



## 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	<b>Изграждане на елементи от система за киберзащита на споделените информационни ресурси – Етап I</b>
Цел	Интервенцията предвижда финансиране на етап I от изграждането на защитено споделено информационно пространство на електронното управление (ЗСИПЕУ) – като мярка за въвеждане на система за киберзащита на споделени информационни ресурси за електронно управление. Защитените споделени ресурси за е-управление се използват от администрациите и техни звена за предоставяне на електронни административни услуги на гражданите и фирмите. Като централизирана политика за прилагане на универсален и всеобхватен подход за защитата на данните и създаването на добавена стойност от процеса на дигитализация, споделените ИКТ ресурси се стопанисват и поддържат от определена администрация която е отговорна за внедряването на иновативни технологии за надграждане и актуализация на базовите елементи от споделената инфраструктура, чрез които да се гарантира централизирано интелигентно управление на информационните и комуникационните ресурси на държавната администрация и електронно управление в условията на ефективна екосистема на киберсигурност.
Обосновка	<p>В стратегическите насоки за развитие на публичния сектор, очертани в Националната програма за развитие - България 2030 и Актуализираната стратегия за развитие на електронното управление в Република България 2019-2025 г., се поставя приоритет върху цифровизацията на услугите и дигитализацията на работните процеси, изискващи използването на споделени информационни ресурси за дигитална трансформация и оптимизация на дейността на администрациите.</p> <p>Очакван резултат глобални процеси в Европа върху основополагащи елементи от бизнеса и живота на гражданите, като свободното придвижване на хора, стоки и услуги (предвид логистичните затруднения и особеностите на някои производствени сфери) е задълбочаващият се процес на цифровизация както във фирмите, позволяващ отдалечена работа от дома и прилагане на инструменти за образование, обучение, изследване на икономически възможности, предприемачество и реализация на продукцията, така и в администрациите – по отношение на организацията на вътрешните работни процеси и най-вече предоставянето на по-сигурни и разнообразни електронни административни услуги.</p>



В контекста на критично нарасналия виртуален обмен на информация, защитеността на информационните системи и опазването на сигурността на личните и служебни данни става все по-важна. И частният и публичният сектор инвестират средства и усилия за осигуряване на висока защитеност на своите ИКТ (информационни и комуникационни технологии) ресурси. А по-високата киберзащитеност от своя страна повишава доверието в продуктите и услугите и това още повече активизира обмена на данни.

Работата от разстояние и увеличеният обем на обмен на служебна информация извън споделената инфраструктура на публичните институции създадоха както необходимост от централизиран подход за защитата на тази информация, така и гарантираност на процесите по нейната обработка и съответно въвеждането на инструменти за осигуряване на надеждни качествени електронни услуги, предоставяни от администрациите.

Изграждането на защитено споделено информационно пространство на електронното управление (ЗСИПЕУ) се превръща в приоритетна задача за България предвид новите модели за управление на бизнеса и процесите в живота на гражданите. Настоящата процедура е първи етап - въвеждане на централизирано управление и ефективно използване на споделени информационни ресурси на администрациите.

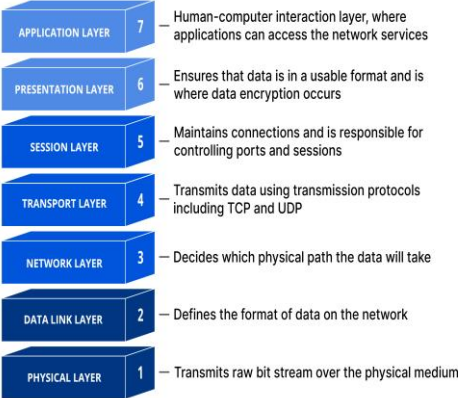
Взаимодействието между две и повече администрации, както и вътре в администрациите с териториално разсредоточени административни структури се осъществява чрез външни интернет доставчици, изграждат се частни виртуални мрежи. Към момента споделените ресурси на електронното управление използват най-вече централизирана организация, базирана на технологии като защитени облачни среди и софтуерно-дефинирани мрежи. Например Държавният хибриден частен облак (ДХЧО) предоставя достъп до хоризонтални и централизирани системи на електронното управление услуги по децентрализиран и специфичен за всеки конкретен случай сценарий, а не по общоприет такъв.

