



**РЕПУБЛИКА БЪЛГАРИЯ**  
**МИНИСТЪР НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ**

---

**ЗАПОВЕД**

№ ...../.....202... г.

На основание чл. 25, ал. 4 от Закона за администрацията, във връзка с чл. 5, т. 8 и чл. 10 от Устройствения правилник на Министерството на електронното управление, Споразумение за финансиране № 101128086 — NCC-BG — DIGITAL-ECCC-2022-CYBER-03 на проект „Национален координационен център – България NCC-BG“, във връзка със Заповед № МЕУ-8161/06.06.2025 г. за утвърждаване на пакет документи за провеждане на процедура за предоставяне на безвъзмездна финансова помощ „Подкрепа за подобряване на киберсигурността в малките и средни предприятия в Република България“ и одобрен доклад с рег. № .....

**НАРЕЖДАМ:**

**I.** Изменям т. 8 от Условията за кандидатстване за предоставяне на безвъзмездни средства, както следва:

Минималният и максималният размер на безвъзмездното финансиране по всяко индивидуално проектно предложение по процедурата е както следва:	
Минимален размер на безвъзмездното финансиране за предприятие	Максимален размер на безвъзмездното финансиране за предприятие
5 000 лева	до 60 000 лева за микро и малко предприятие
	до 60 000 евро или 117 349,80 лева (равностойност в лева по официалния курс на БНБ – 1,95583 лв. за 1 евро) за средно предприятие

**II.** Изменям т. 13.2 от Условията за кандидатстване за предоставяне на безвъзмездни средства, като текста „Друго приложимо решение“ се заличава навсякъде, където се среща.

**III.** Изменям т. 20 от Условията за кандидатстване за предоставяне на безвъзмездни средства, както следва:

„Крайният срок за подаване на предложения по настоящата процедура е 16:30 часа на 15.08.2025 г.“.

**IV.** Изменям т. 1.2. от Условието за изпълнение за предоставяне на безвъзмездни средства по процедура чрез подбор на предложения за подкрепа за подобряване на киберсигурността в малките и средни предприятия в Република България, както следва:

**„1.2. Правила за възлагане на дейности по проекти на бенефициенти**

В процеса на изпълнение на проекта, бенефициентите възлагат дейностите по него по реда на ЗОП и по реда на чл. 208 от Регламент (ЕС, Евратом) 2024/2509 на Европейския парламент и на Съвета от 23 септември 2024 година за финансовите правила, приложими за общия бюджет на Съюза (Регламент (ЕС, Евратом) 2024/2509), както следва:

1.2.1. В случаите, когато бенефициентът е възложител по смисъла на ЗОП (чл. 5), за възлагане на дейности по проекта същият задължително прилага разпоредбите на ЗОП и актовете по прилагането му.

1.2.2. В случаите, когато бенефициентът не е възложител по смисъла на ЗОП (чл. 5), за възлагане на дейности по проекта същият прилага реда на чл. 208 от Регламент (ЕС, Евратом) 2024/2509, при спазване на следните правила за възлагане:

При възлагане на дейности по чл. 208 от Регламент (ЕС, Евратом) 2024/2509, бенефициентите следва да гарантират спазването на принципите за добро стопанско управление, определяне реалистичността на разходите и осигуряване на ефективност, ефикасност и икономичност при разходването на средствата, както и спазване на принципите за публичност и прозрачност, свободна и лоялна конкуренция, равнопоставеност и недопускане на дискриминация при разходването на средствата.

А) Бенефициентът следва да направи **пазарно проучване** до минимум 2 (два) доставчика на стоки/услуги, като изпрати съобщение по електронна поща с приложени документи: технически изисквания за изпълнение на доставката/услугата; техническо предложение (образец), ценово предложение (образец), критерии за оценка на получените оферти и проект на договор (образец).

