

МИДТ

Рег. № 02-02-12-1/18.06.2026



НАРОДНО СЪБРАНИЕ	
Вх. №	52-654-06-288
Дата	18.06.2026

19.06
1906

РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

ЧРЕЗ

Г-ЖА МИХАЕЛА ДОЦОВА

ПРЕДСЕДАТЕЛ

НА НАРОДНОТО СЪБРАНИЕ НА РЕПУБЛИКА БЪЛГАРИЯ

ДО

Г-Н БОЖИДАР БОЖАНОВ

НАРОДЕН ПРЕДСТАВИТЕЛ

ОТ ПГ НА „ДЕМОКРАТИЧНА БЪЛГАРИЯ“

На Ваш № 52-654-06-288/08.06.2026 г.

ОТНОСНО: Проблеми при проекти за киберсигурност

УВАЖАЕМА ГОСПОЖО ПРЕДСЕДАТЕЛ,

УВАЖАЕМИ ГОСПОДИН БОЖАНОВ,

Детайлната информация относно всички изпълнявани проекти с европейско финансиране, включително по Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027 (ПНИИДИТ), е публична и свободно достъпна чрез Инфорционната система за управление и наблюдение на средствата от Европейския съюз в България 2020 (ИСУН 2020). Конкретно за посочения от Вас проект № BG16RFPR002-2.018-0001-C01 и наименование „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността“ (проекта), по процедура BG16RFPR002-2.018 „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността“ на програма ПНИИДИТ, информацията е налична на следния електронен адрес:



РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

<https://2020.eufunds.bg/bg/8010851/0/Project/BasicData?contractId=hhdwc4IeVnseDbU5yxkmgw%3D%3D&isHistoric=False>

При изпълнение на проекта са реализирани общо седем открити процедури по Закона за обществените поръчки (ЗОП). Този тип процедури предвиждат най-широки възможности за участие на всички заинтересовани икономически субекти и създават най-благоприятните възможни условия за свободна конкуренция, равнопоставеност публичност, прозрачност и недопускане на дискриминация. За изпълнението на проекта не са предвиждани и не са реализирани друг тип процедури по ЗОП. Цялата информация относно проведените открити процедури, осъществения предварителен контрол и процеса по конкурентен избор на изпълнителите е налична в Централизираната автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП).

Предвид размера на прогнозната стойност на обществените поръчки, същите са обект на задължителен предварителен контрол от страна на Агенцията по обществени поръчки. По всички седем публикувани процедури за провеждане на открити обществени поръчки становището на компетентния орган е „Не са установени несъответствия с изискванията на ЗОП“. Становищата са публикувани в документацията към съответната процедура.

Подходът на възлагащия орган при реализирането на проекта залага на пълна публичност на техническите спецификации. Цялата документация, включително техническите спецификации, могат да бъдат открити в ЦАИС ЕОП в тяхната цялост, така че всяка заинтересована страна може да се запознае с пълния обем на търсените и доставени продукти, услуги и решения.

Също така показателен е и фактът, че нито една от обществените поръчки не е обжалвана нито по отношение на документация, обхват и изисквания, нито по отношение на процеса на избор на изпълнител. Наличието на множество кандидати, дългогодишни широко разпознаваеми участници - утвърдени в сектора български компании, също е индикатор за благоприятните условия и създадената пазарна конкуренция при избора на изпълнители.

Създадената високо конкурентна среда и доказаната липса на нарушения в процедурите гарантират високата прозрачност и ефективност на разходите по проекта, което изключва твърдението за „съмнителна прозрачност и ефективност на разходите“.

