**МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ**

**ДИРЕКЦИЯ „УПРАВЛЕНИЕ НА ПРОГРАМИ“ – МЕЖДИННО ЗВЕНО ПО ПРИОРИТЕТ 2 НА ПРОГРАМА „НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ“ 2021-2027**

**УСЛОВИЯ ЗА КАНДИДАТСТВАНЕ**

**за предоставяне на безвъзмездна финансова помощ по**

**Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027**

**Приоритет 2 „Цифрова трансформация на публичния сектор“,**

**Специфична цел: RSO1.2. Усвояване на ползите от цифровизацията за гражданите, дружествата, изследователските организации и публичните органи,**

**Приоритетно направление 2: Киберсигурност**

**Процедура чрез директно предоставяне на безвъзмездна финансова помощ BG16RFPR002-2.018 “Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността”**

[1. Наименование на програмата: 3](#_Toc209015659)

[2. Наименование на приоритета и специфичната цел: 3](#_Toc209015660)

[3. Наименование на процедурата: 3](#_Toc209015661)

[4. Измерения по кодове: 3](#_Toc209015662)

[5. Териториален обхват: 3](#_Toc209015663)

[6. Цели на предоставяната безвъзмездна финансова помощ по процедурата и очаквани резултати: 4](#_Toc209015664)

[7. Индикатори (показатели): 11](#_Toc209015665)

[8. Общ размер на безвъзмездната финансова помощ по процедурата и разпределение по категория региони: 13](#_Toc209015666)

[9. Минимален (ако е приложимо) и максимален размер на безвъзмездната финансова помощ за конкретен проект: 13](#_Toc209015667)

[10. Процент на съфинансиране: 14](#_Toc209015668)

[11. Допустими кандидати: 14](#_Toc209015669)

[12. Допустими партньори (ако е приложимо): 15](#_Toc209015670)

[13. Дейности, допустими за финансиране: 15](#_Toc209015671)

[14. Категории разходи, допустими за финансиране: 17](#_Toc209015672)

[14.1. Условия за допустимост на разходите 18](#_Toc209015673)

[14.2. Допустими разходи 21](#_Toc209015674)

[14.3. Недопустими разходи 22](#_Toc209015675)

[15. Допустими целеви групи (ако е приложимо): 22](#_Toc209015676)

[16. Приложим режим на минимални/държавни помощи (ако е приложимо): 22](#_Toc209015677)

[17. Хоризонтални политики: 23](#_Toc209015678)

[18. Минимален и максимален срок за изпълнение на проекта (ако е приложимо): 24](#_Toc209015679)

[19. Ред за оценяване на концепциите за проектни предложения (ако е приложимо) 24](#_Toc209015680)

[20. Критерии и методика за оценка на концепциите за проектни предложения (ако е приложимо) 24](#_Toc209015681)

[21. Ред за оценяване на проектните предложения: 24](#_Toc209015682)

[22. Критерии и методика за оценка на проектните предложения: 25](#_Toc209015683)

[23. Начин на подаване на проектните предложения/концепциите за проектни предложения: 26](#_Toc209015684)

[24. Списък на документите, които се подават на етап кандидатстване: 26](#_Toc209015685)

[25. Краен срок за подаване на проектните предложения: 27](#_Toc209015686)

[26. Допълнителна информация 27](#_Toc209015687)

[27. Приложения към Условията за кандидатстване: 28](#_Toc209015688)

## 1. Наименование на програмата:

Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027 (ПНИИДИТ)

## 2. Наименование на приоритета и специфичната цел:

Приоритет 2 „Цифрова трансформация на публичния сектор“

Специфична цел: RSO1.2. „Усвояване на ползите от цифровизацията за гражданите, дружествата, изследователските организации и публичните органи“

Приоритетно направление 2„Киберсигурност“

## 3. Наименование на процедурата:

BG16RFPR002-2.018 „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността”

## 4. Измерения по кодове:

**Измерение 1 – Област на интервенция**

017. ИКТ решения на държавното управление, електронни услуги, приложения, отговарящи на критериите за намаляване на емисиите на парникови газове или за енергийна ефективност

037. ИКТ: Други видове ИКТ инфраструктура (включително големи компютърни ресурси/оборудване, центрове за данни, датчици и друго безжично оборудване), които отговарят на критериите за намаляване на въглеродните емисии и за енергийна ефективност

**Измерение 2 — Форма на финансиране**

01. Безвъзмездни средства

**Измерение 3 — Териториален механизъм за изпълнение и териториална насоченост**

33. Друг подходи — Без целеви територии

**Измерение 6 – Допълнителни тематични области във връзка с ЕСФ+:**

09. Не се прилага

**Измерение 7 – Равенство между половете във връзка с ЕСФ+, ЕФРР, КФ и ФСП**

03. Полово неутрално

## 5. Териториален обхват:

Дейностите по настоящата процедура следва да бъдат изпълнени на територията на Република България.

Съгласно член 63, параграф 4 на Регламент (ЕС) 2021/1060 на Европейския парламент и на Съвета от 24 юни 2021 година за установяване на общоприложимите разпоредби за Европейския фонд за регионално развитие, Европейския социален фонд плюс, Кохезионния фонд, Фонда за справедлив преход и Европейския фонд за морско дело, рибарство и аквакултури, както и на финансовите правила за тях и за фонд „Убежище, миграция и интеграция“, фонд „Вътрешна сигурност“ и Инструмента за финансова подкрепа за управлението на границите и визовата политика част от дейностите по проекта може да се изпълняват извън територията на Република България, включително извън територията на Съюза, при условие че допринасят за постигане на целите на програмата/процедурата.

Резултатите от изпълнението на проекта следва да се ползват на територията на Република България.

## 6. Цели на предоставяната безвъзмездна финансова помощ по процедурата и очаквани резултати:

**Цел на процедурата:**

Целта на процедурата е цялостното технологично осигуряване на националната система за киберсигурност чрез надграждане на съществуващи и придобиване на нови централни технологични решения за повишаване на нивото на защита на конституенти - административни органи.

**Обосновка:**

Мрежите и информационните системи се превърнаха в ключов елемент на всекидневния живот на фона на бързата цифрова трансформация и взаимосвързаността в обществото, включително в трансграничния обмен. Това поражда увеличаването на броя на киберзаплахите и изисква адаптирани, координирани и новаторски реакции, вкл. на ниво Европейски съюз.

Броят, мащабът, сложността, честотата и въздействието на киберинцидентите се увеличават и представляват съществена заплаха за функционирането на мрежите и информационните системи. В резултат на това инцидентите могат да попречат на функционирането на вътрешния пазар, да причинят финансова загуба, да подкопаят доверието на потребителите и да причинят съществени вреди на икономиката и обществото. Затова подготвеността и ефективността в областта на киберсигурността сега са по-важни от всякога.

По данни на Европейската агенция за киберсигурност (ENISA) най-уязвим на различни типове кибератаки е публичния сектор като почти 20 % от всички кибератаки са насочени именно към данните на администрацията.

Затова адекватно ниво на киберсигурност е ключов фактор, който предоставя възможност на редица критични сектори да се включат успешно в цифровата трансформация и да се възползват изцяло от икономическите, социалните иустойчивите предимства на цифровизацията[[1]](#footnote-1). Като се имат предвид тези развития, бъдещите задачи и отговорности, свързани с киберсигурността, са от съществено значение за оцеляването и жизнеспособността на всяка една организация.

Развитието на националната система за киберсигурност допринася за развитие на системата за защита на националната сигурност. Сигурността на киберпространството е неотделима част от националната сигурност. За развитие и гарантиране на сигурно киберпространство, като един от важните национални интереси се изгражда Националната система за киберсигурност, която е интегрален елемент на системата за управление и защита на националната сигурност. Системата за киберсигурност гарантира демократично и ефикасно управление на държавните и административните органи, публичните институции, предоставящи обществени услуги, и споделяне на усилията от лицата, осъществяващи публични функции, ръководителите на стратегически обекти от значение за националната сигурност, операторите, предоставящи съществени и/или цифрови услуги, гражданите и техните организации.

Взаимосвързаността и многоаспектността поставят високи изисквания към съвременната архитектура за киберсигурност. Изискват се способности за координиран отговор на мащабни киберинциденти, както на национално ниво, така и на европейско ниво.