**Техническите изисквания за изпълнение на доставката/услугата** следва да са съобразени със съответната инвестиционна област, посочена в т. 12.1. и допустимите за финансиране дейности по т. 13.2. от Условието за кандидатстване по процедурата и следва да включват минимум следните изисквания:

➤ Бенефициентът определя техническите изискванията съобразно приложимите нормативни актове в съответната област, като прилага някой от следните начини:

1. чрез посочване на работните характеристики или функционалните изисквания, включително екологичните, които позволяват точно определяне на параметрите на доставката/услугата;

2. чрез посочване (допълнено с думите „или еквивалентно/и“) в следния ред на:

- а) български стандарти, които въвеждат европейски стандарти;
- б) европейски технически оценки;
- в) общи технически спецификации;
- г) международни стандарти;
- д) други стандартизационни документи, установени от европейски органи по стандартизация, или когато няма такива - чрез български стандарти, български технически одобрения или български технически спецификации, отнасящи се до използването на стоките;

3. чрез определяне на работни характеристики или на функционални изисквания чрез посочване на спецификации по т. 2, позоваването на които се приема за постигане на съответствие с изискванията за работните характеристики или функционални изисквания;

4. чрез спецификации по т. 2 за част от характеристиките, а за други - чрез посочване на работните характеристики или функционалните изисквания по т. 1.

Бенефициентът може да постави допълнителни изисквания, които са свързани с предмета на доставката/услугата и са пропорционални на нейната стойност и цели. Те могат да се отнасят до специфичен процес или метод за производство или предоставяне на доставки или услуги, или до специфичен процес на друг етап от жизнения им цикъл.

Техническите изисквания не трябва да нарушават конкурентните условия и равното третиране на доставчиците на стоки/услуги, участващи в пазарното проучване, както и да създава необосновани пречки пред възлагането на съответната дейност по проекта в условията на конкуренция.

➤ Предметът на дейност на доставчика на стоки/услуги следва да е относим към избраната от бенефициента инвестиционна област, съгласно т. 12.1. от Условиата за кандидатстване по процедурата.

➤ Доставчикът на стоки/услуги трябва да осигури лицензионен срок/гаранционен срок/гаранционна поддръжка на предоставените стоки/услуги, не по-кратък от 12 (дванадесет) месеца.

**Техническото и ценовото предложение за изпълнение на доставката/услугата** се изготвят по образец на бенефициента и се прилагат към офертата. Цените, предложени от участниците, трябва да бъдат посочени в лева, до втори знак след десетичната запетая.

#### **Критерии за оценка на получените оферти**

Подборът на получените оферти следва да се извърши въз основа на **критерий за оценка „оптимално съотношение качество/цена“**, чрез прилагане на методика за оценка или въз основа на **критерий за оценка „най-ниска цена“**, в зависимост от избраната допустима дейност за финансиране по чл. 13.2. от Условиата за кандидатстване по процедурата:

- Бенефициентът следва да избере най-изгодната оферта за изпълнение на следните допустими дейности за финансиране по чл. 13.2. от Условиата за кандидатстване по процедурата, въз основа на **критерий за оценка „оптимално съотношение качество/цена“**:
1. Реализиране на център за киберсигурност като услуга (SoCaaS);
  2. Изграждане или наемане на WAF (Web Application Firewall);
  3. Решение за споделяне на файлове с криптирана връзка;
  4. IaaS – Инфраструктура като услуга;
  5. Облачно базирано DLP решение;
  6. EDR решение (Endpoint Detection and Response);
  7. SIEM решение;
  8. Платформа за разпознаване и превенция на киберзаплахи (CTI);
  9. XDR решение (Extended Detection and Response).