По отношение на участието на системния интегратор по Закона за електронното управление в планирането и реализирането на проекта следва да се има предвид, че предвид обстоятелството, че „Информационно обслужване“ АД не участва в изпълнението на проекта като доставчик на необходимото оборудване за реализация на националната система за киберсигурност, не би могло да се твърди, че неговата роля в изпълнението на проекта е основна. Целият цитиран от Вас проект се реализира на база на взети решения от



РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

Съвета по киберсигурността към Министерския съвет (Съвет). Решенията на Съвета обуславят централизиране на планирането и осигуряването на решения за киберсигурност за административните органи чрез Министерство на електронното управление и използване на вече изградения и наличен държавен капацитет в областта на киберсигурността на националния системен интегратор по чл. 7с от Закона за електронното управление (ЗЕУ), държавното дружество „Информационно обслужване“ АД. Моделът на използване на притежавани от държавата дружества за целите на изпълнението на публични политики е утвърден и се прилага в множество държави-членки на Европейския съюз. Специално по отношение на ролята на „Информационно обслужване“ АД в електронното управление и киберсигурността в България и правния статут на системен интегратор, са потвърдени изрично с решение на Европейската комисия от 4 юни 2026 г. като не нарушаващи европейската рамка за обществени поръчки.

Министерството на електронното управление и системният интегратор са работили съвместно и прозрачно за цялостната подготовка и последваща реализация на проекта. Ролята на държавното дружество за целите на проекта е детайлно представена на отговорните европейски служби още на етап обсъждане на методологията и критериите за подбор на операции по процедурата. По време на заседания на проведените Комитети за наблюдение също е посочена ролята и обхвата на дейността на „Информационно обслужване“ АД. Следва отново изрично да се отбележи, че обществените поръчки за реализацията на проекта не са възложени от или за изпълнение на системния интегратор.

Същевременно капацитетът на държавното дружество в областта на киберсигурността е неоспорим. За последните години извън обхвата на цитирания от Вас проект и по реда на системната интеграция по чл. 7с от ЗЕУ чрез системния интегратор е осигурена киберсигурността на повече от 19 000 работни места и над 550 сървъра в държавната администрация. Договорите по системна интеграция са публично достъпни на интернет страницата на системния интегратор <https://is-bg.net/bg/system-integrator/data/>. Екипът за киберсигурност на държавното дружество включва 44 високо квалифицирани специалисти с експертиза, доказан опит и комбинация от различни международно признати сертификати в областта на киберсигурността.

Във връзка с конкретно поставените от Вас въпроси, информация за изпълнението и разплащането по проекта е публично достъпна в ИСУН 2020. Видно от публикуваната информация, целият проект не е разплатен. Следва да обърнете внимание, че датата на приключване на проекта е 06.11.2027, т.е. до неговия край има повече от 16 месеца, и проектът е все още в процес на изпълнение.

Ефективността на проекта, както и постигането на заложените цели и индикатори се оценяват и измерват текущо, при настъпване на междинни срокове или при цялостното



РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

приключване на проекта. Към настоящия момент проектът е в изпълнение от 8 месеца при общо 24 месеца срок за неговата реализация.

Процесът на внедряване на доставените информационни ресурси и услуги започва още през януари 2026 г. проектът все още се изпълнява и продължителността е две години, т.е. все още инсталираме лицензи и бройката се променя.

Необходимо е да имате предвид, че изпълнението на проекта към момента щеше да бъде в много по-напреднала фаза, ако същият не беше на практика блокиран за периода на управление на служебното правителство (февруари-май 2026 г.). През този период не е налице никакъв напредък по практическото изпълнение и имплементиране на ключовите негови дейности в резултат на практическото блокиране на изпълнението от служебния министър на електронното управление и представителите на неговия политическия кабинет. Към момента тече процесът по подписване на Общите условия и параметри за предоставяне на услуги за киберсигурност (Общи условия), утвърдени със Заповед № МЕУ-1029/23.01.2026 на министъра на електронното управление. Този документ дефинира условията и параметрите на услугите, нивата на обслужване, отговорностите и процедурите за управление и наблюдение на киберсигурността на информационно-комуникационната инфраструктура (ИКИ) на съответния конституент по проекта. Документът обхваща услугите, извършвани чрез информационни ресурси, предоставени безвъзмездно на съответния конституент чрез подробен приемо-предавателен протокол, които осигуряват изпълнението на технологичните нормативни изисквания за мрежова и информационна сигурност.

