-ва година – до **720 000 (седемстотин и двадесет хиляди) лева** без ДДС, за доставка на две нови устройства на локално ниво, облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво;
   2-ра година – до **459 000 (четиристотин петдесет и девет хиляди) лева** без ДДС, за поддръжка на услугата, както и облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво;
   3-та година – до **459 000 (четиристотин петдесет и девет хиляди) лева** без ДДС, за поддръжка на услугата, както и облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво.
   Кандидат, предложил по-висока от максималната обща цена и/или от максималната годишна вноска, ще бъде отстраняван от участие в процедурата.

7. Срок на валидност на предложението - срокът на валидност да бъде не по-малко от 60 (шестдесет) календарни дни, считано от датата на представяне на предложението.

8. Подаване на предложението:

8.1. **Срок, място и начин:**

Предложението следва да бъде подадено по електронен път в срок **до 13:00 часа на 07.02.2024 г.**, на следния адрес на електронна поща: office@is-bg.net.

8.2. **Изисквания към подаването на предложението:**

Техническото предложение (Приложение № 3), Ценовото предложение (Приложение № 4) и Декларацията (Приложение № 5) се съставят като електронни документи във формат .pdf и се подписват с квалифициран електронен подпис.

Ако към предложението е необходимо да бъде представен документ, който е издаден на хартиен носител, същият се представя сканиран и заверен с квалифициран електронен подпис.

В случай, че обстоятелства от документите за идентификация и квалификация са достъпни чрез публичен безплатен регистър или информацията е публично достъпна на друг официален адрес, кандидатите могат да посочат електронен адрес, на който тази информация е налична и достъпна.

Електронното съобщение, с което се подава предложението в настоящата процедура, следва да съдържа данни за:

1. наименованието на участника;
2. телефон и електронен адрес;
3. наименованието на процедурата, за която се подават документите.

За дата и час на получаване на предложението се приемат датата и часа на получаване на предложението на посочения в т. 8.1. адрес на електронна поща за подаване на предложения.

„Информационно обслужване“ АД използва инструменти за осигуряване на сигурността на информацията, предавана по електронна поща, които могат да забавят получаването на електронни съобщения, поради което е препоръчително предложенията в настоящата процедура да се изпращат най-малко 30 минути преди крайния срок по т. 8.1.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

9. Лице за контакти с „Информационно обслужване” АД

Георги Костадинов – старши мрежови администратор - отдел „Комуникации“, тел.: +359 876 548 419, e-mail: g.kostadinov@is-bg.net

10. Участници в процедурата

В процедурата могат да участват и кандидати, до които не е изпратена изрична покана.

11. Приложения:

1. Техническо задание – Приложение № 1;
2. Методика за оценка на предложенията – Приложение № 2;
3. Техническо предложение – образец – Приложение № 3;
4. Ценово предложение – образец – Приложение № 4;
5. Декларация – образец – Приложение № 5;
6. Указания за участие в процедурата – Приложение № 6.

Ivaylo Borisov Filipov
Digitally signed by Ivaylo Borisov Filipov
Date: 2024.01.29 11:30:51 +02'00'

Ивайло Филипов
Изпълнителен директор
„Информационно обслужване” АД

Приложение №1

ТЕХНИЧЕСКО ЗАДАНИЕ
с
количествена и техническа спецификация за процедура „Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“

