Приложение № 2
към рамков договор № 67/24.10.2024г.

ЗАЯВКА по Рамков договор № 67/24.10.2024 г. **(№ ПО-16-3173/24.10.2024 г. на ИО АД)**	☒
ЗАЯВКА по Рамков договор № ……от ……г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ: 3*	
Описание на проект съгласно ПГ:	*Осигуряване на Интернет и защита от DDOS атаки*	
CPV код	*72411000-4*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-5426/11.04.2025 г.*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика*) **без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*		*15 600,00 лв. без ДДС, от които:* *За 2025 г. – 7 800,00 лв.;* *За 2026 г. – 7 800,00 лв.;*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*		*На части, както следва:* *• За периода от 12.05.2025 г. до 12.05.2026 г. на тримесечие, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на Интернет и защита от DDOS атаки и издадена фактура на стойност 3 900,00 лв. без ДДС за съответния тримесечен период.* *Към приемо-предавателния протокол се прилага доклад за извършените дейности за съответния тримесечен период.*
Плащане с акредитив или авансово ДА/НЕ		*НЕ*
Документи за плащане с акредитив или авансово		*НЕ*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата*)		*от 12.05.2025 г. до 12.05.2026 г.*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата*)		*Неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*На части, както следва:* *• За периода от 12.05.2025 г. до 12.05.2026 г., на тримесечие, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на Интернет и защита от DDOS атаки за съответния тримесечен период.* *Към приемо-предавателния протокол се прилага*

[1] Отбелязва се в случай че заявката е актуализирана

	доклад за извършените дейности за съответния тримесечен период.
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически спецификации*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:	
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):	*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:	*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:	*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Ръководител на проект по заявката	*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	*Подпис:*

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

Осигуряване на Интернет и защита от DDOS атаки за нуждите на Министерство на енергетиката

1. ПРЕДМЕТ

Предметът на заявката е осигуряване на Интернет, предоставяне на защита от Distributed Denial of Service (DDoS) атаки за Министерство на енергетиката.

Услугата по предоставяне на Интернет включва:

- Изграждане на Интернет свързаност за Министерство на енергетиката на адрес ул. Триадица 8, 1000 София.
- Осигуряване на реални статични адреси – 16 IP адреса.
- Изградената Интернет свързаност отговаря минимум на следните параметри;
  - Минимална скорост за обмен на данни 400 Mbps (симетричен достъп).
  - Свързаност между технически центрове на Информационно обслужване и Министерство на енергетиката с гарантирано MTU от 1500 байта.
  - Интернет достъпът трябва да позволява гарантиран достъп, както до международното Интернет пространство, така и до българските доставчици на Интернет.
  - Свързаността между технически центрове на Информационно обслужване и Министерство на енергетиката следва да е реализирана през две независими тъмни влакна през различни трасета.
  - Гарантирана пропускателна способност на канала в двете посоки до точката на трансминиране на връзката - 100%
  - 100 % симетричност на услугата (Upload/Download = 1/1)
  - Висока надеждност и достъпност на Интернет услугата
  - Наличност на услугата на месечна база - 99,9%
  - Достъпът до Интернет е неограничен по количество трафик
- Осигуряване на поддръжка за времето на договора със следните минимални параметри:
  - Осигурена денонощно техническо обслужване на клиентите - Поддръжка на крайни мрежови устройства и кабелни трасета.
  - Осигурено управлението и поддръжката на Интернет достъпа в режим на работа „24x7".
  - В рамките на 1 час от подаване на сигнал за проблем с Интернет достъпа, проблемът да се диагностицира и да започне отстраняването му.

Услугата по предоставяне на защита от Distributed Denial of Service (DDoS) атаки включва следното решение:

REQ. 1.	Тип решение: Хибридно решение под формата на облачна услуга и физически устройства за DDoS защита в мрежата на доставчика на услугата.
REQ. 2.	Компоненти за хибридна DDoS защита на мрежови слоеве 3 и 4, както и компоненти за Web DDoS защита на мрежови слой 7.
REQ. 3.	Облачна услуга за защита.
REQ. 4.	Инспекция и защита от DDoS в реално време.
REQ. 5.	Капацитет от минимум 400 Mbps чист трафик.
REQ. 6.	Функции за защита от криптирани flood атаки на база поведение, TLS инспекция, защита на приложения и информация за заплахи (threat intelligence).

REQ. 7.	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. 8.	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. 9.	Инспектиране на криптиран (SSL) трафик.
REQ. 10.	Функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението.
REQ. 11.	Автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging).
REQ. 12.	Синхронизиране на политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението.
REQ. 13.	Предоставяне на информация в регулярни отчетни документи на референтно сравнение на обема мрежови трафик по времето, когато няма активни атаки с обема на трафика при протичаща атака, с възможност за предприемане на автоматични защитни мерки срещу атаките според обемите им.
REQ. 14.	Автоматично известяване 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. 15.	Предоставяне на детайлни отчети със следствени данни (forensics) относно възникнали атаки.
REQ. 16.	Извършване на 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. 17.	Засичане на 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. 18.	Функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентикиране на източника на трафика.
REQ. 19.	Предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението.
REQ. 20.	Поддържане използването на ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението.
REQ. 21.	Анализиране на 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. 22.	Засичане и да блокиране на непознати до момента заплахи (0-day защита).
REQ. 23.	Засичане и блокиране на burst атаки и botnet атаки.
REQ. 24.	Задаване и регулиране автоматично прагови стойности за брой: пакети в секунда (PPS), транзакции в секунда (TPS).
REQ. 25.	Функционалност за автоматично създаване на динамични сигнатури посредством анализиране на трафика.
REQ. 26.	Осигуряване на защита от UDP атаки, TCP атаки, DNS атаки., волуметрични атаки, ICMP атаки, HTTP атаки.
REQ. 27.	Осигуряване на защита от следните типове атаки, пропускайки легитимния потребителски трафик: SYN Floods , RST Flood, TCP ECE Flood, TCP NULL Flood.