



**Приложение № 2**  
**към рамков договор № ИС-28/02.10.2023 г.**

**Заявка**  
*по рамков договор № ИС-28/02.10.2023 г.*

<b>Позиция от ПГ-2024 г.:</b>	<i>№ по ред от ПГ</i>	6
<b>Описание на дейност/проект съгласно ПГ:</b>	<i>Доставка на интернет свързаност и осигуряване на защита от DDoS атаки за АГКК</i>	
<b>CPV код</b>	7222300-0	
<b>Изискване за достъп до класифицирана информация ДА/НЕ</b>	Не	
<b>Стойност: (стойността следва да съответства на заложената в План-графика) без ДДС</b>	135 000 лв. за 2024 г. – 45 000 лв., за 2025 г. – 45 000 лв., за 2026 г. – 45 000 лв.	
<b>Срок за плащане: (еднократно, на части, периодично или др.)</b>	<p><i>На части, след подписването на приемо-предавателен протокол по чл. 6 от договора за приемане на услугата по доставка на интернет свързаност и осигуряване на защита от DDoS атаки, ведно с отчет, съдържащ статистика на засечени и спрени атаки за съответния период и фактури, както следва:</i></p> <p><b>Периоди за 2024г.:</b>  <i>За 1-ви период 01.01.2024 г. до 30.04.2024 г. – 15 000 лв.;</i>  <i>За 2-ви период 01.05.2024 г. до 31.08.2024 г. – 15 000 лв.;</i>  <i>За 3-ри период 01.09.2024 г. до 31.12.2024 г. – 15 000 лв.</i></p> <p><b>Периоди за 2025 г.:</b>  <i>За 1-ви период 01.01.2025 г. до 30.04.2025 г. – 15 000 лв.;</i>  <i>За 2-ри период 01.05.2025 г. до 31.08.2025 г. – 15 000 лв.;</i>  <i>За 3-ти период от 01.09.2025 г. до 31.12.2025 г. – 15 000 лв.</i></p> <p><b>Периоди за 2026 г.:</b>  <i>За 1-ви период 01.01.2026 г. до 30.04.2026 г. – 15 000лв.;</i>  <i>За 2-ри период 01.05.2026 г. до 31.08.2026 г. – 15 000лв.;</i>  <i>За 3-ти период от 01.09.2026 г. до 31.12.2026 г. – 15 000лв.;</i></p>	
<b>Плащане с акредитив ДА/НЕ</b>	Не	
<b>Документи за плащане с акредитив</b>	Не	
<b>Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</b>	<i>В срок до 01.01.2024 г. да се предостави доставка на интернет свързаност и налична услуга защита Distributed Denial of Service /DDoS/ атаки . Предоставяне на услугата по осигуряване на защита от DDoS атаки от 01.01.2024 г. до 31.12.2026 г.</i>	
<b>Гаранционен срок:</b>	Не е приложимо	
<b>Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)</b>	<p><i>На части,</i></p> <ul style="list-style-type: none"> <li><i>В срок до 01.01.2024 г. да предостави доставка на интернет свързаност и налична услуга защита Distributed Denial of Service /DDoS/ атаки, като работата се приема с приемо-предавателен протокол.</i></li> <li><i>Приемо-предавателен протокол по чл. 6 от</i></li> </ul>	

	<p>договора за приемане на услугата осигуряване на защита от DDoS атаки, ведно с отчет, съдържащ статистика на засечени и спрени атаки за съответния период, както следва:</p> <p><b>Периоди за 2024 г.:</b>  1- ви период от 01.01.2024 г. до 30.04.2024 г.  2- ри период от 01.05.2024 г. до 31.08.2024 г.  3- ти период от 01.09.2024 г. до 14.12.2024 г.  4- ти период от 15.12.2024 до 31.12.2024 г., предава се до 10.01.2025 г. (без финансов ангажимент)</p> <p><b>Периоди за 2025 г.:</b>  1- ви период 01.01.2025 г. до 30.04.2025 г.  2- ри период 01.05.2025 г. до 31.08.2025 г.  3- ти период от 01.09.2025 г. до 14.12.2025 г.  4- ти период от 15.12.2025 г. до 31.12.2025 г., предава се до 10.01.2026 г. (без финансов ангажимент)</p> <p><b>Периоди за 2026 г.:</b>  1- ви период 01.01.2026 г. до 30.04.2026 г.  2- ри период 01.05.2026 г. до 31.08.2026 г.  3- ти период от 01.09.2026г. до 14.12.2026 г.  4- ти период от 15.12.2026 г. до 31.12.2026 г., предава се до 10.01.2027 г. (без финансов ангажимент)</p>
Приложения: (напр.: технически параметри, образци на отчетни документи)	Технически параметри
<b>Настоящата заявка да се изпълни при условията на приложените Технически параметри.</b>	
<b>ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:</b>	
Координатор по заявката:	
Ръководител на проект/действие по заявката (напр.: представител на дирекцията – Заявител):	
Ръководител на договора от страна на АГКК:	
<b>ЗАЯВКАТА е ОДОБРЕНА ОТ:</b>	
Главен счетоводител на АГКК:	
Изпълнителен директор на АГКК:	
<b>ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:</b>	
Координатор от „Информационно обслужване“ АД по заявката	
Ръководител на проект/действие по заявката	

