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 „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 мрежовата и информационна сигурност (МИС) в инфраструктура на компетентни органи с цел защита на публичните услуги**
Цел	Целта на процедурата е повишаване на нивата на мрежовата и информационната сигурност на критични системи, бази данни и регистри, имащи отношение към предоставяне на публични услуги.
Обосновка	Действие CS6 „Повишаване на мрежовата и информационна сигурност (МИС) в инфраструктура на компетентни органи с цел защита на публичните услуги“ от Приоритет 2 на ПНИИДИТ ще надгради резултатите по комбинираната процедура CS1-CS5 (BG16RFPR002-2.018 „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността“). Действие CS6 ще се фокусира върху повишаване капацитета на националния екип за реакция при инциденти в компютърната сигурност (НЕРИКС)/секторния екип за реагиране при инциденти с компютърната сигурност на публичната администрация (СЕРИКС в Министерството на електронното управление, МЕУ) с фокус върху защитата на публичните услуги. 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 сектори. Нарастващият брой и въздействие на инцидентите с МИС създава сериозни рискове за непрекъснатостта на публичните услуги и икономическата дейност, както

	и за доверието на потребителите. За постигане на високо ниво на МИС трябва да се гарантира, че съществените субекти предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи, които тези субекти използват при своите операции или при предоставяне на своите услуги, както и за предотвратяване или свеждане до минимум на въздействието на инцидентите върху получателите на услугите им и върху други услуги. Мерките се основават на подход, обхващащ всички опасности, който има за цел да защити мрежовите и информационните системи и физическата среда на тези системи от инциденти, и включват поне следното: а) политики за анализ на риска и сигурност на информационните системи; б) действия при инцидент; в) непрекъснатост на дейността, например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи; г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите преки снабдители или доставчици на услуги; д) сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им; е) политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността; ж) основни киберхигиенни практики и обучение в областта на киберсигурността; з) политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране; и) сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи; й) използването на многофакторни решения за удостоверяване на автентичността или непрекъснато удостоверяване на автентичността, защитени гласови, видео и текстови съобщения и защитени системи за спешна комуникация в рамките на субекта, когато е целесъобразно. НЕРИКС/СЕРИКС за публичната администрация трябва да са в състояние да изпълняват следните задачи: а) наблюдение и анализ на киберзаплахи, уязвимости и инциденти на национално равнище, както и, при поискване, предоставяне на помощ за засегнати съществени и важни субекти във връзка с наблюдението на техните мрежови и информационни системи в реално време или почти в реално време; б) подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за киберзаплахи, уязвимости и инциденти до засегнатите съществени и важни субекти, както и до компетентните органи и други относими заинтересовани страни, по възможност в почти реално време;

	в) реагиране на инциденти и оказване на помощ на засегнатите съществени и важни субекти, когато е приложимо; г) събиране и анализиране на криминалистични данни и осигуряване на динамичен анализ на рисковете и инцидентите и ситуационна осведоменост за киберсигурността; Стратегическата цел поставена в националната стратегия за киберсигурност на РБългария „Киберустойчива България 2023“ е постигане на киберустойчивост на цялото общество и държава, изразяващо се в ефективна защита и адекватна реакция на кибератаки и киберинциденти, ограничаване на вредните последствия от тях, максимално устойчиво функциониране на жизненоважни дейности и услуги, и своевременно възстановяване до нормалното състояние . За постигането на киберустойчивост на национално ниво е необходимо надграждане способностите на НЕРИКС/СЕРИКС за публичната администрация с цел осигуряване изпълнението на всички задачи заложени в Директива МИС 2. Настоящата процедура стъпва върху необходимостта за разполагането на допълнителен набор от централни компоненти (централни технологични решения), които да гарантират непрекъснатото предоставяне на публични услуги чрез минимизирането на конкретни рискове. Кражбата на идентификационни данни и злоупотребата с привилегирован достъп е заплаха за киберсигурността, която може да причини сериозни и големи щети на всяка организация. **Системата за привилегирован достъп** (Privileged Access Management, PAM) помага на организациите да защитят своите най-чувствителни ИТ активи, като гарантира, че идентификационните данни на привилегирован акаунт – като администраторски акаунти за критични системи – са достъпни само за потребители с подходящите разрешения. Чрез налагане на политики за достъп с най-малко привилегии, софтуерът PAM минимизира риска от външно компрометиране или вътрешна злоупотреба, като предоставя на потребителите само минималното ниво на достъп, необходимо за изпълнение на работните им функции. Софтуерът PAM е предназначен да защитава достъпа на супер потребители, споделени акаунти и акаунти за услуги, осигурявайки централизиран контрол, видимост и наблюдение на тези идентификационни данни на високо ниво. С нарастването на работата от разстояние, все повече организации осъзнават ползите от PAM. Благодарение на PAM бързо могат да бъдат предоставяни и управлявани правата за достъп на отдалечени служители и външни изпълнители, без това да нарушава ефективността на ежедневната работа и да носи допълнителен риск за сигурността. Освен това, деактивирането на достъпа за напускащи служители или при приключване на работата на външни изпълнители става бързо и лесно. Това е изключително важно, а доста често напълно подценявано. Скорошно проучване установява, че 25% от служителите все още имат достъп до акаунти от предишни работни места. Осведомеността в областта на киберсигурността и киберхигиената са от съществено значение за повишаване на равнището на киберсигурност. Следва да приемат политики за насърчаване на активната киберзащита като част от по-широка отбранителна стратегия. Вместо да се реагира, активната киберзащита се състои от превенция, откриване, наблюдение,