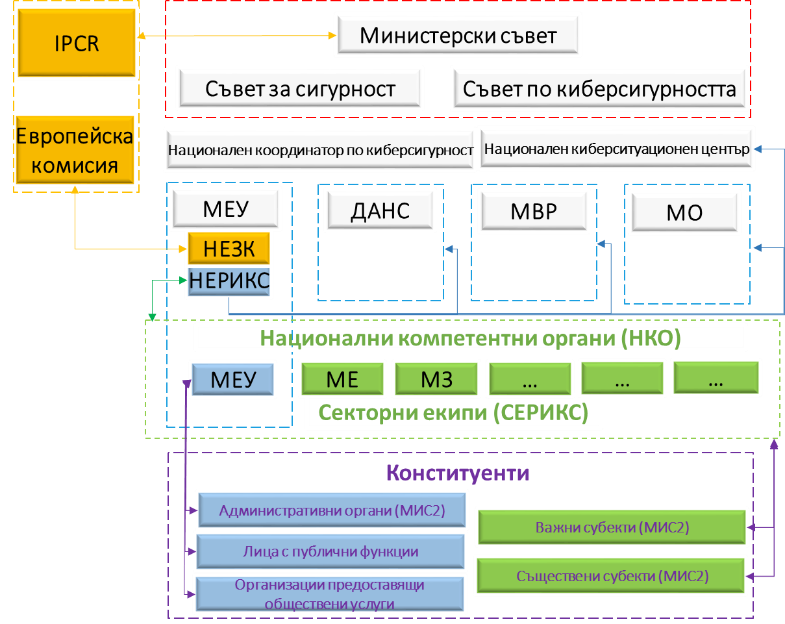
Един от механизмите за укрепване на националния капацитет в областта на киберсигурността е развитието на националната система за киберсигурност чрез реализиране на цялостен подход към технологичното осигуряване на нейните централни компоненти и защитата на споделените информационни ресурси на електронното управление.

Управлението и организацията на системата за киберсигурност се осъществяват от Министерския съвет. За подпомагане изпълнението на тези дейности към Министерския съвет е създаден Съвет по киберсигурността (Съвета), председателстван от министъра на електронното управление.

Националният координатор по кибурсигурност, определен от МС, ръководи изготвянето на Националната стратегия за киберсигурност, участва при изграждането и развитието на Националната координационно-организационна мрежа за киберсигурност (НКОМКС) и при създаването и развитието на Националния киберситуационен център (НКСЦ).

Националният киберситуационен център (НКСЦ) е част от Националния ситуационен център и има функции по събиране, анализиране и незабавното докладване на постъпила информация във връзка с предотвратяване, ограничаване и овладяване на кризи, както и за координиране на действията и комплексната реакция при заплахи за националната сигурност в резултат на кибератака.

Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи (НКО) по мрежова и информационна сигурност за секторите и услугите, обект на закона, когато такива не са създадени със специален закон. Към националните компетентни органи, включително към Министерство на електронното управление, се създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Националният екип за реагиране при инциденти с компютърната сигурност (НЕРИКС) към Министерство на електронното управление действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво.



Затова обхватът на настоящата процедура се разширява (спрямо процедури BG16RFPR002-2.009 Изграждане на елементи от система за киберзащита на споделените информационни ресурси – Етап I (CS 5) и BG16RFPR002-2.006 Изграждане на централните компоненти на национална система за киберсигурност (CS 1), прекратени във връзка със заявено желание на конкретния бенефициент – Изпълнителна агенция „Инфраструктура на електронното управление“), за да може едновременно да обхване цялостното изпълнение на действие CS1: Изграждане на национална система за киберсигурност и CS5: Изграждане на система за киберзащита на споделените информационни ресурси от ПНИИДИТ.

В предвидените дейности не е включено изграждането на платформа за симулация на комплексни дейности по кибератака и защита (Cyber Range), която е финансиранa в рамките на процедура BG16RFPR002-2.005 „Изграждане на обучителен център като елемент от националната система за киберсигурност (CS 1)“ по Приоритет 2 на ПНИИДИТ, като ще се гарантира пълна интеграция с изгражданите способности и технологична инфраструктура на националната система за кибурсигурност.

По настоящата процедура ще се надградят съществуващи и придобиването на нови централни компоненти (централни технологични решения) от цялостната екосистема на киберсигурността в Република България. Интервенциите по процедурата няма да бъдат насочени към създаването на нови организации или звена в рамките на екосистемата за киберсигурност, а **ще подкрепят технологичното развитие и оборудването на националната система за киберсигурност, което ще повиши възможностите й за даване на координиран отговор на мащабни киберинциденти** в контекста на експоненциално нарастващия брой на киберзаплахите, повишаване на тяхната комплексност и за предотвратяване на техните икономически последици.

Предвидените интервенции по настоящата процедура надграждат резултатите, постигнати при изпълнението на проект BG65ISNP001-6.007-0002 „Изграждане на елементи от национална система за киберсигурност“, финансиран по линия на Фонд „Вътрешна сигурност“. По този проект са положени основите на националната система за киберсигурност посредством изграждане на Национална координационно-организационна мрежа за киберсигурност, Национален киберситуационен център (НКСЦ), Национален център по киберпрестъпност, Национален екип за реагиране при инциденти в компютърната сигурност (НЕРИКС).

Споменатите централни компоненти представляват набор от системи, инфраструктура и технологични решения, разположени за нуждите на НЕРИКС и НКСЦ и за подобряване на защитата на всички обхванати конституенти и други заинтересовани страни. Обновяването на централните компоненти ще вземе предвид направените до момента инвестиции за най-ефикасното им надграждане.

Реализирането на предстоящата процедура допълва действие CS3 „Укрепване на капацитета на Национални компетентни органи (НКО) и секторните екипи за реагиране при инциденти с компютърната сигурност към тях (СЕРИКС)“, в рамките на което вече се извършва изграждане и укрепване на капацитета на национални компетентни органи и прилежащите им секторни екипи за постигане на високо ниво на киберсигурност в критичните сектори, като се съобразява с Директивата МИС 2. Към момента такива органи се изграждат в сектор „Здравеопазване“ и сектор „Енергетика“. Предстои изграждането и в други сектори, обхванати от директивата, след приемането на законовите изменения и във връзка с нарочни решения на Министерския съвет в изпълнение на закона.

Индиректно настоящата процедура ще се ползва от резултатите и на проект „Широкомащабно разгръщане на цифрова инфраструктура на територията на България“, финансиран по линия на Националния план за възстановяване и устойчивост, който също е в процес на изпълнение. Една от специфичните цели по проекта е насочена към надграждане на Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация и разширяване на мрежата до всички 265 общински центрове, за осигуряване на защитени киберустойчиви комуникации и „clean pipe“ Интернет (защитен от волуметрични DDoS атаки) за нуждите на държавното управление и националната сигурност. Към настоящия момент за изпълнение на проекта са проведени шест обществени поръчки (една от които с две обособени позиции), като са сключени седем договора с изпълнители. Очаква се инвестицията да бъде завършена през м. юни 2026 г.

Както беше споменато по-горе, системата за киберсигурност на Република България е част от системата за защита на националната сигурност. Управлението и организацията на системата за киберсигурност се осъществяват от Министерския съвет. За подпомагане изпълнението на тези дейности към Министерския съвет е създаден и функционира като консултативен и координиращ орган Съвет по киберсигурността (Съвета).

В изпълнение на своите функции и правомощия Съветът е провел заседания през 2025 г., в рамките на които са взети решения за адресиране на конкретни установени слабости и проблеми, както и реализиране на конкретни мерки и инициативи, свързани с цялостното изграждане на национална система за киберсигурност, отчитайки направените до момента инвестиции. Част от тези мерки и инициативи, посочени тук, попадат в обхвата на действия CS1 и CS5 към Приоритетно направление 2: Киберсигурност, Приоритет 2 на ПНИИДИТ и са обект на реализация чрез настоящата процедура, както следва:

• Надграждане на Национален екип за реагиране на инциденти с компютърната сигурност чрез осигуряване на необходимите технологични решения, необходими за всички етапи от цикъла на управление на киберинциденти – предотвратяване, установяване и разрешаване. (Мерки с очакван резултат: осигурени за НЕРИКС надградени и/или добавени централни компоненти (централни технологични решения, осигуряващи превенция, установяване и разрешаване на киберинциденти).

Към настоящия момент функциониращият НЕРИКС разполага с базова технологична обезпеченост, както и с ограничен човешки ресурс. След извършен анализ и приет от Съвета за киберсигурност доклад с предложения са идентифицирани и систематизирани всички необходими технологични решения, които да осигурят пълноценна работа на НЕРИКС. Същите попадат в обхвата на настоящата процедура и целят засилване на проактивния подход за защита на държавата, т.е. преминаване от реактивен в проактивен режим на действие – установяване на уязвимости и заплахи, идентифициране и изясняване на рисковете и тенденциите на кибератаките и др. Обхватът на технологичните решения съответства на приетата от Съвета технологична архитектура на националната система за киберсигурност. НЕРИКС ще бъде подкрепен единствено от гледна точка на осигуряване на необходимите технологични решения.

Наборът от необходимите технологични решения включва напр. системи за периметрова защита, система за филтриране на достъпи, система за разширено откриване и реакция при атаки свързани с работни станции и сървъри, система за наблюдение на инфраструктура и активна директория за промени по конфигурация и вписване, система за привилегирован достъп и мониторинг на достъпите, включително по-голяма отказоустойчивост и подобряване на методите на защита и филтриране на трафика.

