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 и проекти“, Министерство на електронното управление, на основание РМС № 712 от 2020 г. ,(изм. и доп. с РМС № 272 от 2022 г., и РМС № 519 от 2022 г., РМС № 97 от 2023 г. и РМС № 275 от 2023 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 капацитета на Държавна агенция „Национална сигурност“ за наблюдение и контрол в стратегическите обекти**
Цел	Целта на процедурата е да бъде осигурено надграждане и развиване на способностите на Държавна агенция „Национална сигурност“ (ДАНС) за ефикасен мониторинг, откриване и предупреждение за уязвимости и киберзаплахи към критичните системи, анализ и оценка на рисковете по отношение на киберсигурността, осъществяване на предотвратяване и възпиране, своевременна реакция и съдействие за възстановяване функционирането на поразените системи, както и за наличие на обобщена киберкартина отразяваща процесите в реално време.
Обосновка	Националната система за киберсигурност (НКС) обхваща пет области и приоритетни насоки за действие в сферата на киберсигурността: • установяване и развитие на националната система за киберсигурност, като част от системата за защита на националната сигурност; • мрежова и информационна сигурност; • защита и устойчивост на стратегически обекти и първични администратори; • ефективно противодействие на киберпрестъпността; и • киберотбрана и защита на националната сигурност. НКС функционира като виртуална мрежа на взаимодействие (Национална координационно-организационна мрежа за киберсигурност ((НКОМКС)),

	а архитектурата ѝ следва модела „ориентиран към услуги“. За реализиране на целите в област „защита и устойчивост на стратегически обекти и първични администратори“ отговорната институция е Държавната агенция „Национална сигурност“ (ДАНС). Съгласно чл. 15 на Закона за киберсигурност (ЗКС) ДАНС изпълнява политиката по защита от киберинциденти в комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност, като осъществява: • мониторинг и събиране на информация за събития и инциденти, свързани със сигурността на комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност; • подаване на предупреждения за киберзаплахи и информация за киберинциденти към стратегическите обекти и дейности, които са от значение за националната сигурност; • оказване на методическо съдействие в процеса на управление на киберинциденти; и • осигуряване на цялостен анализ на постъпващата информация и оценка на информационната защита на стратегическите обекти и дейности, които са от значение за националната сигурност. ДАНС поддържа готовност за координирана съвместна реакция в рамките на НКОМКС, свързани със сигурността на комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност. В чл. 4 на Закона за Държавна агенция „Национална сигурност“ (ЗДАНС) са конкретизирани задължения на ДАНС да извършва дейности за защита на националната сигурност от посегателства, насочени срещу националните интереси, независимостта и суверенитета на Република България, териториалната цялост, основните права и свободи на гражданите, демократичното функциониране на държавата и гражданските институции и установения в страната конституционен ред, вкл. свързани със застрашаване сигурността на стратегически за страната обекти и дейности; и деструктивно въздействие върху комуникационни и информационни системи. В допълнение, съгласно чл. 6 на ЗДАНС Агенцията осъществява функциите на орган по криптографска сигурност и орган по акредитиране на сигурността на комуникационните и информационните системи, в които се създава, обработва, съхранява и пренася класифицирана информация. В изпълнение на тези си функции ДАНС оценява и разработва криптографски алгоритми и средства за криптографска сигурност на класифицираната информация; одобрява и контролира криптографските мрежи за класифицирана информация; изработва и разпределя използваните криптографски ключове; разрешава и контролира производството и вноса на средства за криптографска сигурност; извършва акредитиране на комуникационните и информационните системи, в които се създава, обработва, съхранява и пренася