Спецификация на решение за DDoS защита и защита на уеб приложения	
REQ. 1.	Тип решение: Хибридно решение под формата на облачна услуга и 2 бр. физически устройства за DDoS защита и защита на уеб приложения (WAF) и абонамент с включена поддръжка за период от 36 месеца.
REQ. 2.	Предложеното решение да включва компоненти за хибридна DDoS защита на мрежови слоеве 3 и 4, както и компоненти за Web DDoS защита и защита на уеб приложения (WAF) на мрежови слой 7.
REQ. 3.	Решението да включва абонамент за облачна услуга за защита.
REQ. 4.	Решението да включва 2 физически устройства за DDoS защита и защита на уеб приложения (WAF) и да може да се разшири с добавяне на физически устройства, които да са паралелно интегрирани с облачната услуга на същия производител, като облачната услуга за защита от производителя не може да е базирана на устройства за засичане и справяне със заплахи на други производители.
REQ. 5.	Решението да предоставя възможност за използване на виртуални устройства за по-малки изолирани среди или лабораторни среди.
REQ. 6.	Предложеното решение да е с включена платформа за управление на решението, която да може да управлява атаки с капацитет от до 40 Gbps. Лицензът за платформата за управление да включва управлението на 2 физически устройства и 10 виртуални устройства и да предоставя опция за разширяване на тези параметри в бъдеще.
REQ. 7.	Предложеното решение да включва 2 броя физически устройства, всяко с възможност за справяне с атаки с капацитет от до 20 Gbps. Устройствата да разполагат с по 4 слота за разширителни модули и да имат резервирано захранване (по 2 ел. захранвания на устройство)
REQ. 8.	Предложеното решение да включва 2 броя разширителни NIC модула (по един за всяко физическо устройство) с по 4x10G SR слотове с вътрешен байпас за всеки от модулите.
REQ. 9.	Предложеното решение да включва 8 броя 10GE SR (SFP+) компонента.
REQ. 10.	Решението да включва базов абонамент за 36 месеца за облачна DDoS защита за до 500 Mbps легитимен трафик. Абонаментът да позволява задаването на до 4 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 20 защитени IP адреса (DNS).

REQ. 11.	Решението да включва допълнителен абонамент за периода от 36 месеца за допълнителни 50 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 250 защитени IP адреса (DNS), които да се предпазват от облачната DDoS услуга с опции за използване при поискване/хибридно/винаги включена защита.
REQ. 12.	Решението да включва 2 броя разширителни SSL карти за физическите устройства с абонамент за 36 месеца за прилежащи функции за защита от криптирани flood атаки на база поведение, TLS инспекция, защита на приложения и информация за заплахи (threat intelligence).
REQ. 13.	Решението да включва базов абонамент за 36 месеца за модул за защита на облачни приложения (Облачна DDoS + WAF защита на мрежови слой 7) за 1 брой приложение и за до 50 Mbps реален HTTP/S трафик.
REQ. 14.	Решението да включва допълнителен абонамент за 36 месеца за защита на 5 броя допълнителни облачни приложения.
REQ. 15.	Решението да предоставя защита от уеб-базирани атаки срещу приложения по OWASP Top10 модела, стандартни уеб атаки, атаки с фокус върху данни и данни за достъп, както и непознати 0-day атаки.
REQ. 16.	Решението да включва следните функции за WAF модула: използване на негативен или позитивен модел на сигурност, защита на API, управление на ботове, контрол на достъпа, гео-политики за IP адреси, лимитиране на обема трафик към приложенията, използване на напреднали правила за сигурност, използване на ERT Active Attackers Feed (EAAF) технология за защита.
REQ. 17.	Решението да предоставя хибридна DDoS защита, синхронизирайки работата на облачните и на локално разположението компоненти.
REQ. 18.	Решението да може да инспектира криптиран (SSL) трафик.
REQ. 19.	Решението да предоставя функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението.
REQ. 20.	Решението да разполага с автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging).
REQ. 21.	Решението да може да синхронизира политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението.
REQ. 22.	Решението да разполага с облачна Web-DDoS услуга за справяне с атаки на мрежови слой 7 с много голям обем, като да може да засича криптирани атаки, които изглеждат като нормален трафик и използват множество техники за избягване на засичане (evasion techniques).
REQ. 23.	Решението да може да показва референтно сравнение на обема мрежови трафик по времето, когато няма активни атаки (в мирно време) с обема на трафика при протичаща атака, с възможност за предприемане на автоматични защитни мерки срещу атаките според обемите им.