	анализ и смекчаване на нарушенията на сигурността на мрежата по активен начин, в съчетание с използването на способности, разположени във и извън мрежата. Способността за бързо и автоматично споделяне и разбиране на информация и анализ на заплахи, предупрежденията за кибердейности и действията за реагиране са от решаващо значение за осигуряване на единство на усилията за успешно предотвратяване, откриване, противодействие и блокиране на атаки срещу мрежови и информационни системи. **За целта е предвидено осигуряване на система за мрежови примамки – HONEYPOT.** Практическото приложение на подобни софтуерни системи позволява да се извършат задълбочени анализи, свързани с киберсигурността, рисковете и определянето на потенциалните атаки и извършителите им, базирани на реални данни. Инсталирането и наблюдението на honeypot е полезно и до голяма степен помага на екипите отговарящи за киберсигурността и на системните администратори. Honeypot служи като примамка, която отвлича вниманието на киберпрестъпниците от действителните цели. Той може да служи и като инструмент за разузнаване, като използва опитите им за проникване, за да оцени техниките, възможностите и сложността на противника. Honeypots могат да идентифицират както вътрешни, така и външни заплахи за сигурността. Докато много техники за киберсигурност се фокусират върху рисковете, идващи отвън, honeypots могат да привлекат и вътрешни участници, които се опитват да получат достъп до данните, IP адреса или друга чувствителна информация на организацията. Мерките за управление на риска в областта на киберсигурността следва да отчитат степента на зависимост на съществения или важния субект от мрежовите и информационните системи и следва да включват мерки за идентифициране на всякакви рискове от инциденти с цел предотвратяване, откриване и реагиране на инциденти, както и ограничаване на тяхното въздействие. Сигурността на мрежовите и информационните системи следва да включва сигурността на данните, които се съхраняват, предават и обработват. Мерките за управление на риска в областта на киберсигурността следва да предвиждат системен анализ, при който се отчита човешкият фактор, за да се получи пълна картина на сигурността на мрежовата и информационната система. **За целта като елемент от националната система за киберсигурност е необходимо да се внедри система за защита от загуба на данни (DLP).** Предотвратяването на загуба на данни (DLP) е цялостен технологичен и процедурен подход, който позволява да се идентифицират, наблюдават и защитават поверителна информация от случайно или умишлено разкриване, загуба или изтичане. Използването на DLP може да предотврати неконтролираното изтичане на данни от организацията – чрез електронна поща, USB устройства, приложения, облак или човешки грешки. DLP системите анализират данни в покой, в движение и в употреба. Това означава, че те могат да наблюдават данни, съхранявани на диск, предавани по мрежата и обработвани в реално време от потребителите. Тази многопластова защита дава на организациите по-голяма видимост и контрол върху жизнения цикъл на информацията. DLP помага за противодействие както на външни, така и на вътрешни заплахи. Първите включват кибератаки – опити за завладяване на данни от злонамерен софтуер, ransomware, фишинг или атаки DDoS. Чрез