• Осигуряване дейността на Националния киберситуационен център (НКСЦ), включително чрез прилагането на иновативни технологични решения и осигуряване на видимост на сигурността. (Мерки с очакван резултат: надграден и обезпечен с иновативни технологии НКСЦ, осигуряващ актуална и детайлна видимост върху киберобстановката и възможност за координирани решения при киберкриза).

Към настоящия момент НКСЦ разполага с базова технологична обезпеченост, която трябва да бъде надградена и допълнително обогатена като технологични ресурси, за по-детайлен и актуален преглед на киберобстановката в страната. Разширяването и актуализирането на ресурсите на НКСЦ ще вземе предвид направените до момента инвестиции за най-ефикасното им надграждане. Предоставяната от НКСЦ видимост на киберсигурността представлява осигуряване на ситуационна осведоменост за спецификите на киберзаплахите в държавата, като ще има възможност да се наблюдават в реално време атаки и събития във всеки един сектор в страната, както и да се извършват сравнения и корелации между атаките в различните сектори. Това ще помогне за подобряване на киберсигурността в мащаб, гарантиращ поддържане на непрекъсната киберзащита, като дава ясна представа на НКСЦ относно възможности за координирани и правилни решения в случай на киберкриза.

• Осигуряване на технологично решение за опериране на Национална мрежа на екипи, свързани със сигурността, за реализиране на работещо сътрудничество и обмен на информация между публични и частни организации. (Мерки с очакван резултат: създадена и функционираща Национална мрежа на екипи, свързани със сигурността, за реализиране на работещо сътрудничество и обмен на информация между публични и частни организации с внедрено технологично решение за ефективно сътрудничество и обмен на информаиця между публични и частни организации).

Технологичното решение за опериране на Национална мрежа на екипи, свързани със сигурността е инструмент за свързване на НЕРИКС с всички секторни екипи в административни структури / центрове за киберсигунорст в частния сектор (независимо дали са определени като СЕРИКС, SOC, CERT или CSIRT) за осигуряване на възможност за координиран отговор.

Участници в тази мрежа потенциално са всички публични и частни организации на територията на страната, които оперират такива екипи/центрове (напр. Министерство на енергетиката, Министерство на здравеопазването, A1, Европейския цифров и иновационен хъб „Тракия“ и др.). Тази дейност директно се вписва в подхода на Стратегията на ЕС за киберсигурност, в която акцентът е поставен върху осигуряване на възможност за интеграция между всички възможни организации в сферата на киберсигурността. Планираната архитектура/топология на мрежата е звездовидна и цели да подобри защитата на участниците в нея чрез почти незабавно блокиране на всяка заплаха във всяка точка на мрежата. Участниците от частния сектор ще могат да се свържат с мрежата чрез програмни интерфейси за автоматизиран обмен на информация и данни, вкл. канали за комуникация, като достъпът ще бъде свободен и безплатен за всеки участник, който желае да се присъедини.

Предоставянето на подкрепа за надграждането на съществуващи и придобиването на нови централни компоненти (централни технологични решения) от националната система за киберсигурност и повишаване на нивото на защита на конституенти ще спомогне за адресиране на идентифицирани трудности и слабости, както и на постоянно нарастващия брой и мащаб на киберзаплахите и ще допринесе за укрепването на националния капацитет в киберсигурността, както и за подобряването на мрежовата и информационна сигурност. В рамките на процедурата няма да бъдат реализирани дейности и разходи, свързани с осигуряването на необходимия за оперирането и управлението на технологичните решения човешки ресурс. Същият ще бъде осигурен извън процедурата със средства от държавния бюджет.

• Изграждане на защитено споделено информационно пространство на електронното управление (ЗСИПЕУ). (Мерки с очакван резултат: изградено защитено споделено пространство на електронното управление, гарантиращо висока сигурност надеждност на услугите и защитен отдалечен достъп до ресурсите на администрацията).

МЕУ създава и развива споделените информационни ресурси на електронното управление, които се използват споделено от всички административни органи. Същите включват техническата инфраструктура, единната електронна съобщителна мрежа, информационните центрове, защитеното споделено информационно пространство и държавния хибриден частен облак. В рамките на процедурата ще бъде финансирано изграждане на система за киберзащита на споделените информационни ресурси чрез създаване на защитено споделено информационно пространство на електронното управление - набор от мрежови и хардуерни компоненти със софтуерно определени права и условия на достъп и обмен на данни, чрез който се гарантира високо ниво на сигурност, наличност на предоставяните услуги, централизирано управление на достъпа до вътрешни и външни ресурси, осигуряващо възможност за изпълнение на служебни задължения на служители, независимо от физическото им местоположение. Това пространство ще гарантира централизирано интелигентно управление на информационни и комуникационни ресурси, като реализацията му се извършва на база изградените до момента споделени ресурси на електронното управление. Съвременните изисквания по отношение създаване на възможности за отдалечена работа поставят съществени предизвикателства пред технологичната инфраструктура и необходимост от платформи и инструменти за сътрудничество, до мрежи, които свързват служителите, изпълняващи своите функции извън физическите си работни места. Ключовото предизвикателство е свързано с осигуряването на сигурността в дигиталния свят.

Защитеното споделено информационно пространство ще поддържа по-бързо, по-надеждно, много сигурно свързване между служителите, споделените ресурси на електронното управление, приложения и други информационни ресурси, като то ще се реализира чрез набор от взаимодействащи си софтуерни и хардуерни решения.

Комбинират се функции за мрежова сигурност като Secure Web Gateways (SWG), брокери за сигурност на достъп до облак, защитна стена като услуга (FWaaS) с WAN възможности (SDWAN), за поддържане на нуждите на административните органи от динамичен защитен достъп. Тези способности трябва да бъдат предоставени „като услуга“ (as a service), с цялостни проверки на самоличност, проверки на устройства и вградени политики за съответствие, за да се гарантира, че само оторизирани потребители имат достъп до ресурси, приложения и услуги.

За да се поддържа високо ниво на киберсигурност, както и възможности за хибридна работа, административните органи се нуждаят от ясно дефиниран контрол на достъпа и политики за сигурност за всички крайни потребители. Освен това, устройствата на крайните потребител (крайни точки) трябва да бъдат идентифицирани и защитени поотделно преди да имат достъп до информационните ресурси и данни. По този начин ще се защитят устройствата, използвани за достъп до мрежата, независимо от местоположението им. За допълнително повишаване на сигурността, ще се внедрят шлюзове около мрежата на държавната администрация, което позволява потребителският трафик да бъде защитен в охранителен периметър (създава контролиран шлюз за свързване към интернет (както вход, така и изход). В допълнение към тези предимства, решението ще поддържа „разделено тунелиране“, за да се даде възможност за директно маршрутизиране на трафик за дистанционна работа.

В резултат на планираната интервенция ще се гарантира надлежно удостоверяване на достъп до системи, данни и приложения, като този подход позволява безпроблемна интеграция на множество потребителски директории и източници на данни, и многофакторни решения за удостоверяване, а резултатът е унифицирано, високоефективно решение, което изпълнява всички необходими проверки за сигурност и съответствие съгласно изискванията на нормативната уредба.

**Очаквани резултати:**

В резултат от изпълнението на предвидените мерки и инициативи по настоящата процедура се очаква да бъдат постигнати следните резултати:

• осигурени за НЕРИКС надградени и/или добавени централни компоненти (централни технологични решения), осигуряващи превенция, установяване и разрешаване на киберинциденти – не по-малко от 10 бр.;

• осигурени за използване от административните органи централни компоненти (централни технологични решения) – не по-малко от 5 бр.;

• осигурени технологични решения за актуална и детайлна видимост върху киберобстановката и възможност за координирани решения при киберкриза и за ефективно сътрудничество и обмен на информация между публични и частни организации;

• изградено защитено споделено пространство на електронното управление;

• обхванати от националната система за киберсигурност не по-малко от 50 административни органи - конституенти, включително 17 министерства (всички министерства без Министерство на вътрешните работи и Министерство на отбраната).

## 7. Индикатори (показатели):

За доказване ефективността на дейностите, включени в проектното предложение по настоящата процедура, е необходимо конкретният бенефициент да посочи обективно измерими индивидуални за процедурата индикатори за изпълнение, както следва:

**- Брой доставени и инсталирани инфраструктурни компоненти – бр.**

Показателят ще измери доставени и внедрени/инсталирани типове инфраструктурни компоненти (напр. сървъри, мрежови устройства, защитни стени) в съответния брой и вид, необходим за реализиране на цялостната визия за националната система за киберсигурност.

В раздел „Индикатори“ от Формуляра за кандидатстване (ФК) кандидатът следва да попълни данни за базова и целева стойност по горепосочения индикатор за изпълнение. Базовата стойност, която следва да бъде посочена в раздел „Индикатори“ от ФК е 0 (нула), а целевата стойност следва да бъде 5 (пет) или по-голяма.

В поле „Източник на информация“ кандидатът следва да посочи конкретните документи, които ще служат за източник на информация при отчитане и верификацията на индикатора.