REQ. 24.	Решението да може автоматично да известява при настъпила атака (като да има опция за автоматично генериране на pcap файл след завършване на атаката). Да може да се предоставя информация за параметрите на наложената политика за сигурност на решението, която е спомогнала за спирането на дадена атака.
REQ. 25.	Решението да може автоматично да издава различни отчети по подразбиране в различни формати по зададен график (седмични, месечни).
REQ. 26.	Решението да може да предоставя детайлни отчети със следствени данни (forensics) относно възникналите предишни атаки и настоящите такива.
REQ. 27.	Решението да може да извършва анализ на поведението на IT мрежата (network behavioral analysis). Решението да може да използва механизми за самообучение и засичане на заплахи според промените на обема мрежови трафик и други негови параметри.
REQ. 28.	Решението да може да засича заплахи на базата на собствена база от данни с репутации на IP адреси, която да се поддържа и обновява от производителя на решението в периода на поддръжката.
REQ. 29.	Решението да разполага с функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентикиране на източника на трафика.
REQ. 30.	Решението да може да предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението.
REQ. 31.	Да не е необходимо да се декриптира целият мрежови трафик, за да се предпазва от SSL Flood атаки, а само трафикът от съмнителни източници, за да се намали забавянето откъм производителност на системите.
REQ. 32.	Решението да поддържа използването на поне 50 ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението.
REQ. 33.	Решението да може да анализира поведението на DNS трафик. Да може да се изграждат сигнатури в реално време за възникнали атаки и да се автентикират източниците на мрежовия трафик за справяне с water-torture атаки, DNS flood атаки и Amplification атаки.
REQ. 34.	Решението да може да засича и да блокира непознати до момента заплахи (0-day защита).
REQ. 35.	Решението да може да засича и да блокира Web DDoS атаки чрез маркиране на криптиран HTTPS трафик като зловреден такъв на базата на познати сигнатури или на непознати пръстови отпечатъци (TLS Fingerprinting).
REQ. 36.	Решението да може да засича и блокира burst атаки и botnet атаки.
REQ. 37.	Решението да се обновява автоматично от производителя с нови сигнатури за атаки в периода на поддръжката.
REQ. 38.	Решението да включва услуга за техническа консултация с SOC екипа на производителя при възникване на атака, като времето за реакция от момента на известяването да е не повече от 10 минути.

REQ. 39.	Решението да включва предплатена услуга за имплементация и конфигурация на елементите на решението за работата на облачната DDoS защита.
REQ. 40.	Решението да включва предплатени професионални услуги от производителя за до 20 дни (или до 8 при физическо посещение на място) за консултации, допълнителни услуги по инсталацията на решението или провеждане на обучения на персонала на организацията.

Приложение № 2

Методика за оценка на предложенията

подадени в процедура за избор на доставчик с предмет:

„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“

1. Предложенията се оценяват за съответствие с техническите изисквания в Техническото задание (Приложение № 1).

2. Предложенията, отговарящи на изискванията по т. 1, се оценяват по критерия ***„най-ниска предложена цена за изпълнение“***, като се сравнява предложената обща цена в лева без ДДС.

3. **На първо място се класира участникът, предложил най-ниска цена, като участниците се подреждат по възходящ ред.**

Приложение № 3

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ“ № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за

участие в процедура за избор на доставчик с предмет:

„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“

След запознаване с документацията за участие в процедурата с настоящото техническо предложение правим следните обвързващи предложения:

1. Приемаме да изпълним доставката на системата и абонаментна ѝ поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД, съгласно всички изисквания на Възложителя, посочени в Поканата за участие и съгласно Техническото задание, в съответствие с изискванията и параметрите, посочени в тях.
2. Срок за доставка на системата и абонаментната ѝ поддръжка ……..работни дни /*не повече от 10 (десет) работни дни*/, считано от датата на сключване на договор.
3. Техническото предложение е със срок на валидност …….. /……/ календарни дни (*не по-малко от 60 календарни дни*).
4. Приемаме да осигурим възможност за обновяване по всяко време на софтуерното решение до последна версия за целия период на действие на лицензa.
5. Приемаме да доставим система и абонаментната ѝ поддръжка със следната спецификация:

Спецификация на решение за DDoS защита и защита на уеб приложения	
REQ. 1.	Тип решение: Хибридно решение под формата на облачна услуга и 2 бр. физически устройства за DDoS защита и защита на уеб приложения (WAF) и абонамент с включена поддръжка за период от 36 месеца.
REQ. 2.	Предложеното решение да включва компоненти за хибридна DDoS защита на мрежови слоеве 3 и 4, както и компоненти за Web DDoS защита и защита на уеб приложения (WAF) на мрежови слой 7.

