МЕТОДОЛОГИЯ И КРИТЕРИИ ЗА ПОДБОР НА ОПЕРАЦИИ

1. Основни параметри	
Междинно звено	Дирекция „Управление на програми и проекти“, Министерство на електронното управление
Програма	ПРОГРАМА „НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ“ 2021 - 2027
Приоритет	Приоритет 2 „Цифрова трансформация на публичния сектор“
Специфична цел	Специфична цел: RSO1.2. Усвояване на ползите от цифровизацията за гражданите, дружествата, изследователските организации и публичните органи
Наименование на процедурата/процедурите	**Пилотно укрепване на капацитета на три Национални компетентни органа и три секторни екипи за реагиране при инциденти с компютърната сигурност към тях**
Цел	Да се подобри националният капацитет в киберсигурността и да се адаптират националните компетентни органи (НКО) и секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС) към постоянно променящите се рискове и заплахи за мрежовата и информационна сигурност.
Обосновка	Мрежовите и информационните системи се превърнаха в централен елемент на всекидневния живот на фона на бързата цифрова трансформация и взаимосвързаността на обществото, включително в трансграничния обмен. Това развитие води до разширяването на броя на киберзаплахите, пораждайки нови такива, и изисква адаптирани, координирани и новаторски реакции във всички държави членки. Броят, мащабите, сложността, честотата и въздействието на инцидентите се увеличават и представляват съществена заплаха за функционирането на мрежовите и информационните системи. В резултат на това инцидентите могат да попречат на извършването на икономически дейности в рамките 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 за правилното функциониране на вътрешния пазар. Освен това киберсигурността 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 и устойчивите предимства на цифровизацията[1]. Броят на киберзаплахите, рисковите сценарии и уязвимостите нарасна експоненциално. Киберсигурността се разви като ново поле на интерес, привличайки политическо и обществено внимание. Като се има предвид този мащаб, бъдещите задачи и отговорности, свързани с киберсигурността, са от съществено

[1] Съгл. Преамбюл на ДИРЕКТИВА (ЕС) 2022/2555 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 14 декември 2022 година

значение за оцеляването и жизнеспособността на съответната организация.

Европейско законодателство в областта на киберсигурността, като ДИРЕКТИВА (ЕС) 2022/2555 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) акцентира върху и адресира горепосочените предизвикателства и определя изискванията за създаването и развитието на капацитета на компетентните органи и екипите за реагиране при инциденти с компютърната сигурност.

Един от инструментите за укрепване на националния капацитет в киберсигурността е изграждането и осигуряването на ефективната работа на НКО и СЕРИКС. Посредством подкрепата по настоящата процедура се предвижда да бъде укрепен капацитета на 3 бр, НКО и 3 бр. СЕРИКС към тях за осигуряване на киберсигурността на административни органи в сектори с висока степен на критичност съгласно Приложение I Сектори с висока степен на критичност от Директива (ЕС) 2022/2555 на Европейския Парламент и на Съвета от 14.12.2022 г.

Съгласно чл. 16 от Закона за киберсигурност (ЗКС) сред ключовите задачи на Националните компетентни органи са да:

- координират и контролират изпълнението на задачите, свързани с мрежовата и информационната сигурност на административните органи, операторите на съществени услуги и доставчиците на цифрови услуги съгласно този закон;
- оценяват дали административните органи, операторите на съществени услуги и доставчиците на цифрови услуги изпълняват задълженията си по осигуряване на мрежовата и информационната сигурност и предприемат съответните мерки при неизпълнение и при необходимост задължителни указания за отстраняване на установените пропуски в изпълнението на изискванията;
- изграждат екипите за реагиране при инциденти с компютърната сигурност.

От друга страна, съгласно чл. 18 от ЗКС сред ключовите задачи на Секторни екипи за реагиране при инциденти с компютърната сигурност са да,:

- изграждат комуникационни канали с висока надеждност;
- осигуряват непрекъснатост на дейността си чрез:
  - подходяща система за управление и разпределяне на заявките;
  - достатъчен персонал, който да е постоянно на разположение;
  - инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение;
- изпълняват реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на Агенцията на

	Европейския съюз за мрежова и информационна сигурност (ENISA) и с българското законодателство. Предвидените интервенции по настоящата процедура са в съответствие с гореспоменатите изисквания, определени в Директива МИС 2, като се основават на и надграждат резултатите, постигнати при изпълнението на проект 2018-BG-IA-0114 „Изграждане на капацитет и подобряване на услугите на CERT България (CBSEC-BG)“, финансиран от Механизма за свързване на Европа, по който бяга изградени необходимите портали и инфраструктура за националния CERT, както и системи за свързване към мрежата на екипи за реагиране при инциденти с компютърната сигурност на ЕС с помощта на платформата MeliCERTes. Пилотното укрепване на капацитета на три НКО и три СЕРИКС към тях ще допринесе за укрепването на националния капацитет в киберсигурността, както и за подобряването на мрежовата и информационна сигурност.
Очаквани резултати	В резултат от изпълнението на предвидените дейности по настоящата процедура се очаква да бъдат постигнати следните резултати: Подкрепени и ефективно функциониращи три Национални компетентни органа и три секторни екипи за реагиране при инциденти с компютърната сигурност към тях.
Продължителност на процедурата/процедурите	2023 – 2025 г.
Териториален обхват	*Дейностите по настоящата процедура следва да бъдат изпълнени на територията на Република България.*
Бюджет (ЕФРР и национален)	**Общият размер на безвъзмездната финансова помощ е 7 823 320 лева (4 000 000 евро), в т.ч. за:** • по-слабо развити региони - 6 293 861 лева (3 218 000 евро); • региони в преход (ЮЗР) – 1 526 459 лева (782 000 евро).
Режим на държавна/минимална помощ	**Неприложимо** 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. В процедурата по конкурентен подбор могат да участват само административни органи (съгласно чл. 16, ал. 1 и чл. 18 от Закона за киберсигурност), поради което при предоставянето на финансовите средства и извършването на оценката на държавната помощ не са налице елементите „икономическо предимство” и „въздействие върху конкуренцията и търговията“, тъй като въпросните административни органи, които са задължени да изградят секторни компетентни органи и екипи за реагиране при инциденти с компютърната сигурност към тях не осъществяват дейност на пазар, на който се осъществява търговия между държави-членки. Предвид

