Приложение № 2

към рамков договор № РД-02-29-19/09.07.2025 г

ЗАЯВКА по Рамков договор № РД-02-29-19/09.07.2025 г (ПО-16-2225/09.07.2025 г. на ИО АД)	☒
ЗАЯВКА по Рамков договор № РД-02-29-19/09.07.2025 г (ПО-16-2225/09.07.2025 г. на ИО АД) (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*4*
Описание на проект съгласно ПГ:	*Доставка на интернет свързаност и осигуряване на защита от DDoS атаки*	
CPV код	*72411000-4*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-15240/17.10.2025 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*	*23 200.00 лв. без ДДС*[2]
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, за периода от 17.10.2025 до 31.12.2026 г., след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ осигуряване Интернет и защита от DDOS атаки и издадена фактура за периода.*
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 17.10.2025 г до 31.12.2026 г*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*НЕПРИЛОЖИМО*

[1] Отбелязва се в случай че заявката е актуализирана

[2] Съгласувано между страните дейностите по проекта са стартирали от 17.10.2025 г., преди подписване на настоящата заявка.

Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*На части:* *• За периода от 17.10.2025 г до 31.12.2026 г., на тримесечие с подписване на приемо-предавателен протокол за извършените дейности по осигуряването на Интернет и защита от DDOS атаки за съответния период.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*
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

ДОСТАВКА НА ИНТЕРНЕТ СВЪРЗАНОСТ И ОСИГУРЯВАНЕ НА ЗАЩИТА ОТ DDOS АТАКИ

София, 2025

1. Предмет

Предметът на заявката е доставка на Интернет свързаност и осигуряване на защита от DDoS атаки за Министерство на иновациите и растежа.

Услугата по предоставяне на Интернет включва:

- Изграждане на Интернет свързаност за Министерство на иновациите и растежа на адрес: гр. София, ул. „Княз Александър I“ № 12
- Осигуряване на реални статични адреси – 32 IP адреса.
- Изградената Интернет свързаност отговаря минимум на следните параметри;
  - Минимална скорост за обмен на данни 400 Mbps (симетричен достъп).
  - Свързаност между техническия център на Информационно обслужване и МИР 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 техническия център на Информационно обслужване и МИР следва да е реализирана през тъмни влакна.
  - 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 възможност 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.	Инспектиране на криптиран (SSL) трафик.
REQ. 9.	Функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението.
REQ. 10.	Автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging).
REQ. 11.	Синхронизиране на политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението.
REQ. 12.	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. 13.	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. 14.	Предоставяне на детайлни отчети със следствени данни (forensics) относно възникнали атаки.
REQ. 15.	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. 16.	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. 17.	Функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентикиране на източника на трафика.
REQ. 18.	Предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението.
REQ. 19.	Поддържане използването на ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението.
REQ. 20.	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. 21.	Засичане и да блокиране на непознати до момента заплахи (0-day защита).
REQ. 22.	Засичане и блокиране на burst атаки и botnet атаки.
REQ. 23.	Задаване и регулиране автоматично прагови стойности за брой: пакети в секунда (PPS), транзакции в секунда (TPS).
REQ. 24.	Функционалност за автоматично създаване на динамични сигнатури посредством анализиране на трафика.
REQ. 25.	Осигуряване на защита от UDP атаки, TCP атаки, DNS атаки., волуметрични атаки, ICMP атаки, HTTP атаки.
REQ. 26.	Осигуряване на защита от следните типове атаки, пропускайки легитимния потребителски трафик: SYN Floods , RST Flood, TCP ECE

	Flood, TCP NULL Flood.

2. Място на доставка и гаранционно обслужване

Мястото на изпълнение на Услугите по техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място е сградата на Министерство на иновациите и растежа в гр. София, ул. „Княз Александър I“ № 12

3. Изисквания към мрежовата и информационната сигурност[2]

3.1 Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

3.2 Във връзка с мрежовата и информационната сигурност на Бенефициера/Възложителя/ МИР/МЕУ и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера/Възложителя/ МИР/МЕУ ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера/Възложителя/ МИР/МЕУ. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Бенефициера/Възложителя/ МИР/МЕУ, подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера/Възложителя/ МИР/МЕУ. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

3.3 Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Бенефициера/Възложителя/ МИР/МЕУ.

3.4 Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на Бенефициера/Възложителя/ МИР/МЕУ;

---

[2] Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на административните органи, които са предмет на защита съгласно приложимото законодателство в областта.

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Бенефициера/Възложителя/ МИР/МЕУ;

(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Бенефициера/Възложителя/ МИР/МЕУ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МИР от страна на Бенефициера/Възложителя/ МИР/МЕУ и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.