REQ. 3.	Решението да включва абонамент за облачна услуга за защита.
REQ. 4.	Решението да включва 2 физически устройства за DDoS защита и защита на уеб приложения (WAF) и да може да се разшири с добавяне на физически устройства, които да са паралелно интегрирани с облачната услуга на същия производител, като облачната услуга за защита от производителя не може да е базирана на устройства за засичане и справяне със заплахи на други производители.
REQ. 5.	Решението да предоставя възможност за използване на виртуални устройства за по-малки изолирани среди или лабораторни среди.
REQ. 6.	Предложеното решение да е с включена платформа за управление на решението, която да може да управлява атаки с капацитет от до 40 Gbps. Лицензът за платформата за управление да включва управлението на 2 физически устройства и 10 виртуални устройства и да предоставя опция за разширяване на тези параметри в бъдеще.
REQ. 7.	Предложеното решение да включва 2 броя физически устройства, всяко с възможност за справяне с атаки с капацитет от до 20 Gbps. Устройствата да разполагат с по 4 слота за разширителни модули и да имат резервирано захранване (по 2 ел. захранвания на устройство)
REQ. 8.	Предложеното решение да включва 2 броя разширителни NIC модула (по един за всяко физическо устройство) с по 4x10G SR слотове с вътрешен байпас за всеки от модулите.
REQ. 9.	Предложеното решение да включва 8 броя 10GE SR (SFP+) компонента.
REQ. 10.	Решението да включва базов абонамент за 36 месеца за облачна DDoS защита за до 500 Mbps легитимен трафик. Абонаментът да позволява задаването на до 4 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 20 защитени IP адреса (DNS).
REQ. 11.	Решението да включва допълнителен абонамент за периода от 36 месеца за допълнителни 50 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 250 защитени IP адреса (DNS), които да се предпазват от облачната DDoS услуга с опции за използване при поискване/хибридно/винаги включена защита.
REQ. 12.	Решението да включва 2 броя разширителни SSL карти за физическите устройства с абонамент за 36 месеца за прилежащи функции за защита от криптирани flood атаки на база поведение, TLS инспекция, защита на приложения и информация за заплахи (threat intelligence).
REQ. 13.	Решението да включва базов абонамент за 36 месеца за модул за защита на облачни приложения (Облачна DDoS + WAF защита на мрежови слой 7) за 1 брой приложение и за до 50 Mbps реален HTTP/S трафик.
REQ. 14.	Решението да включва допълнителен абонамент за 36 месеца за защита на 5 броя допълнителни облачни приложения.
REQ. 15.	Решението да предоставя защита от уеб-базирани атаки срещу приложения по OWASP Top10 модела, стандартни уеб атаки, атаки с фокус върху данни и данни за достъп, както и непознати 0-day атаки.

REQ. 16.	Решението да включва следните функции за WAF модула: използване на негативен или позитивен модел на сигурност, защита на API, управление на ботове, контрол на достъпа, гео-политики за IP адреси, лимитиране на обема трафик към приложенията, използване на напреднали правила за сигурност, използване на ERT Active Attackers Feed (EAAF) технология за защита.
REQ. 17.	Решението да предоставя хибридна DDoS защита, синхронизирайки работата на облачните и на локално разположението компоненти.
REQ. 18.	Решението да може да инспектира криптиран (SSL) трафик.
REQ. 19.	Решението да предоставя функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението.
REQ. 20.	Решението да разполага с автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging).
REQ. 21.	Решението да може да синхронизира политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението.
REQ. 22.	Решението да разполага с облачна Web-DDoS услуга за справяне с атаки на мрежови слой 7 с много голям обем, като да може да засича криптирани атаки, които изглеждат като нормален трафик и използват множество техники за избягване на засичане (evasion techniques).
REQ. 23.	Решението да може да показва референтно сравнение на обема мрежови трафик по времето, когато няма активни атаки (в мирно време) с обема на трафика при протичаща атака, с възможност за предприемане на автоматични защитни мерки срещу атаките според обемите им.
REQ. 24.	Решението да може автоматично да известява при настъпила атака (като да има опция за автоматично генериране на pcap файл след завършване на атаката). Да може да се предоставя информация за параметрите на наложената политика за сигурност на решението, която е спомогнала за спирането на дадена атака.
REQ. 25.	Решението да може автоматично да издава различни отчети по подразбиране в различни формати по зададен график (седмични, месечни).
REQ. 26.	Решението да може да предоставя детайлни отчети със следствени данни (forensics) относно възникналите предишни атаки и настоящите такива.
REQ. 27.	Решението да може да извършва анализ на поведението на IT мрежата (network behavioral analysis). Решението да може да използва механизми за самообучение и засичане на заплахи според промените на обема мрежови трафик и други негови параметри.
REQ. 28.	Решението да може да засича заплахи на базата на собствена база от данни с репутации на IP адреси, която да се поддържа и обновява от производителя на решението в периода на поддръжката.
REQ. 29.	Решението да разполага с функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентикиране на източника на трафика.

