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	**Изграждане на киберсигурна среда за уязвими обществени и бизнес организации (CS4)**
Цел	Целта на процедурата е повишаване на киберсигурността и устойчивостта в уязвими обществени и бизнес организации, определени като съществени и важни субекти по смисъла на Директива (ЕС) 2022/2555 (NIS2) чрез прилагане на система за оценка на киберрисковете и позволяваща формулиране на препоръки за въвеждане и подобряване на мерки за киберсигурност.
Обосновка	**Правна рамка** Директива (ЕС) 2022/255 (Директива МИС2) на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерките за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 има за цел да осигури **високо общо ниво на киберсигурност в Европейския съюз чрез**

	въвеждане на общи мерки за управление на киберрискове, задължения за докладване на инциденти и засилено сътрудничество между държавите членки. С разширяването на обхвата на Директивата МИС2 значително се увеличава броят на организациите, подлежащи на регулаторните изисквания. Това налага повишаване на техния капацитет за оценка на риска и изграждане на устойчиви механизми за управление на киберсигурността. Съгласно чл. 21 от Директива МИС2, държавите членки следва да гарантират, че съществените и важните субекти предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи, които използват при предоставянето на услуги. Тези мерки целят предотвратяването или свеждането до минимум на въздействието на инцидентите върху получателите на услугите. Мерките трябва да бъдат съобразени със съвременните технологии, приложимите стандарти и добри практики в областта на киберсигурността. При спазване на принципа на технологична неутралност и като се вземат предвид последните постижения в областта на киберсигурността, когато е приложимо, съответните европейски и международни стандарти и разходите за прилагането им, чрез предприетите мерки за управление на риска, се гарантира ниво на сигурност на мрежовите и информационните системи, съответстващо на вида и степента на риска. При оценката на пропорционалността на тези мерки следва да се вземат предвид степента на излагане на рискове, размерът на субекта, вероятността от възникване на инциденти, както и тяхната значимост, включително обществено и икономическо въздействие. Мерките следва да се основават на подход, обхващащ всички видове заплахи и тяхната цел е да защитят мрежовите и информационните системи, както и физическата среда от инциденти. Те включват: политики за анализ на риска и сигурност на информационните системи, процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността и задължения за докладване на инциденти. Министерството на електронното управление (МЕУ) е определено за национален орган по киберсигурност в Република България съгласно Закона за киберсигурност (ЗКС) и изпълнява функциите на Национално единно звено за контакт (НЕЗК). Съгласно Директива МИС2 секторните национални компетентни органи (НКО) следва да изготвят ежегодна оценка на риска, включваща икономическия и социалния ефект за съответния сектор, която докладват на НЕЗК. Въз основа на анализите, НЕЗК изготвя

	годишен обобщен доклад за оценка на риска, който отразява състоянието на киберсигурността на национално ниво. **Дейности** Интервенциите по настоящата процедура се предвижда да финансират 1) разработване на методика за оценка на риска и методика за оценка нивото на зрялост на киберсигурността на съществени и важни субекти, 2) създаване на ефективна система за оценка на киберрисковете в организациите и 3) провеждане на информационни кампании и обучения за придобиване на познания и умения с цел идентифициране и оценка на киберрисковете и тяхното въздействие върху услугите, предоставяни от субектите. *Създаване на платформа за оценка на риска* Основната цел на процедурата ще се изпълни чрез предоставяне на национална платформа, която да служи като технологичен инструмент за подпомагане изготвянето на оценка на риска на ниво организация (съществени и важни субекти) за предоставяне на индивидуализирани препоръки и осигуряване съответствие с приложимите нормативни изисквания за укрепване на киберсигурността в публичния сектор и бизнеса. Платформата ще предостави възможност за създаване на отделни „тенанти“ (виртуални защитени среди за работа) на организациите от публичния и частния сектор. Всеки тенант ще бъде изолирана, защитена и индивидуализирана среда, в която съответната администрация или организация ще може самостоятелно да извършва идентификация на активите си, анализ и оценка на рисковете, генериране на препоръки и планове за действие, без достъп до данните на други потребители. Така се гарантира високо ниво на защита на данните и гъвкавост при управлението на риска според особеностите на всяка администрация/организация. *Разработване и утвърждаване на методики* В рамките на процедурата ще бъде разработена специализирана методика за оценка на риска. Разработването и прилагането на специализирана методика за оценка на риска, базирана на индустриални стандарти като ISO 27001 и NIST SP 800-53 може да бъде осъществено чрез структуриран и интегриран процес, който комбинира както стратегическо, така и техническо ниво на управление на киберрисковете. Въз основа на индустриалните стандарти като ISO 27001 (международен стандарт за внедряване на цялостна система за управление на сигурността на информацията, фокусиран върху идентифицирането, оценката и управлението на рисковете за процесите за обработка на информация) и NIST (особено NIST SP 800-53 за контроли на сигурността) се предвижда да се осигури възможност да бъдат следвани добри практики, които могат да бъдат адаптирани към