Едно от решенията за повишаване на защитеността и на личните данни, и на бизнес сделките, е интегрираният подход за защита на публичните информационни ресурси – критичната ИКТ инфраструктура, съчетана с централизиран национални и Европейски политики и внедряването на цялостни решения, използващи добри практики от целия свят. ЗСИПЕУ ще позволи да се наложат по най-ефективен начин централизиран автоматизирани политики за достъп и сигурност, да се унифицират и стандартизират процесите и процедурите за мониторинг на общото състояние на споделените информационни ресурси на електронното управление, както и да се предприемат координирани мерки за превенция и възстановяване на данни и системи.

Надграждането на защитните механизми в ДХЧО и Защитения интернет възел (ЗИВ) за да функционират като базови елементи от ЗСИПЕУ съществено ще минимизира рисковете за информационните ресурси на публичния сектор. Предвижда се като следваща стъпка в рамките на действието да се инвестира в следващите базови елементи на ЗСИПЕУ – Единната електронна съобщителна мрежа.

Стъпвайки върху вече изградена физическа и виртуална инфраструктура с финансовата помощ на националния бюджет, Оперативна програма „Добро управление“, Националния план за възстановяване и устойчивост, Фонд „Вътрешна сигурност“, Механизъм Свързана Европа и в допълнение на инвестициите по други действия от Приоритет 2, конкретният бенефициент има амбицията да изгражда по интегриран подход различните слоеве от всеобхватната система за мрежова и информационна сигурност.



	<p>Предвидената по настоящата интервенция ще бъде насочена към ниво 6 „Презентационен слой“ (Level 6 “Presentation layer”) от Модела за взаимно свързване на отворени системи (Open Systems Interconnection Model - OSI<sup>1</sup>).</p> <p>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.</p>  <p>The diagram illustrates the seven layers of the OSI model, numbered 1 to 7 from bottom to top:</p> <ul style="list-style-type: none"> <li><b>7 APPLICATION LAYER</b> – Human-computer interaction layer, where applications can access the network services</li> <li><b>6 PRESENTATION LAYER</b> – Ensures that data is in a usable format and is where data encryption occurs</li> <li><b>5 SESSION LAYER</b> – Maintains connections and is responsible for controlling ports and sessions</li> <li><b>4 TRANSPORT LAYER</b> – Transmits data using transmission protocols including TCP and UDP</li> <li><b>3 NETWORK LAYER</b> – Decides which physical path the data will take</li> <li><b>2 DATA LINK LAYER</b> – Defines the format of data on the network</li> <li><b>1 PHYSICAL LAYER</b> – Transmits raw bit stream over the physical medium</li> </ul>
<p>Очаквани резултати</p>	<p>В резултат от изпълнението на предвидения проект по настоящата процедура се очаква да се изградят базови елементи от ЗСИПЕУ с инструменти за защитена комуникационна свързаност, предпазваща от отпадания на услугата и инциденти с информационните системи, както и възможност за работа в защитени мрежи.</p>
<p>Продължителност на процедурата/процедурите</p>	<p>2023 – 2025 г.</p>
<p>Териториален обхват</p>	<p>Дейностите по настоящата процедура следва да бъдат изпълнени на територията на Република България.</p>
<p>Бюджет (ЕФРР и национален)</p>	<p>Общият размер на безвъзмездната финансова помощ е 21 514 130 лв. (11 000 000 евро), в т. ч.:</p> <ul style="list-style-type: none"> <li>• по-слабо развити региони – 17 308 117,58 лева (8 849 500 евро)</li> <li>• региони в преход (ЮЗР) – 4 206 012,42 лева (2 150 500 евро)</li> </ul>
<p>Режим на държавна/минимална помощ</p>	<p>Неприложимо</p> <p>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</p>