REQ. 30.	Решението да може да предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението.
REQ. 31.	Да не е необходимо да се декриптира целият мрежови трафик, за да се предпазва от SSL Flood атаки, а само трафикът от съмнителни източници, за да се намали забавянето откъм производителност на системите.
REQ. 32.	Решението да поддържа използването на поне 50 ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението.
REQ. 33.	Решението да може да анализира поведението на DNS трафик. Да може да се изграждат сигнатури в реално време за възникнали атаки и да се автентикират източниците на мрежовия трафик за справяне с water-torture атаки, DNS flood атаки и Amplification атаки.
REQ. 34.	Решението да може да засича и да блокира непознати до момента заплахи (0-day защита).
REQ. 35.	Решението да може да засича и да блокира Web DDoS атаки чрез маркиране на криптиран HTTPS трафик като зловреден такъв на базата на познати сигнатури или на непознати пръстови отпечатъци (TLS Fingerprinting).
REQ. 36.	Решението да може да засича и блокира burst атаки и botnet атаки.
REQ. 37.	Решението да се обновява автоматично от производителя с нови сигнатури за атаки в периода на поддръжката.
REQ. 38.	Решението да включва услуга за техническа консултация с SOC екипа на производителя при възникване на атака, като времето за реакция от момента на известяването да е не повече от 10 минути.
REQ. 39.	Решението да включва предплатена услуга за имплементация и конфигурация на елементите на решението за работата на облачната DDoS защита.
REQ. 40.	Решението да включва предплатени професионални услуги от производителя за до 20 дни (или до 8 при физическо посещение на място) за консултации, допълнителни услуги по инсталацията на решението или провеждане на обучения на персонала на организацията.

Прилагаме като неразделна част към настоящото предложение всички необходими документи, както следва:

/Описват се подробно приложените документи, съгласно т. 4 от поканата, както и допълнителни документи, представени по преценка на кандидата/

ПОДПИС

[качество на представляващия участника]

Забележка: *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 4

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ” № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ЦЕНОВО ПРЕДЛОЖЕНИЕ
за
участие в процедура за избор на доставчик с предмет:
„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“

След запознаване с документацията за участие в процедурата с настоящото ценово предложение правим следните обвързващи предложения за изпълнение на доставката съгласно представеното Техническо предложение:

Приемаме да изпълним доставката и абонаментна поддръжка, предмет на настоящата процедура, при обща цена в размер на ……..……(словом:……) лева без вкл. ДДС, на три годишни вноски, както следва:

1-ва година – …… (……..) лева без ДДС, за доставка на две нови устройства на локално ниво, облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво;
2-ра година – ……..(……..) лева без ДДС, за поддръжка на услугата, както и облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво;
3-та година – …… (……..) лева без ДДС, за поддръжка на услугата, както и облачна услуга за волуметрични атаки и Web DDoS защита от нови комплексни атаки на приложно ниво.

В общата цена са включени всички разходи за изпълнение на доставката и абонаментната поддръжка на система за защита от DoS/DDoS атаки, за нуждите на „Информационно обслужване“ АД“, съгласно Техническото предложение.

Начин на плащане - по банков път, в срок ……(*минимум 30 (тридесет) календарни дни)* след:

- подписване на приемо-предавателен протокол и приемане без възражения и забележки от Възложителя и издадена фактура (за първата годишна вноска);

- издадена фактура (за втората и третата годишна вноска).

ПОДПИС:

[качество на представляващия участника]

Забележка: *Ценовото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 5

Образец

ДЕКЛАРАЦИЯ

От.....,

представляващ ..... – кандидат в процедура с предмет: „**Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД**“, в качеството ми на .....,

ДЕКЛАРИРАМ, че представляваното от мен дружество:

1. Не е обявено в несъстоятелност и не е в производство за обявяване в несъстоятелност;
2. Не е в производство по ликвидация.

