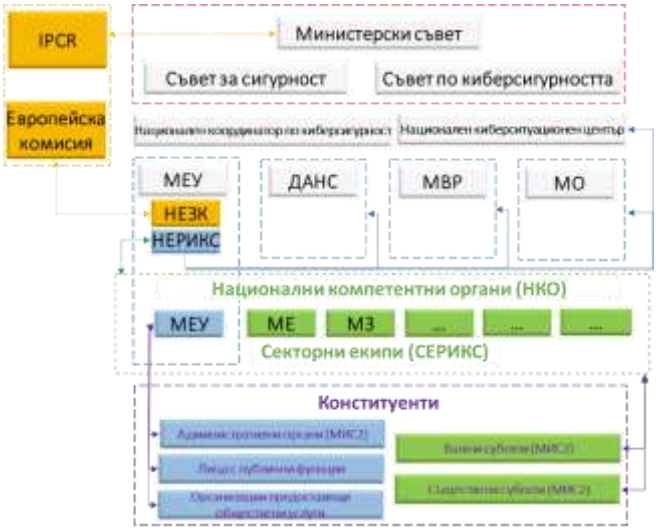
МЕТОДОЛОГИЯ И КРИТЕРИИ ЗА ПОДБОР НА ОПЕРАЦИИ

1. Основни параметри	
Управляващ орган	Главна дирекция „Европейски фондове за конкурентоспособност”, Министерство на иновациите и растежа, чрез Междинно звено – дирекция „Управление на програми“, Министерство на електронното управление, на основание РМС № 712 от 2020 г. (в изменението му с РМС № 519 от 2022 г.)
Програма	ПРОГРАМА „НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ“ 2021 - 2027
Приоритет	Приоритет 2 „Цифрова трансформация на публичния сектор“ Приоритетно направление 2 „Киберсигурност“
Специфична цел	Специфична цел: RSO1.2. Усвояване на ползите от цифровизацията за гражданите, дружествата, изследователските организации и публичните органи
Наименование на процедурата/процедурите	**Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността**
Цел	Настоящата процедура има за цел 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 и устойчивите предимства на цифровизацията[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

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

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 финансирана 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 изградените 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 ѝ 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 от предвидените шест обществени поръчки по проекта има сключен договор по една от тях, други четири са на различни етапи преди сключване на договор, а за една предстои обявяване. Очаква се инвестицията да бъде завършена през м. юни 2026 г. Въпреки вече осъществените инвестиции в изграждането на националната система за киберсигурност, усилията в тази посока следва да бъдат постоянни и ежегодни поради експоненциално растящия брой киберзаплахи и икономическите последствия от тях – проучване[2] предвижда, че финансовите щети, нанесени от киберпрестъпността ще костват на световната икономика 8 трилиона щатски долара през 2023 г. (ако се измерва

[2] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

като държава, тогава киберпрестъпността ще бъде третата по големина икономика в света след тази на САЩ и Китай). От своя страна, увеличеният брой киберзаплахи води до очакван ежегоден скок от 15% в размера на разходите за киберсигурност в световен мащаб[3].

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.

[3] https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

- 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 информация 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, А1, 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).
Продължителност на процедурата/процедурит	2025-2029

<table>
<tr><td>е</td><td></td></tr>
<tr><td>Териториален обхват</td><td>Дейностите по настоящата процедура следва да бъдат изпълнени на територията на Република България.</td></tr>
<tr><td>Бюджет (ЕФРР и национален)</td><td>Общият размер на безвъзмездната финансова помощ е 161 861 000 лева (82 758 215.18 евро), в т.ч. за:
- по-слабо развити региони - 130 231 271.89 лева (66 586 191.99 евро)
- региони в преход (ЮЗР -.31 629 728.11 лева (16 172 023.19 евро)
<table>
<tr><th></th><th>По-слабо развити региони</th><th>Региони в преход</th><th>Общо финансиране по ПНИИДИТ</th></tr>
<tr><td rowspan="2">ОБЩО ЕФРР+национален</td><td>130 231 271.89 лв</td><td>31 629 728.11 лв</td><td>161 861 000 лв</td></tr>
<tr><td>66 586 191.99 евро</td><td>16 172 023.19 евро</td><td>82 758 215.18 евро</td></tr>
<tr><td rowspan="2">ЕФРР</td><td>110 696 581.10 лв</td><td>22 140 809.68 лв</td><td>132 837 390.78 лв</td></tr>
<tr><td>56 598 263.19 евро</td><td>11 320 416.23 евро</td><td>67 918 679.42 евро</td></tr>
<tr><td rowspan="2">национален</td><td>19 534 690.78 лв</td><td>9 488 918.43 лв</td><td>29 023 609.22 лв</td></tr>
<tr><td>9 987 928.80 евро</td><td>4 851 606.96 евро</td><td>14 839 535.76 евро</td></tr>
</table></td></tr>
<tr><td>Режим на държавна/минимална помощ</td><td>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.
„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</td></tr>
</table>

	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.
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	**Министерство на електронното управление чрез дирекция „Мрежова и информационна сигурност“** 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, 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.
Изисквания към партньори (ако е приложимо)	Неприложимо
Допустими проекти/дейности	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 Осигуряване и имплементиране на технологични решения за изграждане на