**- Брой доставени и инсталирани информационни и комуникационни системи за киберсигурност – бр.**

Показателят ще измери доставени и внедрени/инсталирани типове информационни и комуникационни системи за киберсигурност от съответния вид и с обхват, необходим за реализиране на цялостната визия за националната система за киберсигурност.

В раздел „Индикатори“ от Формуляра за кандидатстване (ФК) кандидатът следва да попълни данни за базова и целева стойност по горепосочения индикатор за изпълнение. Базовата стойност, която следва да бъде посочена в раздел „Индикатори“ от ФК е 0 (нула), а целевата стойност следва да бъде 10 (десет) или по-голяма.

В поле „Източник на информация“ кандидатът следва да посочи конкретните документи, които ще служат за източник на информация при отчитане и верификацията на индикатора.

**Показатели за резултат:**

Процедурата ще допринесе за изпълнението на следните индикатори за резултат, заложени по Приоритет 2 на ПНИИДИТ 2021-2027:

SR 19 Участници в партньорската мрежа за сътрудничество в областта на киберсигурността и в обмена на информация във връзка с регистрирани заплахи и атаки

SR 20 Публични организации, обхванати от системата за киберсигурност

**ВАЖНО:** Предвид териториалния обхват на процедурата, който обхваща и двете категории региони - „В преход“ и „По-слабо развити региони“, в раздел „Индикатори“ от ФК, кандидатът следва да посочи целева стойност на показателите в проектното си предложение за двата типа региони, спазвайки следното съотношение: 1/6 от целевата стойност следва да бъде посочена за „Региони в преход“ и 5/6 за „По-слабо развити региони“. Напредъкът по показателите се отчита по категория региони в същото съотношение. Всяка стойност се закръглява до втория знак след десетичната запетая.

При неизпълнение на одобрените целеви стойности на показателите, съгласно чл. 70, ал. 1, т. 7 на Закона за управление на средствата от европейските фондове при споделено управление (ЗУСЕФСУ), финансовата подкрепа със средства от Европейските фондове при споделено управление може да бъде отменена изцяло или частично чрез извършване на финансова корекция.

## 8. Общ размер на безвъзмездната финансова помощ по процедурата и разпределение по категория региони:

Общият размер на безвъзмездната финансова помощ по процедура BG16RFPR002-2.018 „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността” е 161 861 000,00 лева ( 82 758 215,18 евро).

При изготвяне на бюджета на проектното предложение, Кандидатът следва да спазва определения бюджет за съответната категория регион, като същият не може да се надвишава.

|  |  |  |
| --- | --- | --- |
| **Общ размер на безвъзмездната финансова помощ** | **Съфинансиране от Европейския фонд за регионално развитие** | **Национално съфинансиране** |
| **161 861 000,00 лв.**  **(82 758 215,18 евро)** от които за: | **132 837 390,78 лв.**  (67 918 679,42 евро) | **29 023 609,22 лв.**  (14 839 535,76 евро) |
| По-слабо развити региони[[2]](#footnote-2)  **130 231 271,89 лв.** (66 586 191,99 евро) | **110 696 581,10 лв.**  (56 598 263,19 евро) | **19 534 690,79 лв**  (9 987 928,80 евро) |
| Региони в преход[[3]](#footnote-3) (ЮЗР)  **31 629 728,11 лв.** (16 172 023,19 евро) | **22 140 809,68 лв.**  (11 320 416,23 евро) | **9 488 918,43 лв.**  (4 851 606,96 евро) |

## 9. Минимален (ако е приложимо) и максимален размер на безвъзмездната финансова помощ за конкретен проект:

По настоящата процедура няма изискване за **минимален размер** на безвъзмездната финансова помощ.

**Максималният размер** на безвъзмездна финансова помощ е **161 861 000,00 лева (82 758 215,18 евро).**

## 10. Процент на съфинансиране:

**Интензитетът** на безвъзмездната финансова помощ по настоящата процедура е 100 %.

## 11. Допустими кандидати:

**Допустим кандидат** по процедурата, по смисъла на чл. 25, ал. 1, т. 2 от Закона за управление на средствата от европейските фондове при споделено управление (ЗУСЕФСУ) и чл. 2, т. 2 от ПМС № 23 от 13.02.2023 г. за определяне на детайлни правила за предоставяне на безвъзмездна финансова помощ по програмите, финансирани от Европейските фондове при споделено управление за програмен период 2021 – 2027 г. (ПМС № 23 от 13.02.2023 г.), е Министерството на електронното управление чрез дирекция „Мрежова и информационна сигурност“.

На седмото си официално заседание, проведено на 17 септември 2025 г., Комитетът за наблюдение на ПНИИДИТ 2021-2027 е одобрил Министерството на електронното управление чрез дирекция „Мрежова и информационна сигурност“ като конкретен бенефициент, който може да получи безвъзмездна финансова помощ по настоящата процедура за изпълнение на допустимите дейности, посочени в т.13 от Условията за кандидатстване по-долу.

Съгласно разпоредбите на Закона за киберсигурност, министърът на електронното управление провежда държавната политика в областта на мрежовата и информационната сигурност, издава методически указания и координира изпълнението на политиките за мрежова и информационна сигурност. Министерство на електронното управление е Национален компетентен орган за всички административни органи. Към Министерството на електронното управление са създадени Национално единно звено за контакт, секторен екип за реагиране при инциденти с компютърната сигурност и Национален екип за реагиране при инциденти с компютърната сигурност.

Министерството на електронното управление координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция „Национална сигурност“, Министерството на вътрешните работи и Министерството на отбраната.

Конкретният бенефициент следва да разполага с достатъчен капацитет, който да гарантира успешното изпълнение на дейностите по проекта, както следва:

**- Административен капацитет**

Екипът за организация и управление на проекта трябва да бъде съобразен със спецификата и обема на предвидените дейности, като ръководителят на проекта следва да има минимум седем (7) години опит в организацията и/или управлението/изпълнението на сходен тип дейности и/или проекти.

В раздел „Екип“ на ФК следва да се посочи информация за ръководителя на проекта – име и контакти. В поле „Квалификация и отговорности“ следва да се посочи относимостта на опита на лицето към поставените изисквания и да се опишат отговорностите му по проекта.

Към проектното предложение в раздел „Прикачени документи“ на ФК следва да се приложи и Автобиография на Ръководителя (по образеца на Приложение Е).

**- Финансов капацитет**

Конкретният бенефициент следва да разполага с финансов капацитет, който да гарантира успешното изпълнение на дейностите по проекта и следва да може да осигури необходимото финансиране за изпълнение на дейностите по проекта.

В раздел „Допълнителна информация, необходима за оценка на проектното предложение“ поле „Финансов капацитет на кандидата“ от ФК, като минимум, същият следва задължително да представи информация относно утвърдените разходи по бюджета му за текущата финансова година, както и че разполага с необходимите финансови ресурси и механизми, позволяващи да се изпълнят предложените в проектното предложение дейности и да се гарантира тяхната финансова устойчивост.

Кандидатът трябва да е директно отговорен за изпълнението на дейностите по проекта, а не да действа в качеството на посредник.

**ВАЖНО**: Конкретният бенефициент може да кандидатства с едно проектно предложение.

## 12. Допустими партньори (ако е приложимо):

Конкретният бенефициент изпълнява проекта по настоящата процедура за директно предоставяне на безвъзмездна финансова помощ самостоятелно, без участието на партньори.

## 13. Дейности, допустими за финансиране:

Проектното предложение и включените в него дейности следва да съответстват на принципа за ефективност и ефикасност и да водят до постигане на целта на процедурата при най-адекватно съотношение между очакваните разходи и ползи.

Допустимите дейности трябва да са в съответствие с принципа за „ненанасяне на значителни вреди“ и с принципите за равнопоставеност на жените и мъжете и осигуряване на равни възможности за всички, което се описва в раздел „Допълнителна информация необходима за оценка на проектното предложение“ на ФК.

Допустими за финансиране по настоящата процедура са дейности, които допринасят за изпълнение на целта на процедурата, посочена в т. 6 от тези Условия за кандидатстване и водят до резултати, чрез които се постига целевата стойност на индикаторите по процедурата, включително:

1.Повишаване на капацитета на НЕРИКС и НКСЦ чрез технологични и организационни мерки чрез надграждане на съществуващи и придобиване на нови централни компоненти (централни технологични решения) от цялостната екосистема на киберсигурността в Република България.

2.Осигуряване и имплементиране на технологични решения за изграждане на ЗСИПЕУ. 3.Имплементиране на технологични решения за повишаване на нивото на защита от кибер заплахи на конституенти - административни органи.

4.Интегриране на системи и ресурси на конституенти към Националната система за киберсигурност, включително интеграции от типа НЕРИКС-СЕРИКС, интеграция с НКСЦ и др.

5.Надграждане на технологичните ресурси за увеличаване на обхвата и обема на споделената и обменената информация между всички заинтересовани страни.

