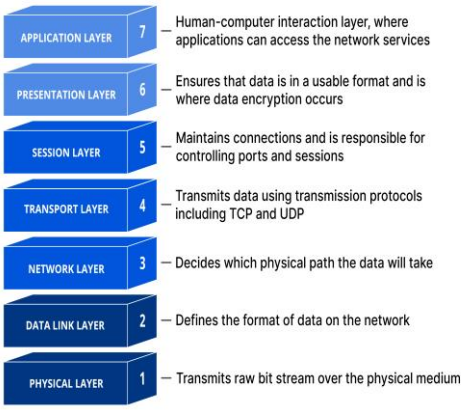
МЕТОДОЛОГИЯ И КРИТЕРИИ ЗА ПОДБОР НА ОПЕРАЦИИ

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	**Изграждане на централните компоненти на националната система за киберсигурност**
Цел	Да бъде повишено нивото на защита от киберзаплахи на конституентите на националната система за киберсигурност
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 значение за оцеляването и жизнеспособността на съответната организация. Един от механизмите за укрепване на националния капацитет в областта на киберсигурността е развитието на националната система за киберсигурност, като по настоящата процедура се предвижда да

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

	бъде подкрепено изграждането на централните компоненти на национална система за киберсигурност. Актуализираната национална стратегия за киберсигурност „Киберустойчива България 2023”[2] акцентира върху и адресира горепосочените предизвикателства, определяйки като една от приоритетните насоки за действие развитието на националната система за киберсигурност, като част от системата за защита на националната сигурност. Съгласно горепосочената стратегия 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. С оглед на гореизложеното по настоящата се предвижда да бъде подкрепено изграждането на централните компоненти на Националната система за киберсигурност. Интервенциите по процедурата няма да бъдат насочени към създаването на нови организации или звена в рамките на екосистемата за киберсигурност, а по-скоро ще подкрепят технологичното развитие и оборудването на Националната система за киберсигурност, което ще позволи на системата да бъде в крак с експоненциално нарастващия брой на киберзаплахите и техните икономически последици. Предвидените интервенции ще бъдат насочени към ниво 4 „Транспортен слой“ (Level 4 “Transport layer”) на Модела за взаимно свързване на отворени системи (open systems interconnection (OSI) model).**Какво представлява Моделът за взаимно свързване на отворени системи OSI?**[3] Моделът OSI е концептуален модел, създаден от Международната организация за стандартизация, който позволява на различни комуникационни системи да комуникират, използвайки стандартни протоколи. Моделът OSI предоставя стандарт за различни компютърни системи, за да могат да комуникират помежду си. Моделът OSI може да се разглежда като универсален език за компютърни мрежи. Той се основава на концепцията за разделяне на комуникационна система на седем абстрактни слоя, всеки от които е подреден върху предходния. Всеки слой на модела OSI обработва специфична работа и комуникира със слоевете над и под себе си. DDoS атаките са насочени към конкретни слоеве на мрежова връзка; приложният слой атакува целевия слой 7, а протоколният слой атакува целевите слоеве 3 и 4.

[2] https://e-gov.bg/wps/wcm/connect/e-gov.bg-18083/d58389e4-6dac-4015-aeea-59f10d01854c/21RH301pr.doc?MOD=AJPERES
[3] https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/



Настоящата процедура представлява начална фаза от изпълнението на действие CS1: Изграждане на национална система за киберсигурност към Приоритетно направление 2: Киберсигурност, Приоритет 2 на ПНИИДИТ, като подкрепените по процедурата интервенции ще послужат като основа, над която да бъде надградено с бъдеща/и процедура/и, които предстои да бъдат обявени по действие CS1 през следващите години в рамките на програмен период 2021-2027.

Предвидените интервенции по настоящата процедура са в съответствие с горепосочените тенденции, като се основават на и надграждат резултатите, постигнати при изпълнението на проект BG65ISNP001-6.007-0002-C04 „Изграждане на елементи от национална система за киберсигурност“, финансиран по линия на Фонд "Вътрешна сигурност“. По горепосочения проект, който е в процес на изпълнение и следва да приключи до 31.12.2023г., се очаква да бъда положени основите на националната система за киберсигурност посредством изграждане на Национална Координационно-Организационна Мрежа за Киберсигурност, Национален Киберситуационен Център, Национален център по киберпрестъпност, Национален екип за реагиране при инциденти в компютърната сигурност.