	ЗСИПЕУ Имплементиране на технологични решения за повишаване на нивото на защита от кибер заплахи на конституенти - административни органи Интегриране на системи и ресурси на конституенти към Националната система за киберсигурност, включително интеграции от типа НЕРИКС-СЕРИКС, интеграция с НКСЦ и др. Надграждане на технологичните ресурси за увеличаване на обхвата и обема на споделената и обменената информация между всички заинтересовани страни
Допустими разходи	1. Разходи за дълготрайни материални активи 2. Разходи за дълготрайни нематериални активи 3.Разходи за услуги 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.
Минимален размер на помощта	Неприложимо
Максимален размер на помощта	161 861 000 лева
Интензитет на помощта	100 %
Кръстосано финансиране *(ако е приложимо)*	Неприложимо
Критерии за подбор/ оценка на съответствието	А. Критерии за административно съответствие 1. Формулярът за кандидатстване е подаден в рамките на избрания краен срок по електронен път чрез системата ИСУН 2020 и е на български език, с изключение на раздел „Основни данни“, полета „Наименование на проектното предложение на английски език“ и „Кратко описание на проектното предложение на английски език“, които следва да са попълнени на английски език. 2. Проектното предложение е подписано с валиден КЕП от законния представител на кандидата или оправомощено за целите на подаването на проектното предложение лице. 3. Документът за оправомощаване на лицето, което подписва с КЕП от името на кандидата документите за кандидатстване в ИСУН 2020 (в случай че е приложимо) е подписан с КЕП от законния представител на кандидата. 4. Представена е Декларация при кандидатстване по образец. 5. Представена е Декларация относно статута по ЗДДС по образец. 6. Финансовата обосновка на бюджета на проекта (по образец) е попълнена съгласно Указанията за попълване на финансовата обосновка на бюджета на проекта и приложения към нея.

	Б. Критерии за оценка на допустимостта на кандидата и проекта 1.Кандидатът е допустим бенефициент по настоящата процедура съгласно Условията за кандидатстване. 2. Кандидатът разполага с необходимите финансови ресурси и механизми за покриване на оперативните разходи и разходите за поддръжка, за да гарантира тяхната финансова устойчивост. 3. Предвижда се проектът да бъде осъществен в съответствие с посочения териториален обхват за операцията съгласно Условията за кандидатстване. 4. Продължителността на проекта е в съответствие с посочената информация в Условията за кандидатстване. 5. Дейностите и разходите по проекта съответстват на допустимите за финансиране дейности и разходи по процедурата съгласно Условията за кандидатстване. 6. Дейностите по проекта не са били физически завършени или изцяло осъществени преди подаването на проектното предложение за финансиране по програмата, независимо дали всички свързани плащания са направени от бенефициента или не. 7. В проектното предложение са присъединени/включени всички индикатори, посочени в Условията за кандидатстване, като представената информация отговаря на изискванията на Условията за кандидатстване. 8. Общият размер на заявената безвъзмездна помощ от страна на конкретния бенефициент е до максималния размер на безвъзмездна финансова помощ за конкретния бенефициент съгласно Условията за кандидатстване. 9. Заложените ограничения на разходите съгласно Условията за кандидатстване са спазени при формиране на бюджета и не са допуснати изчислителни грешки/технически грешки. 10. Проектното предложение е преминало проверка и е утвърдено от Министъра на електронното управление в съответствие с чл. 7в, ал. 2, т. 10 от Закона за електронното управление. В. Специфични критерии за оценка 1. Проектното предложение допринася за постигане на целите на ПНИИДИТ. 2. Предвидените дейности допринасят за постигането на специфичните цели на Приоритет 2 на ПНИИДИТ. 3. Предвидените дейности допринасят за постигането на целите на настоящата процедура. Целите на проекта са конкретни и измерими и обвързани със срокове. 4. Предвидените дейности не са в противоречие с принципите на чл. 9 от Регламент 2021/1060. 5. Проектното предложение демонстрира ясна връзка между цели, дейности и резултати. Резултатите са измерими и ясно е представено текущото и желаното състояние. 6. Планираните резултати са ясно дефинирани, реалистични и постижими и е налице причинно-следствена връзка между тях и междинните/целевите

	стойности на индикаторите. 7. Всички дейности по проекта са допустими, ясно и последователно описани, като са посочени причините за избора на всяка една дейност. 8. Планът за изпълнение на дейностите е реалистичен и осъществим. Обособени са ясно разграничени етапи на изпълнение и всеки етап е обвързан с конкретни срокове и отговорности. 9. Планът за изпълнение на дейностите е съобразен с плана за външно възлагане, като съдържа подходящи мерки за контрол на качеството, наблюдение и оценка, за да се гарантира, че изпълнението на проекта е с високо качество, завършено навреме и в рамките на бюджета. 10. На ниво проектно предложение кандидатът е идентифицирал ключови рискове за успешното изпълнение на дейностите по проекта и е разработил процедури за управление на риска за намаляване на идентифицираните рискове. Представен е план за план за управление на риска. 11. На ниво проектно предложение 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. 12. За всяка една дейност, предвидена за външно възлагане, кандидатът е обосновал защо е избрал да пристъпи към външно възлагане на съответната дейност, както и ясно е разписал обхвата на възлагането и ангажимента на изпълнителя. 13. На ниво проектно предложение са описани конкретни мерки, чрез които се планира да бъде осигурена дългосрочната устойчивост на резултатите и ефекта от изпълнението на проекта.14. 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. 15. Всички разходи, включени в бюджета на проектното предложение съответстват изцяло на дейностите, предвидени за изпълнение.
Индикатори	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 <u>Индивидуални за процедурата индикатори</u> Брой доставени и инсталирани инфраструктурни компоненти – бр. Брой доставени и инсталирани информационни и комуникационни системи за киберсигурност – бр.