	класифицирана информация; координира и контролира контрамерките по TEMPEST. Стратегическите обекти и дейности, предоставени за управление, съответно възложени за осъществяване на Министерството на отбраната, на Министерството на вътрешните работи, на Националната служба за охрана и на Държавна агенция „Разузнаване“, се определят със заповед на ръководителя на съответното ведомство след съгласуване с председателя на ДАНС. С Постановление №181 от 20.07.2009 г. (ПМС 181/2009) са определени стратегическите обекти и дейности, които са от значение за националната сигурност на Република България и които са част от критичната инфраструктура. В този смисъл по отношение на стратегическите обекти ДАНС осъществява разнообразни функции, вкл. контрол на информационната защита, осъществявана чрез административни, организационни, технически и криптографски мерки; както и оказва съдействие на ръководителите на стратегически обекти и на възлагащите или извършващите стратегически дейности при идентифициране и оценка на потенциални заплахи, насочени срещу стратегически обекти и дейности от значение за националната сигурност. Потребностите на държавите да придобиват капацитет за справяне със заплахите в областта на киберсигурността расте ежегодно. През 2015 г. в Република България за пръв път беше извършена интензивна кибератака насочена към държавни структури, свързани с провеждания вот за местна власт. От тогава до момента броят на атаките срещу различни информационни инфраструктури в страната и в чужбина непрекъснато се увеличава. Атакуващи са различни хакерски групи, самостоятелни хакери или държавно спонсорирани групи. Все повече инструменти за компрометиране на системи и мрежи са лесно достъпни, като някои се предоставят като услуга срещу заплащане с биткойн. Бързото развитие на технологиите и инвестирането на големи ресурси в държавно спонсорирани групи извършващи кибератаки налага развиване на способностите и експертизата в ДАНС по отношение на защитата от киберинциденти в комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност. През последните три години в ДАНС се полагат усилия за развиване на технологичните способности за справяне с предизвикателствата на дигитализацията и достъпността на всякакви инструменти за въздействие върху комуникационните и информационните системи чрез национални и европейски средства. В Агенцията регулярно се следят възможностите, които предоставят различните технологични решения в областта на киберсигурността, като се отчитат споделените от партньори мнения и отзиви за ползваните инструменти. Следвайки добрите практики в областта на киберсигурността и научавайки уроците от различните по мащаб киберинциденти в страната и чужбина, ясно се оцени необходимостта от увеличаване на възможностите за извършване на обективен анализ и своевременна оценка на рисковете и повишаване на

	способностите по линия на киберсигурност в ДАНС. През 2024 г. Агенцията на Европейския съюз за киберсигурност (ENISA) публикува първият в историята на ЕС доклад за състоянието на киберсигурността, в който се отправят шест препоръки за повишаване на нивото на киберсигурност в Съюза, сред които водеща е укрепването на техническата и финансова подкрепа, предоставена на европейските и националните органи, ангажирани с киберсигурността, както и на органи и субекти, попадащи в обхвата на Директивата NIS2, за да осигурят хармонизирано, цялостно, навременно и съгласувано прилагане на развиващата се рамка на ЕС за киберсигурност. При осъществяването на обмен на информация по линия на партньорството с държави-членки на ЕС и европейски организации в областта на киберсигурността също се потвърждава необходимостта от повишаване на способностите на ДАНС с цел прилагане на по-ефективни мерки за превенция, разработване на по-успешни сценарии за реакция и възстановяване на поразени системи и прилагане на по-надеждни механизми за киберзащита на стратегическите обекти, както и развиване на възможности за проверка и гарантиране на целостта на веригите на доставки. ДАНС следва да повиши капацитета си за използване на системи с изкуствен интелект и съответно да надгради съществуващата инфраструктура с цел осигуряване на необходимата изчислителна мощ и достатъчно място за съхранение на обработваните данни. Същевременно ДАНС следва да подсигури изпълнението на задачи, свързани с функциите по чл. 6, ал. 5 от ЗДАНС на орган по акредитиране на сигурността на комуникационните и информационните системи, в които се създава, обработва, съхранява и пренася класифицирана информация, както и интегрирането на центъра със съществуващи системи в Агенцията. Надграждането на способностите на ДАНС в областта ще допринесе за укрепване на националния оперативен капацитет за предотвратяване, възпиране и реагиране на киберинциденти и ще подпомогне по-активното участие на Република България в процесите по атрибутиране с цел увеличаване на съвместните способности на държавите-членки на ЕС за противодействие на киберзаплахите. *Демаркация и допълняемост* През 2023 г. със съдействието на Министерство на електронното управление в ДАНС е изграден Център за мониторинг и реакция на киберинциденти (ЦМР). Осигурена е защита в областта на киберсигурността за пет (5) стратегически обекта от ПМС 181/2009 и дейности и са създадени и/или усъвършенствани пет (5) механизма за улесняване на защитата на критичната инфраструктура във всички сектори на икономиката.
Очаквани резултати	1. Въведени в експлоатация хардуерни и софтуерни инструменти и изградени механизми за интегриране на системи в ДАНС.

<table>
<tr><td></td><td>2. Осигурено устойчиво развитие и експлоатация на системи в ДАНС.