**ВАЖНО:** При разработване на проектното предложение кандидатът може да обединява, разделя и конкретизира горепосочените дейности в зависимост от спецификата на проекта.

**ВАЖНО:** Конкретният бенефициент е пряко отговорен за управлението на проекта и осигуряването на качественото изпълнение на заложените дейности, като следва да сформира екип, отговорен за организацията и управлението на проекта с ясно описано разпределение на отговорностите и функциите между отделните членове.

Всяка дейност следва да бъде детайлно описана във ФК, раздел „План за изпълнение / Дейности по проекта“. В поле „Описание“ се посочват основанията за избор на дейността. В поле „Начин на изпълнение“ се посочват методите за изпълнение на дейността, включително възлагането й на външен изпълнител, методите за осъществяване на вътрешен мониторинг и по какъв начин ще бъде осигурена устойчивостта на резултатите от изпълнението й. В поле „Резултат“ се описват конкретните очаквани резултати от изпълнението на дейността и връзката им с индикаторите.

Процедурите за избор на изпълнител следва да бъдат описани в раздел „План за външно възлагане“ на Формуляра за кандидатстване.

**ВАЖНО:** Конкретният бенефициент няма право да подава проектно предложение за дейности вече финансирани по друг проект, програма или каквато и да е друга финансова схема, произлизаща от националния бюджет, бюджета на Общността или друга донорска програма.

**ВАЖНО:** Дейности, свързани с организацията и управлението на проекта и с осигуряването на видимост, прозрачност и комуникация, не следва да бъдат описвани като отделна дейност в раздел „План за изпълнение / Дейности по проекта“ нито в друг раздел на ФК.

**ВАЖНО:** В случай че преди подаването на проектното предложение кандидатът/партньорът е започнал изпълнение на дейности, съществени за постигането на резултатите по проекта, в раздел „Допълнителна информация необходима за оценката на проектното предложение“ от ФК следва да се опише на какъв етап е тяхното изпълнение и кога е стартирала съответната дейност в поле „Начална и крайна дата на изпълнение на проекта“ и с какво допринасят за успешното постигане на целевите стойности на индикаторите по процедурата. Следва да се има предвид, че дейностите по проектното предложение не трябва да са физически завършени или изцяло осъществени преди подаването на Формуляра за кандидатстване, независимо дали всички свързани плащания са извършени.

**За да бъдат допустими дейностите, трябва да отговарят на следните условия:**

- да са в съответствие и да не противоречат на разпоредбите на Регламент (ЕС) 2021/1060, вкл. да са в съответствие с хоризонталните принципи, съгласно чл. 9 от Регламент (ЕС) 2021/1060;

- да съответстват на предвиденото в ПНИИДИТ, да гарантират постигането на целта на настоящата процедура и да осигуряват ефективен принос за постигането на целите на Програмата;

- да са извършени от допустимия конкретен бенефициент;

- да съответстват на изискванията на европейското и националното законодателство в сферата на обществените поръчки при спазване на принципите на прозрачност, пропорционалност, равно третиране и недискриминация при осигурена конкуренция на най-широка основа;

- да се реализират в рамките на наличния бюджет и да имат ясни и реалистични количествени резултати;

- да бъдат ясно обосновани и да имат конкретни цели;

- да не са започнали и/или физически завършени или изцяло осъществени преди подаването на формуляра за кандидатстване от бенефициента.

- да са в съответствие с политиката на Съюза в областта на околната среда, съгласно член 11 и член 191, параграф 1 от ДФЕС, като се отчитат целите на ООН за устойчиво развитие, Парижкото споразумение и условията по Регламент (ЕС) 2020/852, свързани със зачитането на принципа за „ненанасяне на значителни вреди”, така че да не се засяга в значителна степен постигането както на екологичната, така и на социалната цел.

## 14. Категории разходи, допустими за финансиране:

Без да противоречи на разпоредбите и правилата, описани в Регламент (ЕС) 2021/1060, ЗУСЕФСУ, ПМС №86/2023 за определяне на национални правила за допустимост на разходите по програмите, финансирани от Европейските фондове при споделено управление, за програмен период 2021 – 2027 г., НАРЕДБА № Н-5 от 29.12.2022 г. за определяне на правилата за извършване на плащания, за верификация и счетоводно отчитане на разходите, за възстановяване и отписване на неправомерни разходи и за осчетоводяване, както и сроковете и правилата за приключване на счетоводната година по програмите, съответната подзаконова нормативна уредба, уреждаща национални правила за допустимост на разходите за средствата от Европейските фондове за споделено управление, приложимото право на Европейския съюз и българското законодателство и за да бъдат признати за допустими по проекта, разходите трябва да отговарят и на изискванията, предвидени в настоящите Условия за кандидатстване.

**ВАЖНО:** При попълване на раздел „Бюджет“ от ФК кандидатът следва да заложи преките разходи, съответстващи и обвързани с конкретните дейности по проекта, като преките разходи трябва да бъдат обособени по категорията регион на планиране - По-слабо развити региони и Регион в преход (ЮЗР) – както и по области на интервенция – код 017. ИКТ решения на държавното управление, електронни услуги, приложения, отговарящи на критериите за намаляване на емисиите на парникови газове или за енергийна ефективност и код 037. ИКТ: Други видове ИКТ инфраструктура (включително мащабни компютърни ресурси и оборудване, центрове за данни, датчици и друго безжично оборудване).

В тази връзка, при попълване на раздел „Бюджет“ от ФК кандидатът следва да спазва следните съотношения:

**Категории региони** - По-слабо развити региони: **80.46%** и Регион в преход (ЮЗР): **19.54%.**

**Области на интервенция:** код 017. ИКТ решения на държавното управление, електронни услуги, приложения, отговарящи на критериите за намаляване на емисиите на парникови газове или за енергийна ефективност: **50%** и код 037. ИКТ: Други видове ИКТ инфраструктура (включително мащабни компютърни ресурси и оборудване, центрове за данни, датчици и друго безжично оборудване**): 50%.**

Непреките разходи за организация и управление на проекта, посочени в т.14.2 от Условията за кандидатстване, не следва да се обвързват с конкретни дейности по проекта, но трябва да се обособяват по категорията регион на планиране и по области на интервенции при спазване на горепосочените съотношения.

*Непреките разходи за организация и управление на проекта се предоставят под формата на финансиране с единна ставка, която се определя чрез прилагане на до 3 % към допустимите преки разходи по проекта в съответствие с чл. 54, буква а) от Регламент (ЕС) 2021/1060. При подготовката на проектното предложение кандидатът определя конкретна сума за непреки разходи по проекта в границите на ставка до 3 % от преките разходи и я попълва в раздел „Бюджет“ от Формуляра за кандидатстване.*

**ВАЖНО:** По време на оценката на проектното предложение е възможно да бъдат установени обстоятелства, които да налагат промяна в бюджета (раздел „Бюджет“ от Формуляра за кандидатстване). Възможните изменения на бюджета не могат да доведат до увеличаване на сумата на исканата безвъзмездна помощ по настоящата процедура над максималния размер на БФП спрямо точка 9 по-горе.

Междинното звено може да извърши корекции в раздел „Бюджет“ от Формуляра за кандидатстване във връзка с установени в процеса на оценката недопустими и/или необосновани разходи и/или на конкретния бенефициент се предоставят указания и срок за отстраняване на установените нередовности, непълноти и/или несъответствия.

## 14.1. Условия за допустимост на разходите

Съгласно чл. 57, ал. 1 на ЗУСЕФСУ разходите се считат за допустими, ако са налице едновременно следните условия:

- разходите са за дейности, съответстващи на предвидените в одобрения проект и се извършват от допустими бенефициенти съгласно съответната програма;

- разходите попадат във включени в документите по чл. 26, ал. 1 на ЗУСЕФСУ и в одобрения проект категории разходи;

- разходите не надхвърлят праговете за съответната категория в документите по чл. 26, ал. 1 на ЗУСЕФСУ и в одобрения проект;

- разходите са за реално доставени продукти, извършени услуги, и положен труд;

- разходите са извършени законосъобразно съгласно приложимото право на Европейския съюз и българското законодателство;

- разходите са отразени в счетоводната документация на бенефициента чрез отделни счетоводни аналитични сметки или в отделна счетоводна система;

- за направените разходи е налична одитна следа съгласно минималните изисквания на Приложение XIII от Регламент (ЕС) 2021/1060 и са спазени изискванията за съхраняване на документите съгласно чл. 82 от Регламент (ЕС) 2021/1060;

- разходите са съобразени с приложимите правила за предоставяне на държавни помощи.

За целите на настоящата процедура допустими са разходите по процедурата, които отговарят на следните условия:

1. Да са необходими за изпълнението на проекта и да отговарят на принципите за добро финансово управление - икономичност, ефикасност и ефективност на вложените средства.

Съгласно чл. 33 на 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:

- принципът на икономичност изисква ресурсите за осъществяване на дейностите да бъдат осигурени своевременно, в подходящо количество и качество и при най-добра цена;

- принципът на ефикасност се отнася до най-доброто съотношение между използваните ресурси, предприетите дейности и постигането на целите;

- принципът на ефективност се отнася до степента, в която се постигат поставените цели посредством предприетите дейности.