<b>Ръководител по изпълнението на Договора от „Информационно обслужване“ АД</b>	

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

## Технически параметри за заявка

### „Доставка на интернет свързаност и осигуряване на защита от Distributed Denial of Service /DDoS/ атаки за Агенцията по геодезия, картография и кадастър“

#### 1. Общи положения

Агенция по геодезия, картография и кадастър (АГКК) е изпълнителна агенция към Министъра на регионалното развитие и благоустройството и е създадена на основание Закона за кадастър и имотния регистър (ЗКИР). Основна задача на Агенцията е създаването и поддържането на кадастралната карта и регистри на страната, с което да се повиши правната сигурност при сделките с недвижими имоти и да се подпомогне развитието на поземлено-имотните отношения за постигане на ефективен пазар на недвижими имоти (съответно увеличаване на инвестициите в строителството, земеделието, търговията, производството и услугите).

Всички дейности по приемане и поддържане на кадастралната карта и кадастралните регистри и предоставянето на услуги с кадастрална информация се извършват чрез централизираните Информационна система на кадастърта и имотния регистър и Кадастрална административна информационна система. Системите изискват сигурна защита срещу всякакъв тип атаки, включително и такива от типа DDoS.

Съгласно Чл. 24 от Наредбата за минимални изисквания за мрежовата и информационна сигурност, АГКК трябва да прилага набор от указания за защита на Web сървърите. Съгласно Чл. 24. т. 9 от Наредбата за минимални изисквания за мрежовата и информационна сигурност, трябва да се реализира противодействие на кибер атаки от типа DDoS (Отказ от услуга).

#### 2. Цел на настоящата заявка

Цел на настоящата заявка е доставка на интернет свързаност и предоставяне на услуга „Защита от Distributed Denial of Service /DDoS/ атаки“. Услугата трябва да е в режим „Винаги налична“ и да осигурява неутрализирането на атаки от Интернет пространството към мрежата и изчислителните устройства на АГКК, които могат да доведат до консумиране на честотна лента на атакуваната мрежа или да претоварят изчислителните ресурси на атакуваните устройства.

#### 3. Обхват на работата и задачи

- 3.1. Предоставяне на винаги налична защита Distributed Denial of Service /DDoS/ атаки;
- 3.2. Осигуряване на интернет свързаност със минимална скорост 100 Mbps и диапазон от минимум 16 реални статични адреса
- 3.3. Изграждане на интернет свързаност за централен офис АГКК:

- да се осигури интернет свързаност за град София със скорост минимум 100 Mbps.

- да се предоставят 16 реални статични IP адреса, които да не се променят в

рамките на договора, освен при изрично искане от АГКК. Да има възможност за осигуряване на допълнителни реални статични IP адреси

- 3.4. До 100Mbps капацитет на входящия български и международен интернет трафик към портовете на АГКК;
- 3.5. Услугата не засяга изходящия от АГКК трафик;
- 3.6. Проактивен мониторинг за установяване на DDoS атаки към мрежата на АГКК, извършван Изпълнителя;
- 3.7. Осигуряване на 24/7 активни телефон и мейл за връзка с Изпълнителя при установени от Възложителя атаки или проблеми в предоставяната услуга.

#### **4. Резултати от работата**

- 4.1. Интернет достъп с минимална скорост 100 Mbps и набор от 16 реални статични IP адрес
- 4.2. Защита от Distributed Denial of Service /DDoS/ атаки на входящия в АГКК Интернет трафик;
- 4.3. Защитата се осъществява с технически и програмни средства на Изпълнителя;
- 4.4. Осигуряване на „чист“ трафик към АГКК със скорост до 100Mbps;
- 4.5. Наличност на услугата на 80% на месечна база;
- 4.6. Възможност за 24/7 поддръжка при възникнали атаки или проблеми с услугата.

#### **5. Време за реакция**

- 5.1. В процеса на изпълнение на настоящата заявка, Възложителят ще получи достъп до „тикет системата“ на Изпълнителя за проследяване на инциденти. Всички възникнали проблеми ще се регистрират, проследяват и управляват през тази система.
- 5.2. Време за реакция - до 1 час след регистриране на проблем.
- 5.3. Време за отстраняване на проблем - до 4 часа след регистриране на проблем.