3. Повишена експертиза на служителите след преминати специализирани обучения и обмяна на опит с организации, имащи сходни задължения в държави от ЕС или участие във форуми в ЕС в областта на киберсигурността.

4. Повишен капацитет и наличие на надеждни инструменти за предотвратяване, възпиране и реагиране на киберинциденти в стратегическите обекти</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 48 000 000 лева (24 542 010,30 евро), в т.ч. за:

- по-слабо развити региони - 38 620 180,59 лева (19 746 184,79 евро);

- региони в преход (ЮЗР) – 9 379 819,41 лева (4 795 825,51 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>38 620 180,59 лв.</td><td>9 379 819,41 лв.</td><td>48 000 000,00 лв.</td></tr>
<tr><td>19 746 184,79 евро</td><td>4 795 825,51 евро</td><td>24 542 010,30 евро</td></tr>
<tr><td rowspan="2">ЕФРР</td><td>32 827 153,50 лв.</td><td>6 565 873,59 лв.</td><td>39 393 027,09 лв.</td></tr>
<tr><td>16 784 257,07 евро</td><td>3 357 077,86 евро</td><td>20 141 334,93 евро</td></tr>
<tr><td rowspan="2">национален</td><td>5 793 027,09 лв</td><td>2 813 945,82 лв.</td><td>8 606 972,91 лв.</td></tr>
<tr><td>2 961 927,72 евро</td><td>1 438 747,65 евро</td><td>4 400 675,37 евро</td></tr>
</table>
</td></tr>
</table>

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. По настоящата процедура за безвъзмездна финансова помощ чрез директно предоставяне на конкретен бенефициент е допустимо да кандидатства единствено ДАНС, 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 конкретният бенефициент не осъществява 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. Процедурите за избор на изпълнители следва да бъдат извършвани по реда на Закона за обществените поръчки 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.
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	Държавна агенция „Национална сигурност“ (ДАНС)
Изисквания към партньори (ако е приложимо)	н/п
Допустими проекти/дейности	• Доставка и въвеждане в експлоатация на инфраструктура в системи, свързани с дейности по киберсигурност в ДАНС. • Внедряване и интегриране на софтуерни платформи и специализирани услуги, обслужващи дейността по киберсигурност. • Внедряване на инфраструктура за интеграция и колаборация на системи в ДАНС за цялостно използване на наличните ресурси по линия на киберсигурност. • Осигуряване на експертни услуги и оперативна поддръжка на

	системите, обслужващи дейностите по киберсигурност с оглед на повишаване и развиване на способностите за превенция и реакция, както и възможностите за възстановяване и използване на механизми за киберзащита на наличните системи. • Въвеждане в експлоатация на иновативни технологии за повишаване на оперативните възможности за придобиване на информация и анализ с цел прилагане на механизми за защита, превенция и възпиране на въздействието на актуални киберзаплахи към стратегическите обекти. • Обмяна на опит и придобиване на познания за превенция и противодействие на актуалните киберзаплахи. • Присъединяване на стратегически обекти/секторни центрове за киберсигурност към системи/инфраструктура, оперирани от ДАНС. • Развиване и разработване на модулни, лесно адаптивни процеси, препоръки и решения за киберсигурност, чрез използване на стандарти, добри практики в индустрията за актуални налични на пазара решения за защита и превенция за стратегическите обекти.
Допустими разходи	Допустимите разходи са в съответствие с разпоредбите на Регламент (ЕС) 2021/1060, Регламент (ЕС) 2021/1058, Регламент (ЕС, Евратом) 2024/2095, Директива (ЕС) 2022/2555, приложимата национална уредба и приложимото общностно законодателство в областта на държавните помощи. 1. Разходи за доставка на оборудване (материални активи). 2. Разходи за доставка/разработване на софтуер и лицензи (нематериални активи). 3. Разходи за такси за специализирани обучения на служителите на ДАНС. 4. Разходи за услуги. 5. Разходи за командировки на служители на ДАНС. 6. Непреки разходи за организация и управление (свързани с изпълнението на проекта и 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). 7. Разходи за ограничени СМР
Минимален размер на помощта	н/п
Максимален размер на помощта	48 000 000 лв.
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. 7. Приложена е автобиография на Ръководителя на проекта по образец. 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. 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. 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. 6. Планираните резултати са ясно дефинирани 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. 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 рискове за успешно изпълнение на дейностите по проекта и е разработил процедури за управление на риска за намаляване на идентифицираните рискове. 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 начините, чрез които се планира да бъде осигурена устойчивостта 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