ДЕКЛАРИРАМ, че:

3. Не съм лишен от правото да упражнявам търговска дейност;
4. Не съм осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 – 260 от НК, за подкуп по чл. 301 – 307 от НК, участие в организирана престъпна група по чл. 321 и чл. 321а от НК, както и за престъпление против собствеността по чл. 194 – 217 от НК или против стопанството по чл. 219 – 252 от НК.

ДЕКЛАРАТОР:

Забележки:

1. Декларацията се представя в електронен вид във формат .pdf, подписана с квалифициран електронен подпис.

2. Декларацията се подписва задължително от управляващия и представляващ дружеството. Когато управляващите дружеството са повече от едно лице, декларацията се подписва от всички лица, вписани в Търговския регистър като представляващи и се представя в отделен екземпляр за всяко представляващо лице.

Приложение № 6

УКАЗАНИЯ

за участие в процедура за избор на доставчик с предмет:

„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“

1. Кандидатите изготвят и окомплектоват предложенията си съгласно изискванията, посочени в поканата и приложенията към нея.
2. Не по-късно от 11:00 ч. на 02.02.2024 г. всеки кандидат може да поиска от Възложителя писмено разяснения по документацията. Възложителят изпраща разяснението до всички кандидати, които са получили документация за участие и са посочили адрес за кореспонденция и го публикува на интернет-страницата на „Информационно обслужване” АД.
3. Предложенията се приемат по начина и в срока, посочени в поканата. Приемат се и предложения на кандидати, които не са поканени с изрична покана.
4. Предложение, получено след изтичане на крайния срок, не се разглежда от Възложителя. В този случай до кандидата се изпраща уведомление.
5. Изборът на доставчици се извършва въз основа на подадените предложения.
6. Изпълнителният директор на „Информационно обслужване” АД назначава комисия за разглеждането и оценяването на подадените предложения.
7. Комисията отстранява от процедурата кандидат, който:
   - е обявен в несъстоятелност/ е в производство по ликвидация / е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - управител или член на управителните органи на кандидат, а в случай, че членове са юридически лица – за техните представители в съответния управителен орган е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - не е изготвил и окомплектовал предложението си съгласно изискванията, посочени в документацията за участие;
   - е представил непълно техническо или ценово предложение.
8. Възложителят може да изиска от кандидатите да представят допълнително документи, с които да докажат икономическото и финансовото си състояние, техническите възможности и/или квалификацията им.
9. След разглеждане на получените предложения, Възложителят може еднократно да поиска от кандидатите да представят подобрено ценово предложение.

10. Кандидатите са длъжни в процеса на провеждане на процедурата да уведомяват за всички настъпили промени в обстоятелствата, за които са представили декларация по образец (Приложение № 5 към поканата) - в 7-дневен срок от узнаването им.
11. Лице, което е дало съгласие и фигурира като подизпълнител в офертата на друг кандидат, не може да представя самостоятелна оферта.
12. Когато при изпълнението на договора кандидатът ще използва подизпълнител, предложението трябва да съдържа изискваните документи за идентификация и квалификация и за подизпълнителя.
13. Когато кандидат за участие в процедурата е обединение на юридически лица (консорциум) за всеки от участниците в консорциума се представят документите за идентификация и квалификация, изисквани от участниците в процедурата.
14. Всички кандидати се уведомяват за резултатите от процедурата в срок от три работни дни, считано от датата на решението на Съвета на директорите, с което се одобрява изборът на доставчик, като на избрания за изпълнител кандидат се предлага да сключи договор при условията на подаденото предложение.
15. Когато избраният за изпълнител кандидат откаже, не представи изискваните документи или по друга причина договорът с него не може да бъде подписан, изпълнителният директор предлага на класирания на следващо място кандидат да сключи договор при условията на подаденото предложение или прекратява тази и насрочва нова процедура за избор на доставчик.
16. При подписване на договора кандидатът, определен за изпълнител, представя електронно свидетелство за съдимост за удостоверяване на обстоятелствата, заявени с декларация по образец (Приложение № 5 към поканата). При невъзможност за представяне на електронно свидетелство за съдимост кандидатът представя свидетелство за съдимост или друг еквивалентен документ – сканирани и заверени с квалифициран електронен подпис. Представените документи не се съхраняват от „Информационно обслужване“ АД.