Реализирането на проекта е в резултат на надлежно взети решения от страна на Съвета, като същият е приел технологична архитектура за киберсигурност на високо ниво, която за първи път детайлизира техническите и технологични елементи на организационната и процесна архитектура на киберсигурността на национално ниво, свързана с Националния екип за реагиране при инциденти с компютърната сигурност (НЕРИКС), секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС), конституентите и мрежата за обмена на информация между заинтересованите страни. Приемането на тази технологична архитектура е създала условията за въвеждането на единен общ подход за развитие на киберсигурността на национално ниво и за първи път операционализира и конкретизира като модел обхвата на системата за киберсигурност. Идентифицираните мерки и инициативи, в тяхната взаимна обвързаност и приоритетност, са заложили и планирани за реализиране в обхвата на няколко действия към Приоритетно направление 2 Киберсигурност, Приоритет 2 на ПНИИДИТ.

Съществена слабост на прилагания през годините подход е липсата на целенасочено национално планиране на наличния ограничен финансов ресурс и свързаните с това



РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

слабости при бюджетиране на залаганите мерки – при планиране „на парче“ не могат да бъдат постигнати ефектите от мащаба и не са адекватно приложени принципите на ефективност, ефикасност и икономичност. Отговорността за развитие на способности, компетенции и осигуряване на информационни ресурси е на всеки отделен административен орган, но този подход не е довел до систематично планиране и координация на дейностите между администрациите.

С реализирането на проекта, чрез избирането на централизацията на подхода обхваща планиране и осигуряване на капацитет и ресурси, като по този начин се осигурява прилагането на комплексен подход при изграждане на системата за киберсигурност. Подходът е практическата реализация на механизма на делегиране на технически и организационни мерки на други участници в мрежата за киберсигурност съгласно съществуващите нормативно регламентирани функции и компетенции на отговорната администрация, която изпълнява функциите на НЕРИКС, СЕРИКС на публичната администрация, и функциите на министъра, който осъществява координация и контрол в областта на киберсигурността по отношение на административните органи, което от своя страна допринася за по-голяма ефективност при изпълнението на предвидените мерки.

С реализирането на проекта ще бъде налице пълният набор от необходими технологии и решения, свързани с мониторинг на киберсигурността – ще бъдат обхванати най-критичните административни органи на централно и областно,. Проектът осигурява приоритетните идентифицирани потребности по отношение на НЕРИКС и СЕРИКС в областта на откриване на киберзаплахи, откриването на уязвимости и атаки на повърхността.

В допълнение на горното и в изпълнение на решенията на Съвета е извършено проучване и анализ на реалното текущо състояние на наличната инфраструктура и нужди на административните органи на централно ниво, на база на който се извършва както приоритизация на административните органи, които предстои да бъдат обхванати от националната система за киберсигурност, така и обхвата на необходимата интервенция. Анализът детайлизира конкретно нуждите спрямо приетия архитектурен модел и обуславя конкретния обхват на проекта за постигане на синергичен ефект, както и за оптимизация на предвидените разходи – постигане на максимален обхват с разполагаемия финансов ресурс.

Приоритизираниите административни органи са утвърдени с решения на Съвета по киберсигурността, а тяхната роля е такава каквато е предвидено да бъде в Закона за киберсигурност. Относно включените минимум 50 административни органа не се променят техните задължения, уредени в закона, напротив осигурява се ресурс за постигане на високо ниво на мрежова и информационна сигурност и защита на 30 000 крайни устройства и сървъри. Обхватът на проекта включва и необходими решения за НЕРИКС, СЕРИКС, Националния киберситуационен център, Национална мрежа на екипи, свързани със



РЕПУБЛИКА БЪЛГАРИЯ
МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

сигурността, като ще бъде изградено и защитеното споделено информационно пространство, част от споделените информационни ресурси на електронното управление. Предвид множеството ограничителни фактори и текущи проблеми пред системата за киберсигурност, изграждането на централните компоненти, защитеното споделено информационно пространство и повишаването на нивата на киберсигурност на ключови административни органи на централно ниво не само предполагат, но и налагат интегрирани действия за оптимално постигане на целите.

X **Ivan Rumenov**
Vasilev

Digitally signed by Ivan
Rumenov Vasilev
Date: 2026.06.18
16:22:02 +03'00'

ИВАН ВАСИЛЕВ

МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