Съгласно съображение 12 от преамбюла на Регламент (ЕС) 2021/1060 когато изпълняват фондовете при споделено управление, Комисията и държавите членки следва да зачитат посочените във Финансовия регламент принципи, като добро финансово управление, прозрачност и недискриминация.

С оглед определяне на съответствието на предвидените разходи с горепосочените принципи и реалистичността им, за всички доставки и услуги, които се възлагат по реда на Закона за обществени поръчки (ЗОП) конкретният бенефициент следва да представи една оферта за всяка отделна инвестиция в ДМА и/или ДНА и/или услуга с предложена цена, получена чрез един от следните способи:

1) проведени пазарни консултации съгласно чл. 21, ал. 2 от ЗОП;

или

2) други подходящи източници на информация, ако не са проведени пазарни консултации, както следва:

• изпратени/публикувани запитвания и минимум 1 брой индикативна оферта, получена не по-рано от 12 месеца преди датата на кандидатстване, или

• (приложимо само за административните органи, посочени в Решение на Министерския съвет № 727/ 05.12.2019 г.) индикативна оферта, представена от системния интегратор, съгл. § 45 (1) (Доп. - ДВ, бр. 102 от 2019 г. в сила от 29.11.2019 г.) от Преходните и заключителни разпоредби към Закона за електронното управление.

Конкретният бенефициент задължително прилага документ/и, съдържащ/и минимални изисквания/технически и/или функционални характеристики за всяка отделна услуга/актив.

В случаите, когато и след допълнително изискване от страна на оценителната комисия, не са посочени минимални технически и/или функционални характеристики на даден актив, заложен в бюджета на проекта, Оценителната комисия ще премахне разходите за съответния/те актив/и от бюджета на проекта.

Бенефициентът следва да представи информация за планираната/ите обществена/и поръчка/и в съответната дейност в раздел „План за изпълнение/Дейности по проекта“, раздел „Бюджет (в лева)“ и раздел „План за външно възлагане“ от ФК. От представената от бенефициента информация за обществената поръчка/поръчки, която/които се планира/т да се проведе/ат, следва да е ясен обектът на всяка обществена поръчка; редът, по който ще се възлага; предметът на обществената поръчка; мерна единица (количество, брой и т.н), единични цени, обща стойност на поръчката и друга приложима информация.

2. Да бъдат извършени след датата на решение на Комитета за наблюдение на ПНИИДИТ за одобряване на методологията и критериите за подбор на настоящата операция (17 септември 2025 г.) и до изтичане на крайния срок, определен за представяне на окончателния отчет за изпълнение на дейностите по проекта. В случай че изпълнението на проекта е започнало преди подаването на проектното предложение (видно от датата, посочена от кандидата в поле „Начална и крайна дата на изпълнение на проекта“ на раздел „Допълнителна информация необходима за оценка на проектното предложение.“), по отношение на всички извършени дейности и разходи по проекта следва да са спазени всички изисквания на приложимото законодателство.

Разходооправдателните документи, свързани с изпълнението на допустимите по проекта дейности, следва да бъдат издадени в периода на допустимост на разходите, посочен по-горе. Плащанията могат да бъдат извършени и след края на изпълнение на дейностите по проекта, но не по-късно от крайния срок, определен за представяне на окончателния отчет.

3. За разходите да е налична адекватна одитна следа съгласно минималните изисквания на Приложение XIII от Регламент (ЕС) 2021/1060 в съответствие с чл. 57, ал. 1, т. 7 от ЗУСЕФСУ, включително да са спазени изискванията за съхраняване на документите по чл. 82 от Регламент (ЕС) 2021/1060.

4. Да са действително платени (т.е. да е платена цялата стойност на представените фактури или други първични счетоводни документи, включително стойността на ДДС), в срока на допустимост.

5. Да са отразени в счетоводната документация на бенефициента чрез отделни счетоводни аналитични сметки по проекта или в отделна счетоводна система в съответствие с чл. 57, ал. 1, т. 6 на ЗУСЕФСУ.

6. Да могат да се установят и проверят, да бъдат подкрепени от оригинални разходо-оправдателни документи.

7. Да са за реално доставени продукти/извършени услуги въз основа на договори, които са сключени при спазване изискванията на националното и европейското законодателство за възлагане на обществени поръчки.

8. Да са в изпълнение на посочените в т. 13 от настоящите Условия за кандидатстване допустими дейности.

9. Да не са финансирани по друг проект, програма или друга финансова схема, финансирана от публични средства на националния или европейския бюджети.

**ВАЖНО:** Относно третирането на ДДС конкретният бенефициент следва да се запознае с Указание НФ-1 от 09.01.2024 г. за третиране на данък върху добавената стойност като допустим разход при изпълнение на проекти по програмите, финансирани от Европейския фонд за регионално развитие (ЕФРР), Европейския социален фонд плюс (ЕСФ+), Кохезионния фонд (КФ), Фонда за справедлив преход (ФСП) и Европейския фонд за морско дело, рибарство и аквакултури (ЕФМДРА), Фонд "Убежище, миграция и интеграция" (ФУМИ), Фонд "Вътрешна сигурност" (ФВС), програмата по Инструмента за финансова подкрепа за управлението на границите и визовата политика (ИУГВП), както и на средствата за финансиране на подхода "Водено от общностите местно развитие" от Европейския земеделски фонд за развитие на селските райони (ВОМР) на ЕС, за програмен период 2021 – 2027 г. (Приложение Г).

## 14.2. Допустими разходи

**ВАЖНО:** При попълване на раздел „Бюджет“ от Формуляра за кандидатстване при въвеждане от страна на кандидата на разходите от трето ниво, чрез натискане на бутон „Детайли“ за всеки бюджетен ред трябва да се попълни информация от падащите менюта, Категория/ региони“.

**Допустимите по настоящата процедура са следните видове разходи:**

I РАЗХОДИ ЗА ДЪЛГОТРАЙНИ МАТЕРИАЛНИ АКТИВИ (преки разходи)

I.1. Разходи за доставка на оборудване (материални активи).

II. РАЗХОДИ ЗА ДЪЛГОТРАЙНИ НЕМАТЕРИАЛНИ АКТИВИ (преки разходи)

II.2. Разходи за доставка/разработване на софтуер и лицензи (нематериални активи).

III.РАЗХОДИ ЗА УСЛУГИ (преки разходи)

III.3. Разходи за услуги.

IV. НЕПРЕКИ РАЗХОДИ

IV.4. Непреки разходи за организация и управление (разходи, които са свързани с изпълнението на проекта, не допринасят пряко за постигането на неговите цели и резултати, но са необходими за неговото цялостно администриране, управление, оценка и добро финансово изпълнение, както и разходите за видимост, прозрачност и комуникация), съгласно чл. 53, параграф 1, буква г) на Регламент 2021/1060.

Екипът за управление на проекта следва да бъде съобразен със спецификата и обема на предвидените в проекта дейности.

В рамките на проекта задължително се изпълняват дейности за видимост, прозрачност и комуникация. Тези дейности трябва да отговарят на условията и изискванията, описани в Наръчник за визуализация на подкрепата от ЕС 2021-2027 (Брандбук за бенефициенти), който може да бъде намерен на интернет страницата на ПНИИДИТ на адрес: <https://pniidit.egov.bg/wps/portal/program-niidit/for.beneficiaries/visibility-and-transparency-requirements/beneficiary.handbook>.

Непреките разходи, свързани с организацията и управлението на проекта, вкл. с осигуряване на видимост, прозрачност и комуникация, следва да бъдат заложени на един бюджетен ред, като за тях не следва да бъде представяна обосновка.

ВАЖНО:Непреките разходи се предоставят под формата на финансиране с единна ставка, определена в размер на до 3 % от преките допустими разходи по проекта съгласно чл. 54, т. а) от Регламент (ЕС) 2021/1060.

**ВАЖНО:** Съгласно чл. 7в, ал. 2, т. 10 от Закона за електронното управление /ЗЕУ/ министърът на електронното управление утвърждава проектни предложения и дейности, както и изменения на проекти и дейности, координира и контролира изпълнението на проектите за електронно управление, информационни и комуникационни технологии на административните органи, финансирани със средства от държавния бюджет, от структурните и инвестиционните фондове на Европейския съюз и от други източници.

При кандидатстване кандидатът следва да представи писмо за утвърждаване на проектното предложение от Министъра на електронното управление съгласно чл. 7в, ал. 2, т. 10 от ЗЕУ.

Правилата в тази връзка са публикувани на адрес: <https://egov.government.bg/wps/portal/ministry-meu/home/budget-project-control/approval-project-proposals>

## 14.3. Недопустими разходи

Независимо от гореизброените условия за допустимост на разходите, за недопустими ще се считат всички разходи, които са в противоречие с правилата на Европейските фондове за споделено управление (Регламент (ЕС) 2021/1060, Регламент (ЕС) 2021/1058, ЗУСЕФСУ и съответната поднормативна уредба, уреждаща национални правила за допустимост на разходите за средствата от ЕФСУ).