Методиката е както следва:

Показатели за оценяване	Максимален брой точки	Относителна тежест
ТП – Технически показател	50	50%
ЦП – Ценови показател	50	50%

Оценка на техническия показател ТП – максимален брой точки – 50 т., се изчислява по следната формула:

$$ТП = 50 \times \frac{ТП_{\text{участник}}}{5}$$

$$ТП_{\text{участник}} = ТП1+ТП2+ТП3+ТП4+ТП5$$

Подпоказателите ТП1-ТП5 са различни за всяка допустима дейност за финансиране по чл. 13.2. от Условията за кандидатстване по процедурата, която подлежи на оценка чрез критерий за оценка „оптимално съотношение качество/цена“. Доставчикът на стоки/услуги, който не притежава/изпълнява съответния подпоказател за оценка получава 0 т., а в случай че притежава/изпълнява съответния подпоказател, получава 1 т.

#### 1. Реализиране на център за киберсигурност като услуга (SoCaaS)

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
ТП1	Наличие на 24/7 мониторинг Центърът осигурява денонощно наблюдение.	1 т.
ТП2	Реално време за реакция и нива на SLA Определени време за реакция при инциденти (TTR, TTI, SLA нива)	1 т.
ТП3	Включване на SIEM/EDR/Threat Intel Интегрира ли други технологии за пълно покритие	1 т.
ТП4	Капацитет за разследване и отчитане Аналитични доклади, root cause анализи, препоръки	1 т.
ТП5	Конфиденциалност и място на данните Къде се съхраняват и как се криптират клиентските данни?	1 т.

#### 2. Изграждане или наемане на WAF (Web Application Firewall)

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3

<b>ТП1</b>	<b>Обхват на защита</b> OWASP Top 10, Zero-day защиты, rate limiting	1 т.
<b>ТП2</b>	<b>Интеграция с приложения</b> Интеграция с уеб сървъри и уеб платформи	1 т.
<b>ТП3</b>	<b>Логване и анализ</b> Достъп до log-и, API, SIEM интеграция	1 т.
<b>ТП4</b>	<b>Актуализиране на сигнатури</b> Автоматични обновления на политики и правила	1 т.
<b>ТП5</b>	<b>Управление и видимост</b> GUI, API достъп, конфигурационни опции	1 т.

### 3. Решение за споделяне на файлове с криптирана връзка

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Ниво на криптиране</b> AES-256, TLS 1.2/1.3, end-to-end encryption.	1 т.
<b>ТП2</b>	<b>Контрол на достъпа</b> Ролева политика, 2FA, еднократни връзки	1 т.
<b>ТП3</b>	<b>Водене на audit logs</b> Пълна история на достъпите и действията	1 т.
<b>ТП4</b>	<b>Хостинг и локация на данни</b> Данните хоствани ли са в ЕС?	1 т.
<b>ТП5</b>	<b>Управление на срокове и разрешения</b> Валидност, download ограничения, класификация на файлове	1 т.

### 4. IaaS – Инфраструктура като услуга

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Надеждност и SLA</b> Наличие на Tier III/IV, висока наличност	1 т.
<b>ТП2</b>	<b>Сигурност на виртуалната инфраструктура</b> Изолиране на мрежи, защита от външни заплахи	1 т.
<b>ТП3</b>	<b>Управляемост и автоматизация</b> Интерфейс, Terraform/API достъп, автоматично скалиране	1 т.
<b>ТП4</b>	<b>Интеграция с защитни компоненти</b> Може ли да се ползват DLP, EDR, WAF и др.	1 т.

<b>ТП5</b>	<b>Съответствие с регулации</b> GDPR, ISO 27001, локален контрол върху данните	1 т.
------------	---	------

### 5. Облачно базирано DLP решение

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Покритие на канали</b> Имейл, облачни услуги, външни носители, браузър	1 т.
<b>ТП2</b>	<b>Методи за откриване</b> Content inspection, регулярен израз, ML класификация	1 т.
<b>ТП3</b>	<b>Политики за предотвратяване</b> Автоматични действия при нарушение – блок, лог, известие	1 т.
<b>ТП4</b>	<b>Централизирано управление</b> Единна конзола, роли и права	1 т.
<b>ТП5</b>	<b>Съхранение и конфиденциалност</b> Място на данни, криптиране, GDPR съответствие	1 т.

