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 (ЕФРР)
Наименование на процедурата	Изграждане на обучителен център като елемент от националната система за киберсигурност
Цел	Надграждане и увеличаване на налични ресурси и изграждане на нови елементи от цялостната екосистема на киберсигурността чрез изграждане на център за провеждане на обучения, свързани с информационна сигурност, повишаване на осведомеността, компетентностите и механизмите за контрол и управление на инциденти, със съответната техническа платформа за симулация на комплексни дейности по кибератаки и защити, и развитие на стимулираща среда за изследвания и иновации в областта на киберсигурността.
Обосновка	Актът на ЕС[1] за киберсигурността определя киберсигурността като „дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи. Киберсигурността не е само въпрос, свързан с технологията, но и такъв, при който и човешкото поведение е от съществено значение.“ Поради това следва да бъдат активно насърчавани мерките, прилагани от физически лица, организации, предприятия и структурите на държавната администрация, които свеждат до минимум излагането им на рискове от киберзаплахи. Броят на кибератаките срещу институциите, организациите и агенциите в Европейския съюз се увеличава рязко. Тъй като тези институции са тясно свързани по между си, слабостите в една от тях могат да изложат останалите на заплахи за сигурността. В специален доклад[2] съгласно член 287, параграф 4, алинея втора от Договора за функциониране на общността, Европейската сметна палата препоръчва на Комисията да предприеме действия за подобряване на подготвеността на институциите в Европейския съюз, като предложи въвеждането на задължителни правила за киберсигурност и увеличаването на ресурсите, заделени за киберсигурност. Комисията следва също така да насърчава полезните взаимодействия между институциите. Съгласно доклада, обученията, свързани с киберсигурността, невинаги се провеждат систематично. Едва малко

[1] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32019R0881
[2] https://op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/bg/

над половината от институциите в ЕС предлагат текущо обучение в областта на киберсигурността за ИТ служителите и специалистите по ИТ сигурност. Само някои осигуряват задължително обучение в тази област за служителите, които отговарят за управлението на информационни системи, съдържащи чувствителна информация. Предвид факта, че броят на кибератаките рязко се увеличава, целта на одита е да определи дали институциите в Европейския съюз като цяло разполагат с установени практически механизми за защита срещу киберзаплахи. Заключението на Европейската сметна палата е, че не е постигнато ниво на подготвеност в областта на киберсигурността, което да съответства на заплахите.

На следващо място, Агенцията на Европейския съюз за киберсигурност (ENISA) и CERT на институциите, органите и агенциите на ЕС (CERT-EU) публикуваха съвместно доклад, за да предупредят за продължителна дейност от страна на определени злонамерени актьори. CERT България, съвместно с ENISA и CERT-EU, препоръчват организациите от публичния и частния сектор в ЕС да се запознаят с доклада: „Устойчива дейност от конкретни злонамерени актьори"[3]. Съществена препоръка в доклада е инвестиции в образованието по киберсигурност, което включва насърчаване на специалисти по киберсигурност да се запишат и/или бъдат включени в специализирани курсове за професионално обучение в тяхната област и провеждане на кратки информационни кампании за крайните потребители.

Една от приоритетните насоки за действие, определена в актуализираната национална стратегия за киберсигурност „Киберустойчива България 2023”4 е развитието на националната система за киберсигурност, като част от системата за защита на националната сигурност. За да е налице обаче ефективно функционираща Национална система за киберсигурност е необходимо да бъдат създадени съответните условия за повишаване и укрепване на националния капацитет, като едно от тези условия е провеждането на обучения, свързани с информационната сигурност. Развитието на мрежовите и информационните системи води до разширяването на броя на киберзаплахите, пораждайки нови такива, което от своя страна изисква адаптирани, координирани и новаторски реакции във всички държави членки. Колкото повече се развиват киберзаплахите, толкова повече расте необходимостта от адекватни реакции, които могат да се постигнат чрез обучение и тренинги на всички заинтересовани субекти в областта на киберсигурността и ползвателите на мрежи. Ключов механизъм в развитието на Национална система за киберсигурност е подходящото професионално обучение за повишаване квалификацията на заинтересованите страни в публичния сектор в съответствие с използваните технологии.

Вменената на Дирекция „Мрежова и информационна сигурност“ към Министерството на електронното управление функция на Национален компетентен орган по мрежова и информационна сигурност (МИС) по смисъла на Закона за киберсигурността, националното в България и европейско законодателство в областта на МИС е трудно изпълнима и изисква комплекс от мерки и условия за повишаване на капацитета за превенция при кибератаки.

Посредством подкрепата по настоящата процедура се предвижда създаване на условия за изграждане на капацитет на национална система за киберсигурност чрез изграждане на обучителен център като елемент от националната система за киберсигурност.