	това, подпомагането не следва да се разглежда като попадащо в обхвата на чл. 107, § 1 от ДФЕС.
2. Методология и критерии за подбор на операции	
Вид процедура за предоставяне на безвъзмездна финансова помощ	Ще се прилага процедура за безвъзмездна финансова помощ чрез директно предоставяне на конкретен бенефициент съгласно чл. 25, ал. 1, т. 2 от Закона за управление на средствата от европейските фондове при споделено управление (ЗУСЕФСУ).
Допустими кандидати	Административни органи по чл. 16, ал. 1 и чл. 18, ал. 1 от Закона за киберсигурност. *Бележка: Съгласно Решение №3 от 02.06.2023 г. на Съвета за Киберсигурността са определени за пилотни НКО и СЕРИКС в сектори Здравеопазване, Енергетика и „Образование и наука“.*
Изисквания към партньори *(ако е приложимо)*	Неприложимо
Допустими проекти/дейности	1. Разполагане на независимо функционираща инфраструктура в НКО и СЕРИКС в съответния сектор. 2. Внедряване и интегриране на обслужващи софтуерни платформи в НКО и СЕРИКС в съответния сектор 3. Развитие на специализиран административен капацитет в НКО и СЕРИКС в съответния сектор. 4. Включване на заинтересовани групи/конституенти в процеса на предоставяне на услуги и информация от НКО и СЕРИКС в съответния сектор.
Допустими разходи	1. Разходи за оборудване, необходимо за изграждането и функционирането на самостоятелен НКО и СЕРИКС (материални активи). 2. Разходи за софтуер и лицензи, необходим за изграждането и функционирането на самостоятелен НКО и СЕРИКС (нематериални активи). 3. Разходи за услуги, необходими за изграждането и функциониране на самостоятелен НКО и СЕРИКС. 4. Разходи за ограничени строително-монтажни работи във връзка с изграждането на независимо функционираща инфраструктура в НКО и СЕРИКС в съответния сектор. 5. Разходи за персонал (възнаграждения на лица, пряко ангажирани с дейности по изпълнението и/или управлението на проекта, включително задължителните социални и здравни осигурителни вноски за сметка на осигурителя, съгласно националното законодателство;). 6. Разходи за участие на служители на НКО и СЕРИКС в специализирани обучения, свързани с функционирането на съответния НКО и СЕРИКС. 7. Разходи за такси и абонаменти в специализирани бази данни и платформи, необходими за функционирането на НКО и СЕРИКС. 8. Непреки разходи за организация и управление на проекта (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) .
Минимален размер на помощта	Неприложимо
Максимален размер на помощта	2 607 773.33 лв. (1 333 333.33 евро) .
Интензитет на помощта	100 %
Продължителност на проектите	15 месеца
Кръстосано финансиране *(ако е приложимо)*	Неприложимо
Критерии за подбор/ оценка на съответствието	1. Проектното предложение допринася за постигане на специфичната цел на приоритета, целите на настоящата процедура и целите на програмата. 2. Предвидените дейности следва да: - допринасят за постигането на специфичните цели на Приоритет 2 на ПНИИДИТ; - са недискриминационни и прозрачни; - не са в противоречие с принципите на чл. 9 от Регламент 1060/2021; 3. Проектното предложение демонстрира ясна връзка между цели, дейности и резултати. 4. Всички дейности по проекта са допустими, ясно и последователно описани, като са посочени причините за избора на всяка една дейност, и нейният принос за постигане на очакваните резултати. 5. Планът за изпълнение на дейностите е реалистично планиран и осъществим, като е съобразен с плана за външно възлагане. 6. Планът за външно възлагане е в съответствие с предвидените дейности, като кандидатът е предвидил механизми, позволяващи мониторинг и текущ контрол на изпълнението на предвидените поръчки и своевременното предприемане на коригиращи мерки. 7. В проектното предложение са описани начините, чрез които се планира да бъде осигурена устойчивостта на резултатите и ефекта от изпълнението на проекта. 8. Кандидатът не е получил финансиране от източник с публичен характер (друг проект/програма/бюджетна линия или друга финансова схема с източник националния бюджет, бюджета на ЕС или друга донорска програма) за същите разходи, за финансирането, на които кандидатства по настоящата процедура. 9. Всички разходи, включени в бюджета на проектното предложение съответстват изцяло на дейностите, предвидени за изпълнение. 10. Всички разходи са ефективни, обосновани и допустими съгласно Условията за кандидатстване, като не е налице дублиране на разходи.

	11. Размерът на исканата безвъзмездна финансова помощ е в съответствие с максималния размер, указан в Условията за кандидатстване.
Индикатори	**Показатели за крайния продукт:** SO08 Действащи национални компетентни органи и секторните екипи за реагиране при инциденти с компютърната сигурност към тях **Показатели за резултата:** 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