### 6. EDR решение (Endpoint Detection and Response)

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Поведенчески анализ и ML</b> Открива нови типове атаки, не само сигнатури	1 т.
<b>ТП2</b>	<b>Реакция на инциденти</b> Изолиране, блокиране, rollback, forensic tools	1 т.
<b>ТП3</b>	<b>Поддържани ОС</b> Windows, macOS, Linux, мобилни устройства	1 т.
<b>ТП4</b>	<b>Централно управление</b> Конзола, логове, известия, политики	1 т.
<b>ТП5</b>	<b>Интеграция с SIEM и SOC</b> Възможност за автоматично известяване и триаж	1 т.

### 7. SIEM решение

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Обхват на събиране на данни</b> Сървъри, мрежови устройства, приложения, cloud	1 т.
<b>ТП2</b>	<b>Корелация на събития</b> Вградени правила и възможност за custom правила	1 т.

<b>ТП3</b>	<b>Реално време</b> Dashboard, alert-и, нотификации	1 т.
<b>ТП4</b>	<b>Форензика и история</b> Запазване на логове, анализ по време	1 т.
<b>ТП5</b>	<b>Поддръжка и разширяемост</b> Поддръжка на нови източници, скалируемост	1 т.

#### 8. Платформа за разпознаване и превенция на киберзаплахи (CTI)

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Източници на информация</b> OSINT, dark web, партньорски бази	1 т.
<b>ТП2</b>	<b>Автоматична корелация</b> Интеграция със SIEM/EDR за реакция	1 т.
<b>ТП3</b>	<b>Индикатори и тактики</b> IoC, TTPs, съвместимост с MITRE ATT&CK	1 т.
<b>ТП4</b>	<b>Формиране на доклади и съвети</b> Автоматични анализи, превантивни препоръки	1 т.
<b>ТП5</b>	<b>Своевременност и обхват</b> Колко често се обновява и какъв обхват покрива?	1 т.

#### 9. XDR решение (Extended Detection and Response)

№	ПОДПОКАЗАТЕЛИ ЗА ОЦЕНКА	МАКСИМАЛЕН БРОЙ ТОЧКИ
1	2	3
<b>ТП1</b>	<b>Централизирана видимост</b> Обединение на endpoint, мрежа, cloud, identity telemetry	1 т.
<b>ТП2</b>	<b>Автоматични отговори</b> Response playbooks, автоматично изолиране и блокиране	1 т.
<b>ТП3</b>	<b>Интеграция със SIEM, EDR, DLP</b> Съвместимост с други решения	1 т.
<b>ТП4</b>	<b>ML и аналитика</b> Аномалии, поведенчески анализ	1 т.
<b>ТП5</b>	<b>Разширяемост и управление</b> Възможност за добавяне на нови източници, скалируемост	1 т.

Оценка на ценовия показател ЦП – максимален брой точки – 50 т., се изчислява по следната формула:

$$\text{ЦП} = 50 \times \frac{\text{Ц}_{\min}}{\text{Ц}_n},$$

където:

$C_{\min}$  е най-ниската цена за изпълнение, предложена от доставчик на стоки/услуги;

$C_n$  е предложена от оценявания доставчик на стоки/услуги цена за изпълнение на дейността.

**Комплексната оценка** се изчислява по следната формула:

$$КО = ТП \times 0,50 + ЦП \times 0,50$$

Максималната възможна комплексна оценка е 50 точки.

Офертите се класират по сумарно получения брой точки от всички показатели за комплексна оценка (КО) – технически показател (ТП) и ценови показател (ЦП). Офертата, получила най-висока оценка КО, се класира на първо място.