[3] https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication
[4] https://e-gov.bg/wps/wcm/connect/e-gov.bg-18083/d58389e4-6dac-4015-aeea-59f10d01854c/21RH301pr.doc?MOD=AJPERES

	Обучителният център ще бъде изграден от Дирекция „Мрежова и информационна сигурност“ към МЕУ и ще подпомага изграждането на оперативни способности посредством обучение и практически учения на всички заинтересовани страни от публичния и частния сектор, които стопанисват, управляват, функционират и отговарят за различни активи, компоненти и сегменти на киберпространството, покривайки широк спектър от дейности. За да предлага максимално реалистични условия за обучение, в центъра ще бъде изградена виртуална платформа /така нареченият Кибер полигон/ за разработване, предоставяне и използване на интерактивни симулационни среди за казуси от различно естество, включително симулация на атаки, потребители и техните дейности, както и на всякакви други публични услуги или услуги на трети страни, от които симулираната среда може да зависи. Предвиденият по процедурата Обучителният център не представлява надграждане на съществуващ център, а ще положи основите на изцяло нов модел на провеждане на обучения в публичния сектор, какъвто до момента не съществува и не е бил разработен. Бенефициент по настоящата процедура ще бъде Дирекция „Мрежова и информационна сигурност“ към Министерство на електронното управление в качеството й на Национален компетентен орган по мрежова и информационна сигурност (МИС) по смисъла на Закона за киберсигурността, националното и европейско законодателство в областта на МИС. Укрепването на капацитета Дирекция „Мрежова и информационна сигурност“ към Министерство на електронното управление посредством предоставянето на подкрепа за изграждането на нов модел на обучителен център в областта на киберсигурността ще доведе до установяване на ефективни механизми за споделяне на опит, информация и ангажираност на всички заинтересовани лица, което от своя страна ще допринесе за укрепването на националния капацитет в киберсигурността, както и за подобряването на мрежовата и информационна сигурност. Демаркация и допълняемост Идентифицирани са три проекта, които имат отношение към темата и съдържат дейности по обучение на персонала, и/или в които организацията-допустим кандидат по настоящата процедура участва, но тези проекти са с напълно различни предмети, обхват и целеви групи. Нито един от проектите не изгражда и не създава център за обучение с програми и модули за обучение, собственост на организацията, и с интегриран кибер полигон (технологична среда), който да позволява развитието на практически умения. Обучителните дейности по тези проекти представляват инструкции относно оборудването и/или конкретно обучение по специфична дейност от проекта. Проектите са както следва: - BG65ISNP001-6.007-0002-C04 „Изграждане на елементи от национална система за киберсигурност“, финансиран по линия на Фонд "Вътрешна сигурност“; - 2018-BG-IA-0114 „Изграждане на капацитет и подобряване на услугите на CERT България (CBSEC-BG)“; - Център за наблюдение и реакция при киберинциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегически обекти и дейности от значение за националната сигурност (ЦНСС). 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. Предвидените интервенции се основават на 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 бъдат 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. Бенефициент по проекта е Държавна агенция "Електронно управление" с партньор Главна дирекция „Борба с организираната престъпност“ към Министерство на вътрешните работи. Посочените дейности са свързани с разработването на определени компоненти на екосистемата за киберсигурност, които са насочени към определена цел на национално ниво. Включени са и дейности по закупуване на ИТ оборудване и софтуер за нуждите на Главна дирекция "Борба с организираната престъпност" в Република България във връзка със създаването на Национален център по киберпрестъпност, което е в съответствие с целта и очакваните резултати от проекта. Една от дейностите по проекта е обучение на служителите на партньорската организация в областта на анализа и мониторинга на информационни носители, софтуерни продукти, процедури за превенция и противодействие на киберинциденти, а другите предвидени обучения съдържащи се в дейностите са обучение на служители на бенефициента за компилиране и мониторинг на национална киберкартина и процедури за координирана реакция при инциденти и кризи на следващо място, интервенциите по настоящата процедура се основават и надграждат резултатите, постигнати при изпълнението на проект 2018-BG-IA-0114 „Изграждане на капацитет и подобряване на услугите на CERT България (CBSEC-BG)“, финансиран от Механизма за свързване на Европа, Видно от наименованието на проекта, дейностите са насочени към CERT Bulgaria - Национален екип за реагиране при инциденти с компютърната сигурност, а основна разлика с подкрепяните по настоящата процедура дейности е насочеността и фокуса на предоставяните обучения. Докато във вече изградения по проект 2018-BG-IA-0114 център се предоставят обучения с основно лекционен характер, фокусът на изграждания по настоящата процедура е върху практическите учения и предлагането на максимално реалистични условия за обучение посредством изграждането на виртуална платформа /така наречения Кибер полигон/ за разработване, предоставяне и използване на интерактивни симулационни среди за казуси от различно естество, включително симулация на атаки. По отношение на дейностите по проект „Център за наблюдение и реакция при киберинциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегически обекти и дейности от значение за националната сигурност (ЦНСС), ситуацията е същата: дейностите по проекта включват обучение относно мониторинга. В рамките на проекта ще бъде създаден Център за наблюдение и реакция при киберинциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегически обекти и дейности от значение за националната сигурност (ЦНС). Проектът се фокусира върху придобиването на специализирано оборудване и софтуер, инсталиране, интегриране и обучение на персонала по използването на съответното оборудване. Освен това центърът се създава на основание чл. 15, ал. 2 и ал. 7 на Закона за киберсигурност, за изпълнение на дейностите посочени в чл. 15, ал.3 и ал. 4 на този закон. Независимо че горепосочените проекти съдържат дейности по обучение на персонала, Центърът за обучение по настоящата