Междинното звено може както да извърши корекции в раздел „Бюджет“ от ФК във връзка с установени в процеса на оценката недопустими и/или необосновани разходи и/или на конкретния бенефициент се предоставят указания и срок за отстраняване на установените нередовности, непълноти и/или несъответствия.

## 15. Допустими целеви групи (ако е приложимо):

Неприложимо.

## 16. Приложим режим на минимални/държавни помощи (ако е приложимо):

Съгласно чл. 107, § 1 от Договора за функциониране на Европейския съюз (ДФЕС) „всяка помощ, предоставена от държава-членка или чрез ресурси на държава-членка, под каквато и да било форма, която нарушава или заплашва да наруши конкуренцията чрез поставяне в по-благоприятно положение на определени предприятия или производството на някои стоки, доколкото засяга търговията между държавите-членки, е несъвместима с вътрешния пазар“.

Според постоянната съдебна практика на Съда на ЕС „Предприятие“ се определя като субект, предоставящ стоки и услуги на пазара, независимо от правния си статут и начина на финансиране.

„Предприятие“ по смисъла на чл.20, ал.2 от Закона за държавните помощи е всяко лице, което осъществява икономическа дейност без значение на неговата правноорганизационна форма, статут и начин на финансиране, независимост от това дали същото формира и разпределя печалба.

По настоящата процедура за безвъзмездна финансова помощ чрез директно предоставяне на конкретен бенефициент е допустимо да кандидатства единствено Министерството на електронното управление чрез дирекция „Мрежова и информационна сигурност“, която е структура в администрацията на изпълнителната власт и изпълнява публични функции по силата на нормативен акт.

Съгласно т. 17 от Известието на Комисията относно понятието за държавна помощ, посочено в член 107, параграф 1 от Договора за функционирането на Европейския съюз „дейностите, които по същество са част от прерогативите на официалната власт и се извършват от държавата, не представляват стопански дейности“. В тази връзка, предвид факта че процедурата укрепва капацитета на кандидата да изпълнява изцяло и само публични функции възложени му по силата на нормативен/ни акт/ове, конкретният бенефициент не следва да бъде разглеждан като предприятие, извършващо икономическа дейност. Предвид това, подпомагането не следва да се разглежда като попадащо в обхвата на чл. 107, § 1 от ДФЕС.

При закупуване на активи и възлагане на дейности/услуги от/на външни изпълнители, бенефициентът следва да прилага ЗОП и Правилника за прилагане на ЗОП по открит, прозрачен, в достатъчна степен публичен, недискриминационен и безусловен начин по смисъла на т.89-96 от Известие на комисията относно понятието за държавна помощ, посочено в чл.107, пар.1 от ДФЕС. В този смисъл, на ниво изпълнители, подпомагането също не следва да се счита за държавна помощ.

## 17. Хоризонтални политики:

Кандидатът следва да посочи в своето проектно предложение, че при изпълнение на проекта конкретният бенефициент се задължава да спазва чл. 9 от Регламент (ЕС) 2021/1060 относно следните хоризонтални принципи:

- гарантиране зачитането на основните права и спазването на Хартата на основните права на Европейския съюз.

- гарантиране равенството между мъжете и жените, интегрирането на принципа на равенство между половете и отчитането на социалните аспекти на пола.

- предотвратяване на всякаква дискриминация, основана на пол, расов или етнически произход, религия или вероизповедание, увреждане, възраст или сексуална ориентация, както и достъпност за хората с увреждания.

- насърчаване на устойчивото развитие, съгласно член 11 от ДФЕС, като се отчитат целите на ООН за устойчиво развитие, Парижкото споразумение и принципът за ненанасяне на значителни вреди.

Кандидатът ще гарантира и съблюдаване на принципите, заложени в Хартата на основните права на ЕС и Конвенцията на ООН за правата на хората с увреждания (КПХУ) съгласно Насоките за прилагането им, които са изготвени за периода 2021-2027.

Кандидатът посочва в проектното предложение (в раздел „Допълнителна информация необходима за оценка на проектното предложение“, поле „Принос на проектното предложение за реализиране на хоризонталните принципи“), че предложените дейности съответстват и допринасят за реализиране на хоризонталните политики.

Целите на фондовете се преследват при пълно зачитане на достиженията на правото на Съюза в областта на околната среда.

## 18. Минимален и максимален срок за изпълнение на проекта (ако е приложимо):

Продължителността на изпълнение на проекта не следва да е по-малко от 12 месеца и да надвишава **36 (тридесет и шест) месеца**, считано от датата, посочена от кандидата в поле „Начална и крайна дата на изпълнение на проекта“ на раздел „Допълнителна информация необходима за оценка на проектното предложение.“

Началната дата на проекта следва да бъде след датата на решението на Комитета за наблюдение на ПНИИДИТ за одобряване на методологията и критериите за подбор на настоящата операция (17 септември 2025 г.).

Крайната дата на проекта следва да бъде не по-късно от 30.06.2029 г.

## 19. Ред за оценяване на концепциите за проектни предложения (ако е приложимо)

Не е приложимо.

## 20. Критерии и методика за оценка на концепциите за проектни предложения (ако е приложимо)

Не е приложимо.

## 21. Ред за оценяване на проектните предложения:

Оценката на всяко от проектните предложения по процедурата се извършва от Комисия за оценка, определена със заповед на Овластеното от Ръководителя на Управляващия орган (РУО) лице съгласно Заповед № РД 14-221/06.06.2024г. Всяко проектно предложение се оценява за съответствие с предварително одобрените от Комитета за наблюдение на ПНИИДИТ, Методология и критерии за подбор на операции по процедурата, посочени в т. 22 „Критерии и методика за оценка на проектните предложения“ **и Приложение В „Критерии и методика за оценка“** от Условията за кандидатстване. Оценителната комисия изготвя доклад, който се предоставя на Овластеното от Ръководителя на Управляващия орган (РУО) за одобрение. Не се допуска въвеждането на допълнителни критерии за оценка или изменение на критериите по време на провеждането на процедурата по оценка на проектното предложение.

В случаи на установени в процеса на оценката нередовности, непълноти и/или несъответствия на проектното предложение, Междинното звено изпраща на конкретния бенефициент уведомление за тях, като определя срок за отстраняването им, който не може да бъде по-кратък от една седмица. Искането за предоставяне на информация/документи се изпраща чрез модул „Е-кандидатстване“ на ИСУН, за което конкретният бенефициент получава съобщение на електронния адрес, посочен при регистрацията на потребителя, подал проектното предложение. Предвид това, промени в профила на конкретния бенефициент в ИСУН са невъзможни. Допуснатите от конкретния бенефициент нередовности, непълноти и/или несъответствия могат да доведат до препоръки от страна на Междинното звено за отстраняване на установените нередовности, непълноти и/или несъответствия с оглед постигане на съответствие с критериите за оценка.

В уведомлението задължително се съдържа информация, че неотстраняването на установените нередовности може да доведе до прекратяване на производството по отношение на конкретния бенефициент. Срокът за оценка на проектното предложение спира да тече до датата на отстраняването им. В случай че конкретният бенефициент не отстрани в срок нередовност, непълнота и/или несъответствие с изискванията, процедурата може да бъде прекратена.

При наличие на положителен резултат от оценяването Овластеното от РУО лице в едноседмичен срок от приключване на оценяването взема решение за предоставяне на безвъзмездна финансова помощ за одобреното проектно предложение. Решението на Овластеното от РУО лице се обективира в административен договор с конкретния бенефициент за предоставяне на БФП. Одобреният проект и документите по чл. 26, ал. 1 от ЗУСЕФСУ в частта, определяща условията за изпълнение, са неразделна част от договора.

Подробно описание на техническия процес, свързан с електронното кандидатстване и представянето на допълнителна информация/документи, е посочено в Ръководството за потребителя за модул „Е-кандидатстване“ в ИСУН (Приложение Д „Ръководство за потребителя за модул „Е-кандидатстване“ към Условията за кандидатстване), както и във видео материалите и ръководствата, налични на следния адрес:

<https://eumis2020.government.bg/bg/s/Default/Manual>

## 22. Критерии и методика за оценка на проектните предложения:

Оценката се извършва въз основа на критериите, подробно описани в **Приложение В** „Критерии и методика за оценка“към Условията за кандидатстване. Критериите и методиката за оценка не подлежат на изменение по време на провеждането на оценката.

## 23. Начин на подаване на проектните предложения/концепциите за проектни предложения:

Подаването на Формуляра за кандидатстване се извършва изцяло по електронен път чрез попълване на уеб базиран формуляр за кандидатстване и подаване на формуляра и придружителните документи чрез **Информационната система за управление и наблюдение на средствата на ЕС в България (ИСУН)** единствено с използването на **Квалифициран електронен подпис** (КЕП), чрез модула „Е-кандидатстване“ на следния интернет адрес: [**https://eumis2020.government.bg**](https://eumis2020.government.bg)**.**

Подготовката и подаването на проектното предложение в ИСУН се извършва съгласно Приложение Д „Ръководство за потребителя за модул „Е-кандидатстване“.

