ИНФОРМАЦИОННО ОБСЛУЖВАНЕ Вх.№ 30-00-162/05.11.2026 София

към рамков договор № 1005-40-42 от 08.06.2026 г.

ЗАЯВКА по Рамков договор № 1005-40-42 от 08.06.2026 г. **(вх. № ПО-16-2118/08.06.2026г. на ИО АД)**	☒
ЗАЯВКА по Рамков договор № ……./……..2026 г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*23*
Описание на проект съгласно ПГ:	*Осигуряване на Интернет и защита от DDOS атаки*	
CPV код	*72400000-4*	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	*МИДТ-33-00-143/4.11.2026г*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) евро без ДДС***, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*43 200,00 евро без ДДС**	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*На части:* *За периода от 16.10.2026г – 15.10.2028г - след подписване на Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на Интернет и защита от DDOS атаки за съответния тримесечен период и издадена фактура на стойност 5 400,00 евро без ДДС.* *Към приемо-предавателните протоколи се прилага доклад за извършените дейности за съответния тримесечен период.*	
Плащане с акредитив или авансово ДА/НЕ	*НЕ*	

[1] Отбелязва се в случай, че заявката е актуализирана

* Съгласувано между страните, с оглед осигуряване на непрекъснатост на услугата, дейностите по проекта са стартирали от 16.10.2026 г., преди подписване на настоящата заявка.

Документи за плащане с акредитив или авансово	*Неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за осигуряване – от 16.10.2026г.* *Срок за изпълнение - 24 месеца*
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:* *За периода от 16.10.2026г – 15.10.2028г - с подписване на Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера 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-предавателните протоколи се прилага доклад за извършените дейности за съответния тримесечен 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

Осигуряване на Интернет и защита от DDOS атаки за нуждите на Национален Осигурителен Институт (НОИ)

I. ПРЕДМЕТ

Предметът на заявката е осигуряване на Интернет, предоставяне на защита от Distributed Denial of Service (DDoS) атаки за Национален Осигурителен Институт (НОИ).

Услугата по предоставяне на Интернет включва:

- Изграждане на Интернет свързаност за НОИ на адрес бул. „Александър Стамболийски“ № 62-64, София.

- Национален Осигурителен Институт разполага със собствена AS регистрирана в RIPE и собствено IP адресно пространство. НОИ ще обяви до 2 клас С мрежи с публични адреси, които ще използват услугата и ще бъдат защитени. НОИ трябва да направи необходимите промени в страницата на RIPE и да позволи използване на интернет услуга през AS 16344, собственост на Информационно Обслужване.

- НОИ трябва да попълни формуляр за разрешение за използване на облачно базирана DDoS защита – Приложение 1

- Изградената Интернет свързаност отговаря минимум на следните параметри;
  - Осигурена скорост за обмен на данни - 800 Mbps (симетричен достъп).
  - Свързаност между технически центрове на Информационно обслужване и НОИ 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 НОИ 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 и 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 и защита на уеб приложения (WAF) 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 800 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.

II.ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

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.

2. Във връзка с мрежовата и информационната сигурност на Бенефициера (НОИ) 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 (НОИ), 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 (НОИ). 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 (НОИ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (НОИ). При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

[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 Бенефициера (НОИ), които са предмет на защита съгласно приложимото законодателство в областта.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Бенефициера (НОИ) при възникване на инцидент по МИС.

(г) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

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 (НОИ).

4. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Заявката(„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 съответната администрация;

(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 (НОИ);

(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 (НОИ), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Бенефициера (НОИ) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.

Letter of Authorization

To: Radware Ltd / SecurityDam (AS 198949)

From: ……..
(Third Party Company)

Subject: Letter of Authorization
Date: March 26, 2024

This letter gives *explicit* permission to Radware Ltd. / SecurityDam (AS 198949) to advertise or host the following networks:

ASN _____ And/ Or IP Block(s)_____
ASN _____ And/ Or IP Block(s)_____
ASN _____ And/ Or IP Block(s)_____
ASN _____ And/ Or IP Block(s)_____

Full Name: ……..
Position: ……..
Email: …….
Phone: …….
Date: ……

(Authorized Signature)
[Please add your name, title and company name here]