	процедура не надгражда съществуващ такъв, а поставя основите на изцяло нов модел на обучение, какъвто не съществува и не е развиван в публичния и частния сектор. Моделът на обучение ще бъде първият в България, разработен по този проект, с авторско право, собственост на дирекция "Мрежова и информационна сигурност" на Министерство на електронното управление.
Очаквани резултати	В резултат от изпълнението на предвидените дейности по настоящата процедура се очаква да бъдат постигнати следните резултати: - ***Изграден*** и ***функциониращ център за обучения,*** който позволява провеждането на учения и обучения за повишаване на капацитета и развитие на професионални компетентности в областта на киберрисковете и превенция срещу кибервъздействия и противодействия, на всички служители на субектите по киберсигурност. Симулационната среда за казуси от различно естество ще разкрие отговори за адекватна и навременна реакция при кибервъздействие, ще повиши общата осведоменост и разбиране на възможните директни и индиректни последствия от кибервъздействия и същевременно ще предостави нови възможности за изчерпателни анализи на различните ситуации и предприемане на нов комплекс от мерки и регулаторни рамки за борба за киберпрестъпността. - ***Повишаване административния, организационен и технически капацитет и способности на компетентните структури в условията на киберзаплаха/кибератака*** чрез установяване на ефективен механизъм за споделяне на информация и способности, в това число и колективен отговор и обмен на информация в различни ситуации. Дейностите по настоящата процедура ще изградят нова база и среда за обучение, посредством която ще се повиши капацитета и способностите на органите за противодействие, разкриване, разследване, санкциониране на престъпни дейности в киберпространството, и същевременно ще подсилят ефективното взаимодействие между всички заинтересовани страни (публични и частни) от националната система за киберсигурност. - **Приложени *препоръки*** от докладите на Агенцията на Европейския съюз за киберсигурност (ENISA) и CERT на институциите, органите и агенциите на ЕС (CERT-EU), Европейска сметна палата. Прилагайки тези препоръки ще се намали риска от компрометиране от злонамерени кибердейности, и значително ще се подобри сигурността и цялостната устойчивост срещу кибератаки.
Продължителност на процедурата	2023 – 2025 г.
Териториален обхват	*Дейностите по настоящата процедура следва да бъдат изпълнени на територията на Република България.*
Бюджет (ЕФРР и национален)	**Общият размер на безвъзмездната финансова помощ е 1 955 830 лева (1 000 000 евро), в т.ч. за:** • по-слабо развити региони - 1 629 206,39 лева (833 000 евро); • региони в преход (ЮЗР) – 326 623,61лева (167 000 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 Дирекция „Мрежова и информационна сигурност“ към Министерство 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, 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“
Изисквания към партньори *(ако е приложимо)*	Изпълнителна агенция „Инфраструктура на електронното управление“
Допустими дейности	1. Изграждане и оборудване на център за обучение като елемент на националната система за киберсигурност за служители на субектите по киберсигурност. 2. Внедряване и интегриране на обслужващи софтуерни платформи в обучителния център. 3. Разработване на програми и материали за работа на обучителния център. 4. Провеждане на обучения.
Допустими разходи	1. Разходи за оборудване, необходимо за изграждането и функционирането на обучителния център. (материални активи). 2. Разходи за софтуер и лицензи, необходим за изграждането и функционирането на обучителния център (нематериални активи). 3. Разходи за услуги, необходими за изграждането и функциониране на обучителния център, консултантски услуги за разработване на обучителни програми и материали. 4. Разходи за провеждане на обученията. 5. Разходи за текущи строително-монтажни работи във връзка с изграждането на независимо функциониращ обучителен център по системата за киберсигурност. 6. Разходи за персонал (възнаграждения на лица, пряко ангажирани с дейности по изпълнението на проекта, включително задължителните социални и здравни осигурителни вноски за

	сметка на осигурителя, съгласно националното законодателство, вкл. за постигнати резултати.) 7. Непреки разходи за организация и управление на проекта (разходи, които са свързани с изпълнението на проекта, не допринасят пряко за постигането на неговите цели и резултати, но са необходими за неговото цялостно администриране, управление, оценка и добро финансово изпълнение, както и разходите за видимост, прозрачност и комуникация).
Минимален размер на помощта	Неприложимо
Максимален размер на помощта	1 955 830 лева (1 000 000 евро)
Интензитет на помощта	100 %
Продължителност на проектите	18 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	Индивидуални за процедурата индикатори за изпълнение: Изграден и функциониращ обучителен център към националната система за киберсигурност **Показатели за резултата:** Процедурата косвено допринася за изпълнението на следните индикатори за резултат 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