**Проектното предложение се подава електронно чрез ИСУН, като се подписва с валиден КЕП от законния представител на кандидата или оправомощено за целите на подаването на проектното предложение лице.**

Проектното предложение да се подава от профила на конкретния бенефициент, тъй като впоследствие именно този профил ще бъде използван за комуникация с Междинното звено и за отстраняване на установените нередовности по време на оценката на проектното предложение. По време на оценката, комуникацията с конкретния бенефициент и отстраняването на нередовностите по подаденото проектно предложение ще се извършват електронно чрез профила на конкретния бенефициент в ИСУН, от който е подаден проектът и промени на посочения профил (вкл. промяна на имейл адреса, асоцииран към съответния профил) са недопустими.

Всички документи се представят на български език без корекции. Документ, чийто оригинал е на чужд език, се представя и в превод на български език.

Документите към Формуляра за кандидатстване, посочени в т. 24 отУсловията за кандидатстване, се подават изцяло електронно. Документите се описват в раздел „Прикачени електронно подписани документи“ от ФК преди подаването му.

След обявяването на процедурата, Междинното звено изпраща **покана** до конкретния бенефициент, посочен в т. 11 от настоящите Условия за кандидатстване, с което го информира за възможностите за кандидатстване.

## 24. Списък на документите, които се подават на етап кандидатстване:

Конкретният бенефициент следва да представи следните документи, по изцяло електронен път чрез ИСУН:

1)Декларация, че е запознат с условията за кандидатстване и условията за изпълнение – по образец **(Приложение А)** към Условията за кандидатстване.

2)Декларация относно статута по ЗДДС – по образец **(Приложение Б)** към Условията за кандидатстване.

*Декларациите по точки 1) и 2) се подават чрез попълване на раздел „E-ДЕКЛАРАЦИИ“ на ФК, в случай че ФК е подписан с валиден КЕП от законния представител на кандидата. В случай че ФК е подписан от оправомощено за целите на подаването на проектното предложение лице, декларациите по точки 1) и 2) се подписват с валиден КЕП от законния представител на кандидата и се прикачват в ИСУН в Раздел „Прикачени документи“ към ФК. Законният представител на конкретния бенефициент на БФП няма право да оправомощава други лица да подписват декларациите по точки 1) и 2), тъй като с тях се декларират данни в лично качество или съответно данни за представлявания от него орган, като за верността им се носи наказателна отговорност, която също е лична.*

3) **Документ за оправомощаване на лице, което да представлява конкретния бенефициент** и да подписва всички документи, свързани с подаването, оценката на подаденото проектно предложение (включително комуникация с оценителната комисия), предоставянето на документи, необходими за подписване на административния договор за предоставяне на БФП или заповед и изпълнението на проекта (ако е приложимо). Прилага се, в случай че проектното предложение е подадено от лице, различно от законния представител на кандидата.

Документът за оправомощаване следва да бъде подписан с валиден КЕП от законния представител на кандидата.

4). Индикативни оферти и минимални изисквания/технически и/или функционални характеристики за всички планирани активи/услуги. *Документите се прикачват в Раздел „Прикачени документи“ на ФК.* *Документи, които са на хартиен носител първо се сканират, след което се прикачват в Раздел „Прикачени документи“ на ФК.*

5) **Приложение Е** Автобиография на Ръководителя на проекта (по образец) .

6) Писмо за утвърждаване на проектното предложение от Министъра на електронното управление съгласно чл. 7в, ал. 2, т. 10 от ЗЕУ.

**ВАЖНО**: Формулярът за кандидатстване се подписва с валиден КЕП от законния представител на кандидата или оправомощено за целите на подаването на проектното предложение лице.

**ВАЖНО**: Кандидатът следва да се увери, че всички документи са представени в изискуемата форма съгласно изискванията на настоящите Условия за кандидатстване.

Достоверността на документите, приложения към ФК се удостоверява чрез подписването на ФК с КЕП посредством ИСУН.

## 25. Краен срок за подаване на проектните предложения:

Ще се прилага процедура чрез директно предоставяне с **един краен срок за кандидатстване – 16:30 часа на 05 декември 2025 г.**

По настоящата процедура чрез директно предоставяне на безвъзмездна финансова помощ конкретният бенефициент може да поиска разяснения по документите ***в срок до три седмици*** ***преди изтичането на срока за кандидатстване***. Разясненията се утвърждават от Овластеното от РУО лице. Разяснения се дават по отношение на условията за кандидатстване, не съдържат становище относно качеството на проектното предложение и са задължителни. Разясненията се съобщават по реда на чл. 26, ал. 8-9 от ЗУСЕФСУ, като се публикуват в ИСУН и на интернет страницата на програмата и/или в Единния информационен портал.

## 26. Допълнителна информация

Решение за предоставяне на безвъзмездна финансова помощ и сключване на Административен договор за предоставяне на безвъзмездна финансова помощ.

**При наличие на положителен резултат от оценяването Овластеното от РУО лице в едноседмичен срок от приключване на оценяването взема решение за предоставяне на безвъзмездна финансова помощ за одобреното проектно предложение.** **Решението на Овластеното от РУО лице се обективира в Административен договор за директно предоставяне на безвъзмездна финансова помощ с конкретния бенефициент. Одобреният проект и документите по чл. 26, ал. 1 от ЗУСЕФСУ в частта, определяща условията за изпълнение, са неразделна част от договора.**

При одобрен оценителен доклад конкретният бенефициент се поканва да предостави:

1. Заявление за профил за достъп на ръководител на бенефициента до ИСУН (**Приложение VII** към АДБФП) и/или Заявление за профил за достъп на оправомощени от бенефициента лица до ИСУН (**Приложение VIII** към АДБФП);
2. Декларация за запознаване с определението за нередност и измама (**Приложение VI** към АДБФП);.
3. Декларация за липса на конфликт на интереси (**Приложение V** към АДБФП);
4. Декларация от бенефициента за съгласие за предоставяне на информация от компетентния орган по приходите (**Приложение III** към АДБФП); Заповед за оправомощаване на лице, което да представлява конкретния бенефициент при подписване на АДБФП (ако е приложимо).

Документите по точки 1-4 следва да бъдат подписани с валиден КЕП от законния представител на конкретния бенефициент, като е препоръчително подписването да е чрез attached signature – файл и подпис в един документ (подписът да се съдържа в документа).

Решение за прекратяване на процедурата чрез директно предоставяне може да се вземе при следните случаи:

- когато няма постъпило проектно предложение, в случай че е определен краен срок за подаване или когато всички подадени проектни предложения са оттеглени;

- при спиране на финансирането по съответната програма или на част от нея;

- в случай че конкретният бенефициент не отстрани в срок нередовност/и, непълнота/и и/или несъответствие/я с изискванията.

## 27. Приложения към Условията за кандидатстване:

**Приложение А** Декларация, че кандидатът е запознат с условията за кандидатстване и условията за изпълнение.

**Приложение Б** Декларация относно статута по ЗДДС.

**Приложение В** Критерии и методика за оценка.

**Приложение Г** Указание НФ-1 от 09.01.2024 г. за третиране на данък върху добавената стойност като допустим разход при изпълнение на проекти по програмите, финансирани от Европейския фонд за регионално развитие (ЕФРР), Европейския социален фонд плюс (ЕСФ+), Кохезионния фонд (КФ), Фонда за справедлив преход (ФСП) и Европейския фонд за морско дело, рибарство и аквакултури (ЕФМДРА), Фонд "Убежище, миграция и интеграция" (ФУМИ), Фонд "Вътрешна сигурност" (ФВС), програмата по Инструмента за финансова подкрепа за управлението на границите и визовата политика (ИУГВП), както и на средствата за финансиране на подхода "Водено от общностите местно развитие" от Европейския земеделски фонд за развитие на селските райони (ВОМР) на ЕС, за програмен период 2021 – 2027 г.

**Приложение Д** Ръководство за потребителя за модул „Е-кандидатстване“.

**Приложение Е** Автобиография на Ръководителя на проекта (образец).

1. Съгл. Преамбюл на ДИРЕКТИВА (ЕС) 2022/2555 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 14 декември 2022 година [↑](#footnote-ref-1)
2. Процентът на съфинансиране от Европейския фонд за регионално развитие (ЕФРР) и от националния бюджет, като нормативно определената ставка е 85% от ЕФРР и 15% национално съфинансиране. [↑](#footnote-ref-2)
3. Процентът на съфинансиране от Европейския фонд за регионално развитие (ЕФРР) и от националния бюджет, като нормативно определената ставка е 70% от ЕФРР и 30% национално съфинансиране. [↑](#footnote-ref-3)