	контролиране на изходящия трафик и анализ на съдържанието на прехвърлените файлове, DLP системата може да идентифицира опити за кражба на данни, преди те дори да бъдат извършени. Вътрешните заплахи, от друга страна, са все по-често срещани в организациите и включват действията на потребители с легитимен достъп до системата. Съществените субекти трябва да извършват редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган. МЕУ е Национален компетентен орган (НКО) за публичната администрация и като такъв трябва да упражнява своите надзорни задачи върху съществените субекти най-малко като искания за доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността и съответните подкрепящи доказателства. За улеснение на публичната администрация е предвидено надграждане капацитета на НЕРИКС/СЕРИКС **с изграждането на система за одит на промените в ИКТ среди**, която ще събира одитна информация от локални и от облачни приложения и ще ги съхранява в защитен, централизиран архив, което ще позволява използването на общи аларми, търсене, отчитане и анализ на рисковете по сигурността. Настоящата процедура ще разшири обхвата на включените за наблюдение и защита субекти в централната система за киберсигурност с нови 28 публични администрации – областни администрации, част от териториалната администрация на изпълнителната власт. За тях **допълнително ще бъдат закупени инфраструктурни компоненти и допълнителни лицензи за система за анализ и откриване на заплахи на база мрежови трафик (**Network Detection and Response - **NDR)**. NDR решенията анализират мрежовия трафик, откриват аномалии и сигнализират при необичайна активност. Така бързата реакция на екипите за сигурност и системните администратори намалява времето на уязвимост, което прави критичната клиентска инфраструктура надеждна и стабилна. NDR са усъвършенствани продукти за сигурност, които използват изкуствен интелект (AI), като машинно обучение, за да наблюдават и анализират целия мрежов трафик, за да откриват и предупреждават организациите за потенциални киберзаплахи в мрежата на тяхната организация. Вместо да разпознава известни сигнатури на заплахи, NDR открива аномална активност, свързана с злонамерен софтуер, целеви атаки, злоупотреба от вътрешни лица и рисково поведение, което е показателно за активна атака. NDR решенията откриват подозрителни дейности в ранен етап, като осигуряват непрекъсната видимост за всички потребители и технологии, свързани с мрежата, от центъра за данни до облака и крайните точки, използвани от дистанционните работници и IoT системите. Накратко, гореописаната комбинация от технологични решения ще: - осигури защита за уеб приложения, API и backend инфраструктура от неоткрити странични атаки, zero-day атаки или скрити прониквания, които заобикалят защитните стени и антивирусните инструменти; - предотвратява „отвличането“ на администраторски идентификационни данни от нападатели (или злонамерени

	вътрешни лица), за да компрометират системи, бази данни или облачна инфраструктура; - гарантира, че клиентските данни не изтичат през компрометирани крайни точки, неправилно конфигурирани облачни услуги или злонамерени вътрешни лица; - действа като система за ранно предупреждение — напр. ако нападател взаимодейства с honeypots, имитиращи електрони услуги, НЕРИКС/ СЕРИКС може да реагира, преди съответните системи да бъдат засегнати. В допълнение на административните органи, за които ще бъде осигурена защита по процедура CS1-CS5, по настоящата процедура обхватът на националната система за киберсигурност ще бъдат разширен с осигуряването на защита и за 28-те областни администрации, а технологичният набор от решения (централни компоненти) в НЕРИКС/ СЕРИКС за публичната администрация ще бъде надграден за защита на публичните услуги. За нуждите на националната система за киберсигурност ще бъдат закупени лицензи за сървърни системи и система за отдалечен достъп (конзолен сървър) за всички присъединени до момента административни органа (80 броя) . Примерен набор от инфраструктурни и софтуерни елементи, който ще бъде разгърнат за надграждане способностите на НЕРИКС/СЕРИКС за публичната администрация и присъединяването на областните администрации към националната система за киберсигурност включват: - система за анализ и откриване на заплахи на база мрежови трафик (NDR) – областни администрации; - система за мрежови примамки – honeypots; - система за защита от загуба на данни – DLP; - система за привилегирован достъп (PAM); - система за одит на промените в ИКТ среда; - комутатори, сървъри и защитни стени; - система за отдалечен достъп (конзолен сървър); - осигуряване на лицензи за сървърни системи - Microsoft 365 E5, Windows Server Standard и SQL Server Standard. В рамките на процедурата ще бъдат изработени процедури, касаещи реакцията на сигнали от НЕРИКС/СЕРИКС към конституентите, особено в случаите когато попадат под пълния мониторинг на системата за киберсигурност. Те ще имат за цел да разпишат задълженията, да установят времето за реакция и ескалационния механизъм на отговорниците по МИС в присъединените административни органи.
Очаквани резултати	В резултат от изпълнението на предвидените мерки и инициативи по настоящата процедура се очаква да бъдат постигнати следните резултати: • осигурени за НЕРИКС/СЕРИКС за публичната администрация