Също така, настоящата процедура ще продължи и надгради интервенциите по 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.

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[4] предвижда, че финансовите щети, нанесени от киберпрестъпността ще костват на световната икономика 8 трилиона щатски долара през 2023 г. (ако се измерва като държава, тогава киберпрестъпността ще бъде третата по големина икономика в света след тази на САЩ и Китай). От своя страна, увеличеният брой

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

	киберзаплахи води до очакван ежегоден скок от 15% в размера на разходите за киберсигурност в световен мащаб[5]. Централните компоненти на националната система за киберсигурност, които ще бъдат подкрепени по настоящата процедура, представляват активни устройства, които осъществяват защитената комуникацията през националната цифровата инфраструктура между конституентите и останалите части на националната система за киберсигурност. Предоставянето на подкрепа за изграждането на централните компоненти на националната система за киберсигурност ще спомогне за адресирането 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.
Очаквани резултати	В резултат от изпълнението на предвидените дейности по настоящата процедура се очаква да бъдат постигнати следните резултати: - функциониращи централни компоненти на националната система за киберсигурност; - интегрирани към националната система за киберсигурност системи на 3 бр. конституенти от централната и териториалната администрация.
Продължителност на процедурата/процедурите	2023 – 2026 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) – 1 529 459 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. По настоящата процедура за безвъзмездна финансова помощ чрез директно предоставяне на конкретен бенефициент е допустимо да кандидатства единствено Изпълнителна агенция „Инфраструктура на електронното управление“, 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,

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

	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	Изпълнителна агенция „Инфраструктура на електронното управление“ (ИА „ИЕУ“) ИА „ИЕУ“ е създадена с ПМС 89 от 19 май 2022г. Агенцията е администрация към Министъра на електронното управление за изпълнение на държавната политика в областта на електронното управление и на държавната политика в областта на мрежовата и информационна сигурност. Изпълнителната агенция е второстепенен разпоредител с бюджет по бюджета на Министерство на електронното управление. Съгласно чл.2, ал.4 Устройствения правилник на Изпълнителна агенция "Инфраструктура на електронното управление“ (приет с ПМС № 89 от 19.05.2022 г., Обн. ДВ. бр.38 от 20 Май 2022г., изм. и доп. ДВ. бр.60 от 29 Юли 2022г., изм. ДВ. бр.70 от 30 Август 2022г.) Агенцията изпълнява самостоятелно или съвместно с други органи или организации проекти и програми в областта на електронното управление и мрежовата и информационната сигурност. В тази връзка и с оглед на обстоятелството, че ИА „ИЕУ“ управлява инфраструктурата на електронното управление, вкл. националната система за киберсигурност, Агенцията е определена за конкретен бенефициент по настоящата процедура.
Изисквания към партньори *(ако е приложимо)*	Неприложимо
Допустими проекти/дейности	1. Изграждане и въвеждане в експлоатация на централните компоненти на националната система за киберсигурност. 2. Интегриране на системите на първите конституенти към националната система за киберсигурност.
Допустими разходи	1. Разходи за оборудване, необходимо за изграждане и въвеждане в експлоатация на централните компоненти на националната система за киберсигурност (материални активи). 2. Разходи за оборудване, необходимо за интегриране на системите на конституентите към националната система за киберсигурност (материални активи). 3. Разходи за софтуер и лицензи, необходими изграждане и въвеждане в експлоатация на централните компоненти на националната система за киберсигурност (нематериални активи). 4. Разходи за софтуер и лицензи, необходими за интегриране на системите на конституентите към националната система за киберсигурност (нематериални активи). 5. Разходи за персонал (възнаграждения на лица, пряко ангажирани само с дейности по изпълнението на проекта, включително задължителните социални и здравни осигурителни вноски за сметка на осигурителя, съгласно националното законодателство вкл. за постигнати резултати).

	6. Разходи за участие на служители на бенефициента в специализирани обучения. 7. 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).
Минимален размер на помощта	Неприложимо
Максимален размер на помощта	7 823 320 лева (4 000 000 евро) .
Интензитет на помощта	100 %
Продължителност на проектите	24 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 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 Индивидуални за процедурата индикатори за изпълнение: Внедрени и функциониращи централни компоненти на национална система за киберсигурност – бр. Интегрирани към националната система за киберсигурност конституенти – бр.