<sup>1</sup> <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>



	<p>положение на определени предприятия или производството на някои стоки, доколкото засяга търговията между държавите-членки, е несъвместима с вътрешния пазар“.</p> <p>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.</p> <p>Конкретният бенефициент е административен орган (второстепенен разпоредител с бюджет към министерство – също административен орган). При предоставянето на финансовите средства по планираната процедура 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.</p>
<p><b>2. Методология и критерии за подбор на операции</b></p>	
<p>Вид процедура за предоставяне на безвъзмездна финансова помощ</p>	<p>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).</p>
<p>Допустими кандидати</p>	<p>Изпълнителна агенция „Инфраструктура на електронното управление“ (ИА ИЕУ),</p> <p>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.</p> <p>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. ЗСИПЕУ, Агенцията е определена за конкретен бенефициент по настоящата процедура.</p>
<p>Изисквания към партньори</p>	<p>Неприложимо</p>
<p>Допустими проекти/дейности</p>	<ol style="list-style-type: none"> <li>1. Изграждане на защитено споделено информационно пространство на електронното управление /ЗСИПЕУ/ чрез внедряване и интегриране на базови елементи, включително системи за гарантиран обмен на информация, контрол и управление на информационни ресурси, обезпечаване на комуникационна свързаност и защита на публични споделени информационни ресурси.</li> <li>2. Интегриране на информационната инфраструктура на първите конституенти към ЗСИПЕУ от централната и териториалната администрация).</li> </ol>



Допустими разходи	<ol style="list-style-type: none"><li>1. Разходи за оборудване, необходимо за изграждането и функционирането на защитени базови елементи от ЗСИПЕУ, които се намират в ДХЧО и ЗИВ (материални активи).</li><li>2. Разходи за софтуер и лицензи, необходими за изграждането и функционирането на защитени базови елементи от ЗСИПЕУ, които се намират в ДХЧО и ЗИВ (нематериални активи).</li><li>3. Разходи за услуги, необходими за изграждането и функциониране на защитени базови елементи от ЗСИПЕУ, които се намират в ДХЧО и ЗИВ.</li><li>4. Разходи за ограничени строително-монтажни работи във връзка с гарантираното функциониране на защитените базови елементи от ЗСИПЕУ, които се намират в ДХЧО и ЗИВ.</li><li>5. Разходи за участие на служители на бенефициента в специализирани обучения, отговарящи за поддръжката на базовите елементи от ЗСИПЕУ.</li><li>6. Разходи за персонал (възнаграждения на лица, пряко ангажирани с дейности по изпълнение на проекта, включително задължителни социални и здравни осигурителни вноски за сметка на осигурителя, съгласно националното законодателство).</li><li>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).</li></ol>
Минимален размер на помощта	Неприложимо
Максимален размер на помощта	21 514 130 лв. (11 000 000 евро)
Интензитет на помощта	100 %
Продължителност на проектите	30 месеца
Кръстосано финансиране (ако е приложимо)	Неприложимо
Критерии за подбор/ оценка на съответствието	<ol style="list-style-type: none"><li>1. Проектното предложение допринася за постигане на специфичната цел на Приоритет 2, целите на настоящата процедура и на Програмата.</li><li>2. Предвидените дейности се изпълняват по недискриминационен и прозрачен начин.</li><li>3. Предвидените дейности не са в противоречие с принципите на чл. 9 от Регламент 2021/1060.</li><li>4. Проектното предложение демонстрира ясна връзка между цели, дейности и резултати.</li><li>5. Всички дейности по проекта са допустими, ясно и последователно описани, посочени са причините за избор на всяка дейност и е показан нейният принос за постигане на очакваните общи резултати.</li><li>6. Планът за изпълнение на дейностите е реалистичен и е съобразен с плана за външно възлагане.</li><li>7. Планът за външно възлагане е в съответствие с предвидените дейности; кандидатът е предвидил механизми, позволяващи мониторинг и текущ</li></ol>



	<p>контрол на изпълнението на предвидените поръчки и своевременното предприемане на корективни мерки.</p> <p>8. В проектното предложение са описани начините, чрез които ще се осигури устойчивостта на резултатите и ефекта от изпълнението на проекта.</p> <p>9. 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.</p> <p>10. Всички разходи, включени в бюджета на проектното предложение съответстват изцяло на предвидените дейности.</p> <p>11. Всички разходи са ефективни, обосновани и допустими съгласно Условието за кандидатстване, като не е налице дублиране на разходи.</p> <p>12. Размерът на исканата безвъзмездна финансова помощ е в съответствие с максималния размер, посочен в Условието за кандидатстване.</p>
Индикатори	<p>Индивидуален за процедурата показател:</p> <p>Конституенти от централната и териториалната администрация с инфраструктура, интегрирана към базовите елементи на защитеното споделено пространство за е-управление – брой</p> <p><b>Показатели за резултата за действие CS5:</b></p> <p>SR 20 Публични организации, обхванати от системата за киберсигурност</p>