<table>
<tr><td></td><td>допълнителни централни компоненти, осигуряващи превенция, установяване и разрешаване на киберинциденти с акцент върху защитата на публичните услуги – не по-малко от 4 бр. ИКТ системи за киберсигурност, не по-малко от 2 бр. инфраструктурни компоненти и лицензи.
• допълнително обхванати от националната система за киберсигурност нови 28 административни органа (областни администрации).</td></tr>
<tr><td>Продължителност на процедурата/процедурите</td><td>2025 – 2029 г.</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 16 624 584,34 лева (8 500 015,00 евро), в т.ч. за:
- по-слабо развити региони – 13 375 926,09 лв. (6 839 002,41 евро);
- региони в преход (ЮЗР) – 3 248 658,25 лв. (1 661 012,59 евро).
<table>
<tr><th></th><th>По-слабо развити региони</th><th>Региони в преход</th><th>Общо</th></tr>
<tr><td rowspan="2">ОБЩО ЕФРР+ национален</td><td>13 375 926,09 лв.</td><td>3 248 658,25 лв.</td><td>16 624 584,34 лв.</td></tr>
<tr><td>6 839 002,41 евро</td><td>1 661 012,59 евро</td><td>8 500 015,00 евро</td></tr>
<tr><td rowspan="2">ЕФРР</td><td>11 369 537,18 лв.</td><td>2 274 060,77 лв.</td><td>13 643 597,95 лв.</td></tr>
<tr><td>5 813 152,05 евро</td><td>1 162 708,81 евро</td><td>6 975 860,86 евро</td></tr>
<tr><td rowspan="2">национален</td><td>2 006 388,91 лв.</td><td>974 597,48 лв.</td><td>2 980 986,39 лв.</td></tr>
<tr><td>1 025 850,36 евро</td><td>498 303,78 евро</td><td>1 524 154,14 евро</td></tr>
</table></td></tr>
<tr><td>Режим на държавна/минимална помощ</td><td>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</td></tr>
</table>

	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.
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	Внедряване на централни инфраструктурни компоненти за повишаване на нивото на защита от киберзаплахи на конституенти - административни органи (областни администрации) Повишаване на капацитета на НЕРИКС/СЕРИКС за публичната администрация чрез внедряване на ИКТ системи за киберсигурност Обучение на администратори/потребители за администриране/използване на предоставените системи Изготвяне на правила и процедури за конституенти за обмен на информация; работа с предоставените системи и реакция/управление на получените сигнали от НЕРИКС/СЕРИКС за публичната администрация
Допустими разходи	1. Разходи за дълготрайни материални активи 2. Разходи за дълготрайни нематериални активи 3.Разходи за услуги 4. Разходи за командировки 5. 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	н/п
Максимален размер на помощта	16 624 584,34 лв. (8 500 015,00 евро)
Интензитет на помощта	100 %
Кръстосано финансиране *(ако е приложимо)*	н/п
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 20 Публични организации, обхванати от системата за киберсигурност **Индивидуални за процедурата индикатори** Брой доставени и инсталирани информационни и комуникационни системи за киберсигурност – бр. Брой инсталирани инфраструктурни компоненти – бр. Брой обучени администратори от присъединените административни органи към националната система за киберсигурност – бр. Брой обучени служители на НЕРИКС/СЕРИКС – бр.