	специфичните нужди на различни организационни и индустриални контексти. Процесът на създаване и прилагане на специализирана методика за оценка на рисковете ще повиши нивото на киберсигурност в публичния и частния сектор и ще осигури структурирана основа за добро управление на рисковете. Това ще доведе до висока устойчивост на организациите към киберзаплахи и ще подобри тяхната готовност за реакция при киберинциденти, като същевременно ще се осигури съответствие с международните и местни регулации. Ще бъде разработена методика за оценка на нивото на зрялост на киберсигурността, базирана на международни стандарти NIST и ISO 27001, както и на анализи и доклади на ENISA и достъпни източници с отворени данни. Методиката ще помогне за идентифициране на уязвимости и ключови заплахи, определяне на приоритети за подобряване на защитата, повишаване на устойчивостта и готовността за реакция при киберинциденти. Методиките ще бъдат утвърдени от Министъра на електронното управление и ще имат задължителен характер, като изпълнението на мерките, получени в резултат на тяхното прилагане ще бъдат проследявани от Националните компетентни органи в съответните сектори. *Провеждане на информационни кампании и обучения* В рамките на процедурата ще бъдат проведени информационни кампании и обучения за прилагане на методиката за оценка на риска и методиката за оценка нивото на зрялост на киберсигурността на съществените и важните субекти, както и за работа с платформата за идентификация на активи, анализ и оценка на риска. Обученията ще бъдат проведени в шестте района на планиране от NUTS-2 -Северозападен, Северен централен, Североизточен, Югозападен, Южен централен и Югоизточен. присъствено или онлайн в зависимост от предварителните проучвания и възможности на заинтересованите страни. Обученията ще бъдат проведени в хибриден формат, за да позволят максимално широко участие на важни и съществени субекти. Служители на дирекция „Мрежова и информационна сигурност“ (МЕУ) ще бъдат обучени за IT одитори с цел изготвяне на анализ за текущото състояние на информационна сигурност. **Демаркация и допълняемост** С реализирането на процедурата ще бъдат осигурени методична рамка и инструментариум с цел прилагане на европейските стандарти в националните практики. Процедурата не се дублира с други национални инициативи и има ясна добавена стойност чрез

	осигуряване на технологична подкрепа и обучение за практическо прилагане. Процедурата има допълващ ефект към процедура BG16RFPR002-2.003 Пилотно укрепване на капацитета на три Национални компетентни органа и три секторни екипи за реагиране при инциденти с компютърната сигурност към тях (CS 3) {по която са сключени два административни договора – с Министерството на енергетиката и с Министерството на здравеопазването} и бъдещата процедура BG16RFPR002-2.013, която ще бъде насочени към други НКО и СЕРИКС, като ще подпомогне конституентите на НКО и СЕРИКС в съответните сектори.
Очаквани резултати	• Предоставена национална платформа за оценка на риска на ниво организация; • Разработена и утвърдена методика за оценка на риска, съобразена с ISO стандарти за управление на риска в информационната сигурност и NIST стандарти; • Разработена и утвърдена методика за оценка на зрелостта • Проведени информационни кампании и обучения на съществените и важните субекти в шестте района на планиране от NUTS-2 – минимум 12обучения (6 присъствени и 6 онлайн), • Обучени служители от ДМИС (МЕУ) за IT одитори – не-по-малко от 12.
Продължителност на процедурата/процедурите	2026 – 2029 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 4 889 584,78 лв. (2 500 005 евро), в т.ч. за: - по-слабо развити региони – 3 934 097,42 лв. (2 011 472,07 евро); - региони в преход (ЮЗР) – 955 487,36 лв.(488 532,93 евро).

	По-слабо развити региони	**Региони в преход**	**Общо**
ОБЩО ЕФРР+	3 934 097,42 лв.	955 487,36 лв.	4 889 584,78 лв.

	национален	2 011 472,07 евро	488 532,93 евро	2 500 005 евро
	ЕФРР	**3 343 982,80 лв.**	**668 841,15 лв.**	**4 012 823,95 лв.**
		1 709 751,26 евро	341 973,05 евро	2 051 724,31 евро
	национален	**590 114,62 лв**	**286 646,21 лв.**	**876 760,83 лв.**
		301 720,81 евро	146 559,88 евро	448 280,69 евро
Режим на държавна/минимална помощ	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 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)	н/п
Допустими проекти/дейности	• Предоставяне на национална платформа за оценка на риска на ниво организация (съществени и важни субекти); • Разработване и утвърждаване на Методика за оценка на риска по ISO стандарти за управление на риска в информационната сигурност и NIST стандарти[1];

[1] Методиките ще бъдат адаптирани към националния контекст и утвърдени от Министъра на електронното управление.

	• Разработване и утвърждаване на Методика за оценка на зрялост на киберсигурността; • Провеждане на информационни кампании и обучения за прилагане на методика за оценка на риска и методика за оценка на зрялост на киберсигурността, както и работа с платформата; • Провеждане на обучения за IT одитори за служители на дирекция МИС (МЕУ).
Допустими разходи	1. Разходи за дълготрайни нематериални активи 2. Разходи за услуги (вкл. разходи, свързани с разработване и утвърждаване на Методика за оценка на риска по ISO стандарти за управление на риска в информационната сигурност и NIST стандарти и за разработване и утвърждаване на Методика за оценка на зрялост на киберсигурността; разходи за услуги за подготовка, организиране и провеждане на информационни кампании и обучения за прилагане на методика за оценка на риска и методика за оценка на зрялост на киберсигурността, както и работа с платформата). 3. Разходи за такси за специализирани обучения на служители на дирекция МИС за IT одитори. 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	4 889 584,78 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. 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	**Показател за резултат:** RCR 11 Потребители на нови цифрови услуги и приложения **Индивидуални за процедурата индикатори** • Национална платформа за оценка на риска – бр. • Методика за оценка на риска - бр. • Методика за оценка на зрялост на киберсигурността - бр. • Проведени обучения в шестте района на планиране от NUTS-2– бр. • Брой служители от дирекция МИС (МЕУ), преминали обучение за IT одитор – бр.

Съфинансирано от
Европейския съюз

ПРОГРАМА
НАУЧНИ ИЗСЛЕДВАНИЯ,
ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА
ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