- Бенефициентът следва да избере най-изгодната оферта за изпълнение на следните допустими дейности за финансиране по чл. 13.2. от Условието за кандидатстване по процедурата, въз основа на **критерий за оценка „най-ниска цена“**:

1. Надграждане/изграждане на 2FA за уеб приложение;
2. Внедряване на EDR, XDR решения за откриване и реагиране на заплахи;
3. Внедряване на SIEM решения за управление на уязвимостта;
4. Внедряване/надграждане на система за защита на информацията в локална мрежа (напр. защитна стена; система за разпознаване на пробиви (IPS));
5. Внедряване/надграждане на система за архивиране на информация (напр. автоматично архивиране на информация от сървъри/работни станции/мобилни устройства; вграждане на защита от атаки от типа "ransomware" и др.);
6. Изграждане на защитени канали за предаване на данни между клиенти или офиси (VPN свързаност);
7. Изграждане на система за управление на достъпа;
8. Внедряване/надграждане на система за управление на съхранението и споделянето на информация (напр. централизирано управление на достъпа на служителите до информация и споделянето; наличие на журналиран запис на действията на потребителите (audit log); DLP система; хардуерни елементи, включени в минималния обхват; сървър за съхранение и управление на информация и данни и др.);
9. Развитие на професионалния капацитет и повишаване на квалификацията на персонала в областта на киберсигурността;
10. Покупка на лицензи (например антивирусни, база данни, NextGENFirewall, сървъри, сертификати и др.);
11. Одити по информационна сигурност;
12. Сертифициране по ISO 27001;
13. Обучения;
14. Провеждане на тестове за уязвимости.

Бенефициентът класира на първо място доставчика на стоки/услуги, предложил най-ниска обща цена за изпълнение на съответната допустима за финансиране дейност.



\*Когато доставчиците на стоки/услуги не могат да бъдат класирани при критерий за оценка „оптимално съотношение качество/цена“, тъй като са получили една и съща комплексна оценка при прилагане на методиката за оценка, или ако при критерий за оценка „най-ниска цена“ най-ниската обща цена се предлага в две или повече оферти, класирането се извършва чрез жребий, на който могат да присъстват представители на доставчиците на стоки/услуги, които участват в жребия.

Б) След получаване на офертите бенефициентът **съставя протокол**, който съдържа констатация, че получените офертите отговарят/не отговарят на техническите изисквания на бенефициента и мотиви за допускане/недопускане на офертите до оценка, съобразно посочения по-горе критерий за оценка на офертите, оценка и класиране на допуснатите оферти.

В) Бенефициентът сключва **писмен договор** с избрания доставчик на стоки/услуги, съобразно проекта на договор, приложен към пазарното проучване. Във връзка с изпълнението на договора за финансиране, бенефициентите нямат право да сключват договори с лица, с които са свързани по смисъла на § 1. от Допълнителните разпоредби на Търговския закон и/или са обект на конфликт на интереси. В случай че кандидатът реши да пристъпи към изпълнение на дейностите по проекта след подаване на проектното предложение и преди сключване на договора за финансиране, следва да се има предвид, че ако предложението не бъде одобрено за финансиране, разходите, които са направени по отношение на дейностите, за които е приложено предварително изпълнение, няма да бъдат възстановени.“.

V. Документите по т. I - IV да се публикуват на интернет страницата на Министерството на електронното управление, в Информационната система за управление и наблюдение „ИСУН 2020“ <https://umis2020.government.bg/>, както и на Портала за финансиране и обществени поръчки на ЕС <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>.

**VI.** Контрола по изпълнението на настоящата заповед ще осъществявам лично.

Настоящата заповед да се сведе до знанието на главния секретар на Министерството на електронното управление, на директорите на дирекция „Мрежова и информационна сигурност“, дирекция „Правни дейности и обществени поръчки“, дирекция „Връзки с обществеността и протокол“, дирекция „Финанси“ и дирекция „Административно обслужване“ в Министерството на електронното управление, чрез електронната деловодна система, за сведение и изпълнение.

**ВАЛЕНТИН МУНДРОВ**

*Министър на електронното управление*